

РОССИЙСКАЯ АКАДЕМИЯ НАУК
Федеральный исследовательский центр «Информатика и управление»
(ФИЦ ИУ РАН)

На правах рукописи

МИЛОСЛАВСКАЯ Наталья Георгиевна

**ПОСТРОЕНИЕ ЦЕНТРОВ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ В
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ**

ДИССЕРТАЦИЯ

на соискание ученой степени доктора технических наук

по специальности

05.13.19 «Методы и системы защиты информации, информационная безопасность»

Научный консультант
Доктор технических наук,
Академик Академии криптографии РФ
Будзко В.И.

Москва – 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	7
ГЛАВА 1. АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ.....	27
1.1. Анализ информационно-телекоммуникационной сети как основного объекта защиты в едином информационном пространстве организаций.....	27
1.1.1. Особенности современного использования информационно-телекоммуникационных сетей.....	27
1.1.2. Определение информационно-телекоммуникационной сети.....	28
1.1.3. Информационно-телекоммуникационная сеть как симбиоз телекоммуникационной и информационной сетей	30
1.1.4. Информационные ресурсы информационно-телекоммуникационной сети и среда их обработки ..33	
1.1.5. Логическая структура информационно-телекоммуникационной сети	35
1.1.6. Информационно-телекоммуникационная сеть как системообразующая структура единого информационного пространства организации	37
1.2. Современные проблемы защиты информации в информационно-телекоммуникационных сетях.....	38
1.2.1. Тенденция возрастания угроз информационной безопасности для информационно-телекоммуникационных сетей.....	38
1.2.2. Задачи обеспечения информационной безопасности для информационно-телекоммуникационных сетей.....	42
1.2.3. Эволюция технологий и средств обеспечения сетевой безопасности	46
1.2.4. Необходимость сложной аналитики данных для обеспечения сетевой безопасности	53
1.2.5. Понятие сетевой безопасности для информационно-телекоммуникационной сети.....	55
1.3. Нормативная и правовая база в области обеспечения информационной безопасности, применяемая к объекту исследования и использованная для разработки глоссария предметной области исследования..	57
1.3.1. Правовая база исследования.....	57
1.3.2. Нормативная база исследования.....	58
1.4. Цель и задачи исследования.....	61
Выводы по главе 1	66
ГЛАВА 2. ТАКСОНОМИЯ УЯЗВИМОСТЕЙ, УГРОЗ, СЕТЕВЫХ АТАК И ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	69
2.1. Таксономия понятий уязвимости, угроз, сетевых атак и инцидентов информационной безопасности	69
2.2. Системная классификация уязвимостей элементов информационно-телекоммуникационной сети...72	
2.3. Системная классификация угроз информационной безопасности информационно-телекоммуникационной сети.....	84
2.4. Системная классификация сетевых атак на информационно-телекоммуникационную сеть	99

2.5. Системная классификация инцидентов информационной безопасности для информационно-телекоммуникационной сети.....	117
Выводы по главе 2.....	129
ГЛАВА 3. ИССЛЕДОВАНИЕ И РАЗРАБОТКА ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И СЕТЕВОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ.....	135
3.1. Понятие обеспечения информационной безопасности информационно-телекоммуникационной сети	135
3.1.1. Понятие процесса и процессного подхода к деятельности организации	135
3.1.2. Определение понятия обеспечения информационной безопасности информационно-телекоммуникационной сети	138
3.1.3. Модель обеспечения информационной безопасности информационно-телекоммуникационной сети	141
3.1.4. Определение понятия обеспечения сетевой безопасности информационно-телекоммуникационной сети	147
3.2. Управление информационной безопасностью информационно-телекоммуникационной сети как часть обеспечения ее информационной безопасности	148
3.2.1. Определение понятия управления информационной безопасностью информационно-телекоммуникационной сети.....	149
3.2.2. Уровни управления информационной безопасностью информационно-телекоммуникационной сети	150
3.2.3. Система управления информационной безопасностью информационно-телекоммуникационной сети	154
3.2.4. Циклическая модель рассмотрения процессов управления информационной безопасностью информационно-телекоммуникационной сети	155
3.2.5. Определение понятия управления сетевой безопасностью информационно-телекоммуникационной сети	158
3.3. Проверка информационной безопасности информационно-телекоммуникационной сети как средство постоянного контроля общего управления информационной безопасностью организации	160
3.3.1. Определение понятия мониторинга информационной безопасности информационно-телекоммуникационной сети.....	162
3.3.2. Взаимосвязь процессов мониторинга и аудита информационной безопасности информационно-телекоммуникационной сети.....	167
3.3.3. Взаимосвязь процессов мониторинга и управления инцидентами информационной безопасности в информационно-телекоммуникационной сети	168
3.4. Разработка процесса управления инцидентами информационной безопасности для информационно-телекоммуникационной сети.....	170
3.4.1. Задачи процесса управления инцидентами информационной безопасности	170
3.4.2. Нормативная база управления инцидентами информационной безопасности.....	171
3.4.3. Деятельность в рамках процесса управления инцидентами информационной безопасности	172
3.4.4. Требования к разрабатываемому процессу управления инцидентами информационной безопасности	179

3.4.5. Формализация разработанного процесса управления инцидентами информационной безопасности	181
3.4.6. Разрабатываемый Центр интеллектуального управления сетевой безопасностью как фундамент системы управления инцидентами информационной безопасности для информационно-телекоммуникационной сети	212
Выводы по главе 3	213
ГЛАВА 4. КРИТИЧЕСКИЙ АНАЛИЗ СУЩЕСТВУЮЩИХ ЦЕНТРОВ И ВЫРАБОТКА ТРЕБОВАНИЙ К ЦЕНТРАМ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ	217
4.1. Понятие SIEM-системы	217
4.2. Эволюция центров управления безопасностью	224
4.3. Центры мониторинга безопасности	225
4.3.1. Цели и задачи Центров мониторинга безопасности	225
4.3.2. Функции SIEM-системы 1.0 в Центрах мониторинга безопасности	228
4.3.3. Классификация Центров мониторинга безопасности	230
4.3.4. Ограниченность Центров мониторинга безопасности	235
4.4. Концепция интеллектуальной безопасности	236
4.5. Центры интеллектуальной безопасности	243
4.5.1. Назначение Центров интеллектуальной безопасности	243
4.5.2. Расширение бизнес-логики функционирования центров мониторинга безопасности для ее применения в Центрах интеллектуальной безопасности	245
4.5.3. SIEM-системы 2.0 в Центрах интеллектуальной безопасности	248
4.6. Модели зрелости Центров управления безопасностью	251
4.7. Формулирование требований к разрабатываемому Центру интеллектуального управления сетевой безопасностью	253
4.7.1. Общие требования к Центру интеллектуального управления сетевой безопасностью	255
4.7.2. Специальные требования к Центру интеллектуального управления сетевой безопасностью	255
4.7.3. Перечень детальных требований к Центру интеллектуального управления сетевой безопасностью	257
4.7.4. Требования по обеспечению информационной безопасности Центра интеллектуального управления сетевой безопасностью	258
Выводы по главе 4	261
ГЛАВА 5. ПОСТРОЕНИЕ ТИПОВОГО ЦЕНТРА ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ ДЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ	264
5.1. Методология построения типового Центра интеллектуального управления сетевой безопасностью	265
5.2. Принципы построения типового Центра интеллектуального управления сетевой безопасностью	271
5.3. Типовой Центр интеллектуального управления сетевой безопасностью как объединение Центра интеллектуальной безопасности и Сетевого операционного центра	273

5.3.1. Сетевой операционный центр	274
5.3.2. Функциональные возможности объединенного типового Центра интеллектуального управления сетевой безопасностью	276
5.3.3. Визуализация информации в типовом Центре интеллектуального управления сетевой безопасностью для принятия решений по управлению инцидентами информационной безопасности в информационно-телекоммуникационной сети	280
5.4. Архитектура типового Центра интеллектуального управления сетевой безопасностью	283
5.4.1. Функциональная архитектура типового Центра интеллектуального управления сетевой безопасностью	283
5.4.2. Архитектура обработки относящихся к информационной безопасности информационно-телекоммуникационных сетей данных в типовом Центре интеллектуального управления сетевой безопасностью	285
5.4.3. Зональная архитектура обеспечения информационной безопасности в типовом Центре интеллектуального управления сетевой безопасностью	299
5.5. Проект SIEM-системы 3.0 для типового Центра интеллектуального управления сетевой безопасностью	312
5.6. Функциональная устойчивость типового Центра интеллектуального управления сетевой безопасностью в едином информационном пространстве организации	323
5.7. Вопросы кадрового обеспечения типового Центра интеллектуального управления сетевой безопасностью	334
5.8. Демонстрация выполнения требований к типовому Центру интеллектуального управления сетевой безопасностью	343
Выводы по главе 5	350
ГЛАВА 6. ВНЕДРЕНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ	356
6.1. Внедрение результатов в Ситуационном центре Газпромбанка	356
6.2. Внедрение результатов в Банке России	361
6.3. Внедрение результатов в компании Qualys	367
6.4. Реализация типового ЦИУСБ в НИЯУ МИФИ	368
6.5. Внедрение результатов в компании «ЛИНС-М»	376
6.6. Внедрение в Федеральном Учебно-методическом объединении в системе высшего образования по укрупненной группе специальностей направления подготовки «Информационная безопасность»	377
Выводы по главе 6	378
ЗАКЛЮЧЕНИЕ	382
СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ	388
СЛОВАРЬ ТЕРМИНОВ	392
СПИСОК ЛИТЕРАТУРЫ	419
СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА	447
ПРИЛОЖЕНИЯ	450
ПРИЛОЖЕНИЕ А АКТ О ВНЕДРЕНИИ в Банке ГПБ (АО)	451

ПРИЛОЖЕНИЕ Б АКТ О ВНЕДРЕНИИ в ЗАО «ЕС-лизинг»	453
ПРИЛОЖЕНИЕ В АКТ О ВНЕДРЕНИИ в компании «Qualys GmbH»	455
ПРИЛОЖЕНИЕ Г АКТ О ВНЕДРЕНИИ в НИЯУ МИФИ.....	456
ПРИЛОЖЕНИЕ Д АКТ О ВНЕДРЕНИИ в ООО «ЛИНС-М»	457
ПРИЛОЖЕНИЕ Ж АКТ О ВНЕДРЕНИИ в Федеральном УМО в СВО по УГСНП «ИБ»	459

ВВЕДЕНИЕ

Актуальность темы исследования. Интенсивное развитие и использование современных информационно-коммуникационных технологий (ИКТ) для обработки цифровой информации привели к серьезным качественным изменениям в экономической, социально-политической и духовной сферах жизни общества. Этот феномен большой зависимости от ИКТ и их резко возрастающего влияния на формирование цифрового общества XXI века был впервые отмечен в «Окинавской Хартии глобального информационного общества», принятой в 2000 г. лидерами «восьмерки» [1]. В 2016 г. в «Доктрине информационной безопасности Российской Федерации» также отмечалось, что эти технологии «приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства» [2].

В России в рамках реализации Указа Президента Российской Федерации № 204 «О национальных целях и стратегических задачах развития Российской Федерации (РФ) на период до 2024 года» [3] была принята Национальная программа «Цифровая экономика Российской Федерации» [4], одна из трех целей которой – «создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств». Для обеспечения ее решения в Национальный проект включен Федеральный проект «Информационная безопасность», который полностью согласуется с направлением обеспечения информационной безопасности (ИБ) в области государственной и общественной безопасности РФ, сформулированным в [2] как «повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации». В основе названной инфраструктуры лежит информационно-телекоммуникационная система [5], которая базируется на информационно-телекоммуникационной сети (ИТКС) – технологической системе (ТС), предназначенной для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (СВТ) [6, статья 2].

Согласно Федеральному закону № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», к объектам критической информационной инфраструктуры (КИИ) относятся ИТКС, информационные системы (ИС), автоматизированные системы управления (АСУ) субъектов КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Субъекты КИИ – государственные органы и учрежде-

ния, российские юридические лица и (или) индивидуальные предприниматели (далее – ОРГАНИЗАЦИЯ), которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в различных сферах деятельности и областях промышленности, а также российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [7, статья 2]. Следовательно, для ИТКС как неотъемлемой части обеспечения деятельности организаций необходимо обеспечить функциональную устойчивость и ИБ их информационных ресурсов и предоставляемых услуг.

В то же время в последнее десятилетие риски нарушения безопасности для объектов КИИ, включая ИТКС ее субъектов, приобрели статус компонентов системного риска. В качестве основных причин данной тенденции можно выделить, в первую очередь, сложность и разнообразность ИТКС разных субъектов по функциям, структуре и организационно-правовым формам, растущую роль различных технологий в предоставлении услуг и все большую зависимость последних от имеющих различные уязвимости ИКТ, усиливающуюся взаимозависимость между всеми участниками информационных взаимодействий, а также рост сложности, широкой направленности и разнообразия компьютерных атак и появление новых категорий злоумышленников и целей, которые они преследуют. Многочисленные ежегодные исследования в области ИБ ИТКС показывают, что стратегии обеспечения ИБ, которые традиционно были основаны на соблюдении нормативных и правовых требований и ограничивались лишь «защитой периметра», не успевают за растущим количеством и все более изощренными методами, применяемыми злоумышленниками. В качестве примеров подобной тенденции можно привести атаки на системы Интернета вещей (англ. *Internet of Things, IoT*) и APT-атак (англ. *Advanced Persistent Threats, APTs*), направленные на цели определенной категории (как правило, делового или политического характера), промышленный шпионаж и кражу бизнес-информации. Часто злоумышленники сначала получают доступ к плохо защищенным серверам и компьютерам пользователей, а затем с них производят атаки на системы по всему миру. Они умеют осторожно тестировать защиту ИТКС, избегая обнаружения, и, найдя уязвимости, используют их для достижения своих целей. Например, прибегают к целевому фишингу (англ. *spear phishing*) в отношении группы пользователей с определенным сходством и, как результат, незаконным путем получают необходимую информацию от сотрудников компаний. Для внедрения вредоносного кода могут использоваться как технические средства, так и социальная инженерия (англ. *social engineering*). Например, статистика атак за 2020 г. от аналитической компании Hackmaggedon показывает, что большинство из них связаны с распространением вредоносного программного обеспечения (ПО) (39,3 %), похищением учетных записей (16,7 %), целенаправленными атаками (10,7 %), внедрением вредоносных скриптов (3,7 %), спамом (1,8 %), DDoS-атаками (англ.

Distributed Denial of Service) (1,7 %), созданием поддельных страниц (1,5 %) и неверных конфигураций (1,1 %) [8].

Одновременно с этим увеличивается число потенциальных точек проникновения в ИТКС, по которым злоумышленники наносят «точечные удары», приводящие к утечке конфиденциальной информации, загрузке приложений через почтовые сообщения, несанкционированному переводу денежных средств и т.д. Системотехническая основа современных ИТКС может включать элементы, которые входят в состав систем общего пользования (систем облачных вычислений, различных хранилищ и центров обработки данных (ЦОД) с множеством ИС и т.п.), что несет повышенную угрозу ее ИБ. Программируемые сети, управляемые ПО, а не аппаратными средствами, обладают рядом уязвимостей, а также создают задержки в обработке трафика управления передачей данных, что позволяет реализовывать компьютерные атаки на уровне ПО. Пятое поколение мобильных сетей (сети 5G), как и любое новшество, кроме пользы содержит в себе множество возможностей, которыми может воспользоваться злоумышленник, и т.п. Проиллюстрируем один аспект незащищенности облачных хранилищ, открывающий путь к атакам и представленный в обзоре за 2020 г. компанией Verizon [9]: 22 % нарушений были связаны с облачными активами, а 43 % – с веб-приложениями, в 71 % зарегистрированных инцидентов были затронуты локальные активы; 70 % атак было совершено внешними нарушителями, организованная преступность имела отношение к 55 % из них; 81 % нарушений были обнаружены в течении нескольких дней или раньше; у 58 % жертв были скомпрометированы личные данные; 86 % нарушений имели финансовые мотивы.

В целях обеспечения ИБ в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, субъект КИИ создает систему безопасности объекта и обеспечивает ее функционирование [7, статья 10]. При этом безопасность КИИ, включающей ИТКС разных субъектов – это состояние защищенности КИИ, обеспечивающее ее функциональную устойчивость при проведении в отношении нее компьютерных атак [7, статья 2]. Наравне с законностью, к принципам обеспечения безопасности КИИ относятся непрерывность и комплексность этого процесса и приоритет предотвращения компьютерных атак [7, статья 4].

Реализуемые в настоящее время реактивные меры обеспечения ИБ для информационных ресурсов ИТКС ОРГАНИЗАЦИЙ с целью минимизации времени их восстановления (длительности реагирования) после прерываний, вызванных инцидентами ИБ, были разработаны два-три десятилетия назад. В 2005-2006 гг. компанией Cisco Systems была впервые озвучена идея разработки центра мониторинга безопасности (ЦМБ) (англ. *Security Operations Center, SOC*) [10-12], которому в русскоязычных публикациях долгое время соответствовали разные термины

типа «система централизованного мониторинга ИБ», или «центр координации деятельности по ИБ» [13], «координирующий центр мониторинга ИБ» или «ситуационный центр мониторинга ИБ» (например, [14, 15]). Основными целями разворачивания ЦМБ Cisco определил управление средствами защиты информации (СЗИ) в сетях (например, виртуальными частными сетями, межсетевыми экранами, системами обнаружения и предотвращения вторжений, системами отражения DDoS-атак, решениями для борьбы с вредоносным кодом, вирусами и шпионскими программами) и мониторинг их состояния в режиме реального времени, а также анализ записей в журналах регистрации событий [16], сведений об уязвимостях, информации о ресурсах и предупреждений об опасности.

В тоже время дальнейшего развития требует качество управления сетевой безопасностью в ЦМБ, поскольку оно существенно отстает от требуемого сегодня уровня – ЦМБ первого поколения не были рассчитаны на сложную корреляцию и аналитику всех происходящих в ИТКС событий в определенном контексте как основы полноценного управления, а не просто мониторинга ИБ. Результатом является неудовлетворительное время обнаружения инцидентов ИБ. К сожалению, единой общемировой статистики по его оценке не существует – данные в отчетах разных исследовательских компаний существенно различаются. Но общие тенденции выявить можно. Так, например, известный в мире ИБ центр Ponemon Institute (США) в отчете 2019 г. отмечает, что компании необходимо в среднем 276 дней (против 197 в 2018 г.) для выявления инцидентов, связанных с утечкой данных [17]. Некоторые исследования показывают, что большинство инсайдерских атак обнаруживаются в течение нескольких минут (22 % опрошенных), часов (28 %) или одного дня (26 %) (Crowd Research Partners 2018 Insider Threat Report, [18]). Другой отчет показывает, что для выявления такого нарушения требуется от нескольких месяцев (30 % опрошенных) до нескольких лет (40 %) (Verizon 2019 Insider Threat Report: Executive Summary, [19]). И это при том, что, согласно Website hacking statistics of 2020 [20], хакеры атакуют каждые 39 секунд, в среднем 2244 раза в день; крадут 75 записей каждую секунду (источник: Breach Level Index); в среднем взламывают 30000 новых веб-сайтов каждый день (источник: Forbes). Они ежедневно создают 300000 новых вредоносных программ (источник: McAfee). 73 % хакеров заявили, что традиционный межсетевой экран и антивирусная защита неактуальны или устарели (источник: Thycotic.com).

Из выше изложенного очевиден вывод, что в настоящее время актуален поиск решения для построения центра управления ИБ для ИТКС (центра управления сетевой безопасностью), за счет которого достигается соблюдение для ИТКС ОРГАНИЗАЦИИ соответствующих требований по обеспечению ее ИБ (например, для субъекта КИИ в соответствии с присвоенной ему категорией значимости [21]). Такое решение обеспечит *информационную защищенность ИТКС ОРГАНИЗАЦИИ* – такую ее способность, при которой в едином информационном пространстве

(ЕИП) ОРГАНИЗАЦИИ создана адекватная защищенная среда функционирования ИТКС, обеспечивающая необходимый уровень ИБ для получения (поиска и сбора), обработки, хранения, распространения (передачи и предоставления) и уничтожения информации. Обобщив определения из [2, 5-7, 22], определим *ИБ ИТКС ОРГАНИЗАЦИИ* как состояние защищенности ТС ОРГАНИЗАЦИИ, предназначенных для обработки и передачи по линиям связи информации, доступ к которой осуществляется с использованием современных информационных технологий (ИТ), СВТ и средств связи, включающее безопасность информационных ресурсов и предоставляемых услуг и обеспечивающее функциональную устойчивость ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ. При этом уровень риска нарушения осуществления деятельности ОРГАНИЗАЦИИ с использованием ИТКС и уровень риска нарушения свойств ИБ информационных ресурсов ИТКС на всех стадиях их жизненного цикла приемлемы как для их пользователя, так и владельца. Защищенность достигается обеспечением совокупности свойств ИБ – конфиденциальности, целостности, доступности, подлинности, подотчетности, неотказуемости и достоверности, приоритетность которых определяется значимостью информации для интересов (целей) ОРГАНИЗАЦИИ.

Требуемое решение должно обеспечить *ИБ ИТКС ОРГАНИЗАЦИИ* на основе предоставления следующих возможностей:

1) консолидированное (единое) управление ИБ ИТКС для недопущения несанкционированных воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование ИТКС;

2) не только предотвращение неправомерных действий (доступ, уничтожение, модифицирование, блокирование и т.п.) с информацией, обрабатываемой ИТКС, но и *упреждающее управление сетевой безопасностью ИТКС*, основанное на принятии решений в отношении возможных инцидентов ИБ до их проявления, направленном на предотвращение и минимизацию их последствий за счет постоянного интеллектуального анализа в определенном контексте всех консолидированных (совместно рассматриваемых и анализируемых) данных о происходящих в ИТКС событиях, имеющих отношение к ИБ, прогнозирования развития ситуации и своевременной установки «барьеров защиты» на пути распространения таких действий;

3) обеспечение неотъемлемого свойства ИТКС – ее функциональной устойчивости как способности регулировать функционирование с целью поддержания выполнения операций при ожидаемых условиях и в условиях ужесточения требований, нарушений и непредвиденных обстоятельств «в малом», когда достаточно малое отклонение режима работы от исходного (установившегося) с течением времени уменьшается и функционирование ИТКС возвращается в исходное состояние, и «в большом», когда функционирование ИТКС, получив достаточно боль-

шое начальное отклонение, возвращается в исходное состояние после прекращения действия компьютерной атаки [23, 24];

4) непрерывное и продуктивное взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА [25]).

Актуальность исследования определяется необходимостью эффективного и результативного противодействия компьютерным атакам в ИТКС, масштаб и сложность которых постоянно растет при совершенствовании способов реализации с учетом развития информационно-коммуникационных технологий (ИКТ), когда при применении традиционных стратегий и систем обеспечения ИБ, основанных на принципе реагирования, а не упреждения угроз и инцидентов ИБ, невозможно обеспечить требуемый уровень ИБ ИТКС ОРГАНИЗАЦИИ.

Проведенный анализ показывает необходимость исследования и разработки научно обоснованной методологии и принципов построения организационно-технических средств обеспечения ИБ для ИТКС. Поэтому **объектом исследования** определена ИТКС ОРГАНИЗАЦИИ как важнейший объект субъектов КИИ с точки зрения необходимости защиты ее информационных ресурсов на всех стадиях их жизненного цикла (создания, сбора, обработки, накопления, хранения, поиска, распространения, использования и уничтожения).

Для упреждающего управления сетевой безопасностью ИТКС требуется использование новейших методов обработки и хранения информации. Только при таком походе удастся обеспечить возможность синтезировать новые знания о будущих угрозах ИБ для ИТКС и обоснованно прогнозировать развитие событий в области ИБ ИТКС. Это и определяет **предмет исследования** – построение специализированных центров, обеспечивающих информационную защищенность передаваемых по таким сетям данных на всех стадиях жизненного цикла ИТКС в условиях угроз ИБ в ЕИП ОРГАНИЗАЦИИ, а также при возникновении отказов в работе, требующих реструктуризации системотехнической составляющей ИТКС, за счет создания в ее составе с применением современных интеллектуальных подходов типового специализированного структурного элемента – «Центра интеллектуального управления сетевой безопасностью» (ЦИУСБ). Первоочередной целью развертывания ЦИУСБ является предоставление ОРГАНИЗАЦИИ возможностей по организации непрерывных процессов предотвращения, выявления и оперативного реагирования на события ИБ, происходящие в ИТКС в реальном времени, а также прогнозированию и предупреждению компьютерных атак на защищаемые объекты ИТКС на всех стадиях их жизненного цикла на основе своевременного интеллектуального анализа данных об этих событиях и выявленных требующих немедленной корректировки тенденций в уровне ИБ ИТКС в сравнении с заданными критериями.

Проведенные в работе исследования решают **научную проблему**, состоящую в формиро-

вании научной основы обеспечения информационной защищенности и функциональной устойчивости сложных систем класса ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ, что может быть достигнуто в результате разработки методологии и принципов построения специализированного структурного элемента ИТКС ОРГАНИЗАЦИИ – ЦИУСБ, призванного осуществлять упреждающее управление сетевой безопасностью ИТКС на всех стадиях жизненного цикла ее информационных ресурсов за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных. Непременным условием результативного функционирования ЦИУСБ для оперативной коррекции текущего уровня ИБ ИТКС в ЕИП ОРГАНИЗАЦИИ будет являться его обязательное вхождение в состав общей системы обеспечения ИБ (СОИБ). ЦИУСБ как ее важнейшая часть должен быть жестко связан с СОИБ ИТКС и влиять на ее развитие и совершенствование, для чего требуется комплексное обеспечение ИБ всех элементов ИТКС и разработка образовательных аспектов в части обучения разработчиков и персонала ЦИУСБ тому, как квалифицированно создавать, внедрять и эксплуатировать ЦИУСБ. Внедрение ЦИУСБ позволит устранить имеющееся в настоящее время острое противоречие между, с одной стороны, невозможностью избежать компьютерных атак в ИТКС, осуществляемых искушенными злоумышленниками, имеющими доступ к новейшим ИКТ, учитывая тенденцию к постоянному росту масштаба и сложности этих атак, и с другой стороны, использованием в этих условиях для обеспечения на одинаково высоком уровне информационную защищенности и, следовательно, функциональной устойчивости современных ИТКС устаревших стратегий и СОИБ, основанных на принципе реагирования, а не упреждения угроз и инцидентов ИБ, и, как следствие, обеспечивающих недостаточный уровень ИБ ИТКС ОРГАНИЗАЦИИ.

Степень разработанности проблемы. Рассматриваемая проблема обеспечения ИБ в вычислительных сетях находится в центре внимания специалистов уже около 40 лет, с момента появления интернет-протокола (англ. *Internet Protocol, IP*) в качестве стандартного сетевого протокола ARPANET с 1982 г. В настоящее время известны подходы и лучшие практики к обеспечению ИБ сетей, которые были взяты за отправную точку данной работы.

Исследованиями в области защищенности ИС и систем мониторинга ИБ занимались такие отечественные и зарубежные ученые, как П.Д. Зегжда, О.Б. Макаревич, А.А. Малюк, Е.Б. Белов, В.В. Романов, А.В. Лукацкий, А.К. Скуратов, И.В. Щербакова, А.В. Андронов, А.В. Мамаев, А.А. Лавров, К.Г. Абрамов, С.Ю. Исхаков, А.В. Гирик, С.И. Штеренберг, Т.Р. Кашаев, Авад Маркад Лебнан, M. Basseville, A. Benveniste, R. Bidou, M. Bishop, H.R. Debar, L.A. Johnson, R. Marchan, J. Myers, V. Paxson, D. Shin, F.W. Feather, M. Thottan, C. Ji G. Wang, H. Zhang и дру-

гие. Наиболее близкими к теме данного исследования являются следующие работы:

- по методическому и информационно-аналитическому обеспечению и взаимодействию для ситуационного управления защищенностью АС и ситуационно-аналитических центров – Соловьев С.В. [26], Ламонов А.В. [27], Лукашин А.А. [28], Попов В.М. [29] и Глухов А.П. [30];
- по вопросам адаптивного управления ИБ – Калинин М.В. [31], Исаев А.С. [32], Цыганков А.С. [33], Ушаков Д.В. [34] и Лаврова Д.С. [35];
- по применению интеллектуальных подходов к управлению ИБ – Машкина И.В. [36], Демидов Р.А. [37] и Карайчев Г.В. [38].

Центры мониторинга ИБ (*SOC*) первого поколения упоминаются всего в двух работах: И.А. Шелудько («Разработка и исследование системы оперативного сетевого мониторинга событий безопасности») (2004 г.) [39] и Д.О. Ковалева («Выявление нарушений информационной безопасности по данным мониторинга информационно-телекоммуникационных сетей») (2011 г.) [40].

Анализ показал, что в настоящее время проблема обеспечение ИБ ИТКС с применением современных интеллектуальных подходов до сих пор остаётся до конца научно не решенной, а обеспечение ИБ ИТКС на основе создания специализированного структурного элемента в составе ИТКС ранее не было темой специального комплексного научного исследования.

Цель исследования: разработка научно обоснованной методологии и принципов построения специализированного структурного элемента ИТКС – типового ЦИУСБ в составе СОИБ ИТКС, призванного осуществлять упреждающее управление сетевой безопасностью при передаче данных в ИТКС на всех стадиях ее жизненного цикла за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных. При этом все процессы обеспечения ИБ с применением ЦИУСБ в ИТКС ОРГАНИЗАЦИИ будут работать наиболее результативно только в том случае, когда операционные (текущие), тактические (в ближайшей перспективе) и стратегические (в отдаленной перспективе) задачи обеспечения ИБ ИТКС будут четко определены и будут решаться на взаимоподдерживающей основе в рамках СОИБ ИТКС.

Для реализации цели были поставлены и решены **следующие задачи исследования**, определившие структуру диссертационной работы:

1. Обосновать включение в ИТКС как основного объекта защиты в ЕИП ОРГАНИЗАЦИИ (объектов КИИ) нового специализированного структурного элемента, предназначенного для упреждающего управления сетевой безопасностью ИТКС на всех стадиях ее жизненного цикла, выявив противоречие между усложнившимся характером современных сетевых атак и существующими подходами и средствами обеспечения сетевой безопасности.
2. Провести научно обоснованную структуризацию понятий информационной защищен-

ности ИТКС и описания внутреннего и внешнего контекста деятельности ОРГАНИЗАЦИИ в виде единой таксономии, необходимой для конкретизации требований к ЦИУСБ, которая позволит получить научную систематизацию и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей (базовых понятий ИБ: «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»).

3. Исследовать основные подходы к управлению сетевой безопасностью и разработать и formalизовать процесс управления инцидентами ИБ (ПУИИБ) для его реализации в ЦИУСБ как ключевой структуры системы управления инцидентами ИБ ИТКС, а, следовательно, и СОИБ ИТКС.

4. На основе анализа недостатков известных видов центров управления безопасностью обосновать применимость концепции интеллектуальной безопасности с расширенной бизнес-логикой функционирования в разрабатываемом типовом ЦИУСБ, а также сформулировать требования к нему.

5. Разработать научно обоснованную методологию и принципы построения типового ЦИУСБ, включая решение задач разработки функциональной архитектуры, архитектуры обработки относящихся к ИБ данных и архитектуры обеспечения собственной ИБ ЦИУСБ с *SIEM*-системой следующего поколения в качестве его ядра и исследование вопросов обеспечения его функциональной устойчивости в ЕИП ОРГАНИЗАЦИИ и кадрового обеспечения.

6. Внедрить основные результаты диссертационного исследования по двум направлениям: в крупных организациях России, включая методологию и принципы построения и функционирования типового ЦИУСБ, и в ведущих университетах России, включая образовательную деятельность по подготовке высококвалифицированных специалистов для проектирования, внедрения, сопровождения и совершенствования ЦИУСБ на всех стадиях их жизненного цикла.

Методология и методы исследований. В основу исследования положены общая методология построения систем, общая теория систем, теория открытых систем, теория управления, теория связи, передачи, обработки и хранения информации, теория информационно-телекоммуникационных систем и сетей, теория ИБ, а также ИТ больших данных и блокчейна. Применимые к исследованию методы исследования: аналитические подходы, а именно системный анализ объекта исследования, позволяющий провести его высокоуровневое моделирование; поисковые исследования, анализ, систематизация и классификация типичных уязвимостей элементов ИТКС, угроз ИБ, сетевых атак и инцидентов ИБ; процессный подход, используемый для описания управления ИБ, включая мониторинг ИБ, современных сетей; аналитическое исследование текущего состояния предмета исследования; сравнительный анализ двух поколений ЦУБ и *SIEM*-систем; синтез требований к новой структурной единице ИТКС для осуществления централизованного управления ее ИБ с учетом основных положений теории управления и

выявления ближайших аналогов; синтез требований к следующему поколению *SIEM*-систем как ядру ЦИУСБ, методы нечетких множеств, лингвистических переменных (нестрогой математики), неформального оценивания, неформального поиска оптимальных решений; оценка разработанной концепции ЦИУСБ; метод карт процессов для представления процесса управления инцидентами ИБ; разработка глоссария основных понятий, используемых в исследовании.

Основные положения и результаты, выносимые на защиту:

1. Научно обоснованная методология и принципы построения типового ЦИУСБ, его функциональной и организационной архитектуры, включая обеспечение собственной ИБ ЦИУСБ, разработанные на основе выявления недостатков существующих центров.

2. Таксономия, обеспечивающая систематизацию и классификацию сущностей, базовых понятий ИБ, таких как «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», позволяющая регламентировать процесс определения уровня информационной защищенности ИТКС, описания функциональной деятельности ОРГАНИЗАЦИИ, требующей обеспечения информационной защищенности ИТКС, и для разработки документационного обеспечения ее ИБ на всех стадиях жизненного цикла ИТКС.

3. Детальное и формализованное описание основных взаимосвязанных процессов управления инцидентами ИБ, требующих первоочередной реализации в ЦИУСБ ОРГАНИЗАЦИИ, с применением расширенного метода составления карт процессов, который позволяет оптимизировать существующие процессы путем отслеживания избыточных действий и выявления рисков их успешной реализации.

4. Бизнес-логика функционирования типового ЦИУСБ, расширенная функциональными группами модулей, отвечающими за обратную связь процессов управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ, включая оперативное изменение конфигурационных настроек СЗИ в динамически изменяющейся среде функционирования ИТКС и взаимодействие с источниками информации о тенденциях в области сетевой безопасности (*Threat Intelligence*).

5. Защищенное по своему дизайну на основе технологий блокчейна средство блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ в составе рекомендуемой в качестве ядра типового ЦИУСБ *SIEM*-системы 3.0, предназначенное для обеспечения целостности этого массива.

6. Уточненная и существенно расширенная по сравнению с используемой временная шкала появления технологий и средств обеспечения сетевой безопасности, что позволяет наглядно отслеживать эволюцию существующих и своевременно фиксировать появление новых технологий и средств.

7. Глоссарий предметной области обеспечения сетевой безопасности на основе типового ЦИУСБ, отвечающий существующей нормативной и правовой базам и включающий 205 тер-

минов и расширяющий терминологию действующего ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».

Совокупность перечисленных результатов и теоретических положений, сформулированных в ходе проведения научного исследования, можно квалифицировать как значительное научное достижение в области обеспечения сетевой безопасности. В работе решена крупная научно-техническая проблема, имеющая большое народно-хозяйственное значение и заключающаяся в научно обоснованном выборе конкретных методов, принципов, способов и средств построения ЦИУСБ для достижения требуемого уровня информационной защищенности ИТКС. Внедрение результатов подтверждается соответствующими актами.

Степень обоснованности и достоверности научных положений, выводов и рекомендаций. Результаты исследования были получены при использовании утвержденных в установленном порядке российских ГОСТов и международных стандартов. Исследование проводилось с учетом материалов научно-практических конференций и публикаций в периодической печати, соблюдая принципы научной преемственности с предшествующими работами по данной проблематике, согласованности полученных в диссертации результатов с основными теоретическими положениями, а также комплексности и системности. Исследование опиралось как на общенаучные методы познания (анализ и синтез, сравнение и обобщение, научная абстракция, формальная логика), так и на специальные методы научного познания явлений и процессов: системный, структурный и функциональный анализы, графические, экспертные методы, моделирование и т.д. Результаты исследования также подтверждены формальными выводами основных утверждений, сформулированных в работе, использованием известных проверенных на практике методов и лучших практик соответствием предложенных усовершенствований общим архитектурным принципам построения систем вычислительных сетей и СОИБ, апробацией в печати и на научных конференциях, а также практикой их внедрения.

Новизна научных полученных результатов. Научная новизна полученных результатов диссертационного исследования и их научная ценность заключаются в следующем:

1. Обосновано включение в ИТКС (объект КИИ) нового специализированного структурного элемента – ЦИУСБ, предназначенного для упреждающего управления сетевой безопасностью ИТКС на всех стадиях ее жизненного цикла как системообразующего элемента СОИБ ЕИП ОРГАНИЗАЦИИ (субъект КИИ).

2. Разработаны научно обоснованная методология и принципы построения типового ЦИУСБ с применением интеллектуальных подходов (включая корреляционный, контекстный, поведенческий и структурный анализ) обработки больших относящихся к ИБ данных для упреждающего управления сетевой безопасностью ИТКС.

3. Проведена научно обоснованная структуризации понятий информационной защищенности ИТКС и описания внутреннего и внешнего контекста деятельности ОРГАНИЗАЦИИ как единая таксономия, необходимая для конкретизации требований к ЦИУСБ, которая позволила получить научную систематизацию и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей (базовых понятий ИБ: «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»).

4. На основе обобщения опыта построения ИТКС с централизованной обработкой и хранением больших объемов данных разработаны основные принципы и базовые архитектурные решения построения перспективных ЦИУСБ для объектов КИИ в условиях Российской Федерации, а также необходимое расширение оригинальной бизнес-логики их функционирования при управлении инцидентами ИБ в ИТКС ОРГАНИЗАЦИИ.

5. Для обеспечения целостности накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ в составе рекомендуемой в качестве ядра ЦИУСБ *SIEM*-системы 3.0 обосновано и спроектировано средство блокирования попыток компрометации с применением технологий блокчейна.

6. Для реализации в ЦИУСБ ОРГАНИЗАЦИИ детально разработаны и формализованы с применением расширенного метода составления карт (с добавлением табличного описания) основные взаимосвязанные процессы управления инцидентами ИБ ИТКС.

7. Для типового ЦИУСБ при реализации ИБ-аналитики и синтеза новых знаний об ИБ ИТКС ОРГАНИЗАЦИИ для ее упреждающей защиты обосновано использование концепции озер данных при организации хранения и обработки в режиме реального времени связанных с ИБ ИТКС данных.

8. Уточнена и существенно расширена по сравнению с используемой временная шкала появления технологий и средств обеспечения сетевой безопасности, что позволяет наглядно отслеживать эволюцию существующих и своевременно фиксировать появление новых технологий и средств.

9. Разработан глоссарий взаимосогласованных терминов предметной области обеспечения сетевой безопасности, отвечающий существующей нормативной и правовой базам и расширяющий терминологию ГОСТ Р ИСО/МЭК 27033-1-2011.

10. Практические внедрения полученных результатов научных исследований подтвердили их достоверность и результативность.

Личный вклад автора. Работа выполнена автором самостоятельно. Автору принадлежит организация и непосредственно осуществление исследований по всем выше перечисленным задачам диссертационного исследования. В работе использованы материалы, полученные лично автором, а также в соавторстве.

Личный вклад Милославской Н.Г. в работах, опубликованных в соавторстве, составляют следующие результаты:

- в работе [41] – формулирование и конкретизация задачи по защите больших данных, относящихся к ИБ; выделение связанных с ИБ данных, которыми необходимо управлять; словесное описание защищенной инфраструктуры для обработки больших данных, связанной с ИБ (далее эти результаты были использованы для разработки инфраструктуры ЦИУСБ;

- в работах [42, 43] – участие в разработке содержания и учебного плана образовательной программы для магистров «Обеспечение информационной безопасности и непрерывности бизнеса» направления 10.04.01 «Информационная безопасность»; разработка собственных дисциплин для программы;

- в работе [44] – идея использования технологии блокчейна для задач мониторинга ИБ и определения содержания транзакции;

- в работе [45] – разработка критериев классификации для таксономии угроз ИБ, уязвимостей, сетевых атак и инцидентов ИБ; примеры использования предложенной таксономии;

- в работе [46] – совместная разработка терминологии для теории ИБ и системных классификаций угроз ИБ;

- в работе [47] – описание процесса и подпроцессов управления инцидентами ИБ в целом и в табличной форме;

- в работе [48] – демонстрация роли систем мониторинга ИБ и *SIEM*-систем в решении задач управления инцидентами ИБ, а также определение информации ИБ, которую требуется визуализировать для принятия решений в области безопасности;

- в работе [49] – сравнение понятий больших данных, быстрых данных и озер данных и описание их взаимосвязи в отношении данных, связанных с ИБ;

- в работе [50] – идея и общее описание ЦИУСБ; описание реализации ЦИУСБ в МИФИ на кафедре «Информационная безопасность банковских систем»;

- в работе [51] – дальнейшее развитие концепции ЦИУСБ в отношении применения и изучения в нем *DLP*-систем;

- в работе [52] – идея создания практических лабораторных работ для обучения будущих сотрудников ЦИУСБ; содержание и задания для лабораторных работ; выбор специализированного инструмента для использования в лабораторных работах;

- в работе [53] – описание особенностей, которые применимы к подготовке высококвалифицированных кадров для ЦИУСБ;

- в работе [54] – анализ современных СЗИ.

Всем соавторам выражаю глубокую благодарность за помощь и поддержку.

Теоретическая и практическая значимость работы. *Теоретическая значимость полу-*

ченных результатов исследования заключается в следующем:

1. Обоснована необходимость совершенствования современных подходов к обеспечению ИБ современных сетей, которые не справляются с обработкой всех поступающих из гетерогенных источников данных о многочисленных и усложнившихся компьютерных атаках для реагирования в режиме жесткого реального времени на инциденты ИБ в ЕИП ОРГАНИЗАЦИИ (объекта КИИ).

2. Разработаны научно обоснованная методология и принципы построения типового ЦИУСБ ОРГАНИЗАЦИИ как объединения ЦИБ и СОЦ, что вносит значительный теоретический вклад в подходы к обеспечению сетевой безопасности ИТКС объектов КИИ, поскольку они направлены на решение проблемы совершенствования технического и организационного обеспечения сетевой безопасности в условиях угроз ИБ при одновременной интенсификации использования ИКТ в России.

3. Разработана таксономия как научная систематизация и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей, базовых понятий ИБ, а именно «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», которая вносит существенный вклад в развитие теории ИБ, к настоящему времени до конца пока не сформировавшейся в качестве самостоятельной теории.

4. Разработана обобщенная модель процессов функционирования типового ЦИУСБ, которая может быть использована не только применительно к ЦИУСБ, но и к ИТКС ОРГАНИЗАЦИИ, и в рамках этой модели сформулированы задачи анализа, то есть определить значения показателей защищенности информации в ЦИУСБ, синтеза и управления обеспечением ИБ в ЦИУСБ.

5. Для типового ЦИУСБ разработана архитектура хранения и обработки в режиме жесткого и мягкого реального времени больших и быстрых относящихся к ИБ ИТКС данных, основанная на использовании озер данных и ориентированная на применение в ЦИУСБ предложенного в рамках исследования процесса ИБ-аналитики и синтеза новых знаний об информационной защищенности ИТКС ОРГАНИЗАЦИИ для ее упреждающей защиты.

6. С применением расширенного (с добавлением табличного описания) метода составления карт процессов разработаны и формализованы основные взаимосвязанные процессы в рамках управления инцидентами ИБ ИТКС.

7. Представлен обзор основных возможностей ИБ-аналитики и выделены преимущества ее использования при решении задач управления инцидентами ИБ ИТКС ОРГАНИЗАЦИИ.

8. Обоснована необходимость разработки SIEM-системы нового поколения для использования в типовом ЦИУСБ и с применением технологий блокчейна со сверткой в составе SIEM-системы 3.0 разработано средство блокирования попыток компрометации массива накапливае-

мых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ.

9. Разработан глоссарий взаимосогласованных терминов предметной области обеспечения сетевой безопасности, который может стать основой для дальнейшего расширения.

10. Разработана структурно-логическая схема проведенного исследования, наглядно показывающая преемственность полученных результатов по отношению к ранее существовавшим и их значимость для эволюции методов и средств обеспечения сетевой безопасности.

Практическая значимость полученных результатов, созданных диссертантом и внедренных в промышленную эксплуатацию, заключается в следующем:

1. Построен типовой ЦИУСБ, описана методология его построения и рассмотрены вопросы ее использования при реализации ПУИИБ, что готово к доработке под конкретный внешний и внутренний контекст любой организации, владеющий ИТКС и желающий результативно управлять инцидентами ИБ в ИТКС.

2. Предложены вербальные описания ключевых типовых признаков (индикаторов), характеризующих типичные действия злоумышленника и свидетельствующих об удаленных сетевых атаках на ИТКС ОРГАНИЗАЦИИ, которые могут быть положены в основу разработки индикаторов компрометации (*IoC*) для источников *Threat Intelligence*.

3. В связи с отсутствием в международной и отечественной нормативных базах четких рекомендаций по разработке реестра (классификатора) рисков ИБ, предложены вид реестра рисков ИБ для ИТКС, построенный на основе Модели угроз ИБ и Модели нарушителей ИБ, и примерная типовая структура частной Политики ИБ для элемента ИТКС ОРГАНИЗАЦИИ.

4. Приведены примеры постоянной и временной информации, подлежащей сбору при расследовании инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ.

5. Установлены особенности визуализации информации об ИБ и то, какая информация об ИБ ИТКС ОРГАНИЗАЦИИ подлежит визуализации в ЦИУСБ для принятия обоснованных решений по управлению сетевой безопасностью обобщенно по всей ИТКС или по отдельным событиям ИБ.

6. Определены типы контекста, в рамках которого должна проводиться ИБ-аналитика относящихся к ИБ ИТКС ОРГАНИЗАЦИИ данных.

7. Для зональной архитектуры ЦИУСБ указаны применимые меры и средства обеспечения ИБ, предназначенные для защиты ЦИУСБ путем обеспечения защиты его сетевой инфраструктуры, функций устройств, информационных ресурсов и данных, управления пользователями и т.д., с указанием их расположения в зонах безопасности ЦИУСБ.

8. Введено понятие функциональной устойчивости ЦИУСБ в ЕИП ОРГАНИЗАЦИИ в штатном режиме, в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций как активной формы устойчиво-

сти для динамической системы, что должно быть изначально встроено в проект ЦИУСБ, как и система оценки уровня функциональной устойчивости и восстановления ЦИУСБ после нарушений и инцидентов ИБ (для нее приведен начальный набор показателей), а также перечислены основные мероприятия, осуществляемые в рамках процесса управления функциональной устойчивостью ЦИУСБ в ЕИП ОРГАНИЗАЦИИ.

9. Определен примерный состав кадрового обеспечения типового ЦИУСБ, который обычно делится на три-четыре линии. Для каждой линии указаны типовые трудовые функции персонала и их профессиональные компетенции.

10. Кратко описан международный опыт разработки документов, устанавливающих компетенции профессионалов в области ИБ, а также рассмотрены возможности российской системы высшего образования в формулировании таких компетенций. Кратко продемонстрировано, как это может быть применено при подготовке специалистов для типового ЦИУСБ.

11. Результаты диссертации использовались для разработки уникальной в России и мире образовательной программы подготовки магистров под названием «Обеспечение непрерывности и информационной безопасности бизнеса» в рамках направления подготовки 10.04.01 «Информационная безопасность».

12. Практические внедрения полученных результатов научных исследований подтвердили их достоверность и результативность.

Таким образом, в диссертационном исследовании изложены научно обоснованные технические, технологические или иные решения, внедрение которых вносит значительный вклад в развитие научной области обеспечения сетевой безопасности.

Соответствие паспорту специальности. Тема исследования и полученные результаты соответствуют областям исследования, изложенным в пунктах 1-3, 5-8, 12-15 паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Внедрение результатов работы. Результаты диссертационной работы использованы при разработке СОИБ для Банка России (акт головного исполнителя работ – российской компании «ЕС-лизинг»), при создании решений для ЦИУСБ организаций в регионах Восточной Европы, Кавказа и Центральной Азии (акт головного исполнителя работ – компании Qualys), при модернизации Ситуационного центра Службы ИБ Газпромбанка, при реализации типового ЦИУСБ в НИЯУ МИФИ, включая подготовку высококвалифицированных специалистов для проектирования, внедрения, сопровождения и совершенствования ЦИУСБ, в практике деятельности ООО «ЛИНС-М» при разработке средств ИБ для Банка России и стандарта обеспечения ИБ для Банка ВТБ (ПАО), а также при разработке и внедрении нормативных правовых и учебно-методических документов в Федеральном Учебно-методическом объединении в системе высшего образования по укрупненной группе специальностей направления подготовки «Ин-

формационная безопасность». Внедрение результатов подтверждается соответствующими актами.

Апробация работы. Основные результаты диссертационной работы были доложены на следующих международных конференциях:

— 3-я международная конференция по интернет-технологиям и приложениям (3rd International Conference on Internet Technologies and Applications), ITA2009, 2009 г., Рексхэм, Великобритания;

— 1-й, 3-й и 4-й международные симпозиумы по исследованиям и инновациям в области больших данных (1st, 3rd and 4th International Symposiums on Big Data Research and Innovation), BigR&I-2014, 2014 г., Барселона, Испания; BigR&I-2016, 2016 г., Вена, Австрия, BigR&I-2017, 2017 г., Прага, Чехия);

— 7-я международная конференция по безопасности информации и сетей (7th International Conference on Security of Information and Networks), SIN2014, 2014 г., Глазго, Великобритания;

— 4-я и 6-я международные конференции «Интернет вещей и облака будущего» (4th and 6th International Conferences «Future Internet of Things and Cloud»), FiCloud 2016, 2016 г., Вена, Австрия, FiCloud 2018, 2018 г., Рим, Италия;

— 5-я Всемирная конференция по информационным системам и технологиям (5th World Conference on Information Systems and Technologies), WorldCIST-2017, 2017 г., остров Порту-Санту, Португалия;

— 8-я ежегодная международная конференция по биологически вдохновленным когнитивным архитектурам (8th Annual International Conference on Biologically Inspired Cognitive Architectures), BICA 2017, 2017 г., Москва, Россия;

— 8-я, 10-я и 11-я Всемирные конференции по образованию в области информационной безопасности (8th, 10th and 11th World Conferences on Information Security Education), WISE8, 2013 г., Окленд, Новая Зеландия, WISE10, 2017 г., Рим, Италия, WISE11, 2018 г., Познань, Польша.

Результаты проведенных исследований были также доложены на Пленумах Учебно-методического объединения (УМО) по образованию в области ИБ (Москва, 2011 г, Иркутск, 2014 г., Таганрог, 2015 г., Санкт-Петербург, 2017 г., Томск, 2018 г.), Всероссийских научно-технических конференциях «Проблемы информационной безопасности в системе высшей школы» (Москва, 2008-2011 гг.), конференциях «Информационная безопасность» (Красноярск, 2008 г., Таганрог, 2008 г.), общероссийской научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2008 г.) и на научных семинарах кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ (Моск-

ва, 2009-2020 гг.).

Публикации. По результатам диссертации опубликовано единолично и в соавторстве 56 научных и учебно-методических работ, в том числе 21 научная статья, из них 16 опубликованы в журналах, входящих в Перечень рецензируемых научных журналов, рекомендованных ВАК РФ для публикации основных научных результатов диссертаций на соискание ученых степеней, и 5 в иностранных журналах на английском языке, и 24 полнотекстовых доклада 11 международных конференций на английском языке. Диссертантом издан в соавторстве 1 учебник с грифом Министерства образования и науки РФ, 8 учебно-методических пособий с грифом УМО по образованию в области ИБ, 1 учебное пособие с грифом УМО «Ядерная физика и технологии» и 1 глава в учебнике для студентов Европейского сообщества на английском языке. 28 публикаций по теме диссертации проиндексированы в базах Scopus и Web of Science (еще одна работа ожидает индексации).

Объем и структура диссертации. Структура диссертации подчинена логике исследования. Материалы диссертации изложены на 461 странице машинописного текста и включают введение, шесть глав, заключение, список литературы (307 источников, из которых 165 отечественных и 142 иностранных авторов) и разработанный глоссарий из 205 терминов. Работа содержит 20 таблиц, 57 рисунков, 12 страниц приложений.

В первой главе с целью постановки научной проблемы диссертационного исследования и определения его границ на основе критического анализа положения дел по исследуемому вопросу и открытых источников выбирается и описывается объект исследования – типовая ИТКС ОРГАНИЗАЦИИ, вводятся основы терминологического аппарата, используемого в работе, а также выделяются особенности текущего состояния обеспечения ИБ информационных ресурсов ИТКС в условиях существования угроз ИБ в ЕИП ОРГАНИЗАЦИИ, для чего прослеживается эволюция средств обеспечения сетевой безопасности начиная с 70-х годов XX века и по настоящее время. Выбирается нормативная и правовая база в области обеспечения ИБ, взятая за основу при проведении исследования. В заключении первой главы формулируются цель и задачи исследования, а также приводятся основные выводы по главе.

Во второй главе разрабатывается таксономия взаимосвязанных сущностей – базовых понятий ИБ («уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ») для ИТКС, необходимых для упорядочивания знаний об информационной защищенности ИТКС ОРГАНИЗАЦИИ и которые следует своевременно предотвращать или устранять, если они уже состоялись и были выявлены. Написание адекватных Стратегии и Политик ИБ, обоснованная разработка системы и выбор методов и средств обеспечения ИБ для ИТКС ОРГАНИЗАЦИИ напрямую зависит от полноты и качества разработанной таксономии и представленных классификаций. В заключении главы формулируются основные выводы.

В третьей главе для ИТКС ОРГАНИЗАЦИИ как основного объекта защиты в ЕИП ОРГАНИЗАЦИИ определяются понятия «процесс», «результативность процесса», «эффективность процесса», «обеспечение ИБ», «информационная защищенность», «СОИБ», «управление ИБ», «система управления ИБ», «мониторинг ИБ» и другие. На этой основе детально описываются процессы обеспечения и управления ИБ, показывается их взаимная связь и даются определения обеспечения и управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ. Приводятся результаты анализа эволюции основных подходов к управлению сетевой безопасностью. Перечисляются основные процессы проверки ИБ с особым вниманием к процессу мониторинга ИБ ИТКС ОРГАНИЗАЦИИ как основы выявления событий, связанных с ее ИБ, в рамках функционирования ЦИУСБ ОРГАНИЗАЦИИ. Подробно разрабатывается являющийся основой деятельности ЦИУСБ ОРГАНИЗАЦИИ процесс управления инцидентами ИБ для ИТКС с детальным представлением карт его процессов и их описанием. В заключении раздела показывается место разрабатываемого ЦИУСБ среди систем обеспечения и управления ИБ ОРГАНИЗАЦИИ в качестве фундамента системы управления инцидентами ИБ ИТКС и делаются выводы по главе.

В четвертой главе вводится и подробно анализируется понятие являющейся ядром ЦМБ и ЦИБ *SIEM*-системы как основы для дальнейшего построения ЦИУСБ, устраняющей ограниченность своих предшественников. Поясняется концепция интеллектуальной безопасности (англ. *Security Intelligence*), положенная в основу разрабатываемого ЦИУСБ. Анализируются два вида ЦУБ: ЦМБ, осуществляющего только мониторинг инцидентов ИБ, и ЦИБ, способного управлять инцидентами ИБ в ИТКС. Для ЦИБ разрабатывается расширенная по сравнению с оригинальной бизнес-логика функционирования для ее дальнейшего применения в типовом ЦИУСБ. Рассматриваются различные модели зрелости ЦУБ. Глава завершается формулированием общих и специальных требований, требований по обеспечению собственной ИБ ЦИУСБ, а также основными выводами.

В начале пятой главы пояснена хронология событий, касающихся идеи автора исследования разработать типовой ЦИУСБ и состояния этого вопроса в отечественной и зарубежной науке. Далее излагается разработанная методология построения типового ЦИУСБ ОРГАНИЗАЦИИ, после чего формулируются основные принципы его построения. Представляется основная идея построения и функциональные возможности типового ЦИУСБ как центра, объединяющего все преимущества ЦИБ и СОЦ в одном месте ОРГАНИЗАЦИИ для централизованного управления ИБ ИТКС и, в частности, ПУИИБ. Рассмотрены вопросы визуализации информации в типовом ЦИУСБ для принятия решений по управлению инцидентами ИБ в ИТКС. С учетом требований, изложенных в четвертой главе, для типового ЦИУСБ разрабатываются три основные архитектуры – функциональная, обработки больших и быстрых относящихся к ИБ ИТКС данных и обеспечения собственной ИБ. Кроме этого, для обеспечения ИБ

названных данных, поступающих для обработки в *SIEM*-систему ЦИУСБ, представлен проект *SIEM*-системы 3.0 с новым элементом, построенным с применением технологий блокчейна. Завершает главу рассмотрение вопросов функциональной устойчивости ЦИУСБ в штатном режиме и в условиях угроз ИБ в ЕИП ОРГАНИЗАЦИИ, кадрового обеспечения ЦИУСБ высококвалифицированными специалистами и демонстрация выполнения в разработанном типовом ЦИУСБ сформулированных в четвертой главе требований. В заключении главы приводятся основные выводы.

В шестой главе приведено краткое описание внедрения результатов диссертационной работы при модернизации Ситуационного центра Службы ИБ Газпромбанка, в проектно-конструкторскую деятельность российской компании «ЕС-лизинг» при разработке СОИБ для Банка России и компании Qualys в регионах Восточной Европы, Кавказа и Центральной Азии при создании решений для ЦУБ организаций-заказчиков, при реализации типового ЦИУСБ в НИЯУ МИФИ, в практике деятельности ООО «ЛИНС-М» при разработке СОИБ для Банка России и стандарта обеспечения ИБ для Банка ВТБ (ПАО), а также при разработке и внедрении нормативных правовых и учебно-методических документов, регулирующих высшее образования в области ИБ, в Федеральном Учебно-методическом объединении в системе высшего образования по укрупненной группе специальностей подготовки «Информационная безопасность» и при подготовке высококвалифицированных специалистов для проектирования, внедрения, сопровождения и совершенствования ЦИУСБ в ИИКС НИЯУ МИФИ. Главу завершают основные выводы.

В заключении выделены основные положения и результаты исследования, выносимые на защиту, обобщены и перечислены остальные полученные теоретические и практические результаты, а также указаны возможные направления дальнейших исследований.

Таким образом, в диссертационном исследовании решена научная проблема, имеющая важное значение для создания функционально устойчивой и защищенной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств России и заключающаяся в научно обоснованном рациональном выборе конкретных методов, принципов, способов и средств построения того главного, от чего в первую очередь зависит достижение информационной защищенности информационных ресурсов ИТКС, и изложены научно обоснованные технические, технологические и кадровые решения, внедрение которых вносит значительный вклад в развитие страны и научной области обеспечения сетевой безопасности.

ГЛАВА 1. АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В главе с целью постановки научной проблемы диссертационного исследования и определения его границ на основе критического анализа положения дел по исследуемому вопросу и открытых источников выбирается и описывается объект исследования – типовая информационно-телекоммуникационная сеть (ИТКС) ОРГАНИЗАЦИИ, вводятся основы терминологического аппарата, используемого в работе, а также выделяются особенности текущего состояния обеспечения информационной безопасности (ИБ) информационных ресурсов ИТКС в условиях существования угроз ИБ в едином информационном пространстве (ЕИП) ОРГАНИЗАЦИИ, для чего прослеживается эволюция средств обеспечения сетевой безопасности начиная с 70-х годов XX века и по настоящее время. Выбирается нормативная и правовая база в области обеспечения ИБ, взятая за основу при проведении исследования. В заключении главы формулируются цель и задачи исследования.

1.1. Анализ информационно-телекоммуникационной сети как основного объекта защиты в едином информационном пространстве организаций

1.1.1. Особенности современного использования информационно-телекоммуникационных сетей

Современные организации разных размеров, сфер деятельности и типов (государственные учреждения, коммерческие компании, некоммерческие организации) и их работники используют различные сетевые технологии для повседневной деятельности, корпоративного обучения, организации деловых мероприятий, взаимодействия с бизнес-партнерами и т.д., что предполагает активный обмен информацией в глобальном масштабе с помощью предоставляемых дистанционно услуг, безопасность которых не гарантирована и не доказана. Деятельность этих организаций базируется на гетерогенных распределенных сетевых инфраструктурах, предлагающих потребителям различные информационные ресурсы и услуги. Подключение к компьютерным сетям может осуществляться из любого места планеты в любое время. Облачные технологии, инструменты виртуализации, мобильные (беспроводные) сети, домашние офисы, роуминг, многочисленные персональные устройства и т.п. стали обычной реальностью, размывающей периметр сетей организаций. Локальные (автономные) компьютеры практически ушли в прошлое, что означает, что любая сеть начинается или заканчивается на любом подключен-

ном к ней устройстве. Для различных групп пользователей требуется бесперебойная работа и дифференцированное качество обслуживания. Широкое распространение теневых сетей (типа *Tor*, *DarkNet*) и средств работы в них добавляет негативных красок в эту картину. При этом ценность коммерческой информации, персональных данных, платежной информации и т.п. возрастает день ото дня – давно стало истиной то, что те, кто владеет информацией, владеют миром. Также растет количество вовремя не устраненных уязвимостей в веб-технологиях, программном (ПО) и аппаратном (АО) обеспечении. Неверно настроенные системы защиты, отсутствие необходимых политик, руководств и регламентов в области обеспечения информационной безопасности (ИБ), избыточные права доступа – далеко не все типичные проблемы, используемые злоумышленниками для реализации как простейших, так и сложных и разрушительных целенаправленных атак на информационные системы (ИС), подключенные к сетям. Кроме того для достижения своих бизнес-целей и поддержания конкурентоспособности, защиты клиентов и сотрудников не только внутри, но и вне самой организации, для нее важно соответствовать множеству внутренних и внешних требований.

Типовая схема распределенной корпоративной компьютерной сети (интранета), обеспечивающей разным группам пользователей ее использование и совместный доступ к услугам, процессам и информационным ресурсам, находящимся в разных подразделениях, упрощенно представлена на рис. 1 [55]. Она отличается существенной неоднородностью используемых в разных подразделениях АО и ПО и интеграцией этих гетерогенных компонентов в единую систему, различными технологиями подключения потребителей предоставляемых услуг к общей сети, необходимостью дифференцированного качества обслуживания отдельных групп пользователей и всеми ранее перечисленными особенностями.

Представленное поверхностное описание создает далеко не полное представление о современном мире компьютерных сетей и насущной потребности организаций в защите их информационных ресурсов и предоставляемых пользователям услуг.

1.1.2. Определение информационно-телекоммуникационной сети

Согласно Федеральному закону № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации», информационно-телекоммуникационные сети (ИТКС), ИС, автоматизированные системы управления (АСУ) субъектов критической информационной инфраструктуры (КИИ), а также сети электросвязи, используемые для организации взаимодействия таких объектов, относятся к объектам КИИ. Под субъектами КИИ подразумеваются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели (далее –

ОРГАНИЗАЦИЯ), которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ, функционирующие в сфере здравоохранения, транспорта, связи, энергетики, науки, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [7, статья 2].

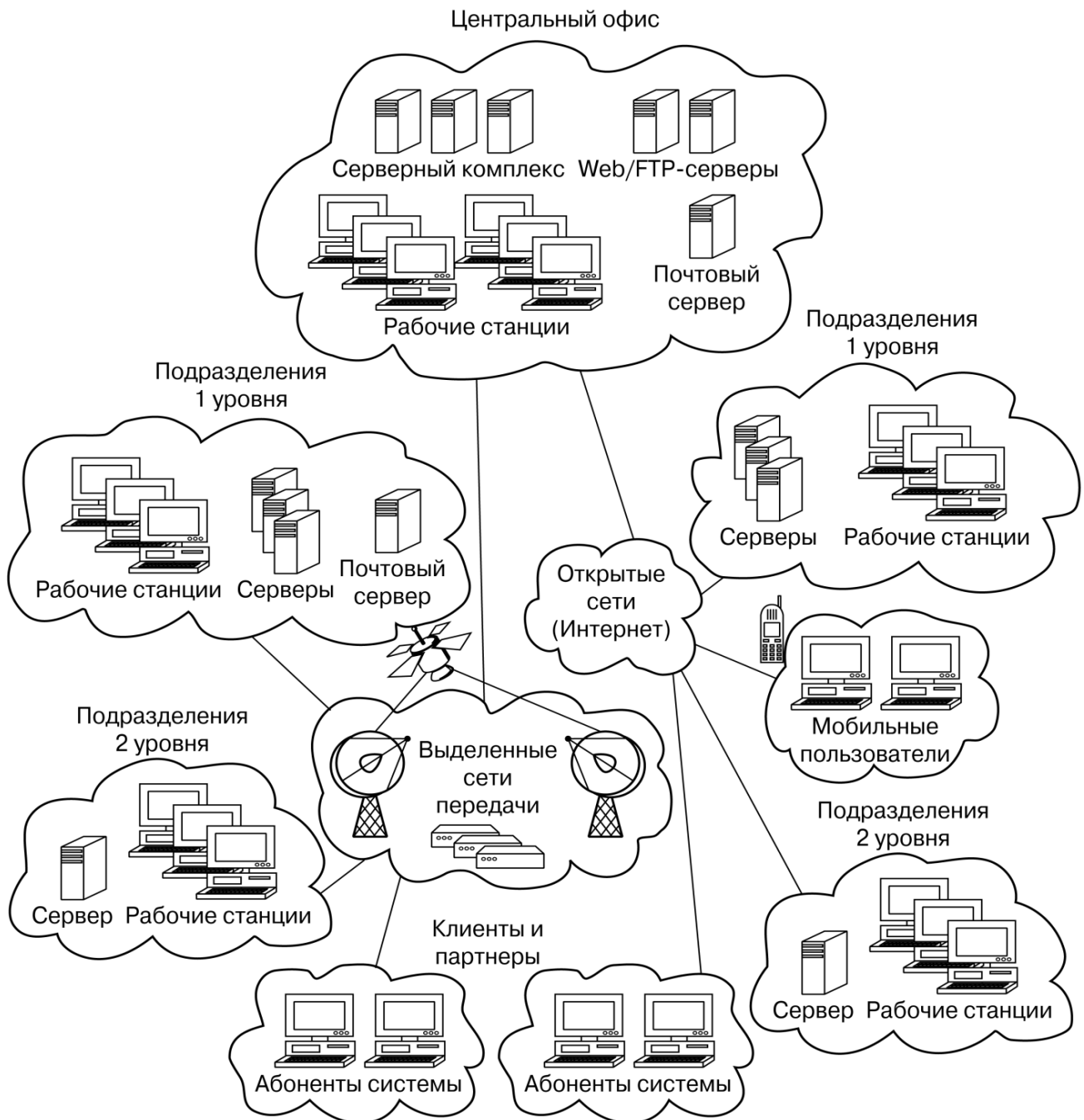


Рисунок 1 – Типовая схема распределенной сети организации

Как определяется в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации», **информационно-телекоммуникационная сеть (ИТКС)** – это технологическая система (ТС), предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (СВТ) [6, статья 2]. В свою очередь, ТС – это совокупность функционально взаимосвязанных средств технологического оснащения, предметов производства и исполнителей для выполнения в регламентированных условиях производства заданных технологических процессов или операций. Выделяют четыре иерархических уровня таких систем: операций, процессов, производственных подразделений и предприятий [56]. СВТ – это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [57].

Самым полным и детальным с точки зрения автора исследования описанием информационно-телекоммуникационной системы (ИТС), включающей в свою архитектуру ИТКС, является описание, данное М.Ю. Сенаторовым для ИТС Банка России [58]. Поэтому именно оно и было взято за основу формирования общесистемного представления о типовой ИТКС ОРГАНИЗАЦИИ.

Современные ИТКС могут быть глобальными (типа интернета), локальными (в одном здании ОРГАНИЗАЦИИ), корпоративными (для одной корпорации), региональными (в пределах городов, областей и других территориальных единиц), ведомственными (в пределах ведомства) и специального назначения (например, ГАС «Выборы»). При этом ИС большинства государственных учреждений и коммерческих компаний, организующие хранение и обработку информации о конкретной предметной области [59], связаны между собой компьютерными сетями. Их сетевые соединения могут существовать в пределах одной организации (организации А и В), между различными организациями (организации А и С) или между организацией и неограниченным кругом лиц (организации А и С) (рис. 2) [60].

1.1.3. Информационно-телекоммуникационная сеть как симбиоз телекоммуникационной и информационной сетей

Как следует из названия, ИТКС представляет собой симбиоз двух видов сетей – информационной и телекоммуникационной [61]. Эти сети территориально распределены по месту размещения, объединяют большое количество разнообразных технических средств обработки, передачи и хранения информации, различаются по масштабу, решаемым задачам и типам обрабатываемых данных с разными требованиями по обеспечению ИБ, а также реализуют сложные режимы автоматизированной обработки данных и совмещают выполнение информационных

запросов различных категорий пользователей – потребителей информации и ИТ-услуг (услуг информационных технологий (ИТ), англ. *IT services*). При этом все составляющие ИТКС должны функционировать непрерывно и устойчиво в условиях высокой интенсивности информационных потоков.

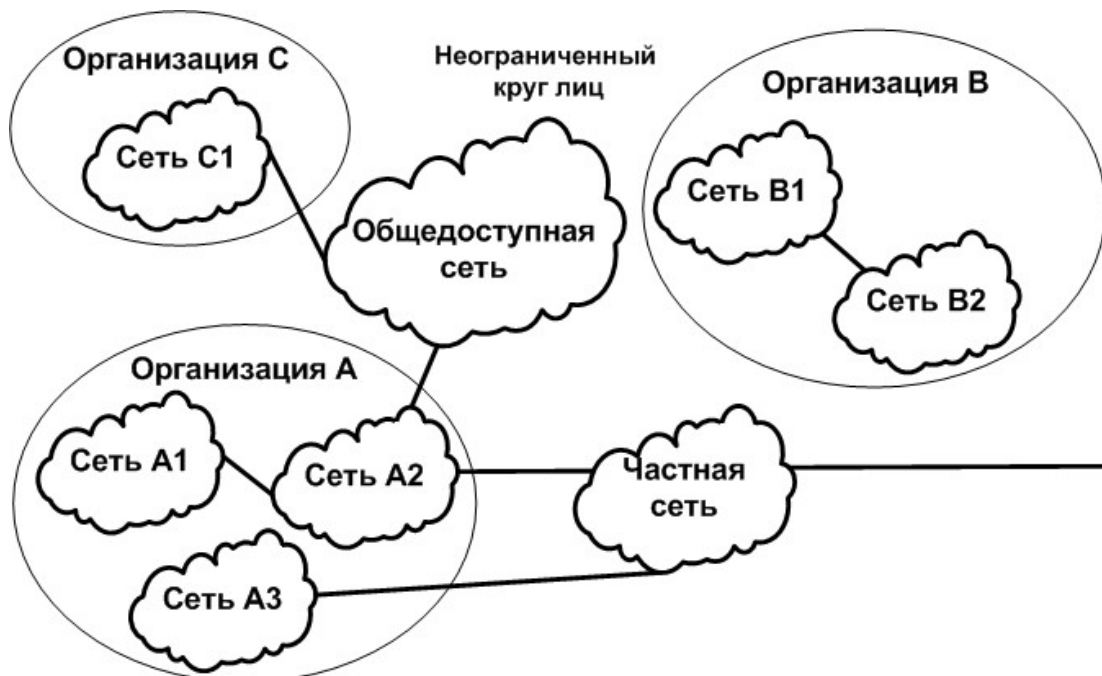


Рисунок 2 – Виды сетевых соединений

Телекоммуникационная сеть является системообразующей компонентой в общей архитектуре ОРГАНИЗАЦИИ, выполняя роль интегратора при перемещении информационных ресурсов, и представляет из себя совокупность взаимосвязанного телекоммуникационного (ИТ-) оборудования – технических средств (устройств, оборудования), используемых для построения сетей передачи данных и приема-передачи цифровой информации и предоставления телекоммуникационных услуг конечным потребителям (адаптировано на основе [62, 63]). Цифровая информация (англ. *digital information*) – это информация, представленная в виде последовательности цифр и доступная для обработки, передачи и хранения с помощью технических устройств в результате применения ИТ. К телекоммуникационным можно отнести услуги транспортные, предоставление каналов связи, включая видеосвязь, приема-передачи документов с использованием телекоммуникационных средств и т.п.

С этимологической точки зрения термин «телекоммуникация», образованный от греч. *tele* (далеко, вдаль) и латинского *communicatio* (общение), означает «общение на расстоянии». Вкладываемый сегодня в этот термин смысл включает в себя все многообразие средств дистанционного обмена информацией, например, беспроводная и спутниковая связь, телефония и пр.,

осуществляемые в синхронном (в реальном или близком к реальному режиму времени) и асинхронном (с временной задержкой) режимах.

Традиционно телекоммуникационную сеть упрощенно представляют иерархической моделью (рис. 3), в которой выделяют три логических уровня [64]:

- базовый уровень, предназначенный для быстрой и надёжной передачи данных и представленный коммутационными узлами, соединенными каналами первичной сети;
- уровень распределения, предназначенный для маршрутизации трафика (состоящего из сетевых пакетов, специфичных для конкретного сетевого протокола) и установления политик доступа пакетов к базовому уровню и включающий физическую среду распространения данных;
- уровень доступа потребителей данных к транспортной сети.

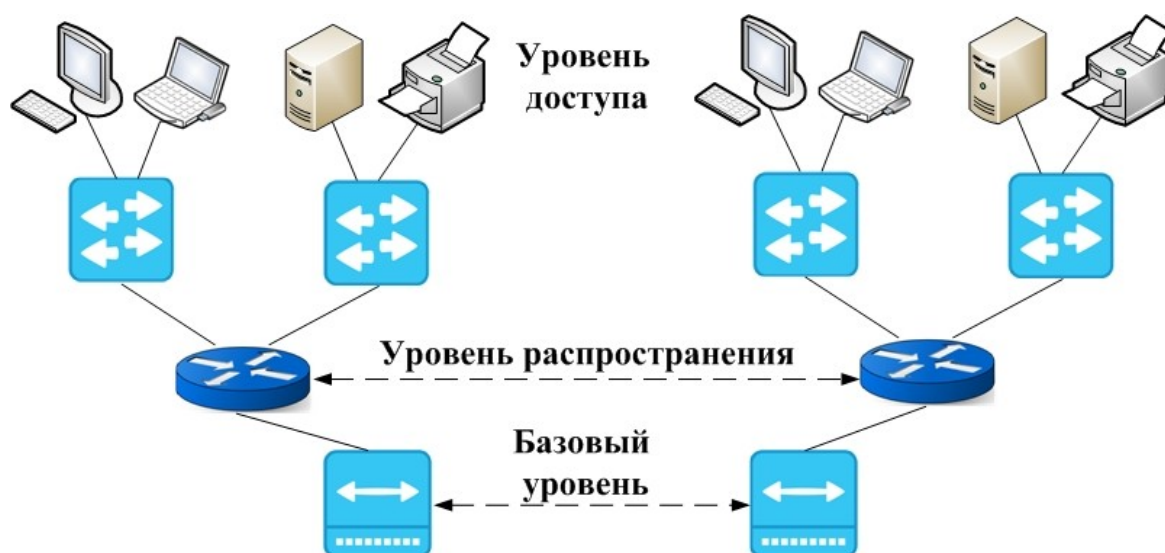


Рисунок 3 – Упрощенная иерархическая модель телекоммуникационной сети

Информационная сеть предназначена осуществлять информационное обеспечение процессов выработки стратегических решений ОРГАНИЗАЦИИ в сфере ее деятельности. Она предоставляет потребителям по запросу или в соответствии с определенными временными интервалами информационные услуги, включая ИТ-услуги – совокупность функциональных возможностей информационных и неинформационных технологий, предоставляемая конечным пользователям в качестве услуги (например, передача сообщений, сервисы файлов и печати, бизнес-приложения, сетевые сервисы и т.д.) [22].

Примерами информационных сетей являются справочные и научно-технические сети и интернет, а результатом предоставления ИТ-услуг – информационные ресурсы. Информационная сеть поддерживается совокупностью связанных между собой программно-техническими средствами (СВТ) и, возможно, иными средствами, которые участвуют в поддержании всего

жизненного цикла информационного ресурса – начиная от их получения (поиск и сбор), обработки, хранения, распространения (передача по линиям связи и предоставление) и заканчивая уничтожением информации, в рамках данного исследования для краткости в совокупности называемые «обработка, передача и хранение информации».

Процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации называются информационными процессами, реализуемыми в рамках информационных сетей [22].

Из приведенных выше рассуждений очевидно, что информационная и телекоммуникационные сети сегодня практически не существуют отдельно – они взаимно дополняют друг друга, образуя общую ИТКС, составляющими которой они и являются. Таким образом, современные ИТКС представляют собой, как правило, многоуровневые иерархические структуры, построенные на принципе открытых систем (то есть обладающие свойствами интероперабельности (англ. *interoperability*) – способности к взаимодействию с другими системами, переносимости (англ. *portability*) во времени и пространстве ПО, данных и пользователей между системами, а также использующие стандартизированный набор решений для функционирования [64]) с разграничением функций и доступа к ним и всем информационным ресурсам ИТКС на каждом уровне иерархии.

1.1.4. Информационные ресурсы информационно-телекоммуникационной сети и среда их обработки

ИТКС с информационной точки зрения объединяет распределенные в пространстве упорядоченные по типам информационные ресурсы и различные ИТ, информационные процессы и решения по обработке, передаче и хранению информации на основе централизованной иерархической информационной инфраструктуры (ИИ) (англ. *information infrastructure*) – системы организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия [65].

Под информационным ресурсом традиционно понимается информационный актив ОРГАНИЗАЦИИ, который используется или потребляется в процессе выполнения некоторой деятельности, и используемая для его обработки ИИ. Информационный актив (англ. *information asset*) – это информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для ОРГАНИЗАЦИИ, находящаяся в распоряжении ОРГАНИЗАЦИИ и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме [22, 65]. Примерами информационных ресурсов являются циркулирующие по линиям связи данные, подключенные базы данных (БД) и базы знаний, справочники, архивы, резервные ко-

пии и т.п., содержащие управленческую, нормативную, справочную, платежную информацию, информацию бизнес-процессов, конфигурационные настройки сетевого оборудования и средств защиты информации (СЗИ) и т.п. Примерный перечень типов информационных активов, который формируется каждой организацией самостоятельно на основе их классификации и который не должен противоречить нормам законодательства Российской Федерации (РФ), может содержать следующие два основных типа с подтипами:

1) открытая (общедоступная) информация (например, опубликованная на веб-сайте ОРГАНИЗАЦИИ в интернете, или представленная в ее рекламных роликах);

2) информация ограниченного доступа, включающая в себя:

— управляющую информацию, используемую для настройки оборудования ИТКС, и информацию о процедурах его эксплуатации и поддержки;

— технологическую информацию, включая системную документацию, руководства администраторов, разработчиков и пользователей и т.п.;

— информацию по обеспечению ИБ и непрерывности функционирования элементов ИТКС;

— информацию, содержащую сведения, составляющие различные виды тайн (коммерческую, банковскую, страховую, налоговую и т.п.);

— персональные данные (ПДн);

— платежную информацию;

— аналитическую информацию;

— информацию о бизнес-контактах, деловой переписке, контрактах и пр.

ИТКС с телекоммуникационной точки зрения можно описать как широкий спектр телекоммуникационных сетей и сетей связи, обеспечивающих взаимодействие территориально распределенных элементов ИТКС при коллективном обслуживании ее удаленных потребителей. В рамках данного исследования телекоммуникационная составляющая ИТКС будет интересна как среда обработки информационных активов (СОИА) – среда использования и (или) эксплуатации информационного актива, в которой осуществляется получение (поиск и сбор), обработка, хранение, распространение (передача и предоставление) и уничтожение информации [66]. Для СОИА выделяют объекты – материальные объекты среды использования и (или) эксплуатации информационного актива, формирование перечней типов которых также осуществляется ОРГАНИЗАЦИЕЙ самостоятельно в соответствии с иерархией уровней ее ИИ. Так, в [65] выделены семь уровней ИИ, которым соответствуют следующие типы объектов СОИА:

— на физическом уровне – сети передачи данных, линии связи, оборудование (в том числе контроля доступа), аппаратура и СВТ (в том числе периферийные устройства, клиентские компьютеры), носители информации и прочее, а также помещения, здания, сооружения, где

размещаются все элементы ИТКС ОРГАНИЗАЦИИ;

- на уровне сетевого оборудования – сетевые программные и аппаратные средства: маршрутизаторы, коммутаторы, концентраторы, сетевые серверы, сетевые принтеры и пр.;

- на уровне сетевых приложений и сервисов – сервис поддержки точного времени, система доменных имен (англ. *Domain Name System, DNS*), почтовые клиенты, веб-браузеры, удаленные терминалы, вычислительные и коммуникационные сервисы, средства разработки и другие прикладные и общесистемные программные средства;

- на уровне операционных систем (ОС) – процессы, порождаемые ОС, приложения ОС, прикладное ПО и пр.;

- на уровне систем управления базами данных (СУБД) – файлы данных, БД, хранилища данных, архивированная информация, резервные копии и пр.;

- на уровне технологических процессов и приложений – информационные и иные технологические процессы, служебно-информационные и тестовые сообщения, результаты работы приложений и пр.;

- на уровне бизнес-процессов ОРГАНИЗАЦИИ – бизнес-планы, финансовые сметы, прогнозы, аналитическая информация, эксплуатационные или поддерживающие процедуры, планы по обеспечению непрерывности деятельности, меры по нейтрализации рисков, системная документация, руководства пользователей, бизнес-контакты, деловая переписка и пр.

1.1.5. Логическая структура информационно-телекоммуникационной сети

Обобщив выше представленное, логическая структура ИТКС ОРГАНИЗАЦИИ изображена на рис. 4. Кроме информационной и телекоммуникационной сетей, она включает в себя систему их интеграции, систему доступа и представления услуг и информации потребителям, а также централизованную систему обеспечения функционирования ИТКС, имеющую в своем составе систему управления всей ИТКС в целом и отдельными ее элементами. Подсистемами двух последних систем являются система обеспечения ИБ (СОИБ), включающая систему управления ИБ (СУИБ).

СОИБ ИТКС объединяет подсистемы обеспечения ИБ отдельных элементов ИТКС и поддерживает гарантированную защиту ИТКС в целом, ее подсистем, информационных ресурсов, процессов и предоставляемых услуг на основе применения многоуровневого (эшелонированного) подхода и использования современных технологий и средств защиты информации в процессе всего жизненного цикла обрабатываемой информации.



Рисунок 4 – Логическая структура ИТКС ОРГАНИЗАЦИИ

Определим *СОИБ ОРГАНИЗАЦИИ* как централизованную систему поддержания состояния информационной защищенности ЕИП организации (ее информационных ресурсов, информационных процессов, ИТ-услуг, хранилищ информации, средств обработки и передачи информации и т.п.). СОИБ состоит из системы управления ИБ (СУИБ) и мер обеспечения ИБ (англ. *security controls*) и процессов их эксплуатации.

СОИБ ИТКС включает в себя соответствующую организационную структуру (в которую будет входить ЦИУСБ как ее системообразующий элемент, что показано далее), политику, планирование действий, роли и обязанности, установившийся порядок, процессы и процедуры обеспечения ИБ, меры обеспечения ИБ и ресурсы, необходимые для обеспечения ИБ ИТКС ОРГАНИЗАЦИИ. В третьей главе показано, что при этом неперенным условием результативного функционирования разрабатываемого в рамках данного исследования ЦИУСБ для оперативной коррекции текущего уровня ИБ ИТКС будет являться его обязательное вхождение в состав СОИБ ИТКС – ЦИУСБ как ее важнейшая часть должен быть жестко связан с СОИБ ИТКС и влиять на ее развитие и совершенствование, для чего требуется комплексная методика обеспечения ИБ всех элементов ИТКС и разработка образовательных аспектов в части обучения тому, как квалифицированно создавать, внедрять и эксплуатировать ЦИУСБ. Таким образом, обеспечение ИБ ИТКС основывается на комплексном системном подходе, включающем организационную (документальное обеспечение), техническую (технологии и средства обеспечения сетевой безопасности), кадровую (подготовленный персонал) и другие составляющие, что будет рассмотрено в последующих главах работы.

1.1.6. Информационно-телекоммуникационная сеть как системообразующая структура единого информационного пространства организации

В современных условиях значительная часть решаемых задач и функций единого информационного пространства (ЕИП) фокусируется в ИТКС ОРГАНИЗАЦИИ. С этих позиций ИС как базовые элементы ИТКС должны рассматриваться и как типовые элементы ЕИП ОРГАНИЗАЦИИ. Основой их построения являются современные аппаратно-программные платформы, включающие в себя мощные серверы, промышленные СУБД, сетевые массивы данных, ОС и прикладные программные средства, а их архитектура основана на применении современных многозвенных и клиент-серверных технологий с частым использованием почтового и веб-интерфейсов.

Выше приведенный анализ показывает, что ИТКС ОРГАНИЗАЦИИ может рассматриваться как системообразующая структура ее ЕИП. В «Концепции формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов» [67] ЕИП определено как «совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей». Оно включает в себя следующее:

- 1) информационные ресурсы, содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации;
- 2) ИИ в составе:
 - организационные структуры, обеспечивающие функционирование и развитие ЕИП, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации;
 - средства информационного взаимодействия его участников, в том числе программно-технические средства и организационно-нормативные документы, обеспечивающие доступ к информационным ресурсам на основе соответствующих ИТ.

В Стандарте Банка России СТО БР ИББС-1.0-2014 [65] введено похожее понятие информационной сферы – «совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений». Это понятие существенно шире, чем более «техническое» понятие ЕИП, поскольку включает в себя также взаимодействующих в рамках ЕИП субъектов и систему регулирования возникающих при этом отношений. Поэтому в дальнейшем будут использоваться оба термина в зависимости от контекста их рассмотрения.

Принимая во внимание выше приведенные рассуждения, сделаем вывод, что с системно-технической точки зрения ИТКС ОРГАНИЗАЦИИ можно описать как:

- открытую систему с централизованным управлением ИТКС в целом и централизованно-децентрализованным управлением ее отдельными элементами;
- направленную на обеспечение функциональной устойчивости всех ее составляющих в штатном режиме и в условиях угроз ИБ в ЕИП;
- включающую интегрированную совокупность технических и программных средств, обеспечивающую автоматизацию всех информационных сфер деятельности ОРГАНИЗАЦИЯ и эффективное использование информационных ресурсов, а также систему связи, использующую современные телекоммуникационные технологии для обмена цифровой информацией с учетом ее срочности и важности;
- основанную на сложной пространственно и функционально распределенной иерархической человеко-машинной системе, в которой сочетаются машинная обработка информации с применением СВТ и средств связи с деятельностью человека, выступающего в качестве потребителя информационных и телекоммуникационных услуг, предоставляемых ИТКС в автоматизированном режиме в соответствии с установленными регламентами;
- имеющую в своем составе комплексную СОИБ.

1.2. Современные проблемы защиты информации в информационно-телекоммуникационных сетях

1.2.1. Тенденция возрастания угроз информационной безопасности для информационно-телекоммуникационных сетей

Передача информации по каналам связи ИТКС при взаимодействии ОРГАНИЗАЦИИ со своими бизнес-партнерами, удаленными офисами и потребителями является огромным достижением новых информационно-коммуникационных технологий (ИКТ) (англ. *Information and Communication Technology, ICT*), но и вызывает вполне обоснованное беспокойство тех, кто отвечает за передаваемые таким образом данные или доступность самой инфраструктуры ИТКС со всеми ее информационными ресурсами и предоставляемыми услугам. Отсутствие должного внимания к обеспечению ИБ ИТКС может привести к значительным убыткам.

Параллельно с кардинальными изменениями в ИТ-сфере, приведшими к созданию ИТКС в разных организациях, постоянно расширяется диапазон и сложность угроз нарушения информационной безопасности (ИБ) (далее – угроз ИБ), особенно связанных с новыми ИКТ, сетевыми технологиями, устройствами и услугами. Определим *угрозу ИБ ИТКС ОРГАНИЗАЦИИ* как совокупность факторов и условий, создающих опасность нарушения ИБ ИТКС

ОРГАНИЗАЦИИ, вызывающую или способную вызвать негативные последствия (ущерб/вред) для нее. Формой реализации (проявления) угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств ИБ объекта(ов) ИТКС ОРГАНИЗАЦИИ [22].

Многочисленные ежегодные исследования по вопросам ИБ показывают, что стратегии обеспечения ИБ, которые традиционно были основаны на соблюдении нормативных и правовых требований и ограничивались лишь «защитой периметра» (англ. *perimeter defense*) компьютерных сетей, не успевают за растущим уровнем рисков ИБ в данной области. В отдельный класс выделяют кибератаки, совершаемые в киберпространстве. Методы, применяемые злоумышленниками при их реализации для проникновения через устаревшую защиту периметра, также усложняются и становятся все более изощренными. В качестве примеров подобной тенденции можно привести появление и развитие в последние годы атак на системы Интернета вещей (англ. *Internet of Things, IoT*) и APT-атак (англ. *Advanced Persistent Threats*), направленных на цели определенной категории (как правило, делового или политического характера), промышленный шпионаж и кражу бизнес-информации. Один из самых распространенных способов атак начинается с того, что злоумышленники сначала получают доступ к плохо защищенным серверам и компьютерам пользователей, а затем с них производят атаки на ИС по всему миру. Они умеют осторожно тестировать защиту сетей, избегая обнаружения, и, найдя уязвимости, используют их для достижения своих целей. Например, прибегают к целевому фишингу (англ. *spear phishing*), заключающемуся в направлении сообщений отдельной группе пользователей с определенным сходством и, как результат, получении незаконным путем необходимой информации от сотрудников компаний. Для внедрения вредоносного кода могут использоваться как технические средства и каналы, так и социальная инженерия (англ. *social engineering*). Одновременно с этим увеличивается число потенциальных точек проникновения в сети, по которым злоумышленники наносят «точечные удары», приводящие к утечке конфиденциальной информации, загрузке приложений через почтовые сообщения, несанкционированному переводу денежных средств и т.д.

Утрата конфиденциальности, целостности и доступности информации и недоступность предоставляемых услуг может оказывать существенное неблагоприятное влияние на репутацию и деятельность ОРГАНИЗАЦИИ. Например, секретные сведения могут попасть в руки конкурентов, шпионов и тех, кто по определенным соображениям сможет их модифицировать или подменить, а недоступность веб- или почтового сервера не позволит своевременно получить требуемую информацию и на ее основе принять необходимое в данный момент решение.

В качестве иллюстрации приведем статистику атак за 2020 г. от известной аналитической компании Hackmaggedon, которая показывает, что большинство из них связаны с распро-

странением вредоносного ПО (39,3 %), похищением учетных записей (16,7 %), целенаправленными атаками (10,7 %), внедрение вредоносных скриптов (описанных с помощью языка программирования последовательностей действий) (3,7 %), спамом (незапрашиваемых сообщений электронной почты) (1,8 %), DDoS-атаками (англ. *Distributed Denial of Service*) (1,7 %), созданием поддельных страниц (1,5 %) и неверных конфигураций (1,1 %) [8].

Постепенная эволюция методик атакующих и используемого для сетевых атак готового ПО за годы, начиная с 1980 и по настоящее время, резко снизила уровень знаний, необходимых для выполнения успешных атак. По мере развития сетевых технологий сложность атак постоянно возрастала при снижении общего уровня знаний злоумышленников. Рис. 5 [55], первоначально отражающий период с 1980 по 2000 гг. и созданный в университете Карнеги-Меллона (*University Carnegie Mellon*), был дополнен на период до 2014 г. Национальной лабораторией университета Айдахо (*University Idaho National Laboratory*). Он наглядно демонстрирует тенденции последних нескольких десятилетий, когда человек, имеющий достаточную мотивацию, время и минимальные ресурсы, может без особых проблем нанести значительный ущерб незащищенным сетевым ресурсам. Все это показывает, что в последнее время риски ИБ для объектов КИИ, включая ИТКС ее субъектов, приобрели статус компонентов системного риска. (Под **риском нарушения ИБ (для краткости – риск ИБ)** будем понимать потенциальную возможность использования уязвимостей актива/группы активов конкретной угрозой ИБ для причинения ущерба организации. Измеряется риск ИБ исходя из комбинации вероятности события и его последствия [66]).

В качестве основополагающих причин данной тенденции можно выделить, в первую очередь, сложность и разнородность ИТКС разных субъектов по функциям, структуре и организационно-правовым формам, растущую роль различных технологий в предоставлении услуг и все большую зависимость последних от ИКТ, усиливающуюся взаимозависимость между всеми участниками информационных взаимодействий, а также рост сложности, широкой направленности и разнообразия компьютерных атак и появление новых категорий злоумышленников и целей, которые они преследуют, как фактор возникновения новых угроз ИБ от ранее не рассматриваемых источников и уязвимостей.

В целях обеспечения безопасности субъект КИИ в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, создает систему безопасности такого объекта и обеспечивает ее функционирование [7, статья 10]. При этом безопасность КИИ, включающей ИТКС разных субъектов – это состояние защищенности КИИ, обеспечивающее ее функциональную устойчивость при проведении в отношении ее компьютерных атак [7, статья 2]. Под **компьютерной атакой**

(англ. *computer attack*) понимается целенаправленное воздействие программных и (или) аппаратно-программных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации. Наравне с законностью, к принципам обеспечения безопасности КИИ относятся непрерывность и комплексность этого процесса и приоритет предотвращения компьютерных атак [7, статья 4].

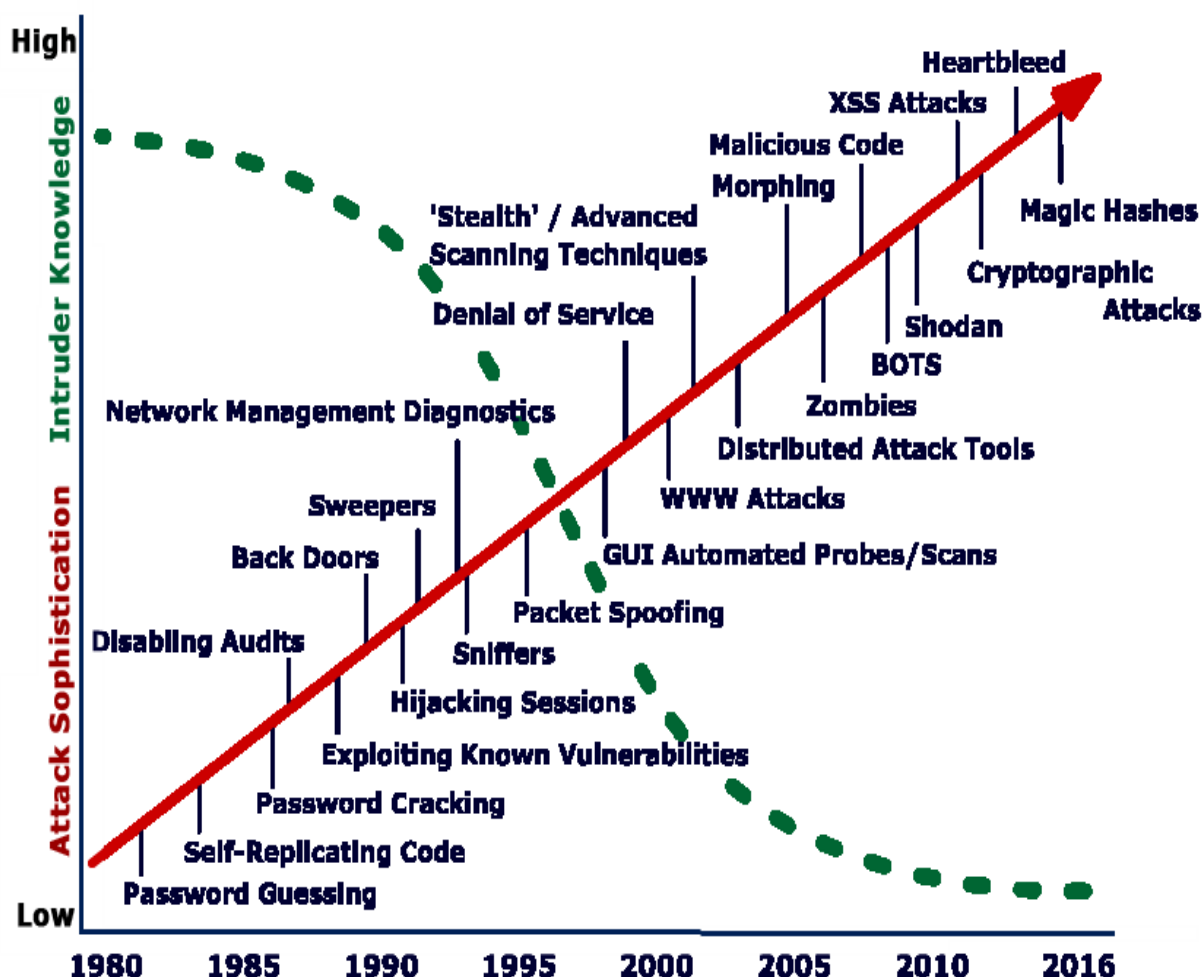


Рисунок 5 – Возрастание сложности атак при снижении общего уровня знаний злоумышленников

Особо выделим, что системотехническая основа современных ИТКС может включать элементы, которые входят в состав систем общего пользования (систем облачных вычислений (англ. *cloud computing*), различных хранилищ и центров обработки данных (ЦОД, англ. *Data Centers*) с множеством ИС и т.п.), что несет повышенную угрозу ее защищенности. Программируемые сети, управляемые ПО, а не аппаратными средствами, обладают рядом уязвимостей, а также создают задержки в обработке трафика управления передачей данных, что позволяет реализовывать компьютерные атаки на уровне ПО. Пятое поколение мобильных сетей (5G), как и

любое новшество, содержит в себе возможности, которыми может воспользоваться злоумышленник, и т.п. Проиллюстрируем только один аспект незащищенности облачных хранилищ, открывающий путь к атакам и представленный в обзоре за 2020 г. компанией Verizon [9]: 22 % нарушений в этом году были связаны с облачными активами, при этом в 71 % зарегистрированных инцидентов были затронуты локальные активы; 70 % атак было совершено внешними нарушителями, организованная преступность имела отношение к 55 % из них; 81% нарушений были обнаружены в течении нескольких дней или раньше; у 58 % жертв были скомпрометированы личные данные; 86 % нарушений имели финансовые мотивы; 43% атак были связаны с веб-приложениями.

1.2.2. Задачи обеспечения информационной безопасности для информационно-телекоммуникационных сетей

Проблема обеспечения ИБ ИТКС ОРГАНИЗАЦИИ является сложной и многоплановой, охватывает ряд важных задач, связанных с применением законодательных, организационных и программно-технических мер и процессов обеспечения ИБ. При создании СОИБ ИТКС положение усложняется тем, что ИТКС, как правило, одновременно оперирует как информацией ограниченного доступа – конфиденциальной, так и открытой (общедоступной) информацией. С другой стороны, несмотря на реализацию в ИТКС современных технологий, методов и средств обеспечения ИБ, число уязвимостей элементов ИТКС в процессе ее эксплуатации не только не уменьшается, но и постоянно возрастает. Поэтому в СОИБ ИТКС должны интегрироваться и комплексно функционировать компоненты общей безопасности, ИБ, управления и контроля.

Необходимость противодействия сложным сетевым атакам является движущей силой разработки новых технологий в области обеспечения ИБ, что требует сложных структур и адекватных подходов к управлению ИБ на различных уровнях: для частных лиц, организаций различного размера, подчиненности и сферы деятельности, а также для более высокого уровня – стран и сохранения мира в целом. В связи с этим субъекты КИИ в соответствии с присвоенной ему категорией значимости [21] (самая высокая – первая, самая низкая – третья) или отсутствием необходимости присвоения категории обязаны соблюдать соответствующие требования по обеспечению безопасности своих ИТКС и создавать системы безопасности, основными задачами которых являются следующие [7, статья 10]:

- 1) предотвращение неправомерных действий, включая доступ, уничтожение, модифицирование, блокирование, копирование, предоставление и распространение информации, обрабатываемой ИТКС ОРГАНИЗАЦИИ;
- 2) недопущение воздействия на технические средства обработки информации, в резуль-

тате которого может быть нарушено и (или) прекращено функционирование ИТКС ОРГАНИЗАЦИИ;

3) восстановление функционирования ИТКС ОРГАНИЗАЦИИ, обеспечиваемого, в том числе, за счет резервирования необходимой для этого информации;

4) непрерывное взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА [25]).

Решение первой задачи базируется на обеспечении высокой **информационной защищенности ИТКС ОРГАНИЗАЦИИ**, которая рассматривается как такая ее способность, при которой в ЕИП ОРГАНИЗАЦИИ создана адекватная защищенная среда ее функционирования, обеспечивающая необходимый уровень ИБ для получения (поиска и сбора), обработки, хранения, распространения (передачи и предоставления) и уничтожения информации. Обобщив определения из [2, 5-7, 22], в целях данного исследования сформулируем следующее понятие: **информационная безопасность информационно-телекоммуникационной сети ОРГАНИЗАЦИИ (ИБ ИТКС ОРГАНИЗАЦИИ)** – состояние защищенности ТС ОРГАНИЗАЦИИ, предназначенных для обработки и передачи по линиям связи информации, доступ к которой осуществляется с использованием современных ИТ, СВТ и средств связи, включающее безопасность информационных ресурсов и предоставляемых услуг и обеспечивающее функциональную устойчивость ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ. При этом уровень риска нарушения осуществления деятельности ОРГАНИЗАЦИИ с использованием ИТКС и уровень риска нарушения всех свойств ИБ информационных активов ИТКС на всех стадиях их жизненного цикла приемлемы как для их пользователя, так и владельца. Защищенность достигается обеспечением совокупности свойств ИБ – конфиденциальности, целостности, доступности, подлинности, подотчетности, неотказуемости и достоверности, приоритетность которых определяется значимостью информации для интересов (целей) ОРГАНИЗАЦИИ.

Тогда *обеспечение ИБ ИТКС ОРГАНИЗАЦИИ* подразумевает осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению угроз ИБ и ликвидации последствий их проявления для ИТКС (адаптировано на основе [2]) (далее это понятие уточнено в главе 3). При этом защиту информационного взаимодействия локальных сегментов ИТКС и отдельных СВТ (например, компьютеров) через открытые сети типа интернета можно свести к качественному и оперативному решению двух базовых задач (рис. 6):

1) защита данных в процессе передачи по открытым каналам связи, высокая результативность которой может быть достигнута за счет реализации следующих связанных между собой и дополняющих друг друга мер обеспечения ИБ, что сделано, например, в виртуальных частных сетях (ВЧС) (англ. *Virtual Private Networks, VPN*):

- аутентификация (установление подлинности) взаимодействующих сторон;
- шифрование передаваемых данных;
- подтверждение подлинности и целостности доставленных данных;
- защита от атак повтором (англ. *replay attack*), задержки и удаления сообщений;
- защита от отрицания фактов отправления и приема сообщений;

2) защита подключенных к публичным каналам связи отдельных сегментов ИТКС и СВТ от несанкционированных действий в первую очередь со стороны потенциально опасной внешней среды путем управления и фильтрации двусторонних потоков данных – входящего и исходящего, а также выполнения функций посредничества при обмене данными, реализованная в межсетевых экранах (МЭ) (англ. *Firewalls*) разного уровня, системах отражения атак типа «распределенный отказ в обслуживании» (*DDoS*-атак), системах обнаружения и предотвращения вторжений (СОВ/СПВ) (англ. *Intrusion Detection and Prevention Systems, IDS/IPS*) и других средствах обеспечения сетевой безопасности.

Вторая и третья задачи означают, что к ИТКС ОРГАНИЗАЦИИ предъявляется требование непрерывно обеспечивать поддержание ее важнейшего интегрального свойства – **функциональной устойчивости** (англ. *operational resilience*) – способности регулировать функционирование с целью поддержания выполнения операций при ожидаемых условиях и в условиях ужесточения требований, нарушений и непредвиденных обстоятельств [23] (сразу оговоримся, что данный термин используется в [2] в формулировке «устойчивость функционирования», в терминологии Банка России это – «операционная надежность», хотя иногда в публикациях еще встречается термин «операционная устойчивость»). В случае потери этого свойства всей ИТКС ОРГАНИЗАЦИИ или ее отдельными элементами в результате компьютерных атак, длительного реагирования и восстановления после них или по другим причинам затронутые информационные ресурсы и услуги становятся недоступными пользователям. Следовательно, функциональная устойчивость ИТКС ОРГАНИЗАЦИИ при воздействии компьютерных атак должна обеспечиваться в двух режимах [24]: «в малом» — при нем достаточно малое отклонение режима работы от исходного (установившегося) с течением времени уменьшается и функционирование ИТКС возвращается в исходное состояние и «в большом» — при нем функционирование ИТКС, получив достаточно большое начальное отклонение, возвращается в исходное состояние после прекращения действия компьютерной атаки. ИТКС как сложной системе, поведение которой основано на акте решения – выборе из альтернатив, присуща активная

форма функциональной устойчивости. Поведение ИТКС при этом является целенаправленным, поскольку ИТКС стремится достигнуть предпочтительного для нее состояния – выполнения цели функционирования.

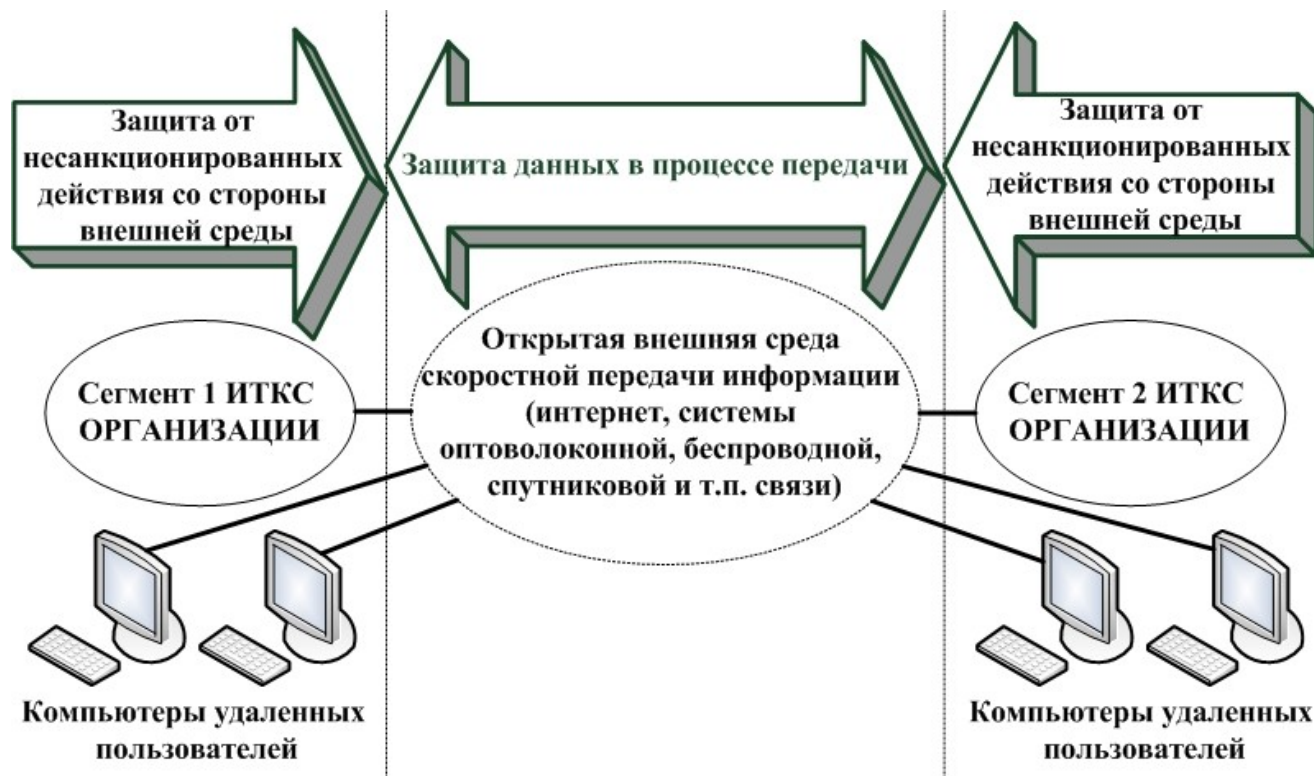


Рисунок 6 – Задачи защиты информационного взаимодействия в ИТКС ОРГАНИЗАЦИИ

Конкретизация четвертой задачи в отношении обязанностей субъектов КИИ приводится в [7, статья 9]. Так, субъекты КИИ обязаны:

1) незамедлительно в установленном порядке информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования ГосСОПКА, и, если субъект КИИ осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, то и Центральный банк РФ;

2) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах КИИ средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на инциденты ИБ, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

Четвертая задача может быть решена наиболее результативным образом за счет создания соответствующей структурной единицы, интегрированной в ИТКС ОРГАНИЗАЦИИ, наделен-

ной должными полномочиями и имеющей необходимые инструментальные средства и компетенции для непрерывного и квалифицированного взаимодействия с ГосСОПКА с целью обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы ИТКС ОРГАНИЗАЦИИ субъекта КИИ. Эта же структурная единица должна быть способна решать и первые три задачи, реализуя упреждающую стратегию обеспечения ИБ и, в конечном счете, функциональная устойчивость ИТКС ОРГАНИЗАЦИИ. Принцип упреждающего управления сетевой безопасностью ИТКС в первую очередь заключается в принятии решений в отношении возможных инцидентов ИБ до их появления, направленном на предотвращение и минимизацию их последствий за счет постоянного интеллектуального анализа в определенном контексте всех консолидированных (совместно рассматриваемых и анализируемых) данных о происходящих в ИТКС событиях, имеющих отношение к ИБ, прогнозирования развития ситуации и своевременной установки «барьеров защиты» на пути распространения таких действий. Под **событием ИБ** (англ. *information security event, IS event*) понимается идентифицированное появление определенного состояния актива организации (системы, сервисы или сети), указывающего на возможное нарушение Политики обеспечения ИБ (далее – Политики ИБ) или нарушения в работе средств защиты, либо возникновение ранее неизвестной ситуации, которая может иметь отношение к ИБ [68]. Соответственно, **инцидент ИБ** (англ. *information security incident, IS incident*) заключается в появлении одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операций и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации [68].

1.2.3. Эволюция технологий и средств обеспечения сетевой безопасности

Реализуемые в настоящее время реактивные меры обеспечения ИБ (англ. *reactive security controls*) для информационных ресурсов ИТКС ОРГАНИЗАЦИЙ с целью минимизации времени их восстановления (длительности реагирования) после прерываний, вызванных инцидентами ИБ, были разработаны два-три десятилетия назад. В 2005-2006 гг. компанией Cisco Systems была впервые озвучена идея разработки Центра мониторинга безопасности (ЦМБ) (англ. *Security Operations Center, SOC*) [10-12], которому в русскоязычных публикациях долгое время соответствовали разные термины типа «система централизованного мониторинга ИБ» или «центр координации деятельности по ИБ» [13], «координирующий центр мониторинга ИБ» или «ситуационный центр мониторинга ИБ» (например, [14, 15]) или просто SOC. Основными целями разворачивания ЦМБ Cisco определил управление СЗИ в сетях (например, ВЧС (VPN), МЭ, СОВ/СПВ (IDS/IPS), системами отражения DDoS-атак, решениями для борьбы с вредоносным

кодом, вирусами и шпионскими программами) и мониторинг их состояния в режиме реального времени, а также анализ записей в журналах регистрации событий (ЖРС) (англ. *log files/audit trails/audit logs*), сведений об уязвимостях, информации о ресурсах и предупреждений об опасности (англ. *alert/alarms*).

Перечисленные средства обеспечения сетевой безопасности уже прошли достаточно большой эволюционный путь начиная с 1970 г., основные вехи которого с 1984 по 2011 гг. представлены в работе [69]. После анализа главных тенденций в области сетевой безопасности, представленных в материалах разработчиков и на многочисленных международных конференциях последнего десятилетия, эти вехи были дополнены и расширены до настоящего времени автором данного исследования (табл. 1). Жирным шрифтом в таблице помечены дополнения и уточнения по сравнению с [69].

Таблица 1 – Эволюция технологий и средств обеспечения сетевой безопасности (начало)

ГОДЫ	ТЕХНОЛОГИИ	СРЕДСТВА
2018	<i>XDR (Extended Detection and Response)</i> как сочетание <i>EDR, UEBA, NTA</i> и некоторых других технологий, где <i>X</i> обозначает любой источник данных, <i>D</i> – обнаружение, <i>R</i> – реагирование	ПО мониторинга сотрудников (<i>Employee Monitoring (EM) Monitoring Software</i>)
2017	Оркестровка безопасности и автоматическое реагирование/ Действия, аналитика и отчетность по безопасности (<i>Security Orchestration, and Automated Response / Security Operations, Analytics and Reporting, SOAR</i>), Аудит и защита, ориентированные на данные (<i>Data-Centric Audit and Protection, DCAP</i>), Анализ сетевого трафика (<i>Network Traffic Analysis, NTA</i>), Управление привилегированным доступом (<i>Privileged Access Management, PAM</i>)	Брокер безопасности облачного доступа (<i>Cloud Access Security Broker, CASB</i>)
2015	Анализ поведения пользователей и сущностей/ Анализ безопасности поведения пользователей (<i>User and Entity Behavior Analytics / Security User Behavior Analytics, UEBA/SUBA</i>)	
2013	Обнаружение и реагирование на угрозы для конечных точек (<i>Endpoint Threat Detection and Response / Endpoint Detection and Response, ETDR/EDR</i>)	Платформа реагирования на инциденты безопасности (<i>(Security) Incident Response Platform, (S)IRP</i>)
2011	«Охота за угрозами» (<i>Threat Hunting</i>)	
2010	Использование знаний о контексте (<i>Context Awareness</i>)	Система предотвращения вторжений нового поколения (<i>Next-Generation Intrusion Prevention System, NGIPS</i>)
2008-2009	Использование знаний о пользователях и приложениях (<i>User/Application Awareness</i>)	Средства защиты следующего поколения (<i>Next-Generation</i>), МЭ следующего поколения (<i>Next-Generation Firewall, NGFW</i>), Шлюзы безопасности веб-среды (<i>Secure Web Gateway, SWG</i>)

Таблица 1 – Эволюция технологий и средств обеспечения сетевой безопасности (окончание)

2007	Управление уязвимостями и обновлениями безопасности (<i>Vulnerability/Patch Management</i>)	
2006	Предотвращение утечки данных (<i>Data Loss Prevention, DLP</i>)	
2005	Управление учётными данными и доступом (<i>Identity and Access Management, IAM</i>), Управление информацией и событиями безопасности (<i>Security Information and Event Management, SIEM</i>)	Центр мониторинга безопасности (<i>Security Operations Center, SOC</i>)
2004	Технология полной инспекции контента (<i>Full Content Inspection</i>) Интеллектуальное управление угрозами (<i>Threat Intelligence</i>)	Средство унифицированного управления угрозами (<i>Unified Threat Management, UTM</i>), ПО для защиты от мошенничества (<i>Anti-Fraud Software</i>)
2002		URL-фильтрация, МЭ веб-приложений (<i>Web Application Firewall, WAF</i>)
2001	Контроль исходящих коммуникаций (<i>Outbound Control</i>), Технология «глубокой» инспекции пакетов (<i>Deep Packet Inspection, DPI</i>)	Системы предотвращения вторжений (<i>Intrusion Prevention System, IPS</i>), Средства защиты от DDoS-атак (<i>Anti-DDoS</i>), Виртуальные частные сети (<i>Virtual Private Network, VPN</i>)
Бум сетевой безопасности	Технология «поверхностной» инспекции пакетов (<i>Shallow Packet Inspection</i>)	
1992		Сканер анализа защищенности (<i>Security Scanner</i>)
1991	Технология инспекции пакетов «средней глубины» (<i>Medium Depth Packet Inspection</i>)	МЭ – посредник приложений (<i>Application Proxy Firewall</i>)
1988	Технология инспекции пакетов на основе состояний (<i>Stateful Packet Inspection, SPI</i>)	Межсетевой экран (<i>Firewall</i>)
1987	Пакетная фильтрация (<i>Packet Filtering</i>)	
1984	Распознавание сигнатур (<i>Signature Detection</i>)	Система обнаружения вторжений (<i>Intrusion Detection System, IDS</i>)
1983	Аутентификация уровня сети (<i>Network Authentication</i>)	Антивирус (<i>Anti-Virus</i>)
1970е	Распознавание человека по биометрическим признакам (<i>Biometrics</i>)	

В 1970-е годы появились различные технологии распознавания человека по биометрическим признакам (сначала по лицу, голосу, отпечаткам пальцев, а потом и по клавиатурному почерку, радужной оболочке глаза и т.п.), которые затем стали использоваться для биометрической аутентификации пользователей компьютерных систем (краткое англ. *biometrics*) [70].

В 1983 г. в Массачусетском технологическом институте (MIT) была разработана первая версия протокола *Kerberos*, созданного для осуществления сетевой аутентификации (англ. *network authentication*) [71].

Распознавание сигнатур (типичных признаков) простейшими в то время COB (*IDS*) [72] и первыми антивирусами (с 1983 г.) [73] сменилось пакетной фильтрацией (англ. *packet*

filtering), реализуемой МЭ (1988 г., [74]) (первым появился DEC Packet Filter Firewall от Digital Equipment Corporation). Далее МЭ были усовершенствованы применением технологии инспекции пакетов на основе анализа состояний (англ. *Stateful Packet Inspection, SPI*) и чуть позднее, в 1991 г., появился МЭ – посредник приложений (англ. *Application Proxy Firewall*), кратко называемый МЭ приложений (англ. *Application Firewall*). Третье поколение МЭ базировалось на технологии инспекции пакетов «средней глубины» (англ. *Medium Depth Packet Inspection*) [75].

С 1992 г. известны системные и сетевые сканеры анализа защищенности (САЗ) (англ. *Security Scanner*), включающие современные средства тестирования безопасности приложений (англ. *Application security testing, AST*) [76].

В период с 1993 по 2001 гг. отмечался особый расцвет рынка СЗИ. Например, второе поколение МЭ реализовывало технологию «поверхностной» инспекции пакетов (англ. *Shallow Packet Inspection*) с конца 90-х годов XX века [75]. С 2001 г. в особый класс выделились средства защиты от DDoS-атак, появились СПВ (IPS) [77], ВЧС (VPN) [78] и была создана технология «глубокой» (всесторонней) инспекции пакетов (англ. *Deep Packet Inspection, DPI*), ставшая базовой для МЭ этого периода [75].

Далее в 2002 г. последовала разработка технологии контроля всех исходящих коммуникаций (англ. *Outbound Control, OC*), МЭ для межсетевого экранирования веб-приложений (англ. *Web Application Firewall, WAF*), работающие на основе «белых» и «черных» списков (англ. *whitelists and blacklists*), и средств фильтрации унифицированных указателей ресурсов (англ. *Uniform Resource Locator, URL*) [79].

С 2004 г. основной акцент защиты был сделан на проверку контента (содержания), и возникла технология его полной инспекции (англ. *Full Content Inspection, FCI*) [76]. Появились средства унифицированного управления угрозами (англ. *Unified Threat Management, UTM*), сочетающие в себе, в первую очередь, функционал МЭ, СПВ и антивирусов [80] и первые решения для защиты от мошенничества – *Anti-Fraud Software*. В 2004 г. впервые начали обсуждаться вопросы интеллектуального управления угрозами (англ. *Threat Intelligence*) [81].

В 2005 г. компания Cisco предложила концепцию ЦМБ (SOC) [10], а исследовательская и консалтинговая компания Gartner впервые описала централизованное управление учётными данными и доступом (англ. *Identity and Access Management, IAM*) [82] и управление информацией и событиями безопасности (от англ. *Security Information and Event Management, SIEM*) [83].

2006 г. отмечен в истории появлением первых систем, реализующих идею предотвращения утечки данных (англ. *Data Loss Prevention, DLP*) [84].

2008-2009 гг. ознаменовали появление средств защиты следующего поколения (англ. *Next-Generation, NG*), понимающих работу пользователей и приложений (англ. *Application/User awareness*) и способных фильтровать информацию в зависимости от контекста (англ. *Context*

awareness) [69]. Примеры новинок рынка – МЭ (англ. *NGFW*) и СПБ (англ. *NGIPS*) нового поколения и шлюзы безопасности веб-среды (англ. *Secure Web Gateway, SWG*) [70]. В это же время активно заговорили о практике управления уязвимостями (англ. *Vulnerability Management*) и установкой обновлений безопасности (англ. *Patch Management*) для их устранения [85].

В качестве небольшого отступления приведем статистику за 2009-2010 гг. (рис. 7), собранную американским институтом Computer Security Institute в 15-ом ежегодном обзоре по компьютерным преступлениям и безопасности «2010/2011 CSI Computer Crime and Security Survey» [86], показывающую, что самыми распространенными были антивирус, МЭ, средства защиты от шпионского ПО, *VPN*, средства управления уязвимостями и установкой обновлений безопасности, средства шифрования передаваемых по линиям связи данных и COB.

Предположительно в 2011 г. возникла идея упреждающего циклического процесса «охоты за угрозами» (англ. *Threat Hunting*), которая принадлежит Р. Бейтслиху [87].

В 2013 г. сотрудник компании Gartner А.Чувакин ввел термин «обнаружение и реагирование на угрозы для конечных точек» (англ. *Endpoint Threat Detection and Response/Endpoint Detection and Response, ETDR/EDR*) [88]. Эти системы также известны под более широким названием – «платформы реагирования на инциденты безопасности» (англ. *(Security) Incident Response Platform, (S)IRP*), которые в 2017 г. стали интегрироваться в *SOAR*-системы (англ. *Security Orchestration, and Automated Response, SOAR*).

В 2015 г. компания Gartner определила новый подход, ориентированный на ЖРС (англ. *log-centric*) и названный «анализ поведения пользователей и сущностей» (англ. *User and Entity Behavior Analytics, UEBA*) [89], который компания Forrester обозначает как «анализ безопасности поведения пользователей» (англ. *Security User Behavior Analytics, SUBA*), а компания IDC как «анализ поведения пользователей» (англ. *User Behavioral Analytics, UBA*).

В 2017 г. компания Gartner ввела термин «оркестровка безопасности и автоматическое реагирование» (*SOAR*; значение первого слова в переводе лучше передается по смыслу словом «интеграция»), который расшифровывается и несколько иначе – «действия, аналитика и отчетность по безопасности» (англ. *Security Operations, Analytics and Reporting, SOAR*) [54, 90]. Также в 2017 г. появились системы, реализующие с учетом контекста и контента аудит и защиту, ориентированные на структурированные и неструктурированные данные (англ. *Data-Centric Audit and Protection, DCAP*) [91]. Стали обсуждаться системы, реализующие анализ сетевого трафика (англ. *Network Traffic Analysis, NTA*) с учетом активности пользователей и приложений и поддержкой технологии *DPI* [92]. В отдельный класс из *IAM* выделились системы, управляющие привилегированным доступом (англ. *Privileged Access Management, PAM*) с учетом контекста [93]. В это же время стали говорить о брокере безопасности облачного доступа (англ. *Cloud Access Security Broker, CASB*) [94].

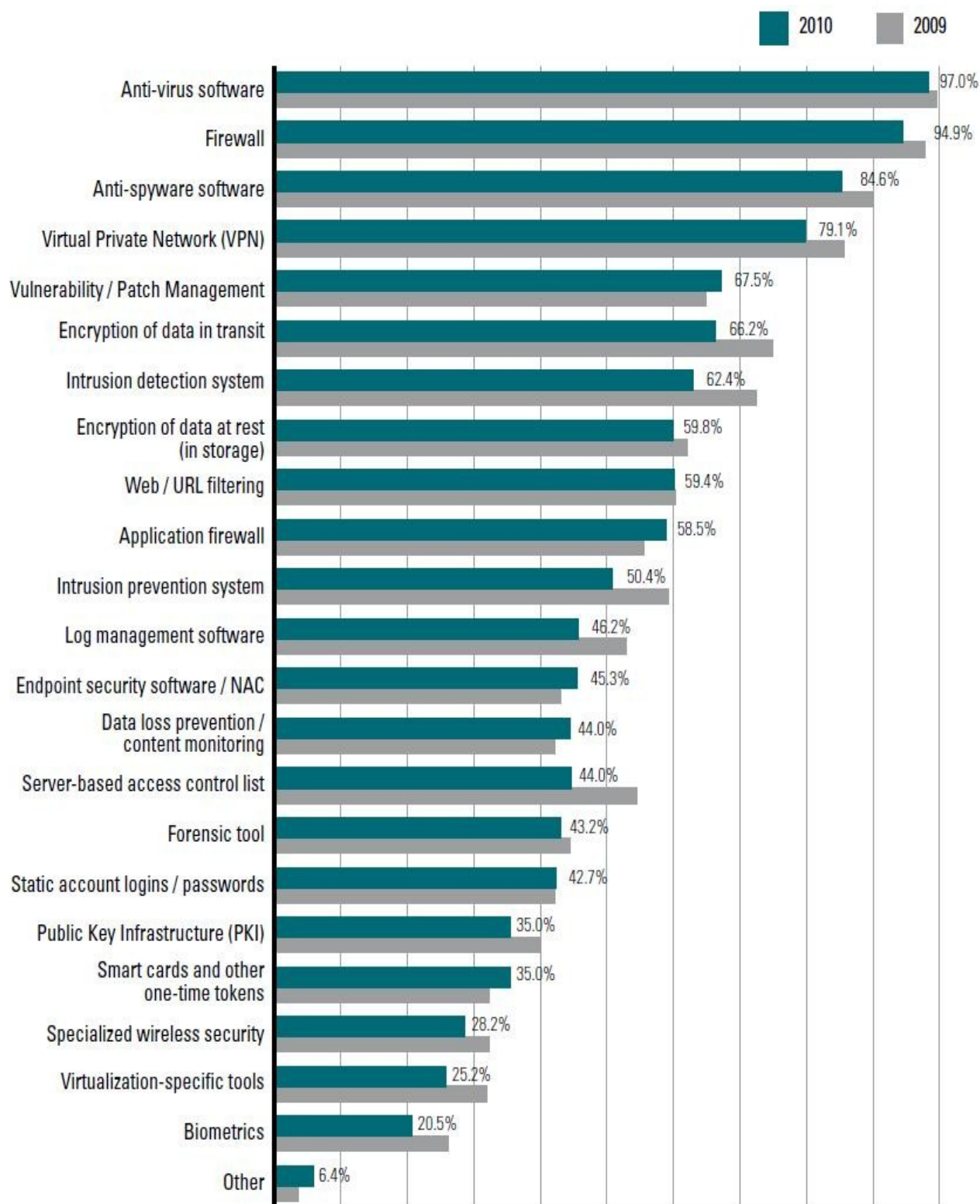


Рисунок 7 – Использование средств обеспечения сетевой безопасности в 2009-2010 гг. [86]

На год позже – в 2018 г. – были представлены системы *Employee Monitoring (EM) Software*, занимающиеся мониторингом работы сотрудников организаций и фиксирующие запуск ими программ, использование файлов и БД, передачу информации на внешние устройства и пр. с учетом контекста [95].

Самым новым подходом считается *XDR* (англ. *Extended Detection and Response*), который

сочетает в себе возможности *EDR*, *UEBA*, *NTA* и некоторых других средств, где «X» обозначает любой источник данных, такой как сеть, конечная точка или облако, а «D» и «R» – это обнаружение и реагирование соответственно [96]. Системы, реализующие эту технологию, собирают и сопоставляют данные электронной почты, конечных точек, серверов, анализируют нагрузку в облаках и сетях, обеспечивая тем самым видимость и контекст для сложных угроз и расставляя приоритеты для их устранения и предотвращая потерю данных и инциденты ИБ.

Для сравнения с рис. 7 приведены результаты опроса, который проводился в 2019 г. в Европейском сообществе (рис. 8) [97]. 92 % предприятий стран ЕС используют различные меры обеспечения безопасности для ИКТ, 87 % обновляют ПО, 76 % применяют аутентификацию со стойкими паролями и столько же хранят резервные копии данных отдельно от основных средств их обработки, 65 % используют средства контроля доступа к сетям. Меньше половины опрошенных (45 %) анализируют ЖРС после свершившихся инцидентов ИБ. 42 % шифруют данные, документы и сообщения электронной почты. Только треть (35 %) проводят тесты защищенности и оценивают риски для используемых ИКТ. Биометрия интересует в два раза меньшее количество организаций по сравнению с данными десятилетней давности (10 % против 20%).

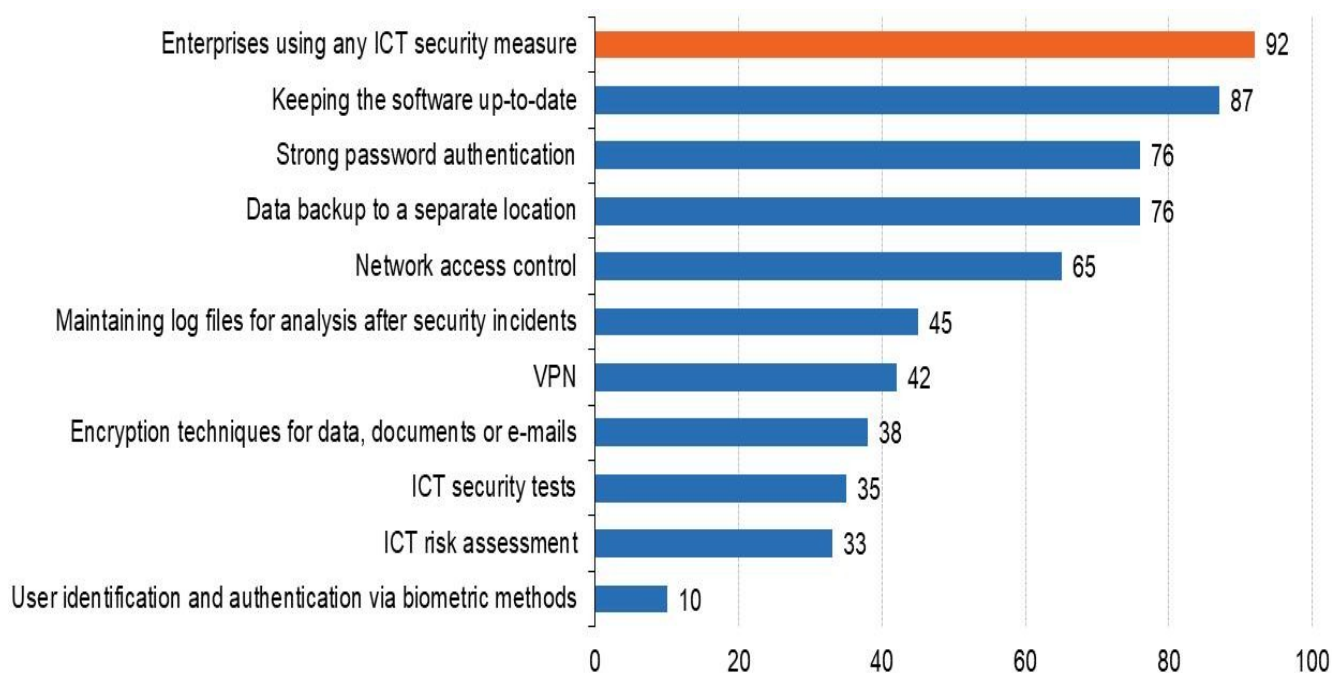


Рисунок 8 – Использование мер обеспечения безопасности ИКТ в 2019 г. на предприятиях стран Европейского сообщества [97]

В повседневной деятельности современных организаций из разных источников генерируется огромный объем данных о текущем состоянии ИТКС и несвязанных на первый взгляд событиях, происходящих в них. Эти данные должны быть корректно и оперативно обработаны для выявления инцидентов ИБ и определения тех областей ИТКС, которые подвержены наибольшему риску и требуют его быстрого устранения. Данные поступают не только от *DNS*-

серверов, контроллеров доменов, прокси-серверов, СЗИ, а также содержат текущие конфигурационные настройки сетевых устройств, характеризуют особенности сетевого трафика, работу приложений и сетевых сервисов, конкретные действия отдельных конечных пользователей, электронную почтовую переписку, звонки IP-телефонии и конференцсвязи, веб-контент, метаданные, цифровое аудио и видео, геолокации, данные бизнес-процессов, внутренние документы и аналитические данные ОРГАНИЗАЦИИ за многие годы ее существования [41]. Все эти данные следует рассматривать в конкретном контексте и оценивать с точки зрения любого инцидента ИБ с целью найти его источник, определить его тип, взвесить его последствия, визуализировать его направление, связать все вовлеченные в него и целевые системы, приоритезировать меры обеспечения ИБ и предложить обоснованные решения для быстрого реагирования на инцидент ИБ. Крайне важно знать, какие угрозы ИБ существуют в данный момент в ИТКС, как они могут перерасти в инцидент ИБ, а затем повлиять на деятельность ОРГАНИЗАЦИИ, особенно если это приведет к раскрытию конфиденциальных данных, краже интеллектуальной собственности и прерыванию предоставления услуг потребителям, поставить под угрозу репутацию или финансовое благополучие и т.д.

1.2.4. Необходимость сложной аналитики данных для обеспечения сетевой безопасности

Постоянно увеличивающиеся объемы, скорость поступления и неоднородность данных от гетерогенных источников породило известную проблему больших данных и связанную с ними деятельность по дальнейшему скрупулезному мониторингу и анализу их с точки зрения нарушения ИБ. Так, по данным Сбербанка, его система фрод-мониторинга, блокирующая подозрительные транзакции, анализировала в 2018 г. около 150 млн. операций в сутки, 625000 в час, 104166,6(6) в минуту, 1736,1(1) в секунду [98]. Более ранний расчет был представлен в работе сотрудника компании Gartner А.Чувакина [99]: если рассмотреть организацию с одним головным офисом и несколькими региональными филиалами, имеющую в 2012 г. около 25 различных сетевых устройств и СЗИ для мониторинга (типа МЭ, системы IAM, СОВ/СПВ, веб-сервера, почтового сервера, сервера БД, прокси-сервера, антивируса, различных приложений безопасности и т.д.), то в сети этой организации события фиксировались в ЖРС со скоростью около 30000 событий/с. Это были не пиковая скорость, а усредненная за 24 часа. Таким образом, размерность ЖРС составляла порядка 750 тыс. потенциальных событий для анализа. Некоторые события относились только к функционированию систем, некоторые были связаны с ИБ, а некоторые относились сразу к обеим этим категориям. Уменьшая интересные с точки зрения ИБ типы событий, например, до 25 %, получим число данных для анализа в 187,5 тыс. единиц. В начале исходные данные умножались всего лишь на 25 отдельных устройств. В современных

ИТКС их на порядки больше. Независимо от самоотверженности и квалификации, сотрудники службы ИБ не могут справляться с подлежащими анализу объемами данных, передаваемых по ИТКС ОРГАНИЗАЦИИ с той же скоростью, с которой связанные с этим события происходят. Поэтому остро встает проблема структурированного, консолидированного и визуализированного представления определенным образом проанализированных «сырых» (англ. *raw*) данных, относящихся к ИБ, для принятия своевременных, наиболее рациональных и обоснованных решений по корректировке текущей ситуации, связанной с состоянием ИБ ИТКС. Но перспективнее, если в результате анализа будут выявлены некоторые тенденции и получен прогноз на будущее – какие инциденты ИБ могут произойти и как их избежать, устранив соответствующие факторы и уязвимости.

ЦМБ первого поколения не были рассчитаны на сложную корреляцию и аналитику всех происходящих в ИТКС событий как основы полноценного управления, а не просто мониторинга ИБ. Результатом являлось неудовлетворительное время обнаружения инцидентов ИБ. К сожалению, единой общемировой статистики по времени их обнаружения не существует; время существенно различает в отчетах разных исследовательских компаний. Но общие тенденции выявить можно. Так, например, известный в мире ИБ центр Ponemon Institute (США) в отчете 2019 г. отмечает, что компании необходимо в среднем 276 дней (против 197 в 2018 г.) для выявления инцидентов, связанных с утечкой данных [14]. Некоторые исследования показывают, что большинство инсайдерских атак выявляются в течение минут (22 % опрошенных), часов (28 %) или одного дня (26 %) (Crowd Research Partners 2018 Insider Threat Report, [15]). Другое исследование показывает, что для выявления такого нарушения требуется от нескольких месяцев (30 % опрошенных) до нескольких лет (40 %) (Verizon 2019 Insider Threat Report: Executive Summary, [16]). И это при том, что, согласно Website hacking statistics of 2020 [17], хакеры атакуют каждые 39 секунд, в среднем 2244 раза в день; они крадут 75 записей каждую секунду (источник: Breach Level Index); в среднем 30000 новых веб-сайтов взламываются каждый день (источник: Forbes); 73 % «черных» хакеров заявили, что традиционный МЭ и антивирусная защита неактуальны или устарели (источник: Thycotic.com); они ежедневно создают 300000 новых вредоносных программ (источник: McAfee).

Из выше представленного, следует вывод, что до настоящего времени никаких прорывных решений на рынке средств обеспечения сетевой безопасности, чем в свое время являлись СОВ, МЭ, СПВ и ВЧС, так и не появлялось, хотя этого очень ждут, например, экосистемы *IoT* [100] и облачные и виртуальные системы. При всем многообразии перечисленных технологий и средств обеспечения сетевой безопасности дальнейшего повышения требуют в первую очередь качество и результативность управления сетевой безопасностью в ЦМБ, поскольку они существенно отстают от требуемого сегодня уровня. Организации все больше понимают, что своевре-

менное выявление инцидентов ИБ и, что более важно, предотвращение их в будущем не только возможно, но и необходимо. Любые задержки и только ответные действия на инциденты ИБ подвергают риску активы и услуги, предоставляемые на базе их ИТКС, и всю деятельность ОРГАНИЗАЦИИ в целом. Следовательно, только описательной и диагностической аналитики недостаточно; нужна аналитика прогнозирующая и предписывающая.

1.2.5. Понятие сетевой безопасности для информационно-телекоммуникационной сети

Очевидно, что стоит проблема обеспечения информационной защищенности ИТКС организаций и ее информационных ресурсов на всех этапах их жизненного цикла в условиях угроз ИБ в ЕИП ОРГАНИЗАЦИИ, решение которой может быть достигнуто за счет разработки методологии и принципов поддержания функциональной устойчивости ИТКС от проектирования и внедрения до совершенствования, развития и масштабирования, а также при возникновении отказов в работе, требующих реструктуризации системотехнической составляющей ИТКС (например, немедленный перевод обработки данных на резервную площадку после выхода из строя основной). Все эти процессы могут быть поддержаны в рамках создания специализированного структурного элемента ИТКС ОРГАНИЗАЦИИ, призванного осуществлять управление ИБ информационных ресурсов ИТКС на всех стадиях жизненного цикла на основе использования современных интеллектуальных подходов и названного «Центр интеллектуального управления сетевой безопасностью» (ЦИУСБ). При этом сам ЦИУСБ должен входить в состав СОИБ ИТКС, быть с ним жестко связан и влиять на ее развитие и совершенствование.

Построение СОИБ ИТКС при использовании имеющихся в настоящее время подходов и на традиционных технологиях, которые показали себя в последнее время нерезультативными, требует кардинально новых подходов. Таким образом, основным требованием сегодняшнего времени является обеспечение надлежащей защиты сетей и связанных с ними ИС, информации и услуг, называемой далее сетевой безопасностью. При этом под ***сетевой безопасностью ИТКС*** (от англ. *network security*) будем понимать безопасность устройств ИТКС, безопасность деятельности по управлению этими устройствами, приложениями, предоставляемыми услугами и конечными пользователями, в дополнение к безопасности информации, передаваемой по линиям связи ИТКС (адаптировано на основе [60]).

В дальнейших рассуждениях потребуются понимание соотношения информационной и сетевой безопасности. Оно наглядно представлено в международном стандарте ISO/IEC 27032:2012 [101] (рис. 9) и в целом согласуется с ГОСТ Р ИСО/МЭК 27033-1-2011 [60], в котором отмечается, что ИБ пересекается с сетевой безопасностью в части обеспечения свойств ИБ информационных ресурсов, обрабатываемых, передаваемых и хранимых в сетях. При этом в

сетевой безопасности есть еще, по крайней мере, две части, относящиеся к рассмотрению безопасности сетевых устройств и безопасности деятельности по управлению ими. Но в ISO/IEC 27032:2012 есть и ряд несоответствий с ГОСТ Р ИСО/МЭК 27033-1-2011, связанных, например, с не совсем корректным (с точки зрения автора данного исследования) изображением безопасности приложений, ибо функционирование сетей поддерживается большим количеством разнообразных сетевых приложений.



Рисунок 9 – Соотношение понятий ИБ и сетевой безопасности согласно ISO/IEC 27032:2012 [101]

Таким образом, в данной главе было показано, что имеется проблема, требующая как скорейшего решения для реализации и поддержки адекватной современным угрозам ИБ СОИБ ИТКС, абсолютно необходимой для успеха деятельности организаций. Использование новейших методов обработки и хранения данных предоставляет широкие возможности получать новую информацию о текущем состоянии и тенденциях в области обеспечения ИБ ИТКС ОРГАНИЗАЦИИ и на ее основе синтезировать новые знания о будущих возможных уязвимостях и угрозах ИБ, а также позволяет обоснованно прогнозировать развитие событий и внедрять комплексное упреждающее управление сетевой безопасностью ИТКС для защиты ее информационных ресурсов.

1.3. Нормативная и правовая база в области обеспечения информационной безопасности, применимая к объекту исследования и использованная для разработки глоссария - предметной области исследования

Стандарты и иные документы, которые составляют нормативную и правовую базу данного исследования, можно представить в виде следующей иерархии (рис. 10).



Рисунок 10 – Нормативная и правовая база исследования

1.3.1. Правовая база исследования

Среди правовых и организационно-распорядительных документов самыми важными в рамках данного исследования являются следующие:

— Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; принят Государственной Думой 8 июля 2006 г.; одобрен Советом Федерации 14 июля 2006 г. [6];

— Федеральный Закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; принят Государственной Думой 12 июля 2017 г.; одобрен Советом Федерации 19 июля 2017 г. [7];

— Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [3];

— Указ Президента Российской Федерации от 12 декабря 2014 г. № К 1274 «О Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [25];

— Доктрина информационной безопасности Российской Федерации; утверждена Указом Президента Российской Федерации № 646 от 05.12.2016 [2];

— Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [21];

— Приказ Федеральной Службы Безопасности Российской Федерации от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» [102];

— Паспорт национального проекта. Национальная программа «Цифровая экономика Российской Федерации»; утверждён решением президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г. [4].

1.3.2. Нормативная база исследования

Основу нормативных документов исследования составили следующие:

Специальные нормативные документы:

— Федеральная служба по техническому и экспортному контролю. Информационное сообщение об утверждении требований к межсетевым экранам от 28.04.2016 № 240/24/1986 [103];

ГОСТы:

— ГОСТ 15971-90 «Системы обработки информации. Термины и определения» [104];

— ГОСТ 27.004-85 «Надежность в технике (ССНТ). Системы технологические. Термины и определения» [56];

— ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования» [105];

— ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [106];

— ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [107];

— ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Уг-

розы, методы проектирования и вопросы управления» [108];

— ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» [109];

— ГОСТ 34.321-96 «Информационные технологии (ИТ). Система стандартов по базам данных. Эталонная модель управления данными» [59];

— ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» [110];

— ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [111];

— ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» [112];

— ГОСТ Р 51513-99 «Совместимость технических средств электромагнитная. Оборудование распределительных сетей приемных систем телевидения и радиовещания. Нормы электромагнитных помех, требования помехоустойчивости и методы испытаний» [62];

— ГОСТ Р 52653-2006 «Информационно-коммуникационные технологии в образовании. Термины и определения» [113];

— ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» [22];

— ГОСТ Р 53801-2010 «Связь федеральная. Термины и определения» [114];

— ГОСТ Р 54619-2011 «Глобальная навигационная спутниковая система. Система экстренного реагирования при авариях. Протоколы обмена данными автомобильной системы/устройства вызова экстренных оперативных служб с инфраструктурой системы экстренного реагирования при авариях» [115];

— ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» [116];

— ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» [117];

— ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» [60];

— ГОСТ Р ИСО/МЭК 38500-2017 «Информационные технологии (ИТ). Стратегическое управление ИТ в организации» [118];

— ГОСТ Р ИСО 7498-2-99 «Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации» [119];

— ГОСТ Р ИСО/МЭК 9594-8-98 «Информационная технология (ИТ). Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации» [120];

Рекомендации в области стандартизации:

— Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» [121];

— Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» [122];

Европейские стандарты Международной организации по стандартизации (ИСО, англ. International Organization for Standardization, ISO) и Международной электротехнической комиссии (МЭК, от англ. International Electrotechnical Commission, IEC), а именно серия стандартов семейства 27000, посвященная системам управления ИБ (СУИБ) (далее перечисляются только те стандарты, которые не имеют гармонизированных российских ГОСТов):

— ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary (Общий обзор и терминология) [123];

— ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (Требования) [124];

— ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity (Руководство по кибербезопасности) [101];

— ISO/IEC 27033-2:2012 Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security (Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации сетевой безопасности) [125];

— ISO/IEC 27033-4:2014 Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways (Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности) [126];

— ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management (Управление инцидентами ИБ — Часть 1. Принципы управления инцидентами) [68];

— ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response (Часть 2. Руководящие принципы планирования и подготовки для реагирования на инциденты) [127];

— ISO/IEC 27041:2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method (Руководящие указания по обеспечению пригодности и адекватности метода расследования инцидентов) [128];

— ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence (Руководящие указания по анализу и интерпретации свидетельств в цифровой форме) [129];

— ISO/IEC 27043:2015 Information technology — Security techniques — Incident investiga-

tion principles and processes (Принципы и процессы расследования инцидентов) [130];

Специальная публикация Национального института стандартов и технологий США (англ. *National Institute of Standards and Technology, NIST*):

— NIST Special Publication 800-61. Revision 2. 2012. Computer Security Incident Handling Guide (Руководство по обработке инцидентов компьютерной безопасности) [131];

Ведомственные нормативные документы:

— Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [65];

— Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» [66].

Все перечисленные документы были использованы для создания глоссария основных терминов, упоминаемых в данном исследовании. Многие существующие определения, связанные с ИБ, могут быть приняты с точки зрения практики, но они не отражают специфику современного информационного общества и требуют их согласования с современными научными взглядами. Поэтому предлагаются и объясняются собственные определения. Разработанный глоссарий в полном объеме представлен после заключения и содержит 205 терминов, включая такие термины как «ИБ», «угроза ИБ», «уязвимость», «источник угрозы ИБ», «сетевая атака», «событие ИБ», «инцидент ИБ», «риск нарушения ИБ», «функциональная устойчивость ИТКС» и многие другие. Они были введены в разных работах автора, например, в [45-47, 132].

1.4. Цель и задачи исследования

На основе проведенного анализа типовой ИТКС ОРГАНИЗАЦИИ с информационной и телекоммуникационной точек зрения и средств обеспечения ее ИБ можно заключить, что современные достижения в области ИКТ формируют благоприятные условия для создания ИТКС как основы построения ЕИП ОРГАНИЗАЦИИ. Эти условия определяются теми возможностями, которые предоставляют сложные пространственно и функционально распределенные иерархические человеко-машинные открытые системы с централизованным управлением в целом и централизованно-децентрализованным управлением их отдельными элементами и в которых на основе интегрированной совокупности технических и программных средств, обеспечивающих автоматизацию всех информационных сфер деятельности ОРГАНИЗАЦИЯ, сочетаются машинная обработка информации с применением СВТ и средств связи с деятельностью человека, выступающего в качестве потребителя информационных и телекоммуникационных услуг, предоставляемых ИТКС.

В составе ИТКС, к которым предъявляются требования по обеспечению ИБ, обязательно имеется СОИБ, объединяющая различные подсистемы обеспечения ИБ для создания единой защищенной среды обработки данных и поддерживающая информационную защищенность ИТКС на основе применения многоуровневого (эшелонированного) подхода и использования современных технологий и средств защиты информации в процессе всего жизненного цикла обрабатываемой информации.

В то же время следует сознавать, что с ростом компьютерных атак возрастает значение адекватного построения и эксплуатации СОИБ ИТКС с учетом следующих факторов:

1) увеличивается потенциальный ущерб, который может быть нанесен ОРГАНИЗАЦИИ в результате нарушения функциональной устойчивости ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ и в результате преодоления обеспечения ИБ ИТКС в целом и ее отдельных элементов, которая особенно чувствительна к несанкционированным действиям и ошибкам обслуживающего персонала;

2) существенно возрастает объем данных, характеризующих среду функционирования ИТКС и являющихся результатом обработки данных пользователей и ИС, собираемых из гетерогенных источников, причем также возрастает потребность в обработке этих данных в режиме реального времени (чаще жесткого, но и мягкого тоже);

3) традиционных подходов для управления и анализа собранных данных уже не хватает, и требуются более интеллектуальные методы, которые смогут анализировать эти данные совместно в определенном контексте с максимальным использованием возможностей автоматизации всех рутинных операций и реагирования в зависимости от получаемых результатов ИБ-аналитики в такой многогранной предметной области как обеспечение ИБ;

4) меры превентивного подхода к обеспечению ИБ, основанные на результатах оценки рисков ИБ ИТКС, уменьшают большинство, но не все инциденты ИБ. Поэтому для обнаружения и прогнозирования возникновения нарушений и инцидентов ИБ «на лету» необходима такая система управления сетевой безопасностью ИТКС с «лучшими в своем классе» типовыми технологиями и средствами защиты, которая способна сводить к минимуму потери и разрушения, устранять используемые угрозами ИБ уязвимости до того, как ими воспользуется нарушитель ИБ, и быстро восстанавливать функционирования ИТКС и предоставляемые ею услуги и информационные ресурсы их потребителям.

Актуальность исследования определяется необходимостью эффективного и результативного противодействия компьютерным атакам в ИТКС, масштаб и сложность которых постоянно растет при совершенствовании способов реализации с учетом развития ИКТ, когда при применении традиционных стратегий и систем обеспечения ИБ, основанных на принципе реа-

гирования, а не упреждения угроз и инцидентов ИБ, невозможно обеспечить требуемый уровень ИБ ИТКС ОРГАНИЗАЦИИ.

Выше представленный анализ показывает необходимость исследования и разработки научно обоснованной методологии и принципов построения организационно-технических средств обеспечения ИБ для ИТКС. Поэтому **объектом исследования** определена ИТКС ОРГАНИЗАЦИИ как важнейший объект субъектов КИИ с точки зрения необходимости защиты ее информационных ресурсов на всех стадиях их жизненного цикла (создания, сбора, обработки, накопления, хранения, поиска, распространения, использования и уничтожения). (Определение для объекта категории значимости или ее отсутствия в соответствии с [21] выходит за границы данного исследования; результат категорирования объекта считается определенным ранее).

Для упреждающего управления сетевой безопасностью ИТКС требуется использование новейших методов обработки и хранения информации. Только при таком походе удастся обеспечить возможность синтезировать новые знания о будущих угрозах ИБ для ИТКС и обоснованно прогнозировать развитие событий в области ИБ ИТКС. Это и определяет **предмет исследования** – построение специализированных центров, обеспечивающих информационную защищенность передаваемых по таким сетям данных на всех стадиях жизненного цикла ИТКС в условиях угроз ИБ в ЕИП ОРГАНИЗАЦИИ, а также при возникновении отказов в работе, требующих реструктуризации системотехнической составляющей ИТКС, за счет создания в ее составе с применением современных интеллектуальных подходов типового специализированного структурного элемента – «Центра интеллектуального управления сетевой безопасностью» (ЦИУСБ). Первоочередной целью развертывания ЦИУСБ является предоставление ОРГАНИЗАЦИИ возможностей по организации непрерывных процессов предотвращения, выявления и оперативного реагирования на события ИБ, происходящие в ИТКС в режиме реального времени, а также прогнозированию и предупреждению компьютерных атак на защищаемые объекты ИТКС на всех стадиях их жизненного цикла на основе своевременного интеллектуального анализа данных об этих событиях и выявленных требующих немедленной корректировки тенденций в уровне ИБ ИТКС в сравнении с заданными критериями.

Проведенные в работе исследования решают *научную проблему*, состоящую в формировании научной основы обеспечения информационной защищенности и функциональной устойчивости сложных систем класса ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ, что может быть достигнуто за счет разработки методологии и принципов построения специализированного структурного элемента ИТКС ОРГАНИЗАЦИИ – ЦИУСБ, призванного осуществлять упреждающее управление сете-

вой безопасностью ИТКС на всех стадиях жизненного цикла ее информационных ресурсов, а также подтверждение гипотезы о результативном применении в ЦИУСБ для достижений этих целей интеллектуальных подходов. При этом неперенным условием результативного функционирования ЦИУСБ для оперативной коррекции текущего уровня ИБ ИТКС в ЕИП ОРГАНИЗАЦИИ будет являться его обязательное вхождение в состав общей СОИБ – ЦИУСБ как ее важнейшая часть должен быть жестко связан с СОИБ ИТКС и влиять на ее развитие и совершенствование, для чего требуется комплексное обеспечение ИБ всех элементов ИТКС и разработка образовательных аспектов в части обучения разработчиков и персонала ЦИУСБ тому, как квалифицированно создавать, внедрять и эксплуатировать ЦИУСБ.

Цель диссертационной работы можно кратко сформулировать следующим образом: разработка научно обоснованной методологии и принципов построения специализированного структурного элемента ИТКС – типового ЦИУСБ в составе СОИБ ИТКС, призванного осуществлять упреждающее управление сетевой безопасностью при передаче данных в ИТКС на всех стадиях ее жизненного цикла за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных. При этом все процессы обеспечения ИБ с применением ЦИУСБ в ИТКС ОРГАНИЗАЦИИ будут работать наиболее результативно только в том случае, когда операционные (текущие), тактические (в ближайшей перспективе) и стратегические (в отдаленной перспективе) задачи обеспечения ИБ ИТКС будут четко определены и будут решаться на взаимоподдерживающей основе в рамках СОИБ ИТКС.

Для реализации цели были поставлены и решены **следующие задачи исследования**, определившие структуру диссертационной работы:

1. Обосновать включение в ИТКС как основного объекта защиты в ЕИП ОРГАНИЗАЦИИ (объектов КИИ) нового специализированного структурного элемента, предназначенного для упреждающего управления сетевой безопасностью ИТКС на всех стадиях ее жизненного цикла, выявив противоречие между усложнившимся характером современных сетевых атак и существующими подходами и средствами обеспечения сетевой безопасности.

2. Провести научно обоснованную структуризацию понятий информационной защищенности ИТКС и описания внутреннего и внешнего контекста деятельности ОРГАНИЗАЦИИ в виде единой таксономии, необходимой для конкретизации требований к ЦИУСБ, которая позволит получить научную систематизацию и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей (базовых понятий ИБ: «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»).

3. Исследовать основные подходы к управлению сетевой безопасностью и разработать и формализовать процесс управления инцидентами ИБ (ПУИИБ) для его реализации в ЦИУСБ

как ключевой структуры системы управления инцидентами ИБ ИТКС, а, следовательно, и СОИБ ИТКС.

4. На основе анализа недостатков известных видов центров управления безопасностью обосновать применимость концепции интеллектуальной безопасности с расширенной бизнес-логикой функционирования в разрабатываемом типовом ЦИУСБ, а также сформулировать требования к нему.

5. Разработать научно обоснованную методологию и принципы построения типового ЦИУСБ, включая решение задач разработки функциональной архитектуры, архитектуры обработки относящихся к ИБ данных и архитектуры обеспечения собственной ИБ ЦИУСБ с *SIEM*-системой следующего поколения в качестве его ядра и исследование вопросов обеспечения его функциональной устойчивости в ЕИП ОРГАНИЗАЦИИ и кадрового обеспечения.

6. Внедрить основные результаты диссертационного исследования по двум направлениям: в крупных организациях России, включая методологию и принципы построения и функционирования типового ЦИУСБ, и в ведущих университетах России, включая образовательную деятельность по подготовке высококвалифицированных специалистов для проектирования, внедрения, сопровождения и совершенствования ЦИУСБ на всех стадиях их жизненного цикла.

Для решения задач исследования были установлены следующие границы:

— ИТКС с информационной точки зрения представляет собой типичную ИС с присущими ей стадиями жизненного цикла;

— ИТКС функционирует в ЕИП ОРГАНИЗАЦИИ, которое неразрывно связано с киберпространством, являющимся сложноорганизованной средой и имеющим трансграничный характер, что усложняет регулирование информационной защищенности ИТКС как незамкнутой системы в нем;

— определение для ИТКС категории значимости или ее отсутствия в соответствии с [21] выходит за границы данного исследования; результат категорирования объекта считается определенным ранее;

— в рамках исследования оцениваются только угрозы ИБ, актуальные для ИТКС, а не для ее клиентов;

— угрозами ИБ для ИТКС являются угрозы, влияющие в первую очередь на нарушение целостности, затем доступности и других свойств ИБ, и, в последнюю очередь, конфиденциальности ее информационных ресурсов;

— анализируемые компьютерные атаки на информационные ресурсы ИТКС – это сетевые атаки (англ. *network attack*) – компьютерные атаки, осуществляемые с использованием протоколов межсетевого взаимодействия [112, 121, 122], а не локальные атаки на отдельные оконечные устройства и компьютеры пользователей;

— при разработке процесса управления инцидентами ИБ для ИТКС рассматриваются такие стадии как обнаружение, реагирование, расследование, а также прогнозирование их проявления в будущем, что важно для упреждающего управления сетевой безопасностью ИТКС.

Выводы по главе 1

1. Определена типовая структура объекта исследования – ИТКС как основа построения ЕИП ОРГАНИЗАЦИИ, в которой выделены телекоммуникационная и информационная составляющая.

2. На основе критического анализа перечисленных нормативных и правовых документов определены основные понятия, которые используются в ходе изложения полученных результатов исследования и которые составили основу глоссария для области обеспечения ИБ ИТКС. Это такие термины как «ИБ», «угроза ИБ», «уязвимость», «источник угрозы ИБ», «сетевая атака», «событие ИБ», «инцидент ИБ», «риск нарушения ИБ», «функциональной устойчивости ИТКС» и другие. Только комплексное рассмотрение введенных понятий в их взаимосвязи и взаимозависимости позволило в рамках диссертационного исследования наиболее рационально подойти к обеспечению ИБ ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) и построить СОИБ ИТКС в ЕИП ОРГАНИЗАЦИИ.

3. Для решения задач исследования установлены следующие границы:

— ИТКС с информационной точки зрения представляет собой типичную ИС с присущими ей стадиями жизненного цикла;

— ИТКС функционирует в ЕИП ОРГАНИЗАЦИИ, которое неразрывно связано с киберпространством, являющимся сложноорганизованной средой и имеющим трансграничный характер, что усложняет регулирование информационной защищенности ИТКС как незамкнутой системы в нем;

— определение для ИТКС категории значимости или ее отсутствия выходит за границы данного исследования;

— в рамках исследования оцениваются только угрозы ИБ, актуальные для ИТКС, а не для ее клиентов;

— угрозами ИБ для ИТКС являются угрозы, влияющие в первую очередь на нарушение целостности, затем доступности и других свойств ИБ, и, в последнюю очередь, конфиденциальности ее информационных ресурсов;

— анализируемые компьютерные атаки на информационные ресурсы ИТКС, а не локальные атаки на отдельные оконечные устройства и компьютеры пользователей;

— при разработке процесса управления инцидентами ИБ для ИТКС важно рассмотреть такие стадии как обнаружение, реагирование, расследование, а также прогнозирование их проявления в будущем, что важно для упреждающего управления сетевой безопасностью ИТКС.

4. На основе анализа первоисточников уточнена и существенно расширена по сравнению с имеющейся временная шкала возникновения основных технологий и средств обеспечения сетевой безопасности, позволяющая наглядно проследить их эволюцию и сделать вывод об отсутствии в последние годы прорывных технологий.

5. Из введенного в исследовании определения ИБ ИТКС – это не только возможность предвидеть, противостоять и восстанавливаться, но и развиваться (эволюционировать), совершенствуя деятельность в неблагоприятных условиях, при стрессовых ситуациях и атаках на ресурсы, необходимые для непрерывного выполнения бизнес-процессов и доступности услуг. Информационная защищенность ИТКС рассматривается как такая ее способность, при которой уровень риска нарушения осуществления деятельности и уровень риска нарушения всех свойств ИБ информационных ресурсов на всех стадиях их жизненного цикла приемлемы как для их пользователя, так и владельца. Также основной упор необходимо делать на сохранение ИБ ИТКС, а не на количество актуальных для нее угроз ИБ.

6. Функциональная устойчивость ИТКС после прекращения действия возмущения должна проявляться в двух режимах – «в малом» и «в большом». ИТКС как сложной системе, поведение которой основано на акте решения – выборе из альтернатив, присуща активная форма функциональной устойчивости. Поведение ИТКС при этом является целенаправленным, поскольку ИТКС стремится достигнуть предпочтительного для нее состояния – выполнение цели функционирования.

7. В современном глобальном информационном обществе среда сохранения ИБ очень неоднородна, сложна по числу и многообразию элементов и их взаимосвязей и взаимозависимостей между собой. Следовательно, выбор методов и средств обеспечения ИБ ИТКС в нем требует комплексного подхода с выделением различных рубежей защиты и применением правовых, организационных, аппаратно-программных, технических и иных мер и средств обеспечения ИБ. Установленные отличительные особенности обеспечения ИБ ИТКС требуют разработки и в дальнейшем реализации упреждающего управления сетевой безопасностью с применением современных интеллектуальных подходов.

8. По результатам проведенного критического анализа положения дел по исследуемому вопросу и источников концептуальная постановка задачи диссертационного исследования в общем виде может быть сформулирована следующим образом:

для безопасной деятельности субъекта КИИ в информационной сфере чрезвычайно необходимо представить научно обоснованную концепцию создания типового ЦИУСБ как неотъ-

емлемой части СОИБ ИТКС, внедрение которой позволит устранить имеющееся в настоящее время очевидное противоречие между, с одной стороны, невозможностью избежать компьютерных атак в ИТКС, осуществляемых искушенными злоумышленниками, имеющими доступ к новейшим ИКТ, учитывая тенденцию к постоянному росту масштаба и сложности этих атак, и с другой стороны, использованием в этих условиях для обеспечения на одинаково высоком уровне информационную защищенности и, следовательно, функциональной устойчивости современных ИТКС устаревших стратегий и СОИБ, основанных на принципе реагирования, а не упреждения угроз и инцидентов ИБ, и, как следствие, обеспечивающих недостаточный уровень ИБ ИТКС ОРГАНИЗАЦИИ.

9. Данное исследование призвано решить *научную проблему*, состоящую в формировании научной основы обеспечения информационной защищенности и функциональной устойчивости сложных систем класса ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ, что может быть достигнуто за счет разработки методологии и принципов построения специализированного структурного элемента ИТКС ОРГАНИЗАЦИИ – ЦИУСБ, призванного осуществлять упреждающее управление сетевой безопасностью ИТКС на всех стадиях ее жизненного цикла за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных. При этом неременным условием результативного функционирования ЦИУСБ для оперативной коррекции текущего уровня ИБ ИТКС в ЕИП ОРГАНИЗАЦИИ будет являться его обязательное вхождение в состав общей СОИБ – ЦИУСБ как ее важнейшая часть должен быть жестко связан с СОИБ ИТКС и влиять на ее развитие и совершенствование, для чего требуется комплексное обеспечение ИБ всех элементов ИТКС и разработка образовательных аспектов в части обучения разработчиков и персонала ЦИУСБ тому, как квалифицированно создавать, внедрять и эксплуатировать ЦИУСБ.

ГЛАВА 2. ТАКСОНОМИЯ УЯЗВИМОСТЕЙ, УГРОЗ, СЕТЕВЫХ АТАК И ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В условиях возможности реализации угроз незаконного нарушения функционирования и предоставления услуг посредством сетевых атак и инцидентов ИБ ИТКС ОРГАНИЗАЦИИ следует дополнить СОИБ ИТКС. Для достижения этой цели важно адекватно описать среду осуществления деятельности ОРГАНИЗАЦИИ с точки зрения ИБ. Для формулирования требований по обеспечению ИБ, положенных в основу Стратегии и Политик обеспечения ИБ (Политик ИБ), необходимо наиболее полно описать внутреннюю и внешнюю среду ОРГАНИЗАЦИИ, что делается в двух важнейших моделях ИБ – Модели угроз ИБ и Модели нарушителей ИБ. При разработке этих двух моделей из всего многообразия требуется выделить те условия осуществления деятельности ОРГАНИЗАЦИИ, которые актуальны и характерны именно для нее. С этой целью в главе разрабатывается таксономия взаимосвязанных сущностей – базовых понятий ИБ, а именно уязвимостей, угроз ИБ, сетевых атак и связанных с ними инцидентов ИБ для ИТКС как негативных элементов, которые необходимы для упорядочивания знаний об информационной защищенности ИТКС ОРГАНИЗАЦИИ и которые следует своевременно предотвращать или устранять, если они уже состоялись и были выявлены. Написание адекватных Стратегии и Политик ИБ, обоснованная разработка системы и выбор методов и средств обеспечения ИБ для ИТКС ОРГАНИЗАЦИИ напрямую зависит от полноты и качества разработанной таксономии и представленных классификаций.

2.1. Таксономия понятий уязвимости, угроз, сетевых атак и инцидентов информационной безопасности

Под таксономией (от др.-греч. *τάξις* — строй, порядок и *νόμος* — закон) здесь понимается учение о принципах и практике классификации и систематизации сложноорганизованных иерархически взаимосвязанных сущностей, которые необходимы для упорядочивания знаний о них. Для наглядности демонстрации взаимосвязей базовых понятий области ИБ приведем в одном месте определения уязвимости, угрозы ИБ, сетевой атаки и инцидента ИБ.

Уязвимость (англ. *vulnerability*) ИС – свойство ИС, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Примечания: 1. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в ИС. 2. Если уязвимость соответствует угрозе, то существует риск [111].

Угроза нарушения ИБ (угроза ИБ) организации – совокупность факторов и условий, создающих опасность нарушения ИБ организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации. Примечания: 1. Формой реализации (проявления) угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств ИБ объекта(ов) защиты организации. 2. Угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы [22]. *Источник угрозы ИБ* – это субъект (физическое лицо, материальный объект или физическое явление), использующий уязвимости для реализации угрозы ИБ.

Сетевая атака (англ. *network attack*) – компьютерная атака с использованием протоколов межсетевого взаимодействия [112, 121, 122]. В свою очередь, **компьютерная атака** (англ. *computer attack*): целенаправленное воздействие программных и (или) аппаратно-программных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [7, статья 2]. Сетевая атака – это реализовавшаяся угроза ИБ, точнее конкретный способ реализации угрозы ИБ.

Вторжение (англ. *intrusion*) – несанкционированный доступ (НСД) к сети или подсоединенной к сети системе, то есть преднамеренный или случайный НСД к ИС, включая злонамеренную деятельность против ИС или несанкционированное использование ресурсов в ИС [108].

Инцидент ИБ (англ. *IS incident*) – появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операций и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации [68].

Событие ИБ (англ. *IS event*) – идентифицированное появление определенного состояния актива организации (системы, сервисы или сети), указывающего на возможное нарушение Политики ИБ или нарушения в работе средств защиты или неспособность защитной меры обеспечить адекватную защиту информационного актива, либо возникновение ранее неизвестной ситуации, которая может иметь отношение к ИБ (адаптировано на основе [68]).

Из этих определений очевидно, что все они тесно взаимосвязаны. Крайне важно знать, какие угрозы ИБ для ИТКС ОРГАНИЗАЦИИ существуют в настоящий момент, как они могут перерасти в инцидент ИБ, а затем повлиять на бизнес ОРГАНИЗАЦИИ, особенно если они приведут к краже интеллектуальной собственности и нарушению конфиденциальности важных данных или непредоставлению запрашиваемых услуг, поставив под угрозу ее репутацию или финансовое благополучие.

Связь базовых понятий ИБ хорошо иллюстрирует рис. 11 (разработан на основе [133]). Из-за наличия в информационном активе ОРГАНИЗАЦИИ одной не устраненной вовремя уяз-

вимости при стечении соответствующих обстоятельств может реализоваться одна и более угроз ИБ. Сама по себе уязвимость (просто ее наличие) не причиняет ИС вреда – для этого нужны связанная с ней угроза ИБ и ее источник, которые ею воспользуются. Уязвимость лишь создает потенциальные условия для реализации угрозы ИБ. Уязвимость, для которой пока не выявлено соответствующей угрозы ИБ, может не требовать реализации соответствующих мер обеспечения ИБ, но она все равно должна быть осознана, и должен осуществляться мониторинг ее изменений. И наоборот, угроза ИБ, для реализации которой в системе нет уязвимости, не актуальна для этой системы и не влечет за собой риска ИБ. Следует отметить, что некорректная реализация или использование и неправильное функционирование мер обеспечения ИБ (например, при некорректных конфигурационных настройках) может также создать уязвимость(-и).

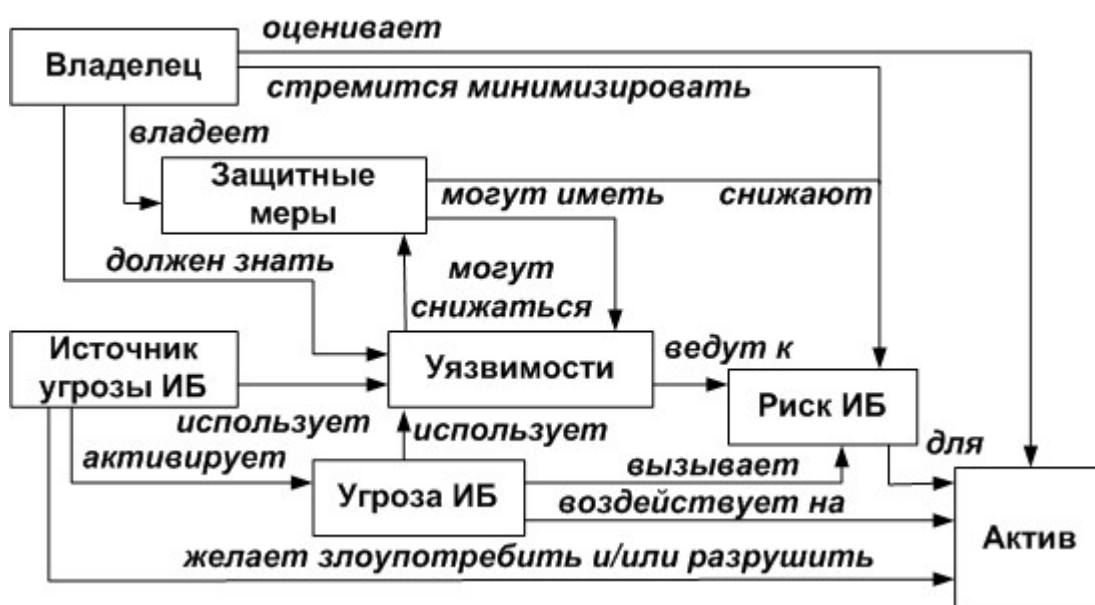


Рисунок 11 – Взаимосвязь базовых понятий ИБ

Немного с другой точки зрения взаимозависимость названных понятий представлена на рис. 12. Основные рассуждения, которые привели к ее появлению, таковы. Угроза ИБ может стать реальной компьютерной атакой, если в активах есть необходимая для этого уязвимость/совокупность уязвимостей и присутствует соответствующий источник. Одна угроза ИБ может быть актуальной для одного или сразу нескольких активов. В реализации угрозы ИБ может участвовать один или несколько источников угрозы ИБ – нарушителей ИБ, действующих в сговоре.

Упрощенно рис. 11 и рис. 12 можно перерисовать, как это показано на рис. 13.



Рисунок 12 – Взаимосвязь базовых понятий ИБ

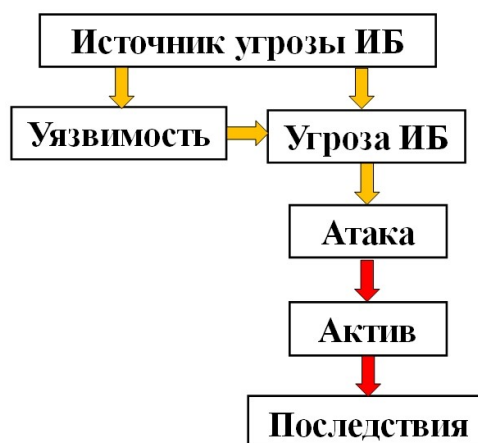


Рисунок 13 – Взаимосвязь базовых понятий ИБ

Формой реализации угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств ИБ объекта(ов) защиты ОРГАНИЗАЦИИ, которые и называются в мире сетевых технологий сетевой атакой.

Анализом уязвимостей, угроз ИБ и сетевых атак автор исследования занимается более 25 лет, что отражено в многочисленных учебно-методических материалах [55, 132, 134-139] и научных публикациях [45, 46, 48, 140, 141], изданных лично и в соавторстве, начиная с 1995 г. и по настоящее время. Далее взяв за основу эти работы, представим разработанные системные классификации применительно к элементам ИТКС ОРГАНИЗАЦИИ.

2.2. Системная классификация уязвимостей элементов информационно-телекоммуникационной сети

Против элементов ИТКС ОРГАНИЗАЦИИ могут быть совершены самые разнообразные компьютерные атаки. Однако не все из них будут успешны. В первую очередь это происходит потому, что необходимым условием для реализации атаки является ее способность использо-

вать (как говорят «эксплуатировать») существующую уязвимость(-и), которую по разным причинам своевременно не устранили. Чтобы понять возможности реализации угроз ИБ против элементов ИТКС и выбрать среди всего многообразия актуальные, характерные только для этой ИТКС, нужно провести инвентаризацию информационных активов ОРГАНИЗАЦИИ и объектов СОИА как среды их использования и (или) эксплуатации. Именно наличие уязвимостей в объектах СОИА и используется источниками угроз ИБ для их реализации.

Мировым лидером в описании уязвимостей ПО и АО является компания *MITRE*, которая многие годы поддерживает англоязычную базу общеизвестных уязвимостей *CVE* (англ. *Common Vulnerabilities and Exposures*) [<https://cve.mitre.org>], финансируемую *US-CERT*. Каждой уязвимости присвоен идентификационный номер вида *CVE*-год-номер и даны описание и ряд общедоступных ссылок для проверки ее наличия или устранения. На 15.09.2020 общее количество записей в базе составляло 141500, начиная с 1999 г. и по настоящее время.

В 2000 г. начала создаваться *NVD* (англ. *National Vulnerability Database*) [<https://nvd.nist.gov/>] – БД с информацией об уязвимостях, основанная на стандартах правительства США. *NVD* является результатом деятельности Отдела компьютерной безопасности *NIST* (*NIST Computer Security Division*), а именно Лаборатории информационных технологий (*Information Technology Laboratory*), и финансируется отделом национальной кибербезопасности Министерства внутренней безопасности (*Department of Homeland Security's National Cyber Security Division*). *NVD* содержит проанализированную информацию, опубликованную в базе *CVE*, и дополняет его ссылками и данными из открытых источников. В ней представлены показатели обобщенного воздействия из Общей системы оценки уязвимостей (англ. *Common Vulnerability Scoring System – CVSS*), типы уязвимостей (англ. *Common Weakness Enumeration*) и типы платформ (англ. *Common Platform Enumeration*), а также другие метаданные. При этом держатели базы не проводят активного тестирования уязвимостей, полагаясь на информацию от поставщиков и сторонних исследователей безопасности, которая затем используется для назначения соответствующих атрибутов и их актуализации с течением времени. Таким образом, *NVD* включает в себя ссылки на ресурсы по безопасности, описания уязвимостей и неправильных конфигураций ПО, названия продуктов и показатели критичности уязвимостей. В *NVD* содержится такое же количество записей, как и в *CVE*.

Кроме названных лидеров, в качестве источников информации по уязвимостям можно упомянуть базу *CERT/CC Vulnerability Notes* [<https://www.kb.cert.org/vuls/>], поддерживаемую отделом *CERT*, который является частью управляемого Университетом Карнеги-Меллона института *Software Engineering Institute*, общий реестр проблемных конфигураций систем *MITRE Common Configuration Enumeration (CCE)*, текущее техническое обслуживание и разработка которой теперь переданы *NIST* (США) [<http://nvd.nist.gov/cce/index.cfm>], отчеты об уязвимостях

ПО исследовательской группы *Secunia* из *Flexera* [<https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020>], бюллетени разработчиков (например, Microsoft) и пр.

На основе анализа *CVE* и *NVD* были выделены следующие типичные уязвимости современных сетей:

- 1) не достаточно защищенная и неотслеживаемая точка удаленного доступа к сети;
- 2) неадекватное управление доступом к маршрутизатору: неправильная конфигурация списка контроля доступа (англ. *Access Control List, ACL*), приводящая к утечке информации и неавторизованному доступу в демилитаризованную зону (ДМЗ) (англ. *Demilitarized Zone, DMZ*) – пограничный сегмент сети, выполняющий функции «нейтральной зоны» между сетями [60];
- 3) неправильно сконфигурированный МЭ, предоставляющий доступ к внутренним системам за ним;
- 4) возможность утечки информации с сервера, исполняющего ненужные сервисы;
- 5) ненадежные, повторно используемые или легко угадываемые пароли (либо их отсутствие) на уровне рабочей станции, что открывает для компьютерных атак и серверы;
- 6) наличие пользователей или проверочных учетных записей со слишком большими правами;
- 7) избыточные права на доступ к файлам и каталогам (совместно используемым ресурсам ОС *Windows*, сетевой файловой системе в ОС *UNIX*);
- 8) неправильно сконфигурированные сервисы и сервисы, не требующие авторизации (например, вход в систему через анонимный FTP-серверов (англ. *File Transfer Protocol*));
- 9) возможность получения за счет сканирования информации из сети об ОС серверов и рабочих станций, их версиях, пользователях, группах, совместно используемых ресурсах, структуре сети и т.п.;
- 10) необновленное, устаревшее, работающее в конфигурации по умолчанию ПО;
- 11) неадекватные и неполные средства регистрации событий, мониторинга и обнаружения вторжений на уровне хостов (устройств с уникальными адресами) и сети в целом и т.д.

Анализом уязвимостей веб-технологий целенаправленно с 2011 г. занимается сообщество *OWASP* (*Open Web Application Security Project*) [<https://www.owasp.org>] со штаб-квартирой в США, включающее в себя корпорации, образовательные организации и частных лиц со всего мира. Согласно *OWASP*, в коде веб-приложений чаще всего встречаются следующие уязвимости:

- 1) отсутствие проверки запросов на соответствие установленному формату (позволяет атаковать внутренние компоненты сервисов через веб-приложение);
- 2) уязвимости в контроле доступа (может предоставить авторизованному пользователю

доступ к чужим учетным записям);

3) уязвимости в управлении учетными записями и сеансами (позволяет получить пароли, *cookie*-файлы сеанса);

4) уязвимость межсайтовых сценариев (использования веб-сервисов в качестве средства извлечения конфиденциальной информации из систем конечных пользователей);

5) уязвимость, связанная с ошибками, приводящими к переполнению буфера;

6) уязвимость, позволяющая манипулировать параметрами (отсутствие блокировки возможности внедрения посторонних команд в параметры, передаваемые веб-приложениями внешним ресурсам, локальной ОС);

7) несовершенство обработки ошибок (предоставляет возможность вызвать *DoS*-атаку);

8) уязвимости в криптосистеме (использование слишком слабых алгоритмов, коротких ключей и т.п.);

9) неправильное конфигурирование (неустановка обновлений безопасности, сохранение учетных записей, предусмотренных по умолчанию, и т.п.);

10) уязвимости в удаленном администрировании (некорректное разделение полномочий администратора и обычного пользователя, возможность получения прав администратора и т.п.).

На сайте ФСТЭК России в Банке данных угроз безопасности информации [<https://bdu.fstec.ru>] также можно ознакомиться с имеющимися, но уже на русском языке, уязвимостями. На 15.09.2020 база содержала 28633 записи, что существенно уступает показателям *CVE* и *NVD*.

При составлении классификации уязвимостей, кроме четырех выше указанных источников, использовались многочисленные обзоры иностранных и российский исследовательских и консалтинговых компаний, а также следующие стандарты:

— ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» – Приложение С. Примеры уязвимостей [107];

— ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» [142];

— ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» [143];

— ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» – Приложение Б. Перечень нарушений защиты информации [144];

— Методический документ «Регламент включения информации об уязвимостях ПО и аппаратно-программных средств в Банк данных угроз безопасности информации ФСТЭК Рос-

сии» (2018) [145];

— ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response – Приложение В. Форма отчета об уязвимости [127].

Учитывая имеющийся опыт рассмотрения уязвимостей в изученных источниках, были сформулированы пять важных требований к разрабатываемой классификации уязвимостей:

1) в классификации должна содержаться информация об инцидентах ИБ, которые характерны как для самой ИТКС ОРГАНИЗАЦИИ, так и ЦИУСБ как ее важнейшей части и системообразующего элемента СОИБ ОРГАНИЗАЦИИ;

2) в классификации должна содержаться информация об этапе жизненного цикла объекта, на котором возникает уязвимость;

3) в классификации должна содержаться информация о местонахождении уязвимости (внешнее окружение, общая архитектура, внутренняя конфигурация, ПО и т.п.);

4) на одном уровне классификации не должны располагаться понятия разной степени абстракции, описывающие достаточно широкий отвлеченный класс проблем или какой-либо редкий частный случай;

5) в классификации необходимо связать уязвимости с видами угроз ИБ, которые могут их использовать для реализации в виде компьютерных атак и инцидентов ИБ.

Обобщенные результаты разработки классификационных признаков для уязвимостей элементов ИТКС ОРГАНИЗАЦИИ сведены в табл. 2. Основными классификационными признаками типов уязвимостей являются следующие: место нахождения или проявления уязвимости, предпосылки появления уязвимости, источник происхождения уязвимости – стадия жизненного цикла, на которой возникла уязвимость, легкость обнаружения уязвимости, легкость устранения уязвимости, вероятность реализации угрозы ИБ на основе уязвимости, использующие уязвимость угрозы ИБ и уровень риска ИБ (критичность, серьезность, потенциальные последствия) в случае использования уязвимости.

В целях выявления и оценки уязвимостей дополнительно для каждого из классов можно еще определить и подклассы (при необходимости), например, как в случае с выделением в подклассы отдельных элементов ИТКС, для которых так нагляднее ввести еще один уровень систематизации, детализирующий описание уязвимости.

Одна и та же уязвимость одновременно должна быть отнесена сразу к нескольким типам. Существуют и многофакторные уязвимости, которые в рамках одного типа могут быть отнесены к разным классам, но в рамках одного класса уязвимость может быть приписана только к одному подклассу.

Таблица 2 – Системная классификация уязвимостей элементов ИТКС (начало)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс (при наличии)</i>	<i>Некоторые примеры уязвимостей</i>
Тип 1. Место нахождения или проявления уязвимости	Класс 1. Физическая среда (место расположения организации)	-	Размещение в местности, предрасположенной к наводнениям. Размещение в местности, где бывают пылевые бури. Зависимость от внешних сторон (например, аутсорсинговой компании).
	Класс 2. Организация в целом	-	Неадекватное или небрежное управление физическим доступом в здания и помещения. Отсутствие физической защиты дверей и окон. Отсутствие контроля над активами, находящимися за пределами организации (например, во время транспортировки). Несоблюдение требований законодательства, надзорных и регулирующих органов.
	Класс 3. ИТКС	Подкласс 1. Уровень каналов связи и телекоммуникационного оборудования	Уязвимости маршрутизаторов, коммутаторов, концентраторов, мультиплексоров, мостов. Уязвимости каналаобразующего оборудования. Уязвимости в АО СВТ, оконечных устройств (компьютеров, серверов) (например, уязвимости микропрограмм в программируемых логических интегральных схемах). Чувствительность к влажности, пыли, загрязнению. Чувствительность к электромагнитному излучению. Отсутствие программ периодической замены. Незащищенное хранение носителей данных. Отсутствие формальной политики по использованию портативных компьютеров.
		Подкласс 2. Уровень сетевой среды и ее отдельных элементов	Уязвимости сетевых протоколов – стека протоколов <i>TCP/IP</i> , <i>NetBEUI</i> и т.п. Плохая разводка кабелей. Ненадежная сетевая архитектура. Передача паролей в незашифрованном виде. Недостаточно защищенные соединения с сетью общего пользования. Отсутствие подтверждения отправления или получения сообщения.
		Подкласс 3. Общесистемное (общее), прикладное, специальное ПО	Присвоение параметру неправильных значений настройки ПО. Возможность прослеживания пути доступа к каталогам. Возможность внедрения нарушителем ссылки на сторонние ресурсы, которые могут содержать вредоносный код. Наличие избыточного числа параметров или неопределенных параметров ПО. Отсутствие проверки значений вводимых (входных) данных. Уязвимости ОС <i>Windows</i> , <i>UNIX</i> . Уязвимости СУБД <i>ORACLE</i> , <i>MSSQL</i> , <i>Sybase</i> . Уязвимости в ПО клиента и сервера. Уязвимости прикладного ПО (процессоры, браузеры...).
		Подкласс 4. Функционирование	Уязвимости в управлении сервисами и операционными процессами, осуществляемыми ИТ-операциями и вспомогательным персоналом. Уязвимости режимов загрузки. Уязвимости средств контроля исполнения мобильного кода. Уязвимости интерфейсов беспроводного доступа.

Таблица 2 – Системная классификация уязвимостей элементов ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры уязвимостей</i>
		Подкласс 5. Предоставление услуг	Уязвимости в ПО сервисных приложений. Уязвимости в приложениях и ПО, обеспечивающих бизнес-активность (например, CRM-системы). Сложный пользовательский интерфейс. Отсутствие документации. Отсутствующее или неудовлетворительное соглашение об уровне услуг (англ. <i>Service Level Agreement, SLA</i>). Отсутствие политики по использованию электронной почты. Наличие функциональных возможностей, способных оказать влияние на СЗИ.
	Класс 4. СЗИ	-	Отсутствие СЗИ. Неправильное конфигурирование СЗИ, например, неполный список правил фильтрации трафика. Неполная запись событий в ЖРС. Уязвимости в средствах управления доступом, идентификации и аутентификации, контроля целостности, доверенной загрузки, антивирусной защиты, СОВ, средствах межсетевого экранирования, управления потоками информации, ограничения программной среды, стирания информации и контроля удаления информации, защиты каналов передачи информации. Уязвимости в иных СЗИ (ошибки программирования, недостатки, связанные возможностью обхода, отключения, преодоления функций безопасности и т.п.). использование несертифицированных средств криптографической защиты информации.
	Класс 5. Установившаяся практика / порядок управления и администрирования	-	Организационные уязвимости. Отсутствующая или неудовлетворительная политика «чистого стола и пустого экрана». Отсутствие установленных процедур мониторинга нарушений ИБ. Отсутствие формальной процедуры для регистрации и снятия с регистрации пользователей. Отсутствие регламентов администрирования. Отсутствие контроля за процессом управления конфигурациями. Отсутствие контроля за процессом управления обновлениями. Отсутствие обязанностей по обеспечению ИБ в должностных инструкциях. Отсутствие оговоренного дисциплинарного процесса в случае инцидента безопасности. Уязвимости в средствах управления и защиты и сервисах для уровней инфраструктуры, платформ и ПО. Уязвимости средств управления потоками информации.
	Класс 6. Процессы и процедуры (организация работ)	Подкласс 1. Бизнес-процессы	Отсутствие процедур оценки бизнес-рисков.
		Подкласс 2. Технологические процессы	Отсутствие политик по правильному использованию телекоммуникационной среды и обмена сообщениями. Неадекватная ответственность за техническое обслуживание. Отсутствие процедуры контроля изменений.

Таблица 2 – Системная классификация уязвимостей элементов ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры уязвимостей</i>
		Подкласс 3. Информационные процессы	Активизация ненужных сервисов. Отсутствие требования аутентификации для выполнения критичных функций. Уязвимости средств управления процессами.
		Подкласс 4. Процессы обеспечения ИБ	Неконтролируемая загрузка и использование программных средств. Ошибки логики процесса аутентификации. Отсутствие запрета множественных неудачных попыток аутентификации.
	Класс 7. Персонал	Подкласс 1. Работники бизнес-подразделений	Отсутствие необходимых ролей пользователей. Отсутствие завершения сеанса при уходе с рабочего места. Недостаточное осознание проблем безопасности. «Дырки» в голове пользователя – более серьезная проблема, чем в ПО!
		Подкласс 2. Работники вспомогательных подразделений и внешний персонал	Неадекватные процедуры набора персонала. Отсутствие или недостаточные условия (касающиеся безопасности) в договорах с клиентами и/или третьими сторонами. Безнадзорная работа внешнего персонала и работников, занимающихся уборкой.
		Подкласс 3. Сотрудники подразделения безопасности	Отсутствие персонала. Недостаточная квалификация персонала. Совмещений в одной роли нескольких полномочий. Неверное распределение прав доступа. Незащищенные таблицы паролей. Ошибки при удалении ненужных учетных данных.
	Класс 8. По отношению к активу	Подкласс 1. Внешние	Некорректная настройка СЗИ. Уязвимость в ПО обработки данных. Неправильная маршрутизация сообщений через сети общего пользования.
		Подкласс 2. Внутренние	Зависят от особенностей и характеристик актива.
Тип 2. Предпосылки появления уязвимости	Класс 1. Объективные	-	Зависят от конструктивных особенностей и технических характеристик оборудования и ПО, применяемого в ИС ИТКС. Способ и цели использования актива, отличный от планируемых при его приобретении или создании. Запись на старый носитель данных. Наличие излучения технических средств (электрического, электромагнитного, звукового, теплового). Запись данных на единственный доступный в тот момент носитель, который быстро размагничивается при хранении в помещении, в котором присутствует электромагнитное излучение.
	Класс 2. Субъективные	-	Зависят от действия персонала. Нарушения режима эксплуатации технических средств. Ошибки при эксплуатации и подготовке ПО к использованию.
	Класс 3. Стихийные (случайные)	-	Зависят от особенностей окружающей среды и непредвиденных обстоятельств. Подверженность сбоям электропитания. Отказы и неисправности технических средств.

Таблица 2 – Системная классификация уязвимостей элементов ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры уязвимостей</i>
Тип 3. Источник происхождения уязвимости – стадия жизненного цикла, на которой возникла уязвимость	Класс 1. Проектирование	Подкласс 1. Архитектура	Ошибка проектирования многопоточной системы или приложения, при которой функционирование системы или приложения зависит от порядка выполнения части кода. Проблемы с логикой функционирования. Нарушение принципов проектирования безопасного ПО.
		Подкласс 2. Технологии	Уязвимости, вызванные технологиями беспроводного доступа. Уязвимости, вызванные особенностями Ethernet-сетей. Уязвимости, вызванные особенностями среды виртуализации.
		Подкласс 3. Протоколы	Использование небезопасных протоколов управления (например, логин и пароль пользователя Telnet передают через интернет открытым текстом и могут быть перехвачены). Уязвимости протоколов управления телекоммуникационным оборудованием.
		Подкласс 4. Сервисы	Проблемы с обработчиками прерываний. Ошибки инициализации и очистки. Недостатки разграничения доступа к объектам. Уязвимости сетевых сервисов. Уязвимости сервисов ввода-вывода.
	Класс 2. Реализация и программирование	-	Ошибки в программировании протоколов стека TCP/IP под конкретной ОС, ведущие к DoS-атакам. Ошибки в реализации приложений, ведущие к переполнению буфера.
	Класс 3. Внедрение и использование	-	Уязвимости систем хранения данных (например, файловых систем). Уязвимости офисных пакетов программ. Неправильное конфигурирование ОС, протоколов и сервисов. Нестойкие пароли. Неудалённые установки по умолчанию. Ошибки, вызванные несовместимостью версий. Неполная или некорректная документация. Количественная недостаточность элементов ИТКС. Качественная недостаточность элементов ИТКС.
	Класс 4. Снятие с эксплуатации	-	Остающаяся в памяти неудалённая информация. Отсутствие очистки ресурса и процессов от сведений ограниченного доступа перед повторным использованием.
Тип 4. Легкость обнаружения уязвимости	Класс 1. Высокая	-	Уязвимость можно обнаружить визуально.
	Класс 2. Средняя	-	Уязвимость можно обнаружить путем несложных действий, выполняемых вручную
	Класс 3. Низкая	-	Уязвимость можно обнаружить только с помощью специализированных САЗ.

Таблица 2 – Системная классификация уязвимостей элементов ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры уязвимостей</i>
Тип 5. Легкость устранения уязвимости	Класс 1. Высокая	-	Уязвимость можно устранить, запустив автоматическую установку обновлений безопасности.
	Класс 2. Средняя	-	Уязвимость можно легко устранить, путем несложных действий, выполненных вручную специалистом.
	Класс 3. Низкая	-	Уязвимость можно устранить, обладая специальными знаниями, или полной заменой того элемента ИТКС, где она была обнаружена.
Тип 6. Вероятность реализации угрозы ИБ на основе уязвимости	Класс 1. Высоково- роятная / вероятная	-	Уязвимость легко использовать; защита отсутствует или слаба.
	Класс 2. Возможная	-	Уязвимость можно использовать, но защита есть.
	Класс 3. Маловероят- ная/ невероятная	-	Уязвимость сложно использовать, есть хорошая защита.
Тип 7. Использо- вующие уязви- мость угрозы ИБ	Класс 1. Угроза нару- шения конфиденци- альности/ приватности	-	Возможность выполнения пользователем команд ОС (например, копирование файлов). Возможность утечки информации при генерировании ПО сообщения об ошибке. Ошибки хранения и передачи информации в незашифрованном виде.
	Класс 2. Угроза нару- шения целостности	-	Возможность внедрения интерпретируемых операторов языков программирования (например, операции добавления) или разметки в исходный код веб-приложения. Неконтролируемая форматная строка, позволяющая нарушителю внедрять произ- вольный код. Ошибка усечения числа, когда часть числа отсекается. Нарушение целостности архива.
	Класс 3. Угроза нару- шения доступности	-	Возможность ПО осуществлять запись данных за пределами выделенного в памяти буфера, что может вызывать аварийное завершение или зависание ПО. Возмож- ность выполнения пользователем команд ОС (например, удаление файлов). Недос- точность мер освобождения выделенных участков памяти после использования, что приводит к сокращению свободных областей памяти.
	Класс 4. Угроза нару- шения подлинности	-	Возможность подмены доверенного пользователя или объекта в сети. Возмож- ность обойти процедуру проверки подлинности. Ошибками подтверждения под- линности сертификата, позволяющая нарушителю получить НСД к защищаемой информации. Недостаточная проверки подлинности данных. Использование нели- цензионного ПО.
	Класс 5. Угроза нару- шения подотчетности	-	Отсутствие сообщений об ошибках, зафиксированных в ЖРС администратора и оператора. Неполная запись событий в ЖРС. Отсутствие места на жестком диске для записи всех событий, собранных агентами COB.

Таблица 2 – Системная классификация уязвимостей элементов ИТКС (окончание)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры уязвимостей</i>
	Класс 6. Угроза нарушения неотказуемости	-	Отсутствие подтверждения отправления или получения сообщения.
	Класс 7. Угроза нарушения достоверности	-	Неконтролируемая форматная строка, позволяющая нарушителю динамически изменять путь исполнения программы. Отсутствие проверки правильности формирования запроса. Возможность внедрения ложного объекта (например, маршрутизатора, сервера, рабочей станции).
Тип 8. Уровень риска (критичность, серьезность, потенциальные последствия) в случае использования уязвимости	Класс 1. Высокий	-	Уязвимости, позволяющие атакующему получить доступ к узлу с правами суперпользователя. Уязвимости, делающие возможным обход МЭ или иных СЗИ. Избыточные права доступа. Уязвимости, приводящие к недовольству клиентов с их последующей потерей.
	Класс 2. Средний	-	Уязвимости, позволяющие злоумышленнику получить информацию, которая с высокой вероятностью позволит ему получить доступ к хосту (например, после перехвата хэш-значения пароля). Уязвимости, приводящих к высокому потреблению ресурсов системы (DoS-атакам).
	Класс 3. Низкий	-	Уязвимости, позволяющие собирать важную информацию о работе систем (например, неиспользуемые сервисы, текущее время на компьютере для атак против алгоритмов шифрования).

Как видно из представленной таблицы, даже в классификационных параметрах уязвимостей не удалось избежать упоминания угроз ИБ, что подтверждает их неразрывную связь.

Более наглядно и компактно все типы возможных уязвимостей в информационной сфере ИТКС ОРГАНИЗАЦИИ изображены на рис. 14.



Рисунок 14 – Системная классификация уязвимостей в информационной сфере ИТКС ОРГАНИЗАЦИИ

Представленная системная классификация не претендует на полноту, поскольку новые уязвимости обнаруживаются почти каждый день. Она может быть использована в качестве основы для расширения в будущем.

Информация о классификации уязвимостей необходима для наиболее полного заполнения сотрудниками подразделения ИБ или работниками ОРГАНИЗАЦИИ отчета по обнаруженной уязвимости. Форма такого отчета приведена в приложении к [127].

Соотношение каждой уязвимости каждого информационного актива ИТКС ОРГАНИЗАЦИИ с каждым конкретным типом, а потом и классом и подклассом (при наличии) позволит наиболее полно охарактеризовать ее и понять ее природу. Это необходимо для того, чтобы в дальнейшем в процессе обеспечения ИБ ИТКС ОРГАНИЗАЦИИ для каждой выявленной уязвимости подобрать наиболее подходящую процедуру и средства устранения (и составить план устранения обнаруженных уязвимостей) и, что еще более важно, не допустить ее появления в будущем или, по крайней мере, существенно снизить вероятность этого появления.

2.3. Системная классификация угроз информационной безопасности информационно-телекоммуникационной сети

Анализ всего комплекса возможных угроз ИБ и оценка последствий их реализации составляет одну из важнейших задач при разработке СОИБ ИТКС, способной не дать им развиваться в реальные инциденты ИБ. На сайте ФСТЭК России в Банке данных угроз безопасности информации [<https://bdu.fstec.ru>] можно ознакомиться с описаниями угроз ИБ, в котором на 15.09.2020 было представлено 217 записей.

Из всего множества существующих на данный момент **актуальной для ИТКС ОРГАНИЗАЦИИ считается та угроза ИБ**, которая может быть реализована в ИС ИТКС и представляет опасность для ее информационных ресурсов (адаптировано на основе [146]). Уточним, что актуальность угрозы можно определить по вызываемому ей недопустимому риску ИБ. ОРГАНИЗАЦИИ нужно защищаться только от актуальных для нее угроз ИБ, а не от всех возможных.

Как и в случае с уязвимостями, общепринятой классификации угроз ИБ до сих пор не существует. При составлении данной классификации угроз ИБ использовались многочисленные обзоры и методики определения угроз ИБ иностранных (например, классификация по использованию нарушителями физического и технического доступа *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)* Университета Карнеги-Меллона (США, 2001 г.) [147] и ее актуальная версия *OCTAVE Allegro* и *Harmonized Threat and Risk Assessment (TRA) Methodology* (Канада, 2007 г.) [148] и российских (например, «ЭЛВИС+» [149]) исследовательских и

консалтинговых компаний, а также следующие стандарты и методические документы:

— Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» – Приложение 1. Рекомендуемый перечень классов, основных источников угроз ИБ и их описание [66];

— ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» – Приложение С. Примеры источников угроз [107];

— ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления» – Приложение В. Каталог угроз [108];

— Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [150];

— Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах», проект, и др.

Учитывая имеющийся опыт рассмотрения угроз ИБ в первоисточниках, были сформулированы пять важных требований к разрабатываемой классификации угроз ИБ:

1) в классификации должна содержаться информация об инцидентах ИБ, к которым приводят угрозы ИБ в случае их реализации и которые характерны как для самой ИТКС ОРГАНИЗАЦИИ, так и ЦИУСБ как ее важнейшей части и системообразующего элемента СОИБ ОРГАНИЗАЦИИ;

2) в классификации должна содержаться информация об этапе жизненного цикла объекта, на котором возникает угроза ИБ;

3) в классификации должна содержаться информация о направленности угрозы ИБ (внешнее окружение, общая архитектура, внутренняя конфигурация, ПО, сама информация и т.п.);

4) на одном уровне классификации не должны располагаться понятия разной степени абстракции, описывающие достаточно широкий отвлеченный класс проблем или какой-либо редкий частный случай;

5) в классификации необходимо связать угрозы ИБ с уязвимостями, которые могут использоваться для их реализации в виде компьютерных атак и инцидентов ИБ.

С термином «угроза ИБ» в области сетевой безопасности связаны еще два важных в настоящее время словосочетания, которые также имеют непосредственное отношение к обеспечению ИБ ИТКС ОРГАНИЗАЦИИ.

1. *Threat Intelligence* [81] – знания (аналитика) об угрозах ИБ, содержащие такую прове-

ренную, определенным образом обогащенную и значимую информацию о них как признаки, по которым можно распознать потенциальную угрозу, например, IP-адреса и домены, связанные с преступной активностью, сигнатуры вредоносного ПО, имена файлов и пользователей, адреса электронной почты, описание деятельности APT-группировок и применяемые ими инструменты и многое другое. Компания Gartner определяет *Threat Intelligence* как «основанные на фактических данных знания, включая контекст, методы, индикаторы, последствия и действенные рекомендации, о существующей или возникающей угрозе или угрозе для ИТ или информационных активов» [151]. Эти знания могут использоваться для принятия решений в отношении реагирования на ту или иную угрозу ИБ. Использование именно интеллектуального подхода при работе с угрозами ИБ уже признано наилучшей практикой в области ИБ – сначала нужно всесторонне изучить и понять угрозу, что потом позволит оценить ее источник, вероятность возникновения на ее основе инцидента ИБ, его серьезность и найти наиболее рациональные подходы для предотвращения последующей реализации данной угрозы. В сетевой среде ИТКС ОРГАНИЗАЦИИ применение интеллектуальных подходов особенно актуально в связи с наличием многообразных сетевых атак и их разновидностей, часто помогающих злоумышленникам избежать обнаружения при малейших изменениях своего поведения, файлов, средств атак и т.п. Системный интеллектуальный взгляд на собранные из разных источников первичные данные об угрозе ИБ ИТКС позволяет их преобразовать в ценную информацию, согласованную по определенным параметрам и критериям, а далее получить из этой информации общедоступные структурированные новые знания (так называемую аналитику, или интеллект – англ. *Intelligence*), своевременно выявляющие актуальные тенденции в изменении существующих и предсказывающие появление новых угроз ИБ. Более детально вопросы использования интеллектуальных подходов при обеспечении сетевой безопасности рассмотрены далее. Платформы *Threat Intelligence* в режиме реального времени накапливают данные о возможных угрозах ИБ из различных источников (открытых и закрытых, бесплатных и коммерческих), позволяют классифицировать её и производить с ней различные операции, включая выгрузку в СЗИ и SIEM-системы. С этим связано еще одно словосочетание – *Threat Intelligence Feeds* – непрерывные потоки структурированных постоянно обновляемых знаний об угрозах ИБ, полученных в результате применения ИБ-аналитики к исходным собранным данным и передаваемым организациям-подписчикам чаще всего из внешних источников. К ним относятся бесплатные и платные каналы информации об индикаторах компрометации (англ. *Indicator of Compromise, IoC*), бюллетени, внутренняя разведывательная информация организаций и их стратегических партнеров, информация известных в данной области компаний (типа *SANS*) и закрытых сообществ обмена информацией, относящихся к конкретным отраслям или приоритетным областям.

2. *Threat Hunting* [87] – постоянная упреждающая и интерактивная «охота за угрозами»,

закрывающаяся в циклическом поиске, обнаружении, локализации и анализе угроз ИБ, которые обходят существующие превентивные СЗИ. Это процесс, выполняемый преимущественно вручную, в рамках которого аналитик на основе эвристик, своих знаний и опыта обрабатывает собранные разными средствами с конечных точек и сетевых сенсоров (например, СОВ/СПВ) данные с целью выделения ранее не замеченных и не описанных признаков сетевых атак, которые далее будут использоваться для их автоматизированного распознавания. Получив из какого-либо источника *Threat Intelligence* информацию о новой атаке, аналитик сначала формулирует гипотезу — предположение о том, что произошел некий инцидент ИБ, который СЗИ могли в большом объеме «сырых» (англ. *raw*) данных пропустить. Далее гипотеза должна быть проверена. Тогда нарушение Политики ИБ будет либо подтверждено либо опровергнуто. Успешность проверки гипотезы во многом зависит от правильности ее формулирования, то есть от мастерства аналитика, что добавляет нежелательный субъективизм в процесс, который было бы хорошо устранить. И снова интеллектуальные подходы могут в этом помочь.

Обобщенные результаты разработки классификационных признаков для угроз ИБ ИТКС ОРГАНИЗАЦИИ, начало которой было положено в [55] и продолжено в [45, 46, 139, 140], сведены в табл. 3. Основными классификационными признаками типов угроз ИБ являются следующие: источник угрозы, расположение источника угрозы, цели реализации угрозы, направленность угрозы, стадии жизненного цикла элемента ИТКС, которые могут затронуть угрозы, используемые угрозой уязвимости, виды нарушения, вызванных угрозой ИБ (последствия/масштаб реализации угрозы), характер угрозы, предпосылки появления и природа происхождения угрозы, вероятность и метод реализации угрозы.

В целях выявления и оценки угроз ИБ дополнительно для каждого из классов можно определить подклассы (при необходимости), например, как в случае с выделением в подклассы отдельных элементов ИТКС, для которых так нагляднее ввести еще один уровень систематизации, детализирующий описание угрозы ИБ.

Следует иметь в виду, что параметры классификации, приведенные в табл. 3, взаимосвязаны сложным образом. Например, источники и формы реализации угроз ИБ определяют возможность порождать множественную природу происхождения угроз ИБ и наоборот. Поэтому при оценке общей защищенности ИТКС ОРГАНИЗАЦИИ предполагается изучение всех возможных комбинаций реализации перечисленных угроз и последствий, к которым они приводят.

Таблица 3 – Системная классификация угроз ИБ ИТКС (начало)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
Тип 1. Источник угрозы ИБ	Класс 1. Антропогенный (связанные с человеком)	Подкласс 1. Внешний	Террористы, лица, совершающий промышленный и экономический шпионаж, криминальные структуры, компьютерные преступники и хакеры, недобросовестные партнеры, технический персонал поставщиков телекоммуникационных услуг, представители аварийных служб и аутсорсинговых компаний и т.п. Социальная инженерия.
		Подкласс 2. Внутренний	Основной персонал (пользователи, программисты, разработчики). Представители подразделения безопасности (администраторы). Вспомогательный персонал (уборщики, охрана). Технический персонал (жизнеобеспечение, эксплуатация).
	Класс 2. Техногенный	Подкласс 1. Внешний	Авария городских средств связи. Авария городских инженерных систем (систем водопровода, отопления, канализации и кондиционирования). Перебои в системе электропитания. Авария на транспорте. Ошибка при передаче данных по сетям общего пользования.
		Подкласс 2. Внутренний	Повреждение кабелей или линий связи. Отказ (сбой) в работе технических средств. Колебания напряжения (перенапряжение, импульсные выбросы). Воздействие статического электричества, промышленных помех и технических наводок. Отказы электронных схем компьютеров и периферийного оборудования. Сбой (ошибки) в работе ПО, отказ ПО. Отказ (сбой, ошибки) в работе СЗИ, средств мониторинга, контроля и администрирования. Отказ в обслуживании вследствие перегрузки сервера. Воздействие вредоносного ПО. Выход из строя дискового накопителя с повреждением диска. Повреждение носителя данных при транспортировке. Повреждение резервной копии.
	Класс 3. Стихийный (естественный, связанный со средой)	Подкласс 1. Стихийные бедствия и природные катастрофы	Пожары, землетрясения, цунами, наводнения, смерчи, ураганы, удар молнии, магнитные бури, радиоактивное излучение.
		Подкласс 2. Нарушения внутриклиматических условий	Сбои или аварии в системе отопления и кондиционирования воздуха, что приводит к недопустимой температуре, влажности. Замерзание. Повышение содержания пыли. Повышение содержания углекислого газа.
		Подкласс 3. Форс-мажор и непредвиденные обстоятельства	Террористический акт, бомбовая атака, авария капитальных сооружений, поджог.

Таблица 3 – Системная классификация угроз ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
Тип 2. Расположение источника угрозы ИБ	Класс 1. Внешнее		Угроза утечки информации по техническим каналам ИТКС. Угроза утечки информации по оптическим каналам. Угроза утечки информации за счет электромагнитного излучения.
	Класс 2. Внутреннее		Угроза несанкционированного раскрытия, создания, изменения, удаления данных в СУБД. Угроза копирования информации с дискового запоминающего устройства на сервер или устройство конечного пользователя. Угроза вставки, изменения и удаления данных в потоке, проводимые несанкционированным способом. Угроза внедрения вредоносных программ, шпионских программ, руткитов. Угроза изменения IP- и MAC-адресов, имитирующие MAC- и IP-адреса других пользователей.
Тип 3. Цели реализации угрозы ИБ			Материальное обогащение. Промышленный и экономический шпионаж. Социальная инженерия. Угроза имиджу и репутации организации. Создание сбоев в ИТКС.
Тип 4. Направленность угрозы ИБ	Класс 1. Организация в целом		Угроза имиджу и репутации организации. Угроза разрушения информации или создания сбоев в ИС ИТКС с помощью вирусов для дезорганизации деятельности организации. Угроза потери доверия к поставщику облачных услуг.
	Класс 2. ИТКС	Подкласс 1. Уровень каналов связи и телекоммуникационного оборудования	Угроза намеренной порчи технических средств. Угроза порчи носителей информации. Угроза повреждения силовых и телекоммуникационных линий/кабелей связи. Угроза НСД к носителям данных из-за их незащищенного хранения.
		Подкласс 2. Уровень сетевой среды и ее отдельных элементов	Угроза перехвата трафика. Угроза разрыва соединения с сетью общего пользования. Угроза прослеживания пути доступа к каталогам.
		Подкласс 3. Общесистемное (общее), прикладное, специальное ПО	Угроза присвоения параметру неправильных значений при настройке ПО. Угроза введения некорректных значений входных данных. Угроза внедрения нарушителя в код ссылки на сторонние ресурсы. Угроза несанкционированного копирования ПО. Угроза использования несертифицированного ПО.

Таблица 3 – Системная классификация угроз ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
		Подкласс 4. Предоставление услуг	Угроза отказа/сбоя при предоставлении услуги. Угроза неподтверждения отправления или получения сообщения. Угроза предоставлению беспроводного доступа. Угроза лавинной маршрутизации пакетов с последующим аварийным отказом веб-сервера. Угроза манипулирования с настройками оборудования для блокировки определенных услуг.
		Подкласс 5. Функционирование	Угроза нештатного функционирования ПО. Угроза ошибок в работе ПО из-за сложного пользовательского интерфейса. Угроза контролю за исполнением мобильного кода. Угроза несоблюдения режимов загрузки. Угроза отслеживания модели обращения пользователя для обнаружения его идентификационных данных. Угроза потребления наибольшее количество ресурсов центрального процессора.
	Класс 3. СЗИ		Угроза выведения из строя СЗИ. Угроза доступа к конфигурационным файлам СЗИ. Угроза снижения функциональных характеристик (параметров) СЗИ. Угроза недоступности критичной для выполнения функций СЗИ информации (например, выход из строя носителей ключевой информации). Угроза нарушения целостности ПО СЗИ. Угроза отклонения параметров настроек СЗИ.
	Класс 4. Установившаяся практика управления и администрирования		Угроза некорректного управления потоками информации. Угроза управлению сервисами и операционными процессами. Угроза несвоевременного реагирования на инцидент ИБ. Угроза несвоевременного обновления базы антивирусного ПО. Угроза спуфинга управляющих сообщений, вызывающая неисправности приложений или перенаправление трафика на ложные адреса назначения. Угроза потери управления облачными ресурсами. Угроза захвата сертификата для управления веб-контентом.
	Класс 5. Процессы и процедуры	Подкласс 1. Бизнес-процессы	Угроза нарушения хода исполнения бизнес-процесса.
		Подкласс 2. Технологические процессы	Угроза нарушения хода исполнения технологического процесса.
		Подкласс 3. Информационные процессы	Угроза активизации ненужных сервисов. Угроза выхода процесса за пределы виртуальной машины.
		Подкласс 4. Процессы обеспечения ИБ	Угроза процессу аутентификации, например, угроза множественных попыток аутентификации. Угроза неконтролируемой загрузки и использования программных средств.

Таблица 3 – Системная классификация угроз ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
	Класс 6. Персонал	Подкласс 1. Работники бизнес-подразделений	Угроза использования социальной инженерии для получения информации о пользователях ИС ИТКС. Угроза несанкционированного раскрытия возможностей обслуживания пользователей. Угроза несанкционированного раскрытия предыдущих или текущего запроса к ИС ИТКС или мониторинга активности пользователя (например, содержание предыстории просмотра пользователем контента, деятельность в режиме онлайн при доступе к сетям общего пользования).
		Подкласс 2. Работники вспомогательных подразделений и внешний персонал	Угроза ошибочного обслуживания вспомогательных средств ИТКС. Угроза прохода злоумышленника в серверную или места хранения данных под видом вспомогательного персонала.
		Подкласс 3. Сотрудники подразделения безопасности	Угроза кражи идентификационных данных администратора ИС. Угроза изменения настроек СЗИ от имени администратора сетевой безопасности. Угроза злоупотребления полномочиями.
	Класс 7. Информация		Угроза хищения (копирования) персональных данных. Угроза доступа к файлу с паролями. Угроза доступа к ЖРС. Угроза ввода некорректных (ложных) данных и значений параметров (например, время). Угроза скрытой несанкционированной передачи конфиденциальной информации в составе легального сообщения.
Тип 5. Угрозы ИБ на стадиях жизненного цикла элементов ИТКС	Класс 1. Проектирование	Подкласс 1. Архитектура	Угроза некорректного проектирования многопоточной системы. Угроза некорректного проектирования ДМЗ. Угроза выбора неверной логикой функционирования ИС. Угроза «зацикливания» при выполнении программ.
		Подкласс 2. Технологии	Угроза некорректной установки среды виртуализации. Угроза некорректного использования облачных вычислений.
		Подкласс 3. Протоколы	Угроза использования небезопасных протоколов управления. Угроза несоблюдения протокола управления телекоммуникационным оборудованием. Угроза отправки искаженных сообщений протокола (например, сообщений с переполнением или потерей значимости) на устройство, снижающих производительность устройства до такой степени, что оно не может обработать обычные сообщения. Угроза несанкционированной активации/деактивации протоколов.

Таблица 3 – Системная классификация угроз ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
		Подкласс 4. Сервисы	Угроза некорректной работы обработчика прерываний. Угрозы некорректного закрытия сеансов пользователей. Угрозы удаленного управления ИС. Угрозы перехвата идентификационной информации при использовании telnet, ftp. Угроза перехвата информации при вводе-выводе. Угроза повторного воспроизведения пакета для получения доступа к сервису. Угроза неполной очистки памяти.
	Класс 2. Реализация и программирование	-	Специфические угрозы, связанные с использованием конкретных языков программирования. Угроза DoS-атаки из-за переполнения буфера. Угроза некорректной реализации протоколов под конкретной ОС. Угроза отсутствия блокировки доступа после неудачных попыток ввода пароля. Угроза анализа криптографических алгоритмов и их реализации.
	Класс 3. Внедрение и использование	-	Угроза использования неправильного сконфигурированных ОС, СУБД, и сервиса. Угроза выведения из строя системы хранения данных. Угроза распространения вредоносного ПО. Угроза использования нарушителем неудалённых установок по умолчанию. Угроза автоматизированного подбора простого пароля пользователя. Угрозы, вызванные несовместимостью версий используемого ПО. Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных.
	Класс 4. Снятие с эксплуатации	-	Угроза оставления в памяти неудалённой конфиденциальной информации. Угроза прямого обращения к памяти вычислительного поля суперкомпьютера.
Тип 6. Используемые угрозой ИБ уязвимости			Угроза, использующая уязвимости в архитектуре. Угроза, использующая уязвимости в реализации протоколов под конкретной ОС. Угроза, использующая уязвимости в ОС. Угроза, использующая уязвимости в приложениях. Угроза, использующая уязвимости в сервисах.
Тип 7. Виды нарушений, вызванных угрозой ИБ – последствия / масштаб реализации угрозы ИБ	Класс 1. Угроза нарушения свойств ИБ	Подкласс 1. Угроза нарушения конфиденциальности / приватности	Угроза хищения (копирования) информации и средств ее обработки. Угроза выполнения пользователем команд ОС с целью копирования файлов. Угроза чтения информации, передаваемой в незашифрованном виде. Угроза утечки информации при генерировании ПО сообщения об ошибке. Угроза получения сведений о владельце беспроводного устройства.

Таблица 3 – Системная классификация угроз ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
		Подкласс 2. Угроза нарушения целостности	Угроза модификации (искажения) информации. Угроза внедрения интерпретируемых операторов языков программирования или разметки в исходный код веб-приложения. Угроза внедрения произвольного кода в ПО. Угроза нарушения резервной копии. Угроза внедрения агента управления, выполняющего не-санкционированные действия.
		Подкласс 3. Угроза нарушения доступности	Угроза блокирования данных. Угроза уничтожения данных и средств их обработки. Угроза записи данных за пределами выделенного в памяти буфера, что вызовет аварийное завершение работы ПО. Угроза удаления файлов за счет выполнения пользователем команд ОС. Угроза искажения сообщения, вызывающая переполнение буфера. Угроза сокращения свободных областей памяти из-за неправильного освобождения памяти после использования.
		Подкласс 4. Угроза нарушения подлинности	Угроза отказа от авторства в отношении электронного документа. Угроза подмены доверенного пользователя или объекта в сети. Угроза обхода процедуры проверки подлинности. Угроза получения НСД к защищаемой информации из-за ошибки подтверждения подлинности сертификата.
		Подкласс 5. Угроза нарушения подотчетности	Угроза неполной записи событий в ЖРС. Угроза стирания информации в ЖРС. Угроза формирования ложных утверждений о полученных/переданных платежных документах.
		Подкласс 6. Угроза нарушения неотказуемости	Угроза отказ пользователя от факта выполнения им транзакции, от отправления или получения сообщения.
		Подкласс 7. Угроза нарушения достоверности	Угроза изменения пути исполнения программы из-за ошибки в форматной строке. Угроза «маскарада» (попытка злоумышленника выдать внедренный ложный объект за легальный маршрутизатор/сервер). Угроза навязывания ложной информации. Угроза несоответствия результатам работы приложения.
	Класс 2. Угроза нарушения физической целостности – физический ущерб		Угроза физического НСД неавторизированных лиц в контролируемую зону расположения технических средств, ИС. Угроза уничтожения резервной копии. Угроза уничтожения ПО. Угроза утраты информационных активов. Угроза отказа или неисправной работы телекоммуникационного оборудования. Угроза разрушения оборудования и носителей информации. Угроза кражи носителей данных, документов, оборудования. Угроза нарушения работоспособности персонала. Угроза незаконного использования аппаратных средств.

Таблица 3 – Системная классификация угроз ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
	Класс 3. Угроза нарушения логической структуры		Угроза нарушения непрерывности процессов. Угроза несанкционированного логического доступа неавторизованных субъектов к элементам ИТКС и информационным активам.
	Класс 4. Угроза утраты, кражи и ухудшения качества предоставляемых информационных услуг		Угроза снижения качества предоставляемых информационных услуг. Угроза утраты информационных сервисов. Угроза нарушения функционирования ПО. Угроза нарушения сопровождения ИС ИТКС. Угроза обмана поставщика услуг. Угроза клонирования устройства. Угроза незаконной обработки данных. Угроза избыточного дублирования/распространения информации, делающая возможным кражу услуг. Угроза нарушения предоставления услуги посредством досрочного завершения сеанса связи.
	Класс 5. Угроза нарушения функций и прав / полномочий, включая права собственности / владения		Угроза присвоения чужого права. Угроза использования нелицензионного ПО. Угроза фальсификации прав. Угроза отказа от осуществления действий. Угроза злоупотребления правами. Угроза «маскарада» с представлением чужого пароля, ключа или сертификата (например, системного администратора). Угроза несанкционированного использования административной информации по аутентификации (например, идентификатор пользователя/пароль). Угроза представления ложных полномочий, будто бы они верные, с намерением ввести в заблуждение. Угроза несанкционированного управления пользователями, например, предоставления деятельности, включая повышение/понижение привилегий.
<i>Тип 8. Характер угрозы ИБ</i>	Класс 1. Активная		Угрозы, оказывающие влияние на работу элементов ИТКС, например, угроза отказа в обслуживании для оборудования, угроза блокирования информации.
	Класс 2. Пассивная		Угроза, в случае реализации которой не вносятся какие-либо изменения в состав и структуру ИТКС, например, копирование и хищение конфиденциальной информации.
<i>Тип 9. Предпосылки и природа появления угрозы ИБ</i>	Класс 1. Объективные		Угроза блокирования конечной точки (например, сервера) посредством отправления большого количества недействительных сообщений, которые могут привести к аварийному отказу, перезагрузке, или исчерпать все ресурсы. Угроза ограниченности пропускной способности канала связи.

Таблица 3 – Системная классификация угроз ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
	Класс 2. Субъективные (связанные с человеческим фактором)	Подкласс 1. Случайная угроза ИБ	Угроза неумышленной порчи оборудования и носителей информации, повреждения силовых и телекоммуникационных линий/кабелей связи. Угроза неумышленного нарушения технологии обработки информации. Угроза неумышленного удаления (искажения) защищаемой информации и удаления (нарушения работы) программ. Угроза неумышленного разглашения конфиденциальной информации. Угроза случайного внесения изменений в ИС. Угроза непреднамеренного заражения компьютера вирусами. Угроза предоставления некачественных услуг третьей стороной. Угроза создания потенциальной опасности нарушения ИБ при использовании мобильных компьютеров и носителей информации вне организации, при дистанционной работе.
		Подкласс 2 Преднамеренная (умышленная, целенаправленная) угроза ИБ	Угроза повреждения (удаления) регистрационной, конфигурационной или иной информации, влияющей на безопасность ИС ИТКС. Угроза визуального перехвата информации с экранов мониторов или вводимой с клавиатуры для выявления паролей, идентификаторов и процедур доступа. Угроза копирования финансовой информации и паролей при негласном пассивном подключении к кабелю (скрытые передатчики) или приеме электромагнитного излучения сетевого адаптера. Угроза выявления паролей пользователей при негласном подключении к коммуникационной сети при имитации запроса сетевой ОС. Угроза анализ трафика при пассивном подключении к каналу связи или при перехвате электромагнитного излучения аппаратуры для выявления протоколов обмена. Угроза подключения к каналу связи в качестве активного ретранслятора для фальсификации платежных документов, изменения порядка следования, повторной передачи, доставки с задержкой или упреждением. Угроза блокирования потоков данных или их перенаправления, в частности, на системы, контролируемые злоумышленником. Угроза изменения даты и времени начала работы, запуска ПО. Угроза негласной переработки оборудования или ПО на фирменном изготовителе, фирме-поставщике, в месте складирования или в пути следования к заказчику. Угроза сканирования для поиска уязвимостей на хостах и определения топологии сети.

Таблица 3 – Системная классификация угроз ИБ ИТКС (окончание)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры угроз ИБ/источников угроз ИБ</i>
Тип 10. Вероятность реализации угрозы ИБ	Класс 1. Высоковероятная	-	Угроза реализуется очень часто, например, угроза сканирования с целью определения открытых портов.
	Класс 2. Возможная		Угроза реализуется часто, например, угроза <i>DoS</i> -атаки на веб-сервер.
	Класс 3. Маловероятная	-	Угроза реализуется редко, например, угроза разрушения помещения серверной вследствие землетрясения.
Тип 11. Метод реализации угрозы ИБ			Сканирование. Маскарад. Подмена доверенного объекта. Внедрение ложного объекта. <i>DoS</i> -атака. Использование скрытых каналов для утечки информации. Расширение прав доступа после взлома ИС.

Как видно из табл. 3, даже в классификационных параметрах угроз ИБ не удалось избежать упоминания уязвимостей и источников угроз ИБ, что в очередной раз подтверждает их неразрывную связь.

Более наглядно и компактно все типы возможных угроз ИБ ИТКС ОРГАНИЗАЦИИ изображены на рис. 15.

Представленная системная классификация не претендует на полноту, поскольку новые угрозы ИБ из-за выявления уязвимости «нулевого дня» (англ. *0day, zero day*) (становится известной до момента выпуска разработчиком компонента ИС соответствующих мер защиты информации, исправлений недостатков или обновлений [142]) могут возникать почти каждый день. Она может быть использована в качестве основы для расширения в будущем.

Данная классификация необходима для определения актуальных для ИТКС ОРГАНИЗАЦИИ угроз ИБ с целью последующего выбора мер обеспечения ИБ, снижающих или устраняющих возможность их реализации злоумышленниками в виде компьютерных атак и инцидентов ИБ.

Обе разработанные системные классификации уязвимостей и угроз ИБ полностью согласованы между собой, что обеспечивает целостный взгляд на природу происхождения инцидентов ИБ для последующего понимания какие уязвимости устранять и каких последствий от их реализации ожидать. Они необходимы для построения Модели угроз ИБ и Модели нарушителей ИБ, составляющих основу разработки положений сначала Корпоративной Политики обеспечения ИБ ОРГАНИЗАЦИИ (далее – Политики ИБ ОРГАНИЗАЦИИ), а затем частной Политики ИБ ИТКС и реестра рисков ИБ для выбора адекватных мер обеспечения ИБ ИТКС ОРГАНИЗАЦИИ и процессов обеспечения ИБ для защищаемых информационных активов ИТКС, который также строится на основе Модели угроз ИБ.

Согласно [65, 150], Модель угроз ИБ представляет собой описание (чаще всего в словесной или табличной форме), которое включает в себя следующее:

- объекты защиты или объекты, пригодные для реализации угрозы ИБ;
- возможные источники угроз ИБ;
- уязвимости/классы уязвимостей, используемые источниками угроз ИБ;
- способ/метод реализации угроз ИБ;
- возможные виды деструктивных воздействий/типы возможной потери (например, конфиденциальности, целостности, доступности информационного актива);
- масштабы потенциального ущерба.



Рисунок 15 – Системная классификация угроз ИБ ИТКС ОРГАНИЗАЦИИ

В случае, если источником угрозы ИБ является человек, то строится вторая модель – Модель нарушителей ИБ [65]. Она представляет собой описание и классификацию нарушителей ИБ, включая определение их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.

2.4. Системная классификация сетевых атак на информационно-телекоммуникационную сеть

На основе составленной системной классификации угроз ИБ выделим только те, которые могут реализоваться в виде сетевых атак на элементы ИТКС ОРГАНИЗАЦИИ или на ИТКС в целом, таких как целенаправленные и избирательные *APT*-атаки, фишинг в отношении отдельных личностей и сотрудников организации (англ. *spear-phishing*), непобедимый «нигерийский спам», атаки типа «отказ в обслуживании» (*DoS*-атаки), межсайтовый скриптинг (англ. *Cross-Site Scripting, XSS*), *SQL*-инъекции, прослушивание трафика, создание сложных и подмена существующих объектов в ИТКС и многие другие. Например, основными типичными сетевыми атаками для отдельного компьютера персонала при использовании различных соединений являются следующие: установление полного контроля с несанкционированным удаленным доступом к информации на компьютере и сбор информации пользователя (через заполненные анкеты, *Java*-скрипты, *cookie*-файлы и т.д.), «подвешивание» компьютера в результате *DoS*-атаки на него; активный и пассивный перехват информации (искажение или уничтожение данных и ПО на компьютере, кража информации, в том числе перехват незашифрованных сообщений по электронной почте и т.д.), перехват установленных сеансов связи (англ. *hijacking*), «сборка мусора» из памяти компьютера (англ. *garbage collection*), спам, фишинг, воздействие компьютерных вирусов и вредоносных программ, «маскарад» (выполнение каких-либо действий одним пользователем от имени другого с присвоением его прав и привилегий) и т.д.

В отличие от ситуации с уязвимостями и угрозами ИБ, сетевым атакам не посвящен ни один нормативный или правовой российский или зарубежный документ. Единственным источником информации подобного уровня может служить серия стандартов по безопасности сетей ISO/IEC 27033 [60, 108], в которой перечислены, например, возможные реализации следующих угроз ИБ:

- вирусные атаки и внедрение вредоносных программ, которые могут привести к потере или повреждению информации, потере контроля над инфраструктурой ИТ;
- загрузка пользователем файлов или программ, которые обходят защиту сети, используя такие методы, как быстрота прохождения порта и шифрование;

- утечка информации с использованием скрытых каналов для сетевых агентов-роботов;
- установка «троянских программ» (программ, приводящим к неожиданным и обычно нежелательным результатам), которые могут разрешать несанкционированный внешний доступ, приводящий к нарушению конфиденциальности;
- несанкционированное воздействие на меры обеспечения ИБ инфраструктуры, систем и приложений, что может привести к мошенничеству, отказу в обслуживании, а также злоупотреблению возможностями;
- атака с целью снижения доступности сети связи, в том числе чрезмерное использование услуг, связанных с пропускной способностью, например, потоковые мультимедийные средства или одноранговое совместное использование файлов может привести к перегрузке сети;
- *DoS*- и *DDoS*-атаки на порталы или расширенные сети услуг «бизнес–бизнес»;
- инсайдерские атаки с помощью авторизованных партнеров по бизнесу [152];
- фальсификация информационного наполнения транзакции (сообщения не передаются получателю или данные изменяются в процессе передачи) и ряд других.

Описанию различных видов атак и их сценариям развития посвящено множество публикаций, которые были кратко описаны в работе [141] автора данного исследования. Первый типичный сценарий, состоящий из пяти этапов, часть из которых можно повторять многократно, представил в 2000 г. Р.Грэхэм (R.Graham) в [153]:

1. Внешняя разведка (англ. *outside reconnaissance*), в ходе которой злоумышленник пытается выяснить как можно больше о «жертве», не представив себя, находя общедоступную информацию или появляясь в системах как обычный пользователь. На этом этапе он не может быть обнаружен, поскольку просто выполняет в интернете «*whois*»–запрос информации о целевой сети, узнает, как, где и кем зарегистрировано доменное имя, просматривает *DNS*-таблицы для поиска имен компьютеров в домене, изучает другую открытую информацию о веб-сайте компании, анонимных *FTP*-серверах и т.д.

2. Внутренняя разведка (англ. *inside reconnaissance*), когда злоумышленник использует более «контактные» методы поиска информации, но все же не делает ничего плохого, например, переходит по веб-страницам, ищет уязвимые *CGI*-скрипты (англ. *Common Gateway Interface*) и работающие в настоящий момент компьютеры, сканирует *UDP/TCP*-порты на выбранных компьютерах для поиска доступных сервисов и т.п.

3. Использование эксплойтов (англ. *exploits*) – программ, использующих (эксплуатирующих) известные уязвимости на целевых компьютерах. Злоумышленник начинает проверять учетные записи с легко угадываемыми или пустыми паролями, пытается скомпрометировать *CGI*-скрипт, отправляя команды оболочки в поле ввода, использует хорошо известные проблемы кода, приводящие к переполнению буфера, посылая большие объемы данных, и т.д.

4. Закрепление/удержание в системе (англ. *foot hold*), направленное на сокрытие следов атаки (например, за счет изменения ЖРС) и удостоверение в том, что он может вернуться в систему снова, установив средства для последующего доступа, например, заменив существующие сервисы троянскими программам, содержащими программные закладки, или лазейки, или «люки» (англ. *backdoor/trapdoors*) (например, точки входа в программу, открывающие доступ к некоторым системным функциям, или намеренно измененный фрагмент ПО), создав новые учетные записи пользователей и т.д. Затем злоумышленник использует взломанную систему для доступа к смежным, поскольку большинство сетей хуже защищены от внутренних атак.

5. Реализация конечных целей атаки и получение желаемой прибыли (англ. *profit*), когда злоумышленник использует свой статус нахождения в системе/сети для кражи конфиденциальных данных, злоупотребления системными ресурсами и т.д.

Немного отличное, но очень похожее представление о том же процессе дает Т.Ользак (T.Olzak) в 2008 г. в [154]:

- 1) разведка для сбора как можно большего количества информации о «жертве»;
- 2) сканирование периметра и внутренних сетевых устройств в поисках уязвимостей;
- 3) получение доступа к ресурсам для извлечения ценной для злоумышленника информации или использования сети как места запуска атак против других «жертв»;
- 4) сохранение доступа в течение достаточно долгого периода времени для достижения своих целей;
- 5) сокрытие следов вторжения в систему и возможных элементов управления, оставленных для будущих посещений.

И только двумя годами позже, в 2010 г., компанией *Lockheed-Martin* был введен термин «*Kill Chain*» [155], который первоначально использовался в военном деле, а сейчас незаслуженно часто упоминается в отношении сетевых атак, без отсылки к самой первой работе [153], с которой все фактически начиналось. Военная концепция развития атаки образно представляет ее как интегрированный сквозной процесс, описываемый «цепочкой», прерывание на любом этапе которой может прерывать весь процесс в целом. Эти этапы таковы: найти/локализовать цель, зафиксировать ее местоположение или затруднить ее перемещение, отслеживать движение, поразить: выбрать для использования подходящее оружие для создания желаемых результатов в отношении цели, вовлечь/применить оружие по отношению к цели, оценить последствия атаки. Согласно [154], модель *Intrusion Kill Chain* для сетевых атак *Lockheed-Martin* содержит следующие этапы:

- 1) разведка (англ. *reconnaissance*) – злоумышленник выбирает цель, исследует ее (посредством пассивного поиска, сканирования портов и т.д.) и пытается выявить уязвимости в целевой сети;

2) создание оружия (англ. *weaponization*) – злоумышленник создает для одной или нескольких уязвимостей систем, приложений и т.п. удаленное вредоносное оружие (например, вирус или червь) в загружаемых данных (например, файлах *Adobe PDF* или *Microsoft Office*);

3) доставка (англ. *delivery*) – злоумышленник пересылает к цели оружие (например, через вложения электронной почты, используя фишинг, зараженные сайты или *USB-накопители*);

4) эксплуатация (англ. *exploitation*) вредоносного оружия, после чего оно отключает триггеры, свидетельствующие об атаке в целевой сети;

5) установка (англ. *installation*) – вредоносное оружие устанавливает точку доступа (например, троянскую программу), которую может использовать злоумышленник и которая разрешает ему постоянный доступ и повышает привилегии;

6) управление и контроль (англ. *command and control*) – вредоносное ПО позволяет злоумышленнику постоянно «держать руки на клавиатуре» в целевой сети;

7) действия по достижению цели (англ. *actions on objective*) – злоумышленник предпринимает действия для достижения цели (целей) атаки, такие как фильтрация данных (выборка данных из всех данных по определенным критериям), уничтожение данных, шифрование с требованием выкупа, перемещение на другое устройство и т.д.

Фактически, модель *Intrusion Kill Chain* просто делит фазу «Использование эксплойтов» Р.Грэхэма, добавляя фазы «Создание оружия» и «Доставка» перед фазой «Эксплуатация». Фазы «Управление и контроль» и «Действия по достижению цели» модели *Intrusion Kill Chain* полностью совпадают с фазами «Удержание» и «Получение прибыли» [153].

Поскольку сегодня чаще говорят о кибератаках, появились еще несколько моделей с названием «*Cyber Kill Chain*» с разными вариантами этапов, например, разведка, сканирование, доступ и эскалация, эксфильтрация конфиденциальных данных, изменение или удаление файлов на скомпрометированных системах, удержание (англ. *sustainment*) (пребывание «в тишине»); нападение с изменением функциональности оборудования жертвы или полным отключением АО (например, атака *Stuxnet*); обфускация с целью запутать, дезориентировать и отвлечь расследование состоявшейся компьютерной атаки. (Намеренно опустим ссылки, потому что установить первого автора очень похожих описаний без дальнейшего расследования фактов плагиата не представляется возможным.)

Самым серьезным и уважаемым источником информации о тактиках, методах и знаниях современных атакующих является модель *ATT&CK* (*Adversarial Tactics, Techniques & Common Knowledge*) компании *MITRE* [156] (предшественник модели появился еще в 2011 г.), в основном ориентированная на сети, использующие ОС *Microsoft Windows*. Каждая категория тактики из модели *ATT&CK*, которых на сентябрь 2020 г. было выделено двенадцать, содержит список приемов, способов и порядков действий, которые может использовать злоумышленник. Методы

разделены таким образом, чтобы предоставить их техническое описание, индикаторы, полезные данные для защиты и анализа при обнаружении и возможные способы смягчения последствий.

Приведем несколько примеров из матрицы *MITRE ATT&CK*, обеспечивающей глубокий уровень детализации в описании этапов модели *Lockheed-Martin* в части того, что может произойти во время атаки после того, как противник получил доступ:

1) первоначальный доступ (англ. *initial access*): эксплуатация открытых приложений, добавление оборудования, репликация через съемные носители, вложение/ссылка для фишинга; фишинг через услугу, компрометация цепочки поставок, использование доверительных отношений и т.д.;

2) выполнение (англ. *execution*): использование интерфейса командной строки, элементов панели управления или динамического обмена данными, через загрузку *API/GUI/PowerShell/module*, скомпилированный *HTML*-файл, запланированная задача, сценарии, использование сервисов, использование пространства после имени файла, удаленное управление и т.д.;

3) присутствие (англ. *persistence*): манипуляция учетной записью, наложение приложений, расширения к браузеру, изменение ассоциации файлов по умолчанию, внешние удаленные сервисы, скрытые файлы и каталоги, подключение, инъекция параметров выполнения файла, запуск агента/демона, элемент входа, выход из системы, новый сервис, запуск приложения, перехват пути, использование локального монитора портов, злоупотребление избыточным доступом, запланированная задача, модификация ярлыков, установка внешних удаленных сервисов и т.д.;

4) эскалация привилегий (англ. *privilege escalation*): манипуляция токеном доступа, наложение приложений, обход пользовательского управления приложениями, *DLL*-инъекция, эксплуатация для эскалации привилегий, инъекция в процесс, работа от имени суперпользователя (*sudo*), перехват маршрута, веб-оболочка и т.д.;

5) обход защиты (англ. *defense evasion*): очистка истории команд, подписывание кода, расшифровка файлов/информации, отключение СЗИ, отключение индикатора блокировки/удаления, удаление файлов, изменение разрешений для файла, логическое смещение в файловой системе, скрытые файлы/окна/пользователи, выполнение команд в фоновом режиме, установка корневого сертификата, маскарад, изменение реестра, удаление процесса, измененное время, обход управления учетными записями пользователей, удаление процесса и т.д.;

6) доступ к учетным данным (англ. *credential access*): сброс учетных данных, захват ввода, прослушивание сети, перехват двухфакторной аутентификации и т.д.;

7) исследование (англ. *discovery*) системных сервисов/информации, приложений, реестра запросов, конфигурации сети, удаленных систем, владельца/пользователей системы, сетевых

сервисов/соединений, процессов, ПО СЗИ, групп разрешений, файлов/каталогов, учетных записей, периферийных устройств, системного времени и т.д.;

8) движение «в бок», или ответвление (англ. *lateral movement*): использование стороннего ПО/ПО для развертывания приложений/удаленных сервисов, удаленное управление *Windows/Admin shares*, сценарии входа в систему, использование эксплойтов, использование протокола удаленного рабочего стола, репликация через съемный носитель, восстановление удаленной копии файла и т.д.;

9) сбор (англ. *collection*) данных от локальной системы/съемных носителей/сетевых устройств, захват входного сигнала/аудио/видео/экрана, пришедших данных, сбор сообщений электронной почты, автоматизированный сбор, сбор данных из буфера обмена и т.д.;

10) команды и контроль (англ. *command and control*): запутывание данных/кодирование, использование резервных каналов, пользовательского криптографического/командного и управляющего протоколов, многополосной связи, обычно/необычно используемый порт, стандартный протокол уровня приложения, многослойное шифрование, соединения через прокси-сервер, связь через съемные носители и т.д.;

11) эксфильтрация (англ. *exfiltration*): доставка информации, интересующей злоумышленника, в его зону доступа, или когда он заставляет пользователя что-то сделать на свою пользу, эксфильтрация через другой сетевой носитель/командный и управляющий канал/альтернативный протокол/физический носитель, автоматизированная эксфильтрация, запланированная передача, сжатие/зашифрование данных, ограничение размера передачи данных и т.д.;

12) воздействие (англ. *impact*): удаление учетной записи, разрушение данных, подмена стартовой веб-страницы, стирание данных на диске, отказ в обслуживании, перехват ресурсов, перезагрузка системы и т.д.

Другой подход к оценке сетевых атак основан на перечислении и классификации общих типов атак *MITRE CAPEC (Common Attack Pattern Enumeration and Classification)* [157], где шаблоны атак организованы иерархически с учетом 1000 методик, которые часто используются при эксплуатации уязвимости. Эти методики подразделяются на 9 категорий: манипулирование системными ресурсами (262), манипулирование структурами данных (255), вмешательство в процесс контроля доступа (225), использование вероятностных методов (223), злоупотребление существующей функциональностью (210), манипулирование временем и состоянием (172), участие в обманчивых взаимодействиях (156 шт.), ввод неожиданных значений (152) и сбор и анализ информации (118).

На основе известной информации о развитии сетевой атаки могут быть сформулированы индикаторы компрометации (*IoC*) – артефакты как описанные специалистами признаки, отражающие наблюдаемые события, действия, объекты и т.п. в сети, ОС, СУБД, приложении, на

рабочей станции, сервере и т.п., которые с высокой степенью вероятности указывают на принимаемую или уже состоявшуюся атаку. Они используются для описания того, что атака, возможно, уже произошла или может произойти прямо сейчас или в будущем, то есть для обнаружения попыток проникновения в компьютерные системы на ранних стадиях и первичной оценки возможного ущерба. Примеры *IoC* – это адреса командных серверов ботнетов (англ. *botnet*, от *robot network*), электронные адреса рассылщиков фишинговых писем и спама, сигнатуры вирусов, хэш-суммы вредоносных файлов.

Данные, характеризующие стадии атаки и ее типичные последствия, можно собрать из различных источников в атакованной сети, а далее извлечь и нормализовать (привести к сопоставимому виду/формату) для последующей корреляции (выявления событий ИБ, имеющих логическую связь и потенциально значимых для выявления возможных нарушений ИБ). Автором данного исследования в [141] были предложены вербальные описания некоторых ключевых типовых признаков, характеризующих типичные действия злоумышленника и свидетельствующих об удаленных сетевых атаках, которые полностью применимы к ИТКС ОРГАНИЗАЦИИ. Приведем ряд примеров.

- Несанкционированный пользователь в сети.
- Активность пользователя в нерабочее время (ночью или в выходной).
- Совместно используемые учетные данные.
- Доступ к учетной записи сервиса в интернете или несанкционированному устройству.
- Несколько входов с одинаковым идентификатором из разных мест за короткое время.
- Одна учетная запись хоста/пользователя пытается войти на несколько хостов в сети через несколько минут из/в разные регионы.
- Многочисленные изменения за короткое время от административных учетных записей.
- Неавторизованное/не соответствующее политике, установке обновлений и т.п. устройство в сети.
- Появление нового неавторизованного хоста или сетевого сервиса во внутреннем сегменте интранета.
- Неавторизованное подключение внутреннего хоста (клиента, сервера) к интернету.
- Взаимодействие внутренних узлов либо с известными ненадежными адресатами, либо с хостами, расположенными в другой стране, где нет деловых партнеров организации, или внешними хостами с использованием нестандартных портов или несоответствия протокола и порта.
- Хосты, которые публично доступны или расположены в ДМЗ сети организации, обмениваются данными с некоторыми внутренними узлами, что указывает на проход извне

внутри и обратно, фильтрацию данных и удаленный доступ к сетевым ресурсам.

— Многочисленные предупреждения об опасности от одного хоста или повтор событий на нескольких компьютерах в одной подсети в течение 24 часов (например, повторные попытки аутентификации).

— Обнаружение связей известного вредоносного ПО, например, доступ с одного или нескольких внутренних узлов на внешний вредоносный веб-сайт (из известных «черных» списков).

— Повторное заражение системы вредоносным ПО в течение короткого времени после очистки (сигнал о наличии руткита (англ. *rootkit/toolkit*) – набора программных средств для маскировки действий злоумышленника или *APT*-атаки).

— Обнаружение нескольких зараженных хостов или типичных широко известных эксплойтов.

— Необычные маршруты доступа (например, некоторые БД обычно доступны только определенным приложениям, а не непосредственно пользователям).

— Чрезмерный исходящий (например, веб-, электронная почта) или входящий (например, потоковая передача, веб-) трафик из одного источника или в один адрес назначения. Например, необычный трафик между серверами может быть характерной чертой для необнаруженных вредоносных программ, ищущих хранилища данных.

— Сканирование/зондирование сети/уязвимостей внутренними узлами, общающимися с несколькими хостами за короткое время или во время неразрешенного периода времени.

— Несанкционированная загрузка драйверов.

— Неожиданное завершение/создание/сетевая активность процесса.

— Создание процессом именованного канала или подключение процесса к именованному каналу.

— Несанкционированная модификация таблицы импорта запущенного процесса.

— Прописывание исполняемого файла/команды в автозагрузку: изменение специфичных ключей реестра, создание/изменение файлов в специфичных каталогах, создание/изменение сервисов, задач планировщика и т.п.

— Обнаружение скрытого процесса или модуля.

— Доступ процесса к памяти другого процесса для чтения/записи.

— Неожиданная загрузка процессом *DLL*-библиотеки.

— Неожиданное создание/изменение/переименование/удаление процессом файла, например, отсутствие или повреждение файлов или появление новых файлов, которые не были созданы внутренними пользователями.

— Имя файла с необычными символами.

- Модификация атрибутов безопасности файла (скрытый, системный и т.д.) или файловой системы.
- Несанкционированное создание общих сетевых каталогов, доступ к ним.
- Манипуляция с объектами каталога *Active Directory*.
- Изменения политики безопасности/аудита событий.
- Исправленные или удаленные на источнике данных о событиях ЖРС или источник данных о событиях, остановивший запись.
- Неавторизованное изменение конфигурации устройства (включая СЗИ).
- Чрезмерный перерыв между сканированиями средствами антивирусной защиты (СAB3).
- Чрезмерные попытки блокировки портов от систем мониторинга, таких как CAB3.
- Обращения по протоколу *HTTPS* к фишинговым доменам, похожим на домены компании.
- Повторная атака из одного источника или одного хоста.
- НСД к конфиденциальным, персональным или финансовым данным.
- Скрытые каналы передачи данных (например, с использованием туннелирования).
- Большое количество отклоненных писем с подозрительным контентом.
- Аномалии в основных настройках доступа и аутентификации пользователей, сети, приложений, подозрительная деятельность, *DoS*-атака и т.д.
- Другие признаки, такие как отказы/сбой ПО, повторение некоторых конкретных событий, неправильные команды, случайные атрибуты, не соответствующие параметры сетевого трафика, попытки передачи больших объемов данных.
- Подозрительные события и процессы, трафик на известный уязвимый хост и т.д.

Приведенный список не ранжирован по частоте встречаемости подобных атак, по тяжести последствий и т.п. Каждая организация должна внедрить свою собственную приоритезацию компьютерных атак. Например, для многих организаций доставка вредоносного почтового сообщения менее важна, чем активное управление и контроль злоумышленником зараженной рабочей станцией.

Как видно из всех приведенных примеров, источником сетевой атаки всегда является человек (антропогенный источник), использующий для достижения своего замысла (цели) различные методы и средства реализации атаки.

Учитывая имеющийся опыт описания сетевых атак в многочисленных источниках, были сформулированы пять важных требований к разрабатываемой классификации сетевых атак:

1) в классификации должна содержаться информация об инцидентах ИБ, к которым приводят сетевые атаки, которые характерны как для самой ИТКС ОРГАНИЗАЦИИ, так и ЦИУСБ

как ее важнейшей части и системообразующего элемента СОИБ ОРГАНИЗАЦИИ;

2) в классификации должна содержаться информация об этапе жизненного цикла объекта, на котором возникает сетевая атака;

3) в классификации должна содержаться информация о целенаправленности атаки на различные элементы ИТКС;

4) на одном уровне классификации не должны располагаться понятия разной степени абстракции, описывающие достаточно широкий отвлеченный класс проблем или какой-либо редкий частный случай;

5) в классификации необходимо связать сетевые атаки с видами угроз ИБ, которые могут использоваться для их реализации, и соответствующими уязвимостями.

Единственный документ по компьютерным атакам, представленный в открытом доступе, который был использован при составлении данной классификации, это «Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (Версия 2.3)», утвержденный Банком России [158]. Опираясь на него и результаты многолетнего анализа, проводимого автором данного исследования [45, 46, 48, 55, 132, 134-141, 159], представим системную классификацию сетевых атак на ИТКС ОРГАНИЗАЦИИ в целом и ее элементы (табл. 4). Основными классификационными признаками типов сетевых атак являются следующие: расположение атакующего, цели (мотивация) реализации атаки, направленность атаки, атаки относительно стадий жизненного цикла элементов ИТКС, используемые атакой уязвимости, условие начала атаки, тип воздействия (характер) атаки, уровень реализации в соответствии с семиуровневой моделью взаимодействия открытых систем *OSI/ISO*, виды нарушений, вызванных атакой – последствия/масштаб реализации атаки, серьезность ущерба (тяжесть последствий) от атаки для деятельности организации, вид атакующего, число жертв и атакующих, наличие обратной связи атакующего с жертвой, метод и средства реализации атаки, а также вероятность реализации атаки, вероятность ее повторения в будущем и сложность обнаружения атаки.

В целях выявления и оценки сетевых атак дополнительно для каждого из введенных классов можно еще определить и подклассы (при необходимости), например, как в случае с выделением в подклассы отдельных элементов ИТКС, для которых так нагляднее ввести еще один уровень систематизации, детализирующий описание сетевой атаки.

Как видно из табл. 4, в классификационных параметрах сетевых атак не удалось избежать упоминания уязвимостей и источников угроз ИБ – атакующих, что в очередной раз подтверждает неразрывную связь всех этих понятий.

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (начало)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
Тип 1. Расположение атакующего	Класс 1. Атака из внешней по отношению к ИТКС среды		Атака из интернета. Атака из облака сервис-провайдера. Атака из сети бизнес-партнера (экстранета). Атака с мобильного устройства. Повреждение носителя данных при транспортировке. Утечки информации за счет электромагнитного излучения.
	Класс 2. Атака внутри ИТКС	Подкласс 1. В одном сегменте сети	Несанкционированное раскрытие, создание, изменение, удаление данных в СУБД. Отказы электронных схем компьютеров и периферийного оборудования. Сбой (ошибки) в работе ПО, отказ ПО. Отказ в обслуживании вследствие перегрузки сервера. Прослушивание (англ. <i>sniffing</i>). Атака «третий по середине» (англ. <i>Man-in-the-Middle, MitM</i>). Атака с <i>USB</i> -накопителя.
		Подкласс 2. В разных сегментах сети	Атака с рабочей станции работника организации. Повреждение кабелей или линий связи. Утечка информации по техническим каналам ИТКС. Отказ (сбой, ошибки) в работе СЗИ, средств мониторинга, контроля и администрирования. <i>MitM</i> -атака. «Шторм» запросов (англ. <i>flooding</i>).
Тип 2. Цель (мотивация) атаки			Материальное обогащение. Промышленный и экономический шпионаж. Социальная инженерия. Угроза репутации организации. Месть. Создание сбоев в ИТКС. Самоутверждение. Вредительство. Хактивизм. Саботаж.
Тип 3. Направленность атаки	Класс 1. ИТКС	Подкласс 1. Уровень каналов связи и телекоммуникационного оборудования	Намеренная порча технических средств. Порча носителей информации. Повреждение силовых и телекоммуникационных линий/кабелей связи. НСД к носителям данных из-за их незащищенного хранения.
		Подкласс 2. Уровень сетевой среды и ее отдельных элементов	Перехват трафика. Разрыв соединения с сетью общего пользования. Проследивание пути доступа к каталогам.
		Подкласс 3. Общесистемное, прикладное, специальное ПО	Присвоение параметру неправильных значений при настройке ПО. Введение некорректных значений входных данных. Внедрение нарушителем в код ссылки на сторонние ресурсы. Несанкционированное копирование ПО.
		Подкласс 4. Предоставление услуг	Отказ/сбой при предоставлении услуги. Неподтверждение отправления или получения сообщения. Атака на точку беспроводного доступа. Лавинная маршрутизация пакетов с последующим аварийным отказом веб-сервера. Манипулирование с настройками оборудования для блокировки определенных услуг.

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
		Подкласс 5. Функционирование	Ошибки в работе ПО из-за сложного пользовательского интерфейса. Нарушение контроля за исполнением мобильного кода. Неверные режимы загрузки. Отслеживание модели обращения пользователя для обнаружения его идентификационных данных. Потребление наибольшее количество ресурсов центрального процессора.
	Класс 2. СЗИ		Атака на СЗИ с целью выведения его из строя. Изменение настроек в конфигурационном файле СЗИ. Недоступность критически важной информации для выполнения функций СЗИ. Нарушение целостности ПО СЗИ. Нарушение целостности аппаратного СЗИ.
	Класс 3. Установившаяся практика управления и администрирования		Атака на управление потоками информации, сервисами, операционными процессами, облачными ресурсами. Спуффинг (англ. <i>spoofing</i>) управляющих сообщений, вызывающая неисправности приложений или перенаправление трафика на ложные адреса назначения. Захват сертификата для управления веб-контентом.
	Класс 4. Процессы и процедуры	Подкласс 1. Бизнес-процессы	Нарушение хода исполнения бизнес-процесса.
		Подкласс 2. Технологические процессы	Нарушение хода исполнения технологического процесса.
		Подкласс 3. Информационные процессы	Активизации ненужных сервисов. Выход процесса за пределы виртуальной машины.
		Подкласс 4. Процессы обеспечения ИБ	Атака на процесс аутентификации. Неконтролируемая загрузка и использование программных средств.
	Класс 5. Персонал	Подкласс 1. Работники бизнес-подразделений	Несанкционированное раскрытие возможностей обслуживания пользователей, их предыдущих или текущего запроса к ИС ИТКС или мониторинга активности пользователя. Фишинг. Социальная инженерия для получения информации о пользователях ИС ИТКС.
		Подкласс 2. Работники вспомогательных подразделений и внешний персонал	Атака на обслуживание вспомогательных средств ИТКС. Проход злоумышленника в серверную или места хранения данных под видом вспомогательного персонала.
		Подкласс 3. Сотрудники подразделения безопасности	Кража идентификационных данных администратора ИС. Изменение настроек СЗИ от имени администратора сетевой безопасности.

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
	Класс 6. Информация		Хищение (копирование) персональных данных. Доступ к файлу с паролями. Доступ к ЖРС. Ввод некорректных (ложных) данных и значений параметров (например, время). Скрытая несанкционированная передача конфиденциальной информации в составе легального сообщения. Перехват и подмена информации о платежах. Атаки на информацию о телекоммуникационной среде. Атаки на управляющую и контролирующую информацию общего/специального назначения.
Тип 4. Атаки на стадиях жизненного цикла элементов ИТКС	Класс 1. Проектирование	Подкласс 1. Архитектура	Вставка «зацикливания» при написании кода программ. Некорректно спроектированная ДМЗ. Выбор неверной логикой функционирования ИС.
		Подкласс 2. Технологии	Некорректная установка среды виртуализации. Некорректное использовании облачных вычислений.
		Подкласс 3. Протоколы	Использование небезопасных протоколов управления. Атака на протокол управления телекоммуникационным оборудованием. Отправка искаженных сообщений протокола на устройство, снижающих производительность устройства. Несанкционированная активация/деактивация протоколов.
		Подкласс 4. Сервисы	Атака на обработчик прерываний. Чтение данных из неочищенной памяти. Удаленное управление ИС. Атака для закрытия сеансов пользователей. Перехват информации при вводе-выводе. Перехват идентификационной информации при использовании сервисов telnet, ftp. Атака повторным воспроизведением (англ. <i>replay attack</i>) пакета для получения доступа к сервису.
	Класс 2. Реализация и программирование	-	DoS-атака из-за переполнения буфера. Атака на блокировку доступа после неудачных попыток ввода пароля. Анализ реализации криптографических алгоритмов для атаки на них.
	Класс 3. Внедрение и использование	-	Выведение из строя системы хранения данных. Распространение вредоносного ПО. Атака на основе использования нарушителем неудалённых установок по умолчанию. Автоматизированный подбор простого пароля пользователя. Атака на управление системой разграничения доступа хранилища больших данных.
	Класс 4. Снятие с эксплуатации	-	Атака на компьютер с целью чтения оставленной в памяти неудалённой конфиденциальной информации. Атака с прямым обращением к памяти вычислительного поля суперкомпьютера.

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
Тип 5. Используемые атакой уязвимости			Атака, использующая уязвимости в архитектуре. Атака, использующая уязвимости в реализации протоколов под конкретной ОС. Атака, использующая уязвимости в ОС. Атака, использующая уязвимости в приложениях. Атака, использующая уязвимости в сервисах. Атака, использующая недостаток знаний в области ИБ/СЗИ. Атака, использующая несоблюдение Политики ИБ работниками организации. Атака, использующая неправильную настройку СЗИ.
Тип 6. Условие начала атаки	Класс 1. Безусловная атака		Прослушивание. Фишинг. «Наводнение» канала связи.
	Класс 2. По запросу от жертвы		MitM-атака.
	Класс 3. По наступлению определенного события		Атака повторным воспроизведением пакета. Спуффинг.
Тип 7. Тип воздействия (характер) атаки	Класс 1. Активная		Атака, вызывающая явное изменение объекта атаки. Атака, оказывающая влияние на работу элементов ИТКС, например, DoS-атака на веб-сервер или телекоммуникационное оборудование. Подмена доверенного объекта. «Шторм» запросов. MitM-атака. Взлом парольной защиты.
	Класс 2. Пассивная		Прослушивание канала связи с целью получения идентификационной информации и определения используемых в сети протоколов. Перехват электронных почтовых сообщений.
Тип 8. Уровень реализации атаки по модели взаимодействия открытых систем ISO/OSI	Класс 1. Физический		Отмыкание замка. Размыкание канала связи. Модификация АО. Прослушивание канала.
	Класс 2. Канальный		MitM-атака. Модификация MAC-адреса. Прослушивание. «Отравление» ARP-кэша (англ. <i>ARP cache poisoning</i>). Деаутентификация клиентов беспроводных сетей. Нехватка DHCP (англ. <i>DHCP starvation</i>).
	Класс 3. Сетевой		Атаки на DHCP. Атаки Wormhole and Blackhole. Подмена, или спуффинг (англ. <i>spoofing</i>). «Наводнение» ICMP (англ. <i>ICMP flooding</i>). «Отравление» кэша маршрута (англ. <i>Route cache poisoning</i>).
	Класс 4. Транспортный		Подмена. Атака Smurf. Перехват сессий. Сканирование TCP-портов. Разведка хостов на основе TCP (англ. <i>TCP host sweeps</i>). «Наводнение» UDP (англ. <i>UDP flooding</i>).

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
	Класс 5. Сессионный, представительный и прикладной		Прослушивание. Вирусы. <i>MitM</i> -атака. Отказ от действий. Переполнение буфера (англ. <i>buffer overflow</i>). <i>DDoS</i> -атака на Telnet.
	Класс 6. Комбинированный		<i>DDoS</i> -атака. Наводнение <i>SYN</i> -флагами (англ. <i>SYN flooding</i>). Атака «заклинивания» (англ. <i>jamming</i>) в беспроводных сетях.
Тип 9. Виды нарушений, вызванных атакой – последствия / масштаб реализации атаки	Класс 1. Нарушение свойств ИБ	Подкласс 1. Нарушение конфиденциальности / приватности	Хищение (копирование) информации и средств ее обработки. Выполнение пользователем команд ОС с целью копирования файлов. Чтение информации, передаваемой в незашифрованном виде. Утечка информации при генерировании ПО сообщения об ошибке. Получение сведений о владельце беспроводного устройства.
		Подкласс 2. Нарушение целостности	Модификация (искажение) информации. Внедрение интерпретируемых операторов языков программирования или разметки в исходный код веб-приложения. Внедрение произвольного кода в ПО. Нарушение целостности резервной копии. Внедрение агента управления, выполняющего несанкционированные действия.
		Подкласс 3. Нарушение доступности	Блокирование данных. Уничтожение данных и средств их обработки. Записи данных за пределами выделенного в памяти буфера, что может вызывать аварийное завершение или зависание ПО. Удаление файлов за счет выполнения пользователем команд ОС. Искривление сообщения, вызывающая переполнение буфера. Длительный простой оборудования.
		Подкласс 4. Нарушение подлинности	Отказ от авторства электронного документа. Обход процедуры проверки подлинности. НСД к защищаемой информации из-за ошибки подтверждения подлинности сертификата. Подмена доверенного пользователя/объекта в сети.
		Подкласс 5. Нарушение подотчетности	Неполная запись событий в ЖРС. Стирание информации в ЖРС. Формирование ложных утверждений о полученных/переданных платежных документах.
		Подкласс 6. Нарушение неотказуемости	Отказ пользователя от факта выполнения им транзакции, от отправления или получения сообщения.
		Подкласс 7. Нарушение достоверности	Изменение пути исполнения программы из-за ошибки в форматной строке. «Маскарад» (попытка злоумышленника выдать свой внедренный ложный объект за легальный маршрутизатор, сервер, рабочую станцию. Навязывание ложной информации.

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
	Класс 2. Нарушение физической целостности, физический ущерб		Физический НСД неавторизованных лиц в контролируемую зону расположения технических средств и(или) информационных активов. Уничтожение ПО. Уничтожение резервной копии. Разрушение оборудования и носителей информации. Снижение производительности устройства. Отказ или неисправная работа телекоммуникационного оборудования. Кража носителей или документов. Преступное использование аппаратных средств. Кража оборудования.
	Класс 3. Нарушение логической структуры		Нарушение непрерывности процессов. Несанкционированный логический доступ неавторизованных субъектов к элементам ИТКС и информационным активам. Искажение структуры данных.
	Класс 4. Утрата, кража и ухудшение качества предоставляемых информационных услуг		Снижение качества предоставляемых информационных услуг. Утрата информационных сервисов. Обман поставщика услуг. Избыточное дублирование/распространение информации, делающая возможным кражу услуг. Нарушение функционирования ПО. Нарушение предоставления услуги посредством досрочного завершения сеанса связи. Нарушение сопровождения ИС. Незаконная обработка данных.
	Класс 5. Нарушение функций и прав / полномочий, включая права собственности / владения		Присвоение чужого права. Фальсификация прав. Злоупотребление правами. Отказ от осуществления действий. Несанкционированное использование административной информации по аутентификации (идентификатор пользователя/пароль). Использование нелегального ПО. «Маскарад» с представлением чужого пароля, ключа или сертификата (например, системного администратора). Представление ложных полномочий, будто бы они верные, с намерением ввести в заблуждение. Несанкционированное управление пользователями для предоставления услуги, повышая/понижая привилегии.
Тип 10. Серьезность ущерба (тяжесть последствий) от атаки для деятельности	Класс 1. Минимальная		Разведка или сбор информации – атака, в результате которой были просканированы открытые порты на сервере без дальнейших действий со стороны атакующего.
	Класс 2. Средняя		Атака, в результате которой атакующий получил доступ к отдельной рабочей станции работника отдела кадров.
	Класс 3. Высокая		Атака, в результате которой атакующий получил возможность управления сервером баз данных с платежной информацией.
	Класс 4. Критичная		Атака, вызвавшая простой ИТКС в течении 4 часов и последующую потерю клиентов.

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
Тип 11. Вид атакующего	Класс 1. Внешний		Представитель аутсорсинговой компании. Компьютерный преступник. Шпион.
	Класс 2. Внутренний		Пользователь ИС. Администратор ИС. Администратор безопасности ИС. Разработчик ПО. Руководитель ИТ-подразделения.
	Класс 3. Комбинированный		Внешний атакующий, действующий в сговоре с администратором ИС.
Тип 12. Число жертв и атакующих	Класс 1. Традиционная атака		Один атакующий – одна или много жертв.
	Класс 2. Распределенная атака		Много атакующих – одна или много жертв.
Тип 13. Наличие обратной связи атакующего с жертвой	Класс 1. Без обратной связи		Прослушивание. <i>DoS</i> -атака. Ввод неожиданных значений. Манипулирование временем и состоянием. Сбор и анализ информации.
	Класс 2. С обратной связью		<i>MitM</i> -атака. Спуффинг. «Шторм» запросов. Вмешательство в процесс контроля доступа. <i>APT</i> -атака.
Тип 14. Метод реализации атаки			Разведка. Сканирование и зондирование. Маскарад. Прослушивание. Подмена доверенного объекта. Внедрение ложного объекта. <i>DoS</i> -атака. Использование скрытых каналов для утечки информации. «Шторм» запросов. Расширение прав доступа после взлома ИС. <i>MitM</i> -атака. <i>APT</i> -атака. Метод «грубой силы» (англ. <i>brute force</i>) при подборе пароля. Подделка. Неправильное использование/ незаконная деятельность. Модификация. Копирование. Удаление. Фишинг. Обход защиты. Эскалация привилегий. Эксфильтрация. Манипулирование структурами данных. Манипулирование системными ресурсами.
Тип 15. Средства реализации атаки			Информационный обмен. Команды пользователя. ПО (включая скрипты). Наборы хакерских средств (<i>toolkits/rootkits</i>). Сетевые вирусы. Сетевые черви. Бактерии. Социальная инженерия. Анонимный прокси-сервер. Вложение в электронной почте. Логическая бомба.
Тип. 16. Завершенность атаки			Свершившаяся, в процессе выполнения, попытка выполнения, подозрение на атаку.

Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы (окончание)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры сетевых атак</i>
Тип 17. Вероятность реализации атаки	Класс 1. Высоковероятная	-	Атака реализуется очень часто, например, сканирование с целью определения открытых портов.
	Класс 2. Возможная		Атака реализуется часто, например, DoS-атака на веб-сервер.
	Класс 3. Маловероятная	-	Атака реализуется редко, например, разрушение сервера при физическом воздействии на него нарушителя ИБ.
Тип 18. Вероятность повторения атаки	Класс 1. Низкая		Атака реализуется редко, например, разрушение сервера при физическом воздействии на него нарушителя ИБ, и вероятность ее повторения – низкая.
	Класс 2. Средняя		Атака реализуется часто, например, DoS-атака на веб-сервер, и вероятность ее повторения – средняя.
	Класс 3. Высокая		Атака реализуется очень часто, например, сканирование с целью определения открытых портов, и вероятность ее повторения – высокая.
Тип 19. Сложность обнаружения атаки	Класс 1. Низкая		Атакующий запускает программу взлома, компилирует легкодоступный код или применяет широко известный метод атаки, практически не внося ничего нового в свое поведение.
	Класс 2. Средняя		Атакующий использует широко известный метод нападения, но начиная атаку, он незначительно модифицирует стандартную тактику проведения атаки.
	Класс 3. Высокая		Атакующий умен (как правило, пишет собственный код), опытен, его атака может долго оставаться незамеченной.
	Класс 4. Очень высокая		Атакующий очень опытен, использует либо неизвестные разработки, либо самые современные технологии, применяет в основном нестандартные методы и, хорошо заматывая следы, часто оставляет скрытые входы для повторного проникновения в систему.

Понимание актуальных для ИТКС ОРГАНИЗАЦИИ сетевых атак необходимо для определения характерных сопровождающих их событий ИБ, которые по отдельности или в некоторой последовательности будут признаны ОРГАНИЗАЦИЕЙ инцидентами ИБ.

Представленная системная классификация не претендует на полноту, поскольку новые сетевые атаки возникают почти каждый день. Она может быть использована в качестве основы для расширения в будущем.

Более наглядно и компактно все типы возможных сетевых атак на ИТКС ОРГАНИЗАЦИИ и ее отдельные элементы изображены на рис. 16.

Как и две предыдущие системные классификации, классификация сетевых атак необходима для заполнения соответствующих позиций в Модели угроз ИБ и Модели и нарушителей ИБ, а именно касающихся методов и средств реализации угроз ИБ ИТКС ОРГАНИЗАЦИИ в виде конкретных сетевых атак.

2.5. Системная классификация инцидентов информационной безопасности для - информационно-телекоммуникационной сети

Даже самые современные технологии и передовые СЗИ следующего поколения не могут полностью предотвратить возникновение в ИТКС ОРГАНИЗАЦИИ событий, связанных с ИБ (событий ИБ). После того, как все необходимые меры обеспечения ИБ будут внедрены, с большой вероятностью останутся неустраненные уязвимости, некорректно установленные настройки оборудования и ПО, ошибки персонала и несоблюдение Политики ИБ. Эти обстоятельства могут способствовать развитию инцидентов ИБ.

Различные инциденты ИБ имеют свои специфические сценарии развития, поэтому их можно охарактеризовать совершенно по-разному. Но не эффективно разрабатывать отдельное описание для каждого инцидента, поскольку их количество постоянно растет. Именно поэтому известными компаниями был разработан ряд спецификаций для унификации таких описаний, представленных ниже в соответствии с годом их публикации для общественности [160].



Рисунок 16 – Системная классификация сетевых атак на ИТКС ОРГАНИЗАЦИИ и ее элементы

2007 г. – Описание объекта и формат обмена информацией об инцидентах (англ. *Incident Object Description and Exchange Format, IODEF*) рабочей группы «Управляемый упрощенный обмен информацией об инцидентах» (англ. *Managed Incident Lightweight Exchange, MILE*) [<https://datatracker.ietf.org/wg/mile/about/>]. Это основанный на XML стандарт, используемый для обмена информацией об инцидентах между Группами реагирования на инциденты компьютерной безопасности (англ. *Computer Security Incident Response Teams, CSIRT*) и применяемый в качестве формата хранения в Системе коллективных знаний (англ. *Collective Intelligence Framework, CIF*). IODEF – это формат данных и расширения для представления данных об инцидентах и индикаторах. Позднее IODEF был опубликован как стандарт RFC5070 Инженерного совета интернета (англ. *Internet Engineering Task Force, IETF*). В 2017 г. рабочая группа MILE подготовила несколько новых документов об обновлении RFC5070, представлении структурированной информации о кибербезопасности в IODEF и т.п.

2007 г. – Формат обмена сообщениями об обнаружении вторжения (англ. *Intrusion Detection Message Exchange Format, IDMEF*), подготовленный IETF (RFC 4765) [<https://www.ietf.org/rfc/rfc4765.txt>]. Он должен был стать стандартным форматом данных COB, предназначенным для оповещения о событиях, которые они рассматривают как подозрительные. Модель данных IDMEF – это объектно-ориентированное представление данных оповещения об опасности, отправляемого анализаторами обнаружения вторжений администраторам.

2009 г. – Система коллективных знаний (CIF), разработанная Центром обмена и анализа информации исследовательской и образовательной сети (англ. *Research and Education Network Information Sharing and Analysis Center, REN-ISAC*) [<http://csirtgadgets.org/>]. Это клиент-серверная система обмена данными об угрозах (например, IP-адресах, номерах автономных систем в интернете, адресах электронной почты, доменных именах, URL-адресах, типах угроз, серьезности атак и достоверности данных). Внутри CIF данные хранятся в формате IODEF. CIF способна экспортировать данные в определенные СЗИ, например Snort или iptables.

2010 г. – Словарь для регистрации событий и обмена информацией об инцидентах (англ. *Vocabulary for Event Recording and Incident Sharing, VERIS*) от компании Verizon [<http://veriscommunity.net/>]. Это система, созданная для определения и обмена стратегической (не тактической) информацией и общим представлением об инцидентах. Она содержит набор метрик, предназначенный для поддержки общего языка описания инцидентов безопасности в структурированном и воспроизводимом виде. VERIS разделена на пять разделов: отслеживание инцидентов, демография жертв, описание инцидентов, обнаружение и реагирование, а также оценка воздействия.

2011 г. – Открытые индикаторы компрометации (англ. *Open Indicators of Compromise, OpenIOC*) от компании Mandiant [<http://www.openioc.org/>]. Это расширяемая среда с открытым

исходным кодом для обмена информацией об угрозах ИБ в виде *XML*-схем для описания технических характеристик, которые идентифицируют известные угрозы, методы злоумышленников и другие доказательства компрометации. Первоначально *OpenIOC* был разработан для того, чтобы в продуктах *Mandiant* можно было систематизировать информацию для быстрого поиска потенциальных нарушений ИБ. Позже *Mandiant* стандартизировала открытый исходный код схемы *OpenIOC* и теперь выпускает инструменты и утилиты, позволяющие быстро передавать информацию об угрозах. *OpenIOC* поставляется с базовым набором индикаторов, описывающих более 500 различных сред, которые можно использовать для отслеживания злоумышленников.

2012 г. – Межсетевая защита в реальном времени (англ. *Real-time Internetwork Defense, RID*) рабочей группы *MILE* [<https://datatracker.ietf.org/wg/mile/about/>]. Это стандарт передачи информации о киберугрозах, облегчающий обмен данными по обработке инцидентов и интегрирующий все этапы процесса управления инцидентами – обнаружение, отслеживание, идентификацию источника и смягчение последствий. *RID* определяет протокол, упрощающий совместное использование информации об инцидентах безопасности для компьютеров и сетей. *RID* определен в RFC 6545, а *RID-over-HTTPS* – в RFC 6546.

2012 г. – Открытый обмен информацией об угрозах (англ. *Open Threat Exchange, OTX*) от компании *Alien Vault* [<https://www.alienvault.com/open-threat-exchange>]. Это общедоступная централизованная система обмена данными об угрозах. Она взаимодействует с *SIEM*-системой с открытым исходным кодом (англ. *Open Source SIEM, OSSIM*). *OTX* также доступен в *CIF*.

2013 г. – Описание объекта и формат обмена структурированной информацией о кибербезопасности (*IODEF-SCI*) [<https://datatracker.ietf.org/doc/rfc7203/>]. Оно является расширением стандарта *IODEF* (в виде RFC 7203), в который добавлена поддержка таких дополнительных данных как схема атаки, информация о платформе, уязвимость, инструкция по противодействию, ЖРС, серьезность и т.д. Описание повышает приспособленность такой информации к машинной обработке (машиночитаемость), предоставляя возможность встраивать идентификаторы и *XML*-данные информации о кибербезопасности, например, из *CVE* и используя открытый язык уязвимостей и оценки (англ. *Open Vulnerability and Assessment Language, OVAL*). Также могут использоваться следующие стандарты: *CAPEC*, Общее описание событий (англ. *Common Event Expression, CEE*), Общее перечисление платформ (англ. *Common Platform Enumeration, CPE*), Общий формат отчетов об уязвимостях (англ. *Common Vulnerability Reporting Format, CVRF*), Общая система оценки уязвимостей (англ. *Common Vulnerability Scoring System, CVSS*), Открытый интерактивный язык контрольных списков (англ. *Open Checklist Interactive Language, OCIL*), Расширяемый формат описания контрольных списков конфигураций (англ. *Extensible Configuration Checklist Description Format, XCCDF*), Распределенная служба аудита (англ. *Dis-*

tributed Audit Service, XDAS) и ряд других.

2013 г. – Представление наблюдений в киберпространстве (англ. *Cyber Observable eXpression, CybOX*) от компании *MITRE* [<https://cybox.mitre.org/about/>]. Это схема для определения, сбора, описания и передачи информации о событиях или свойствах состояний (например, хэш-значения файлов, *IP*-адреса, команда *HTTP GET*, ключи реестра), которые можно наблюдать в работающем домене из 70 объектов (например, файл, *HTTP*-сессия, сетевой поток, сетевое соединение, сертификат *X.509*). Это и стандартизированный язык кодирования и передачи информации о наблюдениях для динамических событий или измерений состояний (типа оценки и характеристик угроз (подробные схемы атак), характеристики вредоносных программ, управления событиями), ведения ЖРС, реагирования на инциденты, совместного использования индикаторов, расследования компьютерных преступлений).

2013 г. – Структурированное представление информации об угрозе (англ. *Structured Threat Information Expression, STIX*) от компании *MITRE* [<https://oasis-open.github.io/cti-documentation/stix/about.html>]. Это язык, который использует *CybOX* для описания информации об угрозах в стандартизированном и структурированном виде и позволяет осуществлять обмен знаниями об угрозах (англ. *Cyber Threat Intelligence, CTI*), например, цель, инцидент, индикатор, источник угрозы. Он был разработан для анализа киберугроз, определения индикаторов схем реализации, управления действиями по реагированию и обмена информацией об угрозах. В 2017 г. появилась вторая версия – *STIX 2.0*, которая расширяет *CTI* за счет включения индикаторов активности противника и контекстную информацию о мотивации, возможностях и действиях противника, а также наилучшие действия для защиты и смягчения последствий атак. *STIX 2.0* основан на модели *MITRE ATT&CK*. Структура *STIX 2.0* не зависит от какого-либо конкретного транспортного протокола.

2013 г. – Доверенный автоматизированный обмен информацией об индикаторах (англ. *Trusted Automated eXchange of Indicator Information, TAXII*) от *MITRE* [<https://oasis-open.github.io/cti-documentation/>]. Это набор услуг по обмену сообщениями, обеспечивающий совместное использование информации об угрозах между организациями и производителями продуктов или услуг с использованием *XML* и *HTTP* для содержимого и транспорта сообщений соответственно, а также поддерживающий форматы и протоколы пользователей. Он работает для нескольких моделей совместного использования (например, «точка-точка») и метода «толкать или тянуть» (англ. *Push or pull*). Это и протокол прикладного уровня для передачи информации о киберугрозах простым и масштабируемым способом, который используется для обмена *CTI* по *HTTPS*. *TAXII* был разработан специально для транспортировки объектов *STIX 2.0*.

Последние три спецификации – *CybOX*, *STIX 2.0* и *TAXII* – в настоящее время используются чаще всего, поскольку они совместимы, машиночитаемы и легко автоматизируются.

При составлении классификации инцидентов ИБ, кроме выше указанных источников, использовались многочисленные обзоры иностранных и российских исследовательских и консалтинговых компаний, а также следующие стандарты:

— ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» [161];

— ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» [162];

— ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» – Приложение Б. Перечень нарушений защиты информации [144];

— Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» [163];

— Стандарт Банка России СТО БР ИББС-1.3-2016 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств» [164];

— Государственный стандарт Республики Узбекистан «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами (ISO/IEC 27035-1:2016, MOD) [165];

— Государственный стандарт Республики Узбекистан «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2 Руководящие указания по планированию и подготовке к реагированию на инциденты (ISO/IEC 27035-2:2016, MOD) [166];

— ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management (Управление инцидентами ИБ — Часть 1. Принципы управления инцидентами) [68];

— ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response (Часть 2. Руководящие принципы планирования и подготовки для реагирования на инциденты) [127];

— CMU/SEI-2004-TR-015 Defining incident management processes for CISRT: A Work in Progress. Technical Report. 2004 [167];

— NIST Special Publication 800-61. Revision 2. 2012. Computer Security Incident Handling

Guide (Руководство по обработке инцидентов компьютерной безопасности) [131];

— Проект ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации» [16].

В подразделе 2.1 были процитированы определения события и инцидента ИБ. Сделаем к ним ряд важных дополнений. Для того чтобы событие ИБ имело место, необходимо, чтобы субъектом было совершено какое-то действие, направленное на какой-либо объект. В определении события ИБ не делается различия между авторизованными и неавторизованными действиями нарушителя ИБ. Обнаруживаемые события ИБ могут быть частью инцидента ИБ или просто иметь отношение к ИБ, без каких либо негативных последствий. Например, если пользователь верно вводит регистрационное имя и пароль, тогда ему дается доступ к его учетной записи – и это событие ИБ, поскольку оно связано с ИБ. Но может оказаться, что была осуществлена подмена пользователя – «маскарад», и тогда это уже инцидент ИБ. Часто наблюдаемое событие ИБ является лишь частью шагов, предпринимаемых злоумышленником для получения какого-то несанкционированного Политикой ИБ ОРГАНИЗАЦИИ результата. Такие события ИБ можно рассматривать как часть инцидента ИБ, а сам инцидент ИБ будет состоять из совокупности событий ИБ [168].

Единого универсального перечня инцидентов ИБ, характерных для любых организаций, существовать не может. Причина заключается в том, что каждая организации в соответствии со своей Политикой ИБ самостоятельно признает инцидентами ИБ определенные события или совокупность событий ИБ. Например, для обычной компании обнаружение компьютерного вируса в ее сети будет событием ИБ, а для компании, которая разрабатывает САВЗ – это замечательная возможность пополнить свою энциклопедию вирусов новым экземпляром, добавив его сигнатуру в следующую версию своего продукта. Событие же обнаружения *DoS*-атаки на веб-сервер для любой компании будет практически всегда являться инцидентом ИБ, требующим немедленного реагирования, поскольку невозможность узнать о ее деятельности может вызвать отток потенциальных клиентов.

Учитывая имеющийся опыт рассмотрения инцидентов ИБ в первоисточниках, были сформулированы пять важных требований к разрабатываемой классификации инцидентов ИБ:

1) в классификации должна содержаться информация об инцидентах ИБ, которые характерны как для самой ИТКС ОРГАНИЗАЦИИ, так и ЦИУСБ как ее важнейшей части и системообразующего элемента СОИБ ОРГАНИЗАЦИИ;

2) в классификации должна содержаться информация об этапе жизненного цикла объекта, на котором возникает инцидент ИБ;

3) в классификации должна содержаться информация о направленности инцидента ИБ на различные элементы ИТКС;

4) на одном уровне классификации не должны располагаться понятия разной степени абстракции, описывающие достаточно широкий отвлеченный класс проблем или какой-либо редкий частный случай;

5) в классификации необходимо связать инциденты ИБ с угрозами ИБ и сетевыми атаками, которые могут использоваться для их реализации, и соответствующими уязвимостями.

Обобщенные результаты разработки классификационных признаков для типов инцидентов ИБ ИТКС ОРГАНИЗАЦИИ, полученные на основе анализа выше перечисленных документов и работ автора данного исследования [45, 46, 48, 55, 132, 134-141, 160, 168], сведены в табл.

5. Основными классификационными признаками инцидентов ИБ являются следующие:

— выполняющие последнее требование и полностью совпадающие с описанием сетевых атак (типы 1-19), но с заменой соответствующих понятий на более близкие к инцидентам ИБ, а именно: расположение нарушителя ИБ, цель нарушителя ИБ, место происшествия и направленность инцидента ИБ (затронутые элементы ИТКС, включая ЦИУСБ), стадия жизненного цикла элемента ИТКС, на которой проявился инцидент ИБ, причины развития инцидента ИБ (используемые уязвимости), условие развития инцидента ИБ, тип воздействия (характер) инцидента ИБ, уровень реализации инцидента ИБ в соответствии с семиуровневой моделью *OSI/ISO*, виды нарушений, вызванных инцидентом ИБ – последствия/масштаб инцидента ИБ, серьезность ущерба от инцидента ИБ для деятельности организации, вид нарушителя ИБ, число нарушителей ИБ, наличие обратной связи с нарушителем ИБ, метод и средства реализации инцидента ИБ, а также вероятность реализации инцидента ИБ, вероятность его повторного возникновения в будущем и сложность обнаружения инцидента ИБ. С целью сокращения результирующей табл. 5 эти признаки указаны только названием типа. В случае необходимости конкретизации по сравнению с описанием сетевой атаки в соответствующую строку внесены изменения;

— дополнительные: источник информации об инциденте ИБ, его статус, преднамеренность возникновения инцидента ИБ, характер действий нарушителя ИБ, негативные последствия инцидента ИБ, область распространения, приоритет при обработке инцидента ИБ (срочность реагирования), сложность реагирования на инцидент ИБ (ликвидации последствий) и сложность закрытия инцидента ИБ.

В целях выявления и оценки инцидентов ИБ дополнительно для каждого из классов можно еще определить и подклассы (при необходимости), например, как в случае с выделением в подклассы отдельных элементов ИТКС, для которых так нагляднее ввести еще один уровень систематизации, детализирующий описание инцидента ИБ.

Таблица 5 – Системная классификация инцидентов ИБ ИТКС (начало)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры инцидентов ИБ</i>
Тип 1. Расположение нарушителя ИБ – как для сетевой атаки			
Тип 2. Цель нарушителя ИБ – как для сетевой атаки			
Тип 3. Место происшествия и направленность (затронутые элементы ИТКС) инцидента ИБ – как для сетевой атаки			
Тип 4. Стадия жизненного цикла элемента ИТКС, на которой проявился инцидент ИБ – как для сетевой атаки			
Тип 5. Причины развития инцидента ИБ (используемые уязвимости) – как для сетевой атаки			
Тип 6. Условие развития инцидента ИБ – как для сетевой атаки			
Тип 7. Тип воздействия (характер) инцидента ИБ – как для сетевой атаки			
Тип 8. Уровень реализации инцидента ИБ в соответствии с моделью ISO/OSI – как для сетевой атаки			
Тип 9. Виды нарушений, вызванных с инцидентом ИБ – последствия / масштаб инцидента ИБ – как для сетевой атаки			
Тип 10. Серьезность ущерба (тяжесть последствий) от инцидента ИБ для деятельности – как для сетевой атаки			
Тип 11. Вид нарушителя ИБ – как для сетевой атаки			
Тип 12. Число нарушителей ИБ – как для сетевой атаки			
Тип 13. Наличие обратной связи с нарушителем ИБ – как для сетевой атаки			
Тип 14. Метод реализации инцидента ИБ – как для сетевой атаки			
Тип 15. Средства реализации инцидента ИБ – как для сетевой атаки			
Тип 16. Завершенность инцидента ИБ – как для сетевой атаки			
Тип 17. Вероятность реализации инцидента ИБ – как для сетевой атаки			
Тип 18. Вероятность повторного возникновения инцидента ИБ – как для сетевой атаки			
Тип 19. Сложность обнаружения инцидента ИБ – как для сетевой атаки			
Тип 20. Источник информации об инциденте ИБ	Класс 1. Работник организации		Обнаружение администратором ИС действий и (или) операций по созданию, удалению, копированию ресурсов доступа. Обнаружение администратором ИС действий и (или) операций по изменению (предоставлению) прав логического доступа.
	Класс 2. Техническое средство		Обнаружение типичных признаков сетевой атаки в ЖРС ОС. Обнаружение типичных признаков сетевой атаки в ЖРС СУБД. Обнаружение изменения топологии сети.
Тип 21. Статус инцидента ИБ			Инцидент ИБ зарегистрирован, назначен, в обработке, закрыт.

Таблица 5 – Системная классификация инцидентов ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры инцидентов ИБ</i>
Тип 22. Преднамеренность возникновения инцидента ИБ	Класс 1. Случайный или ошибочный		Обнаружение случайного заражения компьютера вирусом при использовании учебного пакета. Обнаружение ненамеренного повреждения аппаратуры в результате случайных действий безответственных лиц, например обрыв соединительного кабеля.
	Класс 2. Намеренный		Обнаружение сканирования ИТКС с целью выявления уязвимостей в защите информации. Обнаружение смены аутентификационных данных, используемых для доступа к сетевому оборудованию. Обнаружение внесения изменений в БД, отдельные файлы для подделки информации.
Тип 23. Характер действий нарушителя ИБ	Класс 1. Действия по сети, без доступа к элементам ИТКС		Обнаружение действий при осуществлении логического доступа. Обнаружение операций по изменению состава ПО АРМ эксплуатационного персонала, запускаемого автоматически при загрузке ОС. Обнаружение внешних воздействий из интернета на ПО уровня ОС.
	Класс 2. Действия с единичными проникновениями в помещения, где находятся элементы ИТКС	Подкласс 1. Открытые	Обнаружение нарушений и сбоев в работе технических СЗИ в результате физического воздействия на них сотрудников коммунальных служб. Обнаружение изменения климатических режимов помещений, в которых расположены СВТ, телекоммуникационное оборудование.
		Подкласс 2. Негласные	Обнаружение нарушений и сбоев в работе технических СЗИ в результате физического воздействия на них в выходные дни или ночью.
	Класс 3. Действия со стороны поставщиков оборудования, постоянно работающих в помещениях, и обслуживающего персонала		Обнаружение нарушений и сбоев в установлении (обновлении) системного ПО и параметров его настроек, влияющих на обеспечение ИБ, произведенных поставщиками средств. Обнаружение нарушений и сбоев в установлении (обновлении) ПО и параметров настроек технических СЗИ, их сигнатурных баз (в случае их использования) поставщикам средств. Обнаружение действий по использованию подконтрольных мобильных устройств. Обнаружение фотосъемки.
Тип 24. Негативные последствия инцидента ИБ	Класс 1. Мгновенные		Обнаружение мгновенного отказа в работе телекоммуникационного оборудования. Обнаружение нарушения процессов управления ИТКС.
	Класс 2. Накапливающиеся		Обнаружение отказа оборудования в результате исчерпания его ресурса. Обнаружение ликвидаторов замедленного действия с целью уничтожения информации или оборудования.

Таблица 5 – Системная классификация инцидентов ИБ ИТКС (продолжение)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры инцидентов ИБ</i>
Тип 25. Область распространения инцидента ИБ	Класс 1. Пределы одного элемента ИТКС		Обнаружение нарушения целостности ПО ИС на АРМ пользователей. Обнаружение действий и (или) операций по запуску программных процессов. Обнаружение нарушений доверенной загрузки ОС АРМ пользователей и эксплуатационного персонала.
	Класс 2. Пределы нескольких элементов ИТКС		Обнаружение действия и (или) операций при осуществлении доступа к серверным компонентам виртуализации несколькими виртуальными машинами, логическими разделами или томами.
	Класс 3. Пределы отдельного структурного подразделения		Обнаружение действий и (или) операций при администрировании системы хранения данных. Обнаружение действий и (или) операций по использованию разблокированных коммуникационных портов на веб-сервере подразделения. Обнаружение аномальной сетевой активности.
	Класс 4. Организация в целом		Обнаружение действий и (или) операций по подключению СВТ к ИТКС ОРГАНИЗАЦИИ. Обнаружение нарушений целостности эталонных копий ПО при осуществлении их распространения и (или) обновления в пределах всей ОРГАНИЗАЦИИ. Обнаружение действий, приведших к порождению системных и бизнес-рисков. Обнаружение нетипичных (аномальных) запросов на уровне сетевых приложений и сервисов.
	Класс 5. Выходящий за пределы организации		Обнаружение действий и (или) операций по передаче информации с использованием электронной почты за пределы ОРГАНИЗАЦИИ. Обнаружение действий и (или) операций при осуществлении доступа к ресурсам интернета. Обнаружение действий, приведших к потере конкурентных преимуществ ОРГАНИЗАЦИИ. Обнаружение действий, приведших к нарушению правовых и нормативных требований.
Тип 26. Приоритет при обработке инцидента ИБ (срочность реагирования)			Например, в следующем диапазоне: 0 (наивысший), 1 (высокий), 2 (выше среднего), 3 (средний), 4 (низкий), 5 (минимальный).

Таблица 5 – Системная классификация инцидентов ИБ ИТКС (окончание)

<i>Тип</i>	<i>Класс</i>	<i>Подкласс</i>	<i>Некоторые примеры инцидентов ИБ</i>
Тип 27. Сложность реагирования на инцидент ИБ (ликвидации последствий)	Класс 1. Обычная		Обнаружение нарушения целостности ПО ИС на АРМ пользователей и эксплуатационного персонала. Обнаружение ошибочных действий малоквалифицированного персонала при профилактике, техническом обслуживании или ремонте оборудования. Обнаружение вредоносного кода и (или) мобильного кода. Обнаружение формирования ложных утверждений о полученных (переданных) документах.
	Класс 2. Высокая		Обнаружение действий и (или) операций по изменению состава ПО серверного оборудования. Обнаружение действий и (или) операций, направленных на изменение правил сегментации и межсетевого экранирования. Обнаружение действий и (или) операций по изменению параметров настроек технических СЗИ, параметров настроек системного ПО, влияющих на обеспечение ИБ.
Тип 28. Сложность закрытия инцидента ИБ	Класс 1. Обычная		Обнаружение действий и (или) операций по созданию, удалению, блокированию, разблокированию учетных записей. Обнаружение нарушений при доверенной загрузке виртуальных машин. Обнаружение операций со списками рассылки и адресными книгами.
	Класс 2. Высокая		Обнаружение действий со средствами криптографической защиты информации и ключевой информацией. Обнаружение операций по изменению состава ПО серверного оборудования на нескольких серверах одновременно. Обнаружение анализа сетевого трафика при пассивном подключении к каналу связи ИТКС. Обнаружение скрытой передачи конфиденциальной информации в составе легального сообщения для выявления паролей, ключей и протоколов доступа. Обнаружение негласной переработки оборудования или ПО на фирме-изготовителе, фирме-поставщике, в месте складирования или в пути следования к заказчику с целью внедрения средств НСД к информации извне (программ-перехватчиков, троянских программ), а также уничтожение информации или оборудования (например, с помощью ликвидаторов с дистанционным управлением или замедленного действия).

Как видно из табл. 5, в классификационных параметрах инцидентов ИБ не удалось избежать упоминания уязвимостей, источников угроз ИБ – нарушителей ИБ и методов и средств реализации конкретных сетевых атак, что в очередной раз подтверждает неразрывную связь всех этих понятий.

Представленная системная классификация не претендует на полноту, поскольку новые инциденты ИБ могут возникать практически каждый день. Но она может быть использована в качестве основы для расширения в будущем.

Более наглядно и компактно все типы возможных инцидентов ИБ ИТКС ОРГАНИЗАЦИИ и ее отдельные элементы изображены на рис. 17. Опять подчеркнем, что схожие с сетевыми атаками типы изображены в свернутом виде – без классов и подклассов.

Как и три предыдущие системные классификации, классификация инцидентов ИБ требуется для заполнения соответствующих позиций в Модели угроз ИБ и Модели нарушителей ИБ.

Кроме того, системная классификация инцидентов ИБ является основой для разработки Политики управления инцидентами ИБ и Плана реагирования на инциденты ИБ для ИТКС ОРГАНИЗАЦИИ.

Понимание инцидентов ИБ для ИТКС ОРГАНИЗАЦИИ необходимо для выбора адекватных мер обеспечения ИБ и разработки и внедрения всего процесса управления инцидентами ИБ для ОРГАНИЗАЦИИ, начиная с их обнаружения и заканчивая ликвидацией последствий, закрытием, извлечением уроков и недопущения повторного появления в будущем.

Выводы по главе 2

1. Для создания СОИБ ИТКС требовалось сформулировать смысловые и структурные элементы, описывающие среду построения типового ЦИУСБ ОРГАНИЗАЦИИ. Для этого решена задача разработки таксономии базовых взаимосвязанных понятий ИБ (уязвимость – угроза ИБ – сетевая атака – инцидент ИБ), которая необходима для упорядочивания знаний об информационной защищенности ИТКС ОРГАНИЗАЦИИ и описания внутреннего и внешнего контекста, в рамках которого необходимо обеспечить информационную защищенность передаваемых по ИТКС данных. Используя описанные в исследовании смысловые и структурные элементы, в Стратегии и Политике ИБ можно сформулировать требования по обеспечению ИБ, а также разработать Модели угроз ИБ и Модели нарушителей ИБ, которые актуальны и характерны именно для этой ОРГАНИЗАЦИИ.

2. Предлагаемая таксономия может быть использована любой организацией при написании внутренней документации для поддержки ее системы и процессов обеспечения ИБ как основа для дальнейшего расширения и уточнения. Написание адекватной Стратегии и Политик

ИБ, разработка системы и обоснованный выбор методов и средств обеспечения ИБ для ИТКС ОРГАНИЗАЦИИ напрямую зависит от полноты и качества разработанной таксономии и представленных классификаций.



Рисунок 17 – Системная классификация инцидентов ИБ ИТКС ОРГАНИЗАЦИИ

3. Разработана системная классификация уязвимостей элементов ИТКС ОРГАНИЗАЦИИ. Основными классификационными признаками типов уязвимостей являются следующие: место нахождения или проявления уязвимости, предпосылки появления уязвимости, источник происхождения уязвимости – стадия жизненного цикла, на которой возникла уязвимость, легкость обнаружения уязвимости, легкость устранения уязвимости, вероятность реализации угрозы ИБ на основе уязвимости, использующие уязвимость угрозы ИБ и уровень риска (критичность, серьезность, потенциальные последствия) в случае использования уязвимости. В целях оценки уязвимостей дополнительно для каждого из выделенных классов можно ввести подклассы (при необходимости), детализирующие описание уязвимости. Соотношение каждой уязвимости каждого информационного актива ИТКС ОРГАНИЗАЦИИ с каждым конкретным типом, а потом и классом и подклассом (при наличии) позволит наиболее полно охарактеризовать ее и понять ее природу. Это необходимо для того, чтобы в дальнейшем в процессе обеспечения ИБ ИТКС ОРГАНИЗАЦИИ для каждой выявленной уязвимости подобрать наиболее подходящую процедуру и средства устранения (и составить план устранения обнаруженных уязвимостей) и, что еще более важно, не допустить ее появления в будущем или, по крайней мере, существенно снизить вероятность этого появления.

4. Разработана системная классификация угроз ИБ элементов ИТКС ОРГАНИЗАЦИИ. Основными классификационными признаками типов угроз ИБ являются следующие: источник угрозы, расположение источника угрозы, цели реализации угрозы, направленность угрозы, стадии жизненного цикла, которые могут затронуть угрозы, используемые угрозой уязвимости, виды нарушения, вызванных угрозой ИБ (последствия/масштаб реализации угрозы), характер угрозы, предпосылки появления и природа происхождения угрозы, вероятность и метод реализации угрозы. В целях оценки угроз ИБ дополнительно для каждого из классов можно еще определить и подклассы (при необходимости), например, как в случае с выделением в подклассы отдельных элементов ИТКС, для которых так нагляднее ввести еще один уровень систематизации, детализирующий описание угрозы ИБ. Данная классификация необходима для определения актуальных для ИТКС ОРГАНИЗАЦИИ угроз ИБ с целью последующего выбора мер обеспечения ИБ, снижающих или устраняющих возможность их реализации злоумышленниками в виде компьютерных атак и инцидентов ИБ.

5. Разработанные системные классификации уязвимостей и угроз ИБ полностью согласованы между собой, что обеспечивает целостный взгляд на природу происхождения инцидентов ИБ для последующего понимания какие уязвимости устранять и каких последствий от их реализации ожидать. Они необходимы для построения Модели угроз ИБ и Модели нарушителей ИБ, составляющих основу разработки положений сначала Корпоративной Политики ИБ ОРГАНИЗАЦИИ, а затем частной Политики ИБ ИТКС и реестра рисков ИБ для выбора адек-

ватных мер обеспечения ИБ ИТКС ОРГАНИЗАЦИИ, который также строится на основе Модели угроз ИБ.

6. Разработана системная классификация сетевых атак на ИТКС ОРГАНИЗАЦИИ в целом и ее элементы. Основными классификационными признаками типов сетевых атак являются следующие: расположение атакующего, цели (мотивация) реализации атаки, направленность атаки, атаки относительно стадий жизненного цикла элементов ИТКС, используемые атакой уязвимости, условие начала атаки, тип воздействия (характер) атаки, уровень реализации в соответствии с семиуровневой моделью *OSI/ISO*, виды нарушений, вызванных компьютерной атакой – последствия/масштаб реализации атаки, серьезность ущерба от атаки для деятельности организации, вид атакующего, число жертв и атакующих, наличие обратной связи атакующего с жертвой, метод и средства реализации атаки, а также вероятность реализации атаки, вероятность ее повторения в будущем и сложность обнаружения атаки. В целях выявления и оценки сетевых атак дополнительно для каждого из введенных классов можно еще определить и подклассы (при необходимости), например, как в случае с выделением в подклассы отдельных элементов ИТКС, для которых так нагляднее ввести еще один уровень систематизации, детализирующий описание сетевой атаки. Понимание актуальных для ИТКС ОРГАНИЗАЦИИ сетевых атак необходимо для определения характерных сопровождающих их событий ИБ, которые по отдельности или в некоторой последовательности в дальнейшем будут признаны ОРГАНИЗАЦИЕЙ инцидентами ИБ.

7. Как и системные классификации уязвимостей и угроз ИБ, классификация сетевых атак необходима для заполнения соответствующих позиций в Модели угроз ИБ и Модели нарушителей ИБ, а именно касающихся методов и средств реализации угроз ИБ ИТКС ОРГАНИЗАЦИИ в виде конкретных сетевых атак.

8. Первые три классификации полностью готовы к разработке Модели угроз ИБ и Модели нарушителей ИБ. Эти модели описываются либо в отдельных документах или в документах высокого уровня (стратегии, концепции, политики ИБ) ОРГАНИЗАЦИИ.

9. Разработана системная классификация инцидентов ИБ ИТКС ОРГАНИЗАЦИИ. Основными классификационными признаками инцидентов ИБ являются следующие:

— выполняющие последнее требование и полностью совпадающие с описанием сетевых атак, но с заменой соответствующих понятий на более близкие к инцидентам ИБ, а именно: расположение нарушителя ИБ, цель нарушителя ИБ, место происшествия и направленность инцидента ИБ (затронутые элементы ИТКС, включая ЦИУСБ), стадия жизненного цикла элемента ИТКС, на которой проявился инцидент ИБ, причины развития инцидента ИБ (используемые уязвимости), условие развития инцидента ИБ, тип воздействия (характер) инцидента ИБ, уровень реализации инцидента ИБ в соответствии с семиуровневой моделью *OSI/ISO*, виды нару-

шений, вызванных инцидентом ИБ – последствия/масштаб инцидента ИБ, серьезность ущерба от инцидента ИБ для деятельности организации, вид нарушителя ИБ, число нарушителей ИБ, наличие обратной связи с нарушителем ИБ, метод и средства реализации инцидента ИБ, а также вероятность реализации инцидента ИБ, вероятность его повторного возникновения в будущем и сложность обнаружения инцидента ИБ. С целью сокращения результирующей табл. 6 эти признаки указаны только названием типа. В случае необходимости конкретизации по сравнению с описанием сетевой атаки в соответствующую строку внесены изменения;

— дополнительные: источник информации об инциденте ИБ, его статус, преднамеренность возникновения инцидента ИБ, характер действий нарушителя ИБ, негативные последствия инцидента ИБ, область распространения, приоритет при обработке инцидента ИБ (срочность реагирования), сложность реагирования на инцидент ИБ (ликвидации последствий) и сложность закрытия инцидента ИБ.

10. Системная классификация инцидентов ИБ является основой для разработки Политики управления инцидентами ИБ и Плана реагирования на инциденты ИБ для ИТКС ОРГАНИЗАЦИИ.

11. Представленные системные классификации не претендуют на полноту и могут быть расширения в будущем и, что еще важнее, строго адаптированы под специфику самой ИТКС ОРГАНИЗАЦИИ и ее нужды в отношении обеспечения сетевой безопасности.

12. Все разработанные системные классификации впервые представлены в открытых публикациях в едином стиле все вместе, что позволяет проследить их глубокие взаимосвязи.

13. Эти классификации детально описывают внешний и внутренний контекст осуществления деятельности ОРГАНИЗАЦИИ, что требуется как для создания адекватной ему СОИБ ИТКС, так и для формулирования наиболее полных и специфичных требований по обеспечению ИБ для ЦИУСБ ОРГАНИЗАЦИИ.

14. Представленная таксономия необходима для дальнейшей разработки в следующей главе процессов управления инцидентами ИБ, а именно «Обнаружение уязвимостей, событий ИБ и инцидентов ИБ» и «Анализ инцидентов ИБ» и взаимосвязанного с ними процесса мониторинга ИБ ИТКС ОРГАНИЗАЦИИ.

15. Таким образом, во второй главе разработана таксономия как систематизация и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей – базовых понятий ИБ, а именно «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», которая необходима для упорядочивания знаний об информационной защищенности ИТКС ОРГАНИЗАЦИИ, описания внутреннего и внешнего контекста осуществления деятельности, в рамках которого необходимо обеспечить информационную защищенность ИТКС, и для разработки документальной базы обеспечения ее ИБ в целом и ее элементов на всех стадиях их жиз-

ненного цикла. Она полностью готова для использования в типовом ЦИУСБ ОРГАНИЗАЦИИ в качестве типовой основы, которая может быть доработана (например, расширена и детализирована) под специфику конкретной ОРГАНИЗАЦИИ. Для использования разработанной таксономии в ней необходимо выделить только актуальные для конкретной ИТКС ОРГАНИЗАЦИИ уязвимости, угрозы ИБ, сетевые атаки и инциденты ИБ. После того, как размерность исходной информации будет снижена, для быстроты нахождения первоисточников ее рекомендуется дополнить ссылками на актуальные международные и национальные базы уязвимостей и проблем конфигураций (типа *CVE*, *NVD* и базы ФСТЭК России), классификации угроз ИБ и инцидентов ИБ. Таким образом абстрактная таксономия по результатам анализа используемого АО, ПО, ИС и других активов ИТКС ОРГАНИЗАЦИИ перестанет быть высоко формализованной и примет вид полезного инструмента, пригодного к использованию в конкретном ЦИУСБ ОРГАНИЗАЦИИ.

ГЛАВА 3. ИССЛЕДОВАНИЕ И РАЗРАБОТКА ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И СЕТЕВОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В главе для ИТКС ОРГАНИЗАЦИИ как основного объекта защиты в ЕИП ОРГАНИЗАЦИИ определяются понятия «процесс», «результативность процесса», «эффективность процесса», «обеспечение ИБ», «информационная защищенность», «СОИБ», «управление ИБ», «система управления ИБ», «мониторинг ИБ» и другие. На этой основе детально описываются процессы обеспечения и управления ИБ, показывается их взаимная связь и даются определения обеспечения и управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ. Приводится анализ эволюции основных подходов к управлению сетевой безопасностью. Перечисляются основные процессы проверки ИБ с особым вниманием к процессу мониторинга ИБ ИТКС ОРГАНИЗАЦИИ как основы выявления событий, связанных с ее ИБ, в рамках функционирования ЦИУСБ ОРГАНИЗАЦИИ. Подробно разрабатывается являющийся основой деятельности ЦИУСБ ОРГАНИЗАЦИИ процесс управления инцидентами ИБ (ПУИИБ) для ИТКС с детальным представлением карт его процессов и их описанием. В заключении раздела показывается место разрабатываемого ЦИУСБ среди систем обеспечения и управления ИБ ОРГАНИЗАЦИИ в качестве фундамента системы управления инцидентами ИБ ИТКС.

3.1. Понятие обеспечения информационной безопасности информационно-телекоммуникационной сети

Для противодействия угрозам ИБ, оперативного реагирования на события и инциденты ИБ и снижения рисков ИБ необходимо обеспечивать и на протяжении длительного времени сохранять достаточный для ОРГАНИЗАЦИИ уровень ИБ ее ИТКС. Поэтому в эпоху цифровой экономики обеспечение ИБ как процесс поддержания состояния защищенности информационных активов ИТКС ОРГАНИЗАЦИИ является одним из основополагающих аспектов успешного осуществления деятельности в условиях жесткой конкурентной борьбы и экономических трудностей.

3.1.1. Понятие процесса и процессного подхода к деятельности организации

В первую очередь необходимо ввести базовое понятие процесса (от лат. *processus* – продвижение). Опираясь на ГОСТ Р ИСО 9000-2015 [169] и проведенный анализ, определим про-

цесс как совокупность упорядоченных во времени логически связанных, взаимодействующих и завершенных видов деятельности, направленная на достижение поставленных целей, преобразующая входы в выходы и требующая для этого определенных ресурсов и управляющих воздействий (управления) (рис. 18). Любой процесс имеет заинтересованные стороны – потребителя, внутреннего или внешнего, и осуществляется в соответствии с установленными целями.

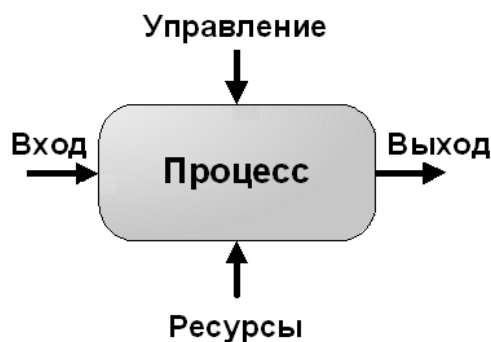


Рисунок 18 – Иллюстрация понятия «процесс»

Входами одного процесса обычно являются выходы других процессов. Входами могут быть специфические требования, включая ресурсы – подмножество активов организации, используемых или потребляемых в процессе выполнения некоторой деятельности. На выходе получают в той или иной степени удовлетворенные требования и непосредственный результат процесса. Входы и выходы процесса могут быть осязаемыми (оборудование, материалы, продукция, информация на различных носителях и т.п.) и неосязаемыми (специфицированные требования, услуга и т.п.).

В [169] содержится ряд требований к реализации процессного подхода, основными из которых являются следующие:

- 1) определение процессов, необходимых для реализации в ОРГАНИЗАЦИИ;
- 2) определение входов и выходов каждого процесса для установления последовательности и взаимодействия процессов;
- 3) планирование и обеспечение ресурсами (включая информацию), необходимыми для осуществления процессов и управления ими;
- 4) определение необходимой степени документирования и собственно документирование процессов;
- 5) осуществление планирования процессов;
- 6) наличие критериев и методов оценки осуществления и управления процессами;
- 7) осуществление мониторинга, оценки и анализа процессов;
- 8) проведение корректирующих (превентивных) и упреждающих действий по результатам анализа процессов, включая совершенствование процессов;

9) определение методов и осуществление управления процессами, результаты которых нельзя проверить посредством последовательного мониторинга и измерения.

Все процессы ОРГАНИЗАЦИИ можно разделить на четыре основные группы [170]:

1) *основные* (процессы жизненного цикла), обеспечивающие намеченный результат деятельности; назначение процесса – создание основных продуктов деятельности; результат – основной продукт и/или полуфабрикат для его изготовления для промежуточных процессов;

2) *вспомогательные*, предназначенные для обеспечения нормального функционирования основных и других процессов необходимыми ресурсами; они обеспечивают работу основных (сервисное обслуживание оборудования, обеспечение энергоресурсами и производственной средой, обеспечение работы офиса, информационное обеспечение, обеспечение финансовой поддержки, управление окружающей средой, связь с общественностью и т.д.); назначение процесса – обеспечение деятельности основных процессов; результат – ресурсы и сервисы для основных процессов. Процесс обеспечения ИБ относится к вспомогательной деятельности;

3) *процессы управления* (менеджмента), относящиеся к стратегическому планированию, постановке целей и установлению политик, обеспечению коммуникаций и т.п.; назначение процесса – управление деятельностью ОРГАНИЗАЦИИ; результат – деятельность всей ОРГАНИЗАЦИИ; управленческие задачи по своей природе являются информационными; управление обеспечением ИБ в рамках управления деятельностью ОРГАНИЗАЦИИ относится к этой группе процессов;

4) *процессы контроля – измерения, анализа и совершенствования*; назначение процесса – получение входных данных для процессов совершенствования деятельности ОРГАНИЗАЦИИ; результат – совершенствование всей деятельности ОРГАНИЗАЦИИ.

Результативность (продуктивность) (англ. *effectiveness*) процесса отражает степень реализации запланированной деятельности и достижения запланированных результатов [171]. Эффективность (англ. *efficiency*) процесса – это в большей степени экономическая категория, показывающая соотношение между достигнутым результатом (характеристикой результативности) и использованными затратами-ресурсами (время, финансы и т.д.), обеспечившим его получение (рис. 19).



Рисунок 19 – Взаимосвязь понятий результативности и эффективности процессов

Следовательно, результативность зависит от качества решений по отношению к целям («делать правильные вещи»), а эффективность – от качества действий («делать вещи правильно»). И результативность и эффективность могут оцениваться посредством внутренних и внешних процессов контроля (проверки).

3.1.2. Определение понятия обеспечения информационной безопасности информационно-телекоммуникационной сети

Прежде чем определить термин «обеспечение ИБ», напомним, что **ИБ ИТКС ОРГАНИЗАЦИИ** – состояние защищенности ТС ОРГАНИЗАЦИИ, предназначенных для обработки и передачи по линиям связи информации, доступ к которой осуществляется с использованием современных ИТ, СВТ и средств связи, включающее безопасность информационных ресурсов и предоставляемых услуг и обеспечивающее функциональную устойчивость ИТКС в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) в ЕИП ОРГАНИЗАЦИИ.

Исходя из введенных понятий процесса и ИБ ИТКС, определим, что обеспечение ИБ ИТКС ОРГАНИЗАЦИИ достигается за счет реализации группы процессов поддержания совокупности свойств ИБ для всех элементов ИТКС – конфиденциальности, целостности, доступности, подлинности, подотчетности, неотказуемости и достоверности, приоритетность которых определяется значимостью информации для интересов (целей) ОРГАНИЗАЦИИ. Таким образом, любое отдельное действие по обеспечению перечисленных свойств ИБ элементов ИТКС ОРГАНИЗАЦИИ можно рассматривать либо как процесс, либо как его часть (в том числе в составе основных бизнес-процессов ОРГАНИЗАЦИИ). Следовательно, **обеспечение ИБ ИТКС ОРГАНИЗАЦИИ** – это деятельность, направленная на реализацию мер по защите ИТКС от компьютерных атак и представляемая сложным процессом, состоящим из множества подпроцессов поддержания безопасного (защищенного) состояния всех ее элементов в отдельности (информационных ресурсов) и ИТКС в целом (объединяющей ИИ) как основы обеспечения ИБ ЕИП ОРГАНИЗАЦИИ. Отсюда следует, что информационная защищенность ЕИП напрямую зависит от информационной защищенности ее ИТКС, когда создана адекватная защищенная среда устойчивого функционирования ИТКС, обеспечивающая необходимый уровень ИБ для обработки, передачи и хранения информационных ресурсов и поддерживающей их ИИ. Ранее отмечалось, что обеспечение ИБ ИТКС ОРГАНИЗАЦИИ осуществляется за счет взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и

иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению угроз ИБ и ликвидации последствий их проявления для ИТКС (адаптировано на основе [2]).

Модель, представленная на рис. 20, иллюстрирует связи деятельности по обеспечению ИБ ИТКС в ЕИП ОРГАНИЗАЦИИ и ее основной деятельности, что характеризует обеспечение ИБ ИТКС именно как процесс [172].



Рисунок 20 – Взаимосвязь деятельности ОРГАНИЗАЦИИ по обеспечению ИБ ИТКС и ее основной деятельности в ЕИП

Для обеспечения ИБ ИТКС ОРГАНИЗАЦИИ необходимы исходные данные, ресурсы и управляющие воздействия.

Входными данными для процесса являются следующие:

- информационные модели основной деятельности ОРГАНИЗАЦИИ – описания бизнес-процессов, реализуемых технологий и т.д.;
- информация о среде функционирования ИТКС;

- потребности ОРГАНИЗАЦИИ в обеспечении ИБ ИТКС;
- информация, используемая для контроля успешности деятельности по обеспечению ИБ ИТКС.

Информационные модели основной деятельности ОРГАНИЗАЦИИ и информация о среде определяют внутренний и внешний контекст всей деятельности по обеспечению ИБ, включая обеспечение ИБ ЕИП ОРГАНИЗАЦИИ и ИТКС в том числе, поскольку именно он позволяет понять, где в деятельности и ИИ поддержки деятельности в части ИТ имеются уязвимости, где и при каких условиях могут на их основе проявиться те или иные угрозы ИБ и действия нарушителей ИБ, где находятся требующие защиты информационные активы, какие меры обеспечения ИБ – организационные, административные, аппаратно-программные, технические – могут потребоваться и какие из них будут наиболее эффективными в каждом конкретном случае.

Кроме этого должны учитываться правовые и нормативные требования по обеспечению ИБ и управления организации в части ИБ, а также все ресурсы (финансовые, материальные, информационные, человеческие и оборудование), необходимые для обеспечения данной деятельности.

Выходом (результатом) деятельности по обеспечению ИБ ИТКС ОРГАНИЗАЦИИ является следующее:

- документы по обеспечению ИБ ИТКС (отчеты, предложения, в том числе по обучению персонала, внутренние нормативные документы и т.д.);
- предупреждение об опасности для основной деятельности организации, вызванные событиями ИБ, возникающими в ИТКС;
- меры обеспечения ИБ для ИТКС в целом и для ее отдельных элементов (СЗИ) и процессы их эксплуатации, а также заказы на их приобретение, поставку и регламентацию использования и т.п.

Результаты деятельности ОРГАНИЗАЦИИ по обеспечению ИБ выступают в качестве ресурсного обеспечения для основной деятельности ОРГАНИЗАЦИИ и непосредственно влияют на эффективность основных бизнес-процессов. Рассмотренная связь задает контекст высокого уровня, позволяющий в ОРГАНИЗАЦИИ в первую очередь позиционировать управленческие, информационные, материальные и ресурсные потоки в рамках взаимоотношения деятельности по обеспечения ИБ ИТКС (как вспомогательной) с основной и другими бизнес-процессами.

3.1.3. Модель обеспечения информационной безопасности информационно-телекоммуникационной сети

Исходя из логики осуществления любого процесса, представим упрощенную модель обеспечения ИБ ИТКС ОРГАНИЗАЦИИ, которая позволяет системно и комплексно решать поставленные задачи по достижению требуемого уровня ИБ ИТКС (рис. 21). Перед тем, как процесс будет разработан и внедрен, должен быть описан контекст (среда), в котором его будут использовать. На этой основе формулируются цели процесса в поддержку основных бизнес-целей ОРГАНИЗАЦИИ. Только после этого начинается реализация целей процесса. И, наконец, когда он внедрен и используется, необходимо постоянно контролировать результативность достижения поставленных в начале целей, и по результатам такого контроля регулярно пересматривать описание контекста (поскольку среда осуществления деятельности динамически меняется) и переформулировать цели процесса, что доказывает итерационность обеспечения ИБ ИТКС. Упрощения в представленной модели касаются намеренного упущения ресурсного обеспечения и управляющих воздействий каждого из этапов процесса, чтобы не перегрузить модель излишней с данной точки зрения информацией.



Рисунок 21 – Упрощенная модель процесса обеспечения ИБ ИТКС

Все начинается с описания внешнего и внутреннего контекста обеспечения ИБ ИТКС как вспомогательного процесса по отношению к основной деятельности ОРГАНИЗАЦИИ. Для этого должна быть определена парадигма (исходная концептуальная схема, модель постановки проблемы и ее решения) обеспечения ИБ (например, противостояние собственника и нарушителя ИБ за получение контроля над информационными активами ИТКС) и определены информационные активы ИТКС, требующие защиты. Исходя из этой схемы и реестра активов, строятся модели ИБ – Модель угроз и Модель нарушителя ИБ (для ИТКС в целом, ее ИС и т.п.). Результаты первого этапа моделирования процесса отражают специфику деятельности ОРГАНИЗАЦИИ и определяют границы, в которых осуществляется обеспечение ИБ ИТКС.

На втором этапе должны быть сформулированы цели обеспечения ИБ ИТКС. В первую очередь должен быть создан реестр (классификатор) рисков ИБ ИТКС, который строится на основе двух моделей ИБ и позволяет подобрать меры обеспечения ИБ, необходимые для приемлемой обработки рассчитанных рисков ИБ. Кроме этого в реестре указываются информационные активы ИТКС, требующие защиты в определенном приоритетном порядке в зависимости от их ценности для деятельности ОРГАНИЗАЦИИ, что дополняет модели ИБ. Во многих нормативных и правовых документах неоднократно упоминается реестр рисков (даже в ГОСТ Р 51901.23-2012 [173], в названии которого присутствует это словосочетание), но ни в одном из них не приводится его вид. Представим шапку таблицы, которая лучше всего соответствует назначению реестра рисков ИБ, а именно описанию основных видов опасных событий – потенциальных инцидентов ИБ и применяемых методов обработки рисков ИБ для последующей разработки интегрированного и всестороннего плана мероприятий по предупреждению и снижению рисков ИБ:

Актив				Угроза ИБ			Оценка начального риска ИБ			Меры обработки риска ИБ	Оценка остаточного риска ИБ		
1	2	3	4	5	6	7	8	9	10	11	12	13	14

В шапке таблицы введены следующие сокращения:

- 1 – информационный актив, имеющий ценность для осуществления деятельности ОРГАНИЗАЦИИ и потому требующий поддержания для него основных свойств ИБ;
- 2 – СОИА (среда обработки информационного актива);
- 3 – уязвимость СОИА, используемые угрозами ИБ для реализации;
- 4 – приоритеты обеспечения свойств ИБ для актива;
- 5 – наименование угрозы ИБ (из Модели угроз ИБ);
- 6 – источник угрозы ИБ (из Модели нарушителей ИБ);

- 7 – метод и способ реализации угрозы ИБ;
- 8 – вероятность/степень возможности реализации угрозы ИБ;
- 9 – последствия/степень тяжести последствий угрозы ИБ;
- 10 – величина и значимость (в терминах «допустимый–недопустимый») начального риска ИБ;
- 11 – меры обеспечения ИБ, снижающие величину начального риска ИБ;
- 12 – вероятность/степень возможности реализации угрозы ИБ после внедрения мер обработки риска ИБ;
- 13 – последствия/степень тяжести последствий угрозы ИБ после внедрения мер обработки риска ИБ;
- 14 – величина и значимость (в терминах «допустимый–недопустимый») остаточного риска ИБ.

Для одного и того же актива, имеющего несколько уязвимостей, заполняются столько строк, сколько есть уязвимостей, поскольку меры обработки для каждой уязвимости могут быть различными. Также если одну и ту же уязвимость могут использовать несколько угроз ИБ, то заполняется столько строк, сколько возможно реализовать на их основе угроз ИБ. Если одну угрозу ИБ может активировать сразу несколько источников угроз ИБ (антропогенных, техногенных, стихийных), то также необходимо заполнить строку на каждый источник. Как видно из этих рассуждений, размерность реестра рисков ИБ будет значительная, но таким образом будет получено очень детальное описание всех рисков ИБ и подобраны наиболее подходящие для них меры обработки рисков ИБ, которые при соответствующем перефразировании будут представлять собой требования по обеспечению ИБ всех элементов ИТКС ОРГАНИЗАЦИИ.

Далее на основе парадигмы и реестра рисков ИБ формулируются основные требования по обеспечению ИБ ИТКС, которые и составляют основную часть содержания частной Политики ИБ ИТКС – документа, отражающего позицию руководства ОРГАНИЗАЦИИ по обеспечению ИБ ИТКС в соответствии с требованиями ее основной деятельности и правовыми и законодательными нормами. Место Политики ИБ ИТКС в общей системе согласованных документов ОРГАНИЗАЦИИ представлено на рис. 22. В ГОСТ Р ИСО/МЭК 13335-1-2006 Политика безопасности ИКТ (англ. *ICT security policy*) – это правила, директивы, сложившаяся практика, которые определяют, как в пределах ОРГАНИЗАЦИИ и ее ИКТ управлять, защищать и распределять активы, в том числе критичную информацию [174]. С целью сохранения логики рисунка обозначим Политику безопасности ИКТ как Политику ИБ ИКТ. При этом согласно ГОСТ Р 50922-2006 Политика безопасности (информации в организации) – это совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [111].

В широком смысле Политика ИБ ОРГАНИЗАЦИИ является системой документированных управленческих решений по обеспечению ее ИБ [172]. В узком смысле Политика ИБ представляет собой отдельный нормативный документ, определяющий требования по обеспечению ИБ, систему мер и/или порядок действий, а также ответственность сотрудников ОРГАНИЗАЦИИ и меры обеспечения ИБ для определенной области применения. Например, это Политика антивирусной защиты или Политика использования паролей работниками для доступа к ИС. Такие частные политики детализируют положения Политики ИБ применительно к одной или нескольким областям обеспечения ИБ, видам деятельности и технологиям, используемым в ОРГАНИЗАЦИИ, и является Политикой ИБ в узком смысле. На рис. 22 примерами частных политик ИБ в узком смысле являются Политики ИБ для всех элементов ИТКС, владеют которыми различные подразделения ОРГАНИЗАЦИИ.

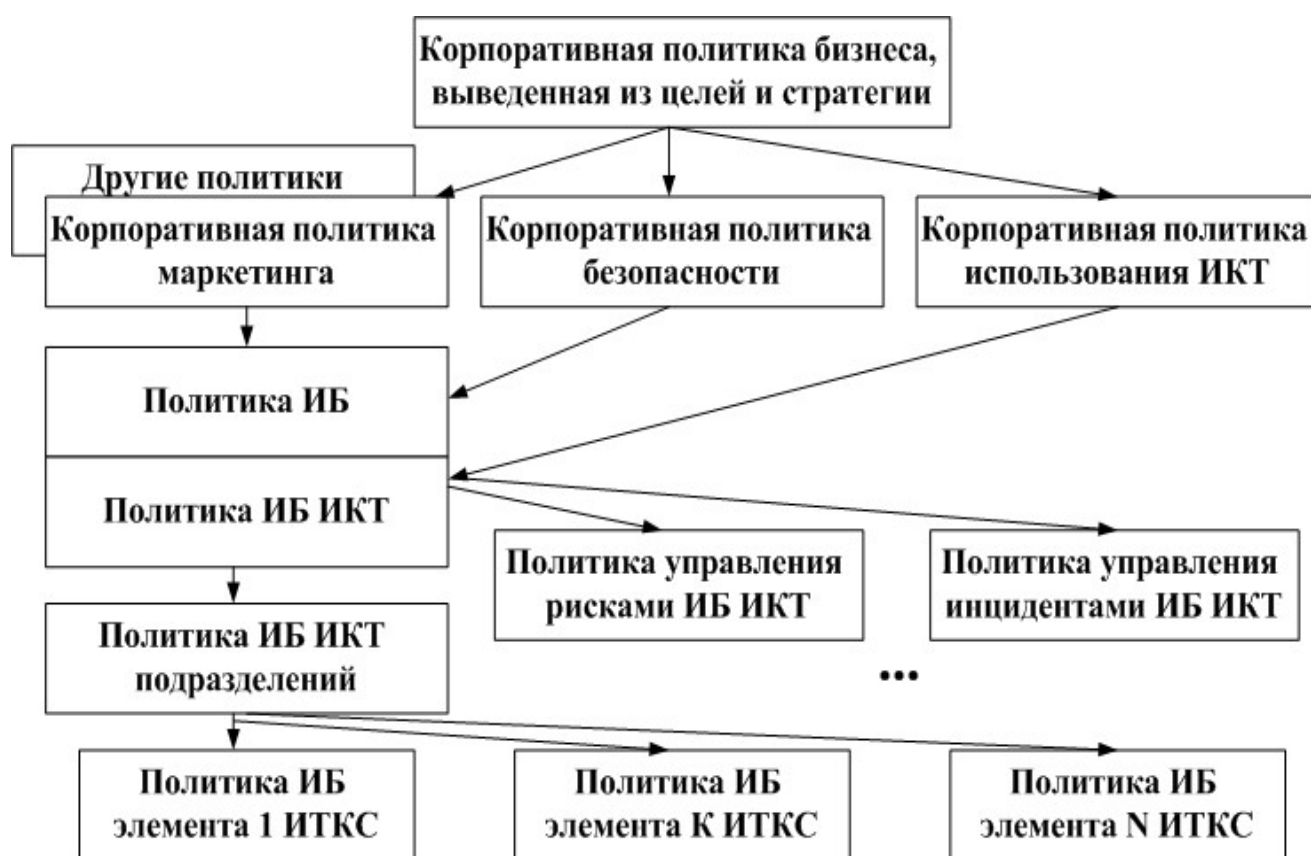


Рисунок 22 – Место Политики ИБ ИТКС в системе документов ОРГАНИЗАЦИИ

Частная Политика ИБ ИКТ ОРГАНИЗАЦИИ является подчиненной по отношению к Политике ИБ (документу, описывающему высокоуровневые требования по обеспечению ИБ, которые должны соблюдаться во всей ОРГАНИЗАЦИИ), которая, в свою очередь, является подчиненной по отношению к Корпоративной политике безопасности (англ. *corporate security policy*) – документу, отражающему позицию руководства по обеспечению безопасности

ОРГАНИЗАЦИИ в соответствии с требованиями ее основной деятельности и правовыми и законодательными нормами. На рис. 22 Политика ИБ и Политика ИБ ИКТ изображены рядом, поскольку в небольшой организации их содержания могут быть изложены в одном документе. Положения Политики ИБ ИКТ детализируются в других политиках, например, Политике управления рисками ИБ ИКТ и Политике управления инцидентами ИБ ИКТ.

Исходя из лучших практик написания частных политик ИБ, предлагаемая примерная типовая структура Политики ИБ для элемента ИТКС (далее – Политики) может быть такой.

Раздел 1. Общие сведения о целях и области действия Политики.

Раздел 2. Цели обеспечения ИБ элемента ИТКС в рамках обеспечения ИБ ИТКС и их соотношение с правовыми и нормативными обязательствами и бизнес-целями ОРГАНИЗАЦИИ.

Раздел 3. Принципы обеспечения ИБ элемента ИТКС.

Раздел 4. Требования, предъявляемые к обеспечению ИБ элемента ИТКС с точки зрения обеспечения конфиденциальности, целостности, доступности, аутентичности, подотчетности, неотказуемости и надежности информации.

Раздел 5. Организация и система обеспечения ИБ элемента ИТКС.

Раздел 6. Сведения об обеспечении ИБ элемента ИТКС, включающие в себя данные об ответственности и полномочиях как ОРГАНИЗАЦИИ, так и отдельных лиц.

Раздел 7. Категорирование подлежащих защите активов элемента ИТКС; общий обзор для них уязвимостей и угроз ИБ, возможно в виде Модели угроз ИБ и Модели нарушителей ИБ (или ссылка на эти модели, которые могут быть оформлены как отдельные документы).

Раздел 8. Подход ОРГАНИЗАЦИИ к управлению рисками ИБ для элемента ИТКС.

Раздел 9. Пути и способы определения приоритетов при реализации мер обеспечения ИБ для элемента ИТКС.

Раздел 10. Сведения об общем уровне ИБ и остаточном риске ИБ для элемента ИТКС, необходимые для ее устойчивого функционирования или использования.

Раздел 11. Сведения о наличии общих правил контроля доступа (логический контроль доступа при одновременном контроле физического доступа лиц в здания, рабочие помещения, а также к ИС и информации).

Раздел 12. Обеспечение непрерывности функционирования/использования элемента ИТКС в бизнес-целях, включая планирование действий при чрезвычайных ситуациях и восстановлении после аварий, стратегии и план (планы).

Раздел 13. Сведения о доведении до персонала мер обеспечения ИБ и обучении лиц, осуществляемом ОРГАНИЗАЦИЕЙ.

Раздел 14. Сведения об общих процедурах контроля и поддержания ИБ элемента ИТКС.

Раздел 15. Общие проблемы обеспечения ИБ элемента ИТКС, касающиеся обслуживаю-

щего персонала.

Раздел 16. Средства и способы доведения положений Политики до всех причастных лиц.

Раздел 17. Положения по контролю реализации Политики.

Раздел 18. Обстоятельства, при которых может быть проведен пересмотр Политики.

Раздел 19. Методы контроля изменений, вносимых в Политику.

Раздел 20. Владелец Политики.

Раздел 21. Ответственность за несоблюдение Политики.

Раздел 22. Термины и определения.

Раздел 23. Ссылочные документы и справочная информация.

При необходимости ОРГАНИЗАЦИЯ может добавить, удалить или переставить выше перечисленные разделы, хотя логика этого документа должна быть именно такой.

Кроме названных Административных, выполняемых людьми, Политик ИБ, должны быть разработаны Технические Политики ИБ, регулирующих обработку, хранение и передачу важной информации и использование ресурсов ПО и АО ИТКС.

На третьем этапе реализации целей обеспечения ИБ ИТКС осуществляется выбор конкретных решений по обеспечению ИБ и их непосредственное внедрение и использование. Для этого создается СОИБ ИТКС как часть СОИБ ОРГАНИЗАЦИИ, поскольку ее основное назначение – это централизованная поддержка состояния защищенности ЕИП ОРГАНИЗАЦИИ (ее информационных активов, ИТ-услуг, хранилищ информации, средств обработки и передачи информации и т.п.). СОИБ состоит из системы управления ИБ (СУИБ) и мер обеспечения ИБ и процессов их эксплуатации. СОИБ ИТКС включает в себя соответствующую организационную структуру (в которую будет входить ЦИУСБ как ее системообразующий элемент), политику, планирование действий, роли и обязанности, установившийся порядок, процессы и процедуры обеспечения ИБ, меры обеспечения ИБ и ресурсы, необходимые для обеспечения ИБ ИТКС ОРГАНИЗАЦИИ. Далее производится обучение работников ОРГАНИЗАЦИИ вопросам обеспечения ИБ и соблюдения Политик ИБ, поскольку такие знания необходимы для корректной работы и обслуживания защищаемых информационных активов ИТКС, владельцами или пользователями которых они являются.

Четвертый этап – контроль достижения целей обеспечения ИБ ИТКС – является инструментом обратной связи за счет выполнения различных контрольных мероприятий (внутренние и внешние аудиты ИБ, самооценка ИБ, мониторинг ИБ и анализ функционирования СОИБ руководством ОРГАНИЗАЦИИ) [175], поскольку по их результатам должно выполняться стратегическое, тактическое и операционное совершенствование СОИБ. На этом этапе внедряется система измерений [176] и задаются критерии оценивания полученных результатов, что позволяет оценить результативность обеспечения ИБ и выработать соответствующие предложения

по его улучшению. Контрольные мероприятия и проведение измерений для оценки результативности реализованной СОИБ позволяют убедиться, что выполняются все высокоуровневые задачи обеспечения ИБ ИТКС, и выявляют нарушения Политики ИБ (инциденты ИБ) и то, насколько корректно на втором этапе были выбраны и настроены меры обеспечения ИБ.

Двунаправленные стрелки на рис. 21 показывают постоянную динамику и цикличность деятельности по обеспечению ИБ, включающую постоянный пересмотр моделей ИБ, итерационность процесса оценки рисков ИБ, соответствующее изменение и уточнение требований по обеспечению ИБ в Политиках ИБ, подстройку под динамически изменяющуюся информационную сферу ОРГАНИЗАЦИИ эксплуатируемых в соответствии с Политикой ИБ мер обеспечения ИБ и последующее совершенствование СОИБ ИТКС и всех процессов обеспечения ИБ.

Очевиден важный вывод, что деятельность по обеспечению ИБ ИТКС шире, чем просто деятельность по управлению ее ИБ, поскольку она также включает в себя систематическое осуществление контрольных мероприятий и повседневную деятельность по поддержанию информационной защищенности ИТКС на достаточном с точки зрения ОРГАНИЗАЦИИ уровне в течение длительного времени за счет внедрения и использования мер обеспечения ИБ и соответствующих процессов обеспечения ИБ (включая процессы эксплуатации таких средств).

3.1.4. Определение понятия обеспечения сетевой безопасности информационно-телекоммуникационной сети

Помня о заключительных абзацах раздела 1.2, определим, что ***обеспечение сетевой безопасности ИТКС*** включает деятельность, направленную на обеспечение безопасности устройств ИТКС, обеспечение безопасности управления этими устройствами, приложениями, предоставляемыми услугами и конечными пользователями, в дополнение к обеспечению безопасности информации, передаваемой по линиям связи ИТКС. Как и ранее, соотношение понятий обеспечения информационной и сетевой безопасности заключается в их пересечении в части деятельности по обеспечению свойств ИБ информационных ресурсов, обрабатываемых, передаваемых и хранимых в ИТКС. При этом при обеспечении сетевой безопасности ИТКС есть еще, по крайней мере, два вида деятельности, которые относятся к обеспечению безопасности сетевых устройств и обеспечению безопасности управления ими.

Стратегическими целями обеспечения сетевой безопасности ИТКС ОРГАНИЗАЦИИ чаще всего являются следующие:

- предупреждение возможности реализации угроз ИБ в отношении информационных активов ИТКС и предоставляемых потребителям на ее основе ИТ-услуг;
- устранение уязвимостей всех элементов ИТКС;

- снижение количества инцидентов ИБ, происходящих в ИТКС;
- минимизация ущерба и времени восстановления ИТКС после нарушений и инцидентов ИБ для возможности ее использования по назначению.

3.2. Управление информационной безопасностью информационно-телекоммуникационной сети как часть обеспечения ее информационной безопасности

Управление ИБ ИТКС ОРГАНИЗАЦИИ является неотъемлемой частью управления любой современной организацией в целом и ее ИТКС в частности. В общем случае *управление ИБ ОРГАНИЗАЦИИ* – это циклический процесс, который состоит из совокупности целенаправленных действий, осуществляемых для достижения заявленных бизнес-целей ОРГАНИЗАЦИИ посредством обеспечения защищенности ее информационной сферы [172, 177]. Этот процесс включает в себя осознание необходимости обеспечения ИБ, постановку задач управления ИБ, оценку текущей ситуации и состояния объектов управления, планирование мер по обработке выявленных рисков ИБ, реализацию, внедрение и оценку результативности соответствующих **защитных мер** (англ. *safeguard*), или **контрмер** (англ. *countermeasure*), или **мер обеспечения ИБ**, ранее называемых *мерами и средствами контроля и управления ИБ* (англ. *controls*) (средства менеджмента риска, включающие в себя политики, процедуры, рекомендации, инструкции или организационные структуры, которые могут быть административного, технического, управленческого или правового характера [106]), распределение ролей и ответственности в области управления ИБ, обучение и мотивацию сотрудников, выбор управляющих и корректирующих воздействий и их реализацию. При этом в качестве целенаправленных действий выделяются оценка ситуации и состояния объекта управления (например, на основе проведения оценки рисков ИБ), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание мер обеспечения ИБ) и многое другое.

Прежде чем сформулировать определение понятия «управление ИБ ИТКС ОРГАНИЗАЦИИ», необходимо сделать несколько важных замечаний.

1. В различных нормативных документах (например, отечественных российских стандартах – гармонизированных аналогах международных) и публикациях можно встретить термины «управление ИБ» и «менеджмент ИБ», имеющих в своей основе одно и то же понятие, как становится ясно после прочтения этих источников. Этому вопросу посвящено достаточно публикаций, поэтому умышленно опустим сравнительный анализ двух понятий. Для единообразия будет использоваться только термин «управление ИБ» как наиболее привычный для российских ученых и специалистов.

2. Более правильным представляется использование словосочетания «управление обес-

печением ИБ», а не просто «управление ИБ», поскольку управлять состоянием защищенности (что непосредственного следует из определения ИБ) можно лишь, осуществляя деятельность по обеспечению ИБ, которая реализуется посредством соответствующих процессов по обеспечению такого состояния. Для краткости далее все же будет использовать общепринятый термин «управление ИБ».

3. В настоящее время, к сожалению, не существует общепринятого определения управления ИБ. Этот термин «моден» и используется многими: производителями и продавцами СЗИ, системными интеграторами, специалистами, представителями средств массовой информации (СМИ) и т.д. Например, первые две категории понимают под этим термином техническую составляющую процесса управления (обнаружение вторжений и вирусов, управление настройками СЗИ и т.д.). Многие пользователи понимают под управлением ИБ только управление программными или аппаратными СЗИ. Такие взгляды слишком ограничены и узконаправлены.

4. Управление ИБ – не разовое мероприятие. Его следует рассматривать как непрерывную деятельность по постоянному поддержанию требуемого ОРГАНИЗАЦИЕЙ уровня ИБ, так как рационально управляемая ИБ – это инструмент успешного осуществления деятельности.

5. Более правильно рассматривать управление ИБ как совокупность целенаправленных действий, осуществляемых для обеспечения функциональной устойчивости основных бизнес-процессов и, в конечном счете, достижения бизнес-целей ОРГАНИЗАЦИИ посредством обеспечения информационной защищенности ее ЕИП в условиях существования угроз ИБ.

3.2.1. Определение понятия управления информационной безопасностью информационно-телекоммуникационной сети

На основе выше приведенных рассуждений сформулируем, что под ***управлением ИБ ИТКС ОРГАНИЗАЦИИ*** будет пониматься циклический процесс, который состоит из совокупности целенаправленных действий, осуществляемых для достижения заявленных бизнес-целей ОРГАНИЗАЦИИ посредством обеспечения информационной защищенности ее ИТКС как основы ЕИП в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций). Данные действия имеют конечной целью обеспечить безопасное, надежное и устойчивое функционирование, а также эксплуатацию, сопровождение и совершенствование ИТКС ОРГАНИЗАЦИИ в течение всего ее жизненного цикла.

Из приведенного определения следует, что управление ИБ ИТКС представляет собой сложный непрерывный процесс, перед которым стоит множество целей и задач. Поэтому этот процесс распадается на тесно взаимосвязанные подпроцессы. Каждый из подпроцессов в раз-

ной степени вносит свой вклад в обеспечение ИБ. Общие эффективность и результативность всей деятельности по обеспечению ИБ в ОРГАНИЗАЦИИ зависят от эффективности и результативности каждого из входящих в деятельность по управлению ИБ подпроцессов.

3.2.2. Уровни управления информационной безопасностью информационно-телекоммуникационной сети

В управлении ИБ ИТКС ОРГАНИЗАЦИИ можно выделить три основных уровня: стратегического, тактического и оперативного управления. Особенности и взаимосвязь данных уровней управления поясняет рис. 23 [172].

Самый верхний уровень – административный, на котором принимаются стратегические решения. *Уровень стратегического управления ИБ* предназначен для постановки целей обеспечения ИБ ИТКС на длительную перспективу и воплощения в жизнь стратегии ОРГАНИЗАЦИИ по отношению к обеспечению ИБ ИТКС в поддержку ее основной деятельности и расстановки соответствующих приоритетов. Стратегия ИБ является официально принятой руководством ОРГАНИЗАЦИИ системой взглядов на проблему обеспечения ее ИБ, методы и средства защиты жизненно важных интересов в информационной сфере, включая ИБ ИТКС ОРГАНИЗАЦИИ. Эта система взглядов определяет цели, задачи, принципы и основные направления обеспечения ИБ ОРГАНИЗАЦИИ и обеспечивается взаимоувязанными правовыми, организационными, аппаратно-программными, техническими и иными мерами обеспечения ИБ и в качестве обратной связи основывается на постоянном анализе информационной защищенности ИТКС ОРГАНИЗАЦИИ средствами мониторинга ИБ для выявления и последующего устранения уязвимостей, угроз ИБ и уже состоявшихся инцидентов ИБ с прослеживанием динамики их развития и недопущения появления в будущем. Именно на этом уровне и представляется целесообразным создать единый Центр интеллектуального управления сетевой безопасностью (ЦИУСБ) ОРГАНИЗАЦИИ, поскольку его главными целями является стратегическое планирование обеспечения сетевой безопасности ИТКС и улучшение для нее показателей уровня ИБ в соответствии с различными требованиями по обеспечению ИБ на длительную перспективу, включающие прогнозирование развития ситуации в ИТКС в связи с внедрением новых ИКТ, тенденций появления новых угроз ИБ в ЕИП ОРГАНИЗАЦИИ и новых подходов к обеспечению ИБ на основе интеллектуальных подходов.

К задачам тактического уровня управления относятся планирование и обеспечение выполнения Политики ИБ ИТКС, разработка соответствующих положений, регламентов, правил, инструкций и т.п., а также расследование инцидентов ИБ. Для результативного управления ИБ ИТКС на тактическом уровне, когда определяются методы и способы обеспечения ИБ, прово-

дится выработка корректирующих и предупреждающих воздействий на ИТКС, хорошо подходит Центр интеллектуальной безопасности (ЦИБ) ИТКС. ЦИБ способен управлять инцидентами ИБ в ИТКС ОРГАНИЗАЦИИ. На уровне оперативного управления сбором и простейшим анализом собранных данных занимается известный Центр мониторинга безопасности (ЦМБ).

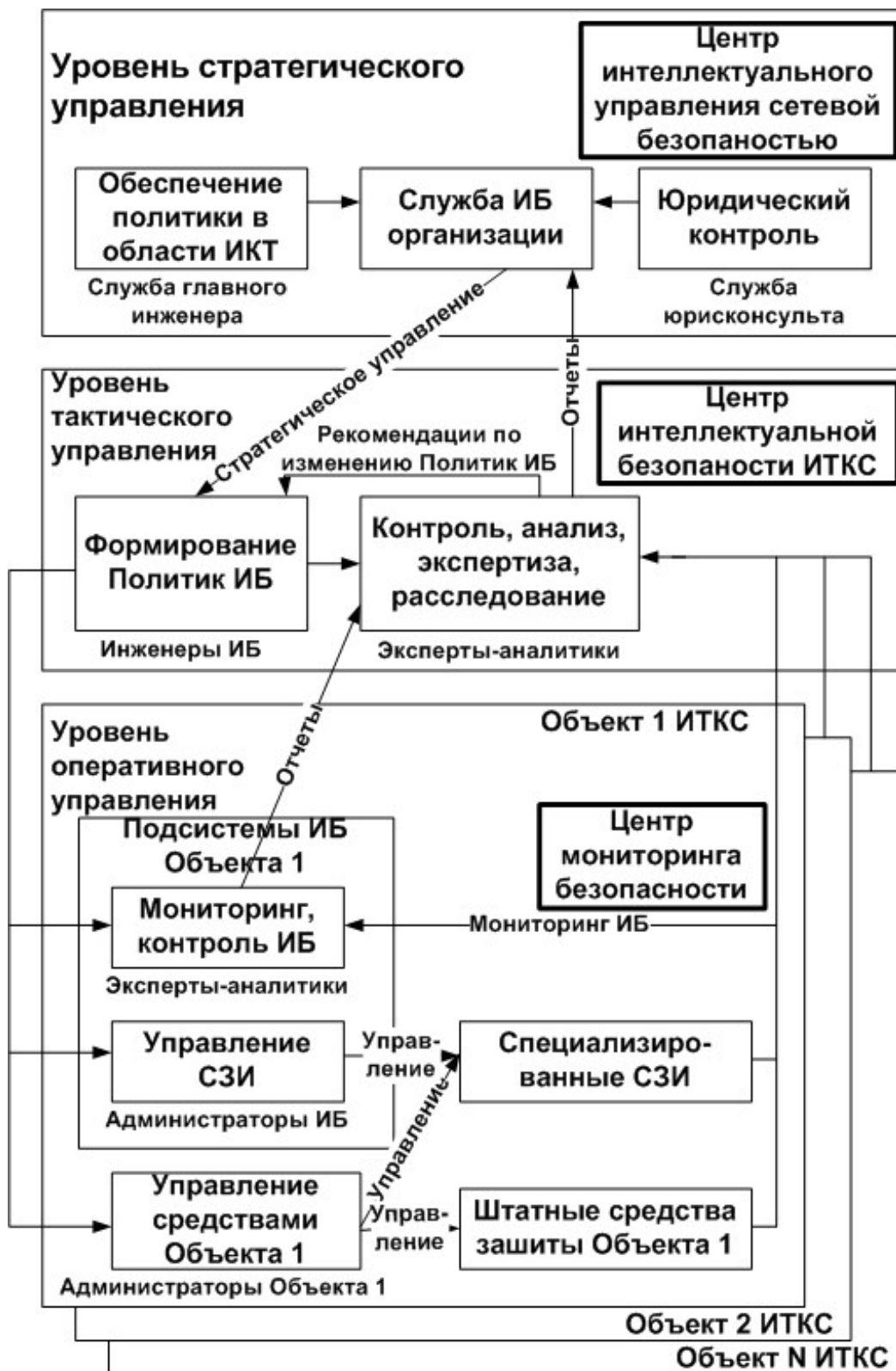


Рисунок 23 – Уровни управления ИБ ИТКС ОРГАНИЗАЦИИ

Основными двумя задачами решения текущих ежедневных проблем обеспечения ИБ – оперативного управления ИБ – отдельных элементов ИТКС, названными на рис. 23 объектами ИТКС, является непосредственная реализация Политики ИБ ИТКС, включая определение способов и средств обеспечения ИБ, формирование частных политик обеспечения ИБ для объектов и контроль за их соблюдением и исполнением, а также реализация и эксплуатация мер обеспечения ИБ. Разработанные специалистами и утвержденные высшим руководством ОРГАНИЗАЦИИ Корпоративная и частные Политики ИБ содержат набор норм, правил и практических приемов, которые различным образом регулируют управление, распределение и защиту ценной для организации в различных смыслах информации. Это правила разграничения доступа, регламентирующие права доступа субъектов доступа к объектам доступа и виды этого доступа. Нижний уровень реализует выполнение частных Политик ИБ. Анализ состояния ИБ проводится на основе сопоставления требований определенной Политики ИБ собранным и проанализированным данным мониторинга и аудита ИБ уровня оперативного управления.

Ранее подчеркивалось, что процесс управления ИБ ИТКС ОРГАНИЗАЦИИ должен быть интегрирован в общий процесс управления ИКТ. Он основывается на изложенных в ГОСТ Р ИСО/МЭК 13335–3 принципах и четырех этапах [178]: анализ требований по обеспечению ИБ ИТКС, разработка плана выполнения этих требований, реализация положений выработанного плана и управление и административный контроль над процессом управления ИБ ИТКС (рис. 24), что представляет данный процесс несколько с иной точки зрения, чем на рис. 23.

Представленный процесс управления ИБ ИТКС соответствует классическому пониманию процесса в целом (рис. 25).

На рис. 24 также показана обратная связь между результатами процесса и его отдельными частями, которая должна устанавливаться по мере необходимости как в пределах выполнения одного из этапов, так и после завершения одного или нескольких этапов.

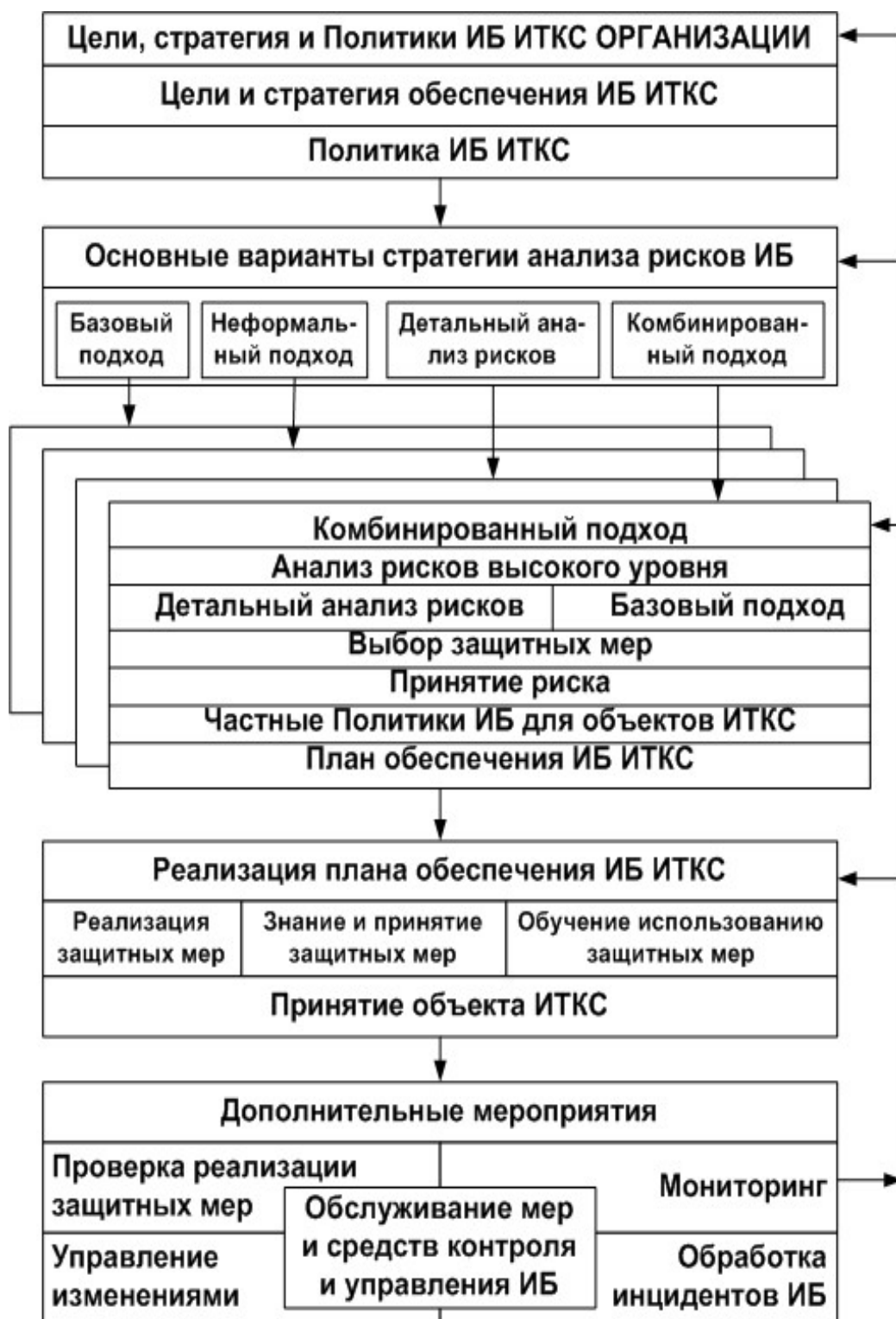


Рисунок 24 – Схема управления ИБ ИТКС ОРГАНИЗАЦИИ



Рисунок 25 – Высокоуровневое представление процесса управления ИБ ИТКС

3.2.3. Система управления информационной безопасностью информационно-телекоммуникационной сети

Неоднократно упоминаемые в данном исследовании элементы ИТКС – это и есть одни из объектов управления (управляемых объектов) ИБ. В рамках подпроцессов управления ИБ для ИТКС понятие объектов управления шире – это не только информационные активы, ИС, ИТ-услуги, но и риски ИБ, инциденты ИБ, непрерывность деятельности, изменения, совершенствования, сами меры обеспечения ИБ, обеспечивающие ресурсы, участвующую в реализации информационных процессов ИТКС, и пр. (рис. 24). Управляющим объектом является специально разработанная и внедренная Система управления ИБ (англ. *information security management system*) ИТКС ОРГАНИЗАЦИИ (СУИБ ИТКС ОРГАНИЗАЦИИ) как часть СОИБ ИТКС [172].

СУИБ ИТКС как важная часть СОИБ ИТКС должна обладать следующими чертами:

- ее построение и функционирование должно быть основано на постоянной оценке бизнес-рисков и рисков ИБ в частности, то есть на риск-ориентированном подходе;
- она должна быть предназначена для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ ИТКС;
- она должна включать организационную структуру, политику, планирование действий, роли и обязанности, установившийся порядок, процедуры, процессы, меры обеспечения ИБ и ресурсное обеспечение для эффективного управления ИБ ИТКС (рис. 26).



Рисунок 26 – Иллюстрация понятия СУИБ ИТКС ОРГАНИЗАЦИИ

Адаптируя введенные в [171] автором данного исследования понятия, определим **эффективность управления ИБ ИТКС** как экономическую категорию, отражающую вклад управленческой деятельности в отношении обеспечения ИБ ИТКС в конечный результат – уровень ИБ ИТКС и определяемую степенью реализации целей ОРГАНИЗАЦИИ в области обес-

печения ИБ ИТКС и ее интегрального показателя – прибыли. Тогда **эффективность СУИБ ИТКС** – это соотношение между достигнутым уровнем ИБ ИТКС, полученным при управлении ИБ ИТКС на основе СУИБ, и использованными ресурсами, обеспечившими его получение [171]. Оценка эффективности СУИБ ИТКС должна осуществляться в рамках системного процесса получения и оценки объективных данных о текущем состоянии СУИБ ИТКС, процессах и событиях, происходящих в ней, устанавливающего уровень их соответствия определенным ОРГАНИЗАЦИЕЙ критериям [171].

3.2.4. Циклическая модель рассмотрения процессов управления информационной-безопасностью информационно-телекоммуникационной сети

Поддержание на должном уровне ИБ ИТКС на основе СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ГОСТ Р ИСО/МЭК 27001-2006 циклическая модель, или цикл, *PDCA* (от англ. *Plan-Do-Check-Act* – Планируй–Выполни–Проверь–Действуй) предусматривает непрерывный цикл мероприятий («планирование – реализация – проверка – совершенствование») по управлению ИБ ИТКС на системной основе применительно ко всем процессам на трех уровнях управления – стратегическом, тактическом и операционном (рис. 27) [172].

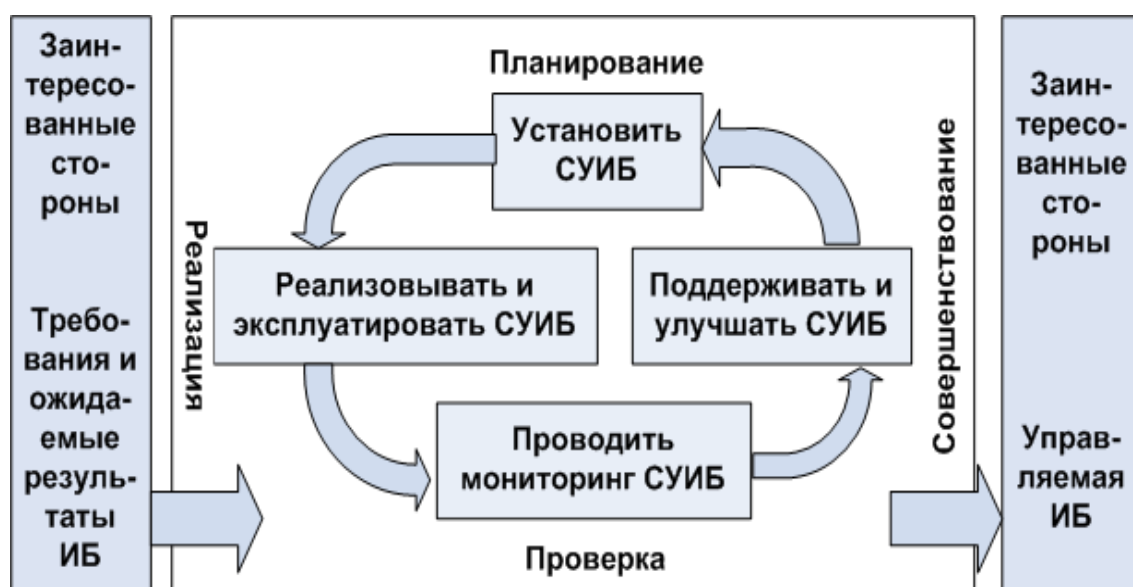


Рисунок 27 – Циклическая модель рассмотрения процессов управления ИБ в рамках СУИБ ИТКС

На стадии планирования должно быть обеспечено корректное задание внешнего и внутреннего контекстов управления ИБ ИТКС и масштаба СУИБ ИТКС ОРГАНИЗАЦИИ. Вместе с владельцами процессов управления ИБ должны быть определены и описаны текущее и желаемое

мое состояния процессов на основе выявленных несоответствий и причин их появления. Должны быть оценены риски ИБ для ИТКС и предложен соответствующий план обработки выявленных рисков, особенно тех, которые попадают в область недопустимых рисков ИБ (**допустимый риск ИБ** – это риск ИБ, предполагаемый ущерб от которого ОРГАНИЗАЦИЯ в данное время и в данной ситуации готова принять [107]). На стадии реализации внедряются принятые во время планирования решения, то есть происходит создание некоторой структуры, которая должна выполнять намеченные планы и тем самым достигать поставленные цели. Чтобы гарантировать, что СУИБ ИТКС в целом достигает их, необходимы периодические проверки внедренных решений – мер обеспечения ИБ и процессов их эксплуатации. На стадиях проверки и совершенствования ранее определенные и уже реализованные решения по управлению ИБ усиливают, корректируются и совершенствуют, то есть предпринимаются соответствующие действия по коррекции отклонений от первоначальных планов и постоянному улучшению функционирования процессов управления ИБ. Если вносимые изменения не решают поставленную задачу, то цикл должен быть повторен.

В зависимости от конкретной ситуации (внутреннего и/или внешнего контекста) проверки СУИБ ИТКС и деятельности по управлению ИБ ИТКС на основе данной СУИБ могут проводиться в любое время и с любой периодичностью. В некоторых элементах ИТКС с целью обеспечения немедленного выполнения и реагирования проверки должны быть встроены в автоматизированные процессы. Для других процессов реагирование нужно только в случае выявленных инцидентов ИБ, а также когда в требующие сохранения свойств ИБ элементы ИТКС внесены изменения или дополнения или произошли изменения ранее выявленных угроз ИБ и уязвимостей.

Детальное содержание основных подпроцессов цикла *PDCA* применительно к процессам СУИБ ИТКС ОРГАНИЗАЦИИ показано рис. 28.

Примерами основных процессов СУИБ ИТКС ОРГАНИЗАЦИИ являются следующие целевые (профильные) виды деятельности, иногда называемые частными управлениями [172]:

- управление информационными активами и объектами СОИА ИТКС;
- управление рисками ИБ ИТКС;
- управление инцидентами ИБ ИТКС;
- управление ролями, выполняемыми сотрудниками в рамках обеспечения ИБ ИТКС;
- управление персоналом, включая службу ИБ ИТКС;
- управление изменениями, улучшениями (тактическими, стратегическими), корректирующими и предупреждающими действиями;
- управление мерами обеспечения ИБ ИТКС и процессами их эксплуатации;
- управление информированием и обучением вопросам обеспечения ИБ ИТКС;

- управление документами и записями, относящимися к деятельности в области обеспечения ИБ в рамках СУИБ ИТКС;
- управление непрерывностью и функциональной устойчивостью ИТКС;
- управление контрольными мероприятиями в области проверки уровня ИБ (мониторинг ИБ, внутренние и внешние аудиты ИБ, самооценка ИБ) ИТКС;
- управление результативностью и эффективностью деятельности в области обеспечения ИБ ИТКС.

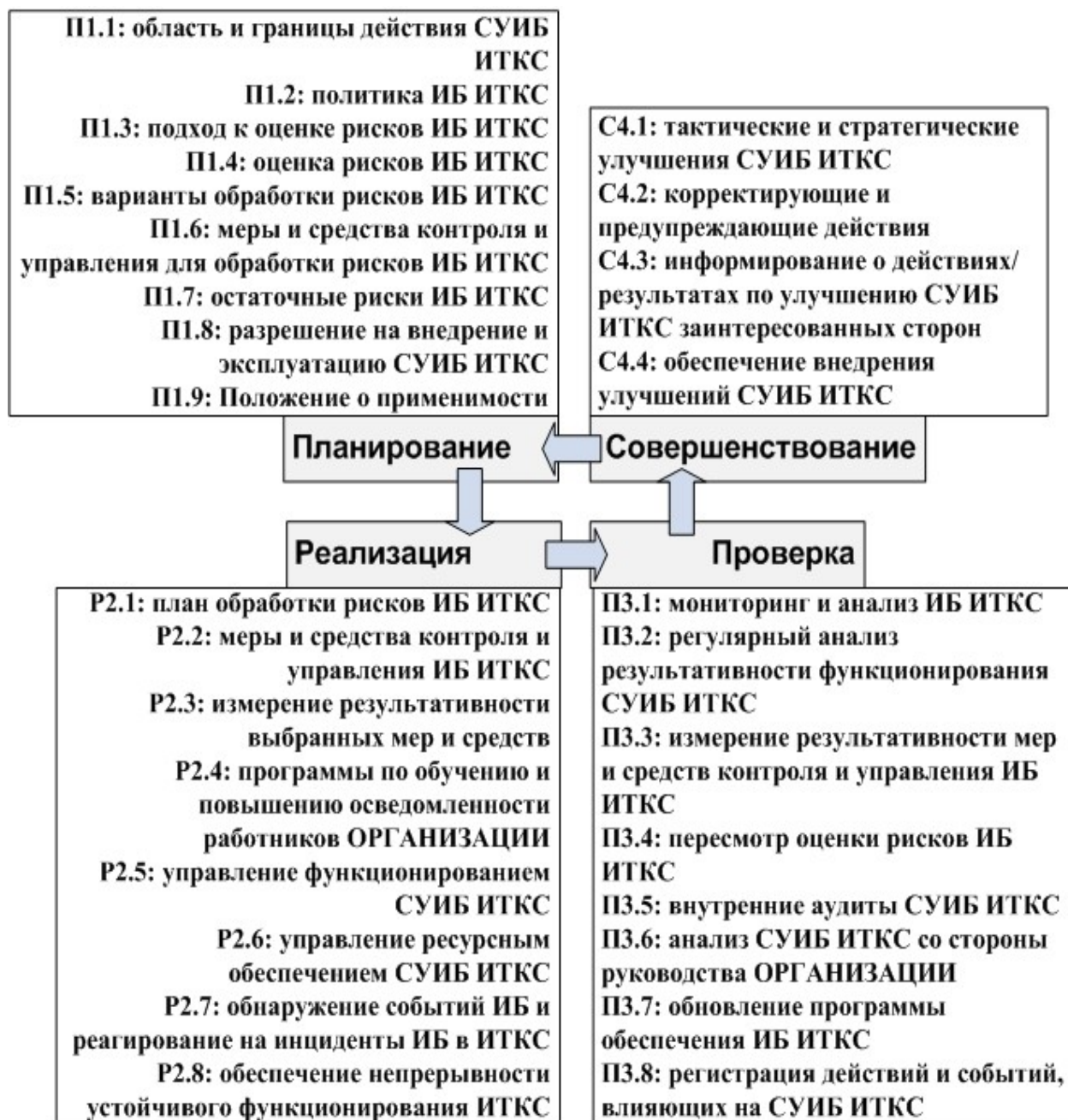


Рисунок 28 – Содержание подпроцессов цикла PDCA применительно к процессам СУИБ ИТКС ОРГАНИЗАЦИИ

3.2.5. Определение понятия управления сетевой безопасностью информационно-телекоммуникационной сети

Как в заключительных абзацах разделов 1.2 и 3.1 отметим, что **управление сетевой безопасностью ИТКС** будет основываться на циклическом процессе, который состоит из совокупности целенаправленных действий, осуществляемых для управления безопасностью устройств ИТКС, используемых приложений, предоставляемых услуг и конечных пользователей, в дополнение к управлению безопасностью информации, передаваемой по линиям связи ИТКС, в целях безопасного и устойчивого функционирования ИТКС ОРГАНИЗАЦИИ в течение всего ее жизненного цикла. Как и ранее, соотношение понятий управления информационной и сетевой безопасности заключается в их пересечении в части управления обеспечением свойств ИБ информационных ресурсов, обрабатываемых, передаваемых и хранимых в ИТКС. При этом при управлении сетевой безопасностью ИТКС есть еще, по крайней мере, один вид деятельности, который относится к управлению безопасностью сетевых устройств.

На основе результатов анализа технологий обеспечения сетевой безопасности (табл. 1) и критического пересмотра [179] была прослежена эволюция подходов к управлению сетевой безопасностью по мере расширения ее возможностей (табл. 6) [180]. Выделено три основных этапа: первый – защита физического периметра сети, второй – более детальное логирование (регистрация) событий ИБ и проверка соблюдения различных требований по обеспечению сетевой безопасности и современный третий – использование интеллектуальных подходов к управлению сетевой безопасностью.

В табл. 6 явно отражено появление двух ЦУБ, предназначенных для оперативного – ЦМБ [11] и тактического – Центр интеллектуальной безопасности (ЦИБ) (англ. *Security Intelligence Center, SIC*) – управления сетевой безопасностью, послуживших отправной идеей для разработки более совершенного ЦИУСБ ОРГАНИЗАЦИИ.

Таблица 6 – Эволюция подходов к управлению сетевой безопасностью (начало)

<i>Этапы</i> <i>Критерии сравнения</i>	<i>Этап 1 – Защита физического периметра сети</i>	<i>Этап 2 – Логирование и проверка соблюдения требований</i>	<i>Этап 3 – Использование интеллектуальных подходов</i>
Временной интервал	1983-2000	2001-2009	2010-по настоящее время
Задачи	Защита периметра за счет пакетной фильтрации от простейшей до «средней глубины» и технологий обнаружения вторжений. Аутентификация на уровне сети. Ручное устранение уязвимостей на основе анализа защищенности. Развита антивирусная защита.	Более «глубокая» инспекция пакетов за счет корреляции событий из консолидированных (рассматриваемых совместно) ЖРС и контроль исходящих коммуникаций. Зарождение аналитики ИБ с использованием знаний о пользователях и приложениях. Развитие компьютерной форензики и более детальные отчеты об ИБ. Обнаружение и предотвращение вторжений. Автоматизированное управление уязвимостями, угрозами и обновлениями.	Защита, ориентированная на данные и логический периметр сети. Полноценное управление консолидированными ЖРС и использование знаний о контексте, в котором проводится анализ. Оценка состояния на соответствие различным требованиям. Обнаружение и реагирование на угрозы ИБ; на этой основе управления рисками ИБ. Мониторинг приложений. Развита подходы к мониторингу работы и активности пользователей.
Архитектура	Управление ИБ как комплексное решение. Глубоко встроена в отдельные существующие системы.	Более зрелое управление ЖРС и ИБ-аналитика. Распределенная архитектура.	Обработанные данные аналитики отделены от данных ИТКС. Весь сетевой поток включен в аналитику. Централизованная консоль.
Источники данных	Небольшое количество источников поддерживается «из коробки».	Большее разнообразие источников данных в ЖРС.	Все относящиеся к ИБ данные со всей организации.
Количество управляемых устройств	От десятков до сотен.	От сотен до тысяч.	Не ограничено, основано на уникальных требованиях к масштабированию каждого решения.
Количество событий в сек	1000-5000.	Более 10000.	Будет определено опытным путем.
Объемы хранения	Сотни гигабайт.	Терабайты.	Будет определено опытным путем.
Аналитика	Фильтрация событий, базовая корреляция событий.	Расширенная корреляция, аналитика ограничена типом данных (только из ЖРС).	Расширенная аналитика, включая события в сети и инфраструктуре (VPN, СОВ/СПВ и т.д.), контекст сети и приложения, данные о пользователях из IAM-систем.

Таблица 6 – Эволюция подходов к управлению сетевой безопасностью (окончание)

Конечные пользователи	Группа реагирования на компьютерные инциденты и защиты периметра (через веб-сервисы).	Группа реагирования на инциденты ИБ (группа безопасности ИТ) и группа проверки соответствия различным требованиям.	Группы безопасности ИТ и проверки соответствия различным требованиям, операторы ЦМБ, аудиторы, специалисты по сетям и направлениям бизнеса.
Реагирование на нарушения ИБ	Медленное. Ручной сбор данных и информации об устройствах. Обнаружение может занять годы.	Обнаружение часто растягивается на месяцы и годы. Быстрее, но быстрому реагированию не способствует ограниченная аналитика. Появление ЦМБ.	Обнаружение нарушений в режиме реального / близкого к реальному времени, часто с исправлением в тот же день. Часто автоматическое реагирование. Появление ЦИБ.
Основные ограничения	Ручной анализ. Ложные положительные/отрицательные срабатывания. Ограниченные форматы ЖРС. Немасштабируемость, небольшое количество поддерживаемых устройств.	Ограниченная аналитика данных. Нельзя собирать данные не из ЖРС. Проблемы производительности при работе с большими данными. Ложные положительные/отрицательные срабатывания.	Стандарты руководящих органов еще не выработаны. Интеграция со сторонними продуктами /источниками все еще трудоемка.

3.3. Проверка информационной безопасности информационно-телекоммуникационной сети как средство постоянного контроля общего управления информационной безопасностью организации

Как показал представленный во введении анализ степени разработанности проблемы данного исследования, в современных условиях достаточно много сделано в направлении обеспечения ИБ, но мало предложено по управлению теми мерами обеспечения ИБ, которые внедрены в ОРГАНИЗАЦИИ. Очень часто организации не осознают, какие элементы их ЕИП являются наиболее критичными и какие из них никак нельзя утратить для дальнейшего успешного осуществления деятельности, какие именно риски ИБ и каким образом связаны с ними, какие меры обеспечения ИБ для них необходимо запланировать и почему, есть ли признаки ослабления (деградации) используемых мер обеспечения ИБ и т.п. Ответы на эти и многие другие вопросы могут дать проанализированные заключения и выводы различных проверок ИБ, в том числе мониторинга ИБ и контроля используемых мер обеспечения ИБ [171], что на практике неотделимо от вопросов реализации СУИБ ИТКС ОРГАНИЗАЦИИ.

Целью выполнения деятельности в рамках группы процессов «Проверка» является обеспечение достаточной уверенности в том, что СУИБ ИТКС, включая все меры обеспечения ИБ

ИТКС, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутреннему и внешнему контексту функционирования ИТКС ОРГАНИЗАЦИИ, влияющим на ее ИБ. Кроме того, необходимо учесть любые изменения в допущениях или области оценки рисков ИБ. ОРГАНИЗАЦИЯ должна своевременно обнаруживать любые проблемы, прямо или косвенно влияющие на ИБ ИТКС и способные повлиять на ее бизнес-цели. Рекомендуется обязательно выявлять причинно-следственную связь возможных проблем и строить на этой основе прогноз их развития. Указанная деятельность может проводиться в любое время и с любой частотой, в зависимости от того, что подходит в каждой конкретной ситуации.

На этапе «Проверка» необходимо осуществлять мониторинг и анализ ИБ ИТКС и используемых мер обеспечения ИБ ИТКС, проводить внутренний и внешний аудит ее ИБ, анализировать функционирование СУИБ ИТКС в целом и ее отдельных элементов, как это рекомендуется в [66] и показано на рис. 27 и 28. При этом, если возможно, производится количественное измерение результативности и эффективности процессов управления ИБ для проверки соответствия требованиям нормативных и правовых документов, стандартов и политик, целям обеспечения ИБ ОРГАНИЗАЦИИ и практическому опыту функционирования СУИБ.

Процессы мониторинга и анализа СУИБ ИТКС должны быть интегрированы в систему единого внутреннего контроля ОРГАНИЗАЦИИ. Перефразируя положения ГОСТ Р ИСО/МЭК 27002-2012 [106], сформулируем перечень первоочередных действий, которые должны предприниматься для выполнения последующих мероприятий по совершенствованию СУИБ ИТКС.

1. Регулярно осуществлять процедуры мониторинга и анализа ИБ ИТКС, а также использовать все доступные меры обеспечения ИБ для своевременного обнаружения ошибок в результатах обработки данных с использованием ИТКС, выявления удавшихся/неудавшихся попыток нарушения ИБ и инцидентов ИБ в ИТКС, предоставления руководству информации о ходе выполнения деятельности по обеспечению ИБ ИТКС и определения, являются ли эффективными действия по устранению нарушений и инцидентов ИБ в ИТКС в рамках СУИБ.

2. Проводить регулярный анализ результативности СУИБ ИТКС, включая проверку ее соответствия Политике ИБ ИТКС и установленным целям и непосредственный анализ мер обеспечения ИБ. Такой анализ должен учитывать результаты аудиторских проверок ИБ ИТКС и ее отдельных элементов, измерений результативности СУИБ ИТКС, опыт выявления инцидентов ИБ в ИТКС, а также предложений и другой информации от всех причастных сторон.

3. Измерять результативность мер обеспечения ИБ ИТКС на предмет соответствия всем применимым требованиям, включая требования по обеспечению ИБ, требования законодательства и регуляторов и договорные обязательства.

4. Через установленные промежутки времени пересматривать проведенную оценку рисков ИБ для ИТКС, анализировать остаточные риски ИБ, их величины и перечень ранее приня-

тых допустимых рисков ИБ, учитывая произошедшие изменения во внутреннем и внешнем контексте функционирования ИТКС, технологиях, процессах, выявленных новых и изменившихся старых угрозах ИБ, результативности реализованных мер обеспечения ИБ.

5. Через установленные промежутки времени проводить внутренние аудиты СУИБ ИТКС силами самой ОРГАНИЗАЦИИ.

6. Регулярно проводить анализ СУИБ ИТКС руководством ОРГАНИЗАЦИИ в целях подтверждения адекватности ее функционирования в рамках установленной области действия и определения направлений дальнейшего совершенствования.

7. Обновлять Программу (План) обеспечения ИБ ИТКС, разработанную в поддержку реализации Политики ИБ ИТКС, с учетом результатов мониторинга и анализа его ИБ.

8. Регистрировать все действия и события, способные повлиять на результативность или само функционирование СУИБ ИТКС.

3.3.1. Определение понятия мониторинга информационной безопасности информационно-телекоммуникационной сети

Мониторинг ИБ может быть назван ключевым элементом непрерывной проверки соблюдения требований по обеспечению ИБ ИТКС ОРГАНИЗАЦИИ и основой выявления событий, связанных с ее ИБ, в рамках функционирования ЦИУСБ ОРГАНИЗАЦИИ (рис. 21). Под ***мониторингом ИБ и контролем защитных мер ИТКС ОРГАНИЗАЦИИ*** (далее – ***мониторинг ИБ ИТКС ОРГАНИЗАЦИИ***) будем понимать процесс постоянного (непрерывного) наблюдения за регистрируемыми событиями, влияющими на обеспечение ИБ ИТКС ОРГАНИЗАЦИИ, а также сбор, анализ и обобщение результатов наблюдений [171].

Мониторинг ИБ ИТКС ОРГАНИЗАЦИИ реализуется в рамках СУИБ ИТКС на базе постоянного контроля за соблюдением базовых требований по обеспечению ИБ и предписанных регламентов функционирования ИТКС (контроль штатности режима функционирования ИТКС). Тогда две основные цели мониторинга ИБ ИТКС ОРГАНИЗАЦИИ можно сформулировать следующим образом:

1) выявление, сбор, анализ и обработка данных для каждого из направлений деятельности по обеспечению ИБ ИТКС в соответствии с заданными целями;

2) обеспечение уполномоченных сторон полной, своевременной, достоверной информацией для принятия обоснованных решений в области обеспечения ИБ ИТКС и, при необходимости, оперативной корректировки всей деятельности в данном направлении.

Первая цель может быть достигнута за счет реализации двух групп процессов мониторинга ИБ в рамках общего процесса управления ИБ ИТКС:

— поиск, отслеживание, наблюдение, накопление, систематизация, оценивание данных, относящихся к обеспечению ИБ ИТКС;

— краткосрочное и долгосрочное прогнозирование состояния всех объектов и процессов в ЕИП ОРГАНИЗАЦИИ.

Исходя из этого можно заключить, что мониторинг ИБ ИТКС – это ключевой элемент управления рисками ИБ в динамически изменяющейся ИТКС ОРГАНИЗАЦИИ, поскольку анализ собранных во время мониторинга ИБ ИТКС данных обычно осуществляется со следующими целями:

1) выявление событий ИБ в ИТКС, часть из которых в дальнейшем будет классифицирована как инциденты ИБ в соответствии с установленными в ОРГАНИЗАЦИИ правилами;

2) выявление нештатных (как неумышленных, так и злоумышленных) действий с информационными активами и бизнес-процессами ОРГАНИЗАЦИИ, поддерживаемыми в рамках функционирования ИТКС;

3) выявление уязвимостей элементов ИТКС (включая уязвимости в самих СЗИ ИТКС), которыми могут воспользоваться злоумышленники для реализации атак на системы, сети и услуги как самой ОРГАНИЗАЦИИ, так и ее бизнес-партнеров или пользователей общедоступных сетей типа интернета, если ИТКС имеет с ними соединение;

4) контроль за реализацией положений внутренних и внешних документов по обеспечению ИБ ИТКС в целом и ее отдельных элементов с целью обнаружения отклонений от принятых требований бизнеса и требований по обеспечению ИБ (например, зафиксированных в Политике в отношении логического доступа к информационным активам ИТКС или Политики использования ресурсов интернета);

5) контроль качества (результативности и эффективности) используемых в ИТКС мер обеспечения ИБ;

6) обеспечение доказательной базы на случай расследования инцидентов ИБ в отношении ИТКС ОРГАНИЗАЦИИ и ее отдельных элементов, которая будет признаваться законной при судебном разбирательстве.

Далее область рассмотрения контрольных проверок ИБ ИТКС сужена до мониторинга ИБ, который и является основным источником данных для функционирования разрабатываемого ЦИУСБ ОРГАНИЗАЦИИ, обеспечивая наблюдаемость и прозрачность всех автоматизированных на основе ИТКС бизнес-процессов (основных, вспомогательных, управленческих) и гарантируя их наблюдаемость в течение всего времени функционирования. В результате этого повышается уровень доверия к ним со стороны бизнеса [170]. Кроме этого мониторинг ИБ способствует повышению чувства ответственности работников ОРГАНИЗАЦИИ за свои действия, влияющие на ИБ. Он помогает в обнаружении неправильного использования ресурсов и во

многим действует в качестве сдерживающего фактора для лиц, способных попытаться нанести ущерб ОРГАНИЗАЦИИ. И, наконец, во время мониторинга ИБ выявляются ошибки в самой обработке информации и ее результатах, связанные как со сбоями в функционировании ИТКС в целом и ее элементов, так и с человеческим фактором. На этой основе в дальнейшем необходимо пересмотреть процесс эксплуатации и функционирования затронутых систем, сетей и сервисов ИТКС с точки зрения выполнения установленных регламентов.

Основной объем информации мониторинга ИБ в компьютерных сетях поступает из различных ЖРС (лог-файлов), хранящих записи о зарегистрированных СЗИ событиях ИБ и протоколирующими работу АО и ПО в строгом хронологическом порядке. Различают регистрацию (занесение в ЖРС) внешних событий и протоколирование работы программ – источников записей (хотя часто всё записывается в единый файл). В ЖРС фиксируются любые сбои и отказы, о которых сообщили системные программы и которые связаны с проблемами в системах обработки или обмена данными.

ЖРС ИТКС – это имеющая отношение к ИБ хронологическая, автоматически создаваемая, с настраиваемой степенью детализации запись/набор записей в файл/БД событий, происходящих с каким-то контролируемым объектом (или в рамках какого-то процесса) ИТКС, с указанием ее источника, документально подтверждающая последовательность действий, сопровождающих конкретную операцию, процедуру, работу программы, событие и т.п.

ЖРС ведутся сетевыми устройствами ИТКС, ОС, приложениями, всеми видами программируемых устройств и т.п. Например, применительно к памяти компьютера это запись в хронологическом порядке операций обработки данных, которая может быть использована для того, чтобы воссоздать существовавшую или альтернативную версию компьютерного файла. В СУБД это записи обо всех событиях изменения данных определённым процессом при работе БД. Таким образом, основными источниками данных о событиях ИБ являются программные и аппаратно-программные средства мониторинга ИБ и контроля эксплуатации применяемых мер обеспечения ИБ. К их числу относятся, например, следующие источники [16, 48]:

- ЖРС систем управления, контроля и мониторинга ИБ;
- ЖРС (системные журналы) ОС и СУБД;
- ЖРС ПО, активного сетевого оборудования и применяемых СЗИ, в том числе ПО проверки целостности файлов, СЗИ от НСД, средств защиты от воздействия вредоносного кода, специализированных средств типа МЭ, СОВ/СПВ, САЗ, *SIEM*-систем и пр.;
- информацию специализированных устройств контроля физического доступа, в том числе телевизионных систем охранного наблюдения, систем контроля и управления доступом и охранной сигнализации.

ЖРС фиксируют такую важную с точки зрения обеспечения ИБ информацию как:

- идентификатор (ID) пользователя;
- даты, времена входа и выхода субъектов доступа и подробности ключевых событий;
- имя хоста, инициировавшего подлежащее регистрации событие, и/или его местоположение;
- записи успешных и отклоненных попыток доступа к объектам доступа;
- изменения в системной конфигурации;
- изменения списков субъектов и объектов доступа;
- изменения полномочий субъектов доступа и статуса объектов доступа (защищаемых информационных ресурсов);
- все привилегированные действия (использование учетной записи супервизора, запуск и останов системы, подсоединение/отсоединение устройств ввода/вывода);
- запуск программ и процессов, осуществляющих доступ к защищаемым информационным ресурсам;
- использование системных утилит и приложений;
- все установленные сессии;
- файлы, к которым осуществлялся доступ, и тип доступа;
- сетевые адреса и протоколы;
- изменения в интенсивности и объемах входящего/исходящего трафика (включая интернет-трафик);
- печать материалов, содержащих сведения конфиденциального характера;
- обращения к критичным системам и сервисам (например, веб-серверу, серверам БД, почтовому серверу, сервисам синхронизации и т.п.);
- системные предупреждения и сбои;
- предупреждения, сгенерированные СОВ/СПВ;
- изменения или попытки изменения настроек и средств управления защитой систем;
- активация и деактивация СЗИ, таких как САВЗ, МЭ и СОВ/СПВ;
- появление новых устройств с неконтролируемым доступом (точки беспроводного доступа, подключенные *USB*-устройства и пр.) и т.п.

Подробнее данный вопрос рассмотрен в проекте ГОСТ Р, посвященного регистрации событий ИБ [16].

Как показано выше, мониторинг ИБ должен осуществляться для различных элементов ИТКС ОРГАНИЗАЦИИ – ИС, ПО и его целостности, устройств и их конфигурационных настроек, сообщений электронной почты, подключений к интернету и сетям бизнес-партнеров, парольной защиты и т.п. Так, например, в рамках процедур мониторинга ИБ ИТКС с различной степенью периодичности соответствующими ответственными лицами (например, систем-

ным/сетевым администратором и оператором разрабатываемого ЦИУСБ) обязательно выполняются, например, следующие действия:

1) ежедневно:

- анализ ЖРС СЗИ и служебных программ;
- выявление попыток несанкционированной установки приложений пользователем;
- анализ доступа пользователей к сетевым ресурсам;

2) один раз в неделю:

- проверка работы сервисов и предоставления услуг пользователям;
- проверка сетевого взаимодействия;
- профилактика БД;
- антивирусная профилактика серверов;
- проверка времени последнего обновления антивирусных баз;
- проверка наличия обновлений ОС и серверных приложений;

3) один раз в две недели (в часы отсутствия работников или наименьшей загрузки):

- принудительная проверка отказоустойчивости систем;
- профилактика дисковой и файловой подсистем на серверах;
- профилактическая остановка серверов;
- проверка целостности ОС;

4) один раз в месяц:

- составление отчета доступа к интернет-ресурсам;

5) по необходимости:

- проверка обновления клиентских приложений;
- удаление временных и устаревших копий файлов и т.п.

В процессе мониторинга все зафиксированные для ИТКС данные об отказах и событиях ИБ должны подвергаться постоянному детальному и регулярному анализу, что включает в себя своевременное выявление и понимание выявленных отказов, состоявшихся компьютерных атак и возникающих угроз ИБ, которым подвержены элементы ИТКС, и причин их возникновения. На этой основе далее делается вывод о явном наличии, отсутствии или возможности наступления инцидента ИБ в ИТКС. Но во многом результаты мониторинга ИБ ИТКС ОРГАНИЗАЦИИ будут зависеть от качества и полноты базовых настроек и возможностей СЗИ по регистрации событий ИБ и на этой основе собранной информации, которая, в свою очередь, влияет на дальнейшую обработку рисков ИБ ИТКС.

Поскольку объем данных в ЖРС очень велик, целесообразно использовать автоматизированные средства для предварительного отбора, анализа и корреляции больших объемов разнородных данных [181].

Полученные во время мониторинга ИБ результаты должны быть зафиксированы в соответствующих отчетах, и должны быть выполнены заранее установленные действия, направленные на устранение выявленных уязвимостей и отказов, прерывание недопустимых видов событий и т.п.

Еще раз подчеркивая контролирующие функции мониторинга ИБ ИТКС, можно отметить, что технической реализации мониторинга ИБ свойственна иерархичность, предполагающая необходимость контролирующих мер на всех уровнях контроля – физическом, сетевом, ОС, СУБД, прикладном.

3.3.2. Взаимосвязь процессов мониторинга и аудита информационной безопасности информационно-телекоммуникационной сети

Понятие мониторинга ИБ тесно связано с понятием аудита ИБ (рис. 29) (на основе [170]). Процесс мониторинг ИБ ИТКС ОРГАНИЗАЦИИ должен в обязательном порядке предшествовать этапу обработки рисков ИБ, предоставляя для него исходные данные за счет выявления отклонений от заданных требований и предписанных регламентов – штатного режима функционирования всей ИТКС и ее отдельных элементов и передавая информацию по уже свершившимся инцидентам ИБ и потенциально возможным нарушениям ИБ ИТКС. Мониторинг ИБ ИТКС позволяет определить, адекватны ли рискам ИБ используемые меры обеспечения ИБ и должным ли образом решаются задачи по обеспечению ИБ ИТКС в ЕИП ОРГАНИЗАЦИИ, возложенные на отдельных работников или эксплуатируемые ИТ, и верно спланировать корректирующие действия для процессов обеспечения ИБ ИТКС, которые будут наиболее результативными в данных обстоятельствах.

В ОРГАНИЗАЦИИ должны быть разработаны и документально оформлены процедуры мониторинга ИБ ИТКС, включая контроль параметров конфигурационных настроек всех СЗИ и процедуры анализа зарегистрированных данных, предпринятых действий и операций. Все эти процедуры должны быть основаны на документально зафиксированных критериях выявления неправомерных или подозрительных действий, транзакций, событий и т.п. Указанные процедуры выполняются персоналом ОРГАНИЗАЦИИ, ответственным за обеспечение ИБ ИТКС, на регулярной основе и должны охватывать все реализованные и эксплуатируемые меры обеспечения ИБ, входящие в СОИБ ИТКС как части СОИБ ОРГАНИЗАЦИИ. Также документально определяются, а затем выполняются процедуры сбора и хранения информации о действиях работников ОРГАНИЗАЦИИ, событиях и параметрах, имеющих отношение к функционированию самих мер обеспечения ИБ.

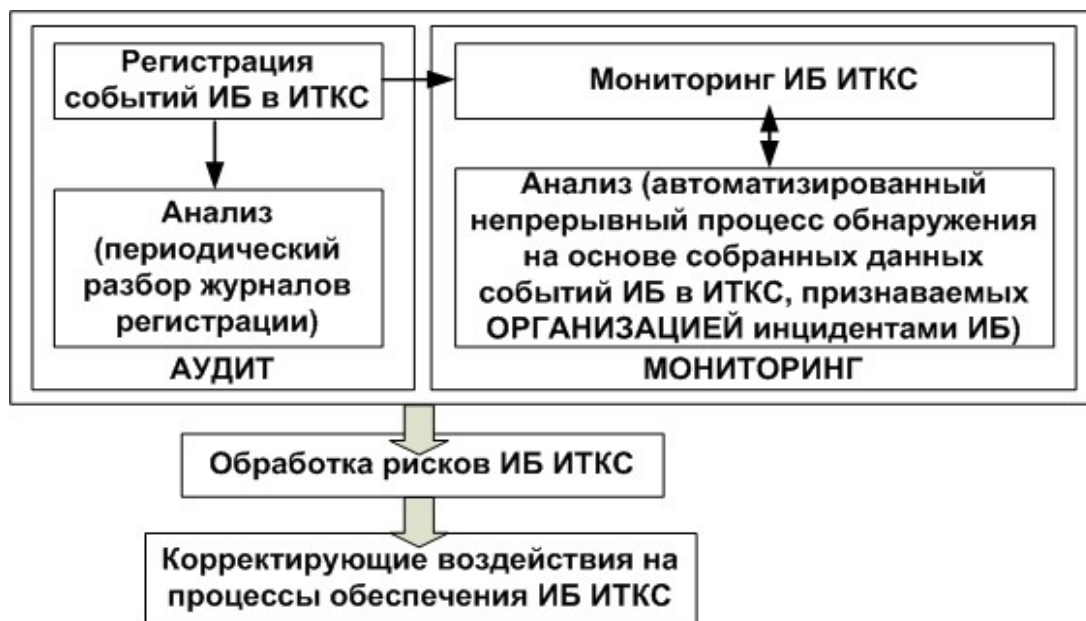


Рисунок 29 – Взаимосвязь процессов мониторинга ИБ и аудита ИБ для ИТКС

Ранее в разделе 1.2 на основе анализа [99] уже подчеркивалось, что общие и более специализированные СЗИ могут регистрировать в ИТКС ОРГАНИЗАЦИИ в течение одного дня миллионы событий ИБ различного происхождения и с разными последствиями. Объем работы, необходимый для выявления событий, действительно важных с точки зрения ИБ данных и получения на основе их анализа информации об инцидентах ИБ может быть огромен. К сожалению, эта деятельность часто до сих пор осуществляется экспертами и аналитиками вручную (с целью корреляции с первого взгляда не связанных между собой событий) и отнимает много времени даже у опытных профессионалов – администраторов ИБ. Своевременное и постоянное наблюдение, сбор, сложный корреляционный анализ и обработка данных в определенном контексте с учетом пользователей и приложений для каждого из поддерживаемых мероприятий по обеспечению ИБ в соответствии с поставленными целями, а также предоставление уполномоченным лицам полной, своевременной и достоверной информации для принятия обоснованных решений в сфере обеспечения ИБ являются основными задачами мониторинга ИБ.

3.3.3. Взаимосвязь процессов мониторинга и управления инцидентами информационной безопасности в информационно-телекоммуникационной сети

Из выше описанных функций мониторинга ИБ очевидно, что процессы мониторинга ИБ также тесно взаимосвязаны с процессами управления инцидентами ИБ в ИТКС (рис. 30) (на основе [170]).



Рисунок 30 – Взаимосвязь процессов мониторинга ИБ и управления инцидентами ИБ для ИТКС ОРГАНИЗАЦИИ

При реагировании на инцидент ИБ должны быть предусмотрены процедуры пересмотра и улучшения процессов управления инцидентами ИБ как на регулярной основе (систематически), так и по результатам обработки любого инцидента ИБ в ИТКС ОРГАНИЗАЦИИ. Финальный отчет по каждому инциденту ИБ сохраняется в БД инцидентов ИБ ИТКС и включает их явные признаки и предвестники, которые могут быть использованы в будущем при прогнозировании и обработке подобных инцидентов. Предложения по улучшению процессов управления инцидентами ИБ касаются вопросов использования дополнительных инструментов или ресурсов, обучения персонала и т.п., то есть всего, что необходимо для принятия решений, направленных на выбор и реализацию мер по совершенствованию процессов управления инцидентами ИБ, оценку рисков ИБ и инициирование улучшений обеспечения ИБ, обновление и/или реализацию новых мер обеспечения ИБ и, в итоге, совершенствование СУИБ ИТКС. Изменение мер обеспечения ИБ, регламентов и ролей персонала также неизбежно отражается на процессах управления инцидентами ИБ. Если, например, при пересмотре этого процесса появилась рекомендация по включению дополнительного параметра мониторинга на сервере ИТКС, то этот вопрос, скорее всего, нельзя решить только в рамках процессов управления инцидентами ИБ,

поскольку потребуются еще внесение изменений в конфигурации СЗИ с соответствующими регламентами и многое другое.

3.4. Разработка процесса управления инцидентами информационной безопасности для информационно-телекоммуникационной сети

3.4.1. Задачи процесса управления инцидентами информационной безопасности

Ни одна самая совершенная мера по снижению рисков ИБ, будь то досконально проработанная Политика ИБ или самый современный МЭ нового поколения, не может полностью предотвратить возникновение в ИТКС ОРГАНИЗАЦИИ событий, потенциально несущих угрозу ИБ ее деятельности. Сложность и разнообразие способов использования ИТКС предопределяют наличие остаточных рисков ИБ, вне зависимости от качества подготовки и внедрения мер противодействия. Кроме того, всегда существует вероятность реализации новых, не известных до настоящего времени, атак «нулевого дня» [142]. Поэтому любой организации необходимо реализовать комплексный подход для решения следующих задач:

- быстрое обнаружение, подтверждение или опровержение факта возникновения инцидента ИБ и/или предупреждение подобных инцидентов ИБ ИТКС в будущем;
- учет инцидентов ИБ в ИТКС для извлечения уроков и информирования о них всех причастных сторон;
- координация реагирования согласно установленным приоритетам действий и дальнейшего анализа инцидента ИБ, включая определение сценариев и технических способов реализаций инцидентов ИБ, а также причастных к этому субъектов;
- минимизация последствий повреждения информационных ресурсов и нарушения функционирования элементов ИТКС, восстановление в кратчайшие сроки непрерывности деятельности ОРГАНИЗАЦИИ при ее нарушении в результате инцидента ИБ;
- сбор полных и достоверных сведений, необходимых для пост-анализа и расследования произошедших инцидентов ИБ и возбуждения гражданского или уголовного дела против нарушителей ИБ;
- обеспечение сохранности и целостности свидетельств того, что инцидент ИБ имел место, накопление и хранения данных в цифровой форме об имевших место инцидентах ИБ;
- обучение персонала ОРГАНИЗАЦИИ действиям по обнаружению, устранению последствий и предотвращению инцидентов ИБ и, в конечном счете, улучшению всего процесса обеспечения ИБ.

Решение всех этих задач наиболее результативным образом возможно только на основе разработки и реализации процесса управления инцидентами ИБ (ПУИИБ) (далее под ПУИИБ

будут обобщенно пониматься все входящие в него процессы) как важнейшей части общей СОИБ ОРГАНИЗАЦИИ и основы деятельности ЦИУСБ ОРГАНИЗАЦИИ. Данные, аккумулируемые в рамках данного процесса, являются необходимыми для работы большого количества других процессов управления ИБ, например, для корректного проведения анализа рисков ИБ или для оценки результативности существующих мер по обеспечению ИБ и процессов управления ею (как это было показано на рис. 30).

3.4.2. Нормативная база управления инцидентами информационной безопасности

В настоящее время существует ряд международных и российских документов, регламентирующих управление инцидентами ИБ и, как правило, последовательно рассматривающих все этапы ПУИИБ: от планирования до улучшения после анализа результатов работы процесса. К таким документам относятся, например, следующие (документы перечислены в хронологическом порядке их опубликования):

- технический отчет CMU/SEI-2004-TR-015, который описывает методику планирования, внедрения, оценки и улучшения процессов реагирования на инциденты, уделяя основное внимание организации работы Группы реагирования на инциденты компьютерной безопасности, а также вводит ряд критериев, на основании которых организация может оценивать результативность предотвращения, обработки и реагирования на инциденты [167];

- ГОСТ Р ИСО/МЭК 27001-2006, который формулирует ряд общих требований по построению процессов управления ИБ, в состав которых входит и ПУИИБ, например, использование циклической модели *PDCA*, надлежащее документирование процессов и процедур, поддержка со стороны руководства организации, непрерывный анализ и улучшения [105];

- ГОСТ Р ИСО/МЭК ТО 18044-2007, который определяет формальную модель ПУИИБ, описывает сам процесс на основе *PDCA*, рассматривает вопросы подготовки для процесса нормативной документации и дает рекомендации по необходимым процедурам и ресурсам [161];

- специальная публикация NIST SP 800-61 (2012 г.), которая представляет собой сборник «лучших практик» по построению процессов реагирования на инциденты компьютерной безопасности с конкретными примерами (*DoS*-атака, вредоносное ПО, НСД, неверное использование и многокомпонентный инцидент), имея в виду более широкое понятие инцидента [131];

- две части международного стандарта ISO/IEC 27035 (2016 г.), которые посвящены принципам управления инцидентами ИБ [68] и руководящим принципам планирования и подготовки к реагированию на инциденты ИБ [127] соответственно и аналогичные им государственные стандарты Республики Узбекистан [165, 166];

- РС БР ИББС-2.5-2014, как и ГОСТ Р ИСО/МЭК 27001-2006, которые рекомендуют

для реализации, эксплуатации, контроля и поддержания на должном уровне управления инцидентами ИБ реализовывать сгруппированные в виде модели *PDCA* процессы, для которых даны детальные рекомендации, включая документирование, выбор технических средств по обнаружению и реагированию на инциденты ИБ, определение ролей процесса реагирования на инциденты ИБ и т.п. [163];

— СТО БР ИББС-1.3-2016, который имеет специализированную направленность на сбор и анализ технических данных при реагировании на инциденты ИБ при осуществлении переводов денежных средств, но при этом содержит и много полезных сведений об организационных, технологических и технических подходах в рамках деятельности по выявлению более общих типов инцидентов ИБ и реагированию на них [164].

3.4.3. Деятельность в рамках процесса управления инцидентами информационной безопасности

На основе анализа перечисленных документов ПУИИБ в данном исследовании рассматривается с точки зрения процессного подхода и циклической модели *PDCA*. Кратко содержание деятельности в рамках ПУИИБ для ИТКС ОРГАНИЗАЦИИ в соответствии с этой моделью приведено в табл. 7.

В самом общем случае управление инцидентами ИБ ИТКС ОРГАНИЗАЦИИ должно включать следующую деятельность (рис. 31).

— Обнаружение и регистрация/фиксация в соответствующей системе (БД) произошедших инцидентов ИБ – осуществляется на основании ЖРС, систем мониторинга доступности ИТ-услуг и обращений пользователей.

— Оценка, классификация и приоритезация обработки инцидентов ИБ – производится идентификация источников и причин возникновения инцидента ИБ, затронутых активов и соответствующих действий для его разрешения, а также определяется критичность инцидента ИБ для деятельности ОРГАНИЗАЦИИ.

— Сохранение детальной информации об инциденте ИБ в БД и сбор свидетельств его осуществления, включая область действия, развитие событий и используемый подход.

— Всестороннее исследование инцидента ИБ при поддержке ИТ-подразделения, партнеров и персонала ОРГАНИЗАЦИИ, а также специалистов, занимающихся сбором свидетельств инцидента ИБ.

— Разрешение и закрытие инцидентов ИБ – осуществляется своевременная обработка и разрешение инцидента ИБ и восстановление затронутых элементов ИТКС и поврежденных ИТ-услуг за счет реконфигурации, переустановки или установки обновлений для СЗИ, систем, сер-

ВИСОВ И Т.П.

— Извлечение уроков из инцидентов ИБ – с подробным описание произошедшего инцидента ИБ, документированием выявленных событий ИБ, предоставлением отчетов руководству, анализом полученных уроков, контролем качества разрешения инцидентов ИБ с целью выявления несоответствий и разработки плана усовершенствования и рекомендаций по управлению инцидентами ИБ.

— Подготовка к усовершенствованию ПУИИБ, включающая предотвращение, повышение осведомленности, обучение, создание ГРИИБ, разработку соответствующих политик и процедур и выбор средств.

Таблица 7 – Содержание деятельности в рамках ПУИИБ для ИТКС ОРГАНИЗАЦИИ

Планирование и подготовка процессов	Определение целей, процессов и процедур, значимых для управления инцидентами ИБ и повышения уровня ИБ ИТКС, с целью получения результатов, соответствующих общим политикам и целям ОРГАНИЗАЦИИ – разрабатываются документы (Политики и Планы), регламентирующие процесс реагирования на инциденты ИБ, создается соответствующая организационная структура (Группа реагирования на инциденты ИБ – ГРИИБ), а также выделяются людские и материальные ресурсы, и проводится обучение персонала.
Реализация процессов (выявление инцидентов и отчетность)	Реализация и использование процессов, процедур и средств управления, в рамках управления инцидентами ИБ ИТКС – происходит мониторинг ИБ, обнаружение и оповещение о возникновении события ИБ, сбор информации о нем и его оценка, определение является ли данное событие инцидентом ИБ, составление отчетов по событиям ИБ, а также реагирование на инцидент ИБ, определение необходимости проведения расследования инцидента ИБ.
Проверка (мониторинг и анализ) процессов	Оценка и, если требуется, измерение характеристик процессов для проверки соответствия целям и практическому опыту, а также передача управленческому персоналу результатов для последующего анализа – проводится анализ и расследование инцидента, на основе чего делаются выводы и составляются рекомендации по улучшению процесса обеспечения ИБ в целом и управления инцидентами ИБ в частности.
Совершенствование (сопровождение и улучшение) процессов	Принятие корректирующих и предупреждающих мер по результатам оценки эффективности и анализа ПУИИБ, выполненного управленческим персоналом, а также на основе другой значимой информации, с целью постоянного совершенствования – реализуются рекомендации, выработанные на этапе анализа, и из ПУИИБ извлекаются полученные уроки.

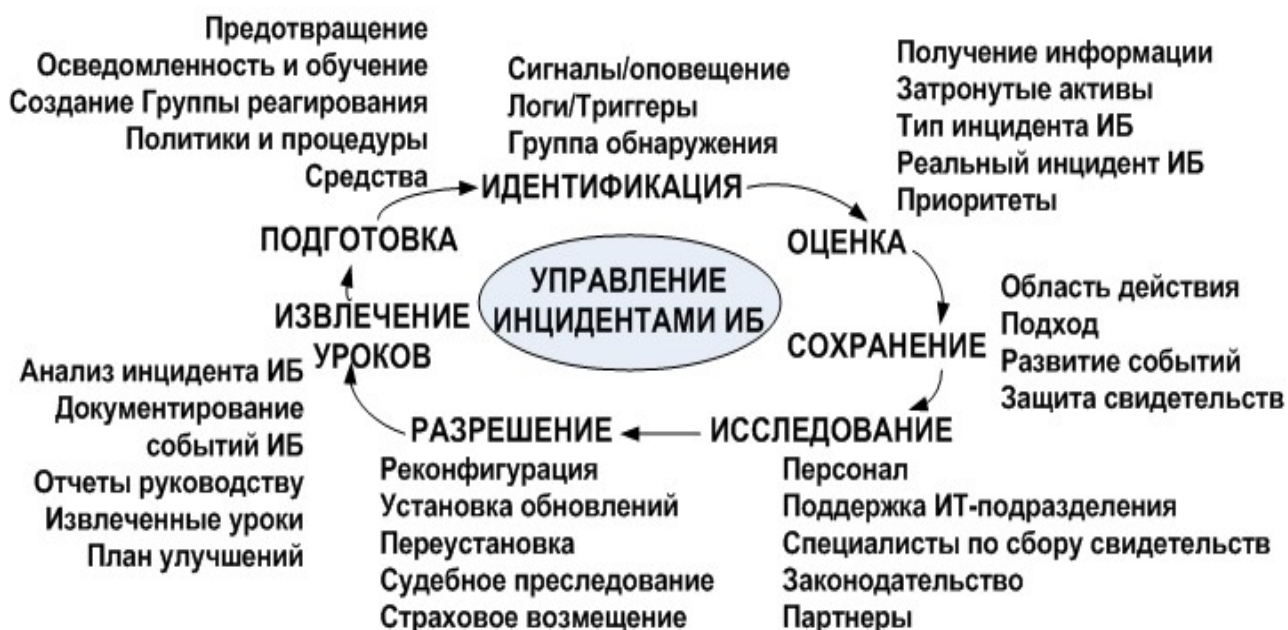


Рисунок 31 – Деятельность в рамках процесса управления инцидентами ИБ для ИТКС

Представляется важным сделать замечание о шкале приоритетов инцидентов ИБ, хотя конечный ее вариант будет зависеть от самой ОРГАНИЗАЦИИ и законов, подзаконных актов и договорных обязательств. Следующий поход к составлению шкалы может послужить отправной точкой при выработке иерархии ответных мер реагирования на инциденты ИБ ИТКС.

Первый приоритет — защитить жизнь и здоровье людей; при всех обстоятельствах защита человеческих жизней должна стоять на первом месте.

Второй приоритет — защитить критически бизнес-процессы и важные данные (в соответствии с применимой правовой и нормативной базой).

Третий приоритет — защитить прочие бизнес-процессы и данные, включая частную, управленческую и другую информацию, поскольку потеря данных дорога и с точки зрения ресурсов, затраченных на их накопление.

Четвертый приоритет — предотвратить повреждение ИС и ИТ-услуг ИТКС (потерю и изменение системных файлов, повреждение дисководов и т.п.), чтобы избежать дорогостоящих простоев и восстановлений.

Пятый приоритет — минимизировать урон, нанесенный телекоммуникационным системам ИТКС; во многих случаях лучше выключить систему или отсоединить ее от ИТКС, чем подвергать риску информацию, ПО или оборудование.

Поскольку управление инцидентами ИБ предполагает осуществление деятельности по их расследованию, то необходим сбор свидетельств инцидента ИБ, представленных в цифровой форме, и их сохранение (в первую очередь для обеспечения целостности) для последующего использования при судебном разбирательстве. Данные аспекты достаточно подробно изложены в следующих специализированных международных стандартах серии ISO 27000, что полностью

может быть применено при расследовании инцидентов ИБ, произошедших в ИТКС ОРГАНИЗАЦИИ:

- международный стандарт ISO/IEC 27037:2012 [182] и ГОСТ Р ИСО/МЭК 27037-2014 [183], которые содержат детальные руководящие указания по идентификации, сбору и/или получению из различных источников, пометке, хранению, транспортировке и сохранению свидетельств в цифровой форме;

- международный стандарт ISO/IEC 27041:2015 [128], который формулирует руководящие указания по обеспечению того, чтобы методы и процессы, используемые при расследовании инцидентов ИБ, соответствовали определенной для них цели;

- международный стандарт ISO/IEC 27042:2015 [129], который предоставляет руководящие указания по анализу и интерпретации свидетельств, представленных в цифровой форме, для обеспечения непрерывности, достоверности, воспроизводимости и повторяемости результатов расследования инцидентов ИБ;

- международный стандарт ISO/IEC 27043:2015 [130], который содержит руководящие принципы, основанные на идеализированных моделях для общих процессов расследования различных сценариев инцидентов ИБ с использованием свидетельств, представленных в цифровой форме.

Перечисленные стандарты определяют цели проведения расследования инцидентов ИБ, которые заключаются в получении и сохранении собранных свидетельств инцидентов ИБ в неприкосновенности, их проверке на неоспоримость и поддержке целостности носителей информации и самой информации, что при обращении в правоохранительные органы обеспечит уверенность в проведении всей аналитической работы с точными копиями исходных данных.

Мировой опыт показывает, что типовой процесс пост-анализа и расследования в компьютерных сетях включает в себя выполнение, например, следующих видов деятельности, которые могут быть в полном объеме реализованы и в случае инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ [168]:

- обеспечение защиты затронутых инцидентом ИБ элементов ИТКС от блокировки доступа к ним, внесения изменений или иной компрометации, включая внесение компьютерных вирусов, и обеспечение отсутствия или минимальности воздействия на их нормальное функционирование;

- назначение приоритетов сбора свидетельств, то есть рассмотрение их от наиболее к наименее изменчивым (что в значительной степени зависит от характера инцидента ИБ);

- идентификация всех необходимых для сбора сведений (например, различные файлы – обычные; кажущиеся удаленными, но не являющиеся таковыми; защищенные паролем; зашифрованные и т.п.);

- восстановление как можно бóльшего числа стертых файлов и других данных;
- раскрытие *IP*-адресов, имен хостов, сетевых маршрутов и информации веб-сайтов;
- извлечение содержимого скрытых, временных файлов и файлов подкачки, использованных как ПО ОС, так и как прикладным ПО;
- доступ к содержимому ПО защищенных или зашифрованных файлов (если это не запрещено законодательством);
- анализ всех возможно значимых данных, найденных в специальных (обычно, недоступных) областях памяти на дисках;
- анализ времен создания, доступа и изменения файла;
- анализ ЖРС систем, сервисов и приложений;
- определение деятельности пользователей и/или приложений по отношению к затронутым элементам ИТКС;
- анализ электронной почты на наличие полезной для расследования информации и ее содержания;
- проведение проверок целостности файлов для обнаружения файлов, содержащих «троянского коня», и файлов, изначально отсутствовавших в системе;
- по возможности, анализ физических доказательств (например, отпечатков пальцев), результатов видеонаблюдения, ЖРС системы сигнализации и доступа по пропускам и опрос свидетелей;
- обработка и хранение собранных потенциальных свидетельств таким образом, чтобы избежать их повреждения, приведения в негодность и предотвращения просмотра конфиденциальных материалов неавторизованными лицами;
- получение выводов о причинах инцидента ИБ, необходимых действиях и времени их выполнения с приведением свидетельств, включая список соответствующих файлов, прикладываемых в приложениях к главному отчету;
- обеспечение экспертной поддержки для любого дисциплинарного или правового действия (при необходимости) и т.п.

Как было отмечено выше, информация, которую собирают для расследования в цифровой форме, бывает двух типов: постоянная и временная [184, 185].

Постоянная информация хранится на жестком диске компьютера или другом типе носителей информации (например, *USB*-накопители, *flash*-карты, *CD-ROM*, внешние жесткие диски) и не теряется в случае его перезагрузки или выключения. Примерами таких свидетельств являются различные документы, сообщения электронной почты и удаленные файлы, находящиеся в корзине. Это также системные файлы, включая настройки параметров базовой системы ввода/вывода (*BIOS*), загрузочные записи, ЖРС (включая системные журналы), системный реестр,

временные файлы, включая .tmp-файлы и спул-файлы, следы веб-активности, источниками которых могут быть закладки, *cookie*-файлы, журнал посещенных *URL*, временные интернет-файлы и другие файлы, например, удаленные, фрагментированные, скрытые, неиспользованное пространство, файлы подкачки и т.п. Исследование постоянной информации часто не сложный процесс – большая часть пользователей умеет искать файлы, смотреть, какие сайты в интернете были посещены, а также выявлять наличие вредоносных программ. Но нахождение скрытой постоянной информации и умение сопоставлять с первого взгляда не имеющие ничего общего события, записи, файлы требует определенных навыков и знаний.

Временная информация хранится в системной памяти (системном реестре, оперативной памяти, кэше) и теряется в случае перезагрузки или выключения компьютера; поэтому ее исследуют в первую очередь. Временная сетевая информация содержит сведения о текущей сетевой конфигурации системы, вовлеченной в инцидент ИБ, например, открытые соединения, очередь запросов на установление сетевых соединений, открытые *TCP/UDP*-порты, маршрутная информация и ее конфигурация, статус сетевого интерфейса и его конфигурация. Временная системная информация показывает текущую конфигурацию и текущее состояние системы, вовлеченной в инцидент ИБ. Примеры такой информации: системный профиль (дает информацию о текущей конфигурации системы, вовлеченной в инцидент ИБ), текущая системная дата и время, история команд (включает в себя список недавно запущенных команд как локальными, так и удаленными пользователями), время, прошедшее с момента последней перезагрузки системы (укажет на наличие/отсутствие временной информации, созданной во время инцидента ИБ), запущенные процессы (среди них могут находиться нетипичные, а, возможно, и вредоносные), образы программ, которые были удалены с носителей, но все еще активны в оперативной памяти, открытые файлы, информация в буфере обмена, подключенные пользователи, программные модули, загруженные в области виртуальной памяти, зарезервированные для ядра ОС, *DLL*-файлы или совместно используемые библиотеки (для изучения, насколько законно их использование) и т.п.

Особо подчеркнем, что при проведении расследования инцидента ИБ в ИТКС ОРГАНИЗАЦИИ любое исследование затронутых инцидентом ИБ систем может привести к изменению свидетельств и сделает этот процесс нерезультативным. В случае сбора временной информации может измениться, например, время последнего доступа к файлам и даже произойти перезагрузка компьютера и, как следствие, потеря важных данных. Любое средство для сбора данных, запущенное на уровне пользователя или ядра ОС, естественным образом изменяет состояние исследуемой системы – создается как минимум один процесс, который может быть записан в область, где до этого хранились данные, возможно имеющие доказательное значение. При создании нового процесса менеджер памяти ОС резервирует для него область памяти. При

этом данные, которые находились в этот момент в свободной области памяти или в области подкачки файловой системы, могут быть перезаписаны данными нового процесса. Поэтому предотвращение внесения изменений в исследуемую систему при сборе свидетельств инцидента ИБ – это первая из задач, которая может быть решена с помощью применения различных техник и соответствующих инструментальных средств. Все названные вопросы достойны отдельного научного исследования, выходящего за установленные в начале границы данного исследования.

На рис. 32 наглядно показаны типичные действия до и после идентификации инцидента ИБ с точки зрения классов процесса, как они описаны в ISO/IEC 27043:2015 [130], и мероприятий, осуществляемых в рамках процесса, согласно ISO/IEC 27035-2:2016 [127], ISO/IEC 27037:2012 [182] и ГОСТ Р ИСО/МЭК 27037-2014 [183], ISO/IEC 27041:2015 [128] и ISO/IEC 27042:2015 [129]. Причем классы и мероприятия изображены таким образом, чтобы была понятна их взаимосвязь [68], что важно при разработке всей деятельности в рамках ПУИИБ для ИТКС ОРГАНИЗАЦИИ.

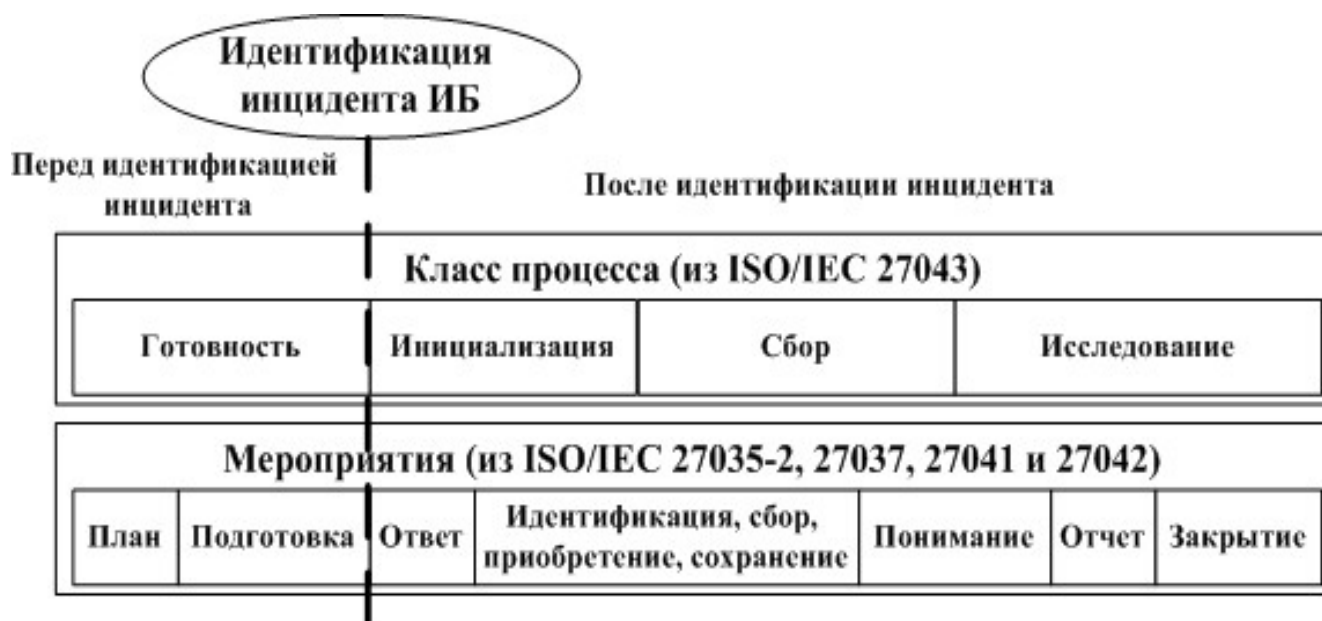


Рисунок 32 – Деятельность в рамках процесса управления инцидентами ИБ для ИТКС

Готовность к идентификации и реагированию на инцидент ИБ должна опираться на заранее продуманный план действий и всестороннюю подготовку к этому событию. После идентификации инцидента ИБ в ИТКС в ответ активируется соответствующий план и инициализируется реагирование на инцидент ИБ. Во время реагирования на инциденты ИБ идет активный сбор всех свидетельств, приобретение всех необходимых технических и другие вспомогательных средств для обеспечения быстрого реагирования, а также сохранение всех собранных сведений, поскольку они могут потребоваться для последующего судебного разбирательства. Еще

при их сборе приходит понимание сути инцидента ИБ, причин возникновения, возможных нарушителей ИБ и т.п., что часто требует сбора дополнительных уточняющих сведений, исследования и, возможно, новых инструментальных средств для этого. После того, как достигнуто понимание инцидента ИБ и осуществлено реагирование на него, необходимо составить о нем детальные отчеты и произвести его закрытие.

3.4.4. Требования к разрабатываемому процессу управления инцидентами информационной безопасности

Основная цель разрабатываемого в рамках данного исследования ПУИИБ для ИТКС ОРГАНИЗАЦИИ – обеспечение использования последовательного и рационального подхода к управлению инцидентами ИБ, включая информирование о событиях ИБ и проблемах в обеспечении ИБ. Поэтому разрабатываемый процесс должен удовлетворять семи требованиям к процессу управления инцидентами ИБ в ИТКС ОРГАНИЗАЦИИ, предъявляемым в пункте А.16 международного стандарта ISO/IEC 27001:2013 [124] (аналогичный гармонизированный российский стандарт пока не принят Федеральным агентством по техническому регулированию и метрологии (Росстандартом) России), а именно:

1) А.16.1.1 «Обязанности и процедуры» – для обеспечения быстрого, результативного и упорядоченного реагирования на инциденты ИБ в ИТКС должны быть установлены обязанности и процедуры управления в рамках СОИБ ИТКС в целом и СУИБ ИТКС в частности;

2) А.16.1.2 «Сообщение о событиях ИБ» – о событиях ИБ в ИТКС должны быть как можно быстрее проинформированы все причастные стороны по соответствующим каналам связи;

3) А.16.1.3 «Сообщение о проблемах в обеспечении ИБ» – сотрудники и подрядчики, использующие ИС и ИТ-услуг ИТКС, должны отмечать и сообщать о любых наблюдаемых или предполагаемых проблемах в обеспечении ИБ в этих системах или услугах ИТКС;

4) А.16.1.4 «Оценка и принятие решения о событиях ИБ» – каждое событие ИБ в ИТКС должно быть всесторонне оценено и в соответствии с Политикой ИБ ОРГАНИЗАЦИИ должно быть принято решение о том, классифицировать ли данное событие ИБ как инцидент ИБ или нет;

5) А.16.1.5 «Реагирование на инциденты ИБ» – на все инциденты ИБ в ИТКС необходимо реагировать в круглосуточном режиме в соответствии с их критичностью в допустимый для реагирования временной интервал в строгом соответствии с документированными процедурами ОРГАНИЗАЦИИ;

6) А.16.1.6 «Изучение инцидентов ИБ» – знания, полученные в результате анализа и

разрешения каждого инцидента ИБ, должны использоваться для снижения вероятности или последствий или и того и другого одновременного в отношении возможных будущих инцидентов ИБ в ИТКС;

7) А.16.1.7 «Сбор свидетельств» – ОРГАНИЗАЦИЯ должна определить и применять процедуры идентификации, сбора, понимания и сохранения всей информации, которая в дальнейшем может служить свидетельством при служебном расследовании или судебном разбирательстве правоохранительными органами в соответствии с требованиями Законодательства РФ.

Опустив первое требование «Обязанности и процедуры», получим, что в поддержку ПУИИБ для ИТКС ОРГАНИЗАЦИИ необходимо реализовать следующие семь основных взаимосвязанных процессов (рис. 31):

1) обнаружение уязвимостей, событий ИБ и инцидентов ИБ (определяет порядок их выявления; в рамках разрабатываемого процесса обнаружение уязвимости может рассматриваться как самостоятельное событие ИБ);

2) оповещение об уязвимостях, событиях ИБ и инцидентах ИБ (в соответствии с А.16.1.2 и А.16.1.3);

3) обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ (в соответствии с А.16.1.4) (включает в себя сортировку, определение типа события, определение типа и степени серьезности инцидента ИБ (если событие ИБ признается таковым) и т.д.);

4) реагирование на инциденты ИБ (в соответствии с А.16.1.5);

5) анализ инцидентов ИБ (в соответствии с А.16.1.6) (с целью выявления причин, источников, оценки ущерба и т.п.; более простой по сравнению с расследованием, поскольку не требует столь детальной и скрупулезной работы);

6) расследование инцидентов ИБ (в соответствии с А.16.1.7) (требует участия сотрудников отдела кадров, юристов, технических экспертов ИТ-систем, внешних консультантов по ИБ, бизнес-менеджеров, конечных пользователей ИС, сотрудников служб технической поддержки, сотрудников службы безопасности и др.);

7) определение опыта, извлеченного из инцидентов ИБ и обнаруженных уязвимостей, а также регулярно выполняемый анализ эффективности (в первую очередь результативности в ранее определенном смысле) ПУИИБ, результаты которого должны передаваться в процессы «Мониторинг эффективности СУИБ ИТКС», «Анализ функционирования СУИБ ИТКС высшим руководством ОРГАНИЗАЦИИ» и «Анализ рисков ИБ ИТКС».

Рис. 33 показывает, что в рамках ПУИИБ организация должна определять и управлять различными действиями, и часто выходные данные одного процесса непосредственно представляют входные данные для следующего процесса [47, 186]. Например, данные, полученные в результате реагирования на инцидент ИБ, являются входными для процессов анализа и рассле-

дования данного инцидента. Такой подход акцентирует внимание на достижении поставленных целей, а также на ресурсах, затраченных на достижения целей.



Рисунок 33 – Высокоуровневая диаграмма процесса управления инцидентами ИБ для ИТКС ОРГАНИЗАЦИИ

3.4.5. Формализация разработанного процесса управления инцидентами информационной безопасности

При разработке отдельных процессов в рамках обобщенного ПУИИБ использовался метод составления карт процессов [47, 186], который позволяет наглядно увидеть последовательность всех действий и взаимозависимости между ними, а также оптимизировать (в смысле принять рациональные решения об улучшениях или изменениях) уже разработанные процессы путем отслеживания избыточных действий и выявления рисков их успешной реализации. Чаще всего этот метод применяется для процессов, одним из важных показателей которых является время выполнения, как в случае с требуемой быстротой реагирования на инциденты ИБ в ИТКС ОРГАНИЗАЦИИ, и когда процесс надо изобразить в координатах двух его параметров (например, исполнители и время). Следовательно, использование данного подхода件лезно как при построении новых, так и при пересмотре, доработке и оценке результативности и эффективности уже эксплуатируемых процессов. Его можно применять для построения любых процессов

обеспечения и управления ИБ, а не только для ПУИИБ.

Разработанные карты процессов ПУИИБ включают в себя диаграмму и описание процесса [47, 186]. При этом указывается следующая информация: действия (операции), предпринимаемые в рамках процесса; особые условия выполнения (если они есть); точки взаимодействия; взаимозависимости; роли, обязанности и ответственность; ресурсы (материальные, технические, людские, информационные и пр.); документы, устанавливающие требования; способы мониторинга; создаваемая отчетность.

Диаграмма отдельного процесса в рамках обобщенного ПУИИБ наглядно отображает весь процесс в целом от начала до завершения и полезна для его анализа. Правила интерпретации диаграмм таковы: их чтение осуществляется слева направо; линии и стрелки обозначают переход (только в направлении стрелки) между различными действиями в последовательности действий или окончание какой-либо из последовательностей действий; каждый блок диаграммы при необходимости может быть детализирован (разложен на составляющие, описывающие действие более детально).

На подобных диаграммах, как правило, отображаются три сущности: роли – участники процесса; обязанности – задания, за которые ответственны участники процесса; маршруты – последовательность действий в рамках работы процесса, точки принятия решений, точки взаимодействия с другими процессами ПУИИБ.

К сожалению, диаграммы не предоставляют достаточно полной информации об использовании процесса. Поэтому было решено расширить данный подход, добавив к нему таблицы–описания процессов, предоставляющие дополнительные сведения о каждом из них, включая управление им, процедуры, которым необходимо следовать, триггеры (события или входные данные, в результате которых запускается процесс), критерии выполнения и т.д. Таким образом, диаграммы совместно с таблицами содержат значительный объем сведений о процессах ПУИИБ, который может быть использован для проведения анализа рисков ИБ и оценки их результативности и эффективности.

Далее последовательно приведены разработанные диаграммы и описания процесса «Обнаружение и оповещение об уязвимостях, событиях ИБ и инцидентах ИБ» (рис. 34 и табл. 8) [47, 186], процесса «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ» (рис. 35 и табл. 9), процесса «Реагирование на инциденты ИБ» (он как самый «объемный» из процессов ПУИИБ был логически разделен для наглядности представления диаграмм процессов на две составляющие: «Реагирование на инциденты ИБ – Первоначальные действия» (рис. 36 и табл. 10) и «Реагирование на инциденты ИБ – Продолжение» (рис. 37 и табл. 11), процесса «Анализ инцидентов ИБ» (рис. 38 и табл. 12) и процесса «Расследование инцидентов ИБ» (рис. 39 и табл. 13).



Рисунок 34 – Диаграмма обобщенного процесса «Обнаружение и оповещение об уязвимостях, событиях ИБ и инцидентах ИБ»

Таблица 8 – Описание обобщенного процесса «Обнаружение, оповещение и обработка сообщений об уязвимостях, событиях ИБ и инцидентах» (начало)

Цели процесса	Триггеры	Критерии выполнения	Процедуры и правила
Выявлять нетипичные (подозрительные) события, которые могут повлечь нарушение политики ИБ, либо ранее неизвестные ситуации, которые могут быть существенными для безопасности.	Возникновение потенциально влияющих на ИБ событий или нетипичных ситуаций; Получение сообщений от ЖРС ОС, СУБД, СЗИ, систем жизнеобеспечения и т.д.; Получение результатов мониторинга уязвимостей.	Принятие решения о дальнейших действиях с событием (например, передать его на классификацию); Передача выходных данных на вход следующему процессу.	«Положение о ролях ПУИИБ»; «Памятка сотрудника по ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ (в т.ч. Политика ИБ).

Таблица 8 – Описание обобщенного процесса «Обнаружение, оповещение и обработка сообщений об уязвимостях, событиях ИБ и инцидентах» (продолжение)

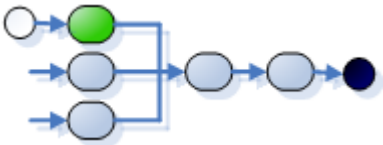
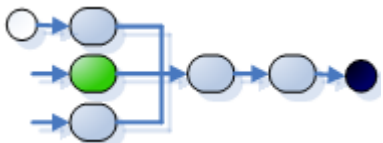
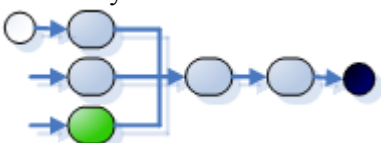
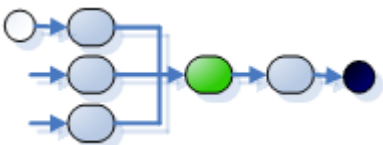
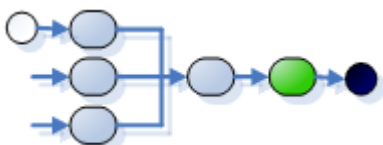
Входные данные	Описание		Форма
Информация о событии, потенциально относящемся к ИБ.	Любая информация о событиях или ситуациях, которые потенциально могут иметь отношение к ИБ.		Любая форма представления.
Информация о потенциальном событии, которое может иметь отношение к ИБ.	Любая информация об условиях , благоприятных для возникновения событий или ситуаций, которые потенциально могут иметь отношение к ИБ.		Любая форма представления.
Результаты мониторинга уязвимостей.	Выходные данные процесса «Управление уязвимостями ИТКС». В случае отсутствия такого процесса результаты проведения периодического анализа защищенности ИТКС ОРГАНИЗАЦИИ.		Отчет о результатах сканирования и мониторинга уязвимостей.
Принятие решения	Выходные данные	Описание	Форма
Передача на вход процессу «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ».	Сообщение об уязвимости, событии ИБ или инциденте ИБ.	Информация, которая должна быть передана на вход процессу «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ».	Документированное сообщение в электронном или бумажном виде.
Подпроцесс	Требования к подпроцессу	Процедуры и правила	Роли
Выявление событий ИБ 	Все пользователи организации, а также подрядчики и пользователи из сторонних организаций, имеющие доступ к ИТКС ОРГАНИЗАЦИИ участвуют в выявлении подозрительных или потенциально относящихся к безопасности событий и ситуаций. Входы: Признаки подозрительных событий и ситуаций из разных источников. Выходы: Информация о событии.	«Положение о ролях ПУИИБ»; «Памятка сотрудника по ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ (включая Политику ИБ).	Все пользователи организации, включая всех сотрудников организации, подрядчиков, пользователей из внешних организаций, имеющих доступ к ИТКС ОРГАНИЗАЦИИ.
Выявление потенциальных событий ИБ 	Все пользователи организации, а также подрядчики и пользователи из сторонних организаций, имеющие доступ к ИТКС ОРГАНИЗАЦИИ участвуют в выявлении ситуаций, которые потенциально могут привести к событию ИБ или инциденту ИБ. Входы: Признаки потенциальных событий ИБ. Выходы: Информация о потенциальном событии ИБ.	«Положение о ролях ПУИИБ»; «Памятка сотрудника по ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ (включая Политику ИБ).	Все пользователи организации, включая всех сотрудников организации, подрядчиков, пользователей из внешних организаций, имеющих доступ к ИТКС ОРГАНИЗАЦИИ.

Таблица 8 – Описание обобщенного процесса «Обнаружение, оповещение и обработка сообщений об уязвимостях, событиях ИБ и инцидентах» (окончание)

Анализ результатов мониторинга уязвимостей 	Ответственные сотрудники (сотрудники подразделения, ответственного за поддержание ИТКС) осуществляют анализ результатов сканирования и мониторинга уязвимостей ИТКС (анализ результатов анализа защищенности ИТКС) и выявляют уязвимости ИТКС ОРГАНИЗАЦИИ. Входы: Отчеты о результатах сканирования и мониторинга уязвимостей. Выходы: Информация об уязвимостях.	«Положение о ролях ПУИИБ»; «Памятка сотрудника по ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по (включая документацию по процессу «Управление уязвимостями»).	Эксперты.
Оповещение об уязвимостях, событиях ИБ или инцидентах ИБ 	Все пользователи организации, а также подрядчики и пользователи из сторонних организаций, имеющие доступ к ИТКС ОРГАНИЗАЦИИ сообщают обо всех ставших им известными событиях ИБ, потенциальных событиях ИБ и об уязвимостях ИБ. Входы: Информация о событии ИБ. Информация о потенциальном событии ИБ. Информация об уязвимостях. Выходы: Сообщение о уязвимости, событии ИБ или инциденте ИБ.	«Положение о ролях ПУИИБ»; «Памятка сотрудника по ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ (включая Политику ИБ).	Все пользователи организации, включая всех сотрудников организации, подрядчиков, пользователей из внешних организаций, имеющих доступ к ИТКС ОРГАНИЗАЦИИ.
Получение сообщения об уязвимости, событии ИБ или инциденте ИБ 	Ответственные сотрудники получают информацию о событиях ИБ, потенциальных событиях ИБ, об инцидентах ИБ или об уязвимостях. Затем они документируют (либо в электронном, либо в бумажном виде) полученные сообщения и передают их на вход процессу «Обработка сообщений об уязвимостях, событиях и инцидентах ИБ». Входы: Сообщение о уязвимости, событии ИБ или инциденте ИБ. Выходы: Документированное сообщение о уязвимости, событии ИБ или инциденте ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ».	Менеджер СУИБ.

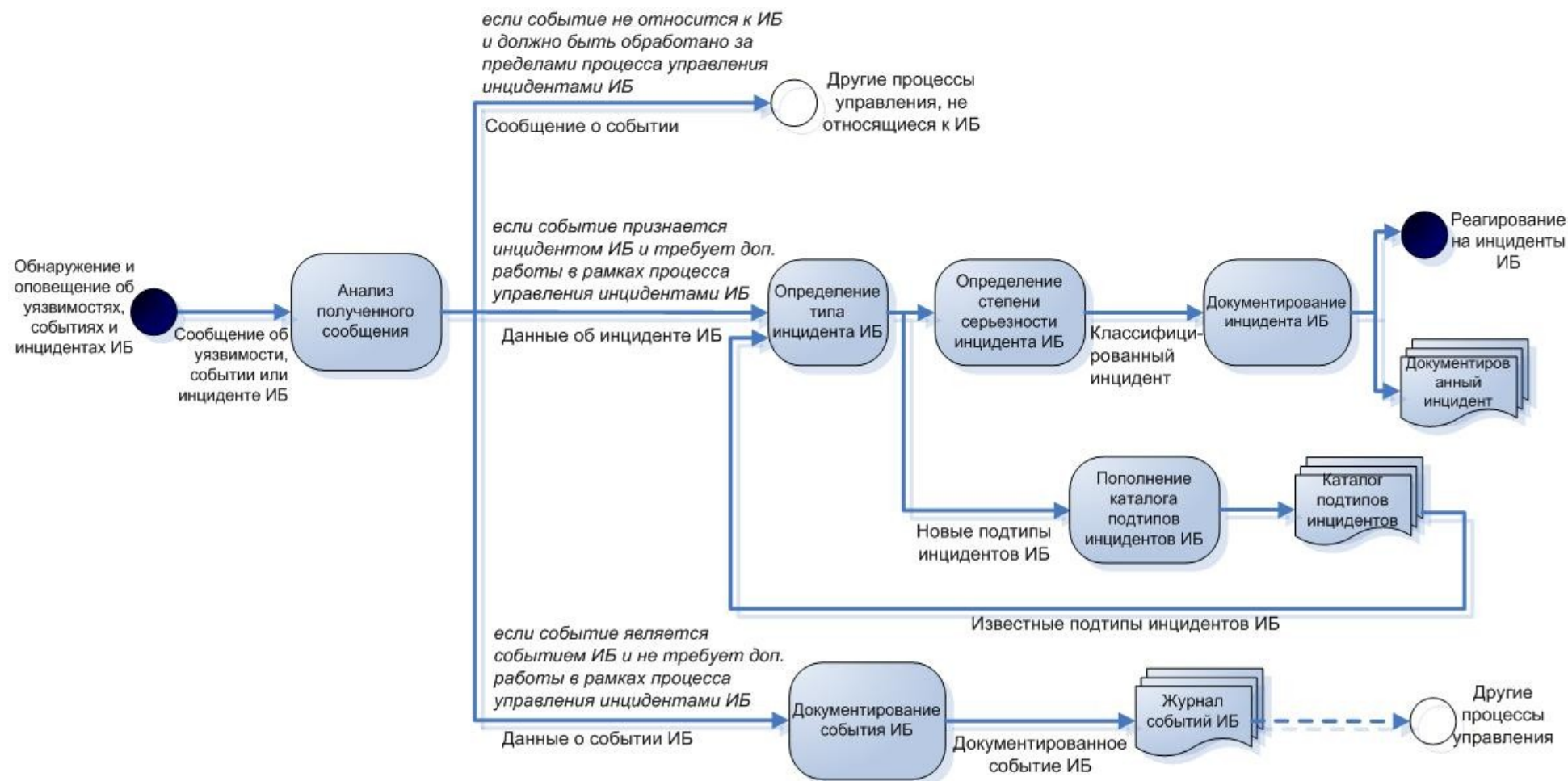


Рисунок 35 – Диаграмма процесса «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ»

Таблица 9 – Описание процесса «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ» (начало)

Цели процесса	Триггеры	Критерии выполнения	Процедуры и правила
Анализировать получаемые сообщения о событиях ИБ и в случае необходимости перенаправлять их соответствующим сотрудникам для дальнейшей обработки.	Получение сообщения об уязвимости, событии ИБ или инциденте ИБ.	События классифицированы и переданы на вход другим процессам (например, процессу «Реагирование на инциденты ИБ»).	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.
Входные данные	Описание		Форма
Документированное сообщение об уязвимости, событии ИБ или инциденте ИБ.	Выходные данные процесса «Обнаружение и оповещение об уязвимостях, событиях ИБ или инцидентах ИБ».		Документированное сообщение в электронном или бумажном виде.
Принятие решения	Выходные данные	Описание	Форма
Если событие не относится к ИБ и должно быть передано в другие процессы управления для дальнейшей обработки.	Сообщение о событии, не относящемся к ИБ.	Включает в себя всю информацию о передаваемом в другой процесс событии.	Документированное событие в электронном или бумажном виде.
Если событие признается инцидентом ИБ и требует дополнительной работы в рамках ПУИИБ.	Документированный инцидент ИБ.	Включает в себя всю информацию об инциденте ИБ, которая затем передается на вход процессу «Реагирование на инциденты ИБ».	Документированный инцидент ИБ в электронном или бумажном виде.
Если событие является событием ИБ и не требует дополнительной работы в рамках ПУИИБ.	Документированное событие ИБ.	Включает в себя всю информацию о закрываемом событии ИБ.	Документированное событие ИБ в электронном или бумажном виде.

Таблица 9 – Описание процесса «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ» (продолжение)

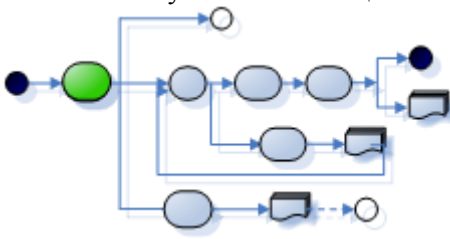
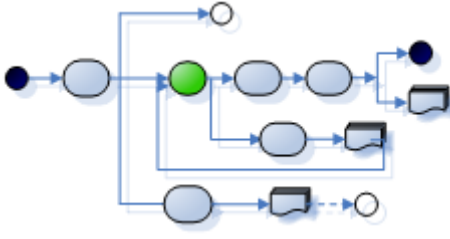
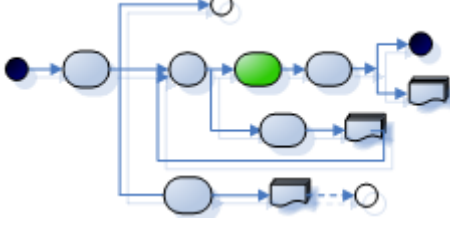
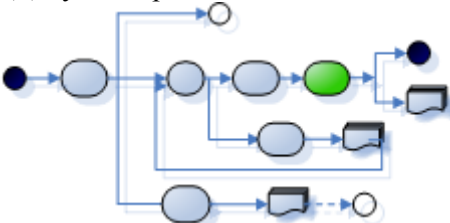
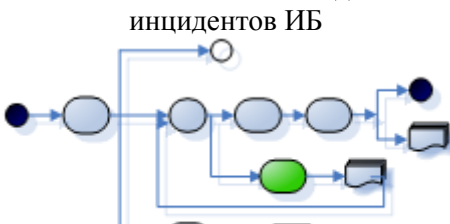
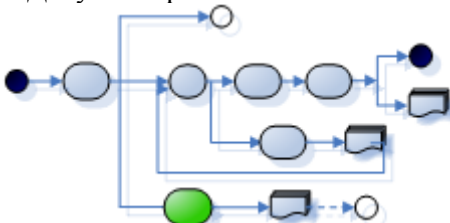
Подпроцесс	Требования к подпроцессу	Процедуры и правила	Роли
Анализ полученного сообщения 	Ответственные сотрудники проводят анализ полученного сообщения и определяют является ли выявленное событие: событием ИБ; событием, не относящимся к ИБ; или инцидентом ИБ (в соответствии с перечнем). Входы: Документированное сообщение об уязвимости, событии ИБ или инциденте ИБ. Выходы: Документированное сообщение о событии, не относящемся к безопасности ИЛИ Документированное сообщение о событии ИБ ИЛИ Документированное сообщение об инциденте ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Перечень событий ИБ, признаваемых инцидентами ИБ»; Другие документы по ИБ в рамках организации.	Менеджер СУИБ.
Определение типа инцидента ИБ 	Ответственные сотрудники проводят анализ сообщения об инциденте ИБ и определяют к какому из типов инцидентов относится данный инцидент: Административные, Программно-технические, Физической охраны, Процессов жизнеобеспечения здания. Входы: Документированное сообщение об инциденте ИБ. Классификатор (каталог подтипов) инцидентов ИБ. Выходы: Документированное сообщение об инциденте ИБ с определением типа инцидента.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Классификатор инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Менеджер СУИБ.
Определение степени серьезности инцидента ИБ 	Ответственные сотрудники проводят анализ сообщения об инциденте ИБ и определяют степень серьезности данного инцидента ИБ. Входы: Документированное сообщение об инциденте ИБ с определением типа инцидента. Выходы: Документированное сообщение об инциденте ИБ с определением типа инцидента и степени его серьезности.	Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Реестр рисков ИБ для ИТКС»; Другие документы по ИБ в рамках организации.	Менеджер СУИБ.

Таблица 9 – Описание процесса «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ» (окончание)

Документирование инцидента ИБ 	Ответственные сотрудники проводят документирование инцидента ИБ в установленной в рамках ПУИИБ форме. Входы: Документированное сообщение об инциденте ИБ с определением типа инцидента и степени его серьезности. Выходы: Документированный инцидент ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.	Менеджер СУИБ.
Пополнение каталога подтипов инцидентов ИБ 	Ответственные сотрудники пополняют Каталог подтипов инцидентов ИБ в случае, если при определении типа инцидента был выявлен новый подтип инцидента ИБ ранее неизвестный. Входы: Данные о новом подтипе инцидента ИБ. Выходы: Обновленный Каталог подтипов инцидентов ИБ.	Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Классификатор инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Менеджер СУИБ.
Документирование события ИБ 	Ответственные сотрудники проводят документирование события ИБ в установленной в рамках ПУИИБ форме, пополняя ЖРС, который затем может быть передан в другие процессы управления для анализа. Входы: Документированное сообщение о событии ИБ. Выходы: Документированное событие ИБ.	Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.	Менеджер СУИБ.

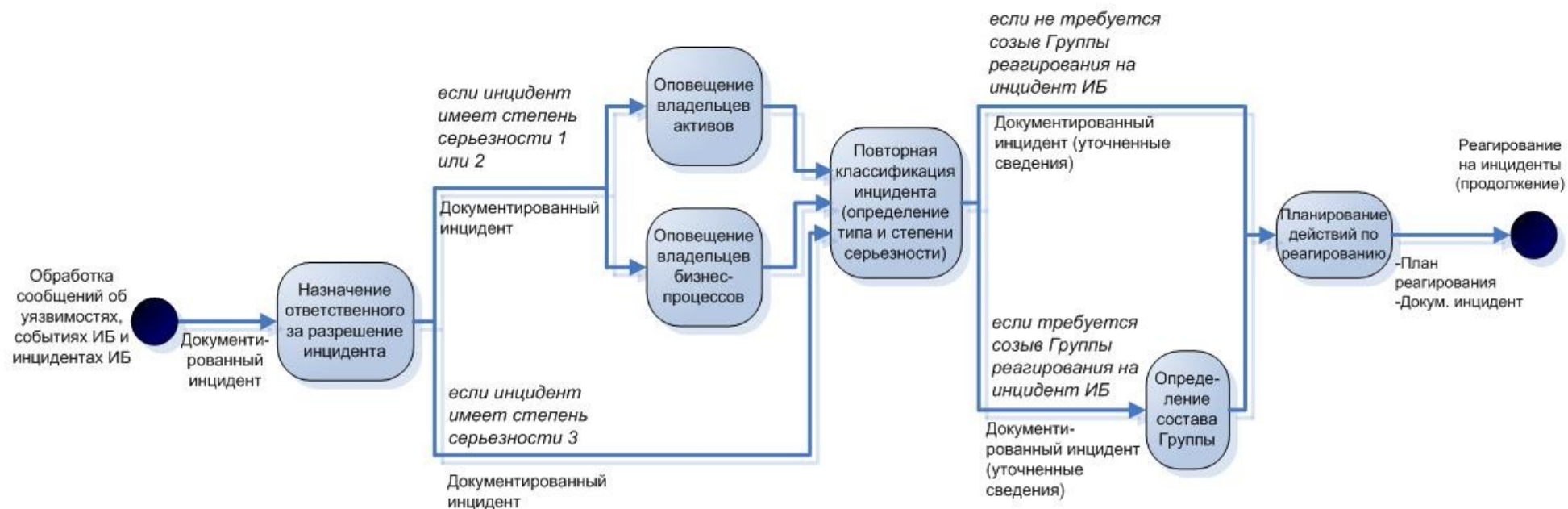


Рисунок 36 – Диаграмма процесса «Реагирование на инциденты ИБ – Первоначальные действия»

Таблица 10 – Диаграмма процесса «Реагирование на инциденты ИБ – Первоначальные действия» (начало)

Цели процесса	Триггеры	Критерии выполнения	Процедуры и правила
Осуществление первоначальных действий по разрешению инцидентов ИБ.	Получение документированных инцидентов ИБ.	Разработка Плана мероприятий по реагированию на инцидент ИБ и антикризисных действий.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.

Таблица 10 – Диаграмма процесса «Реагирование на инциденты ИБ – Первоначальные действия» (продолжение)

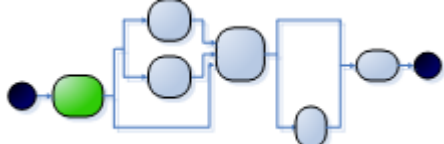
Входные данные	Описание		Форма
Документированный инцидент ИБ.	Включает в себя все данные по инциденту ИБ в том числе тип инцидента и степень его серьезности.		Заполненная форма документирования инцидента в электронном или бумажном виде.
Принятие решения	Выходные данные	Описание	Форма
Требуется реагирование на инцидент ИБ.	Документированный инцидент ИБ.	Включает в себя все данные по инциденту ИБ, в том числе уточненные тип инцидента ИБ и степень его серьезности.	Заполненная форма документирования инцидента ИБ в электронном или бумажном виде.
Требуется реагирование на инцидент ИБ.	План действий по реагированию на инцидент ИБ.	Включает в себя последовательность действий, которые должны быть предприняты для разрешения инцидента ИБ. Для инцидентов степени серьезности 1 и 2 разрабатывается более подробный план мероприятий.	Электронный или бумажный вид.
Подпроцесс	Требования к подпроцессу	Процедуры и правила	Роли
Назначение Ответственного за разрешение инцидента ИБ 	Исходя из типа инцидента, осуществляется назначение ответственного за разрешение инцидента ИБ, который в зависимости от степени серьезности инцидента либо самостоятельно осуществляет реагирование на инцидент, либо руководит ГРИИБ. Входы: Документированный инцидент ИБ. Выходы: Документированный инцидент ИБ, закрепленный за Ответственным за разрешение инцидента ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.	Менеджер СУИБ.

Таблица 10 – Диаграмма процесса «Реагирование на инциденты ИБ – Первоначальные действия» (продолжение)

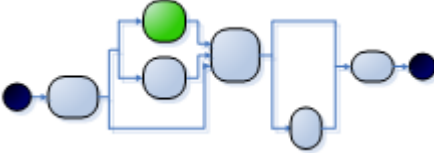
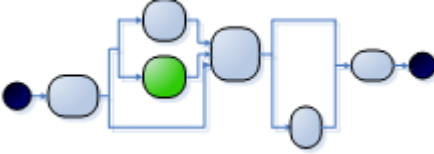
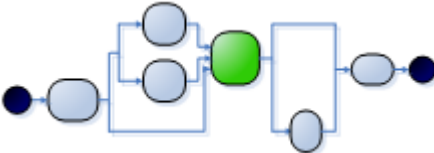
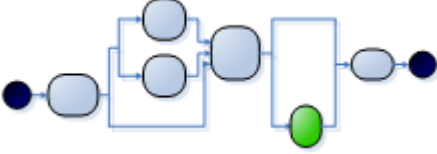
Оповещение владельцев активов 	В случае если инцидент имеет степень серьезности 1 или 2 (в соответствии с введенной в рамках процесса классификацией степеней серьезности инцидентов) осуществляется оповещение Владелец активов, вовлеченный в данный инцидент ИБ. Входы: Документированный инцидент ИБ. Выходы: Документированный инцидент ИБ. Оповещение Владелец активов, вовлеченный в инцидент ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Реестр активов ИТКС»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ.
Оповещение владельцев бизнес-процессов 	В случае если инцидент имеет степень серьезности 1 или 2 (в соответствии с введенной в рамках процесса классификацией степеней серьезности инцидентов) осуществляется оповещение Владелец бизнес-процессов, вовлеченный в данный инцидент ИБ, или бизнес-процессов, на которые оказывается негативное влияние в результате инцидента ИБ. Входы: Документированный инцидент ИБ. Выходы: Документированный инцидент ИБ. Оповещение Владелец бизнес-процессов.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Реестр активов ИТКС»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ.
Повторная классификация инцидента ИБ (определение типа и степени серьезности инцидента ИБ) 	После оповещения владельцев активов и бизнес-процессов, вовлеченный в инцидент (в случае если инцидент имеет степень серьезности 1 или 2) и, возможно, получения дополнительной информации по инциденту – осуществляется повторная классификация инцидента (определение типа и степени серьезности инцидента ИБ) с целью уточнения первоначальной классификации и определения контролируемости инцидента ИБ. Входы: Документированный инцидент ИБ. Выходы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Классификатор инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ.

Таблица 10 – Диаграмма процесса «Реагирование на инциденты ИБ – Первоначальные действия» (окончание)

Определение состава ГРИИБ 	В случае если инцидент имеет высокую степень серьезности, является сложным или имеет широкий масштаб, то может потребоваться созыв ГРИИБ. В этом случае необходимо определить состав ГРИИБ. Входы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. Выходы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. Информация о составе ГРИИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ.
Планирование действий по реагированию 	На основе анализа данных об инциденте ИБ осуществляется планирование действий по реагированию на инцидент ИБ. Для инцидентов степени серьезности 1 и 2 разрабатывается более подробный план мероприятий. Для инцидентов степени серьезности 3, как правило, применимы типовые решения по реагированию на инциденты. Входы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. Возможно, Информация о составе ГРИИБ. Выходы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. План мероприятий по реагированию на инцидент ИБ и антикризисных действий.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ; Члены ГРИИБ.

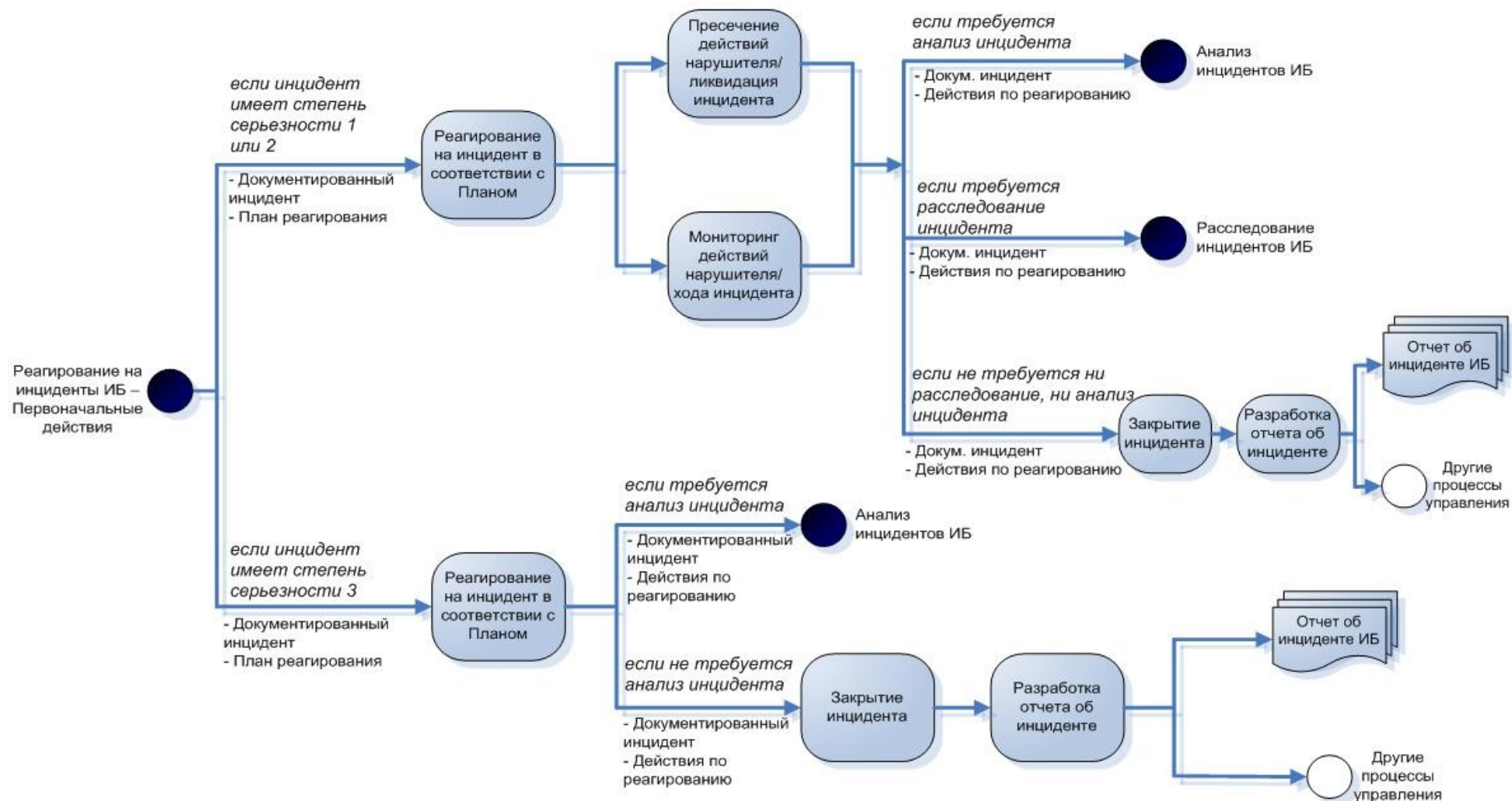


Рисунок 37 – Диаграмма процесса «Реагирование на инциденты ИБ – Продолжение»

Таблица 11 – Описание процесса «Реагирование на инциденты ИБ – Продолжение» (начало)

Цели процесса	Триггеры	Критерии выполнения	Процедуры и правила
Разрешить инциденты ИБ.	Получение документированных инцидентов ИБ и планов реагирования на них в качестве входных данных.	Успешное завершение всех запланированных действий по реагированию на инцидент ИБ и устранению его последствий (или сверх запланированных).	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; Другие документы по ИБ в рамках организации.
Входные данные	Описание		Форма
Документированный инцидент ИБ.	Включает в себя все данные по инциденту ИБ, в том числе уточненные тип инцидента и степень его серьезности.		Заполненная форма документирования инцидента в электронном или бумажном виде.
План действий по реагированию на инцидент ИБ.	Включает в себя последовательность действий, которые должны быть приняты для разрешения инцидента ИБ. Для инцидентов степени серьезности 1 и 2 разрабатывается более подробный план мероприятий.		Электронный или бумажный вид.
Принятие решения	Выходные данные	Описание	Форма
Передается в качестве входных данных в процессы «Анализ инцидентов ИБ» или «Расследование инцидентов ИБ» (если есть необходимость).	Документированный инцидент ИБ.	Включает в себя все данные по инциденту ИБ, в том числе уточненные тип инцидента и степень его серьезности.	Заполненная форма документирования инцидента в электронном или бумажном виде.
Передается в качестве входных данных в процессы «Анализ инцидентов ИБ» или «Расследование инцидентов ИБ».	Документированные действия, принятые в рамках реагирования на инцидент ИБ.	Включает в себя все данные о действиях, предпринятых в рамках реагирования на инцидент ИБ.	Электронный или бумажный вид.
Дополнительная работа по инциденту ИБ не требуется.	Отчет об инциденте ИБ.	Включает в себя все данные по инциденту ИБ, в том числе уточненные тип инцидента ИБ и степень его серьезности, а также все данные о действиях, предпринятых в рамках реагирования на инцидент ИБ.	Заполненная форма Отчета об инциденте ИБ в электронном или бумажном виде.

Таблица 11 – Описание процесса «Реагирование на инциденты ИБ – Продолжение» (продолжение)

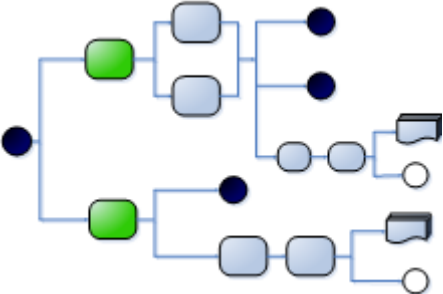
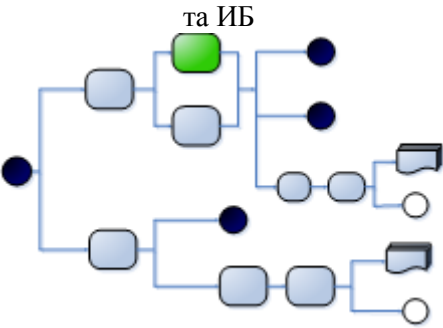
Подпроцесс	Требования к подпроцессу	Процедуры и правила	Роли
Реагирование на инцидент ИБ в соответствии с Планом реагирования 	В зависимости от степени серьезности и сложности инцидента ИБ выбирается одна из последовательностей действий в рамках данного процесса. Однако реагирование осуществляется в соответствии с разработанным Планом реагирования на инцидент ИБ, включая запуск при необходимости антикризисных действий. Входы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. План мер по реагированию на инцидент ИБ и антикризисных действий. Выходы: Информация о предпринятых действиях по реагированию (включая принятые решения, записи).	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «План мер по реагированию на инцидент ИБ и антикризисных действий»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ; Члены ГРИИБ.
Пресечение действий нарушителя/локализация и ликвидация инцидента ИБ 	В случае если инцидент имеет степень серьезности 1 или 2 возможны два варианта развития событий, один из которых – Пресечение действий нарушителя/локализация и ликвидация инцидента ИБ (включая, например, временную остановку работы отдельных элементов ИТКС) с целью прекращения НСД со стороны нарушителя или ликвидации инцидента ИБ, а второй – введение антикризисных действий. Входы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. План мер по реагированию на инцидент ИБ и . Информация о предпринятых действиях по реагированию (включая принятые решения, записи). Выходы: Информация о предпринятых действиях по реагированию (включая принятые решения, записи).	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «План мер по реагированию на инцидент ИБ и антикризисных действий»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ; Члены ГРИИБ.

Таблица 11 – Описание процесса «Реагирование на инциденты ИБ – Продолжение» (продолжение)

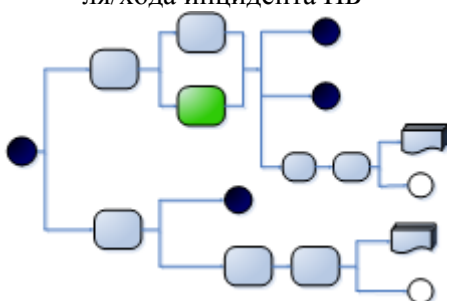
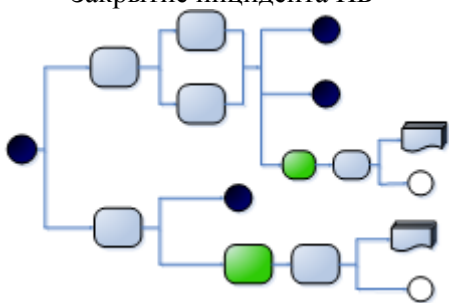
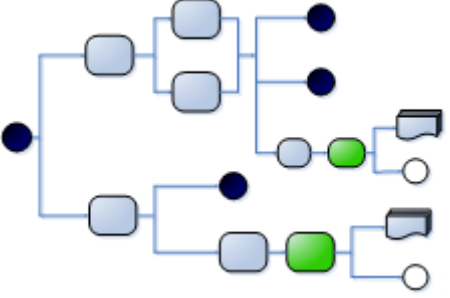
Мониторинг действий нарушителя/хода инцидента ИБ 	В случае если инцидент имеет степень серьезности 1 или 2 возможно два варианта развития событий. Один из которых – Мониторинг действий нарушителя/хода инцидента ИБ без прерывания инцидента позволяет собрать необходимые доказательства и факты для привлечения нарушителя к ответственности. Входы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. План мер по реагированию на инцидент ИБ. Информация о предпринятых действиях по реагированию (включая принятые решения, записи). Выходы: Информация о предпринятых действиях по реагированию (включая принятые решения, записи).	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «План мер по реагированию на инцидент ИБ и антикризисных действий»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ; Члены ГРИИБ.
Закрытие инцидента ИБ 	Независимо от степени серьезности инцидента ИБ, в случае если не требуется Анализ или Расследование инцидента ИБ, осуществляется закрытие инцидента ИБ. Особенно это актуально в случае использования автоматизированных средств управления инцидентами ИБ, которые отслеживают статусы инцидентов ИБ. Входы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. План мер по реагированию на инцидент ИБ. Информация о предпринятых действиях по реагированию (включая принятые решения, записи). Выходы: Информация о предпринятых действиях по реагированию (включая принятые решения, записи).	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «План мер по реагированию на инцидент ИБ и антикризисных действий»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ; Члены ГРИИБ.

Таблица 11 – Описание процесса «Реагирование на инциденты ИБ – Продолжение» (окончание)

Разработка Отчета об инциденте ИБ 	Независимо от степени серьезности инцидента ИБ, в случае если не требуется Анализ или Расследование инцидента ИБ, после процедуры закрытия инцидента ИБ осуществляется разработка Отчета об инциденте ИБ в установленной форме. Входы: Документированный инцидент ИБ с уточнением типа и степени серьезности инцидента. План мер по реагированию на инцидент ИБ. Информация о предпринятых действиях по реагированию (включая принятые решения, записи). Выходы: Отчет об инциденте ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «План мер по реагированию на инцидент ИБ и антикризисных действий»; Другие документы по ИБ в рамках организации.	Ответственный за разрешение инцидента ИБ; Члены ГРИИБ.

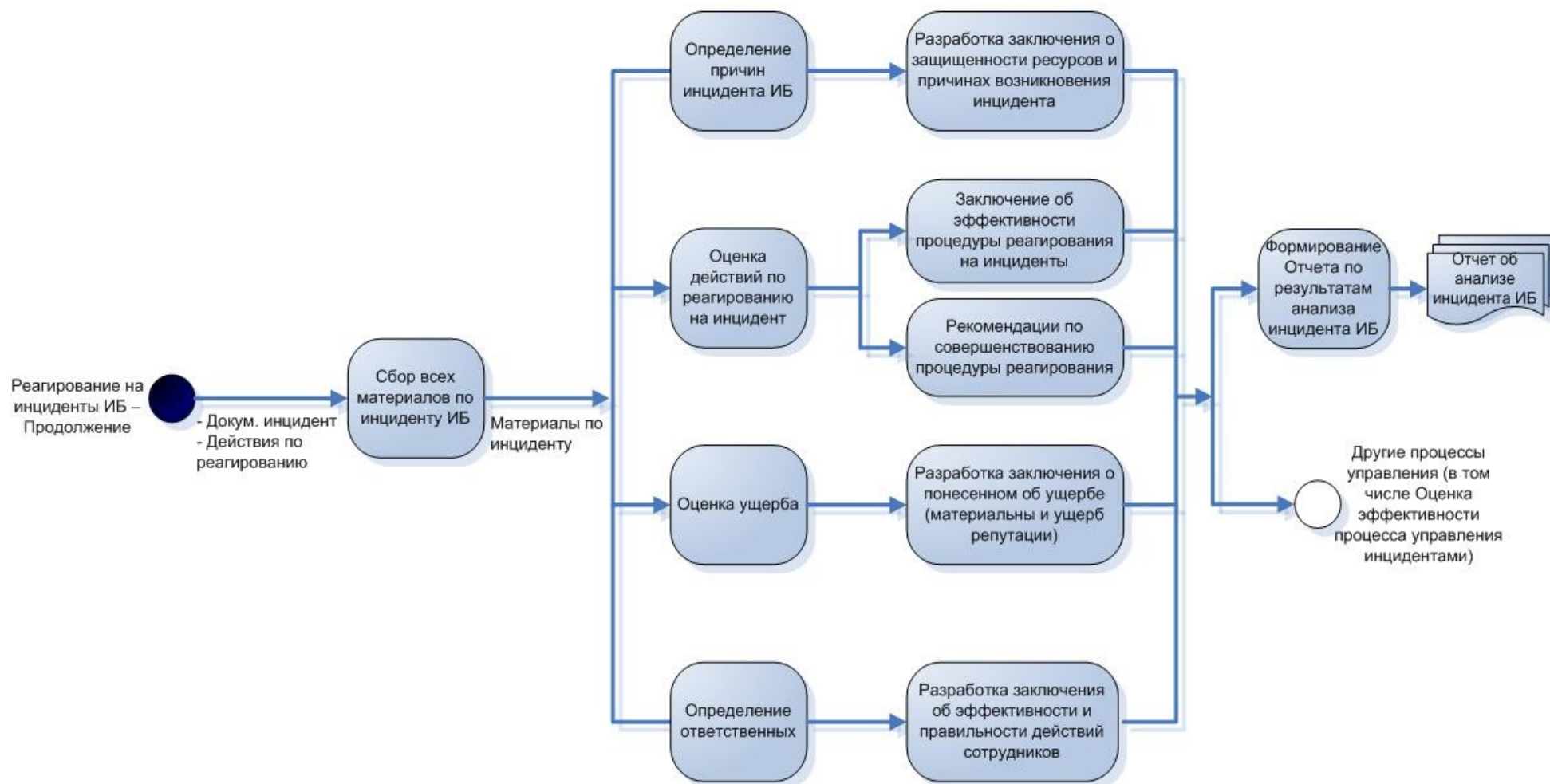


Рисунок 38 – Диаграмма процесса «Анализ инцидентов ИБ»

Таблица 12 – Описание процесса «Анализ инцидентов ИБ» (начало)

Цели процесса	Триггеры	Критерии выполнения	Процедуры и правила
Выявить причины инцидентов ИБ и выработать рекомендации по улучшению ПУИИБ и обеспечения ИБ в целом.	Принятие решения о проведении анализа инцидента ИБ.	Выявление причин инцидента ИБ и выработка рекомендаций по улучшению ПУИИБ и обеспечения ИБ в целом.	«Положение о ролях ПУИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации (включая Политику ИБ).
Входные данные	Описание		Форма
Документированный инцидент ИБ.	Включает в себя все данные по инциденту ИБ, в том числе уточненные тип инцидента ИБ и степень его серьезности.		Заполненная форма документирования инцидента в электронном или бумажном виде
Документированные действия, предпринятые в рамках реагирования на инцидент ИБ.	Включает в себя все данные о действиях, предпринятых в рамках реагирования на инцидент ИБ, принятых решениях и, возможно, разработанных документах		Электронный или бумажный вид
Принятие решения	Выходные данные	Описание	Форма
Передается в качестве входных данных в процессы «Оценка эффективности СУИБ», «Корректирующие и предупреждающие действия» и др.	Отчет по результатам анализа инцидента ИБ	Отчет включает в себя следующие сведения: оценку ущерба; причины инцидента ИБ; предпринятые меры по реагированию; действия сотрудников; ответственные за инцидент ИБ, если это удалось выяснить, и т.д.	Заполненная форма документирования инцидента в электронном или бумажном виде.

Таблица 12 – Описание процесса «Анализ инцидентов ИБ» (продолжение)

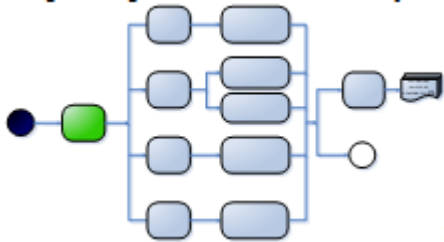
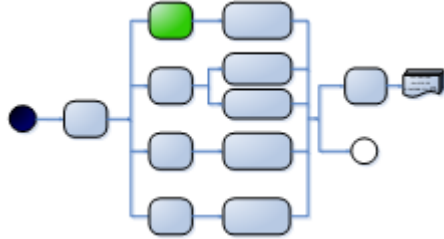
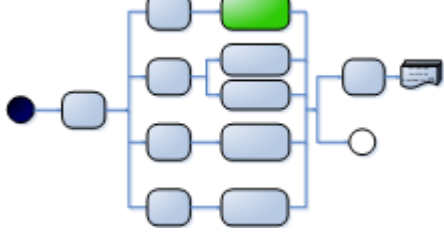
Подпроцесс	Требования к подпроцессу	Процедуры и правила	Роли
Сбор материалов по инциденту ИБ 	После завершения реагирования на инцидент ИБ осуществляется сбор данных по инциденту ИБ, которые включают: перечень всех ресурсов организации, затронутых в инциденте ИБ; угрозы, реализованные против ИТКС ОРГАНИЗАЦИИ; предполагаемые источники угроз ИБ; действия и мотивация нарушителя ИБ; используемые СЗИ. Входы: Документированный инцидент ИБ. Описание действий по реагированию. Выходы: Материалы по инциденту ИБ. Документированный инцидент ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; «Модели угроз и нарушителя ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Эксперт.
Определение причин инцидента ИБ 	На основе собранных материалов по инциденту ИБ осуществляется определение причин инцидента ИБ, включающее: анализ возможностей по реализации данного инцидента; анализ используемых средств и методов для реализации инцидента; оценку адекватности защиты ИТКС ОРГАНИЗАЦИИ. Входы: Материалы по инциденту ИБ. Документированный инцидент ИБ. Выходы: Данные анализа причин инцидента ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Эксперт.
Разработка заключения о защищенности ИТКС и причинах возникновения инцидента ИБ 	В результате анализа причин инцидента ИБ формируется заключение о защищенности затронутых элементов ИТКС, а также о причинах возникновения инцидента ИБ. Выходы: Данные анализа причин инцидента ИБ. Выходы: Заключение о защищенности ресурсов и причинах инцидента ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ.

Таблица 12 – Описание процесса «Анализ инцидентов ИБ» (продолжение)

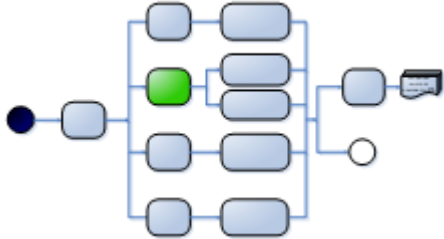
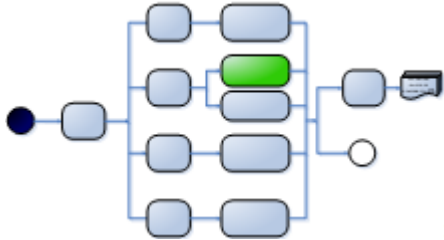
Оценка действий по реагированию на инцидент ИБ 	На основе собранных материалов по инциденту ИБ осуществляется оценка правильности и эффективности действий по реагированию на инцидент ИБ, включающая: восстановление и протоколирование действий каждого члена ГРИИБ и привлекаемых сотрудников; анализ правильности и своевременности действий и решений по реагированию на инцидент ИБ; оценку эффективности действий по реагированию на инцидент ИБ с учетом времени продолжительности инцидента и понесенного ущерба; анализ рекомендаций по предотвращению подобных инцидентов ИБ в будущем. Входы: Материалы по инциденту ИБ. Документированный инцидент ИБ. Выходы: Результаты оценки действий на инцидент ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Члены ГРИИБ.
Разработка заключения об эффективности процедуры реагирования 	В результате оценки действий по реагированию на инцидент ИБ формируется заключение об эффективности процедуры реагирования на инциденты ИБ, дается оценка правильности и своевременности действий и решений ГРИИБ. Входы: Результаты оценки действий на инцидент ИБ. Выходы: Заключение об эффективности процедуры реагирования.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Эксперт.

Таблица 12 – Описание процесса «Анализ инцидентов ИБ» (продолжение)

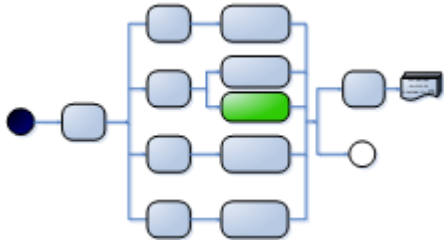
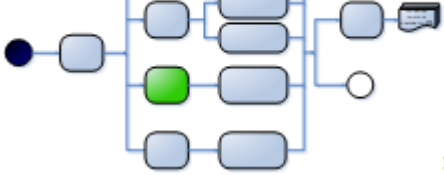
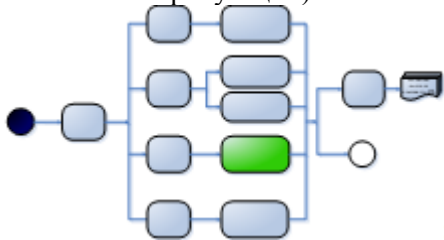
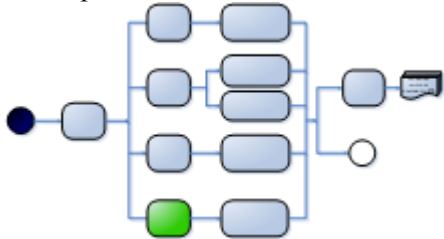
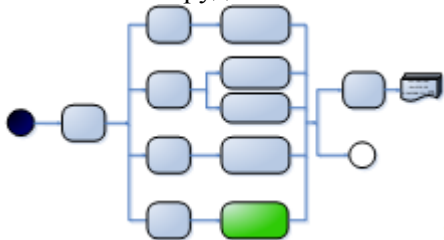
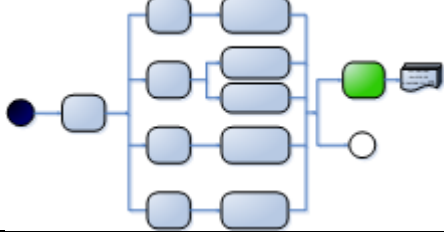
Разработка рекомендаций по совершенствованию процедуры реагирования 	В результате оценки действий по реагированию на инцидент ИБ разрабатываются рекомендации по предотвращению подобных инцидентов ИБ и совершенствованию процедуры реагирования на инциденты ИБ, ПУИИБ и обеспечения ИБ в целом. Входы: Результаты оценки действий на инцидент ИБ. Выходы: Рекомендации по совершенствованию процедуры реагирования.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Владельцы бизнес-процессов; Эксперт.
Оценка ущерба 	На основе собранных материалов по инциденту ИБ осуществляется оценка ущерба, нанесенного инцидентом ИБ, включает в себя: определение ущерба для ИТКС ОРГАНИЗАЦИИ; определение возможных потенциальных потерь для деятельности ОРГАНИЗАЦИИ (финансовых и имиджевых); оценку ущерба по претензиям от партнеров и клиентов. Входы: Материалы по инциденту ИБ. Документированный инцидент ИБ. Выходы: Результаты оценки ущерба.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; «Реестр рисков ИБ»; «Отчет о рисках ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Риск-менеджер; Эксперт.
Разработка заключения о понесенном ущербе (материальном и ущербе репутации) 	В результате оценки ущерба формируется заключение об ущербе, нанесенном инцидентом ИБ, включая заключение о материальном ущербе, ущербе репутации, а также о затратах на восстановление работоспособности ресурсов, вовлеченных в инцидент, в полном объеме. Входы: Результаты оценки ущерба. Выходы: Заключение о понесенном ущербе.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; «Реестр рисков ИБ»; «Отчет о рисках ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Риск-менеджер; Эксперт.

Таблица 12 – Описание процесса «Анализ инцидентов ИБ» (окончание)

Определение ответственных 	На основе собранных материалов по инциденту ИБ осуществляется определение ответственных за произошедшее, что включает: проверку и анализ действий ответственных за элементы ИТКС, их администрирование, обеспечение ИБ и т.д.; оценку адекватности защищенности элементов ИТКС; оценку адекватности действий по прекращению инцидента ИБ; оценку адекватности действий по предотвращению инцидента ИБ. Входы: Материалы по инциденту ИБ. Документированный инцидент ИБ. Выходы: Результаты определения ответственных за инцидент ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Эксперт.
Разработка заключения об эффективности и правильности действий сотрудников 	В результате определения ответственных формируется заключение об эффективности и правильности действий сотрудников, ответственных за элементы ИТКС, за их администрирование и т.д., а также определяется, насколько точно выполнялись инструкции и предписания. Входы: Результаты определения ответственных за инцидент ИБ. Выходы: Заключение об эффективности и правильности действий работников ОРГАНИЗАЦИИ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Эксперт.
Формирование Отчета по результатам анализа инцидента ИБ 	По результатам анализа инцидента ИБ составляется Отчет об анализе инцидента ИБ в установленной форме. Входы: Все выходы предыдущих подпроцессов. Выходы: Отчет по результатам анализа инцидента ИБ.	«Положение о ролях ПУИИБ»; «Положение о ГРИИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Члены ГРИИБ; Менеджер СУИБ; Эксперт.

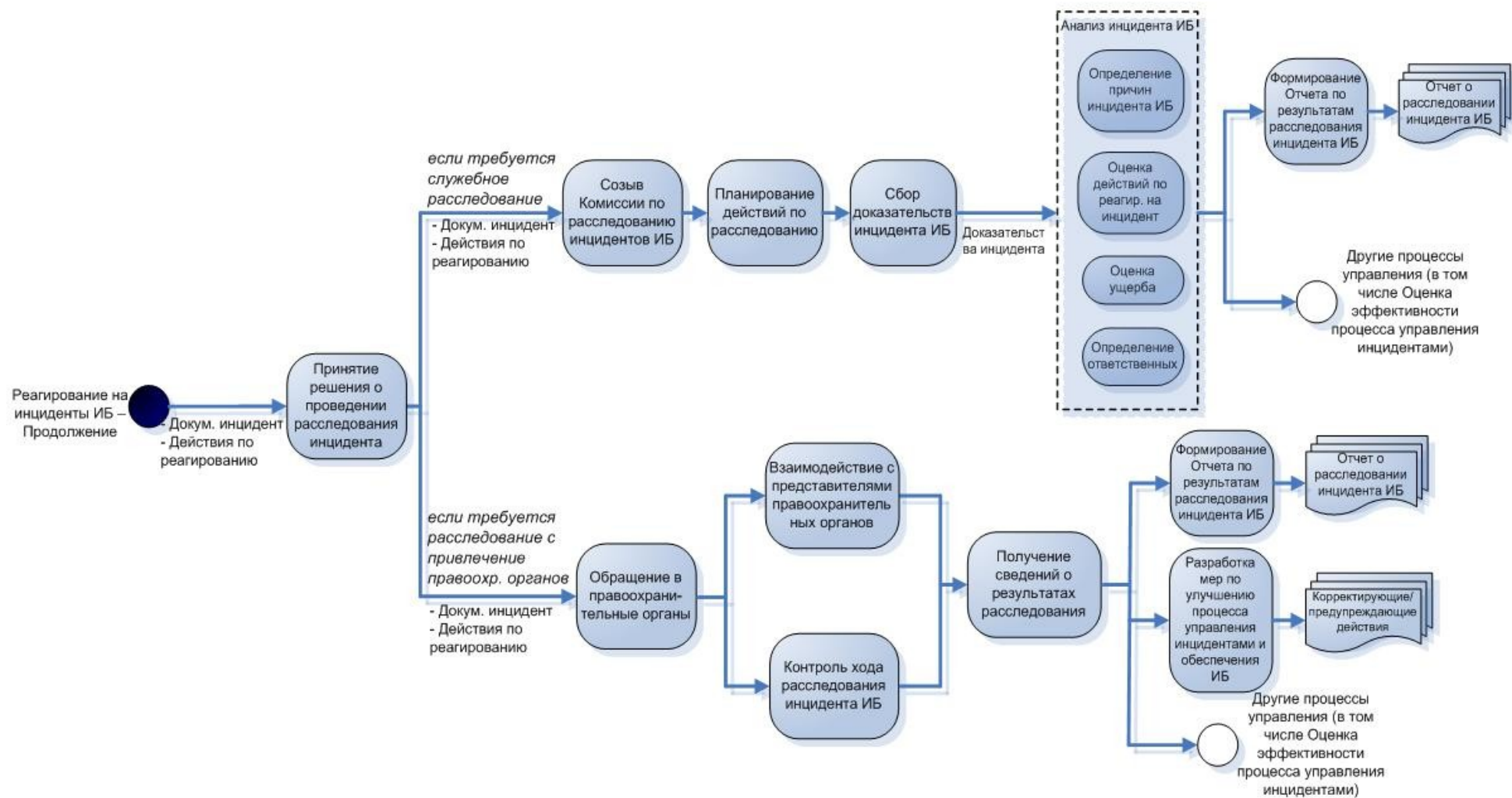


Таблица 13 – Описание процесса «Расследование инцидентов ИБ» (начало)

Цели процесса	Триггеры	Критерии выполнения	Процедуры и правила
Выявить причины инцидента ИБ, выработать рекомендации по улучшению ПУИИБ и обеспечения ИБ в целом, а также в случае проведения уголовного расследования – передача дела в суд.	Принятие решения о проведении расследования инцидента ИБ.	Выявление причин инцидента ИБ и выработка рекомендаций по улучшению ПУИИБ и обеспечения ИБ в целом, а также в случае проведения уголовного расследования – передача дела в суд.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; «Процедура сбора доказательств инцидента ИБ при проведении служебного расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.
Входные данные	Описание		Форма
Документированный инцидент ИБ.	Включает в себя все данные по инциденту ИБ в том числе уточненные тип инцидента и степень его серьезности		Заполненная форма документирования инцидента в электронном или бумажном виде
Документированные действия, предпринятые в рамках реагирования на инцидент ИБ.	Включает в себя все данные о действиях, предпринятых в рамках реагирования на инцидент ИБ, принятых решениях и, возможно, разработанных документах		Электронный или бумажный вид
Принятие решения	Выходные данные	Описание	Форма
Передается в качестве входных данных в процессы «Оценка эффективности СУИБ», «Корректирующие и предупреждающие действия» и др.	Отчет по результатам расследования инцидента ИБ.	Отчет включает в себя следующие сведения: оценку ущерба; причины инцидента ИБ; предпринятые меры по реагированию; действия сотрудников во время инцидента ИБ; ответственные за инцидент ИБ, если это удалось выяснить, и т.д.	Передается в качестве входных данных в процессы «Оценка эффективности СУИБ», «Корректирующие и предупреждающие действия» и др.

Таблица 13 – Описание процесса «Расследование инцидентов ИБ» (продолжение)

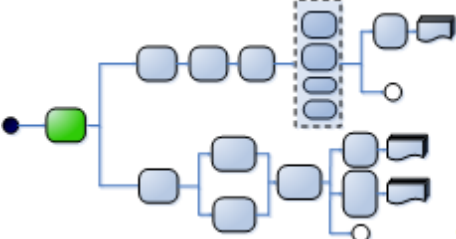
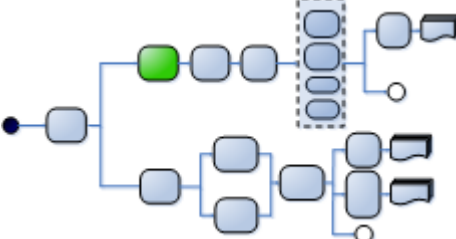
Подпроцесс	Требования к подпроцессу	Процедуры и правила	Роли
Принятие решения о проведении расследования инцидента ИБ 	Необходимо, чтобы высшее руководство организации приняло решение о проведении расследования инцидента ИБ. Также необходимо принять решение о типе расследования инцидента ИБ: с привлечением правоохранительных органов или без. Входы: Документированный инцидент ИБ. Описание действий по реагированию. Выходы: Решение о проведении расследования. Документированный инцидент ИБ. Описание действий по реагированию.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Высшее руководство; Ответственный на разрешение инцидента ИБ; Менеджер СУИБ.
Созыв Комиссии по расследованию инцидентов ИБ 	В случае если требуется проведение служебного расследования инцидента ИБ (без привлечения правоохранительных органов) для планирования и координации расследования инцидента ИБ созывается Комиссия по расследованию инцидента ИБ. Входы: Решение о проведении расследования. Документированный инцидент ИБ. Описание действий по реагированию. Выходы: Состав Комиссии по расследованию инцидента ИБ. Документированный инцидент ИБ. Описание действий по реагированию.	«Положение о ролях ПУИИБ»; «Положение о Комиссии по расследованию инцидентов ИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Высшее руководство; Ответственный на разрешение инцидента ИБ; Менеджер СУИБ.

Таблица 13 – Описание процесса «Расследование инцидентов ИБ» (продолжение)

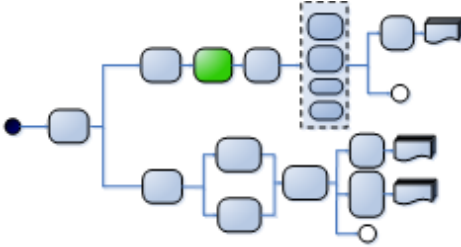
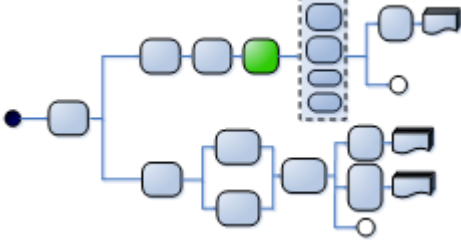
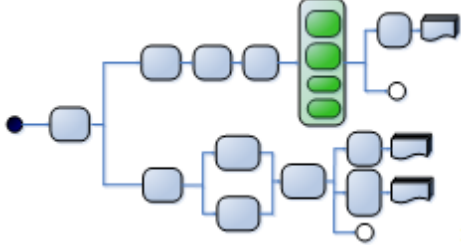
Планирование действий по расследованию инцидента ИБ 	На основе анализа данных об инциденте ИБ и о действиях по реагированию на него осуществляется планирование мероприятий по расследованию инцидента ИБ. Входы: Документированный инцидент ИБ. Описание действий по реагированию. Выходы: План мероприятий по расследованию инцидента ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Председатель Комиссии по расследованию инцидентов ИБ; Члены Комиссии по расследованию инцидентов ИБ.
Сбор свидетельств инцидента ИБ 	После завершения планирования действий по расследованию осуществляется сбор свидетельств инцидента ИБ, в соответствии с разработанным Планом мероприятий по расследованию инцидента ИБ. Входы: План мероприятий по расследованию инцидента ИБ. Выходы: Собранные свидетельства и материалы по инциденту ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; «Процедура сбора доказательств инцидента ИБ при проведении служебного расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Председатель Комиссии по расследованию инцидентов ИБ; Члены Комиссии по расследованию инцидентов ИБ; Эксперт.
Анализ инцидента ИБ 	На основе собранных доказательств и материалов по инциденту ИБ осуществляется анализ инцидента ИБ. Данный процесс практически полностью совпадает с процессом «Анализ инцидентов ИБ», однако, в рамках данного процесса производится более глубокий анализ инцидента ИБ. Входы: Собранные свидетельства и материалы по инциденту ИБ. Выходы: Заключение по результатам анализа (как в «Анализ инцидентов ИБ»).	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Председатель Комиссии по расследованию инцидентов ИБ; Члены Комиссии по расследованию инцидентов ИБ; Эксперт.

Таблица 13 – Описание процесса «Расследование инцидентов ИБ» (продолжение)

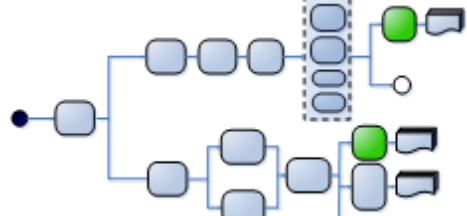
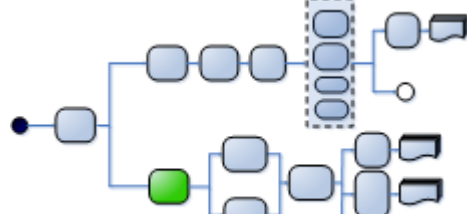
Формирование Отчета по результатам расследования инцидента ИБ 	Независимо от типа расследования по его результатам составляется Отчет по результатам расследования инцидента ИБ в установленной форме. Входы: Все заключения по результатам расследования инцидента ИБ. Выходы: Отчет по результатам расследования инцидента ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Председатель Комиссии по расследованию инцидентов ИБ; Члены Комиссии по расследованию инцидентов ИБ.
Обращение в правоохранительные органы 	В случае если было принято решение о проведении расследования инцидента ИБ с привлечением правоохранительных органов, осуществляется обращение в эти органы. В случае принятия соответствующего решения никаких самостоятельных действий по сбору доказательств до прибытия представителей этих органов предпринимать нельзя. Входы: Решение о проведении расследования. Документированный инцидент ИБ. Описание действий по реагированию. Выходы: Официальное обращение в правоохранительные органы. Документированный инцидент ИБ. Описание действий по реагированию.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Высшее руководство; Ответственный на разрешение инцидента ИБ; Менеджер СУИБ.

Таблица 13 – Описание процесса «Расследование инцидентов ИБ» (продолжение)

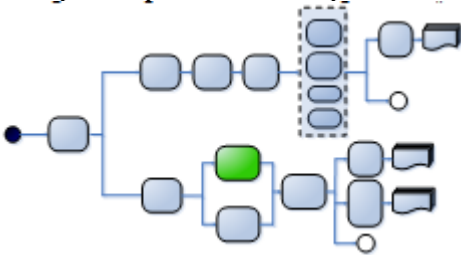
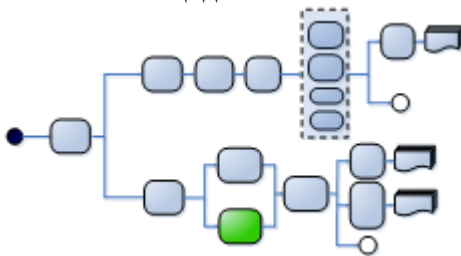
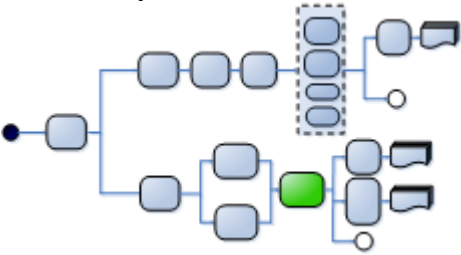
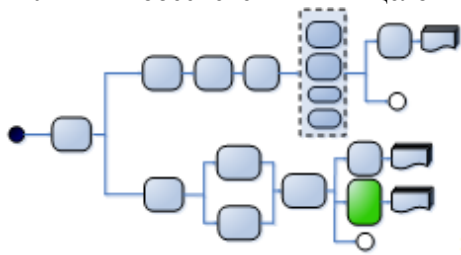
Взаимодействие с представителями правоохранительных органов 	При проведении расследования представителями правоохранительных органов работники ОРГАНИЗАЦИИ должны оказывать содействие и посильную помощь. Руководство ОРГАНИЗАЦИИ несет ответственность за достоверность и полноту предоставляемой представителям этих органов информации, а также за любые ограничения возможности осуществления представителями этих органов действий, необходимых для проведения расследования инцидента ИБ. Входы: Официальное обращение в правоохранительные органы. Документированный инцидент ИБ. Описание действий по реагированию. Выходы: Сведения, получаемые по ходу расследования инцидента ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Менеджер СУИБ.
Контроль хода расследования инцидента ИБ 	Ответственные работники ОРГАНИЗАЦИИ должны контролировать ход работ по расследованию инцидентов ИБ представителями правоохранительных органов, в случае необходимости отстаивать интересы ОРГАНИЗАЦИИ в рамках, установленных законодательством. Входы: Официальное обращение в правоохранительные органы. Документированный инцидент ИБ. Описание действий по реагированию. Выходы: Сведения, получаемые по ходу расследования инцидента ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Менеджер СУИБ.

Таблица 13 – Описание процесса «Расследование инцидентов ИБ» (окончание)

Получение сведений о результатах расследования 	По окончании процедуры расследования инцидента ИБ правоохранительными органами необходимо запросить сведения о результатах проведенного расследования. Входы: Запрос на предоставление сведений о результатах расследования инцидента ИБ. Выходы: Сведения о результатах расследования инцидента ИБ.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Ответственный на разрешение инцидента ИБ; Менеджер СУИБ.
Разработка мер по улучшению ПУИИБ и обеспечения ИБ в целом 	В результате анализа результатов расследования инцидента ИБ разрабатываются рекомендации по предотвращению подобных инцидентов ИБ и совершенствованию процедуры реагирования на инциденты ИБ, ПУИИБ и обеспечения ИБ в целом. Все разработанные рекомендации оформляются в виде запросов на корректирующие и предупреждающие действия. Входы: Сведения о результатах расследования инцидента ИБ. Выходы: Запросы на корректирующие и предупреждающие действия.	«Положение о ролях ПУИИБ»; «Процедура обнаружения, оповещения и реагирования на инциденты ИБ»; «Процедура анализа и расследования инцидентов ИБ»; Другие документы по ИБ в рамках организации.	Председатель Комиссии по расследованию инцидентов ИБ; Члены Комиссии по расследованию инцидентов ИБ; Эксперт; Владелец бизнес-процесса, вовлеченного в инцидент ИБ.

Разработанные процессы в рамках обобщенного ПУИИБ для ИТКС отличает четкая структурированность, которая способствует их результативному последовательному применению ОРГАНИЗАЦИЕЙ на практике, поскольку они позволяют быстро идентифицировать и осуществить немедленное реагирование на выявленный инцидент ИБ в соответствии с его приоритетом, что будет способствовать снижению его неблагоприятных воздействий на ИТКС и деятельность ОРГАНИЗАЦИИ в целом и предотвращению похожих инцидентов ИБ в будущем. Таким образом, все разработанные процессы ПУИИБ готовы к их непосредственному применению в ЦИУСБ ОРГАНИЗАЦИИ. Но подчеркнем, что разработанный обобщенный ПУИИБ может быть реализован различными способами в зависимости от внешнего и внутреннего контекста, в котором он будет использоваться в ОРГАНИЗАЦИИ.

3.4.6. Разрабатываемый Центр интеллектуального управления сетевой безопасностью как фундамент системы управления инцидентами информационной безопасности для-информационно-телекоммуникационной сети

ПУИИБ является ключевым процессом, реализуемым Системой управления инцидентами ИБ (СУИИБ) как части СУИБ, а, следовательно, и СОИБ ОРГАНИЗАЦИИ (рис. 40). Основываясь на [168], определим **СУИИБ ИТКС** как часть общей системы управления ОРГАНИЗАЦИИ, предназначенная для обнаружения и регистрация, оценки, классификации и приоритезации, всестороннего исследования, обработки, извлечения уроков и предотвращения инцидентов ИБ в дальнейшем и включающая организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области реагирования на инциденты ИБ в ИТКС ОРГАНИЗАЦИИ.

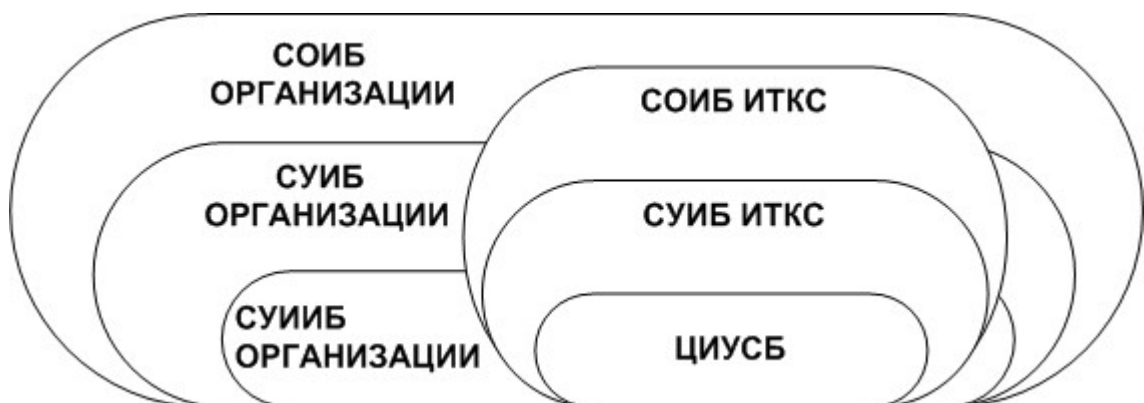


Рисунок 40 – Место ЦИУСБ среди систем в области ИБ ОРГАНИЗАЦИИ

Наличие результативно функционирующей в организации СУИИБ позволяет реализо-

вать следующие возможности:

- создать единый центр управления инцидентами ИБ на уровне всей ОРГАНИЗАЦИИ с целью обеспечения контроля и координации действий по локализации и расследованию инцидентов ИБ, включающий в себя в качестве фундамента специализированный для ИТКС ОРГАНИЗАЦИИ ЦИУСБ;
- создать единую организационную структуру реагирования на инциденты ИБ;
- консолидировать всю информацию об инцидентах ИБ в едином хранилище;
- повысить скорость реагирования и оперативность выявления причин инцидента ИБ;
- повысить достоверность получаемых результатов по выявлению причин инцидента ИБ, ответственных лиц и определению необходимых действий, устранению последствий инцидента и применению соответствующих необходимых мер обеспечения ИБ;
- формировать статистику по инцидентам ИБ, выявлять тенденции в ее изменении, анализировать динамику этих изменений и прогнозировать будущее;
- автоматизировать применение мер обеспечения ИБ мер для снижения риска ИБ при выявлении типовых инцидентов ИБ.

Обратная связь при осуществлении управления инцидентами ИБ на основе СУИИБ помогает сохранять нацеленность действий персонала ОРГАНИЗАЦИИ на борьбу с реальными рисками ИБ в ИТКС за счет сбора более качественных исходных данных и поддерживать общую типизацию, отражающую системный подход к управлению инцидентами ИБ, обеспечивая последовательное получение надежных результатов. Типизация, наряду с общепринятыми метриками результативности ПУИИБ и стандартной структурой БД инцидентов ИБ, обеспечивает возможность сравнивать результаты, улучшать предупреждающую информацию и получать более точное представление об угрозах ИБ и уязвимостях элементов ИТКС. Информация, получаемая от СУИИБ, будет содержать и ценные данные для анализов качества и последующего улучшения Политики ИБ (и другой документации, связанной с ИБ) как на уровне всей ОРГАНИЗАЦИИ, так и для повышения функциональной устойчивости ИТКС.

Выводы по главе 3

1. В эпоху цифровой экономики в условиях жесткой конкурентной борьбы для противодействия угрозам ИБ, оперативного реагирования на события и инциденты ИБ и снижения рисков ИБ необходимо обеспечивать и на протяжении длительного времени сохранять достаточный уровень ИБ ИТКС ОРГАНИЗАЦИИ. Для этого должна быть создана адекватная защищенная среда устойчивого функционирования ИТКС. Эта цель может быть достигнута за счет обеспечения ИБ ИТКС. Показана взаимосвязь деятельности ОРГАНИЗАЦИИ по обеспечению

ИБ ИТКС и ее основной деятельности в ЕИП, характеризующая обеспечение ИБ ИТКС как процесс.

2. Исходя из логики осуществления любого процесса, представлена упрощенная (без ресурсов и управляющих воздействий) модель обеспечения ИБ ИТКС ОРГАНИЗАЦИИ, которая позволяет системно и комплексно решать поставленные задачи по достижению требуемого уровня ИБ ИТКС. Перед разработкой и внедрением процесса должен быть описан внешний и внутренний контекст, в котором его будут использовать. На этой основе формулируются цели процесса в поддержку основных бизнес-целей ОРГАНИЗАЦИИ и начинается реализация этих целей. Когда процесс внедрен и используется, необходимо постоянно контролировать результативность достижения поставленных в начале целей и по результатам такого контроля регулярно пересматривать описание динамически меняющегося контекста и переформулировать цели процесса, что доказывает итерационность обеспечения ИБ ИТКС.

3. В связи с отсутствием в международной и отечественной нормативной базах четких рекомендаций по разработке реестра (классификатора) рисков ИБ, предложен вид реестра рисков ИБ для ИТКС, который строится на основе двух моделей ИБ и позволяет подобрать меры и процессы обеспечения ИБ, необходимые для обработки рассчитанных рисков ИБ.

4. Предложена примерная типовая структура частной Политики ИБ для элемента ИТКС ОРГАНИЗАЦИИ.

5. Выделена специфика обеспечения сетевой безопасности ИТКС по сравнению с обеспечением ИБ, которая заключается в том, что первая, кроме деятельности по обеспечению свойств ИБ информационных ресурсов, обрабатываемых, передаваемых и хранимых в ИТКС, включает также деятельность, направленную на обеспечение безопасности устройств ИТКС, обеспечение безопасности управления этими устройствами, приложениями, предоставляемыми услугами и конечными пользователями.

6. Обоснованно сделан вывод, что деятельность по обеспечению ИБ ИТКС шире, чем деятельность по управлению ее ИБ, поскольку также включает в себя систематическое осуществление контрольных мероприятий и повседневную деятельность по поддержанию информационной защищенности ИТКС на достаточном с точки зрения ОРГАНИЗАЦИИ уровне в течение длительного периода времени за счет внедрения и использования мер обеспечения ИБ и соответствующих процессов обеспечения ИБ (включая процессы эксплуатации СЗИ).

7. В управлении ИБ ИТКС как неотъемлемой части управления ЕИП ОРГАНИЗАЦИЕЙ можно выделить три основных уровня: стратегическое, тактическое и оперативное управление. Показано место ЦИУСБ, ЦИБ и ЦМБ на этих уровнях.

8. Представленный процесс управления ИБ ИТКС соответствует классическому – в нем присутствует обратная связь между результатами процесса и его отдельными частями. Неодно-

кратно ранее упоминаемые элементы ИТКС и есть объекты управления (управляемые объекты) ИБ, наряду с рисками ИБ, инцидентами ИБ, непрерывностью деятельности, изменениями, совершенствованиями, сами мерами обеспечения ИБ, обеспечивающими ресурсами, участвующими в реализации информационных процессов ИТКС. Управляющим объектом является специально разработанная и внедренная СУИБ ИТКС как часть СОИБ ИТКС. К описанию процессов СУИБ применим общеизвестных подход – циклическая модель PDCA.

9. Введены понятия «эффективности управления ИБ ИТКС» и «эффективности СУИБ ИТКС», оценка которых должна осуществляться в рамках системного процесса получения и оценки объективных данных о текущем состоянии СУИБ ИТКС, процессах и событиях, происходящих в ней, устанавливающего уровень их соответствия определенным ОРГАНИЗАЦИЕЙ критериям.

10. Как и для обеспечения сетевой безопасности, сделан вывод, что управление сетевой безопасностью ИТКС основано на циклическом процессе, который состоит из совокупности целенаправленных действий в целях безопасного и устойчивого функционирования ИТКС ОРГАНИЗАЦИИ в течение всего ее жизненного цикла.

11. Проанализирована эволюция основных подходов к управлению сетевой безопасностью, в которой указано время появления ЦУБ, предназначенных для оперативного – ЦМБ – и тактического – ЦИБ – управления сетевой безопасностью, послуживших отправной идеей для разработки более совершенного ЦИУСБ ОРГАНИЗАЦИИ.

12. Показано, что среди контрольных мероприятий по оценке результативности и эффективности СУИБ ИТКС ОРГАНИЗАЦИИ особое место занимает непрерывный мониторинг ИБ и контроль используемых защитных мер, показывающий, насколько эта система функционирует надлежащим образом и адекватна ли они существующим угрозам ИБ, внутреннему и внешнему контекстам функционирования ИТКС ОРГАНИЗАЦИИ, влияющим на ее ИБ, всем применимым требованиям нормативных и правовых документов, политикам и целям обеспечения ИБ ОРГАНИЗАЦИИ. Отмечено, что процессы мониторинга ИБ должны быть интегрированы в систему единого внутреннего контроля и риск-менеджмента ОРГАНИЗАЦИИ. Показана связь мониторинга ИБ с другими процессами, например, аудитом ИБ ИТКС ОРГАНИЗАЦИИ.

13. Из выделенных функций мониторинга ИБ, очевидно, что процессы мониторинга ИБ тесно взаимосвязаны с процессами управления инцидентами ИБ в ИТКС. Как ключевой элемент управления рисками ИБ в динамически изменяющейся ИТКС ОРГАНИЗАЦИИ, он позволяет, среди прочего, выявлять нарушения ИБ и инциденты ИБ, используемые ими уязвимости элементов ИТКС (включая уязвимости в самих СЗИ), а также обеспечивать доказательную базу на случай расследования компьютерных преступлений в отношении ИТКС ОРГАНИЗАЦИИ и ее отдельных элементов.

14. На основе определенной базы разработки ПУИИБ и общеизвестных задач этого процесса, при решении которых требуется применение комплексного подхода, описано содержание деятельности в рамках ПУИИБ применительно к ИТКС ОРГАНИЗАЦИИ. Подчеркнуто, что результативная реализация данного процесса возможно лишь как важнейшая часть СОИБ ИТКС и основы деятельности ЦИУСБ ОРГАНИЗАЦИИ, поскольку данные, аккумулируемые при управлении инцидентами ИБ, являются необходимыми для работы других процессов управления ИБ, например, анализа рисков ИБ или оценки эффективности существующих мер по обеспечению ИБ и процессов управления ею.

15. Поскольку управление инцидентами ИБ предполагает осуществление деятельности по их расследованию, то необходим сбор и сохранение свидетельств инцидента ИБ, представленных в цифровой форме, что подробно описано применительно к случаю ИТКС ОРГАНИЗАЦИИ. Приведены примеры постоянной и временной информации, подлежащей сбору на компьютерах ИТКС и особо акцентировано внимание на необходимости предотвращения внесения изменений в исследуемую систему при сборе свидетельств инцидента ИБ.

16. После выработки требований к ПУИИБ для ИТКС ОРГАНИЗАЦИИ на основе международного стандарта ISO/IEC 27001:2013 определены семь основных взаимосвязанных процессов в рамках обобщенного ПУИИБ. Для их формализации применен расширенный (за счет дополнительного табличного описания) метод составления карт процессов, который позволяет наглядно увидеть последовательность всех действий и взаимозависимости между ними, а также оптимизировать уже разработанные процессы путем отслеживания избыточных действий и выявления рисков их успешной реализации. Данный метод выбран потому, что одним из его показателей является время выполнения, что особо важно в случае с необходимостью быстрого реагирования на инциденты ИБ в ИТКС ОРГАНИЗАЦИИ, и когда процесс надо изобразить в координатах двух его параметров (например, исполнители и время).

17. Разработанный ПУИИБ для ИТКС отличается четкая структурированность, которая способствует его результативному последовательному применению ОРГАНИЗАЦИЕЙ на практике, поскольку он позволяет быстро идентифицировать и осуществить немедленное реагирование на выявленный инцидент ИБ в соответствии с его приоритетом, что будет способствовать снижению его неблагоприятных воздействий на ИТКС и деятельность ОРГАНИЗАЦИИ в целом и предотвращению похожих инцидентов ИБ в будущем. Все разработанные процессы ПУИИБ готовы к их непосредственному применению в ЦИУСБ ОРГАНИЗАЦИИ.

18. В заключении главы показано место ЦИУСБ среди систем обеспечения и управления ИБ ОРГАНИЗАЦИИ в качестве фундамента СУИИБ.

ГЛАВА 4. КРИТИЧЕСКИЙ АНАЛИЗ СУЩЕСТВУЮЩИХ ЦЕНТРОВ И ВЫРАБОТКА ТРЕБОВАНИЙ К ЦЕНТРАМ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ

Постоянно возрастающая сложность управления ИБ для современных ИТКС и недостаток высококвалифицированного персонала является проблемой, которая будет существовать в обозримом будущем еще долго. Два важных источника проблемы – это огромный поток и разнообразие предупреждений об опасности, генерируемых системами управления доступом, САВЗ, СОВ/СПВ, МЭ, системам унифицированного управления угрозами (*UTM*-системами), ОС, СУБД и т.д., и разнообразие задач, выполняемых подразделением ИБ, включая управление ценными активами, рисками ИБ, СЗИ, обновлениями, шифрованием, инцидентами ИБ, большими связанными с ИБ данными и т.д. Только один МЭ может записывать ежедневно в ЖРС гигабайты данных, а СОВ/СПВ за тот же период может выдавать миллионы сообщений. МЭ нового поколения, содержащий СОВ/СПВ как неотъемлемую подсистему, порождает еще больше данных за счет корреляции событий ИБ, ранее воспринимаемых как не связанные между собой. В потоке данных, генерируемых СЗИ, много ложных срабатываний о якобы незаконном использовании ресурсов и услуг ИТКС, просто никогда ранее не проявлявшихся. Поэтому решающее значение приобретает необходимость вычленить и приоритезировать часть сообщений, которые действительно указывают на реальные угрозы и события ИБ, актуальных для данной ОРГАНИЗАЦИИ. Это имеет и экономические основы, требующие от ОРГАНИЗАЦИИ более результативного использования внедренных мер обеспечения ИБ для ее ИТКС.

В главе вводится и подробно анализируется понятие являющейся ядром ЦМБ и ЦИБ *SIEM*-системы как основы для дальнейшего построения ЦИУСБ, устраняющей ограниченность своих предшественников. Поясняется концепция интеллектуальной безопасности (англ. *Security Intelligence*), положенная в основу разрабатываемого ЦИУСБ. Анализируются два вида ЦУБ: ЦМБ, осуществляющего только мониторинг инцидентов ИБ, и ЦИБ, способного управлять инцидентами ИБ в ИТКС. Для ЦИБ разрабатывается расширенная по сравнению с оригинальной бизнес-логика функционирования для ее дальнейшего применения в типовом ЦИУСБ. Рассматриваются различные модели зрелости ЦУБ. Глава завершается формулированием общих и специальных требований, требований по обеспечению собственной ИБ ЦИУСБ и выводами.

4.1. Понятие *SIEM*-системы

Как отмечалось в разделе 1.2.4, в течение только одного дня в интранетах больших кор-

пораций СЗИ могут регистрировать миллионы событий ИБ, имеющих разные происхождение и последствия. Объем трудозатрат, необходимых для выявления действительно важных с точки зрения ИБ событий и сбора информации об инцидентах ИБ, может оказаться чрезвычайно большим и невыполнимым вручную. Для решения задачи управления потоком событий ИБ, получаемых от СЗИ, и для автоматизации процессов обобщенного ПУИИБ используются автоматизированные средства – ПО для управления информацией и событиями ИБ (англ. *Security Information and Event Management*). В англоязычной литературе системы мониторинга ИБ называются системами управления информацией и событиями ИБ и обозначаются аббревиатурой *SIEM*. С точки зрения здравого смысла будет называть их не просто *SIEM*, а *SIEM*-системами.

Термин *SIEM* был впервые введен исследовательской и консалтинговой компанией Gartner в 2005 г. Объединенная *SIEM*-система заменила два типа систем, возникших до нее – простейшие системы управления информацией о безопасности (англ. *Security Information Management, SIM*) и системы управления событиями безопасности (англ. *Security Event Management, SEM*) [187]). *SIM*-системы обеспечивали долгосрочное хранение в централизованном репозитории собранных данных, анализ тенденций и автоматическую отчетность, в то время как *SEM*-системы собирали данные о событиях в режиме реального времени, проводили их быстрый несложный анализ, отправляли соответствующие уведомления и представляли обработанную информацию на консоли оператора для выполнения заранее предписанных защитных действий. Таким образом, *SEM*-система в большей степени была ориентирована на быстроту ответной реакции на собранные данные, в то время как *SIM*-система была предназначена для сохранения исторических (представленных в строгой хронологической последовательности за некоторый прошедший период времени) данных из ЖРС о состоянии контролируемых объектов защиты. Объединенная *SIEM*-система собирает и анализирует данные из ЖРС и другую информацию, связанную с ИБ.

Ключевые функции этих трех систем можно кратко обобщить следующим образом:

- *SIM*-система – сбор и архивирование ЖРС, формирование отчетности с учетом истории и предоставление информации для проведения расследования;
- *SEM*-система – формирование отчетности в режиме близком к реальному времени, сбор данных из ЖРС для их последующей обработки;
- *SIEM*-система – сбор и архивирование ЖРС, нормализация, агрегирование (объединение) и корреляция (сопоставление и совместный анализ) данных из ЖРС для формирования отчетности с учетом истории в режиме близком к реальному времени и составления доказательной базы для предоставления информации при проведении расследования инцидентов ИБ.

Сбор ЖРС, имеющих отношение к ИБ объектов защиты, от гетерогенных источников предоставляет данные для проведения расследования инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ

и помогает понять степень выполнения требований различных нормативных, правовых и договорных документов [188]. Сбор «сырых» данных может осуществляться с помощью инструментальных средств, опросных листов (форм), агентов (ПО и АО) и без агентов (путем чтения из файлов или ЖРС, приема непосредственно от источников, подключения к программному интерфейсу приложения или веб-сервису источника данных [15]). Нормализация собранных «сырых» (англ. *raw*) данных из журналов от многочисленных систем приводит их к общей модели данных – к формату, необходимому для дальнейшей их обработки и хранения и позволяющему с единой точки зрения анализировать связанные события, несмотря на изначально разные форматы представления данных в исходных ЖРС. Корреляция связывает данные из ЖРС и сопоставляет события в разрозненных системах и приложениях для их совместного анализа, ускоряя обнаружение и реагирование на происходящие в ИТКС события ИБ. Агрегирование уменьшает объем данных о событиях путем объединения однородных и повторяющихся записей о событиях. Отчетность представляет взаимосвязанные, агрегированные данные о событиях мониторинга в режиме реального времени и долгосрочных сводках.

Таким образом, *SIEM*-система представляет собой усовершенствованную за счет более детального анализа и корреляции собранных из гетерогенных источников данных систему мониторинга различных аномалий в объектах защиты в сетях и вредоносной активности. Для этого *SIEM*-система содержит консолидированное хранилище информации – БД, отвечающую за накопление и хранение как «сырых» данных, так и уже обработанной информации о событиях ИБ, а также управляющий интерфейс с консолью управления и сервером-коррелятором, отвечающим за сбор информации и ее обработку по правилам и алгоритмам корреляции. Корреляция в *SIEM*-системах может быть основана на правилах (недостатки такого подхода очевидны – это много времени, требуемого для поддержания сотен правил в актуальном состоянии, и слишком много ложных срабатываний (пометок ранее неизвестной активности как враждебной, когда ее нет, или, наоборот, пропуск событий ИБ из-за неполноты знаний о них) для постоянно обновляемых методов злоумышленников) или политиках и иметь возможности статистической корреляции для установления связей между записями ЖРС [187, 188]. Все записи в БД *SIEM*-системы должны быть защищены, поскольку они содержат важные данные, необходимые для расследования и реагирования на инциденты ИБ.

Как видно из описания функций *SIM*- и *SEM*-систем, они строят свою работу на ЖРС. Для управления этими журналами появился специальный термин – управления ЖРС (англ. *log management*). Но эта деятельность уступает по функциональным возможностям *SIEM*-системе. Основываясь на [189], был проведен сравнительный анализ систем управления ЖРС и *SIEM*-систем, результаты которого представлены в табл. 14.

Таблица 14 – Сравнительный анализ систем для управления ЖРС и SIEM-систем

Критерий сравнения	Системы управления ЖРС	SIEM-системы
Реализация	ПО, виртуальное приложение, аппаратное устройство	ПО, виртуальное приложение, аппаратное устройство
Хранилище данных	Обычно собственная БД организации	Коммерческая или собственная БД организации
Типы получаемых из ЖРС данных	Большое, но часто более ограниченное разнообразие	Большое разнообразие
Нормализация данных	Обычно упрощенная	Обычно расширенная
Корреляция	Отсутствует или упрощенная	Расширенная
Возможности подачи предупреждений в режиме реального времени	Отсутствуют или простые	Отличные
Возможности использования исторических данных	Простые или хорошие	Хорошие или отличные
Специальные запросы данных	Поддерживают отлично	Поддерживают удовлетворительно или хорошо
Обнаружение шаблонов и аномалий	Отсутствует или плохо	Хорошо или отлично
Скорость исследования событий	Хорошая или отличная	Удовлетворительная или хорошая
Скорость выполнения структурированных запросов	Хорошая или отличная	Удовлетворительная или хорошая
Скорость выполнения неструктурированных (полнотекстовых) запросов	Хорошая или отличная	Отсутствует или плохая
Проверка соответствия требованиям	Отсутствует или плохо	Хорошо или отлично
Совместимость с управлением угрозами	Отсутствует	Хорошо или отлично
Клиентский интерфейс	Простой или сложный веб-интерфейс с упрощенными возможностями визуализации в виде информационных панелей (англ. <i>dashboard</i>)	Сложный чаще всего веб-интерфейс с расширенными возможностями визуализации в виде различных информационных панелей
Отчеты	Хорошие или отличные	Хорошие или отличные

Типичная архитектура SIEM-системы, которая демонстрирует объединенные в ней SIM- и SEM-системы, представлена на рис. 41 [187]. В нижней части рисунка отражены основные возможности сбора событий и сохранения записей о них. Сохраненные данные используются при решении задач мониторинга ИБ и корреляции данных о событиях (центр рисунка). Верхняя часть показывает, что проанализированные данные могут быть представлены либо в отчетах о безопасности, либо в отчетах о событиях ИБ, которые в том или ином виде визуализируются на консоли управления SIEM-системой. Левая часть рисунка отображает возможности SIM-системы, а правая – SEM-системы.

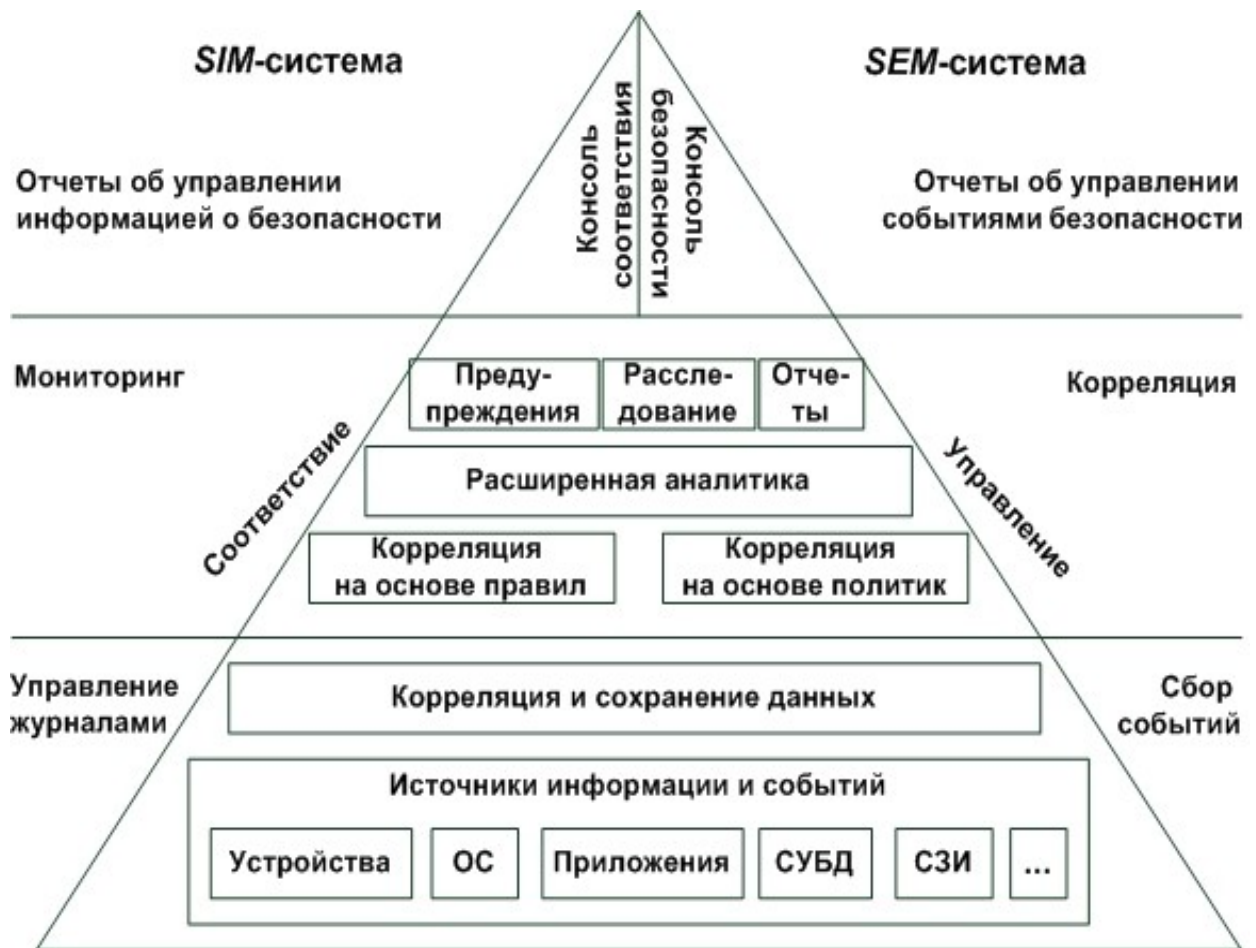


Рисунок 41 – Типичная архитектура *SIEM*-системы

SIEM-системы – это не СЗИ, и сами по себе они не могут предотвращать возникновение инцидентов ИБ в ИТКС. Они используются организациями в первую очередь для решения задач проверки соответствия определенным требованиям по обеспечению ИБ с автоматической генерацией отчетов, подтверждающих факт соответствия, а также управления событиями ИБ в ИТКС ОРГАНИЗАЦИИ. Это позволяет достичь следующих целей при управлении сетевой безопасностью:

- получить информацию о реальном состоянии уровня информационной защищенности всей ИТКС в целом и отдельных ее элементов;
- провести обоснованную оценку рисков ИБ для ИТКС, на основе которой принять соответствующие решения для последующего своевременного устранения или снижения рисков ИБ до допустимых;
- обнаружить расхождения в соблюдении всех применимых требований по обеспечению ИБ и привести активы и бизнес-процессы в соответствии с внутренними Политиками ИБ, требованиями законов, регуляторов и аудиторов.

Как показывает многолетний опыт использования *SIEM*-систем, в повседневной жизни ОРГАНИЗАЦИИ ее использование для ИТКС дает следующие результаты:

- снижает операционные затраты на обработку данных о событиях ИБ из гетерогенных источников в ИТКС и управление такими данными за счет автоматизации этих процессов;

- ускоряет реакцию на возникающие события и инциденты ИБ и обеспечивает информационную защищенность ИТКС в круглосуточном режиме за счет автоматизированного реагирования на обнаруженные события ИБ в соответствии с заданными правилами их корреляции и обработки;

- сокращает затраты на подготовку персонала служб ИБ, которому нужно изучить только управляющий интерфейс с консолью управления *SIEM*-системы, а не всех используемых в ИТКС разнородных СЗИ;

- снимает необходимость в увеличении штата службы ИБ при росте количества СЗИ, предоставляющих информацию о событиях ИБ для ее обработки в *SIEM*-системе;

- автоматизирует деятельность по анализу защищенности ИТКС ОРГАНИЗАЦИИ и созданию отчетов в соответствии с действующими внутренними, отраслевыми, российским и международными документами.

Для этого связанные с ИБ данные и события ИБ в ИТКС ОРГАНИЗАЦИИ могут поступать в *SIEM*-систему из следующих основных источников (рис. 41) [188, 190]:

- встроенные средства телекоммуникационных устройств, СВТ, ОС компьютеров и маршрутизирующего оборудования, приложений и СУБД, фиксирующие все проблемы с их работоспособностью, изменениями конфигурационных настроек и политик и т.п.;

- системы управления активами, контролирующие существующие в ИТКС активы и выявляющие новые незаконно установленные устройства;

- сетевое активное оборудование, осуществляющее контроль изменений и доступа, связанных с сетевым трафиком;

- средства контроля доступа, осуществляющие мониторинг доступа к информационным ресурсам, ИТ-услугам, СЗИ и т.п. в ИТКС и использования привилегированного доступа;

- ЖРС серверов и рабочих станций, записывающие данные о доступе, обеспечении непрерывности функционирования различных систем и соблюдении Политик ИБ и реализующих их правил обеспечения ИБ;

- СОВ/СПВ, следящие за событиями о сетевых атаках, сетевым трафиком, изменениями конфигурационных настроек и доступом к устройствам;

- САВЗ, фиксирующие появление вредоносных программ и компьютерных вирусов;

- САЗ, в функции которых входит, в том числе, инвентаризация активов, сервисов, ПО, топологии и выявление их уязвимостей;

- системы управления рисками ИБ, анализирующие критичность возникающих угроз ИБ и определяющие приоритеты обработки инцидентов ИБ;

— другие системы защиты и контроля политик ИБ: *DLP*-системы, системы выявления мошеннических операций, системы фильтрации веб-контента и т.п.

При сборе «сырых» данных в *SIEM*-системах обычно используется один или сразу оба ниже названных подхода [191, 192]:

1) безагентный, когда генерирующий ЖРС объект защиты напрямую передает эти журналы на централизованную консоль управления *SIEM*-системе или, например, специальному *syslog*-серверу, предназначенному для сбора и хранения системных сообщений;

2) основанный на распределенных по сети программных агентах – коллекторах, установленных на каждом объекте защиты, который генерирует ЖРС. Коллектор представляет собой резидентную программу (так называемый демон) и модули (библиотеки), которые локально занимаются сбором событий, извлечением данных и их первичной обработкой и передают полученные данные в соответствующую подсистему на централизованный сервер *SIEM*-системы, выполняющий последующие разнообразные проверки и выделяющий аномалии в поведение АО, ИС, сервисов и злоупотребления работников. В большинстве *SIEM*-систем имеется сразу несколько коллекторов, которые размещаются в иерархическом порядке для сбора событий ИБ от СЗИ, сетевого оборудования, устройств конечных пользователей, различных серверов и т.д.

Полная последовательность последующих действий с собранными данными в *SIEM*-системе выглядит следующим образом: нормализация, фильтрация, агрегирование, классификация и корреляция данных, анализ отобранных событий и их приоритезация, визуализация обработанной информации, генерация отчетов и принятие решений по событиям ИБ.

Чтобы наиболее полно и результативно решать назначенные задачи и выполнять перечисленные действия, *SIEM*-системы требуют частой настройки и актуализации правил и политик, поскольку они работают в постоянно меняющейся динамической среде ИТКС. Предупреждениями об опасности компрометации элементов ИТКС служат оповещения *SIEM*-систем, как и сигналы тревоги СОВ/СПВ.

Несмотря на 15-летний период развития *SIEM*-систем, проведенный в рамках данного исследования анализ показал полное отсутствие на международном и национальном уровне каких-либо документов, посвященных их проектированию, внедрению и использованию. Но нужно отметить, что несколько лет назад международная организация по стандартизации *ISO* создала соответствующий проект с номером 27044 в рамках серии 27000. Но, к сожалению, через год после этого информация об этом проекте с сайта *ISO* исчезла по неустановленным причинам.

В своем развитии до настоящего момента *SIEM*-системы прошли путь от простейшего первого поколения конца 1990-х годов до более совершенного второго, применяемого в современных сетях. Первые лишь устанавливали наличие событий ИБ за счет настроенных в них

правил и простейших методов корреляции собранных данных, вторые осуществляют поведенческий и контекстный анализ всех собранных данных. Оба поколения *SIEM*-систем проанализированы далее как используемые в ЦМБ и ЦИБ соответственно.

4.2. Эволюция центров управления безопасностью

Одним из известных действенных способов изучения и предотвращения катастроф и других кризисных ситуаций является появление и развитие ситуационных центров. В России одним из первых прототипов таких центров стал оперативный штаб по ликвидации последствий Чернобыльской аварии в 1986 г., на базе которого возник ситуационный центр МЧС. Еще один подобный центр был создан при Совете Безопасности. Свои ситуационные центры есть в федеральных органах государственной власти, Минкомсвязи, Газпром Энергохолдинге, Банке России, многих крупных корпорациях. Эти центры предназначены для оперативного принятия управленческих решений на основе мониторинга состояния объектов различной природы. Они обобщают текущие данные, анализируют имеющиеся в распоряжении средства защиты, рекомендуют те или иные меры, противодействующие возникновению или развитию опасных ситуаций. Традиционные ситуационные центры можно подразделить на три вида: оперативно-диспетчерские центры, центры анализа и управления кризисными ситуациями и информационно-аналитические центры.

Для реагирования на сетевые атаки в интернете, а именно на первый компьютерный «червь Морриса», в 1988 г. в Университете Карнеги-Меллона (США) была создана первая Группа реагирования на компьютерные инциденты (англ. *Computer Emergency Response Team, CERT*). Основным назначением этой группы экспертов был сбор данных для последующего реагирования на подобные происшествия. Далее во многих странах стали появляться аналогичные группы, которые часто называли себя Группой реагирования на инциденты компьютерной безопасности (англ. *Computer Security Incident Response Team, CSIRT*) [167, 184, 193].

Так в конце 1990-х годов в качестве организационной основы процесса мониторинга ИБ в компьютерных сетях появились специализированные ЦМБ (англ. аббревиатура *SOC*, которая именно в таком написании чаще всего и используется и в русскоязычных публикациях, посвященных ЦМБ) со специально подобранными СЗИ и квалифицированным персоналом. Большинство работ по тематике ЦМБ были опубликованы в конце 1990-х – начале 2000-х годов [13, 14, 194-202]. Вклад компании Cisco Systems в зарождение идеи ЦМБ, его построение, рекомендации по эксплуатации и техническому обслуживанию трудно переоценить с 1998 г. и по настоящее время [10-12, 203]. Публикации последователей Cisco в большей степени посвящены различным областям применения и рассматривают в основном используемые инструменталь-

ные средства защиты компьютерных сетей [204-207]. Они ориентированы либо на технологии, исключая при этом людей и процессы, либо наоборот – на процессы и людей без рассмотрения технологий и средств.

И, как в случае с *SIEM*-системами, на основе проведенного анализа следует вывод, что при значительном периоде существования на международном и национальном уровне отсутствуют какие-либо документы, посвященные проектированию, внедрению и использованию ЦМБ. Далее подробно проанализированы функции и выделены недостатки ЦМБ, предопределившие переход ко второму поколению центров, называемых ЦИБ.

4.3. Центры мониторинга безопасности

4.3.1. Цели и задачи Центров мониторинга безопасности

Ключ к более результативной автоматизации работ по обработке информации и событий ИБ заключается в создании ОРГАНИЗАЦИЕЙ собственного специализированного элемента под названием ЦМБ [10-15, 202].

С организационной точки зрения ЦМБ – это централизованное подразделение, которое занимается вопросами мониторинга ИБ на организационном уровне, а также плюс созданная для обнаружения, анализа, подготовки отчетности и реагирования на инциденты ИБ группа, состоящая в основном из операторов, работающих с текущими данными, и аналитиков безопасности, которые выполняют углубленный анализ собранных данных [208]. Аналитики безопасности осуществляют анализ ранее не происходивших и неизвестных событий ИБ и новых уязвимостей, опираясь на различные источники и исторические данные самой ОРГАНИЗАЦИИ (в случае ЦМБ срок давности таких данных обычно составляет от нескольких дней до месяца). У них должно быть четкое понимание локальной, региональной и глобальной среды и событий, которые могут повлиять на безопасность функционирования ИТКС и, как следствие, деятельности ОРГАНИЗАЦИИ в целом. Штат ЦМБ зависит от размера и сложности ИТКС ОРГАНИЗАЦИИ.

С технической точки зрения – это детально разработанные процессы мониторинга ИБ ИТКС с предопределенными процедурами реагирования в конкретных ситуациях и взаимодействия с различными подразделениями внутри самой ОРГАНИЗАЦИИ и другими структурами (в случае необходимости), а также арсенал специализированных средств для автоматизации такой деятельности и, в первую очередь, *SIEM*-системы первого поколения (*SIEM*-системы 1.0), находящиеся в ведении ЦМБ. Однако в публикациях иногда возникает дискуссия на тему, можно ли построить ЦМБ без этой системы. Для большинства специалистов в области ИБ очевиден ответ «нет», например, аргументированный таким уважаемым экспертом из компании Gartner

как А.Чувакин [209]. Эту позицию разделяет и автор данного исследования, поскольку в ЦМБ необходима система для централизованного хранения и быстрого, максимально автоматизированного анализа записей различных ЖРС [188]. Будучи объединены с другими СЗИ для получения от них исходных данных для анализа, *SIEM*-системы служат своеобразным «единым окном» в данные об инцидентах ИБ, происходящих в ИТКС ОРГАНИЗАЦИИ. *SIEM*-системы, используемые для постоянного мониторинга событий ИБ и активности пользователей в ИТКС, могут обнаруживать инциденты ИБ посредством агрегирования больших объемов машинных данных в режиме близкого к реальному (так называемого мягкого реального) времени для последующего принятия обоснованных решений по управлению рисками ИБ для ИТКС. Они способны визуализировать события, которые без подобной автоматизации процессов могли бы остаться незамеченными. Именно поэтому *SIEM*-системы традиционно рассматриваются как ядро ЦМБ. Конечно, теоретически возможно построить ЦМБ и без *SIEM*-системы, но на практике такое практически не встречается.

ЦМБ исключает потребность вручную искать, собирать, оценивать, классифицировать, анализировать и, в конечном счете, дифференцировать и связывать с ИБ данные, полученные из многочисленных гетерогенных источников в ИТКС ОРГАНИЗАЦИИ [203]. Он непрерывно контролирует безопасность сетей, анализирует локально и дистанционно эксплуатируемые злоумышленниками уязвимости элементов ИТКС и может рассматриваться как ядро обеспечения сетевой безопасности в рамках ИТКС на операционном уровне управления ею. ЦМБ как основа для осуществления дальнейшей деятельности по реагированию на инциденты ИБ централизованно собирает данные с сотен СЗИ и обобщает их в единую картину состояния сетевой безопасности ИТКС, помогая персоналу ЦМБ быстро разобраться в текущей ситуации.

Сервисный и аналитический ЦМБ не только управляет всеми операциями по мониторингу ИБ в ИТКС ОРГАНИЗАЦИИ, но и осуществляет мониторинг с последующей оценкой и защитой собственной информации и информации других важных объектов защиты ИТКС, например, серверов, БД, подсетей подразделений, веб-сайтов и т.д. Для этого ЦМБ должен иметь все необходимое (ПО, аппаратные средства, организационные меры и инфраструктуру) для анализа собственных внутренних, периметровых и внешних сетевых соединений и сбора признаваемых в суде свидетельств при серьезных инцидентах ИБ в ИТКС и многое другое.

Не каждое нарушение ИБ в ИТКС обязательно приведет к немедленным критическим для деятельности ОРГАНИЗАЦИИ негативным последствиям, поскольку злоумышленникам обычно требуется время на выполнение нескольких предварительных шагов для получения начального доступа к отдельному элементу сети, а потом расширения зоны проникновения в ИТКС. Выявление и своевременное предупреждение такого рода действий на начальной стадии является лишь одной из многочисленных задач, которые могут быть решены с помощью ЦМБ.

ЦМБ может также помочь выявить источники атак, нацеленные на работников ОРГАНИЗАЦИИ (типа фишинг-атак через электронную почту), и дать им возможность сосредоточиться в первую очередь на решении задач бизнеса. Обнаружение *IP*-адреса хорошо известного ботнет-сервера внутри ИТКС, скорее всего, указывает на то, что одна или несколько ее систем были взломаны. Другим типичным подозрительным событием является доступ к БД или файлам с одной из рабочих станций с помощью *USB*-устройства, что бывает, когда одна из Политик ИБ, а именно политика ограничения использования *USB*, была нарушена и соответствующая защитная мера была обойдена.

ЦМБ в ИТКС должен работать в круглосуточном режиме и выполнять следующие типовые функции [210-212]:

- собственная эксплуатационная поддержка функционирования ЦМБ с командной консолью, используемой для выполнения различных команд расширенного администрирования (повседневной эксплуатации и управления), поиска неисправностей и решения возникающих проблем;
- отслеживания состояния активов ИТКС для их последующего восстановления после инцидентов ИБ;
- идентификация на основе результатов сканирования уязвимостей для последующего управления установкой обновлений для устранения найденных уязвимостей;
- анализ сетевого трафика и информации о потоках данных для поиска любых сведений, которые могут быть полезны для выявления неисправностей и отклонений от штатного функционирования всех элементов ИТКС и, в конечном счете, обнаружения событий ИБ;
- мониторинг устройств и связь с системами управления их конфигурированием и централизованного управления СЗИ, предназначенными для автоматизации и полного контроля их жизненного цикла, включая единое управление процессами конфигурирования, настройки политик, оценки статуса, генерации отчетов о функционировании и т.д.;
- управление информацией о безопасности на основе сбора ЖРС, их хранения, архивирования и подготовки соответствующей отчетности, используемой далее для управления рисками ИБ и их ранжирования на основе анализа воздействия на бизнес, включая пассивную оценку и активную обработку рисков ИБ;
- обработка данных о событиях/инцидентах ИБ, в том числе локальной ГРИИБ с непрерывной обратной связью и, при необходимости, эскалацией проблем на высшие уровни в ОРГАНИЗАЦИИ;
- осуществление действий по сбору свидетельств компьютерных преступлений для реконструкции инцидента ИБ в ИТКС в признаваемом при судебном расследовании порядке, включая идентификацию, сбор, сохранение, восстановление, анализ и представление фактов

нарушения ИБ и данных в цифровой форме для расследования инцидентов ИБ и т.п.

В поддержку выполнения перечисленных функций для ИТКС ОРГАНИЗАЦИИ должны быть определены и документально зафиксированы, как минимум, следующие процессы и процедуры:

- процесс и процедуры мониторинга ИБ ИТКС, включая процедуру мониторинга соблюдения требований по обеспечению ИБ ИТКС;
- процесс и процедура уведомления об обнаруженных событиях ИБ (по электронной почте, на мобильный телефон, в чат и т.д.);
- процесс эскалации проблем на высший уровень руководства при невозможности решить его в рамках ЦМБ;
- процедуры предоставления ежедневных услуг при функционировании ЦМБ;
- процедуры управления ЖРС;
- процедуры регистрации пользователей и изменения их регистрации в ИС ИТКС, включая процедуры входа и завершения работы персонала (смен, англ. *shift*) ЦМБ;
- процедуры регистрации событий ИБ и инцидентов ИБ;
- процедуры выявления уязвимостей и их последующего устранения;
- процедуры управления установкой обновлений безопасности (англ. *patch management*) и изменениями конфигурационных настроек различных элементов ИТКС;
- процедура вывода обработанных данных в виде соответствующей информационной панели (*dashboard*) на экран оператора/аналитика;
- процедуры расследования инцидентов ИБ.

Образно говоря, ЦМБ – это «глаза ПУИИБ» в ИТКС ОРГАНИЗАЦИИ [213], поскольку при осуществлении мониторинга ИБ в них собираются данные о реальном уровне ИБ всей ИТКС и ее отдельных элементов для последующего принятия обоснованных решений по корректировке этого уровня. Эти функции поддерживаются различными методами и средствами извлечения, фильтрации, нормализации, категоризации, корреляции и другими методами анализа и эвристики для определения того, какие вредоносные *IP*-адреса, *URL*, приложения и т.п. могут нанести вред элементам ИТКС и понять, какие уязвимости активов ИТКС чаще всего используются злоумышленниками.

4.3.2. Функции SIEM-системы 1.0 в Центрах мониторинга безопасности

Ключевыми функциями SIEM-системы 1.0 как единого интерфейса мониторинга ИБ для ЦМБ являлись сбор ЖРС, нормализация «сырых» данных, их агрегирование и корреляция, а также предоставление требуемой отчетности, точнее [213]:

— сбор ЖРС от гетерогенных источников ИТКС предоставляет данные для расследования и помогает улучшать обеспечения ИБ ИТКС для соответствия требованиям, сформулированным в различных документах;

— нормализация преобразует данные записей ЖРС от многочисленных систем в соответствии с общей моделью данных в сопоставимые форматы, позволяя ОРГАНИЗАЦИИ использовать их для единообразного анализа соответствующих событий ИБ, несмотря на изначально различное представление этих данных в первоисточниках;

— агрегирование уменьшает большие объемы данных о событиях ИБ путем, например, объединения повторяющихся записей об одном и том же событии ИБ или сохранения информации об определенном типе событий ИБ, а не о каждом из них;

— корреляция событий, собранных различными системами, для установления связей и взаимозависимостей между ними ускоряет обнаружение событий ИБ еще на стадии угроз для своевременного их устранения;

— отчетность различной направленности и детализации предоставляет агрегированные и скоррелированные данные о событиях ИБ как в режиме мягкого реального времени, так и в некотором обобщенном виде – в виде сводок.

Полученные от *SIEM*-системы 1.0 выходные данные дают ГРИИБ информацию для реагирования на критические проблемы и уязвимости. Следовательно, в ЦМБ *SIEM*-системы призваны помочь в достижении следующих целей при мониторинге событий ИБ в ИТКС ОРГАНИЗАЦИИ [48]:

— максимально автоматизировать деятельность и рутинные операции по анализу и составлению отчетности об уровне ИБ в ИТКС в соответствии с применимыми локальными, отраслевыми, международными и российскими правовыми и нормативными документами;

— выявлять несоответствия требованиям по обеспечению ИБ для активов и бизнес-процессов, изложенным во внутренних Политиках ИБ и документа регуляторов и аудиторов;

— предоставлять руководству и специалистам информацию о реальном уровне ИБ всей ИТКС и ее отдельных активов за счет проведенного *SIEM*-системой анализа всех собранных данных и получения обоснованной оценки рисков ИБ для последующего устранения найденных уязвимостей и снижения рисков ИБ;

— ускорять реакцию на появление событий и инцидентов ИБ и обеспечивать круглосуточное автоматизированное реагирование на них в соответствии с predetermined правилами корреляции и дальнейшей обработки;

— исключить необходимость увеличения количества ИБ-персонала вне зависимости от увеличения количества СЗИ, предоставляющих информацию о событиях ИБ, и сократить расходы на него, поскольку необходимо только изучить интерфейс одной *SIEM*-системы, а не

множества разнородных СЗИ, установленных в ИТКС.

При всех несомненных по сравнению с ручной обработкой достоинствах выделим и недостатки *SIEM*-систем 1.0, которые в основном заключаются в следующем:

- использование заранее заданных правил и методов корреляции требует ручного обновления и расширения только экспертом;

- корреляция была реализована в основном для *IP*-адресов, что сегодня практически бесполезно при растущем числе мобильных и удаленных пользователей и изменении адресов, которые использует один пользователь в течение одного дня, хотя отдельные системы были способны сопоставлять использование портов и протоколов с пользователями;

- ЖРС, анализируемых *SIEM*-системой, не всегда содержат достаточно подробностей, необходимых для понимания того, что на самом деле происходит в ИТКС в данный момент. Например, журналы могут оповещать о ненормально длинных строках запроса, неавторизованном туннелировании или шифровании. Но они не могут помочь обнаружить конкретную активность пользователя или вредоносной программы в определенном контексте, использование неавторизованных инструментов, таких как *Tor*, использование протокола *SSL* (англ. *Secure Socket Layer* – уровень защиты сокетов) по необычным портам, нестандартный сетевой трафик, аномалии протоколов, несанкционированные подключения и т.д., о чем свидетельствуют исследования, например, компании *Verizon*, согласно которым в ЖРС не были обнаружены 99 % успешных атак [214];

- *SIEM*-системы 1.0 используют реляционные БД, имеющие следующие ограничения: малое семантическое разнообразие и очень простые структуры, отсутствие поддержки рекурсии и наследования, недостаток обработки/триггеров, что ограничивает возможности обнаружения событий ИБ;

- отсутствие глубокой интеграции *SIEM*-системы в ИТКС ОРГАНИЗАЦИИ и т.д.

4.3.3. Классификация Центров мониторинга безопасности

Существует ряд решений для создания ЦМБ, отличающихся стоимостью, производительностью и реализуемыми функциями. Для выбора под специфические требования конкретной ОРГАНИЗАЦИИ необходимо определить критерии, которые описывали бы ЦМБ с разных точек зрения. На основе анализа таких продуктов была разработана системная классификация ЦМБ (табл. 15). Основными классификационными признаками типов ЦМБ определены тип управления, сценарии и цель развертывания, вариант реализации, возможность ответных действий и метод корреляции данных о событиях ИБ [210-212].

Таблица 15 – Системная классификация ЦМБ для внедрения в ИТКС ОРГАНИЗАЦИИ (начало)

<i>Классификационный параметр</i>	<i>Содержание параметра</i>	<i>Описание</i>
<i>Тип управления</i>	Внутренний (собственный, коммерческий, выделенный)	<i>Преимущества:</i> собственные знания ОРГАНИЗАЦИИ об ИТКС точнее и шире, чем у третьей стороны; поэтому легче настроить более результативные решения; больше вероятность заметить корреляции в пределах ИТКС; меньшая стоимость. <i>Недостатки:</i> большие начальные инвестиции, которые как можно быстрее должны показать эффективность ЦМБ; проще сговор между нарушителем и группой, осуществляющей мониторинг ИБ ИТКС; меньше вероятность выявить известные профессионалам шаблоны событий ИБ, накопленные за многолетний опыт работы аутсорсинговой компании.
	Внешний (аутсорсинговый)	<i>Преимущества:</i> отсутствие капитальных вложений; часто дешевле; меньше возможности сговора между нарушителем и группой, осуществляющей мониторинг ИБ ИТКС; беспристрастность; <i>SLA</i> . <i>Недостатки:</i> меньше знаний об ИТКС; снижение бдительности персонала ОРГАНИЗАЦИИ; риск неправильного обращения с данными вне ОРГАНИЗАЦИИ; ненадежность для долгосрочной перспективы использования.
	Совместное управление	Внутреннее ИТ-подразделение ОРГАНИЗАЦИИ тесно связано с привлеченным сторонним разработчиками для решения задач совместного управления выполнением требований по обеспечению ИБ.
<i>Сценарий развертывания</i>	Централизованный	ЦМБ базируется на выделенном сервере, который выполняет все функции по мониторингу ИБ ИТКС. <i>Преимущества:</i> скорость, простота установки и относительно низкая стоимость. <i>Недостаток:</i> ЦМБ подходит только для небольших и средних сетей (менее 100 СЗИ).
	Распределенный	ЦМБ использует несколько устройств/серверов, одновременно выполняя балансировку нагрузки между ними. Распределение нагрузки может быть основано на географическом (различные серверы отвечают за разные части ИТКС) или функциональном (часть функций выполняется одним сервером, часть другим) принципе. Поскольку используются несколько устройств, стоимость ЦМБ больше, а его развертывание и обслуживание сложнее. Но в целом балансировка нагрузки дает более высокую производительность и эффективность ЦМБ.
<i>Цель развертывания</i>	Контроль	ЦМБ позволяет в динамике наблюдать за уровнем ИБ объектов ИТКС и с помощью экспертов прогнозировать его изменение.
	Управление	ЦМБ помогает активно воздействовать на ИБ объекта за счет принятия обоснованных и своевременных решений.
	Антикризисное управление	ЦМБ начинает функционировать только во время кризисной ситуации.

Таблица 15 – Системная классификация ЦМБ для внедрения в ИТКС ОРГАНИЗАЦИИ (продолжение)

<i>Классификационный параметр</i>	<i>Содержание параметра</i>	<i>Описание</i>
<i>Вариант реализации</i>	Программный	ЦМБ создан на базе специализированного ПО, установленного на одном/нескольких серверах. Преимущество: возможность использования серверов ЦМБ для решения дополнительных задач.
	Аппаратный	ЦМБ – «коробочное» решение на базе одного/нескольких серверов с предварительно установленным ПО. Преимущество: снижение времени развертывания. Поскольку это изолированная среда, на серверах ЦМБ нельзя устанавливать никакое дополнительное ПО.
	Виртуальный	У службы безопасности нет выделенного объекта для ЦМБ. Она работает удаленно.
	Инфраструктурный	ЦМБ построен с использованием имеющихся ПО и аппаратных средств (например, имеющаяся БД Oracle используется для хранения событий. Консолидация нескольких БД реализуется с использованием репликации. Нормализация, агрегирование и корреляция реализуются в БД с помощью <i>SQL</i> -скриптов и т.д.). <i>Преимущества</i> : относительно низкая стоимость решения и повышенная гибкость. <i>Недостатки</i> : необходимость доработки ЦМБ, включая правила нормализации, агрегирования и корреляции, и использование <i>SQL</i> -программирования для реализации этих правил.
	Глобальный, национальный, командный	ЦМБ как структура более высокого уровня, которая наблюдает за ЦМБ более низкого уровня в одном большом регионе.
<i>Возможность ответных действий</i>	Пассивная (без ответных действий)	ЦМБ работает как классическая пассивная СОВ: на основе анализа данных она контролирует и осуществляет приоритезацию событий ИБ. В случае обнаружении атаки никаких ответных действий не предпринимается. ЦМБ обычно используется в средах с высокими требованиями к доступности (например, в банковском секторе или медицине), поскольку ложные срабатывания не требуют создания правил безопасности и блокировки сервисов. Основная цель такого ЦМБ: обработка информации об ИБ, визуализация и установление приоритетов событий ИБ, а также соблюдение нормативных требований.
	Активная (с возможностью ограниченных ответных действий)	ЦМБ строится на концепции СПВ: атака не только обнаруживается, но и проводятся ограниченные ответные действия по недопущению ее распространения. ЦМБ «понимает» составляющие атаки, например, адреса смежных взломанных систем в ИТКС. Автоматически определяется доступное устройство блокировки атаки на пути ее распространения, на котором автоматически запускаются соответствующие команды для быстрого и точного предотвращения или сдерживания атаки. ЦМБ обычно используется в средах с высокими требованиями к конфиденциальности. Быстрая, но ограниченная автоматическая реакция на угрозы ИБ является его основным преимуществом.

Таблица 15 – Системная классификация ЦМБ для внедрения в ИТКС ОРГАНИЗАЦИИ (продолжение)

<i>Классификационный параметр</i>	<i>Содержание параметра</i>	<i>Описание</i>
Метод корреляции	Без корреляции	ЦМБ подходит для небольших сетей, где он выполняет только агрегирование информации об ИБ, а все решения принимаются и выполняются персоналом ЦМБ.
	На основе <i>SLA</i>	ЦМБ связывает события ИБ с важными для ОРГАНИЗАЦИИ требованиями <i>SLA</i> , что помогает оценить потери от взломанных и вышедших из строя элементов ИТКС. ЦМБ строит модели бизнес-процессов и анализирует влияние различных инцидентов ИБ на эти процессы. <i>Недостаток</i> : основные трудности заключаются в определении состава бизнес-процессов и активов, их стоимости (эти трудности естественны для процессно-ориентированного подхода при анализе рисков ИБ).
	Статистическая	Для определения серьезности инцидента ИБ в ИТКС применяются статистические алгоритмы, а затем угрозе ИБ присваивается оценка, основанная на стоимости затрагиваемого угрозой актива. Анализируется поведение ИТКС и в зависимости от наличия и вероятной тяжести аномальных событий идентифицируются угрозы ИБ. Также измеряется эффективность, так как с течением времени число аномальных событий должно уменьшаться по мере того, как ИТКС становится более защищенной. <i>Преимущества</i> : в процессе работы ЦМБ не требуется специальных знаний о моделях угроз ИБ или сценариях атак и до начала его работы не требуется определения правил или эталонного базового уровня (статистически нормального состояния), что помогает в определении приоритетов событий ИБ, основанных на стоимости активов ИТКС.
	На основе правил	Для выявления в течение заданного временного интервала вероятных сценариев атак при наблюдении определенного ряда событий ЦМБ использует предварительно установленные правила условной логики. Правила могут быть «из коробки» разработчика ЦМБ или заданы ОРГАНИЗАЦИЕЙ после детального анализа своего сетевого трафика, что результативно при определении конкретных угроз ИБ на основе предварительных знаний о моделях атак. Многие ЦМБ реализуют конечный набор правил для самых общих сценариев, но они могут быть дополнены правилами ОРГАНИЗАЦИИ. Поэтому важна поддержка в написании новых правил со стороны производителя. Правило может применяться к происходящему во времени событию, тогда менеджер правил сохраняет состояние события в течение разумного периода времени до того, как другие важные события вызовут предупреждение об опасности или истечет лимит времени для исходного события. В ином случае будет много ложных срабатываний, или, что более важно, нельзя будет определить «слабые и медленные» атаки, которые характеризуются малым количеством ежедневных событий в течение длительного временного интервала. <i>Недостатки</i> : требуется много времени для поддержания в актуальном состоянии сотен правил, слишком много ложных положительных и отрицательных срабатываний для постоянно обновляемых нарушителями ИБ методов атак.

Таблица 15 – Системная классификация ЦМБ для внедрения в ИТКС ОРГАНИЗАЦИИ (окончание)

<i>Классификационный параметр</i>	<i>Содержание параметра</i>	<i>Описание</i>
	На основе уязвимостей	ЦМБ берет данные о событиях ИБ от сетевых СОВ и соотносит их с БД известных уязвимостей и профилями уязвимостей для хостов из САЗ, присваивая определенное значение каждому активу. Это помогает уменьшить ложные положительные срабатывания за счет уменьшения «шума» в работе САЗ, а также помогает персоналу ЦМБ определить, какие атаки реальны и какие активы фактически уязвимы для атак. <i>Преимущества:</i> наиболее результативны при распознавании сценариев конкретных атак, в том числе новых для ИТКС сценариев, и особенно подходят для устранения ложных положительных срабатываний и увеличения результативности за счет фокусировки на реальных событиях ИБ, которые соответствуют имеющимся уязвимостям. <i>Недостатки:</i> требуется создание правил корреляции атак, использующих особые уязвимости особо подверженных им активов, а написание таких правил чрезвычайно трудоемко.
	На основе соблюдения требований	ЦМБ связывает события ИБ с существующими законами, нормативными актами, стандартами в области ИБ, ведомственными документами и Политиками ИБ самой ОРГАНИЗАЦИИ. Он требует специальной «ручной» установки и настройки, поскольку каждая ИТКС имеет свои собственные Политики ИБ.
	Смешанная	Когда все типы корреляции применяются совместно, они могут значительно улучшить обнаружение реальных событий ИБ и повысить эффективность управления ИБ. Работа сотрудников ЦМБ становится проще, когда они могут получать единый профиль риска для события ИБ на основе взаимосвязанных статистических данных об угрозах, основанных на правилах предупреждения, имеющихся уязвимостях и стоимости затрагиваемых активов.

Данная классификация не претендует на полноту, поскольку на ее основе ОРГАНИЗАЦИЯ может составить собственный расширенный набор признаков ЦМБ при разработке и внедрении своего ЦМБ.

4.3.4. Ограниченность Центров мониторинга безопасности

Традиционные ЦМБ с устаревшими *SIEM*-системами 1.0, работающими на основе правил, хорошо справлялись с задачей защиты от традиционных атак несколько лет назад. В настоящее время ИТКС как единое целое часто не является конечной целью злоумышленников; наоборот, их интересуют оконечные устройства, поскольку ценные данные часто находятся именно там. Атаки характеризуются большей целенаправленностью, продуманностью, подготовленностью, использованием скрытных технологий взлома (например, *APT*-атаки и атаки на стороне клиента). Можно сделать вывод, что первые ЦМБ не были рассчитаны на растущие объемы данных, относящихся к ИБ современных гетерогенных ИТКС, и им не удавалось сохранять полный контроль над сложной сетевой ситуацией и поддерживать требуемый уровень ИБ ИТКС должным образом.

На основе анализа первоисточников, описывающих практический опыт внедрения и использования ЦМБ, были выявлены следующие серьезные ограничения их функциональных возможностей [213, 215]:

- невозможность работы в крупномасштабных, гетерогенных, сильно распределенных и сложно связанных ИТКС с подключением пользователей из любого места в любое время;
- ручная интеграция различных технологий защиты в едином ЦМБ;
- недостаточная гибкость и производительность ЦМБ для обработки больших объемов ранее накопленных (исторических), только что собранных и аналитически выведенных на их основе данных, известных как «технологии больших данных»;
- невозможность обеспечить высокую степень надежности/устойчивости при сборе, передаче и обработке данных о событиях ИБ, что делает их уязвимыми к атакам на *SIEM*-систему и сам ЦМБ;
- зависимость от централизованных правил корреляции, обрабатываемых на одном узле, что затрудняет масштабируемость, создает уязвимости и единую точку отказа;
- ограниченные возможности анализа, оценки и визуализации уровня ИБ, поскольку ЦМБ осуществляет мониторинг событий на сетевом уровне и поиск неисправностей во внутренних элементах ИТКС, а также обеспечивает не очень сложную корреляцию;
- невозможность интерпретации данных более высоких уровней, таких как данные об услугах или деятельности;

— отсутствие реакции на выявленные атаки в режиме реального времени; в дополнение к автоматизированным операциям аналитики ЦМБ должны оценивать в режиме реального времени большие объемы данных, что практически не осуществимо, и далее вручную реагировать на них;

— использование *SIEM*-систем 1.0 в качестве ядра ЦМБ и, как результат, ограниченный набор источников ЖРС, из которых берутся данные для анализа, отсутствие унификации настроек на самом источнике и форматов представления данных в ЖРС, что влияет на качество записей, анализируемых *SIEM*-системой, и большое количество ложных положительных и отрицательных срабатываний (англ. *false positives, false negatives*) (ошибок первого и второго рода), поскольку на основе шаблонов (англ. *patterns*) выявляются лишь известные или простые в обнаружении события ИБ.

На основе этих недостатков можно сформулировать требования к более функциональным, чем ЦМБ, ЦИБ ИТКС ОРГАНИЗАЦИИ, среди которых ключевыми являются следующие [216]:

- максимальная автоматизация рутинных операций не только по мониторингу ИБ, но и полноценному управлению инцидентами ИБ в ИТКС, приближающая реагирование на инциденты ИБ к режиму реального времени и по возможности предотвращающая их возникновение;
- создание полной видимости происходящего в ИТКС;
- анализ не только состояния, но и поведения всех элементов ИТКС и ее пользователей в определенном контексте для немедленного выявления отклонений по сравнению с нормальным поведением или функционированием, а не просто обнаружение на основе сигнатур, которые требуется постоянно обновлять и пополнять;
- поддержание требуемого ОРГАНИЗАЦИЕЙ уровня ИБ в ИТКС в течение длительного времени без необходимости обращения к экспертам.

4.4. Концепция интеллектуальной безопасности

В начале 2000-х ЦМБ еще эффективно справлялся со стоящими перед ним проблемами в не очень нагруженных ИТКС организаций. Но постепенно за 10 лет существования и по мере усложнения сетевой среды за счет появления новых технологий и возросшего потока передаваемых данных возможностей ЦМБ для их обработки стало не хватать. ЦМБ перестал справляться с объемами, скоростью возникновения атак и хорошей оснащенностью нарушителей ИБ. Новая реальность более частых и сложных атак и «взлом как услуга» (англ. *hacking as a service*) сделала атаки на ИТКС организаций более профессиональными, доступными и достигающими цели. Появились новые угрозы ИБ и их источники. В дополнение к существующим обнаруживались

новые уязвимости. Влияние ИБ на деятельность практически любой организации стало критическим как с точки зрения прямых финансовых потерь, так и репутации. Организации должны были противопоставить этому надлежащим образом разработанные и централизованные средства управления ИБ своих ИТКС, сочетающие в себе более совершенные *SIEM*-системы и СЗИ, потоковую обработку связанных с ИБ больших данных, работу в соответствии с едиными и постоянно контролируруемыми и модифицируемыми Политиками ИБ для соблюдения жестких требований различных правовых и нормативных документов. Для реализации такого подхода и автоматизации как можно большего числа рутинных операций по обработке и реагированию на инциденты ИБ, не требующих принятия решений экспертами, стал необходим более совершенный и высокопроизводительный ЦИБ ИТКС, чем традиционный ЦМБ [216].

В англоязычной литературе новый подход к обеспечению сетевой безопасности в 2010 г. получил названия *Security Intelligence* (что можно перевести на русский язык как «интеллектуальная безопасность») или *Security Analytics* или *Information Security Intelligence* («аналитика», «разведка» или «интеллект» в области ИБ). Суть этого подхода заключается в сборе, нормализации и анализе в режиме реального времени данных, генерируемых пользователями, приложениями и ИИ и показывающих ситуацию с уровнем ИБ и состоянием рисков ИБ в ИТКС ОРГАНИЗАЦИИ [217]. Просмотр ЖРС и исторических данных за больший период времени (от нескольких дней до нескольких месяцев), чем в случае ЦМБ, очень важен при расследовании инцидентов ИБ. Но важнее возможность понимания в режиме реального времени в конкретном контексте того, что происходит во всей ИТКС прямо сейчас, чтобы найти что-то необычное, отличное от штатного.

В другом определении интеллектуальной безопасности подчеркивается, что управляемая интеллектом защита компьютерных сетей – это стратегия управления рисками, которая рассматривает его компоненты, связанные с угрозами ИБ, включая анализ злоумышленников, их возможностей, целей и ограничений [217].

Таким образом, главная цель интеллектуальной безопасности заключается в том, чтобы создать упреждающее, прогнозирующее, действенное (реально работающее) понимание безопасности сети, которое на основе расширенной аналитики позволит снижать риски ИБ в ИТКС любой организации за счет ее всесторонней защиты [218]. Следовательно, концепция интеллектуальной безопасности заключается не просто в сборе данных, относящиеся к ИБ, а в формировании на их основе знаний для прогнозирования развития ситуации и постоянного опережения злоумышленников. Эти знания необходимы не только для тактического, но и, что еще важнее, стратегического совершенствования деятельности ОРГАНИЗАЦИИ в целом и ее СОИБ в частности. Именно поэтому разрабатываемый ЦИУСБ помещен на рис. 23 на верхний стратегический уровень управления ИБ, в то время как ЦИБ размещен на тактическом уровне.

Адаптируя идеи системного теоретика Р.Акоффа (R.Askoff) [219] к области ИБ, формулируем прогресс в результатах обработки данных следующим образом [213]:

— сначала просто собранные данные: набор символов (в случае компьютерных систем это машинные данные в виде набора «0» и «1»). Исходные данные сами по себе имеют ограниченную полезность;

— затем информация: данные, которые относятся к простым фактам и могут быть обработаны для использования при управлении ИБ ИТКС. Эта информация содержит ответы, по крайней мере, на вопросы «кто» (легальный пользователь/злонамеренный человек), «что» (предпринятые действия), «где» (с какого IP-адреса и местоположения) и «когда» (временная метка). Она также содержит смысловые взаимосвязи. Например, реляционная БД позволяет извлекать информацию из данных, хранящихся в ней, а SIEM-система решает проблему обработки потока событий, поступающих от СЗИ, отслеживает активность пользователей, анализирует события и инциденты ИБ посредством корреляции и агрегирования больших объемов машинных данных в режиме реального времени для управления рисками ИБ, визуализирует угрозы ИБ для элементов ИТКС и т.д.;

— и, наконец, знание (интеллект): соответствующий набор информации, который получается в результате ее обработки и анализа и который должен быть полезен с различных точек зрения для принятия решений. Осознанное понимание знания основано на истинной логической и аналитической способности и синтезе новых знаний из ранее накопленных знаний. Знание отвечает на вопросы «как» и «почему», например, о НСД и вредоносных действиях, а также о стратегиях смягчения последствий инцидентов ИБ и СЗИ, требуемых в конкретном контексте. Для управления ИБ SIEM-системы обладают некоторой способностью к пониманию в том смысле, что они могут синтезировать новые знания об угрозах ИБ в ИТКС, тенденциях развития сетевых атак и прогнозах обнаружения уязвимостей «нулевого дня» и т.д. из ранее сохраненной информации и предыдущих знаний.

Устоявшегося русскоязычного аналога понятия *Information Security Intelligence* на сегодня пока не сформировалось. Применяя компьютеризированную бизнес-аналитику в уникальной среде осуществления деятельности, конкурентоспособные организации преуспевают в значительной степени потому, что они знают, как заставить работать всю свою информацию на благо бизнеса и получить максимально возможную отдачу от накопленных терабайт и петабайт данных. Данные становятся новым «бизнес-сырьем», наравне с трудом и капиталом. Аналогичный подход следует применять и к защите этой информации.

По аналогии с «*Business Intelligence*», что переводится как бизнес-аналитика, далее будет использовать наиболее подходящий с точки зрения автора данного исследования краткий термин – «**ИБ-аналитика**» (в др.-греч. *ἀναλυτική* – искусство анализа) [216]. Как бизнес-аналитика

помогает организациям принимать решения, максимизирующие их возможности и минимизирующие бизнес-риски, так и ИБ-аналитика позволяет им качественнее идентифицировать потенциальные угрозы и риски ИБ, выявлять области несоответствия различным требованиям и устанавливать приоритеты в области обеспечения ИБ.

ИБ-аналитика (далее для краткости будет использоваться именно этот термин, а не более длинный «интеллектуальная безопасность»), построенная на тех же понятиях, что и столь значимая для современных организаций бизнес-аналитика, является следующим очень важным шагом для тех из них, кто признает важность обеспечения ИБ для деятельности ОРГАНИЗАЦИИ.

ИБ-аналитика базируется, например, на таких видах анализа данных, что важно для ЦИУСБ:

- корреляционном – вид анализа данных, предназначенный для выявления признаков инцидентов ИБ на основе данных о зарегистрированных событиях ИБ при их совместном рассмотрении; данный вид анализа использует статистический метод изучения взаимосвязи между двумя и более событиями ИБ;

- контекстном – вид анализа данных, при котором учитывается контекст (содержание, временные метки, атрибуты и т.п.), в котором происходят события ИБ, и само содержание с точки зрения ИБ события ИБ;

- поведенческом – вид анализа данных, при котором исследуется поведение различных объектов (систем, ПО, АО, пользователей и т.п.) и выявляются отклонения наблюдаемого поведения от ожидаемого (часто представленного профилем поведения);

- структурном – вид анализ данных, использующий ранее описанные системные классификации уязвимостей, угроз ИБ, сетевых атак и инцидентов ИБ для определения их места в структурной организации данных.

Основными целями ИБ-аналитики являются следующие:

- 1) передавать процессу принятия решений большие объемы информации, имеющей значение для обеспечения ИБ, уменьшая миллиарды единиц первично собранных данных до разумного, обозримого количества действительно значимых для обеспечения ИБ;

- 2) применять сложный анализ собранных данных за счет автоматизации всех процессов и простоты использования соответствующих средств;

- 3) предоставлять приложения, которые помогают организациям извлекать максимальную пользу из своих данных для понимания и контроля рисков ИБ, выявлять проблемы и представлять приоритеты в обеспечении ИБ;

- 4) подтверждать правильность Политик ИБ и степень соответствия их выполнения, как и других требований по обеспечению ИБ, сформулированных в применимых к ОРГАНИЗАЦИИ

нормативных и правовых документах;

5) гарантировать, что используемые процессы и меры обеспечения ИБ результативно воплощают все требования по обеспечению ИБ.

В зависимости от уровня управления ИБ для ИТКС ОРГАНИЗАЦИИ, на котором применяется ИБ-аналитика, можно выделить три ее основных типа [215]:

1) *стратегическая ИБ-аналитика*, связанная с анализом подверженности конкретной ИТКС ОРГАНИЗАЦИИ компьютерным атакам и рассматривающая угрозы ИБ ИТКС с точки зрения текущих и будущих рисков ИБ и функциональной устойчивости всей ИТКС. Основные источники информации для стратегической ИБ-аналитики – это Модель угроз ИБ и Модель нарушителей ИБ для ИТКС и отчеты об уровне ИБ ИТКС. В рамках данной деятельности происходит анализ и интерпретация возможной применимости известных тактик и методов атак нарушителей ИБ (например, согласно модели *MITRE ATT&CK*, рассмотренной в разделе 2.4) для конкретной ИТКС ОРГАНИЗАЦИИ;

2) *совмещенная тактическая и операционная ИБ-аналитика*, идентифицирующая и исследующая конкретные индикаторы взлома (*IoC*) в ИТКС, что повышает качество обнаружения и предупреждения потенциальных нарушений ИБ и инцидентов ИБ в ИТКС, а также выделяет специфические риски ИБ, связанные с конкретными уязвимостями элементов ИТКС и зависящие от персонала ОРГАНИЗАЦИИ. Основные источники информации для ИБ-аналитики – как исторические данные самой ОРГАНИЗАЦИИ, так и упомянутые в разделе 2.3 внешние источники аналитики и обмена знаниями об угрозах ИБ (*Threat Intelligence*) со списками *IoC* и документами, описывающими компьютерные атаки, а также базы уязвимостей типа Базы угроз ИБ ФСТЭК России, *CVE*, *NVD* и пр.;

3) *прикладная ИБ-аналитика*, позволяющая отследить глобальные тенденции в области ИБ и использующая их при создании более защищенных решений для ИТКС с эффективностью и результативностью, отраженными с помощью метрик либо самой ОРГАНИЗАЦИИ, либо общепринятых международных и российских документов. Например, коэффициент возврата инвестиций (англ. *Return On Investment, ROI*), связанный с покупкой СЗИ, является метрикой эффективности. Скорость обнаружения событий ИБ является метрикой результативности наравне с тем, как с применением ИБ-аналитики обрабатываются, локализуются, изолируются и устраняются инциденты ИБ, а затронутые инцидентом объекты восстанавливаются.

Для успешного использования ИБ-аналитики требуются самые разнообразные данные, характеризующие весь контекст функционирования конкретной ИТКС ОРГАНИЗАЦИИ. При соблюдении этого условия ИБ-аналитика полезна тем, что в рамках каждой потенциально проблемной области ИТКС собранные данные будут проанализированы в специфичном для нее контексте и будут выполнены сложные аналитические преобразования, позволяющие увидеть

возрастающее количество различных типов событий ИБ в ИТКС для быстрого реагирования на них и предотвращения их возникновения в будущем.

В [213] автором данного исследования обобщены следующие основные преимущества ИБ-аналитики при ее использовании в целях управления инцидентами ИБ, которые далее сформулированы применительно к ИТКС ОРГАНИЗАЦИИ:

— целостный подход, означающий, что ОРГАНИЗАЦИЯ рассматривает каждый аспект управления инцидентами ИБ для ИТКС в тесной взаимосвязи с другими аспектами управления ИБ и шире, чем просто снижение рисков ИБ путем устранения уязвимостей, а также учитывает возможности и мотивацию нарушителей ИБ ИТКС;

— встроенная и согласованная с потребностями бизнеса система управления ранжированными рисками ИБ ИТКС, включающая в себя соотнесение угроз ИБ для конкретных активов ИТКС с их уязвимостями, ценностью, необходимостью управления СЗИ, исправлениями, соответствием, аудитом ИБ, интегрированными функциями контроля всех изменений и подозрительной активности и т.д.;

— лучшее непрерывное (24x7) понимание общей ситуации с обеспечением ИБ ИТКС, сочетающее в себе локальные наблюдения мониторинга ИБ, внешнюю ИБ-аналитику и внутреннюю разведку угроз ИБ («охоту за угрозами ИБ») и поддерживаемое постоянной видимостью общей ситуации «в одном окне»;

— более сфокусированный и углубленный подход, позволяющий на нескольких стратегических уровнях эшелонированной защиты ИТКС рационально выделить требуемые на защиту от конкретных инцидентов ИБ ресурсы с учетом установленных приоритетов;

— адаптивный (гибкий) и ориентированный на конечный результат с прогнозированием, упреждающий подход к угрозам ИБ, основанный на показателях определенных метрик ИБ для принятия более быстрых и обоснованных решений посредством интеграции исходной информации в режиме реального времени;

— расширенная контекстная аналитика, означающая возможность выявления скрытых и подозрительных связей между пользователями, учетными записями, приложениями и другими сущностями ИТКС на ранних стадиях, например, сопоставления хостов, приложений и активности пользователей, их геолокации, телеметрии сетевого трафика, наблюдаемых событий и т.д. с ЖРС систем, приложений, серверов, СЗИ и т.п. с шаблонами и тенденциями (а не анализ события за событием);

— перекрестная корреляция поведения различных объектов, которая инициирует приоритетные оповещения и автоматизированные реакции на основе оценок рисков ИБ, связанных с конкретными услугами и комбинациями событий или порогов изменения конкретных показателей;

— автоматическая коррекция разных проблем в обеспечении ИБ, «белых»/«серых»/«черных» списков, предупреждений об опасности от СЗИ, обновлений и изменений конфигурационных настроек для закрытия и возможной эскалации инцидентов ИБ в соответствии с существующими инструкциями или требованиями;

— базовое обнаружение аномалий на основе выявления нетипичных действий — после определения «нормального» события такие действия «подсвечиваются» особым образом (помещаются в зону особой видимости) и для них с помощью экспертов или на основе машинного обучения (что предпочтительнее) создаются новые шаблоны для последующего применения;

— широкое использование информации об угрозах ИБ из внешних источников (открытых, частных или коммерческих, таких как репутация и «черные» списки IP/доменных имен, структурированные и неструктурированные сообщения, электронные почтовые сообщения из групп и т.д.) усовершенствует внутренние поведенческие (англ. *behaviour-based*) и базовые методы обнаружения;

— постоянная запись истории связанных с ИБ событий, а не просто сохранение отдельных событий;

— возможность распараллеливания потока работ для ускорения обработки больших данных и, в конечном счете, преимущественно автоматизированного реагирования на инциденты ИБ;

— повышение эффективности (с точки зрения снижения затрат и сложности реагирования на инциденты ИБ и повышения точности обнаружения атак на основе мгновенного понимания всей цепочки стадий атаки, а не отдельных событий и конкретных используемых злоумышленниками инструментов) за счет активизации централизованной защиты от выявленных угроз ИБ с общим хранилищем «сырых» и уже проанализированных данных и общими инструментами документооборота;

— комплексная информационная панель (*dashboard*) для визуализации полученной в результате анализа информации об ИБ ИТКС, согласованная с метриками ИБ и предоставляющая понятную для ИБ-персонала интерпретацию, и т.д.

В заключении данного раздела кратко сформулируем основные особенности ИБ-аналитики [180]:

— Основная идея: более глубокая аналитика всей относящейся к ИБ информации с единой консолью, менее «навязчивая» и отделенная от информационных потоков самой ИТКС, для преимущественно автоматизированного реагирования на инциденты ИБ;

— Основное содержание деятельности: управление ЖРС, мониторинг активности приложений и пользователей, обнаружение уязвимостей элементов ИТКС и угроз ИБ для них, управление рисками ИБ, проверка соответствия всем применимым требованиям по обеспече-

нию ИБ, управление реагированием на инциденты ИБ;

— Источники данных: все структурированные и неструктурированные данные ОРГАНИЗАЦИИ, связанные с ИБ, из всех гетерогенных источников, характеризующих функционирование ИТКС ОРГАНИЗАЦИИ в целом и каждого ее элемента и пользователя в отдельности;

— Аналитика: расширенная аналитика, включающая контекст всех сетевых событий, элементов ИТКС, приложений, услуг и пользователей;

— Реакция на нарушение ИБ: обнаружение нарушений в режиме реального времени/близкому к реальному времени, часто с исправлением в тот же день;

— Количество управляемых устройств, событий в секунду, хранилище: не ограничены, в зависимости от уникальных для каждого решения требований к масштабированию;

— Конечные пользователи: служба ИБ и проверки соответствия требованиям, операторы, аудиторы, аналитики;

— Основные ограничения: не сформированы руководящие органы по разработке международных и российских нормативных и правовых документов по ИБ-аналитике, и интеграция конкретных решений со сторонними продуктами/источниками данных по-прежнему трудоемка.

4.5. Центры интеллектуальной безопасности

4.5.1. Назначение Центров интеллектуальной безопасности

Концепция интеллектуальной безопасности нашла свое воплощение в центре полноценного управления (а не просто мониторинга) ИБ ИТКС ОРГАНИЗАЦИИ второго поколения — ЦИБ. Он имеет интегрированную архитектуру защиты от компьютерных атак и объединяет полную прозрачность и контекстно-управляемый интеллект с действенным и всеобъемлющим пониманием и управлением знаниями в области ИБ [220], что позволяет постоянно контролировать ИБ ИТКС и связанных с ней элементов ЕИП ОРГАНИЗАЦИИ. Внедряя ЦИБ, ОРГАНИЗАЦИЯ получает целостный и глубокий детальный взгляд на «здоровье» своей ИТКС и возможность не только обнаруживать и реагировать на атаки, но и результативно бороться с новыми угрозами ИБ, прежде чем они причинят вред, а также предотвращать инциденты ИБ, постоянно собирая и обобщая знания о сетевых атаках и уязвимостях в контексте конкретной ИТКС [215]. В России ЦИБ, использующий искусственный интеллект, был создан, например, в ПАО «Сбербанк России», в 2016 г., в результате чего количество рассматриваемых в день подозрительных событий в работе систем увеличилось до нескольких миллионов (до создания ЦИБ банку удавалось проанализировать лишь 100-200 инцидентов в день) [221].

Как комплексное решение, ЦИБ с ИБ-аналитикой применительно к ИТКС

ОРГАНИЗАЦИИ в полном объеме сочетает в себе ряд интегрированных в единое целое технологий, а именно [213, 215]:

- управление знаниями в области ИБ и содействие применению комплексного подхода к выявлению, сбору, оценке, поиску и обмену этими знаниями;
- обработка больших относящихся к ИБ данных в определенном контексте – с точки зрения любой возможной атаки для нахождения ее источника, установления ее типа, оценки последствий, визуализации направленности, выявления всех затронутых систем, приоритезации мер обеспечения ИБ и выработки предложений по нейтрализации последствий атаки;
- идентификация, отслеживание и восстановление всех элементов ИТКС после воздействия на них различных инцидентов ИБ;
- сбор данных из гетерогенных источников и управление ЖРС и учетными записями с учетом соблюдения соответствия определенным требованиям;
- централизация и агрегирование данных из разрозненных хранилищ с последующей нормализацией, корреляцией, категоризацией и анализом с применением *SIEM*-систем 2.0 (второго поколения);
- визуализация уровня ИБ ИТКС и усовершенствованное (без использования статически заданных правил) обнаружение вторжений для выявления аномалий в поведении сети;
- управление рисками ИБ, сокращающее число инцидентов ИБ и обеспечивающее выполнение требований по обеспечению ИБ;
- весь цикл обработки инцидентов ИБ, заключающийся в обнаружении, оповещении, предоставлении отчетности, реагировании (включая антикризисные действия) и управлении эскалацией проблем на высшие уровни для принятия решений;
- сканирование уязвимостей с последующей реконфигурацией устройств и управлением изменениями и обновлениями;
- анализ сетевого трафика и приложений, поддерживаемый МЭ следующего поколения (*NGFW*) и инструментами для расследования инцидентов ИБ.

Со своим ЦИБ ОРГАНИЗАЦИЯ может реализовать персонифицированное (индивидуальное) в контексте ее деятельности управление инцидентами ИБ для ИТКС. Образно говоря, если ЦМБ – это «глаза мониторинга инцидентов ИБ», то ЦИБ – это «мозг управления инцидентами ИБ с широко открытыми глазами» [213], поскольку при осуществлении управления инцидентами ИБ собранные данные о реальном уровне ИБ всей ИТКС и ее отдельных элементов и принятые обоснованные решения по корректировке этого уровня должны использоваться для реагирования на инциденты ИБ.

4.5.2. Расширение бизнес-логики функционирования центров мониторинга безопасности для ее применения в Центрах интеллектуальной безопасности

Поскольку впервые упомянутый в 2010 г. ЦИБ является следующим шагом эволюции центров после ЦМБ, обоснованно построить бизнес-логику функционирования ЦИБ на основе описанной в [202] Р.Биду (R.Bidou) бизнес-логики для ЦМБ. Предлагаемое автором данного исследования расширение было первоначально выработано совместно с аспирантом Д.О.Ковалевым в 2009-2010 г. [212], а потом единолично дополнено в 2017 г. специально для применения в ЦИУСБ ОРГАНИЗАЦИИ [180].

Согласно [202], бизнес-логика функционирования ЦМБ должна быть представлена пятью операционными уровнями и соответствующими им блоками (англ. *boxes*), описывающими функциональную группу модулей, выполняющих определенные действия (рис. 42). Эти операционные уровни таковы:

1) генерация коллекторами на основе событий (англ. *event-based*) (например, приходящих от ЖРС программных и аппаратно-программных СЗИ, ОС, СУ – сетевых устройств, П – приложений и из ПД – потока данных, услуг, точек на периметре и границах подсетей, внутренних ресурсов ИТКС и т.д.) и состояний (англ. *status-based*) сообщений о реакции на некоторое внешнее воздействие или запрос (например, в результате отсылки *PING*-пакетов, проверки целостности объекта, проверки доступности услуги и т.п.) (изображены как E Boxes);

2) получение сообщений от E Boxes и приведение их к стандартному формату для составления гомогенной БД сообщений (C Boxes) (о форматах и спецификациях для описания событий ИБ говорилось в разделе 2.5);

3) хранение форматированных и агрегированных связанных с событиями ИБ сообщений в БД (D Box), для которой необходимо решить классические вопросы обеспечения ИБ (поддержание доступности, целостности и при необходимости конфиденциальности), а также обеспечить необходимую производительность;

4) анализ сообщений о событиях ИБ (A Box), включающий в себя различные операции по обнаружению компьютерных атак на основе корреляции и построения их моделей с целью своевременно сгенерировать предупреждения об опасности;

5) управление базой знаний о событиях и инцидентах ИБ (K Box), включая характеристики/сигнатуры атак и уязвимостей, эталонную модель защищенной ИТКС и Политики ИБ для нее, историю событий и инцидентов ИБ и т.д. База знаний в рамках данного исследования – это все применимые к ОРГАНИЗАЦИИ знания об ИБ ее ИТКС, которые используются для управления поиском или оценки полученных закономерностей: событий и инцидентов ИБ, уязвимостей, реальных сетевых атак, рисков ИБ, тенденций в области ИБ и т.д. Такие знания должны

быть основаны на фактических данных и, в частности, включать в себя метаданные, ограничения или пороговые значения и иерархии базовых концепций, используемых для упорядочения атрибутов или значений атрибутов для различные уровни абстракции;

б) выработка ответного реагирования на инциденты ИБ и ведение отчетности по обеспечению ИБ (R Box), что особо важно, поскольку компьютерная атака может быть правильно проанализирована и квалифицирована, но избежать ее все равно не удастся, если в нужный момент времени не будет предпринято соответствующего ответного действия.

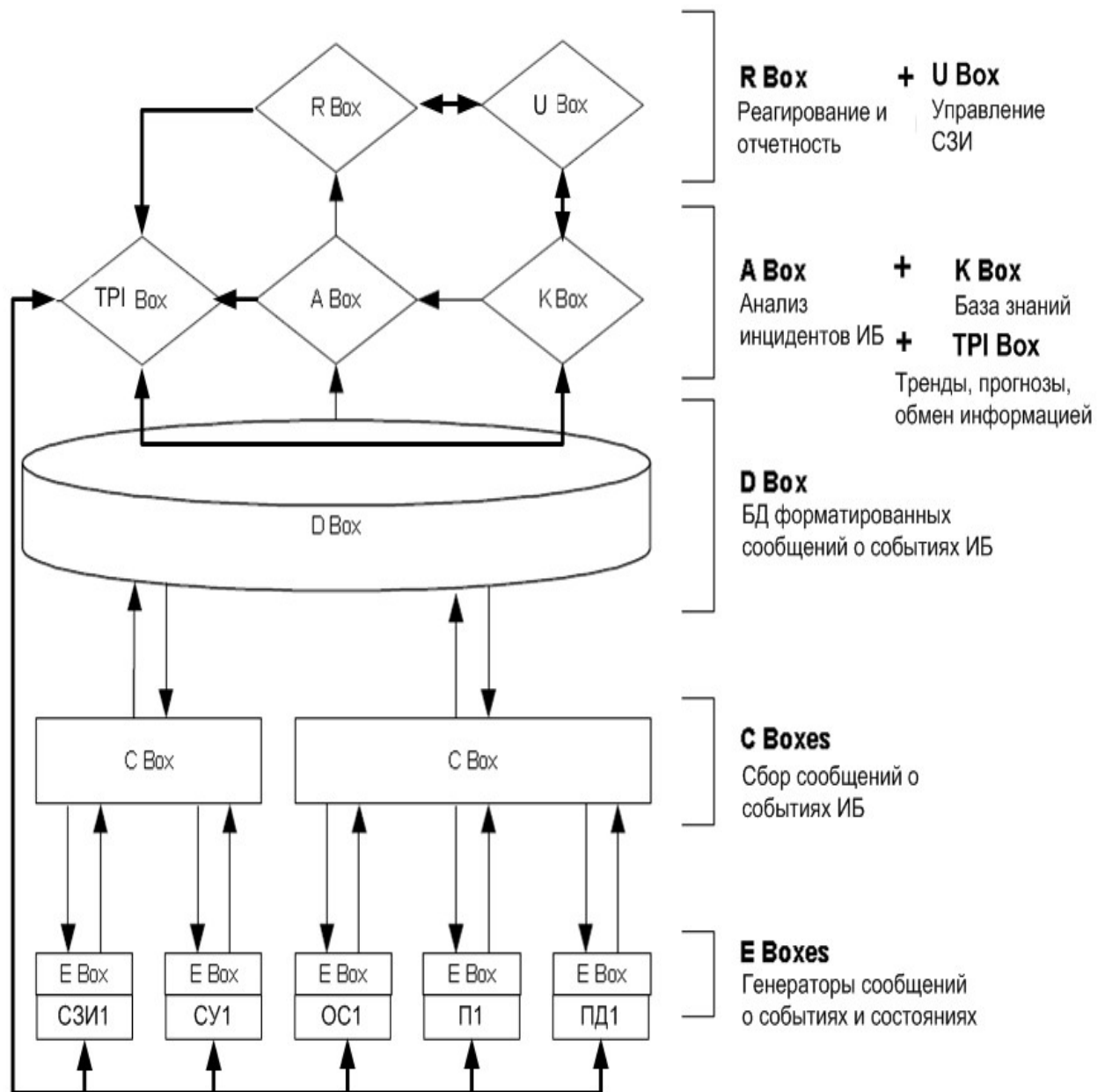


Рисунок 42 – Схема, иллюстрирующая бизнес-логику функционирования ЦИБ

Исходя из приведенного в разделе 4.5.1 анализа функций ЦИБ, предлагается расширить первоначальную схему Р.Биду двумя дополнительными типами блоков: U [40] и TPI [180].

Задача U Box заключается в обеспечении обратной связи управления, а именно в управ-

лении СЗИ, включая периодический сбор конфигурационных файлов от СЗИ (с использованием одного из стандартных протоколов типа *Telnet/SSH/HTTP/HTTPS*) и их хранения в К Вох, отслеживание изменений конфигурационных настроек СЗИ (на основе сравнения двух последних версий конфигурационных файлов и поиска несоответствий и генерации самим СЗИ сообщения, добавляющего новое правило в эти файлы), управление версиями конфигурационных файлов СЗИ (с хранением ссылок на различные версии файла в К Вох), хранение учетных записей доступа к СЗИ и получение набора команд из К Вох или изменение настроек СЗИ непосредственно через интерфейс U Вох. Таким образом, U Вох логично рассматривать как услугу с соответствующим интерфейсом для непосредственного ввода команд, поскольку этот блок может инициировать выполнение некоторых команд для автоматизированного реагирования на инциденты ИБ или внесение изменений в настройки мониторинга ИБ при изменении конфигурационных настроек СЗИ.

Целью TPI Вох является выявление и управление тенденциями в области ИБ (относительно компьютерных атак, уязвимостей, угроз ИБ и инцидентов ИБ), прогнозами для конкретной среды функционирования ИТКС со специфическими для нее историческими данными, собранными самой ОРГАНИЗАЦИЕЙ, и тенденциями в области обеспечения ИБ, а также обмен информацией о безопасности с партнерскими организациями или надежными унифицированными БД в международном, национальном или ведомственном масштабе (например, в рамках аналитики или обмена знаниями об угрозах ИБ (*Threat Intelligence*), упомянутой в разделе 2.3).

В бизнес-логике функционирования ЦИБ TPI Вох должен быть связан с двумя типами блоков, что, как и в случае с U Вох, обеспечивает обратную связь в процессе управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ:

1) непосредственно с R Вох для активизации реагирования (в ЦИБ эти действия могут быть как реактивными, как в ЦМБ, так и упреждающими) и через них косвенно с U Voxes для быстрой перенастройки СЗИ;

2) непосредственно с К Вох для извлечения (майнинга) данных и выработки новых знаний, а через них косвенно с А Вох для более всестороннего анализа данных.

Таким образом, получена расширенная по сравнению с оригинальной [202] бизнес-логика функционирования ЦИБ, добавляющая функциональные группы модулей, отвечающие за обратную связь при осуществлении процессов управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ.

Кроме предложенных усовершенствований, можно также ввести многоуровневую иерархию D Вох, что сократит время обработки отсортированных определенным образом запросов к БД из-за меньшего объема данных в нижней части рис. 42. В дополнение к конфигурационным файлам СЗИ можно также расширить список источников сообщений.

4.5.3. SIEM-системы 2.0 в Центрах интеллектуальной безопасности

Описанная в разделе 4.3.2 ограниченность SIEM-систем 1.0 была в основном преодолена во втором поколении таких систем. SIEM-системы 2.0, появившиеся в конце 2000-х годов, выполняют поведенческий и контекстный анализ исходных данных и реализуют следующие основные функции [188]:

- обнаружение в режиме реального времени и централизованный сбор информации о событиях ИБ от всех установленных в ИТКС распределенных гетерогенных источников – СЗИ, сетевых устройств, приложений, БД, конфигурационных файлов и т.д.;
- непрерывный мониторинг активности пользователей и приложений в определенном контексте;
- обработка всей собранной информации (включая ее нормализацию, фильтрацию, корреляцию, агрегирование и т.д.) в конкретном контексте, с учетом предыдущей и текущей активности пользователя, приложения и т.п. и накопленных во внешних источниках знаний;
- отслеживание всего жизненного цикла каждого события ИБ и инцидента ИБ – анализ и автоматизированное выполнение определенных действий в ответ на события ИБ, классифицируемые ОРГАНИЗАЦИЕЙ как инциденты ИБ;
- автоматизированная генерация отчетов и рекомендаций по обработке событий ИБ и инцидентов ИБ (включая отслеживание статуса их разрешения) и сводных отчетов об уровне ИБ ИТКС ОРГАНИЗАЦИИ;
- активное использование ИТ больших данных с анализом «в-памяти» и «в-БД», массовой параллельной обработкой и т.п. (вместо реляционных БД) для применения масштабируемой ИБ-аналитики.

SIEM-системы 2.0 строятся и как хранилища данных, рассчитанные на их получение и имеющие удобный единый пользовательский интерфейс для автоматизации всех рабочих процессов. Они становятся все более масштабируемыми и совершенными благодаря поддержке кросс-корреляции, а также ускоренным и упорядоченным процессам исследования и анализа больших данных для обнаружения, глубокого анализа и расследования событий ИБ на основе всех получаемых из гетерогенных источников ИТКС данных. Разнообразные настройки в SIEM-системах 2.0, адаптируемые к изменяющейся среде конкретной ИТКС ОРГАНИЗАЦИИ, являются основой для построения ЦИБ и предоставляют ему следующие возможности [188, 213]:

- полностью интегрированное и централизованное управления ЖРС и событиями с горизонтальным масштабированием архитектуры для всей ИТКС для полной ситуационной осведомленности и надежной поддержки единой базы знаний, включающей, кроме прочего, соответствующие внутренние исторические данные и данные из внешних источников;

— масштабируемость, многомерность относящихся к ИБ больших данных с расширенной корреляцией и распознаванием образов, автоматизированным ведением «белых» поведенческих списков и создаваемых на основе анализа шаблонов, настройкой и управлением конфигурациями и обновлениями, «глубокой» (всесторонней) инспекцией пакетов (*DPI*) с анализом полезной нагрузки (англ. *payload*) для выявления несоответствия протоколам, компьютерных вирусов, спама, шпионских программ, сетевых атак, утечки информации и т.п.) и всесторонней инспекцией потоков данных и т.д.;

— расширенная прозрачность (видимость) четко определенных процессов и результатов управления ИБ в рамках всей ИТКС в определенном контексте с мониторингом активности и доступности всех устройств и целостности файлов;

— аналитика, применяемая к логическим группам, включая требующие защиты услуги и активы ИТКС, с целью установления приоритетов разрешения проблем, непрерывного отслеживания текущего состояния этих активов и анализа его влияния на осуществление бизнес-операций ОРГАНИЗАЦИИ, поддерживаемых на основе ИТКС;

— основанное на знаниях, заранее спрогнозированное, действенное, управляющее всеми процессами реагирование на события ИБ с упреждающим оповещением, документированием и предоставлением отчетности в режиме реального времени;

— безагентная во многих решениях прямая связь «контролируемый объект-СЗИ» для улучшения дистанционного выявления и анализа событий ИБ и последующего восстановления затронутых ими элементов ИТКС;

— автоматизированное поддержание соблюдения соответствия определенным требованиям по обеспечению ИБ в ИТКС и проведения аудита ИБ с целью проверки процессов и мер обеспечения ИБ и выявления нарушений соблюдения Политик ИБ и инцидентов ИБ;

— простое в использовании упрощенное администрирование *SIEM*-системы 2.0, богатые возможности визуализации на основе интерактивной топологии ИТКС второго и третьего уровней модели взаимодействия открытых систем *OSI/ISO* и картографирования услуг (англ. *service mapping*), а также различные интегрированные наглядные информационные панели (*dashboard*) со встроенными правилами, виджетами (элементами интерфейса) и отчетами;

— малое количество ложных положительных и отрицательных срабатываний;

— оперативное и результативное расследование инцидентов ИБ с полностью признаваемыми при судебном разбирательстве свидетельствами в цифровой форме.

Обобщая, можно заключить, что внедрив *SIEM*-систему 2.0 в ЦИБ ИТКС, ОРГАНИЗАЦИЯ получает следующие ключевые преимущества [213]:

— согласованное с потребностями бизнеса управление ранжированными рисками ИБ для ИТКС на основе заранее определенных метрик безопасности и обеспечения ИБ в непре-

рывном режиме, сочетающее в себе локальные наблюдения мониторинга ИБ, постоянно записываемую историю событий, внешние источники ИБ-аналитики и внутреннюю информацию об угрозах ИБ, визуализацию «в едином окне» и анализ взаимосвязей объектов для выявления на ранних стадиях скрытых и подозрительных связей между пользователями, учетными записями, процессами, приложениями, вводимыми данными или многим другим в одном месте, не требуя при этом загрузки ИБ-персонала полный рабочий день;

— комплексный упреждающий подход с прогнозированием развития ситуации, основанный на знаниях, полученных в результате перекрестной корреляции и расширенной контекстной ИБ-аналитики (а не анализ события за событием), что означает, что ОРГАНИЗАЦИЯ рассматривает каждый аспект управления инцидентами ИБ в тесной взаимосвязи с другими аспектами управления ИБ и шире, чем просто снижение рисков ИБ путем устранения уязвимостей, а также учитывая возможности и мотивацию нарушителей ИБ ИТКС;

— более целенаправленный и углубленный подход, позволяющий выделить требуемые ресурсы на обработку конкретных инцидентов ИБ в зависимости от установленных стратегических приоритетов в эшелонированной защите ИТКС.

В заключении добавим, что в отличие от ЦМБ, которые в основном строятся вокруг *SIEM*-систем 1.0, в ЦИБ, кроме *SIEM*-систем 2.0, в последнее время стали добавляться следующие системы с «говорящими» названиями, анализу которых может быть посвящено отдельное научное исследование:

— платформа реагирования на инциденты безопасности (англ. *(Security) Incident Response Platform, (S)IRP*) – ПО, предоставляющее возможности автоматизированного выполнения процедур и сценариев (так называемых *playbooks*) мониторинга, регистрации, расследования и реагирования на инциденты ИБ в режиме реального времени, включая контроль устранения использованных в инциденте уязвимостей и контроль восстановления затронутых инцидентом объектов, чего нет в *SIEM*-системах. В настоящее время функционал *(S)IRP* часто интегрируется в *SOAR*-системы. До этого он присутствовал в системах обнаружения и реагирования на уровне угроз ИБ для конечных точек (англ. *Endpoint Threat Detection and Response/Endpoint Detection and Response, ETDR/EDR*) [88];

— *SOAR*-системы для управления и автоматизации обеспечения безопасности, а также реагирования на инциденты [54, 90], которые либо включают в себя *SIEM*-систему для первичного сбора и обработки данных об инцидентах ИБ, либо интегрируются с внешней *SIEM*-системой для получения от нее обработанных данных и предупреждений об уже выявленных инцидентах ИБ. Она получают исходные данные и из источников *Threat Intelligence* для обнаружения индикаторов возможной компрометации (*IoC*);

— *SGRC*-системы (англ. *Security Governance, Risk management and Compliance*) [222] –

ПО для автоматизации построения комплексной СУИБ ОРГАНИЗАЦИИ с консолидированными из множества источников данными в цифровой форме, позволяющее оперативно принимать управленческие решения в области безопасности, рисков и соблюдения соответствия определенным требованиям. Эти системы выделяются в отдельный класс только в России — компания Gartner внутри большего класса GRC-систем выделил сначала два, а потом шесть подклассов, среди которых нет *Security GRC*.

4.6. Модели зрелости Центров управления безопасностью

Введем понятие *модели зрелости ЦУБ* как модели оценки процессов управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ в ее ЦУБ. В России модели зрелости стали применять сравнительно недавно, в то время как в зарубежных странах они получили широкое распространение.

Очевидно, что перед ОРГАНИЗАЦИЕЙ, осуществляющей какую-либо деятельность, рано или поздно встает вопрос о том, как выполнять требования к осуществлению данной деятельности, в каком объеме и т.п. [171]. В международном стандарте ISO/IEC 33004:2015 и его российском аналоге ГОСТ Р ИСО/МЭК 33004-2017 [223] определена модель оценки на основе идентифицированных атрибутов оцениваемых процессов, представляющих измеримые характеристики его возможностей и методов их оценивания. Данная модель выделяет характеристики качества процесса следующим образом:

1) в первом измерении описывается множество процессов, определенных в соответствующих эталонных моделях процесса, включающих область его применения, цель и результаты. Это измерение определяет размерность процесса (при наглядном изображении это может отображаться на оси X);

2) во втором измерении отражаются свойства процесса и уровни качества процесса, определенные в выбранной системе измерения процесса с установленной шкалой оценки. Это измерение определяет размерность качества процесса (ось Y).

Модель зрелости формируется за счет обобщения одной или более моделей оценки процесса. Последние определяют множества процессов для каждого из уровней по шкале организационной зрелости процессов. Они связаны с растущими возможностями ОРГАНИЗАЦИИ по достижению более высоких уровней для некоторой задаваемой характеристики качества определенного процесса. Для каждого уровня зрелости должно быть выбрано и назначено множество процессов из моделей оценки процесса, которые представляют операции (функции), отмеченные как существенные для достижения указанного уровня зрелости. Для определения уровня зрелости процесса должны быть определены характеризующие его атрибуты, которые мож-

но измерить, например, такие: функционирование, управляемость, формализация, развертывание, контроль, инновации, оптимизация и т.п. Степень достижения определенных (желаемых) значений для атрибута оцениваемого процесса может быть определена, например, в категориях «не достигнуто — частично достигнуто — в значительной степени достигнуто — полностью достигнуто».

Для оценки уровня зрелости конкретного процесса в ОРГАНИЗАЦИИ обычно применяется способ «от начального к максимальному», заключающийся в поглощении требований предыдущего уровня последующим. Например, процесс соответствует второму уровню зрелости только в случае, если выполняют все требования для первого.

Для оценивания управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ на основе ЦУБ необходимо воспользоваться информацией из различных источников, в которых формулируются требования к составу процессов управления ИБ (например, из ГОСТ ИСО/МЭК 27001 или других аналогичных стандартов, основывающихся на «процессном подходе» к СУИБ), а также эталонных модель зрелости процессов управления ИБ, в качестве которых могут быть взяты следующие: *Systems Security Engineering – Capability Maturity Model (SSE-CMM)* [224] для разработки ПО, систем, оборудования или их эксплуатации, модель *Business Process Management Maturity Model (BPM MM)* Gartner Group [225], *Information Security Management Maturity Model (модель ISM3 или стандарт O-ISM3)* компании Open Group [226], проанализированных автором данного исследования в работе [227]. Далее в терминах выбранной эталонной модели должен быть описан каждый из процессов управления сетевой безопасностью ИТКС, выполняемый в рамках функционирования СУИБ, а, следовательно, и СОИБ ИТКС, и произведена оценка их зрелости.

В данном исследовании задача разработать собственную модель зрелости ЦУБ не ставилась, поскольку в настоящее время процесс их развития еще не окончен, и любые модели будут не полны и не точны, что потребует их пересмотра в ближайшей перспективе. Поэтому далее воспользуемся существующими моделями зрелости ЦУБ таких уважаемых компаний как *MITRE* [190] и *Hewlett Packard* [228] и результатами анализа их зрелости, проведенными в разное время *Hewlett Packard* (2017 г., проанализировано 140 ЦУБ) [229] и *Accenture* (2020 г., точное количество ЦУБ не указано) [230]. Обобщим их выводы следующим образом.

1. Полная автоматизация при обнаружении любых нарушений ИБ и инцидентов ИБ в ИТКС – в настоящее время завышенная, пока не достижимая цель. Нехватка высококвалифицированных профессионалов-практиков в области ИБ остается насущной проблемой при обеспечении ИБ. Поэтому автоматизация критически важных процессов, разгружающая их при выполнении хорошо известных рутинных операций, для любого ЦУБ просто необходима. Тем не менее, новейшие угрозы ИБ по-прежнему требуют расследования экспертами, а проведение

оценки рисков ИБ часто является неполной без человеческих рассуждений. Именно поэтому ОРГАНИЗАЦИЯ должна самостоятельно найти приемлемый для нее баланс между автоматизацией и осуществление персоналом ЦУБ некоторых операций в ручном режиме.

2. Зрелость ЦУБ существенно возрастает при добавлении к существующим возможностям мониторинга ИБ в режиме реального/близкого к реальному времени ранее упоминавшегося подхода *Threat Hunting* для поиска неизвестных угроз ИБ.

3. Непосредственной связи между размером ОРГАНИЗАЦИИ и зрелостью ее ЦУБ однозначно не прослеживается. Возможности и достигаемые при построении ЦУБ цели часто важнее, чем размер использующей его ОРГАНИЗАЦИИ. Но организации, в которых он создан и является достаточно зрелым, более конкурентоспособны на рынке и выполняют все требования соответствия, принятые в их отрасли деятельности.

4. При невозможности справиться со стоящими перед ЦУБ задачами или повышением его зрелости своими силами лучшим решением для ОРГАНИЗАЦИИ является гибридный подход к его поддержанию с использованием услуг обеспечения безопасности сторонних организаций для совместной работы, привлечением внешних ресурсов и реализацией соответствующей модели штатного расписания для него.

4.7. Формулирование требований к разрабатываемому Центру интеллектуального-управления сетевой безопасностью

Учитывая все ранее выявленные возможности и ограничения ЦМБ и ЦИБ и модели зрелости из работ [190, 228-230], их характеристики были обобщены в табл. 16, которая была дополнена ожидаемыми от более совершенного ЦИУСБ значениями, позволяющими преодолеть эти ограничения. Основными параметрами для сравнительного анализа были выбраны следующие: модель функционирования, возможности и методики обнаружения инцидентов ИБ, возможности, цикл и время реагирования на инциденты ИБ, инфраструктура центра, базовый и дополнительные наборы используемых в центре инструментальных средств, временной охват, компетенции персонала центра и возможности визуализации информации для принятия обоснованных решений.

На основе полученных результатов были сформулированы основные общие и специальные требования к деятельности и обеспечению ИБ ЦИУСБ ОРГАНИЗАЦИИ, которые следует учитывать далее при его построении.

Таблица 16 – Сравнительный анализ характеристик трех видов ЦУБ – ЦМБ, ЦИБ и разрабатываемого ЦИУСБ

Параметр	ЦМБ	ЦИБ	ЦИУСБ
Модель функционирования	На основе триггеров	На основе корреляции	На основе сценариев инцидентов ИБ и моделирования процесса «охоты за угрозами»
Возможности обнаружения	Типовые атаки	Целенаправленные атаки	Усложненные угрозы ИБ и атаки «нулевого дня»
Методики обнаружения	На основе предупреждений об опасности, ЖРС и репутационных списков	На основе корреляции, SIEM-систем и потоки <i>Threat Intelligence</i>	На основе разработки сценариев, исторических данных, машинного обучения и «охоты за угрозами», а также агрегированных внутренних и внешних потоков
Возможности реагирования	Реализация задач, реактивное реагирование, в основном ручное	Реализация задач в зависимости от приоритетов часто в автоматизированном режиме	Упреждающее, в основном автоматизированное реагирование за счет автоматизации выполнения критически важных задач на основе специальных программных модулей (скриптов)
Цикл реагирования на инциденты ИБ	От обнаружения до закрытия	От обнаружения и расширенного анализа до закрытия	На протяжении всего заранее смоделированного периода развития инцидента ИБ с постоянной коррекцией и настройкой поиска связанных с инцидентом данных в зависимости от получаемых результатов его расследования
Время реагирования	Реальное время до закрытия инцидента ИБ	Время до закрытия согласно установленным требованиям	Установленное в документах и в реальности зависящее от последствий инцидента время, включая время, требуемое на коррекцию поиска связанных с инцидентом данных
Инфраструктура	Типичная для мониторинга ИБ инфраструктура	Типичная для анализа инфраструктура	Специализированные лаборатории для разработки сценариев инцидентов и выполнения тестирования защищенности
Базовый набор средств	SIEM-система 1.0	SIEM-система 2.0	Средства расширенного поиска, агрегирования данных от всех источников и управления ими
Дополнительный набор средств	Средства для взаимодействия с устройствами	Специализированные средства мониторинга ИБ	Специализированные средства для обнаружения угроз ИБ, поиска данных и реализации сценариев «охоты»
Временной охват	В пределах работы смены	В пределах всего времени реагирования на инцидент	Постоянно в режиме реального/близкого к реальному времени обнаружения и реагирования
Компетенции персонала	Навыки мониторинга ИБ	Навыки анализа	Навыки моделирования и глубокого анализа корреляций всех собираемых данных и коррекций поиска новых данных
Возможности визуализация	Опрос, сканирование	В режиме «мягкого» реального времени	В режиме «жесткого» реального времени

4.7.1. Общие требования к Центру интеллектуального управления сетевой безопасностью

Сначала сформулируем общие требования к ЦИУСБ в следующем виде [213, 215]:

ТО1. Вся деятельность ЦИУСБ ОРГАНИЗАЦИИ должна быть выстроена и реализована согласно требованиям, изложенным в применимых нормативных, правовых, отраслевых и других документах.

ТО2. ЦИУСБ должен представлять собой комплекс систем (подсистем), технических и программных средств, технологически и организационно объединенных каналами передачи информации различной физической природы, позволяющих обеспечить автоматизацию ПУИИБ ОРГАНИЗАЦИИ, включая реагирование на инциденты ИБ, за счет централизованной обработки связанной с ИБ ИТКС информации, а также предоставляющий услуги и средства связи для персонала, вовлеченного в ПУИИБ.

ТО3. Единство и скоординированность функционирования ЦИУСБ с ИТКС ОРГАНИЗАЦИИ.

ТО4. ЦИУСБ должен быть системообразующим элементом СОИБ ОРГАНИЗАЦИИ на основе жесткой связи с ней, влиять на ее развитие и совершенствование.

ТО5. Наличие необходимой организационной структуры и органа управления ЦИУСБ, основным задачами которого является администрирование управления, управление ходом функциональных процессов, оперативный контроль состояния, оперативный контроль за устранением сбоев в функционировании и информационно-аналитическое обеспечение управления совершенствованием и развитием ЦИУСБ.

ТО6. Интеграция информационных и телекоммуникационных сетей, ресурсов и услуг ЦИУСБ в единую систему.

ТО7. Применение современных средств технического, программного, информационного, аналитического, организационного и документального обеспечения, функционально объединенных в ЦИУСБ (оговоримся, что лингвистическое, математическое и метрологическое обеспечение выходят за рамки данного исследования).

4.7.2. Специальные требования к Центру интеллектуального управления сетевой- безопасностью

Специальные требования к деятельности ЦИУСБ ОРГАНИЗАЦИИ таковы [231].

ТС1. Создание и непрерывное развитие ЦИУСБ как единой экосистемы (сложной динамической системы взаимосвязанных элементов в ЕИП ОРГАНИЗАЦИИ, а не просто единой платформы) для обмена информацией об ИБ ИТКС и совместных скоординированных действий

по обнаружению, расследованию и предотвращению инцидентов ИБ, а также упреждающего управления сетевой безопасностью ИТКС и обучения на полученном опыте как различных подразделений ОРГАНИЗАЦИИ, так и ее бизнес-партнеров, регуляторов, аудиторов и т.п.

ТС2. Управляемость ЦИУСБ с централизованной архитектурой и распределенной/ децентрализованной работой отдельных процессов при совмещении масштабируемости и эластичности сбора, хранения, первичной обработки и корреляции данных для его функционирования в изменяющейся среде осуществления деятельности ОРГАНИЗАЦИИ и при появлении новых угроз ИБ в ЕИП для ее ИТКС.

ТС3. Согласованность процессов, поддерживающих функционирование ЦИУСБ, со всеми передовыми практиками и применимыми к ИТКС ОРГАНИЗАЦИИ требованиями по обеспечению ИБ, определенными в международных и российских законах и подзаконных нормативных правовых актах, а также региональными и ведомственными документами.

ТС4. Расширенная ИБ-аналитика и использование для нее как можно большего количества типов данных, поскольку по-прежнему недостаточно навыков и методов обработки неструктурированных данных в состоянии покоя, например, данных из ОЗУ конечных устройств, данных от мобильных устройств, виртуальных и облачных сред.

ТС5. Адаптивное управление событиями ИБ в ИТКС, поддерживаемое за счет применения предсказательного определения возможных тенденций в области обеспечения ИБ в ЕИП ОРГАНИЗАЦИИ и типовых модульных и конфигурируемых СЗИ, сетевых устройств, протоколов, процессов и мер обеспечения сетевой безопасности, что должно обеспечить повторяемость (тиражируемость) всех процессов управления сетевой безопасностью при их использовании в различных ЦИУСБ.

ТС6. Функциональная устойчивость ЦИУСБ в штатном режиме, в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций (способность регулировать функционирование с целью поддержания выполнения операций при ожидаемых условиях и при ужесточении требований, нарушениях и непредвиденных обстоятельствах, например, способность адаптироваться к изменяющимся шаблонам компьютерных атак или условиям осуществления деятельности на основе ИТКС при внедрении новых ИКТ [232]) для обеспечения долгосрочной постоянной доступности и других важных свойств ИБ для ИТКС и всех ее элементов, АО, ПО, предоставляемых ИТ-услуг, информационных потоков, знаний и БД и т.д., что исключит единую точку отказа.

ТС7. Масштабируемость ЦИУСБ (мера способности ИТКС к увеличению/уменьшению производительности и затрат в ответ на изменения в потребностях ее АО, приложений, систем обработки данных и т.п. [232]) с точки зрения масштабируемости сбора и обработки огромного количества событий из различных гетерогенных внутренних и внешних (типа *Threat*

Intelligence) по отношению к ИТКС источников, что все вместе определяет необходимость применения ИТ больших данных и использования продвинутых технологий для их хранения (типа так называемых «озер» данных, рассмотренных в разделе 5.4.2).

ТС8. Эластичность (способность системы с течением времени увеличивать нагрузку на свои текущие и дополнительные динамически и автоматически добавляемые по требованию вычислительные ресурсы [234]) для распределенных и реализуемых в режиме реального/ близкого к реальному времени агрегирования, пакетной и потоковой обработки и передачи гибридных относящихся к ИБ больших данных.

ТС9. Гибкость при использовании необходимых методов и инструментов ИБ-аналитики таким образом, чтобы персонал ЦИУСБ мог использовать при обработке все доступные в тот момент данные (включая исторические за длительный период времени) и получать результаты, учитывающие разные точки зрения.

ТС10. Собственная защищенность и надежность ЦИУСБ, включая защищенность его инфраструктуры и процессов обработки данных, а также безопасность всех обрабатываемых в нем связанных с ИБ больших данных и хранимых входные и выходные данных процессов, а также надежность управления, поступающими в ЦИУСБ из надежных источников.

ТС11. Прозрачность для руководства ОРГАНИЗАЦИИ всей деятельности ЦИУСБ для принятия своевременных управленческих решений.

4.7.3. Перечень детальных требований к Центру интеллектуального управления сетевой безопасностью

На основе перечисленных выше требований необходимо сформулировать более детальные технические требования к ЦИУСБ ОРГАНИЗАЦИИ с точки зрения среды управления сетевой безопасностью и услуг передачи данных, а также предоставляемых ИТ-услуг и информационных активов, подлежащих защите в ИТКС, в том числе:

- требования к архитектуре ЦИУСБ;
- требования к обеспечению ИБ ЦИУСБ;
- требования к процессам управления сетевой безопасностью ИТКС, поддерживаемым в ЦИУСБ, включая оценку рисков ИБ ИТКС;
- требования к процессу оценки рисков ИБ для ЦИУСБ;
- требования к оснащенности ЦИУСБ персоналом;
- требования к мониторингу ИБ ИТКС, включая контроль защищенности всех элементов ИТКС и предоставляемых услуг передачи, обработки и хранения данных, анализ сетевого трафика, вредоносного ПО и многое другое;

- требования к системе идентификации объектов и субъектов в ЦИУСБ;
- требования к источникам данных для ИБ-аналитики, осуществляемой в ЦИУСБ;
- требования к системам логирования событий (ЖРС), возникающих в ИТКС, для их последующей обработки в ЦИУСБ;
- требования к системам хранения в ЦИУСБ связанных с ИБ ИТКС данных, включая данные о событиях ИБ, произошедших в ИТКС;
- требования к процессам и системам обработки в ЦИУСБ больших связанных с ИБ ИТКС данных;
- требования к управлению телекоммуникационными устройствами ЦИУСБ;
- требования к управлению ПО ЦИУСБ;
- требования к управлению СЗИ и их интеграции в ЦИУСБ, включая подключение новых и снятие с эксплуатации устаревших СЗИ;
- требования к разработке ЦИУСБ собственных модулей, автоматизирующих операции по управлению сетевой безопасностью ЦИУСБ;
- требования к управлению инцидентами ИБ, возникающими в ИТКС;
- требования к процессу расследования инцидентов ИБ, возникших в ИТКС;
- требования к оценке текущего состояния информационной защищенности ИТКС, проводимой в ЦИУСБ, и динамики его изменения с течением времени;
- требования к оценке ключевых показателей эффективности мер обеспечения сетевой безопасности ИТКС, проводимой в ЦИУСБ;
- требования к системе предоставления отчетности об ИБ ИТКС и визуализации информации об ИБ ИТКС в ЦИУСБ;
- требования к взаимодействию с внешними организациями при управлении сетевой безопасностью ИТКС, включая обмен информацией о рисках ИБ и инцидентах ИБ; и т.п.

4.7.4. Требования по обеспечению информационной безопасности Центра интеллектуального управления сетевой безопасностью

Из представленного в разделе 4.7.3 списка требований выберем для более детальной разработки относящиеся к обеспечению ИБ ЦИУСБ как ключевые в рамках данного исследования. Но перед этим важно отметить, что при обеспечении ИБ в ЦИУСБ должно быть учтены следующие обстоятельства:

- 1) наибольшими возможностями для нанесения ущерба и нарушения функционирования ЦИУСБ обладает ее собственный персонал и пользователи;
- 2) одной из серьезных проблем, требующей своего решения, является обеспечение ИБ

критически важных приложений, используемых для автоматизации деятельности ЦИУСБ, включая ПО, посредством которого осуществляется доступ к содержанию хранимой, обрабатываемой и передаваемой в ЦИУСБ информации, относящейся к инцидентам ИБ и их расследованию, а также характеризующей уровень ИБ ИТКС ОРГАНИЗАЦИИ;

3) эффективность и результативность мероприятий по обеспечению ИБ ЦИУСБ существенно зависит от наличия и степени реализации процессов, обеспечивающих не только саму защиту, но и контроль (мониторинг ИБ и аудит ИБ) выполнения на каждом объекте защиты ЦИУСБ требований по обеспечению ИБ, которые должны быть документально зафиксированы в Политике ИБ ЦИУСБ, а также от качества оценки текущего уровня ИБ ЦИУСБ.

Опираясь на [172], сформулируем эти требования следующим образом.

ТБ1. Целенаправленная и эшелонированная (многоуровневая) защита (англ. *defense in depth*) всех ресурсов и подсистем ЦИУСБ и ИТКС, основанная на системном методологическом подходе и реализации на каждом уровне соответствующих процессов и мер обеспечения ИБ и обеспечения независимости уровней друг от друга с точки зрения поддержания ИБ [119]. Нельзя полагаться на один защитный рубеж, каким бы надежным он ни казался: в ЦИУСБ за средствами физической защиты должны следовать аппаратно-программные средства, за идентификацией и аутентификацией – управление доступом, и как последний рубеж – постоянный мониторинг и протоколирование всех событий.

ТБ2. Прогнозируемость характера проблем и задач в области обеспечения ИБ ЦИУСБ (включая прогнозы развития угроз ИБ и возникновения нарушений ИБ и инцидентов ИБ). Подобно общему управлению ОРГАНИЗАЦИЕЙ, управление ИБ ЦИУСБ должно включать прогнозирование, предназначенное для выявления причинно-следственных связей возможных проблем, моделирования действий нарушителей ИБ и последствий от их действий, планирования необходимых защитных мер и оценку последующего положительного эффекта от их применения и т.п.

ТБ3. Своевременность обнаружения проблем, влияющих на безопасность ЦИУСБ – ОРГАНИЗАЦИЯ и сам ЦИУСБ должны своевременно обнаруживать проблемы, прямо или косвенно относящиеся к ИБ и потенциально способные повлиять на успешное достижение ЦИУСБ целей его функционирования.

ТБ4. Своевременность, адекватность угрозам ИБ и разумная достаточность защитных мер ЦИУСБ – выбор защитных мер должен осуществляться с учетом охвата всех объектов защиты ЦИУСБ, Модели угроз ИБ и Модели нарушителей ИБ для них, оценки рисков ИБ для ЦИУСБ, а также оптимального соотношения между стойкостью защиты, ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими важными факторами.

ТБ5. Результативность и эффективность защитных мер с учетом их постепенной деградации – проблема заключается в том, что до наступления инцидента ИБ убедиться в результативности защитных мер и, следовательно, успешном его отражении проблематично. Кроме этого, даже в отсутствии злоумышленной или иной, требующей вмешательства службы ИБ, деятельности защитные меры в результате воздействия изменений среды осуществления деятельности ОРГАНИЗАЦИИ со временем неминуемо ослабевают, в результате чего риски ИБ возрастают, что необходимо учитывать при их оценке и принятия решений о замене новыми мерами и средствами.

ТБ6. Непрерывность процесса безопасного функционирования подсистемы обеспечения ИБ ЦИУСБ – целенаправленный непрерывный процесс обеспечения ИБ ЦИУСБ заключается в постоянном принятии соответствующих корректирующих мер на всех этапах жизненного цикла ЦИУСБ, а также невозможности перехода защитных мер в небезопасное состояние и невозможности миновать используемые СЗИ.

ТБ7. Гибкость управления и применения защитных мер – обеспечение возможности варьировать уровень защищенности ЦИУСБ в зависимости от текущей ситуации и потребности ОРГАНИЗАЦИИ в ИБ в данный период времени.

ТБ8. Способность к интеграции и согласованность (скоординированное функционирование) применения различных защитных мер – при построении целостной системы защиты ЦИУСБ необходимо выбирать такие, которые способны к согласованной работе. Реализация новых мер в работающий ЦИУСБ не нарушит процесса его нормального функционирования. При интеграции не возникнет уязвимостей и будет обеспечен охват всех объектов защиты ЦИУСБ.

ТБ9. Наблюдаемость защитных мер – результат их применения будет явно наблюдаем (прозрачен) и может быть оценен.

ТБ10. Обязательность постоянного (мониторинг ИБ) и систематического периодического (аудит ИБ) контроля защитных мер с целью выяснения, насколько они выполняют возлагаемые на них функции защиты объектов ЦИУСБ.

ТБ11. Мониторинг активности персонала и пользователей ЦИУСБ для своевременного выявления несанкционированных действий и ошибок.

ТБ12. Простота и управляемость защитных мер ЦИУСБ.

ТБ13. Совершенствование обеспечения ИБ ЦИУСБ за счет периодической переоценки защитных мер и потребности в них.

ТБ14. Формирование режима безопасности ЦИУСБ.

ТБ15. Кадровое обеспечение ЦИУСБ высококвалифицированным персоналом с необходимыми компетенциями в области управления сетевой безопасностью и инцидентами ИБ.

ТБ16. Разделение полномочий, распределение ролей и ответственности персонала ЦИУСБ.

ТБ17. Использование отечественного и зарубежного опыта, соответствующих стандартов и нормативных и правовых актов в построении подобных центров.

Далее все перечисленные в разделе 4.7 общие и более специфические требования будут взяты за основу при построении типового ЦИУСБ.

Выводы по главе 4

1. Проанализированы основные цели и функции *SIEM*-систем в ИТКС ОРГАНИЗАЦИИ, собирающих и анализирующих данные из ЖРС перечисленных в работе гетерогенных источников в ИТКС. Проведен сравнительный анализ *SIEM*-систем и систем управления ЖРС, который показал несомненные преимущества первых при проведении расследования инцидентов ИБ в ИТКС и принятии решений о совершенствовании обеспечения ее СОИБ.

2. Представлена типичная трехуровневая архитектура *SIEM*-системы, которая демонстрирует объединенные в ней *SIM*- и *SEM*-системы. Первый уровень отвечает за сбор событий и сохранение записей о них. Эти сохраненные данные затем используются при решении задач мониторинга ИБ и корреляции данных о событиях. На верхнем уровне проанализированные данные представляются в виде отчетов о безопасности или событиях ИБ, которые далее визуализируются на консоли управления *SIEM*-системой.

3. На основе проведенного исследования сделан вывод, что несмотря на 15-летний период развития *SIEM*-систем, на международном и национальном уровне отсутствуют какие-либо документы, посвященные их проектированию, внедрению и использованию.

4. Кратко описана эволюция ЦУБ, начавшаяся в 90-е годы XX в. с ситуационных центров и групп реагирования на компьютерные инциденты. И, как в случае с *SIEM*-системами, проведенный анализ показал, что при значительном периоде существования на международном и национальном уровне отсутствуют какие-либо документы, посвященные их проектированию, внедрению и использованию.

5. Подробно проанализированы функции ЦМБ, реализация которых поддерживается *SIEM*-системами первого поколения. Для этих систем перечислены их функции в ЦМБ и выделены основные недостатки при решении современных проблем обеспечения сетевой безопасности ИТКС ОРГАНИЗАЦИЙ.

6. Проведена системная классификация известных решений для построения ЦМБ различных производителей, помогающая установить критерии выбора конкретного решения для ОРГАНИЗАЦИИ. Данная классификация не претендует на полноту, поскольку

ОРГАНИЗАЦИЯ на ее основе может составить собственный расширенный набор признаков ЦМБ при разработке и внедрении своего ЦМБ.

7. На основе анализа первоисточников, описывающих практический опыт внедрения и использования, выявлены серьезные ограничения функциональных возможностей первых ЦМБ, позволившие сформулировать требования ко второму поколению центров управления инцидентами ИБ.

8. Подробно рассмотрен подход, получивший в англоязычной литературе название *Security Intelligence (Security Analytics, Information Security Intelligence)* и названный в исследовании «ИБ-аналитика», суть которого заключается не только в сборе, нормализации и анализе в режиме реального времени данных, генерируемых пользователями, приложениями и инфраструктурой, но и в формировании на их основе знаний, необходимых для тактического, но и, что еще важнее, стратегического совершенствования СОИБ всей ОРГАНИЗАЦИИ для постоянного опережения злоумышленников. Выделены цели, особенности и основные преимущества использования ИБ-аналитики при решении задач управления инцидентами ИБ ИТКС ОРГАНИЗАЦИИ.

9. Концепция ИБ-аналитики нашла свое воплощение в ЦИБ с его интегрированной архитектурой защиты от компьютерных атак и контекстно-управляемым интеллектом при управлении знаниями для постоянного контроля ИБ ИТКС и связанных с ней элементов ЕИП ОРГАНИЗАЦИИ. Внедряя ЦИБ, ОРГАНИЗАЦИЯ получает возможность не только обнаруживать и реагировать на атаки, но и результативно бороться с новыми угрозами ИБ, прежде чем они причинят вред, а также предотвращать инциденты ИБ.

10. Как комплексное решение, для реализации ИБ-аналитики в полном объеме применительно к ИТКС ОРГАНИЗАЦИИ ЦИБ интегрирует в единое целое такие технологии, как управление знаниями в области ИБ, обработка больших относящихся к ИБ данных в определенном контексте, агрегирование данных из гетерогенных источников с последующей нормализацией, корреляцией, категоризацией и анализом с применением SIEM-систем 2.0, визуализация состояния ИБ ИТКС, усовершенствованное обнаружение вторжений для выявления аномалий в поведении сети без использования правил, управление рисками ИБ, весь цикл обработки инцидентов ИБ, сканирование уязвимостей с последующей реконфигурацией устройств и управлений изменениями и обновлениями, анализ сетевого трафика и приложений и т.п.

11. С собственным ЦИБ ОРГАНИЗАЦИЯ может реализовать персонифицированные (индивидуальное) в контексте ее деятельности управление инцидентами ИБ для ИТКС. Образно говоря, если ЦМБ – это «глаза мониторинга инцидентов ИБ», то ЦИБ – это «мозг управления инцидентами ИБ с широко открытыми глазами».

12. Разработана расширенная по сравнению с [202] бизнес-логика функционирования

ЦИБ, представленная пятью операционными уровнями и соответствующими им семью блоками, описывающими функциональную группу модулей, выполняющих определенные действия в рамках работы ЦИБ, а также указаны возможные пути ее дальнейшего усовершенствования.

13. Показано, что установленная ограниченность *SIEM*-систем 1.0 в основном преодолена в *SIEM*-системах 2.0, выполняющих поведенческий и контекстный анализ исходных данных в ЦИБ. Такие *SIEM*-системы 2.0 строятся и как хранилища данных, имеющие удобный единый пользовательский интерфейс для автоматизации всех рабочих процессов. Они становятся все более масштабируемыми и совершенными благодаря поддержке кросс-корреляции, а также ускоренным и упорядоченным процессам исследования и анализа больших данных для поддержки обнаружения, глубокого анализа и расследования событий ИБ во всех получаемых из гетерогенных источников ИТКС данных. Отмечается, что в последнее время в ЦИБ, кроме *SIEM*-систем 2.0, стали добавляться и другие средства, автоматизирующие и ускоряющие процесс реагирования на инциденты ИБ, такие как (*S*)*IRP*), *SOAR*- и *SGRC*-системы.

14. Учитывая выявленные возможности и ограничения ЦМБ и ЦИБ и проанализировав созданные к данному времени модели зрелости для ЦУБ, обобщены их характеристики.

15. На основе полученных результатов сформулированы основные общие и специальные требования к деятельности современного ЦИУСБ ОРГАНИЗАЦИИ. Далее перечислены требующие разработки более детальные технические требования к ЦИУСБ ОРГАНИЗАЦИИ с точки зрения среды управления сетевой безопасностью и услуг передачи данных, а также предоставляемых ИТ-услуг и информационных активов, подлежащих защите в ИТКС. Из представленного списка требований для более детальной разработки выбраны относящиеся к обеспечению ИБ ЦИУСБ как ключевые в рамках данного исследования.

16. Все перечисленные общие и более технические требования взяты за основу при построении типового ЦИУСБ ОРГАНИЗАЦИИ.

ГЛАВА 5. ПОСТРОЕНИЕ ТИПОВОГО ЦЕНТРА ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ ДЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ОРГАНИЗАЦИИ

В начале главы важно пояснить хронологию событий, касающихся идеи автора данного исследования разработать типовой ЦИУСБ и состояния освещения этого вопроса в отечественных и зарубежных публикациях.

Первый SOC FORUM «Практика противодействия кибератакам и построения центров мониторинга ИБ» состоялся в Москве в ноябре 2015 г., через 10 лет после первого упоминания о ЦМБ компанией *Cisco*. За несколько дней до этого автором данного исследования был написан и отправлен на 4-ю международную конференцию FiCloud-2015 доклад «Security Operations Centers for Information Security Incident Management», который был принят для представления на одной из сессий [210]. В журнале «Безопасность информационных технологий» были в соавторстве опубликованы две статьи: «Адаптивная защита автоматизированной банковской системы при помощи операционного центра информационное безопасности» [212] за пять лет до SOC FORUM (в 2010 г.) и «*Information Security Intelligence* – основа современного управления информационной безопасностью» [216] за два года до него (в 2013 г.), сообщавшие о результатах начатого автором исследования.

На четвертом SOC FORUM (ноябрь 2018 г.) представитель компании *Fortinet* Д.Купецкий в докладе «Драйверы развития ИТ-инфраструктур и инструментов обеспечения ИБ» очень кратко, без каких-либо подробностей, озвучил возможность совмещения функций, выполняемых ЦМБ и Сетевым операционным центром (СОЦ), или Центром управления сетью (англ. *Network Operations Center, NOC*). Данная идея была впервые изложена автором данного исследования в виде доклада «SOC- and SIC-Based Information Security Monitoring» [215], отправленного в конце 2016 г. и принятого к представлению на международной конференции WorldCIST'2017. После успешного представления и бурного обсуждения автору было предложено опубликовать расширенную версию доклада в журнале «*Journal of Intelligent & Fussy Systems*» (IOS Press, Netherlands), где она вышла в 2018 г. под названием «*Information Security Management in SOC's and SIC's*» [213]. Именно в этих двух работах и была опубликована идея объединения функционала не просто ЦМБ, а ЦИБ с СОЦ, хотя с коллегами она начала обсуждаться еще раньше. Одновременно с [215] появилась зарубежная публикация [234], в которой было проведено сопоставление ЦМБ (а не ЦИБ) и СОЦ, а не высказана идея их объединения. Первая очень короткая публикация об объединении была представлена в [235] в конце марта 2017 г., за несколько дней до представления доклада [215] на конференции WorldCIST'2017 в начале

апреля 2017 г. Далее количество публикаций на данную тему начало расти.

Следовательно, можно сделать вывод, что ЦИУСБ как объединение ЦИБ и СОЦ впервые было предложено автором данного исследования.

В главе сначала излагается разработанная методология построения типового ЦИУСБ ОРГАНИЗАЦИИ, после чего формулируются основные принципы его построения. Далее представляется основная идея построения и функциональные возможности типового ЦИУСБ как центра, объединяющего все преимущества ЦИБ И СОЦ в одном месте ОРГАНИЗАЦИИ для централизованного управления ИБ ИТКС и, в частности, ПУИИБ. Рассмотрены вопросы визуализации информации в типовом ЦИУСБ для принятия решений по управлению инцидентами ИБ в ИТКС. С учетом требований, изложенных в разделе 4.7, для типового ЦИУСБ разрабатываются три основные архитектуры – функциональная, обработки больших и быстрых относящихся к ИБ ИТКС данных и обеспечения собственной ИБ. Кроме этого, для обеспечения ИБ названных данных, поступающих для обработки в *SIEM*-систему ЦИУСБ, представлен проект *SIEM*-системы 3.0 с новым элементом, построенным с применением технологий блокчейна. Завершает главу рассмотрение вопросов функциональной устойчивости ЦИУСБ в штатном режиме, в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций в ЕИП ОРГАНИЗАЦИИ, кадрового обеспечения ЦИУСБ высококвалифицированными специалистами и демонстрация выполнения в разработанном проекте типового ЦИУСБ сформулированных в разделе 4.7 требований.

5.1. Методология построения типового Центра интеллектуального управления сетевой безопасностью

В начале сделаем существенное для всего процесса построения замечание, что разработка типового ЦИУСБ как специализированного структурного элемента, встроенного в ИТКС ОРГАНИЗАЦИИ, также означает необходимость отражения его системообразующей роли в обеспечении ИБ этой ОРГАНИЗАЦИИ. Другими словами, являясь частью ИТКС, типовой ЦИУСБ кроме этого служит основой системы управления сетевой безопасностью ОРГАНИЗАЦИИ как части ее СУИБ, а, значит, и СОИБ ИТКС (раздел 3.4.6, рис. 40). Опыт разработки подобных систем в российских и зарубежных организациях свидетельствует о том, что создание многокомпонентных ЦУБ возможно лишь при обязательном соблюдении общесистемной методологии построения всех составных частей типового ЦИУСБ в структуре ИТКС ОРГАНИЗАЦИИ и ЦИУСБ как единой системы в целом.

Разработанная методология построения типового ЦИУСБ ОРГАНИЗАЦИИ как упорядоченная совокупность методов и средств его создания и последующей эволюции представляет

собой теоретическую основу, необходимую для многократно повторяемой различными организациями реализации целей и задач создания типового ЦИУСБ. Она обеспечивает снижение сложности и неоднозначности процесса построения сетей связи, систем обработки данных, других систем и подсистем, предоставляемых услуг и других элементов ЦИУСБ за счет полного и точного описания этого процесса, а также применения современных подходов их построения на протяжении всех стадий жизненного цикла – от замысла до реализации (адаптировано на основе [58]).

Специфика разработанной научно обоснованной методологии построения типового ЦИУСБ заключается в ее универсальности. Ее главная идея – это ориентация на существующие, выбранные в результате системного анализа типовые проектные решения построения его телекоммуникационной сети, ИС, ИТ-услуг, используемых технологий обеспечения ИБ и СЗИ и вспомогательных систем и комплексов, которые отражают развитие современных СВТ и ИКТ. Именно унификация и стандартизация типового ЦИУСБ в целом и его типовых проблемно-ориентированных на ПУИИБ компонентов, на базе которых осуществляется его построение, имеет большое практическое значение в современных условиях. При широком использовании импортных СВТ, телекоммуникационного оборудования, аппаратно-программных СЗИ этот фактор становится объективной необходимостью построения типового ЦИУСБ. Кроме этого, такой подход предоставляет единые принципы и подходы к построению отдельных гомогенных (однородных) систем и компонентов ЦИУСБ с ориентацией на единые базовые технологии их функционирования, а также к обеспечению их совместимости и унификации используемых для них программных и технических решений и модулей.

Основная цель разработанной методологии построения типового ЦИУСБ как сложного организационно-технического комплекса заключается в такой организации процесса построения и обеспечения единства управления им, при которой гарантируется выполнение всех сформулированных требований, предъявляемых как к самому ЦИУСБ, так и к характеристикам процесса разработки каждого его составного элемента.

Основополагающим методологическим принципом построения является системный подход, согласно которому при построение типового ЦИУСБ обеспечивается последовательное получение надежных результатов обеспечения сетевой безопасности ИТКС в рамках всей СОИБ различных организаций и разрабатываются и используются такие методики создания его информационного, аналитического, технического, программного и организационного обеспечения, которые взаимоувязаны с общей концепцией построения и использования организациями своих ИТКС.

Ключевыми задачами, решение которых должна обеспечить методология построения типового ЦИУСБ, являются следующие:

— обеспечение создания типового ЦИУСБ как открытой информационной системы, характеризующейся интероперабельностью (способностью к взаимодействию при выполнении общей работы с использованием стандартных интерфейсов), переносимостью (ПО, данных и пользователей) и функционированием согласно общепризнанным стандартам [55] с учетом всех предъявляемых к нему требований по автоматизации ПУИИБ для ИТКС;

— гарантия создания типового ЦИУСБ с заданными качествами (собственная защищенность, управляемость, функциональная устойчивость, масштабируемость, эластичность, гибкость, способность к непрерывному развитию и т.п.) в заданные сроки в рамках выделенных средств;

— поддержка централизованно управляемых и контролируемых скоординированных действия при разработке каждой системы и комплекса типового ЦИУСБ в соответствии с общей концепцией его построения;

— обеспечение использования в создаваемом типовом ЦИУСБ имеющегося задела организаций в области ИКТ, ПО, БД и т.п. и создание условий для последующей адаптации типового ЦИУСБ в среду ИТКС за счет его интеграции в ЕИП организаций;

— поддержка удобства сопровождения, модернизации и наращивания типового ЦИУСБ для адаптируемости к динамически изменяющейся среде ведения деятельности организаций и функционированию в этой среде ИТКС.

Основные задачи процесса построения типового ЦИУСБ определим следующим образом, что соответствует последовательности действий, каждая из которых может быть дополнительно разбита на этапы и выполняемые на них процессы:

— формулирование целей и задач создания типового ЦИУСБ в зависимости от круга его пользователей и компонентов, обуславливающих выбор принципов построения;

— обследование типовой ИТКС, сбор, систематизация и анализ первоначальной информации, необходимой для построения типового ЦИУСБ, встроенного в ИТКС;

— выбор методов и средств разработки типового ЦИУСБ и организация работ по его построению в соответствии с принятым планом работ;

— разработка моделей деятельности, автоматизируемой на основе типового ЦИУСБ;

— разработка архитектуры типового ЦИУСБ;

— разработка требований к функциональной и территориальной интеграции всех информационных и телекоммуникационных элементов в типовом ЦИУСБ и интеграции типового ЦИУСБ в типовую ИТКС;

— разработка требований ко всем элементам информационной и телекоммуникационной (как средствам поддержки локального и удаленного информационного обмена между объектами и пользователями) составляющих типового ЦИУСБ;

- разработка информационной модели (структуры) типового ЦИУСБ (включая, например, определение множества предоставляемых пользователям типовых ИТ-услуг и информационных ресурсов с указанием приоритетов по обеспечению основных свойств ИБ для них);

- разработка требований к цифровой информации, представленной в различных форматах, для передачи от гетерогенных источников по каналам связи в виде единых информационных потоков как из типовой ИТКС в типовой ЦИУСБ и обратно (например, файлы или команды по изменению конфигурационных настроек СЗИ внутри типовой ИТКС), так и внутри типового ЦИУСБ;

- разработка соответствующих технических заданий на построение и проект технического задания на внедрение типового ЦИУСБ, включая соответствующие программы и методики испытаний;

- осуществление обоснованного выбора средств для реализации типового ЦИУСБ;

- развертывание типового ЦИУСБ на месте его эксплуатации, включая проведение работ по пилотированию технических решений типового ЦИУСБ в типовой ИТКС;

- апробация (проведение предварительных системных испытаний) и доработка по ее результатам технических решений, обеспечивающих функционирование типового ЦИУСБ в типовой ИТКС согласно определенным целям и задачам;

- разработка соответствующей пользовательской и эксплуатационной документации для различной целевой аудитории при внедрении и использовании типового ЦИУСБ;

- сопровождение типового ЦИУСБ, включая управление режимами функционирования, сопровождение технических и программных средств, регистрацию, диагностику и локализацию ошибок, внесение изменений и тестирование и т.п.

Для каждого из перечисленных этапов далее необходимо определить последовательность выполняемых в рамках него работ, исходные данные и получаемые результаты, необходимые для выполнения работ методы, средства и ресурсы, роли и ответственность участников и т.д. Такое формальное описание построения типового ЦИУСБ позволяет спланировать и организовать процесс разработки типового ЦИУСБ и обеспечить его управляемость.

Применение разработанной методологии построения типового ЦИУСБ ОРГАНИЗАЦИИ обеспечит выполнение следующих общесистемных требований к ЦИУСБ (адаптировано на основе [58]):

- типовой ЦИУСБ проектируется в соответствии с типовой организационной инфраструктурой и распределенным типовым ЕИП (с выделением головного офиса и территориально распределенных подразделений) современных организаций;

- типовой ЦИУСБ обеспечивает решение динамически изменяющегося набора управленческих и информационно-аналитических задач в рамках управления сетевой безопасностью

типовой ИТКС;

— типовой ЦИУСБ является системообразующим техническим и организационным компонентом ПУИИБ для типового ЕИП ОРГАНИЗАЦИИ в рамках ее СОИБ;

— типовой ЦИУСБ как специализированный структурный элемент, встроенный в типовую ИТКС, в максимально возможной степени соответствует требованию технической независимости от ИТКС для обеспечения собственной защищенности;

— типовой ЦИУСБ создается и эволюционно развивается поэтапно в течение всего его жизненного цикла, который включает традиционные стадии анализа, проектирования, разработки, тестирования и интеграции, внедрения, сопровождения и развития. Эволюционность развития типового ЦИУСБ и его компонентов здесь означает возможность адаптации к расширяющимся требованиям по обеспечению ИБ для типовой ИТКС и ее пользователей, а также внедрения более совершенных ИКТ, современных отказоустойчивых вычислительных платформ и сетевого оборудования, программных средств, ОС, СУБД и др.

Выше описанные действия в соответствии с разработанной методологией построения типового ЦИУСБ хорошо согласуются с ранее упоминавшимся в отношении СУИБ циклом *PDCA*: планирование (разработка) – осуществление (внедрение и обеспечение функционирования) – проверка (проведение мониторинга и анализа) – действие (поддержка и улучшение) [105]. Кратко представим содержание этих этапов применительно к ЦИУСБ конкретной ОРГАНИЗАЦИИ [236].

Этап 1. Планирование и выработка стратегии для ЦИУСБ.

1.1. Согласовать со всеми заинтересованными сторонами видение ЦИУСБ, которое соответствует бизнес-целям ОРГАНИЗАЦИИ и согласуется с ее бизнес-планами. Установить для ЦИУСБ его цель (миссию), задачи, область действия (в том числе, по крайней мере, области мониторинга ИБ, случаи использования, тип обрабатываемых данных, типы пользователей и их взаимодействие с ЦИУСБ и т.п.), зону ответственности, процессы и процедуры. Разработать Устав и Политику ИБ, а также стратегию и форму управления.

1.2. Определить ресурсы и финансирование для ЦИУСБ.

Этап 2. Внедрение и организация руководства ЦИУСБ.

2.1. Определить и документально зафиксировать ключевые процессы управления ИБ и стандартные операционные процедуры, необходимые для поддержки ПУИИБ со стороны ЦИУСБ, как минимум: мониторинг сети, мониторинг соблюдения соответствия, оповещения и уведомления (электронная почта, мобильный телефон, чат и т.д.), процедуры и рабочий процесс принятия решений и эскалации проблем на верхние уровни управления, ведение ЖРС (логирование), расследование и отчетность по событиям ИБ и инцидентам ИБ, создание информационных панелей мониторинга, реагирование на инциденты ИБ, обмен информацией (коммуника-

ции), предоставление ежедневных услуг, управление изменениями и т.д. В область действия ЦИУСБ может входить сотни процессов и процедур, чье количество определяется многими факторами, например, количеством предоставляемых услуг, поддерживаемых клиентов, используемых технологий и т.д. Также должны быть решены все вопросы, связанные с процессами организации интеграции ЦИУСБ в ИТКС, зонированию (сегментации) ЦИУСБ согласно функциональному назначению, обрабатываемым данным и ролевому доступу и т.д.

Все необходимые средства мониторинга ИБ для сбора и передачи связанных с ИБ необработанных данных настроить таким образом, чтобы гарантировать, что критически важные серверы, услуги (например, *DNS*, контроллер домена, сервис каталогов *Active Directory*, БД, файловая система, почтовый сервер, веб-сервер и т.д.), СЗИ (такие как МЭ, СОВ/СПВ, САЗ, *netflows* и т.п.) ОРГАНИЗАЦИИ отправляют свои ЖРС и другие важные данные для аналитики и управления в ЦИУСБ. Среди этих инструментов должно быть такие, которые исследуют активы, оценивают уязвимости, обнаруживают вторжения, осуществляют мониторинг поведения и ИБ-аналитику.

2.2. Ввести в штат ЦИУСБ высококвалифицированный персонал с техническим образованием, понимающий реальные уязвимости, последствия угроз ИБ и используемые нарушителями ИБ методы взлома систем, в составе, по крайней мере, аналитика безопасности, специалистов в области безопасности, специалистов по расследованию инцидентов ИБ и определить их компетенции (с точки зрения знаний–умений–навыков), роли, часы работы, повышение квалификации и т.д.

2.3. Запустить работу ЦИУСБ и управлять полным жизненным циклом событий ИБ, включая их сбор, категоризацию, приоритезацию, открытие, назначение и закрытие инцидентов ИБ, а также проверку ошибок пользователей.

2.4. Обслуживать ежедневные рутинные операции и использовать СЗИ для поиска подозрительной/вредоносной активности, включая, но не ограничиваясь, следующим: анализ предупреждений и выполнение их сортировки путем определения критичности и масштабов воздействия, оценки вида противника, исследования *IoC* (типа доменов, *IP*-адресов, хэш-значений файлов и т.д.), просмотр и редактирование правил корреляции событий, а также обмен выводами об угрозах с сообществом *Threat Intelligence* и т.д.

2.5. Установить и использовать, где это необходимо, процедуры обратной связи, а также быть основной точкой контактов для пользователей ИТКС ОРГАНИЗАЦИИ.

Этап 3. Исследование/проверка ЦИУСБ.

Выполнить типовые тестирования, измерения и диагностику уровня ИБ ИТКС, а также операции мониторинга ИБ и аудита функционирования самого ЦИУСБ. В результате оценить, в том числе, по возможности, количественно, результативность процессов относительно соблю-

дения требований Политики ИБ, целей обеспечения ИБ для ЦИУСБ и практического опыта функционирования ЦИУСБ и проинформировать руководство о полученных результатах для последующего анализа руководством.

Этап 4. Действие в отношении ЦИУСБ.

Предложить и осуществить улучшения (корректирующие и превентивные действия) для ЦИУСБ в части функционирования, изменения/обновления процессов и т.д.

В соответствии с этими этапами непрерывной (итерационной) эволюции ЦИУСБ организации должны определить и предоставить все необходимые ресурсы, включая финансирование, Политики ИБ (например, для ЦОД в ЦИУСБ), процессы, процедуры и внутренние стандарты, метрики ИБ, услуги, укомплектование штата ЦИУСБ, компетентность персонала, осведомленность сотрудников, обмен информацией (коммуникации) и т.д.

5.2. Принципы построения типового Центра интеллектуального управления сетевой-безопасностью

На основе сформулированных в разделе 4.7 требований в качестве основных и учитывая типичные требования к системам управления [170] были определены следующие принципы построения типового ЦИУСБ, для каждого из которых дано краткое пояснение вкладываемого в них смысла:

- *определенность целей ЦИУСБ*, что обеспечит реализуемость проекта;
- *научная обоснованность и техническая реализуемость ЦИУСБ* – реализация типового ЦИУСБ и его защитных мер на современном уровне развития науки и техники для достижения поставленных перед ЦИУСБ целей и заданного уровня ИБ ИТКС, соответствующего установленным нормам и требованиям по обеспечению ИБ для подобных структур;
- *системность* – учет всех взаимосвязанных элементов, условий и факторов, влияющих на защищенность типовой ИТКС за счет интегрированного типового ЦИУСБ, включая собственную защищенность инфраструктуры ЦИУСБ и процессов обработки данных в нем на всех стадиях жизненного цикла для всех объектов защиты и направлений нарушений ИБ и инцидентов ИБ, уязвимости используемых систем, высокую квалификацию злоумышленника и т.п.;
- *комплексность (мультидисциплинарный подход)* – сочетание и согласованное использование нормативных, правовых, организационных, административных, технических (в том числе программных и аппаратных) и иных мер и средств в рамках единой СОИБ ОРГАНИЗАЦИИ;
- *непрерывность и функциональный устойчивый режим (как одно из условий обеспечения ИБ) типового ЦИУСБ* в штатном режиме, в условиях направленных на него атак, при сбоях повы-

шенной степени серьезности и в условиях чрезвычайных ситуаций для обеспечения долгосрочной постоянной доступности ресурсов и услуги ЦИУСБ для их потребителей;

— *многомерность*, означающая его вертикальную интеграцию в организационную структуру СУИБ для ЕИП ОРГАНИЗАЦИИ, а также горизонтальную – по всем структурным элементам ИТКС;

— *эшелонированная (многоуровневая) защита всех ресурсов и подсистем типового ЦИУСБ и на его основе типовой ИТКС* за счет реализации на каждом уровне соответствующих процессов и мер обеспечения ИБ от различных типов нарушителей ИБ и обеспечения независимости уровней друг от друга с точки зрения обеспечения ИБ;

— *ориентация на использование открытых стандартов*, что позволит построить типовой ЦИУСБ как открытую информационную систему с поддержанием свойств интероперабельности и переносимости (раздел 5.1) и согласовать процессы, поддерживающие функционирование ЦИУСБ, о передовыми отечественными и зарубежными практиками и стандартами;

— *функциональная полнота и методологическое единство функциональных спецификаций* – конкретный состав автоматизируемых типовым ЦИУСБ функций в рамках ПУИИБ определяется соответствующими разработанными на единой методологической основе процессами (раздел 3.4.5);

— *функционально-технологический принцип декомпозиции систем типового ЦИУСБ (модульность систем/подсистем ЦИУСБ и адаптивное управление событиями ИБ)*, который означает применение в нем совокупности унифицированных комплексов и конфигурируемых СЗИ с широкими возможностями по обеспечению ИБ типовой ИТКС, настраиваемых на заданный состав и содержание выполняемых в разные периоды времени функциональных задач;

— *разумная достаточность и эффективность* – типовой ЦИУСБ строится таким образом, что обеспечиваемый им уровень ИБ типовой ИТКС отвечал оптимизированному соотношению рисков ИБ с учетом размера возможного ущерба и требуемых затрат, то есть на основе риск-ориентированного подхода;

— *адаптивность (настраиваемость)* – обеспечение гибкой настройки типового ЦИУСБ и управляемых мер и средств обеспечения сетевой безопасности на совместную работу при изменении нормативных, правовых и других документов и динамически изменяющихся условиях функционирования типовой ИТКС;

— *унификация и типизация (тиражируемость) проектных решений*, предлагаемых для реализованных в типовом ЦИУСБ – в проекте к использованию предполагаются унифицированные и апробированные типовые проектные решения для ИКТ, СВТ, оборудования и СЗИ;

— *управляемость типового ЦИУСБ* за счет его централизованной архитектуры и распределенной/децентрализованной работы отдельных процессов;

— *масштабируемость и расширяемость (эластичность)* – обеспечение возможности увеличения/уменьшения производительности и затрат в ответ на изменения типового ЦИУСБ в потребностях его АО, ПО, систем обработки данных и т.п.;

— *эволюционность типового ЦИУСБ* – развитие СОИБ типовой ИТКС с типовой ЦИУСБ в качестве ее системообразующего элемента должно вестись параллельно с развитием самой ИТКС и ее ЦИУСБ на всех стадиях их жизненного цикла;

— *консолидация информационных ресурсов* – переход от использования разрозненных относящихся к ИБ типовой ИТКС данных из гетерогенных источников к единой инфраструктуре, обеспечивающей их консолидацию в типовом ЦИУСБ перед всесторонним анализом;

— *несекретность построения типового ЦИУСБ* – процессы, меры и средства обеспечения ИБ должны быть результативны даже в тех случаях, когда структура и принципы функционирования типового ЦИУСБ становятся известными (это не распространяется на информацию, предназначенную для управления безопасностью – закрытые ключи шифрования, пароли и т.п., когда типовой ЦИУСБ будет создаваться в конкретной ОРГАНИЗАЦИИ);

— *возможность контроля и минимизация полномочий* – каждому работнику ОРГАНИЗАЦИИ из числа пользователей, обслуживающего и эксплуатирующего персонала ЦИУСБ конкретной ОРГАНИЗАЦИИ должен предоставляться наименьший набор полномочий по доступу к услугам, информации, процедурам ее обработки, а также должны быть предусмотрены специальные средства и методы обнаружения попыток несанкционированного вмешательства в работу ЦИУСБ с возможностью проверки корректности их работоспособности;

— *простота реализации* – процессы, меры и средства обеспечения ИБ, применяемые в типовом ЦИУСБ, должны быть понятны и просты в использовании;

— *экономичность* – учет задаваемых ограничений на трудоемкость, стоимость создания, эксплуатации, сопровождения и развития ЦИУСБ для конкретной ОРГАНИЗАЦИИ.

Одновременная реализация перечисленных принципов при построении типового ЦИУСБ является гарантией выполнения ранее сформулированных требований к его функционированию.

5.3. Типовой Центр интеллектуального управления сетевой безопасностью как- объединение Центра интеллектуальной безопасности и Сетевого операционного центра

Основными типовыми целями функционирования типового ЦИУСБ в ОРГАНИЗАЦИИ могут являться, например, следующие:

— обеспечение функциональной устойчивости и надежности телекоммуникационной составляющей ИТКС за счет максимально возможной автоматизации ПУИИБ;

— обеспечение выявления аномалий, нарушений (актов незаконного вмешательства), компьютерных атак и инцидентов ИБ на ранних стадиях на основе применения ИБ-аналитики ко всем данным, связанным с ИБ и событиями ИБ в ИТКС;

— обеспечение сокращения ущерба от нарушений ИБ и инцидентов ИБ в ИТКС за счет сокращения времени реагирования на них и предупреждения их появления в будущем;

— консолидация и защита связанных с ИБ ИТКС данных из гетерогенных источников и оперативное предоставление уполномоченным лицам информации для расследования нарушений ИБ и инцидентов ИБ в ИТКС;

— предоставление информации о значимых инцидентах ИБ и нарушениях ИБ в ИТКС для целей своевременного информирования ФСТЭК России, ФСБ России, ГосСОПКА, Фин-ЦЕРТ и других уполномоченных органов и заинтересованных организаций в соответствии с установленной формой и в установленное для этих целей время.

Для достижения сформулированных целей, расширения автономности управления инцидентами ИБ в рамках одной ОРГАНИЗАЦИИ и углубления знаний об уровне ИБ ее ИТКС дальнейшее изложение результатов проведенного исследования направлено на объединение всех преимуществ ЦИБ и СОЦ с их уникальными и совместно применимыми инструментальными средствами управления сетью и ее сетевой безопасностью. ЦИБ уже был описан в разделе 4.5, поэтому далее представлен только анализ функциональных возможностей СОЦ.

5.3.1. Сетевой операционный центр

Анализ международной и отечественной практики создания СОЦ показывает, что они, как правило, принадлежат крупным организациям (конечно, возможен аутсорсинг – передача другой организации, но это не входит в область данного исследования). Первые такие центры появились в США в 1960-х годах, например, Центр управления сетью в *AT&T*, известный с 1962 г. и изменивший название на СОЦ в 1977 г.

Главная цель СОЦ заключается в создании и поддержке централизованного подразделения ОРГАНИЗАЦИИ, на основе которого персонал СОЦ может круглосуточно решать текущие вопросы управления функционированием ИТКС для обеспечения бесперебойной работы сетей передачи данных, систем хранения, вычислительных ресурсов, предоставляемых услуг и т.п. Это подразумевает возможность удаленно наблюдать, поддерживать и осуществлять контроль (мониторинг, диагностику) телекоммуникационной сети ИТКС с помощью всего необходимого ПО и АО для управления ее оптимальным функционированием для различных платформ, сред и каналов связи, а также визуализировать подробную информацию о детальном состоянии всех устройств, за которыми ведется наблюдение [231]. Значительно упрощая роль СОЦ, можно

сделать вывод, что он достигает своей цели, выполняя ряд проверок и процедур восстановления для критических подсетей, устройств, приложений, данных и, в конечном счете, всей ИТКС. Эти центры могут рассматриваться как координационные центры, поддерживающие следующие типичные виды деятельности персонала СОЦ [234, 237, 238]:

- исследование, проведение различных оценок, управление и постоянная поддержка высокой доступности телекоммуникационных сетей и устройств за счет анализа основных параметров внутрисетевого трафика, что называется «телеметрией» (от др.-греч. *τῆλε* «далеко» + *μέτρον* — «измеряю»);

- круглосуточный контроль и мониторинг производительности сетевой инфраструктуры и всех компонентов сети, включая телекоммуникационные устройства, выделенные линии связи, международные каналы, каналы доступа в интернет, маршрутизирующее оборудование, серверы, виртуальные машины и т.д.;

- планирование производственной мощности ОРГАНИЗАЦИИ;

- постоянное исследование и контроль возникающих проблем и аномалий (например, выявление отключений и сбоев в сети электропитания, обнаружение ошибок с потерей фреймов или битов при передаче данных по каналам связи, обнаружение ошибок в строках программного кода, выявление выхода из строя каналов связи и другие вопросы, которые могут указывать на проблемы с работоспособностью сетей), изоляция проблем, определение их характера и причин возникновения, выработка рекомендации по устранению проблем, доставка предупреждений правильному персоналу, выделение ресурсов, координация действия по их разрешению, автоматическая эскалация неотложных проблем, подготовка отчетности, внесение информации о проблемах в единую БД и т.п.;

- управление доменными именами;

- управление конфигурациями устройств и версиями (релизами) ПО;

- управление хранилищами данных;

- управление электронной почтой и голосовым и видео- трафиком;

- управление поддержкой конечных пользователей и др.;

- администрирование и резервное копирование систем и данных;

- управление оптимизацией и качеством обслуживания, предотвращение деградации услуг, подготовка соответствующей отчетности;

- установка, распространение, устранение неполадок и обновление прикладного ПО;

- координация доступа в/из аффилированных сетей (например, бизнес-партнеров);

- применение политик и требований *SLA*;

- работа с основными (простейшими) средствами управления ИБ, такими как аутентификации и авторизации, фильтрация *IP*- и *MAC*-адресов; и т.д.

Для достижения наибольшей производительности персонал СОЦ обычно разделен на несколько групп – служба технической поддержки (англ. *Help Desk*), первая линия поддержки (англ. *First Level Operations*), вторая линия поддержки (англ. *Second Level Operations*) и т.д. В каждой группе работают профильные специалисты необходимой квалификации, для которых четко регламентированы действия и зоны ответственности.

Как видно из приведенного описания, по своей сути СОЦ работает с данными о состоянии сети и ее отдельных элементов, что похоже на функционирование ЦИБ с тем различием, что последний имеет дело только с данными о событиях ИБ.

Для большей наглядности сравнительный анализ характеристик ЦИБ и СОЦ, обобщающий собственные результаты и представленные в работах [239, 240], приведен в табл. 17, которая необходима для понимания и формулирования функциональных возможностей ЦИУСБ.

5.3.2. Функциональные возможности объединенного типового Центра интеллектуального управления сетевой безопасностью

В данном исследовании предлагается создать объединенный ЦИУСБ, который сочетает в себе всю специфику и преимущества ЦИБ и СОЦ. Оба этих центра предназначены для выявления, расследования, установления приоритетов, эскалации и решения проблем, но при этом типы проблем и области их действия значительно различаются, что при объединении позволяет получить качественно новую, более функциональную структуру – ЦИУСБ. Его главная цель – предоставить ОРГАНИЗАЦИИ управляемую на основе интеллекта сетевую безопасность ИТКС, что даст возможность опережать возникающие проблемы в области ИБ за счет как можно более тесной интеграции со всеми бизнес-процессами в ОРГАНИЗАЦИИ [213, 215].

Создание ЦИУСБ объективно возможно потому, что реализация основных функций ЦИБ и СОЦ часто организована похожим образом – с многоуровневым подходом, аналогичными ролями на первых линиях поддержки и возможным совместным использованием некоторых инструментальных средств на техническом уровне. Объединение двух центров в один единый выгодно и в долгосрочной перспективе, поскольку главной задачей СОЦ является обслуживание основной деятельности ОРГАНИЗАЦИИ, в то время как ЦИБ призван обеспечить ее ИБ. Так, например, при обнаружении сбоя персонал СОЦ, скорее всего, объяснит его сбоем функционирования устройства или системы и попытается устранить путем замены оборудования или изменения конфигурационных настроек. Персонал же ЦИБ может связать проблему с вирусной активностью и скорее всего начнет самостоятельное расследование, прежде чем инициирует более сложные действия в ответ на это событие ИБ.

Таблица 17 – Сравнительный анализ характеристик СОЦ и ЦИБ

Параметр	СОЦ	ЦИБ
Область действия	Используется для решения задач, связанных с управлением, мониторингом и контролем ИТКС.	Отслеживает угрозы ИБ для всех элементов ИТКС (в первую очередь ее информационных активов), пытающиеся использовать уязвимости и проникнуть внутрь ИТКС.
Ключевая роль	Противостоять угрозам для инфраструктуры ИТКС, постоянно зная о ее текущем состоянии, соблюдая <i>SLA</i> и управляя инцидентами для достижения максимального времени бесперебойной/безотказной работы.	Противостоять угрозам ИБ для информационных активов ИТКС, защищая коммерческую тайну, ПДн, интеллектуальную собственность, данные пользователей и т.п.
Цель	Отслеживать производительность ИТКС, устранять неисправности оборудования, оповещать о нарушениях производительности и устранять проблемы с производительностью в первую очередь с точки зрения обеспечения доступности и сокращения времени простоя, а также улучшения географического покрытия.	Отслеживать сохранение всех свойств ИБ для информационных активов ИТКС и качество предоставления услуг ИТКС, а также быстрое реагирования при его ухудшении и инцидентах ИБ, которые влияют на пользователей ИТКС и ее активы, с целью сокращения потенциальных потерь от инцидентов ИБ и повышения степени удовлетворенности потребителей.
Влияние на бизнес	Операционный уровень.	Стратегический уровень, учет слияния технических проблем с человеческим фактором.
Природа источников решаемых проблем	Естественные прогнозируемые и предсказуемые системные события, происходящие с устройствами.	В первую очередь «умные», часто непредсказуемые противники – нарушители ИБ, а затем и другие источники угроз ИБ.
Технологии, используемые при функционировании	Реактивный подход, доступ к данным в режиме реального времени, интерактивные информационные панели, отображающие показатели производительности, технология автоматического оповещения о нарушениях производительности, аварийные сигналы.	Упреждающий подход, доступ к данным, включая исторические, в режиме реального времени, сложные интерактивные информационные панели, технология прогнозирования для раннего оповещения о потенциальных влияющих на бизнес проблемах.
Средства	Системы управления элементами, ПО для устранения неисправностей, инструменты для регистрации неисправностей, ПО для мониторинга производительности.	МЭ, САЗ, СОВ/СПВ и другие СЗИ, <i>SIEM</i> - и <i>SOAR</i> -системы, ПО для определения качества предоставляемых услуг и т.п.
Примеры метрик	Мониторинг ключевых показателей эффективности сети, таких как потеря видеопакетов и потеря вызовов.	Количество отраженных сетевых атак, количество обнаруженных в режиме реального времени инцидентов ИБ, количество выявленных на конечных устройствах компьютерных вирусов.
Сопровождение	Базируется в одном или нескольких местах, размер штата обычно от 80 до 500+ специалистов.	10-100 специалистов.
Навыки, требуемые от персонала	Сетевая инфраструктура, обслуживание сетей, устранение неисправностей, ИТ, системная инженерия, поддержка приложений и аналитика данных.	ИБ, сетевая безопасность, управление и инфраструктура ИБ, оценка рисков ИБ, моделирование сервисов, ИБ-аналитика и интерпретация данных.

В дополнение ко все еще остающемуся ручному контролю ИТКС, ЦИУСБ предоставляет возможности автоматизированного мониторинга ПО и АО и исследования первопричин событий ИБ для последующего определения характерных тенденций, возникающих при обработке, хранении и передаче данных в ИТКС, а также способен выполнять задачи управления контролем доступа, отражения и предотвращения вторжений и расширенного анализа угроз ИБ.

Просматривая всю ИТКС в конкретном контексте деятельности ОРГАНИЗАЦИИ, ЦИУСБ понимает, как организована сеть и как по ней перемещаются информационные потоки. Получая ЖРС от серверов, БД, ПО, веб-сайтов, СЗИ, конечных точек (компьютеров и других устройств, используемых пользователями), он управляет доставкой собранной информацией к *SIEM*-системе для анализа и сопоставления с известными угрозами ИБ и обнаружения проблем. В таком ЦИУСБ более результативно осуществляется поиск необычного и подозрительного поведения пользователей, систем и конечных точек, сбор свидетельств инцидентов ИБ и «охота за угрозами».

Следовательно, ЦИУСБ получает мощную синергию ЦИБ и СОЦ за счет тесного сотрудничества их персонала и совместного использования применяемых в них инструментальных средств и технологий. В итоге получаемыми функциональными возможностями объединенного ЦИУСБ для их организаций-владельцев являются следующие [213, 215, 231]:

- централизованное управление ЦИУСБ как в части функций, выполняемых ЦИБ, так и СОЦ, с отображением в «едином окне», предназначенном для администрирования и принятия решений;

- полная ситуационная осведомленность с «бесшовной» интеграцией и комплексным отслеживанием контролируемых объектов и процессов ИТКС (с созданием и ведением единой БД активов) и услуг ИБ-аналитики с поддерживающей инфраструктурой, включая мониторинг и СЗИ;

- мониторинг ИТКС и ее ИБ в режиме реального времени, интегрированный с требованиями по обеспечению ИБ и включающий автоматизированный контроль за производительностью и доступностью ИТКС и всех ее элементов, оповещения и уведомления (на основе протоколов управления сетью), стандартные клиент/серверные протоколы, отчетность о выполнении требований *SLA*, интегрированную службу технической поддержки (*Help Desk*) и т.д.;

- централизованное управление и аудит конфигурационных настроек сетевых устройств и СЗИ, БД, архивов и т.п., включая их изменения, отображаемые в привязке к изменению мер обеспечения ИБ и нарушению базовых настроек, а также полную историю их изменения и т.д.;

- управление изменениями сетевых устройств вместе с процессом автоматического утверждения, указанием ссылки на шаблон настройки, проверкой управления изменениями, жур-

налом истории;

— автоматизированный сбор данных, включая сбор событий и потоков, агрегирование и корреляцию посредством автоматизации и расширенной (как с точки зрения сети, так и ИБ) аналитики, с целью извлечения максимальной пользы из огромного количества данных, связанных с ИБ, доступных ЦИУСБ;

— мониторинг всей сетевой активности, связываемой с объектами, а не *IP*-адресами;

— приоритезация предупреждений об опасности от СЗИ в соответствии с наиболее вероятными событиями, которые могут привести к наиболее негативным последствиям;

— извлечение большего интеллектуального контекста в масштабах всего ЕИП ОРГАНИЗАЦИИ, что помогает ей в принятии оперативных и стратегических решений в области ИБ и проверки того, что у нее имеется правильная Политика ИБ;

— возможность предоставлять, записывать и часто обновлять метаданные для каждого обнаруженного события/инцидента ИБ для его рекурсивного анализа во время реагирования на инцидент ИБ. Такие метаданные важны для ИБ-аналитики, чтобы свести к минимуму «шум» в данных и дифференцировать события ИБ и инциденты ИБ друг от друга;

— более быстрое обнаружение событий ИБ и сокращение времени реагирования на инциденты ИБ посредством того, что автоматическое устранение ошибок, обновления и активизация мер обеспечения ИБ работают совместно для достижения общих целей, но при этом ЦИБ и СОЦ предоставляют свои специализированные функции, навыки и опыт, дополняя друг друга;

— расширенное расследование инцидентов ИБ в ИТКС, включающее сохранение всего трафика, реконструкцию пакетов, восстановление сеансов пользователей, интеграцию с реагированием на инциденты ИБ и т.д.;

— улучшенное планирование и реализация мер обеспечения ИБ при совместной ответственности за идентификацию и устранение причин возникновения инцидентов ИБ;

— действенное и рациональное управление инцидентами ИБ (включая аналитику поведения при непрерывном мониторинге, предварительный и последующий анализ) и расширенную отчетность с ценными результатами;

— централизованная управляющая консоль с информационными панелями и отчетами, позволяющая управлять рисками ИБ и соблюдать требования соответствия, а также отображающая топологию ИТКС и визуализирующая информационные потоки в ней;

— регулярный аудит ИБ ИТКС и проведение различных оценок поддающихся измерению характеристик с предоставлением отчетов и обобщающих обзоров с заранее определенными метриками ИБ;

— улучшенный обмен информацией (коммуникации) с предустановленной эскалацией и результативным совместным использованием синтезированных знаний для повышения осве-

домленности о ситуации и координации реагирования;

— измерение ключевых показателей эффективности (англ. *Key Performance Indicators, KPI*) на основе контроля производительности и ложных положительных и отрицательных срабатываний, снижение соотношения «сигнал/шум» для событий ИБ;

— учет и отслеживание интенсивности потребления пользователями ресурсов и услуг ЦИУСБ.

На основе целей и получаемых результатов функционирования можно заключать, что для ЦИУСБ как объединения ЦИБ и СОЦ существует четыре ключевых бизнес-процесса:

- 1) мониторинг, аудит и оценка сетевой безопасности;
- 2) классификация и сортировка событий в ИТКС;
- 3) приоритезация, анализ и прогнозирование событий в ИТКС;
- 4) исправление проблем, связанных с этими событиями, и восстановление после них.

Другими группами бизнес-процессов являются процессы управления ЦИУСБ, процессы измерения, анализа и совершенствования функционирования ЦИУСБ, а также вспомогательные процессы, обеспечивающие осуществление ключевых бизнес-процессов.

Чем более интегрированным и автоматизированным будет взаимодействие ЦИБ и СОЦ, тем более результативным будет функционирование ЦИУСБ. Опять образно говоря, ЦИУСБ – это «быстрый мозг обеспечения адаптивной упреждающей сетевой безопасности с широко открытыми глазами и умелыми руками» [213]. Однако операционные модели и процессы только ведущих организаций являются достаточно зрелыми для поддержки этой расширенной совместной модели упреждающего управления инцидентами ИБ для ИТКС ОРГАНИЗАЦИИ, построенного на архитектуре ИБ-аналитики больших относящихся к ИБ данных.

5.3.3. Визуализация информации в типовом Центре интеллектуального управления сетевой безопасностью для принятия решений по управлению инцидентами-информационной безопасности в информационно-телекоммуникационной сети

Визуализация уже давно стала популярным и наглядным средством выявления и разрешения возникающих проблем в области управления ИБ. Визуализация информации об ИБ ИТКС ОРГАНИЗАЦИИ в ЦИУСБ должна представлять некие абстрактные данные о состоянии защищенности всех объектов защиты ИТКС, если сравнивать ее с визуализацией физически существующих явлений или данных (например, человеческого тела, географических карт, землетрясения, воронки урагана, цунами и т.п.). В реальности чаще всего не существует тех объектов, которые подлежат условному отображению на экране монитора сотрудника ЦИУСБ. Например, довольно сложно представить себе низкоуровневую информацию о сети или информа-

цию, полученную от отдельного сетевого устройства, для выявления событий ИБ в виде свершившихся атак или только развивающихся на глазах администратора или аналитика ИБ попыток атак на оборудование или отдельный сервер ИТКС [48].

Подлежащая визуализации в ЦИУСБ информация об ИБ ИТКС ОРГАНИЗАЦИИ может быть использована для непосредственного анализа, обнаружения событий ИБ в потоке всех собранных событий, принятия решений в области управления ИБ и ознакомления с этой информацией определенного круга уполномоченных лиц. Например, при решении следующих важных задач защиты ИТКС от компьютерных атак из внешних сетей типа интернета или злоупотреблений со стороны инсайдеров ОРГАНИЗАЦИИ:

- трассировка перемещения сетевых пакетов по каналам связи между хостами в ИТКС;
- анализ информационных потоков и выявление несанкционированных (мошеннических) операций с информацией;
- результаты контроля доступа ко всем ресурсам ИТКС (включая оборудование, приложения, БД, серверы, файлы и т.д.);
- результаты контроля системных конфигураций и конфигурационных настроек АО и СЗИ ИТКС и их соответствия установленным требованиям (политикам);
- распознавание удаленных сетевых атак;
- нахождение путей распространения компьютерных вирусов и червей или функционирования так называемых зараженных ботнетов (от англ. *robot networks or botnets*), обычно используемых для злоумышленной деятельности — рассылки спама и вирусов, распределенного подбора паролей на удалённых компьютерах, запуска *DoS*-атак и т.п.;
- исследование кода вредоносных программ или компьютерных вирусов;
- результаты корреляции обнаруженных событий ИБ и «срез» событий ИБ для выделенного канала связи, сетевого устройства, сетевого протокола, сервиса, приложения и т.п.;
- результаты сопоставления событий ИБ с результатами анализа уязвимостей элементов ИТКС;
- показ уведомлений/предупреждений и рекомендаций по устранению возникших проблем с обеспечением ИБ отдельных элементов ИТКС, автоматически генерируемых СЗИ;
- установление некоторых признаков (например, сигнатур сетевых атак);
- построение моделей и разработка правил обеспечения ИБ (например, для настройки в МЭ);
- отображение тенденций в изменении уровня ИБ и рисков ИБ ИТКС;
- визуализация свидетельств инцидентов ИБ для дальнейшего их расследования;
- обнаружение аномальной активности и контроль неблагонадежных сотрудников;
- анализ правильности настроек СЗИ;

- результаты обнаружения уязвимостей в элементах ИТКС;
- результаты инвентаризации (контроля состава) АО, ПО и СЗИ, применяемых в ИТКС;
- изучение взаимодействия при одновременном использовании различных технологий обеспечения ИБ и отдельных СЗИ;
- обучение вопросам ИБ и повышение осведомленности в области обеспечения ИБ работников ОРГАНИЗАЦИИ и т.п.

Проанализировав основные задачи управления сетевой безопасностью ИТКС, можно сделать вывод, что визуализация информации об ИБ ИТКС возможна с двух основных точек зрения – обобщенно по всей ИТКС или по отдельным событиям ИБ [48].

В первом случае объектами визуализации в ЦИУСБ для принятия решений его персоналом может являться следующая обобщенная информация об ИБ ИТКС:

- показатели защищенности ИТКС в целом и ее отдельных частей, включая риски ИБ (по типам, последствиям, вероятностям реализации) и места локализации уязвимостей;
- показатели результативности работы СЗИ по типам и местам их использования;
- статистические данные по количеству событий и инцидентов ИБ по типам, критичности, местам возникновения и т.п.;
- определение приоритетных направлений, требующих немедленного вмешательства;
- статусы и текущие состояния событий ИБ и инцидентов ИБ и т.д.

В отношении отдельного события ИБ должна визуализироваться информация, отвечающая на следующие вопросы:

- кто: субъект доступа;
- почему: например, невольное или непреднамеренное действие (ошибка), неосведомленность, небрежность или безответственность, злонамеренные действия (внешние или внутренние), вследствие аварии;
- что: НСД к системе и/или информации, несанкционированное воздействие на ИС и/или против ИТКС или всей ОРГАНИЗАЦИИ, несанкционированная установка программ (без согласия владельца), дистанционное нарушение работы ИС, создание стрессовых ситуаций, физическое вторжение или незаконное действие, незаконная деятельность в интернете (наносящая вред ОРГАНИЗАЦИИ), различные человеческие ошибки (в администрировании, обработке, программировании, совместном использовании), поломка или неисправность АО, проблемы в окружающей среде (вызывающие недоступность компонент ИС из-за стихийного бедствия);
- как: для каждого вышеупомянутого «что» возможность, список используемых методов и средств – особенно для компьютерных атак;
- статус события ИБ: предпринятая попытка, в стадии реализации, успех или неудача нарушения ИБ;

— какая при этом использовалась уязвимость: в поведении, ПО, конфигурации оборудования или ПО, общей защите, архитектуре или процессах систем, физическом материале;

— на какой тип активов (основных и связанных с ними): БД и приложения (находящиеся на периметре, внутри ИТКС ОРГАНИЗАЦИИ, в общем облаке, на аутсорсинге), системы (находящиеся на периметре, внутри ИТКС ОРГАНИЗАЦИИ, в общем облаке, на аутсорсинге), сети и телекоммуникации (низкоуровневые устройства, высокоуровневые коммуникации, промежуточное ПО, беспроводные устройства, СЗИ), устройства автономного хранения (бумага, электронные устройства, магнитные и оптические устройства), устройства конечного пользователя (ПО локального применения – принадлежащие пользователю или ОРГАНИЗАЦИИ, многоцелевые рабочие станции, люди (работник, бизнес-партнер, поставщики услуг с собственным оборудованием или без), средства и окружающая среда (недвижимость, физические средства или системы защиты, здания и помещения, офисная мебель);

— каковы последствия для свойств информации (нарушения конфиденциальности, целостности, доступности, неотказуемости и т.д.);

— каковы последствиями для бизнеса в целом: прямые или косвенные.

Получая перечисленную информацию на экран монитора, например, оператор ЦИУСБ оперативно отреагирует на выявленные отклонения от штатного функционирования систем или передает данную проблему на следующий уровень эскалации, а аналитик ИБ выделяет какие-либо тенденции и далее учитывает их при описании новой атаки и т.п. и, в конечном счете, выборе упреждающей стратегии защиты отдельного элемента ИТКС.

5.4. Архитектура типового Центра интеллектуального управления сетевой безопасностью

5.4.1. Функциональная архитектура типового Центра интеллектуального управления сетевой безопасностью

Инфраструктура типового ЦИУСБ ОРГАНИЗАЦИИ должна строиться по иерархическому принципу и представляет собой специализированный комплекс современных организационных, технических, аппаратно-программных, технологических и других мероприятий и средств, который обеспечивает ИБ ИТКС и самого ЦИУСБ на всех стадиях их жизненного цикла. С одной стороны типовой ЦИУСБ интегрирован с ИТКС для получения всех относящихся к ИБ данных для их детального анализа и создания защищенного ЕИП ОРГАНИЗАЦИИ, а, с другой стороны, типовой ЦИУСБ рассчитан на обслуживание своих функциональных систем (подсистем) посредством создания своей выделенной транспортной сети с использованием ресурсов и услуг, предоставляемых только внутри ЦИУСБ, которые при этом тем или иным способом интегрируются между собой.

Программно-техническое взаимодействие типового ЦИУСБ с типовой ИТКС и другими внешними системами и источниками информации (например, *Threat Intelligence*) должно осуществляться на основе стандартных или специальных унифицированных протоколов и стандартов и поддерживаться на уровне приложений и информационного обмена с учетом принятых требований. Создание индивидуальных протоколов взаимодействия с каждой из таких систем не целесообразно, ибо это будет серьезно противоречить требованиям унификации.

Руководствуясь лучшими практиками построения инфраструктур для сложных сетевых систем с точки зрения выполняемых на их основе бизнес-операций и упорядочения процессов и мер обеспечения ИБ, для типового ЦИУСБ ОРГАНИЗАЦИИ можно выделить пять функциональных инфраструктурных уровней – уровни платформ, ПО, предоставления услуг, доступа и управления (рис. 43) [236].

Уровень доступа	Уровень управления
Уровень предоставления услуг	
Уровень ПО	
Уровень платформ	

Рисунок 43 – Многоуровневая функциональная инфраструктура типового ЦИУСБ

Уровень платформ предоставляет множество базовых «строительных блоков» для следующего уровня ПО и включает в себя сетевую инфраструктуру, хранилища данных, СВТ, средства резервного копирования, средства виртуализации, вычислительные средства и т.п. На этом уровне находятся и внутренние сервисы этих платформ, отвечающие за управление, например, памятью, процессами и нитями, межпроцессным взаимодействием, событиями, ошибками и исключительными ситуациями, временем, логическим именованием ресурсов, устройствами, файловыми системами, конфигурированием систем и т.д., сервисы обработки транзакций, обмена данными, печати и многое другое [55].

Уровень ПО содержит прикладное ПО, которое поддерживает всю деятельность ЦИУСБ в рамках ПУИИБ и использует услуги приложений, находятся на уровне платформ.

Уровень платформ совместно с уровнем ПО являются системообразующей основой ЦИУСБ с точки зрения применения ИКТ.

Уровень предоставления услуг обеспечивает возможность осуществлять те действия по управлению услугами ЦИУСБ, которые требуют введения входных данных и взаимодействия с владельцами услуг и владельцами ОРГАНИЗАЦИИ. Элементы этого уровня также отвечают за преобразование требований к управлению ИБ в вид, пригодный для дальнейшего использова-

ния при выполнении различных технологических и операционных действий (такие как оптимизация обслуживания, жизненный цикл услуг, работа с каталогами, работа с автоматизированными бизнес-процессами ЦИУСБ и т.д.). Этот уровень отражает специфику деятельности ЦИУСБ, осуществляемой с применением ИКТ.

Уровень доступа связан с уровнями предоставления услуг и управления. На уровне доступа услуги ЦИУСБ и его конечные пользователи подключаются к ЦИУСБ. Этот уровень позволяет управлять и поддерживать доступ к ЦИУСБ из единой точки, используя комбинацию нескольких сервисов на основе каналов ИКТ и решает проблемы доступа большой емкости, высокой производительности и надежности устройств, поддержки протоколов и т.д. (например, путем выполнения балансировки нагрузки). На этом уровне также находятся сервисы человеко-машинного взаимодействия, включая сервисы командного, текстового и графического пользовательских интерфейсов [55].

Уровень управления необходим для оперативного управления ЦИУСБ с помощью ИКТ. Он обеспечивает набор средств для уровней управления платформами и ПО, необходимых для поддержки уровня предоставления услуг и эксплуатационных процессов, осуществляемых с помощью ИКТ, а также для поддержки персонала при решении задач управления доступностью, производительностью, сетями, услугами, установкой, настройкой, изменениями, организацией хранения данных, диспетчеризацией заданий, администрированием пользователей, мониторингом, корректным запуском и остановом систем, сервисами резервного копирования и восстановления информации, знаниями, проблемами, нештатными ситуациями, инцидентами, отчетностью, системой печати, защитой данных и т.д.

Все эти уровни и взаимосвязи между ними должны быть защищены соответствующими мерами обеспечения ИБ. Следовательно, инфраструктура защищенного типового ЦИУСБ должна соответствовать требованиям обеспечения его ИБ с разных точек зрения – АО, ПО, технической, организационной и т.д.

5.4.2. Архитектура обработки относящихся к информационной безопасности-информационно-телекоммуникационных сетей данных в типовом Центре-интеллектуального управления сетевой безопасностью

В последние десятилетия данные организаций, аккумулируемые в их ИТКС как основы ЕИП и используемые для более качественного принятия своевременных и обоснованных решений для эффективной деятельности ОРГАНИЗАЦИИ, растут чрезвычайно быстро. Это огромные объемы данных о текущем состоянии их сетей и, на первый взгляд, несвязанных событиях, происходящих в них. В разделе 1.2.4 уже отмечалось, что данные могут поступать от различ-

ных серверов, контроллеров доменов, СЗИ и характеризовать сетевой трафик, работу средств связи, приложений и сетевых сервисов, действия конечных пользователей, веб-контент, передачу мультимедиа, геолокации, данные бизнес-процессов, внутренние документы и аналитические данные ОРГАНИЗАЦИИ за многие годы ее существования [41]. Все данные, относящиеся к ИБ ИТКС ОРГАНИЗАЦИИ, должны надлежащим образом собираться, интерпретироваться, сопоставляться и оцениваться с точки зрения обеспечения ИБ. Таким образом, можно выделить четыре вида разнородных данных, с которыми работают системы ИБ-аналитики ЦИУСБ [213], типичными представителями которых являются *SIEM*- и *SOAR*-системы:

- 1) данные, находящиеся в отдельных устройствах и СЗИ, приложениях и БД;
- 2) данные, собранные от отдельных систем, приложений и т.д., создающие другие данные, и поступающие, например, в другие БД, где они хранятся и обрабатываются без взаимодействия с источником данных;
- 3) данные в потоках со следующими уникальными характеристиками: огромный или, возможно, бесконечный объем, динамически изменяющиеся, входящие и выходящие в фиксированном порядке, требующие быстрого (в режиме реального времени) отклика и т.д. Типичные примеры включают различные виды последовательных по времени данных и данные, полученные в динамической сетевой среде, такие как сетевой трафик, данные от телекоммуникационного оборудования, систем видеонаблюдения, сенсорных сетей, потоки «кликов» на веб-сайтах, результаты мониторинга ИБ и т.д.;
- 4) данные от различных бизнес-подразделений ОРГАНИЗАЦИИ, операционных групп, отделов и т.д.

Основной особенностью этих данных является то, что они представлены в разных форматах для разных целей часто с разными Политиками ИБ и требованиями соответствия и поступают в системы обработки ЦИУСБ в виде непрерывных потоков больших данных, требующих немедленной и быстрой обработки. При этом данные могут быть структурированными, слабоструктурированными и неструктурированными, что не позволяет результативно управлять ими и обрабатывать традиционным образом. Кроме этого, их не следует рассматривать как простое сочетание отдельных элементов – напротив, необходимо поддерживать фиксированные отношения каждого исполнения и модификации файла, изменения реестра, сетевого соединения, исполняемого бинарного файла в ИТКС ОРГАНИЗАЦИИ и т.д.

Указанные особенности характерны для известной проблемы больших данных (англ. *big data*). Теоретической основой **ИТ больших данных** стал раздел информатики, получивший название «наука о данных» (англ. *data science*), а критериями, определяющими их отличие от традиционных ИТ, являются «три V»: *volume* – сверхбольшой объем данных, *velocity* – очень высокая скорость передачи данных и *variety* – слабая структурированность данных, которая понима-

ется, прежде всего, как нерегулярность структуры данных и трудность извлечения однородных данных из потока для дальнейшей корреляции. Позднее к ним добавились и другие критерии: *veracity* (достоверность), *variability* (изменчивость), *value* (ценность), *visibility* (видимость). В [41] предложена следующая интерпретация понятия «большие данные»: массивы данных такого объема и структуры, которые превышают возможности традиционных программных инструментов (БД, ПО) по сбору, хранению и обработке данных за приемлемое время и тем более превышают возможности их восприятия человеком.

Актуальность применения ИТ больших данных при решении вопросов обеспечения ИБ многократно подчеркивалась в различных работах, например, в [241-243]. Бывший руководитель группы службы безопасности *Barclays*, работающий в компании *Splunk*, С.Гейли сказал [241]: «Безопасность – теперь проблема больших данных, потому что данные, относящиеся к безопасности, огромны. Это не просто набор инструментов безопасности, создающих данные, это вся ваша организация. Если вы собираетесь игнорировать некоторые из этих данных, или если вы не можете проанализировать их, значит, вы не правильно реализуете защиту. Для вашей организации может иметь значение каждая маленькая деталь, которую вы пропускаете или игнорируете».

При управлении сетевой безопасностью чем больше в ЦИУСБ ОРГАНИЗАЦИИ собрано данных для анализа, тем более качественно можно установить важные корреляции, уменьшить количество ложных срабатываний и повысить доверие к обнаруживаемым нарушениям ИБ и, в конечном итоге, сократить среднее время реагирования на инциденты ИБ. Тогда ИТ больших данных в типовом ЦИУСБ могут применяться в основном с двумя целями [49]:

1) предоставление этих технологий в качестве услуг при реализации других ИТ (в частности, технологии поиска и анализа данных для выявления скрытых шаблонов) и в качестве первичных источников поиска информации и извлечения основного содержания (семантики) в сверхбольших массивах документов без их непосредственного чтения человеком и т.д.;

2) собственно ИБ-аналитика для ИТКС с целью выявления аномалий в функционировании систем, инцидентов ИБ, предотвращения вторжений и т.д., которая включает в себя три важных действия [180, 213]:

— собирать: получать миллионы событий в секунду, часть из которых после обработки будут рассматриваться как инциденты ИБ;

— принимать решение, основанное на данных, по каждому событию, потенциально влияющему на ИБ ИТКС;

— анализировать в режиме реального времени: запускать автоматизированный анализ и обеспечивать видимость обнаруженных тенденций по событиям, уязвимостям, угрозами ИБ и т.д.

Известно три типа обработки больших данных [244, 245], все из которых применимы для использования в типовом ЦИУСБ:

1) *пакетная обработка* (англ. *batch processing*) в псевдореальном, или «мягком» реальном времени, когда обработке подвергаются данные, уже сохраненные в энергонезависимой памяти, а вероятностно-временные характеристики процесса преобразования данных в основном определяются требованиями прикладных задач;

2) *потокковая обработка* (англ. *stream processing*) в «жестком» реальном времени, когда обработке подвергаются данные, находящиеся в оперативной памяти, без сохранения на энергонезависимых носителях, а вероятностно-временные характеристики процесса преобразования данных в основном определяются темпом поступления данных, поскольку появление очередей на обрабатывающих узлах приводит к безвозвратной утрате данных. Примерами служат данные от смарт-камер видеонаблюдения или сетевой трафик. Здесь требуется потокковая система и хранилище данных, способные передавать и обрабатывать данные о событиях со скоростью их поступления [213];

3) *гибридная обработка*, использующая гибридную модель (известную как «Лямбда архитектура» [245, 246]) с тремя архитектурными принципами: надежность (система должна быть в состоянии управлять АО, ПО и человеческими ошибками), неизменность данных («сырые» данные сохраняются всегда, и они никогда не изменяются) и повторяемость (результаты всегда можно получить вычислением (повторным вычислением) из хранимых исходных данных), и четырехуровневой архитектурой: пакетный уровень (содержит неизменный, постоянно растущий мастер-набор данных, хранимый в распределенной файловой системе, и обрабатывает пакет исходя из этих исходных данных), уровень сервисов (загружает и предоставляет новые пакеты в хранилище данных для дальнейшего выполнения запросов), уровень скорости (имеет дело только с новыми данными и компенсирует высокую латентность уровня сервиса и обрабатывает новые пакеты в режиме реального времени) и уровень комбинирования (для синхронизации, объединения результатов и других нетривиальных действий).

ИТ больших данных относятся к «дата-центрированными», или «управляемыми данными» (англ. *data-centric, data-driven*). Если в традиционных ИТ в центр процесса обработки данных ставится обрабатывающее устройство или среда (компьютер, кластер, облачная среда), которые обрабатывали запросы (заявки и пр.), то большие данные рассматриваются прежде всего как непрерывно «текущая» субстанция, методики обработки которой должны быть встроены в потоки [49]. При этом скорость приема вновь поступающих данных в обработку и скорость выдачи результатов должны быть не ниже скорости потока, иначе в противном случае это приводило бы к бесконечному росту очередей, либо бесполезному хранению бесконечно увеличивающегося объема необработанных данных.

Сформулируем важные характеристики больших данных, которые хорошо согласуются с требованиями к типовому ЦИУСБ ОРГАНИЗАЦИИ, сформулированными в разделе 4.7 [49]:

- быть своевременными: данные должны быть актуальными и отражать текущий уровень ИБ ИТКС, угрозы ИБ, уязвимости, меры обеспечения ИБ, а также, в случае необходимости, к основным данным в установленном порядке могут быть добавлены исторические данные;
- быть всеобъемлющими: данные должны быть собраны воедино, чтобы отражать полную картину, гибко интегрированы и легко переработаны в полезную и значимую информацию – чтобы незамедлительно помочь в обеспечение ИБ ИТКС ОРГАНИЗАЦИИ;
- быть адаптированными: данные должны быть адаптированы к достижению конкретной задачи в рамках общей цели обеспечения ИБ ИТКС;
- быть точными: данные должны быть корректными и полученными от надежного (доверенного) источника в ИТКС;
- быть релевантными: данные должны быть значимыми и применимыми для дальнейшего использования.

В целом, обработка больших относящихся к ИБ данных в типовом ЦИУСБ направлена на «добычу» новых данных (англ. *data mining*) – получение (извлечение) знаний из больших объемов данных. Это понятие является мультидисциплинарным, объединяющим базы и хранилища данных, машинное обучение, высокопроизводительные вычисления, распознавание образов, нейронные сети, визуализацию данных, поиск информации, обработку изображений и сигналов, пространственный или временный анализ данных, статистические методы и т.п., что и интегрировано в ИБ-аналитике (раздел 4.4). Ее задачи в данном контексте могут быть классифицированы как описательные, характеризующие общие свойства больших относящихся к ИБ данных, так и предсказательные, делающие вывод о текущих данных для составления прогнозов развития ситуации с обеспечением ИБ ИТКС ОРГАНИЗАЦИИ.

Процесс получения знаний об ИБ ИТКС ОРГАНИЗАЦИИ в типовом ЦИУСБ состоит из последовательности шагов, представленных на рис. 44 ([49], адаптировано на основе [247, 248]), часть из которых может итерационно повторяться. По описанию выполняемых операций очевидно, что рис. 42 и рис. 40 полностью согласованы между собой.

Шаг 1: «Очистка» (англ. *cleaning*) данных, когда «шум» (не относящиеся к делу) и противоречивые данные удаляются из собранных из гетерогенных источников в ИТКС для последующего анализа. Данные для очистки поступают из реляционных, объектно-ориентированных, иерархических, мультимедийных, сетевые и иных БД, хранилищ данных и информации (объединенное физическое или логическое хранилище, организованное в рамках единой схемы в одном месте), электронных таблиц, файловых систем, внешних источников типа *Threat Intelligence* и т.д.



Рисунок 44 – Процесс получения знаний об ИБ ИТКС ОРГАНИЗАЦИИ в ЦИУСБ

Шаг 2: Объединение данных для последующего интеллектуального анализа в единую БД.

Шаг 3: Отбор данных для решения конкретной задачи ИБ-аналитики, позволяющий создать меньший по размерам объем анализируемых данных с сохранением целостности исходных данных.

Шаг 4. Преобразование в СУБД или хранилище отобранных данных или их объединение на основе определенным форматов, подходящих для ИБ-аналитики. Так, например, технология хранилищ данных включает в себя аналитическую онлайн-обработку данных (англ. *Online Analytical Processing, OLAP*), в том числе возможности для реферирования, консолидация, агрегирования, сложных аналитических расчетов, предсказаний возможных сценариев «что, если» (например, если при конкретном бюджете требуется составить прогноз) и просмотра данных с разных точек зрения. Хотя *OLAP* поддерживает многомерный анализ и принятие решений, в ЦИУСБ для ИБ-аналитики дополнительно требуются классификация и кластеризация данных, определение характеристик изменения данных с течением времени и т.д.

Шаг 5: ИБ-аналитика с применением интеллектуальных методов и средств для обнаружения и извлечения потенциально полезных данных. Например, в случае обработки потоков многоуровневый, многомерный оперативный интеллектуальный анализ выполняется на потоковых данных в режиме реального времени при локальной потоковой передаче и коллективной параллельной обработке ЖРС, сетевых потоков и т.д. Другой подход заключается в асимметричной аналитике с машинным обучением, кластерным анализом и расширенной визуализацией для нелинейного анализа от запроса к запросу по мере исследования отдельных событий и/или аномального поведения всей ИТКС, отдельных ИС, активности пользователей и т.д. Далее обнаруживаются общие закономерности и динамические изменения на низком и, что более важно, высоком уровнях абстракции для предсказания возникновения нарушений ИБ и инцидентов ИБ. Закономерности описываются в виде шаблонов (англ. *patterns*). ПО ИБ-аналитики представляет собой набор функциональных модулей для определения характеристик данных, анализа связей и корреляции, классификации и кластерного анализа, прогнозирования и анализа эволюции и т.п.

Шаг 6: Оценка полученных закономерностей и выявление среди них действительно интересных и полезных для конкретной ИТКС с использованием специальных мер проверки. Модуль оценки шаблонов, интегрированный в ПО ИБ-аналитики использует, как правило, меры и пороги «интересности» для фильтрации обнаруженных шаблонов и взаимодействует с модулями их нахождения таким образом, чтобы сфокусировать поиск именно на «интересных» с точки зрения ИБ ИТКС.

Шаг 7: В качестве заключительного этапа процесса ИБ-аналитики – представление персоналу (в частности, аналитикам) ЦИУСБ полученных знаний с помощью различных средств визуализации и подготовки отчетности. Пользовательский интерфейс выступает связующим звеном между системой ИБ-аналитики и пользователями, позволяя им взаимодействовать с системой путем задания запросов или запуска отдельных задач ИБ-аналитики, предоставляя информацию, помогающую сфокусировать поиск, выполняя «добычу» данных на основе промежуточных результатов анализа, оценки закономерностей, просмотра хранилищ данных и визуализации закономерностей в различных форматах. Примером могут служить различные информационные панели *SIEM*- [48] и *SOAR*-систем.

Использование ИБ-аналитики в работе типового ЦИУСБ именно с точки зрения ИТ больших данных может быть проиллюстрировано рис. 45 [180], где в овалах показаны данные, включая добавление контекста рассмотрения «сырых» исходных данных, а подписи курсивом относятся к действиям по обработке больших данных в ЦИУСБ.

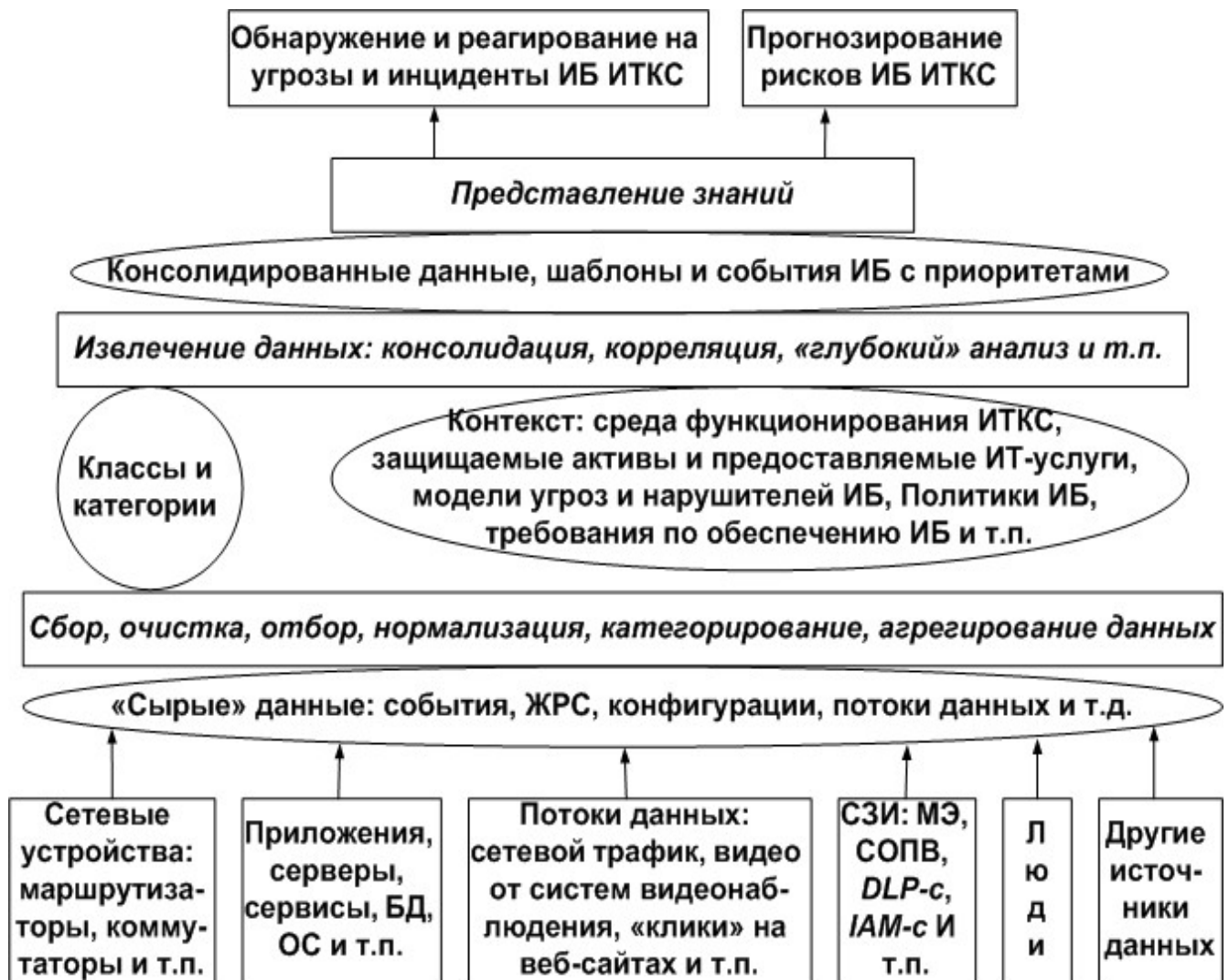


Рисунок 45 – Процесс использования ИБ-аналитики в ЦИУСБ ОРГАНИЗАЦИИ с точки зрения ИТ больших данных

Самый нижний уровень на рис. 45 – это уровень источников данных (требования к ним детально сформулированы в [15]). За ним следуют уровни сбора, обработки и хранения данных. И в верху рисунка находится уровень представления информации и знаний непосредственным их потребителям.

Рис. 42, рис. 44 и рис. 45 полностью согласуются между собой. Получаемые в результате применения ИБ-аналитики знания являются основой не только для обнаружения и реагирования на инциденты ИБ, но и выявления возникающих угроз ИБ, а также для прогнозирования рисков ИБ ИТКС ОРГАНИЗАЦИИ.

Ранее неоднократно отмечалось, что ИБ-аналитика характеризуется тем, что данные анализируются не сами по себе, а вместе, в определенном контексте. Для анализа относящихся к ИБ ИТКС данных определим следующие типы контекста и укажем примеры источников получения информации о каждом *типе контекста*:

1) *внешний*:

— среда (включая место) осуществления деятельности ОРГАНИЗАЦИИ культурная, социальная, политическая, правовая, законодательная, финансовая, технологическая, экономическая, природная и рыночная среда на международном, региональном, национальном и локальном уровне;

— ОРГАНИЗАЦИЯ во внешнем мире – основные факторы и тенденции, влияющие на цели ОРГАНИЗАЦИИ, Стратегия и Политика ОРГАНИЗАЦИИ (особенно в области использования ИКТ и обеспечения ИБ ИКТ), информация об ОРГАНИЗАЦИИ из СМИ, репутационные списки, списки бизнес-партнеров и поставщиков оборудования и услуг, договоры, другие внешние связи и т.д.

— мировые тенденции в области ИБ – источники *Threat Intelligence* (потoki с ненадежными IP-адресами, DNS-серверами, URL и т.п.);

— проход в ОРГАНИЗАЦИЮ – системы контроля физического доступа (системы видеонаблюдения, системы пропуска на территорию ОРГАНИЗАЦИИ и т.п.), местоположение, погодные условия и т.д.;

2) *внутренний*:

— организационная структура – Устав, капитал, сведения о руководстве, сведения об управлении ИТКС, подразделения, персонал, процессы принятия решений, коммуникации внутри ОРГАНИЗАЦИИ и т.д.;

— особенности ИТКС – сетевая карта ИТКС, вся информация о процессах, системах и используемых технологиях, проектная документация, описания используемых протоколов, стандарты, руководящие указания и модели, принятые организацией для ИТКС, подсистемы ИТКС, точки доступа, существующие СЗИ, и т.д.;

— данные, обрабатываемые в ИТКС – категорирование подлежащей защите информации, списки хранения данных (БД, хранилища, носители информации, в том числе бумажные), владельцы информации, схема информационных потоков ИТКС, информация о системах управления данными (англ. *Data Management Systems*) и системах электронного документооборота (англ. *Electronic Data Interchange*), пользователи, правила контроля доступа и т.д.;

— информационные активы, ИС и ИТ-услуги ИТКС – описание структуры информационного обеспечения ИТКС, реестр активов с указанием размещения, списки используемых приложений с указанием разработчиков, границы ИС, точки и каналы взаимодействия с другими ИС, владельцы и пользователи ИС и ИТ-услуг, функциональные схемы ИС и ИТ-услуг, описание автоматизированных функций, описание основных технических решений, структурная схема ИС, описание структуры комплекса технических средств ИС, другая проектная и рабочая документация на ИС и ИТ-услуги и т.д.;

— конфигурации АО и ПО ИТКС – описание структуры ПО, описание структуры АО, организационная структура поддерживающих подразделений, организационная структура пользователей, регламенты настройки и внесения изменений в настройки АО и ПО, данных из БД управления конфигурациями (англ. *Configuration Management Database, CMDB*) и т.д.;

— уязвимости элементов ИТКС – отчеты с результатами использования САЗ и систем статического (англ. *Static Application Security Testing, SAST*) и динамического (англ. *Dynamic Application Security Testing, DAST*) тестирования защищенности приложений, базы уязвимостей, аудиторские отчеты, реестр рисков ИБ, классификация актуальных для ОРГАНИЗАЦИИ уязвимостей, Модель угроз ИБ и т.д.;

— пользователи ИТКС и их бизнес-роли – Модель нарушителей ИБ, IAM-системы, сервис директорий (англ. *Active Directory*), данные учетных записей, информация отдела кадров, список ролей и полномочий, регламенты и инструкции, Политики ИБ, ЖРС DLP-систем, выгрузки по SIM-картам и корпоративным WiFi-сетям, информация из социальных сетей и т.д.

Также отметим, что при рассмотрении возникающих в ИТКС нарушений ИБ и инцидентов ИБ должны быть использованы в качестве внутреннего контекста и все ранее разработанные классификации уязвимостей, угроз ИБ, сетевых атак и инцидентов ИБ (глава 2).

Для обработки относящихся к ИБ данных в типовом ЦИУСБ предлагается использовать не просто ИТ больших данных, но более современные «озера данных» (англ. *data lakes*), или «концентраторы данных». Термин был введен в 2010 г. Дж.Диксоном (J.Dixon) [249], но иногда он пренебрежительно рассматривается как просто маркетинговый ход для распределенных систем, которые поддерживают проект с открытым исходным кодом *Hadoop*. Известен и еще один подход: «вчера́шнее единое хранилище является сегодняшним озером данных организации» [250]. **Озеро данных** – это масштабируемое хранилище огромного количества необработанных данных в исходном формате («как есть»), пока они не понадобятся, промежуточных и конечных результатов их обработки, а также система обработки, которая может принимать данные независимо от их структуры (адаптировано на основе [251]).

Озера данных, как правило, строятся для обработки больших и быстро прибывающих объемов неструктурированных данных (в отличие от хранилищ данных, обрабатывающих хорошо структурированные данные) [49, 180]. Данные в озере становятся доступным, как только они будут туда помещены (в отличие от хранилищ данных, предназначенных для медленно меняющихся данных). Для хранения данных озеро использует «плоскую» архитектуру, в которой каждый элемент данных имеет уникальный идентификатор и набор расширенных тегов метаданных (в отличие от иерархического хранилища данных с файлами и папками). Озеро не требует жесткой схемы или манипуляции данными всех форм и размеров, но требует поддержания порядка прибытия данных. Оно часто включают в себя семантическую БД – концептуальную

модель, использующую те же стандарты и технологии, которые применяются для создания интернет-гиперссылок, и добавляют уровень контекста для данных, определяющий их значение и взаимосвязи с другими данными. Для обработки данных в озере применяю динамические (а не предварительно построенные статические, как в хранилищах данных) аналитические приложения. Его можно представить как большой пул данных, объединяющий все исторические и новые данные в режиме реального/близкого к реальному времени в одном месте, в котором схемы и требования к данным не определены, пока данные не запрашиваются (используется «схема-при-чтении»). Озера данных могут комбинировать подходы *SQL* и *NoSQL*, а также возможности *OLAP* и оперативной обработки транзакций (англ. *Online Transaction Processing, OLTP*).

При необходимости озеро данных можно двумя способами разделить на три уровня:

- 1) исходные данные; ежедневно собираемые данные; данных из внешних источников;
- 2) данные, которым менее чем 6 месяцев, старые, но все еще активные данные, и архивные данные, более не используемые, но обязательно сохраняемые из-за их ценного содержания или по соответствующим требованиям.

Все выше перечисленные характеристики озер данных полностью согласуются с требованиями к типовому ЦИУСБ ОРГАНИЗАЦИИ, сформулированными в разделе 4.7 данного исследования. Озеро данных является экономически эффективным местом для проведения предварительного анализа данных, в то время как гибкое и целенаправленное структурирование данных осуществляется только тогда, когда и для чего это необходимо. «Отток» данных из озера – это проанализированные данные. Таким образом, озеро данных является ключевым компонентом ИБ-аналитики в типовом ЦИУСБ ОРГАНИЗАЦИИ.

Для самого озера, поскольку оно является единым хранилищем данных ЦИУСБ, очень важно обеспечить его эксплуатационную готовность, целостность, контроль доступа, аутентификацию и авторизацию, мониторинг и аудит, непрерывность функционирования и восстановление после аварий. Управление таким озером включает в себя среду приложений для получения и обработки данных в определенном контексте с помощью каталогизации и индексирования и для последующего расширенного управления высоко структурированными данными – метаданными, синтезированных из исходных, для ответа на вторичные запросы к ним.

При указанном подходе к построению типового ЦИУСБ используемые в нем озера данных будут обладать следующими очень важными характеристиками для поддержки относящихся к ИБ данных [49, 180]:

- масштабируемая (с ростом данных) архитектура с высокой доступностью;
- централизованное управление и соблюдение политик сохранения и удаления, идентификации устаревших данных и т.д.;
- централизованная каталогизация и индексация всех доступных данных и метаданных,

включая их источники, управление версиями, обеспечение достоверности и точности;

- поддержание взаимосвязей между данными;
- результативное управление данными, учитывающее удаление и сжатие и устраняющее дублирование;
- возможность отслеживания всех преобразований, выполняемых с данными, включая тип преобразования, время и источник поступления, кто и почему изменял их, какие версии существуют, как долго они будут полезны или актуальны и т.д.;
- единое, простое в управлении и совместно используемое хранилище данных, доступное для всех приложений (вместо создания контейнеров для нового файла и копий данных);
- такая модель данных, при которой каждый бит данных одновременно доступен в различных форматах, что не требует повторного выполнения процессов извлечения, преобразования и загрузки и что позволяет быстро передавать данные аналитику и разнородным приложениям и тем самым ускоряет поддержку рабочих процессов;
- доступ с любого устройства (блокнота, смартфона, ноутбука, рабочего стола и т.д.) для поддержки мобильных сотрудников;
- гибкая аналитика при перемещении данных в/из озера с использованием нескольких аналитических подходов и потоков обработки данных, а также единая ИБ-аналитика, основанная на очень конкретных случаях использования;
- заданный уровень качества обслуживания с надежно изолированными (но по смыслу консолидированными) исполняемыми рабочими процессами в своих зонах в рамках типового ЦИУСБ для обеспечения их защиты;
- сами данные никуда не перемещаются – обработка «идет к ним», а не наоборот;
- заложенный в саму концепцию озер «принцип минимальных привилегий» при доступе к данным, что хорошо согласуется с установленными требованиями к типовому ЦИУСБ.

В настоящее время объемы связанных с ИБ данных – это одна из проблем, но еще большая проблема – это скорость, с которой события в области ИБ ИТКС случаются. Именно поэтому большинство связанных с ИБ данных, приходящих в ЦИУСБ, можно рассматривать и как **быстрые данные** (англ. *fast data*) [252, 253], поскольку они требуют немедленной обработки для принятия соответствующих решений и активации выполнения определенных ответных действий. Следовательно, концепция быстрых (интерактивных) данных дополняет ИТ больших данных в отношении управления и обработки большого количества «летающих» данных, связанных с ИБ ИТКС.

Быстрые данные применяются в ИБ-аналитике к данным в режиме жесткого реального времени для решения той или иной задачи. Они играют важную роль в приложениях, требующих низкой латентности (ожидания, задержки), и зависят от высокой способности ввода/выво-

да. Цель анализа быстрых данных – быстро собрать (захватить) и проанализировать с применением интеллектуальных подходов структурированные и неструктурированные данные из разных источников таким образом, чтобы можно было быстро принять соответствующие меры. Быстрые данные часто приходят в системы данных в потоках и тогда нужна обработка больших потоков данных со скоростью их поступления – «на лету». Пример – это данные смарт-грид приложения, анализирующего в режиме реального времени использование электроэнергии в десятках тысяч локаций и автоматически инициирующего отключение нагрузки, чтобы сбалансировать подачу с потребностью в определенных географических районах [49, 180].

На основе выше изложенного можно сделать вывод, что в типовом ЦИУСБ ОРГАНИЗАЦИИ необходимо создать озеро (рис. 46), рассчитанное на работу с большими «сырыми» данными (они соответствуют E Voxes на рис. 42), большая часть из которых является быстрыми. «Сырые» данные с их источниками на рис. 45 и рис. 46 полностью совпадают.

Чтобы процедуры обработки не выполнять по несколько раз в озере также будут находиться и первоначально обработанные исходные данные (C Voxes) и метаданные (D Vox), полученные на основе форматирования и агрегирования «сырых» данных, и собственно результаты обработки данных после применения методов ИБ-аналитики (рис. 46). Обработанные данные как подмножество необработанных меньше по объему, чем исходные, но все же требуют специализированных инструментов и экспертных навыков для извлечения данных для анализа. Последние представлены в готовом для дальнейшего анализа формате и имеют управляемый доступ. Высокопроизводительные аналитические системы могут обеспечить интеграцию данных для анализа с ранее обработанными данными из озера и необработанными быстрыми данными, чтобы ИБ-аналитика могла осуществляться в режиме жесткого реального времени в контексте любой транзакции в ИТКС, что делает эти данные неотъемлемой частью аналитического процесса.

Озеро данных также выполняет функции K Vox – в его составе выделена база знаний.

Выработка ответного реагирования на инциденты ИБ и ведение отчетности по ИБ (R Vox) изображены на рис. 46 как блок принятия решений на основе визуализированных данных и тенденций в области ИБ в предварительно настроенных форматах.

Исследовательская аналитика предназначена для проведения первоначальных исследований необработанных данных с целью выявления закономерностей и аномалий, а также проверки гипотез и предположений с помощью сводной статистики.

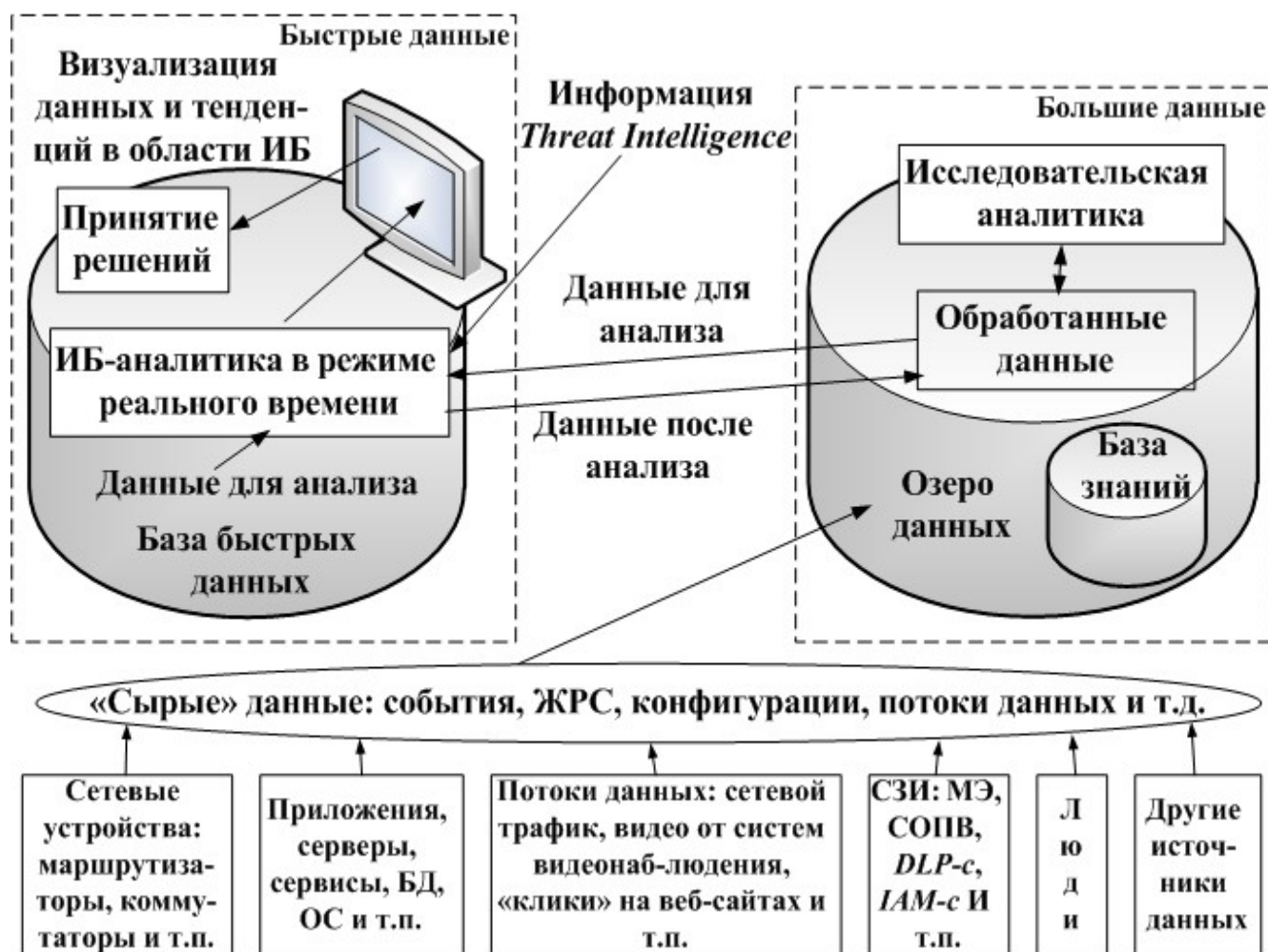


Рисунок 46 – Упрощенная архитектура обработки данных в ЦИУСБ ОРГАНИЗАЦИИ

Действия по выполнению ИБ-аналитики в режиме реального времени соответствует А Вох на рис. 42. В табл. 18 приведены результаты сравнения базовых возможностей традиционных подходов анализа относящихся к ИБ данных в ЦМБ и ИБ-аналитики в ЦИУСБ ОРГАНИЗАЦИИ, которые показывают существенные преимущества ИБ-аналитики для реализации упреждающего управления сетевой безопасностью ИТКС, имеющей в своем составе ЦИУСБ.

Архитектура обработки данных в ЦИУСБ на рис. 46 существенно упрощена и просто показывает, как большие данные могут использоваться в типовом ЦИУСБ ОРГАНИЗАЦИИ.

Организация взаимодействия с быстрыми данными отличается от таковой для больших данных «в покое» и требует систем, которые построены несколько иначе, чем традиционные БД. Ранее уже упоминались ИТ больших данных с анализом «в-памяти» и «в-БД», массивным параллельным программированием и т.п. для применения масштабируемой ИБ-аналитики. Но рассмотрение этого вопроса выходит за рамки данного исследования, поскольку в типовом ЦИУСБ должно быть внедрено типовое аппаратно-программное решение.

Таблица 18 – Сравнение традиционных подходов анализа данных в ЦМБ и ИБ-аналитики в ЦИУСБ ОРГАНИЗАЦИИ

Традиционные подходы анализа данных в ЦМБ	ИБ-аналитика в ЦИУСБ
— Использование <i>SIEM</i>-системой 1.0 для обнаружения распространенных и хорошо формализованных инцидентов ИБ правил «из коробки». — Следование при анализе логике, применяемой нарушителем ИБ на первых стадиях сетевых атак – разведка, заражение и начальное проникновение. — Выявление скомпрометированных учетных записей посредством корреляции событий. — Поиск обращений на подозрительные внешние <i>IP</i>-адреса. — Использование для выявления инцидентов ИБ информации, полученной в результате подписки на потоки <i>Threat Intelligence</i>. — Выстраивание процесса реагирования на обнаруженные инциденты ИБ внутри <i>SIEM</i>-системы на основе «сырых» событий.	— Анализ структурированных, неструктурированных и полуструктурированных данных от гетерогенных источников. — Возможность обработки быстрых данных. — Корреляция сетевых потоков, данных об уязвимостях, событий на оконечных точках, данных, собранных СЗИ, и т.п. — Максимальное устранение «шумов» в данных, подлежащих анализу. — Создание метаданных и профилей (профилирование) действий пользователей и поиск аномалий в этих действиях и данных, указывающих на инциденты ИБ. — Использование контекста (так называемая ситуативная аналитика – от англ. <i>tradeoff analytics</i>) при составлении правил корреляции и применении информации из потоков <i>Threat Intelligence</i>. — Применение «охоты за угрозами» в отношении хранимых в озере исторических данных за длительные периоды времени. — Применение интеллектуальных подходов для синтеза новых знаний с целью обнаружения ранее не выявляемых инцидентов ИБ. — Использование технологий искусственного интеллекта и естественных языков при анализе инцидентов ИБ. — Широкое использование различных возможностей визуализации информации на мониторе аналитика для выявления скрытых инцидентов ИБ и тенденций в области ИБ для разработки упреждающего управления сетевой безопасностью ИТКС.

5.4.3. Зональная архитектура обеспечения информационной безопасности в типовом- Центре интеллектуального управления сетевой безопасностью

Построение типового ЦИУСБ в виде встроенной и неотъемлемой части типовой ИТКС ОРГАНИЗАЦИИ, а также централизованной, многоуровневой системы на основе современных архитектур и решений, предполагает распределение обработки относящихся к ИБ данных с выделением зон их сбора в ИТКС и собственно обработки – первоначальной у мест сбора в ИТКС и окончательной с применением ИБ-аналитики в типовом ЦИУСБ. Для выполнения такой разнообразной и трудоемкой работы требуется надлежащая инфраструктура обеспечения собственной ИБ ЦИУСБ, которая позволяет защищенным образом собирать, нормализовывать, проводить категорирование (например, создание профилей пользователей, ежедневного запуска ПО и т.п.) и агрегирование, коррелировать, анализировать и осуществлять передачу всех связанных с ИБ данных и поддерживать предоставление соответствующих услуг санкционированным группам пользователей.

Обеспечение ИБ типового ЦИУСБ в общей постановке проблемы может быть достигнуто при взаимоувязанном решении двух задач: защиты находящихся в ЦИУСБ информационных

ресурсов и предоставляемых ИТ-услуг от внешних и внутренних угроз ИБ, и защиты внешней среды – ЕИП ОРГАНИЗАЦИИ – от угроз ИБ со стороны самого ЦИУСБ. Таким образом, возникает проблема системной увязки задач обеспечения ИБ типового ЦИУСБ с остальными задачами обеспечения ИБ ЕИП ОРГАНИЗАЦИИ. Эта проблема имеет как научно-методологические, так и организационные аспекты и в своем решении может базироваться на унификации и типизации решений для обеспечения ИБ ЦИУСБ.

Типовой ЦИУСБ ОРГАНИЗАЦИИ можно рассматривать как формальную систему, представляемую четверкой [46]: $Z = \langle R_0, R_n, K, U \rangle$, где R_0 – исходное состояние защищаемого ЦИУСБ, определяемое имеющимися в наличии исходными данными; R_n – прогнозируемое состояние ЦИУСБ, соответствующее его потенциальным возможностям противостоять угрозам ИБ; K – знания о ЦИУСБ в виде неких элементарных и сложных моделей, взаимосвязи между ними, ограничениях на отдельные параметры и т.п.; U – функция эффективности ЦИУСБ при обеспечении ИБ ИТКС ОРГАНИЗАЦИИ, соразмеряющая результативность функционирования и затраты на его обеспечение.

Принципиальным элементом разработанной методологии построения типового ЦИУСБ ОРГАНИЗАЦИИ является построение его адекватных моделей и происходящих в нем процессов. Основой решения этой проблемы может явиться обобщенная модель процессов обеспечения ИБ в ЦИУСБ ОРГАНИЗАЦИИ (рис. 47). Модель оперирует следующими параметрами [46]:

$\{K\}$ – множество показателей информационной защищенности ЦИУСБ;

$\{P^{(s)}\}$ – множество параметров внешней среды, оказывающих влияние на функционирование ЦИУСБ;

$\{R^{(s)}\}$ – множество ресурсов ЦИУСБ, участвующих в обработке защищаемой информации;

$\{P^{(m)}\}$ – множество внутренних параметров ЦИУСБ, которыми можно управлять непосредственно в процессе обработки защищаемой информации;

$\{P^{(i)}\}$ – множество внутренних параметров ЦИУСБ, не поддающихся непосредственному управлению, но поддающихся воздействию (например, в процессе реорганизации или совершенствования компонентов ЦИУСБ);

$\{S^{(m)}\}$ и $\{R^{(m)}\}$ – множества средств и ресурсов текущего управления;

$\{S^{(i)}\}$ и $\{R^{(i)}\}$ – множества средств и ресурсов воздействия;

$\{R^{(g)}\}$ – множество общих ресурсов управления.

Для решения с помощью этой модели задач анализа, то есть для определения значений показателей защищенности информации в типовом ЦИУСБ, можно использовать следующее обобщенное выражение [46]:

$$\{K\} = F[\{P^{(m)}\}, \{P^{(i)}\}, \{R^{(s)}\}, \{P^{(s)}\}].$$

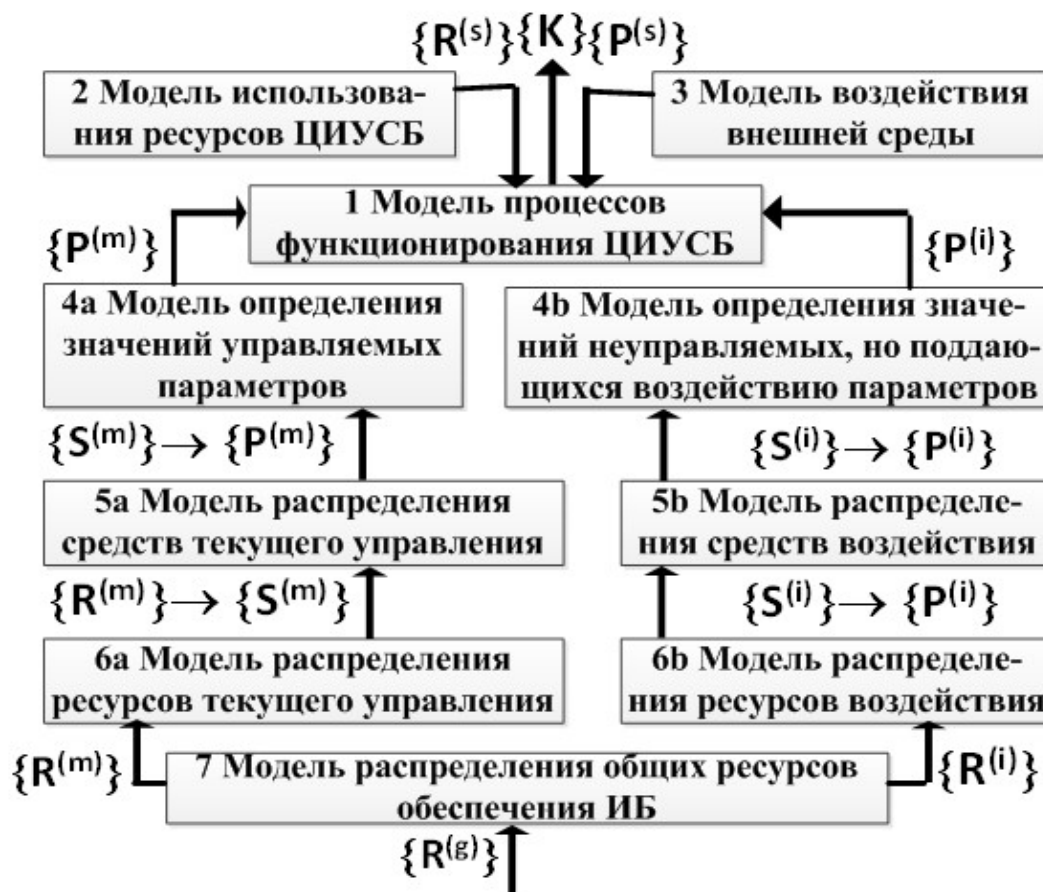


Рисунок 47 – Обобщенная модель процессов обеспечения ИБ в ЦИУСБ ОРГАНИЗАЦИИ

Задачи синтеза в общем виде могут быть представлены следующим образом [46]:

- найти такие $\{R^{(m)}\}$ и $\{R^{(i)}\}$ при $(\{R^{(m)}\} + \{R^{(i)}\} \leq \{\bar{R}^{(0)}\})$, $(\{\bar{R}^{(0)}\})$ – заданные ресурсы, чтобы при заданных $\{R^{(s)}\}$ и $\{P^{(s)}\}$ выполнялось условие $\{K\} \rightarrow \max$;
- выбрать такие $\{R^{(m)}\}$ и $\{R^{(i)}\}$, чтобы при заданных $\{R^{(s)}\}$ и $\{P^{(s)}\}$ условие $\{K\} \geq \{\bar{K}\}$, где $\{\bar{K}\}$ – заданный уровень защищенности, выполнялось при $\{R^{(o)}\} = \{R^{(m)}\} + \{R^{(i)}\} \rightarrow \min$.

Таким образом, задачи управления обеспечением ИБ в типовом ЦИУСБ сводятся к оптимизации распределения $\{R^{(m)}\}$, $\{S^{(m)}\}$, $\{R^{(i)}\}$, $\{S^{(i)}\}$.

Нетрудно видеть, что возможны следующие модификации обобщенной модели [46]:

- модель функционирования типового ЦИУСБ при отсутствии управления обеспечением ИБ (такая модель позволяет лишь определять значения показателей защищенности информации, то есть решать задачи анализа);
- модель текущего управления обеспечением ИБ, основу которого составляет оптимизация использования СЗИ, непосредственно включенных в состав типового ЦИУСБ;
- модель управления ресурсами, выделенными на обеспечение ИБ, которая дополнительно к предыдущим задачам позволяет оптимизировать процесс формирования средств текущего управления обеспечением ИБ;

- модель управления средствами воздействия на параметры, не допускающие текущего управления, но поддающиеся воздействию;
- модель управления ресурсами, выделенными на развитие типового ЦИУСБ;
- полная модель обеспечения ИБ типового ЦИУСБ, которая дополнительно ко всем возможностям, рассмотренным выше, позволяет оптимизировать использование всех ресурсов, выделенных на обеспечение его ИБ.

Результативность практического использования данной модели существенно зависит от представительности и адекватности исходных данных, позволяющих определять функциональные зависимости, устанавливающие взаимосвязи показателей защищенности информации, параметров СЗИ и размеров ресурсов, вкладываемых в реализацию процессов и мер обеспечения ИБ. Поэтому эта модель может применяться только в совокупности с неформальными методами анализа и прогнозирования [46].

Определяющими принципами разработки архитектуры обеспечения ИБ типового ЦИУСБ ОРГАНИЗАЦИИ являются изолированность его внутренних систем и сетей от типовой ИТКС и жесткая регламентация доступа с постоянным анализом ресурсов и услуг ЦИУСБ, к которым было обращение. Такой подход позволяет работать на опережение нарушителя ИБ и снижать риски ИБ до момента их реализации.

Типовой ЦИУСБ как системообразующий элемент обеспечения ИБ ОРГАНИЗАЦИИ может быть построен в соответствии с двумя возможными вариантами: как встроенный в типовую ИТКС защищенный ЦИУСБ или как отдельно размещенный, находящийся на аутсорсинге защищенный ЦИУСБ. В обоих случаях он должен быть открытым, гибким, масштабируемым и устойчивым с четко определенными, стандартизованными форматами входных и выходных данных, высокой производительностью и доступностью. И, чтобы быть по-настоящему эффективным и защищенным, он должен иметь многоуровневую защиту, постоянно контролироваться и грамотно поддерживаться, включая управление операциями, мониторинг производительности и доступности, управление соответствием применяемым требованиям и т.д. В данном исследовании был выбран первый вариант, поскольку в разделе 5.3 было указано, что рассмотрение вопросов аутсорсинга выходит за его границы.

Кроме этого, в разделе 1.1.4 было показано, что ИТКС ОРГАНИЗАЦИИ, а, значит, и ее неотъемлемая часть ЦИУСБ является средой обработки информационных активов (СОИА), которая требует системного подхода к обеспечению ее ИБ на каждом из семи уровней иерархии ее ИИ: физическом, сетевого оборудования, сетевых приложений и сервисов, ОС, СУБД (ЦОД), технологических процессов и приложений и бизнес-процессов ЦИУСБ.

Важными составляющими системного подхода к обеспечению ИБ типового ЦИУСБ также являются выработка требований по обеспечению ИБ на основе специально разработан-

ных Модели угроз ИБ и Модели нарушителей ИБ и составления реестра рисков ИБ (раздел 3.1.3) для ЦИУСБ, а также определение процедур регулярного контроля его уровня ИБ, позволяющих адекватным образом реагировать на постоянные изменения, происходящие во внешнем и внутреннем контексте функционирования ЦИУСБ (раздел 5.4.2).

При таком подходе обеспечение ИБ типового ЦИУСБ рассматривается не как некоторая надстройка к его бизнес-процессам, а как изначальный базис его построения, позволяющий сделать ИБ неременным качеством типового ЦИУСБ ОРГАНИЗАЦИИ, объективно характеризующим его способность противостоять угрозам как внешнего, так и внутреннего характера.

Постоянно помня о созданных до построения ЦИУСБ Модели угроз ИБ и Модели нарушителей ИБ для него, которые для каждого ЦИУСБ будут уникальными (именно поэтому в данном исследовании они не приводятся, но таксономия из главы 2 как раз и потребуется для их построения), к архитектуре обеспечения собственной ИБ типового ЦИУСБ целесообразно применить принцип зонирования с многоуровневой сегментацией, выполняемой МЭ (лучше, если это будут более мощные и функциональные *NGFW*). Планирование зон безопасности определяется типом данных, обрабатываемых в определенной зоне, типом доступа к этим данным и процессам, выполняемым в этой зоне.

Зоны (или контуры) безопасности ЦИУСБ – это абстрактные выделенные в инфраструктуре типового ЦИУСБ части, имеющие установленные границы и связанные между собой разрешенными потоками управляющих данных и данных об ИБ ИТКС ОРГАНИЗАЦИИ. В одной зоне (или подзоне) безопасности типового ЦИУСБ находится совокупность объектов защиты, используемая для реализации бизнес-процессов и (или) технологических процессов ЦИУСБ одинаковой степени критичности (важности), для которой применяется единая политика (режим) защиты информации (единый набор требований к обеспечению ИБ) (адаптировано на основе [144]).

Высокоуровневая схема расположения зон безопасности типового ЦИУСБ изображена на рис. 48 [236, 254]. Она включает в себя четыре зоны: демилитаризованную (полудоверенную), доверенную, запретную и управления.

Недоверенная зона представляет собой ИТКС ОРГАНИЗАЦИИ со всеми ее информационными активами, каналами связи, предоставляемыми услугами и т.д., не принадлежащими ЦИУСБ и поэтому не включенными в него. При этом недоверенная зона находится под постоянным контролем со стороны ЦИУСБ. В этой зоне могут располагаться работающие удаленно привилегированные пользователи, разработчики и администраторы ЦИУСБ, взаимодействующие с определенными для них ресурсами через защищенные протоколы типа *IPsec (IP Security)* или *VPN* с использованием протокола *SSL (SSL VPN)*.

Недоверенная зона – ИТКС ОРГАНИЗАЦИИ	
Демилитаризованная зона (ДМЗ)	Зона управления
Периметр ЦИУСБ	
Доверенная зона	
Запретная зона	

Рисунок 48 – Высокоуровневая схема расположения зон безопасности типового ЦИУСБ

Демилитаризованная (полудоверенная, или частично доверенная) зона ЦИУСБ – это находящаяся снаружи (за пределами сетевого периметра типового ЦИУСБ) физическая или логическая подсеть ЦИУСБ для внешнего сервера и услуг, которая внешне совместно используется ЦИУСБ и ИТКС ОРГАНИЗАЦИИ, а также удаленными и внутренними сервисами ЦИУСБ (такими как *DNS*, *SMTP* и т.д.). Ее цель состоит в том, чтобы отделить ЦИУСБ от недоверенной зоны ЦИУСБ и, следовательно, добавить дополнительный уровень защиты ЦИУСБ. Пользователи из недоверенной зоны имеют прямой доступ только к ДМЗ, но не к любой другой «более глубокой» части ЦИУСБ.

Доверенная зона ЦИУСБ с контролируемой средой за расположенным на границе периметра работающего в фоновом режиме (24x7) МЭ предназначена для внутренних систем типового ЦИУСБ (таких как внутренняя балансировка нагрузки, платформы тестирования устройств и устранения неполадок, сервисы приложений и управления, услуги с ограниченным доступом только для персонала ЦИУСБ и т.д.).

Системы типового ЦИУСБ с высокими рисками и критически важные функциональные системы ЦИУСБ (критические сервисы, услуги и серверы, отдельные системы хранения и ЦОД в целом для размещения озер и быстрых данных и базой знаний с определенными вычислительными мощностями и т.д.) находятся в *запретной зоне ЦИУСБ*.

Зона управления ЦИУСБ создается для всех активов ЦИУСБ, таких как инфраструктурные сервисы, центральная консоль СОВ/СПВ, управление сетевыми устройствами и трафиком с данными телеметрии, приложениями, необходимыми для поддержки в типовом ЦИУСБ централизованного функционирования, виртуализацией, настройками, изменениями, исправлениями, резервным копированием и СУИБ ЦИУСБ, в том числе централизованным в режиме реального времени логированием событий ИБ, мониторингом, отчетностью, *SIEM*-и *SOAR*-системами, инструментами ИБ-аналитики, системами проверки соответствия различным требованиям, САЗ и т.д.

В исследовании определены следующие основные преимущества выбранной зональной сегментации и управления типовым ЦИУСБ ОРГАНИЗАЦИИ [231, 236]:

— основное внимание различным основанным на частной Политике ИБ для типового ЦИУСБ процессам и мерам обеспечения ИБ критически важных активов, сервисов и услуг ЦИУСБ в зависимости от их местоположения, а также оценке рисков ИБ и предопределенным правилам запрета для всех межзонных подключений;

— постоянная готовность и доступность процессов и мер обеспечения ИБ ИТКС, предоставляемых типовым ЦИУСБ;

— строгий ролевой доступ при межзональных взаимодействиях (как для входящих, так и исходящих запросов и подключений), централизованное ведение ЖРС, мониторинг ИБ и контроль, определенные отдельно для каждой зоны, группы критических активов и конкретного актива и предоставляемых пользователям услуг через границы управляемых зон;

— специальные правила обеспечения конфиденциальности, целостности и доступности критически важных данных, хранящихся и обрабатываемых в каждой зоне;

— возможность обнаружения подозрительной активности на основе использования различных правил Политики ИБ для сенсоров сетевых СОВ/СПВ (в сетевых каналах) и агентов СОВ/СПВ (на узлах) в отдельных зонах безопасности типового ЦИУСБ;

— возможность быстрого ограничения воздействия инцидентов ИБ за счет использования расширенной ИБ-аналитики, включая обнаружение аномалий в поведении ЦИУСБ, прогнозное моделирование угроз ИБ, повышенную видимость происходящих связанных с ИБ событий, «глубокую» инспекцию сетевого трафика и его телеметрии, анализ активности пользователей при сравнении с их профилями и оценку состояния активов и услуг в каждой зоне типового ЦИУСБ;

— усложнение компрометации (взлома) типового ЦИУСБ или вирусного инфицирования между зонами путем их блокировки для предотвращения распространения дальнейших негативных воздействий;

— больше возможностей для ускорения обнаружения, расследования, реагирования и восстановления после инцидентов ИБ, не отраженных своевременно;

— все зоны безопасности логически изолированы друг от друга, но передают друг другу все необходимые данные в соответствии с утвержденными для них Политиками ИБ, правилами и регламентами обеспечения ИБ.

Далее высокоуровневая схема (рис. 48) была уточнена и детализирована. Было добавлено несколько подзон в пределах доверенной и запретной зон безопасности, которые предназначены для специальных случаев, перечисленных в рамках описания их функциональных возможностей в типовом ЦИУСБ (раздел 5.3.2) и дополнительного контроля границ подзон. Результирующий вид детализированной зональной архитектуры обеспечения ИБ типового ЦИУСБ ОРГАНИЗАЦИИ представлен на рис. 49 [254].



Рисунок 49 – Зональная архитектура обеспечения ИБ ЦИУСБ ОРГАНИЗАЦИИ

Подробнее поясним разделение ДМЗ на две подзоны, которые физически отделены от ЦИУСБ и обеспечивают дополнительную возможность защиты сетевых приложений типового ЦИУСБ.

ДМЗ 1 (ДМЗ внешней балансировки нагрузки) имеет внешний доступ к ИТКС ОРГАНИЗАЦИИ и управляет входящим трафиком ЦИУСБ на основе внешнего балансировщика нагрузки (для получения больших связанных с ИБ данных, собранных из различных внутренних источников и внешних источников *Threat Intelligence*) и его горячего резерва для обеспечения функциональной устойчивости типового ЦИУСБ после первого внешнего МЭ.

ДМЗ 2 с сервером удаленного доступа (ДМЗ удаленного доступа) имеет выделенный основной шлюз безопасности – второй со стороны внешнего мира МЭ для защиты периметра типового ЦИУСБ. Например, зашифрованный *VPN*-трафик для зоны управления ЦИУСБ от удаленного администратора ЦИУСБ должен быть расшифрован именно здесь. Никакой зашифрованный трафик не должен пересекать сетевой периметр типового ЦИУСБ. В противном случае любой вредоносный код, зашифрованный нарушителем ИБ, может пересечь периметр внутри зашифрованного туннеля.

Кроме этого, как показано на рис. 49, в ДМЗ 2 предлагается добавить «песочницу» (англ.

sandbox) [15]. Эта мера обеспечения ИБ позволит отделить поступающее извне подозрительное ненадежное ПО от непроверенных третьих лиц, пользователей, веб-сайтов и т.д. и обнаружить ранее невидимые угрозы ИБ и предупредить персонал ЦИУСБ, который может быстро принять соответствующие ответные действия [255, 256]. Приложения песочницы для ДМЗ будут поддерживать безопасную и защищенную среду, где поведение процессов, программ, памяти, файлов, пространства файловой системы, неизвестных пользователей и т.д. может внимательно и постоянно наблюдаться и контролироваться без ущерба для ресурсов ИТКС ОРГАНИЗАЦИИ.

Песочницу можно рассматривать как замкнутую среду предварительного выполнения программ или изолированный карантин (специфический пример виртуализации), используемый для тестирования и анализа непроверенных программ, которые могут содержать компьютерный вирус или другой вредоносный код или целевые атаки и которые уклоняются от традиционных средств защиты и обнаружения [254]. Исполняемый файл или документ «захватывается» и активируется в песочнице, имитирующей программную среду его функционирования и обеспечивающей более глубокий, чем САВЗ или МЭ, анализ. Потенциальные угрозы ИБ «распаковываются» и запускаются для наблюдения за их поведением без доступа к ИС, ресурсам и услугам ИТКС. Основная цель состоит в том, чтобы увидеть, вызывают ли они что-то кроме обычно ожидаемого. Возможности проверки хост-системы, чтения с устройств ввода и доступа к внутренним сетевым ресурсам в песочнице обычно запрещены или сильно ограничены.

Таким образом, песочница, используемая в типовом ЦИУСБ в качестве особо контролируемой среды, является неотъемлемым компонентом защиты типовой ИТКС ОРГАНИЗАЦИИ с обнаружением и блокированием любой вредоносной активности (например, *APT*-атак, новых вредоносных программ и атак «нулевого дня») на этапе до заражения, прежде чем нарушители ИБ начнут использовать методы уклонения от обнаружения (англ. *evasion*). В частности, она должна быть способна обнаруживать вредоносное ПО в файлах данных до их полного развертывания, наблюдая за активностью на уровне команд процессора, когда злоумышленник пытается получить незаконные привилегии их выполнения от имени ОС [256]. Плюс детальное изучение активности находящегося в песочнице хоста и потока исполняемых им действий на уровне кода сборки, прежде чем будет запущена вредоносная полезная нагрузка. И последнее, но не менее важное: песочница ЦИУСБ должна делиться всей информацией, собранной о вновь выявленных угрозах ИБ, с базой знаний типового ЦИУСБ (находящейся в запретной зоне в озере данных в ЦОД) для адаптации ЦИУСБ к ним и упреждающего управления сетевой безопасностью типовой ИТКС ОРГАНИЗАЦИИ.

Подводя итог, можно сделать вывод, что предложенный типовым ЦИУСБ с зональной архитектурой обеспечения ИБ за счет изначально примененных подходов к его построению может быть использован для результативного управления сетевой безопасностью типовой

ИТКС ОРГАНИЗАЦИИ и, в частности, для предотвращения и реагирования на инциденты ИБ в нем. Построенный таким образом типовой ЦИУСБ дает полную видимость всех областей деятельности персонала ЦИУСБ, объединяющего группы ИТ-специалистов и ИБ-персонала ОРГАНИЗАЦИИ.

Разработанная зональная архитектура типового ЦИУСБ далее дополнена применимыми мерами и средствами обеспечения ИБ, предназначенными для защиты в типовом ЦИУСБ его сетевой инфраструктуры, функций устройств, информационных ресурсов и данных, управления пользователями и т.д.

Зоны безопасности типового ЦИУСБ требуют внедрения в каждой из них соответствующих мер и средств обеспечения ИБ, включающих в себя следующие основные подсистемы:

- защита сетевого уровня (соответствующая настройка сетевого оборудования, МЭ, криптомаршрутизаторы и т.д.), включая, например, регистрацию процессов взаимодействия различных ИС ИТКС в обычных режимах и при нарушениях ИБ;

- защита от НСД (например, несанкционированного ознакомления и копирования электронных документов, изменения данных и нарушение целостности ПО) для всех элементов ЦИУСБ, включая встроенные средства обеспечения ИБ;

- защита прикладного уровня;

- криптографическая защита информации (для защиты данных и документов при передаче и в состоянии покоя (в хранилищах));

- защита телекоммуникационной сети, включая, например, контроль за функционированием всех элементов ИТКС;

- технологическая защита информации (защита на уровне технологических процессов обработки информации).

Предлагается следующий набор необходимых и достаточных для функционирования типового ЦИУСБ и его самозащиты мер и СЗИ:

- ИАМ-системы: парольная, двух- или более факторная аутентификация, биометрическая аутентификация для особых зон и подзон, включая специальные БД, списки контроля доступа к серверам и т.д.;

- средства захвата потока данных и отдельных пакетов;

- САВЗ и защита от вредоносного ПО;

- СОВ/СПВ с глубокой инспекцией пакетов (*DPI*) и сенсорами на всех критичных (особо важных) каналах связи ЦИУСБ;

- шлюзы безопасности и контроля доступа, включая МЭ (*NGFW* и т.д.) на границах зон и подзон, для управления их периметрами и исследования каждого проходящего через границы пакета для каждой сессии на скорости в режиме «жесткого» реального времени;

- средства контроля целостности файловых систем, файлов, ПО и т.п.;
- *DLP*-система, песочница и средства мониторинга содержимого;
- средства веб-фильтрации и фильтрации *URL*-адресов на основе МЭ для веб-приложений (*WAF*);
- по мере необходимости средства защиты приложений, специализированных облаков, беспроводного доступа и виртуализации;
- средства криптографической защиты информации (СКЗИ) с поддержкой инфраструктуры открытых ключей (*PKI*), электронных подписей и *VPN*, особенно при работе с большими данными, связанными с ИБ-аналитикой;
- средства непрерывного логирования и управления ЖРС;
- средства защиты оконечных точек ЦИУСБ, тестирования устройств и устранения неисправностей в них;
- средства генерации предупреждений об опасности в режиме реального времени с помощью *SIEM*- и *SOAR*-систем;
- средства управления конфигурационными настройками и изменениями;
- средства управления устранением уязвимостей и установкой обновлений безопасности, включая САЗ и системы статического и динамического тестирования защищенности приложений;
- средства балансировки нагрузки и резервные прокси-серверы;
- средства резервного копирования;
- средства оценки рисков ИБ;
- средства сбора свидетельств в цифровой форме для расследования инцидентов ИБ и т.п.

Осознавая, что при комплексном подходе к обеспечению ИБ типового ЦИУСБ ОРГАНИЗАЦИИ очень сложно четко разделить перечисленные СЗИ по зонам безопасности, поскольку многие из них должны функционировать в одно и то же время сразу в нескольких зонах, а сенсоры СОВ/СПВ по своей природе обязательно устанавливаются во всех зонах с центральной консолью на уровне управления, укажем их возможное примерное расположение следующим образом:

- ДМЗ 1 и ДМЗ 2 для пользователей и разработчиков ИТКС, персонала и контрактных работников ЦИУСБ – *IAM*-система (парольная аутентификация), САВЗ, СОВ/СПВ, *VPN*, *NGFW*, СКЗИ, ЖРС, *DLP*-система, песочница, системы статического и динамического тестирования защищенности приложений;
- Доверенная зона (низкие или средние риски ИБ) для разработчиков, персонала и контрактных работников ЦИУСБ – *IAM*-система (парольная аутентификация), САВЗ, СОВ/СПВ, *VPN*, *NGFW* на границе, *WAF*, ЖРС, СКЗИ, средства контроля целостности, средства баланси-

ровки нагрузки, средства защиты оконечных точек, средства тестирования и устранение неисправностей устройств, системы статического и динамического тестирования защищенности приложений;

— Запретная зона (высокие риски ИБ) для ограниченного круга пользователей ЦИУСБ (ИБ-аналитиков и т.п.) – *IAM*-система (двух- или более факторная аутентификация, биометрическая аутентификация для особых подзон), *SABZ*, *COB/СПВ*, *VPN*, *NGFW* на границе, ЖРС, СКЗИ, средства контроля целостности, средства защиты оконечных точек, средства оценки рисков ИБ;

— Зона управления (высокие риски ИБ) для привилегированных сетевых администраторов и администраторов ИБ и аудиторов ЦИУСБ – *IAM*-система (двух- или более факторная аутентификация, биометрическая аутентификация), *SABZ*, *VPN*, *NGFW* на границе, ЖРС, СКЗИ, средства контроля целостности, средства защиты оконечных точек, средства резервного копирования, средства захвата потока данных и отдельных пакетов, *САЗ*, системы статического и динамического тестирования защищенности приложений, средства управления конфигурационными настройками и установкой обновлений безопасности, *SIEM*- и *SOAR*-системы, средства сбора свидетельств инцидентов ИБ в цифровой форме.

В дополнение к списку СЗИ в заключении раздела приведем еще ряд существенных замечаний, касающихся мер обеспечения ИБ в типовом ЦИУСБ ОРГАНИЗАЦИИ.

Важным предложением для данного уровня, которое было внесено в [236], является разделение данных управления и данных, характеризующих ИБ типовой ИТКС ОРГАНИЗАЦИИ, что обеспечит отсутствие вмешательства со стороны второй группы данных в управление типовым ЦИУСБ и свободу управления всем ЦИУСБ от воздействия на данные второй группы, а также управление уровнями платформ и ПО в режиме реального времени и защиту от компьютерных атак.

В зональной архитектуре обеспечения ИБ типового ЦИУСБ при необходимости должны использоваться виртуальные локальные сети (англ. *Virtual Local Area Network, VLAN*), что согласуется с поддержкой работы ЦОД с большими и быстрыми данными и взаимодействия с виртуальными устройствами и хостами, реализующими виртуальные коммутаторы. Важно, чтобы отдельные виртуальные серверы ЦИУСБ, предназначенные для управления большими данными, были защищены в соответствии со всеми применимыми стандартами и документами ОРГАНИЗАЦИИ, например, для них должны быть удалены ненужные сервисы (например, *FTP*), которыми пользуются для взлома нарушители ИБ.

Также необходимо организовать своевременный процесс управления исправлениями ПО и ОС, сервисов резервного копирования и шифрования необходимых данных и документов.

Для обеспечения синхронизации всех событий в ИТКС и точности заполнения ЖРС

важна правильная установка компьютерных часов (таймера) (например, по Универсальному глобальному (по Гринвичу), местному декретному или «летнему» времени). Средства управления ЖРС и данные, содержащиеся в них, должны быть соответствующим образом защищены от возможного НСД и эксплуатационных проблем, включая невозможность отключения, неизменность типов зарегистрированных событий, запрет редактирования или удаления, а также регистрацию полного заполнения ЖРС и случаев невозможности записи событий вследствие сбоя либо случаев перезаписи новых данных поверх старых. Данные от источников в ИТКС должны немедленно по факту регистрации поступать в озеро данных типового ЦИУСБ.

Деятельность администратора, операторов и аналитиков типового ЦИУСБ должна контролироваться СОВ/СПВ, управляемой за пределами области их полномочий, и должна отражаться в отдельном журнале.

Отдельно необходимо рассмотреть проблему обеспечения ИБ больших данных, передаваемых, хранимых в озере данных и обрабатываемых в типовом ЦИУСБ ОРГАНИЗАЦИИ. Начало исследованиям этих вопросов было положено еще в конце 1990-х-начале 2000-х гг. [257-263]. Сразу оговоримся, что подробное рассмотрение данных вопросов выходит за рамки данного исследования, поскольку является темой самостоятельного крупномасштабного исследования. Далее сделаем важные замечания, касающиеся вопросов, которые требуется решить в конкретном контексте функционирования ЦИУСБ.

На оперативное принятие решений в области ИБ в первую очередь, влияет доступность больших данных [264-266]. При увеличении объемов данных вопрос усложняется, поскольку кроме самих данных необходимо работать с дополнительными параметрами, характеризующими их. Для обработки больших данных необходимы надежные инфраструктуры их хранения, ориентированные на предоставление частого доступа к данным, что порождает большое количество соответствующих операций. Передача больших данных как в ЦОД, так и внутри них предполагает достаточную пропускную способность каналов связи. К большим и быстрым данным, обрабатываемым различными приложениями в один момент времени, необходим одновременный доступ, что требует четкой координации загрузок приложениями данных с учетом выполняемых процессов извлечения и передачи и гарантией доступности данных во время выполнения запросов. Имеющиеся в настоящее время подходы и решения для выполнения защищенных вычислений хоть и устойчивы к различным компьютерным атакам, но требуют больших вычислительных затрат и специальных средств обработки больших и быстрых данных.

Обработка больших данных с обеспечением свойств конфиденциальности и целостности – также крупная проблема [264-266], особенно для принятия верных управленческих решений. Часто эту проблему необходимо рассматривать в рамках многоцелевой оптимизации, где для каждого пользователя нужно найти оптимальное решение среди двух возможных конфлик-

тующих целей: максимизация конфиденциальности (или минимизация угрозы нарушения конфиденциальности) и целостности данных или минимизация затрат, связанных с обеспечением необходимых уровней конфиденциальности и целостности. Большинство известных реализованных подходов основано на применении либо криптографических алгоритмов, либо методов преобразования или искажения данных, которые условно можно разделить на несколько видов, например, метод теории возмущений, рассматривающей конфиденциальность и целостность по отношению к информации, поступающей в ответ на запросы внешних объектов к статистическим БД, метод добавления аддитивных или мультипликативных шумов, выработанных из вероятностного распределения значений данных, и метод анонимизации данных. Использование таких методов позволяет избежать разглашения данных и нарушения их целостности, но при этом должен существовать определенный компромисс между обеспечением конфиденциальности и целостности и возможностью дальнейшего использования результата анализа данных.

После представленной детализации рис. 49 не будет расширен добавлением всех перечисленных средств, поскольку после этого он станет «нечитаемым».

5.5. Проект *SIEM*-системы 3.0 для типового Центра интеллектуального управления сетевой безопасностью

Новые передовые технологии оказывают, как правило, огромное влияние на то, как организации внедряют инновации для улучшения своих конкурентных преимуществ. С момента появления интернета технологии блокчейна были признаны одними из самых взрывных инноваций начала XXI века. Впервые они были упомянуты в 2008 г. при появлении биткоина, связанного с псевдонимом его изобретателя С.Накамото [267]. Как технологии создания проверяемых цифровых записей в настоящее время они используются в финансовых приложениях (например, для платежей, обмена валюты, денежных переводов и кошельков, торговли финансами, рынков, микросделок, инвестиции, брокерства, страхования и т.д.), а также в нефинансовых приложениях (например, управление идентификацией в электронном виде, аутентификация и авторизация, системы хранения и доставки данных в электронном виде, системы сертификации, смарт-контракты, разработка приложений, электронное голосование на выборах, управление медицинскими записями пациентов, распределение рабочей нагрузки для систем связи, компьютерные системы, которые должны соответствовать требованиям законодательства без вмешательства человека, интернет вещей и т.д.). И все же применение блокчейна наиболее оправдано при решении задач, связанных в основном с обеспечением целостности сохраняемой информации. Прежде всего это закрепление в блоках цепи последовательности транзакций в их исторической очередности и сути совершенных транзакций, которые и составляют смысловую основу

записываемой в блоке информации [44, 160, 268]. Под транзакцией в [269] понимается запись перемещения между взаимодействующими сторонами активов, например, цифровых денег, материальных ценностей и т.п., а в [270] наименьшая единица рабочего процесса, которая представляет собой одну или несколько последовательностей действий, необходимых для получения регулируемого соответствующими правилами результата.

Под **блокчейном** (англ. *blockchain*) будем понимать особый тип защищенной синхронизированной между его пользователями распределенной структуры данных – БД, которая без главного администратора и централизованного хранилища данных поддерживает постоянно расширяющийся список в виде последовательной цепочки нередактируемых блоков/записей и устанавливает правила работы с транзакциями/событиями, записываемыми в блоках и привязанными таким образом к ним (в отличие от обычных БД, в которых правила часто устанавливаются для всей БД или приложения). Такая БД совместно используется группой пользователей блокчейна – узлами (англ. *nodes*) – сущностями в блокчейн-сети (транспортном уровне блокчейн-платформы), принимающими и обрабатывающими транзакции и делящимися информацией о потенциальной транзакции. Узел либо доказывает (публичный блокчейн) или проверяет (гибридный/частный блокчейн) транзакции и затем добавляет их в блок. Узлы бывают двух типов. Майнеры (англ. *miners*) ищут в соответствующих источниках данных новые транзакции и доказывают, что транзакция законна (обоснована, реальна) для ее включения в блокчейн в составе новых блоков, используя такие доказательные средства, как доказательство выполнения работы/ресурса/состояния/активности и т.д., и предлагают их. Валидаторы (англ. *validators*) проверяют серии или отдельные транзакции на основе соответствующих средств их проверки (например, византийский алгоритм отказоустойчивости или «двойные расходы»).

Иллюстрация одного из примеров, показывающего включение блока в блокчейн, приведена на рис. 50. В блок может входить одна или более транзакций, сгруппированных по определенному правилу. Новый блок включается в блокчейн на основе одного из применяемых способов достижения консенсуса, например, большинства узлов, которые согласны с тем, что все транзакции в нем законны. Транзакции подписываются и могут быть в любое время проверены с помощью пары открытого и закрытого ключей. После включения в цепочку блок не может быть удален или изменен. Блоки связаны друг с другом (как цепь) в хронологическом порядке посредством уникальных криптографических ссылок последующего блока на предыдущий (они строятся с использованием криптографической хэш-функции). В блоках блокчейна в защищенном виде хранится общедоступная история всех транзакций в какой-либо системе, для которой создается данный блокчейн.

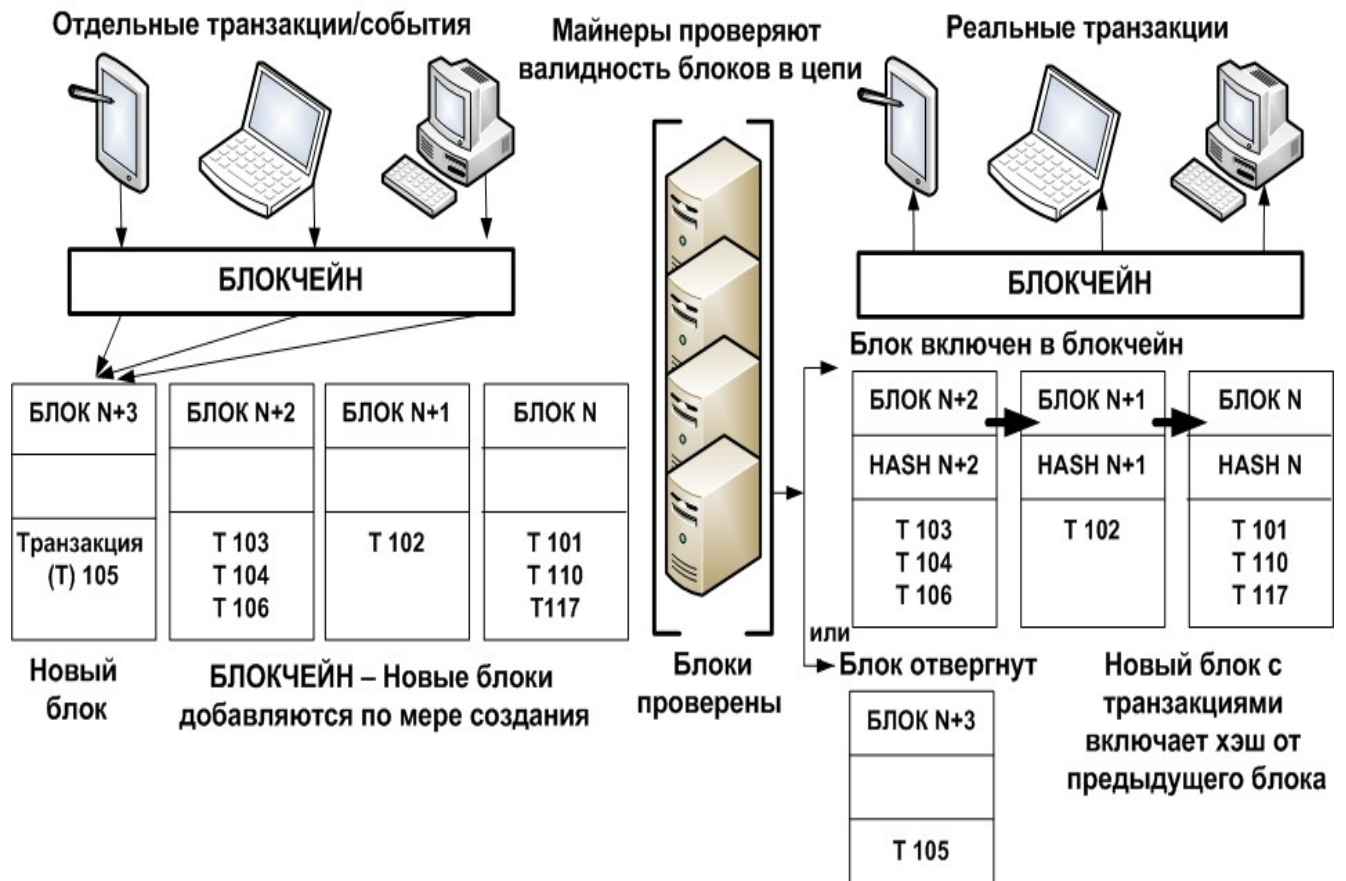


Рисунок 50 – Пример включения блока в блокчейн

Для самого блокчейна также в защищенном виде хранится история включения в него блоков. Эта история используется всеми пользователями блокчейна и является неизменной и проверяемой для записи истории транзакций, для чего используются различные протоколы. Различают четыре таких протокола: протокол транзакций, протокол для одноранговой коммуникации узлов с одинаковыми правами, протокол достижения консенсуса для обсуждения и достижения соглашения по соответствующим вопросам и протокол хранения данных для извлечения и отправки данных в БД.

В рамках диссертационного исследования для *SIEM*-системы нового поколения при ее использовании в качестве ядра типовом ЦИУСБ было предложено защищенное по своему дизайну на основе технологии частного блокчейна с разрешениями (англ. *permissioned*) средство блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ в составе *SIEM*-системы 3.0, предназначенное для обеспечения целостности этого массива. Для его создания был выбран закрытый (в рамках ОРГАНИЗАЦИИ) блокчейн, который является идеальным средством сохранения событий ИБ ИТКС, чтобы компрометация информации о них была невозможна, поскольку блокчейн записывает и выстраивает их в строго хронологическом порядке и оставляет эти цепочки событий в неизменном виде [44]. Таким образом, блокчейн в данном случае может рассматриваться как

однонаправленная (без обратной связи) структура данных (цепь) со связанным списком блоков (структурированных данных с заголовком), каждый из которых ссылается на предыдущий, используя хранимые в заголовке блока хэш-коды-указатели. Один блок с уникальным идентификатором и криптографической ссылкой на предыдущий валидный блок содержит информацию о последовательности подтвержденных и проверенных транзакций – произошедших в хронологическом порядке имеющих отношение к ИБ ИТКС ОРГАНИЗАЦИИ событий ИБ, принадлежащие к одному и тому же инциденту ИБ ИТКС (как его последовательные или параллельные стадии). Создание повторяющегося блока (его содержимое аналогично одному из предшествующих блоков) с новым идентификатором означает наличие повторяющихся событий в ИТКС, характерных, например, для *DoS*-атаки.

Все заранее определенные доверенные источники данных в виде агентов на каждом подлежащем защите объекте ИТКС ОРГАНИЗАЦИИ собирают «сырые» события, отбрасывают те, которые ни при каких обстоятельствах не могут повлиять на ИБ, и отправляют все оставшиеся отобранные подозрительные и точно относящиеся к ИБ «чистые» события в единую находящуюся в типовом ЦИУСБ централизованную БД ожидающих решения событий (БДОРС). В месте сбора «сырых» событий должно быть организовано их хранилище. Из событий из БДОРС формируются блоки, которые затем после их обработки майнерами (создают новый блок из одного или нескольких событий и упорядочивают события в блоке) и валидаторами (используя временные метки событий, принимают решение, что блок станет следующим в блокчейне, и создают его криптографическую ссылку) передаются в общий блокчейн. Затем блок распределяется по блокчейну, то есть реплицируется на все его узлы – майнеры и валидаторы (у них хранятся копии блокчейна). Существенные преимущества этого подхода состоят в том, что если один узел скомпрометирован (взломан), то остальные нет, и общий блокчейн имеет высокую степень прозрачности для углубленного анализа инцидентов ИБ, если это потребуется позднее.

В блокчейне для дополнительной защиты можно выделить специальный тип узлов, называемый «пиры». Они должны иметь информацию о всех других узлах (например, они могут сказать им, что «блок $N+1$ имеет Родительский N , имеет событие 102, его хэш-значение – $N+1$ и т.д.») и их статусе (например, выход из эксплуатации из-за взлома), а также выполняют сами операции чтения/записи в блокчейн. Пирсы осуществляют мониторинг работоспособности источников данных (агентов) в ИТКС, а также майнеров и валидаторов. Очевидно, что такая функция пиров полностью наследуется из функций, осуществляемых СОЦ. Это необходимо для функциональной устойчивости не только блокчейна, но и ЦИУСБ ОРГАНИЗАЦИИ в целом (функциональной устойчивости ЦИУСБ посвящен следующий раздел 5.6).

Создание блокчейна, содержащего только события ИБ из надежных источников данных, хорошо вписывается в технологии блокчейна. Один блок содержит одно подозрительное собы-

тие, одно событие ИБ или состоит из нескольких событий ИБ. Единый формат для записи событий ИБ в блоки может быть взят из одной из спецификаций их описания из раздела 2.5.

Примеры относящихся и не относящихся к ИБ событий на территории некоторой организации А с источниками данных о них и последующими действиями по записи информации о них в блокчейн представлены в табл. 19 [44]. Причем запись блоков с подозрительными событиями лучше всего осуществлять в «боковую» цепь (англ. *Sidechain*), из которой потом блоки можно перемещать в основную цепь (англ. *Main chain*) с «чистыми» событиями ИБ, когда это будет подтверждено. Типичные атомарные события ИБ могут быть вставлены в блок в виде отдельно хранимых повторно используемых шаблонов.

Таблица 19 – Примеры относящихся и не относящихся к ИБ событий в ОРГАНИЗАЦИИ А (начало)

<i>Тип события</i>	<i>События</i>	<i>Источники данных</i>	<i>Последующие действия</i>
Не относящееся к ИБ событие	Единичное (атомарное) событие: работник (уборщик) вошел на территорию организации	Система контроля доступа (СКД)	Блок не формируется, но событие хранится в локальной БД СКД
Не относящееся к ИБ событие	Составное событие: • сотрудник ИТ-отдела вошел на территорию организации; • сотрудник ИТ-отдела вошел в свой офис; • сотрудник ИТ-отдела включил свою рабочую станцию; • сотрудник ИТ-отдела быстро и без ошибок ввел свои учетные данные; • сотрудник ИТ-отдела запустил авторизованное приложение	• СКД; • Система видеонаблюдения (СВ); • Система контроля включения питания компьютера (ВПК); • Система управления объектами и субъектами доступа (СУОСД); • Диспетчер задач	Блок не формируется, но отдельные события хранятся в отдельных БД СКД, СВ и т.д.
Подозрительное событие	Единичное (атомарное) событие: работник (уборщик) включил рабочую станцию	ВПК	Блок формируется для передачи в боковую цепь; событие хранится в БД ВПК; в блок вставляется ссылка на исходное событие

Таблица 19 – Примеры относящихся и не относящихся к ИБ событий в ОРГАНИЗАЦИИ
(окончание)

<i>Тип события</i>	<i>События</i>	<i>Источники данных</i>	<i>Последующие действия</i>
Подозрительное событие	Составное событие: • сотрудник ИТ-отдела вошел на территорию организации; • сотрудник ИТ-отдела вошел в свой офис; • сотрудник ИТ-отдела включил свою рабочую станцию; • сотрудник ИТ-отдела быстро и без ошибок ввел свои учетные данные; • сотрудник ИТ-отдела открыл документ <i>Word</i>, сделал скриншоты на каждой странице этого документа, сохраняя каждый на флэш-накопителе	• СКД; • СВ; • ВПК; • СУОСД; • Диспетчер задач, средство записи действий пользователя (СЗДП), <i>DLP</i>-системы	Блок формируется для передачи в боковую цепь; событие хранится в БД СКД, СВ и т.д.; в блок вставляется ссылка на исходное событие
«Чистое» событие ИБ	Единичное (атомарное) событие: работник (уборщик) сделал скриншоты невыключенного экрана компьютера в отсутствие его владельца	СЗДП	Блок формируется для передачи в основную цепь; событие хранится в БД СЗДП; в блок вставляется ссылка на начальное событие ИБ
«Чистое» событие ИБ	Составное событие: • работник (уборщик) включил рабочую станцию в одном из офисов в отсутствие его пользователя; • работник (уборщик) пытался методом грубой силы подобрать пароль, пока учетная запись не была заблокирована	• ВПК; • СЗДП	Блок формируется для передачи в основную цепь через узел; отдельные события хранятся в отдельных БД СЗДП и т.д.; в блок вставляются ссылки на начальные события ИБ

Каждый блок, передаваемый в блокчейн, должен включать ссылки на все исходные «сырые» события, из которых было получено его содержимое. Все источники данных, передающие данные о событиях в БДОРС, должны быть синхронизованы друг с другом, как правило, через процесс согласования. В этом случае один и тот же инцидент ИБ может быть зафиксирован с разных точек зрения различными источниками данных. Вместо того чтобы средства обеспечения сетевой безопасности хранили и согласовывали свои собственные отдельные записи об одном и том же событии ИБ из своих отдельных, по-разному управляемых ЖРС, многие признаки одного инцидента ИБ одновременно регистрируются в режиме реального времени в блокчейне, который является общим для последующей ИБ-аналитики. Блоки с «чистыми» событиями ИБ

поступают в основную цепь, а блоки с подозрительными событиями записываются в боковую цепь для дополнительного анализа или ожидания прибытия в обе (основную и боковую цепи) блоков с событиями ИБ, которые подтвердят их статус как «чистый» инцидент ИБ. После этого блок будет перенесен в основную цепь.

Чтобы проиллюстрировать процесс формирования блока для дальнейшего включения в боковую цепь, рассмотрим, например, составное подозрительное событие из табл. 19 (строка 4) (рис. 51). Вся деятельность работника после входа на территорию организации будет записана одним или несколькими соответствующими средствами обеспечения сетевой безопасности. Эти действия будут представлены в ЖРС как отдельные необработанные события. Новый блок будет содержать все события, за исключением случаев повторного описания одного и того же события различными средствами обеспечения сетевой безопасности (последние случаи), ссылки на все источники с исходными «сырыми» данными об этих событиях (в случае, если в будущем потребуется дополнительный анализ данного события) и время совершения/фиксации события.

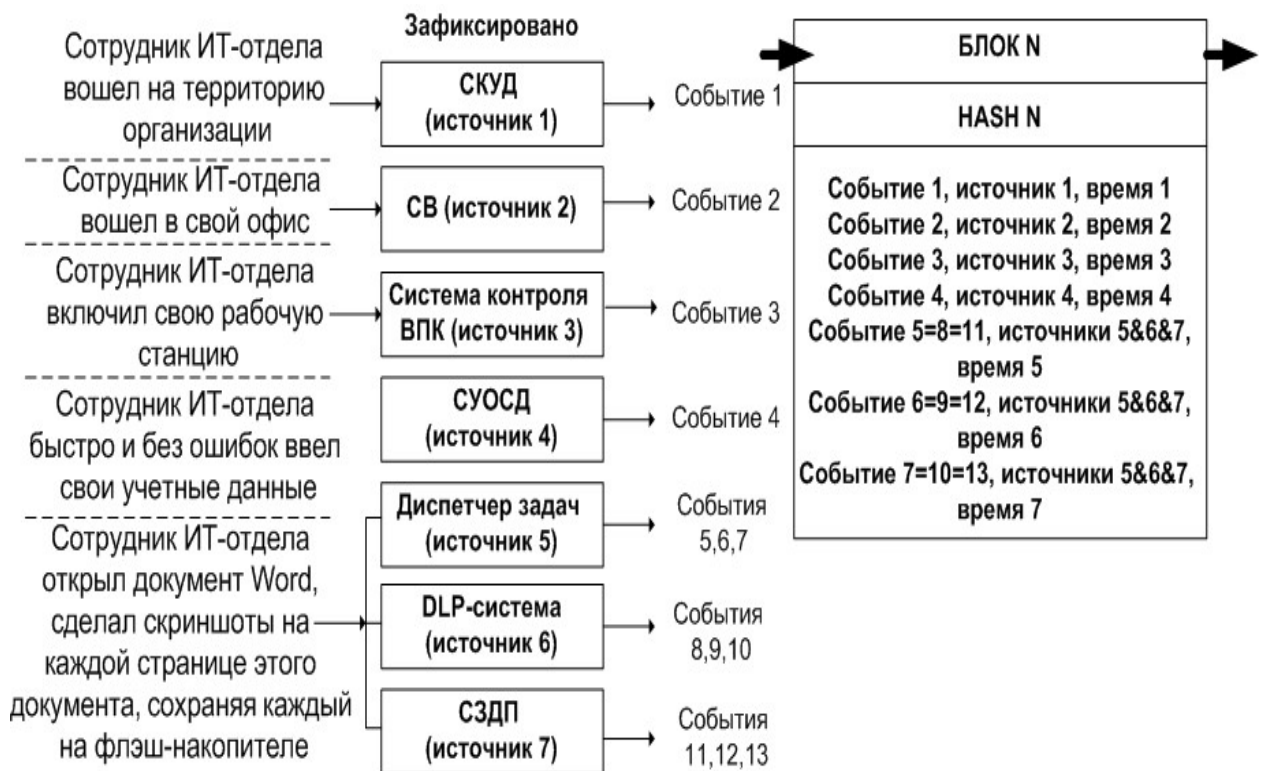


Рисунок 51 – Пример формирования блока для включения в блокчейн

Представление разработанного блокчейна как основы построения средства блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ в составе SIEM-системы 3.0 не будет полным без следующего. Поскольку блокчейн обновляется каждый раз, когда приходит новый блок о новых событиях в ИТКС ОРГАНИЗАЦИИ, его размер будет быстро расти, и система будет работать все медлен-

нее и медленнее. Предлагается сократить необходимые ресурсы и решить проблему масштабируемости блокчейна, используя идею метода свертки, которая может быть реализована на основе двух применимых подходов [160]:

1) автоматический: удаление блоков старше, чем предустановленное время жизни, например, один год или больше (чтобы иметь возможность собрать больше статистических данных об инцидентах ИБ и провести их глубокий анализ);

2) селективный: оператор/администратор блокчейна, который имеет авторизованный доступ ко всему блокчейну, вручную выполняет поиск в блокчейне «старых» событий для удаления (напомним, что данный блокчейн по своему дизайну – блокчейн с разрешениями). Устаревший блок – это блок с событиями ИБ, которые не имели никакого продолжения и не привели к какому-либо фактическому инциденту ИБ в течение длительного периода времени, например, одного года. Тогда необходимо удалить те блоки с событиями, которые, как выяснилось позднее, не связаны с инцидентами ИБ.

Полученный блокчейн можно охарактеризовать как постоянно «сворачиваемый» (усекаемый/сокращаемый/обрезаемый). Причины, почему блокчейн должен со временем быть свернут, например, таковы: истек срок жизни события ИБ, записанного в блоке (например, связанный с ним актив был ликвидирован); статус инцидента ИБ был присвоен событию, которое не было известно ранее, ошибочно; изменилась Политика ИБ ОРГАНИЗАЦИИ. Период времени, после которого необходимо сворачивать блокчейн, зависит от самой ОРГАНИЗАЦИИ, но он также тесно связан с длительностью современных атак. Конечно, этот важный вопрос требует дальнейших исследований, но в целом это время варьируется от нескольких секунд для краткосрочных атак (например, *DDoS*-атак и быстрых сканирований) до нескольких месяцев для долгосрочных атак (например, целенаправленные *APT*-атаки).

Операции свертки будут проводиться персоналом ЦИУСБ с соответствующими полномочиями чаще для боковой цепи, где изначально записываются блоки с подозрительными событиями, которые после более глубокого анализа не будут рассматриваться как части некоторых инцидентов ИБ. Прежде всего операция удаления должна гарантировать, что удаляемый блок – правильный блок, предотвращая тем самым любое несанкционированное удаление для сокрытия следов несанкционированной активности и сохраняя его для расследования и реагирования на инциденты ИБ. Затем операция удаляет из блокчейна блок, который был создан неправильно или больше не имеет ценности, и его криптографическую связь с предыдущим блоком. После этого предыдущий блок и последующий (следующий после удаленного) блок должны быть связаны между собой с использованием хэша-значения предыдущего блока. Целостность данных после удаления будет достигнута в свернутом блокчейне за счет использования ссылок на исходные события от источников данных, которые фиксируются в предыдущем бло-

ке. Этот вопрос требует отдельного детального рассмотрения, и связан он с так называемым редактируемым блокчейном (англ. *redactable blockchain*), основы которого описаны в работах компании *Accenture* [271, 272] с модифицированными «хэшами хамелеона» [273].

Предлагаемый блокчейн для распараллеливания аналитической работы должен работать на выделенной подсети серверов, защищенной традиционными мерами обеспечения сетевой безопасности, и должен автономно резервировать (создавать копии) блокчейна. Таким образом, основными преимуществами основанного на блокчейне средства в составе *SIEM*-системы 3.0 являются надежность (понимается здесь больше с точки зрения целостности) и функциональная устойчивость как способность блокчейна корректировать свою работу для поддержания операций в ожидаемых условиях и в случае эскалации требований, беспорядков и непредвиденных обстоятельств. Все это вместе доказывает, что частный блокчейн с разрешениями предоставляет надежно проверяемые наборы данных с высокой степенью уверенности (доверия) в целостности и защищенности как блокчейна в целом, а также всех его отдельных блоков и их последовательности. Но технологии блокчейна не добавляют уверенности в достоверности полученных из ИТКС «сырых» данных.

Упрощенно говоря, *SIEM*-система 3.0 с разработанным средством блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ дублирует возможности *SIEM*-системы 2.0 в части анализа данных, но при этом дополнительно структурирует результаты работы последней и сохраняет их в неизменном виде в блокчейне для последующего расследования инцидентов ИБ ИТКС ОРГАНИЗАЦИИ.

Следующие возможности блокчейна, взятые за основу построения названного средства в составе *SIEM*-системы 3.0, обеспечивают ее значительные преимущества при использовании в типовом ЦИУСБ [160, 268]:

- поддержка блокчейном возможности исследовать последствия события ИБ, которые привели к инциденту ИБ;
- записывая каждое событие, он поддерживает углубленный анализ и проверку закономерности в тысячах событий в режиме реального времени;
- блокчейн как распределенная сетевая система характеризуется интероперабельностью (функциональной совместимостью), включая возможность использования применимых международных стандартов, взаимодействия данных из всех источников (данные должны иметь одинаковые синтаксические и семантические основы, которые могут быть разработанные на основе спецификаций из раздела 2.5) и взаимодействия политик (политики и процедуры обработки данных должны быть согласованы; поэтому узлы обработки могут быть уверены, что лица, принимающие окончательные решения по совершенствованию стратегии и тактики обеспечения ИБ ИТКС ОРГАНИЗАЦИИ, будут всесторонне рассматривать всю имеющуюся информа-

цию в том виде, в каком она им требуется);

— достаточная способность быстрее регистрировать, проверять, обрабатывать и передавать в транзакции и блоки блокчейна миллиарды событий в секунду, что соизмеримо с обычными объемами, собираемыми различными источниками данных о событиях ИБ, и отвечает потребностям современного связанного сетями мира;

— данные по каждому событию ИБ доставляются в блоки блокчейна в режиме «жесткого» реального времени без каких-либо задержек. Все данные имеют отметку времени (англ. *timestamp*) и представлены в определенном структурированном формате для дальнейшей обработки;

— блокчейн обновляется автоматически каждый раз, когда происходит новое событие ИБ и формируется новый блок. Новые блоки с информацией о новых событиях ИБ отправляются в блокчейн строго по времени их возникновения, один за другим;

— возможность вставки некоторых дополнительных атрибутов (например, цели, пометки о повторяющихся событиях, состоящих из других событий, местоположение затронутого актива) во все данные, поступающие в блокчейн для «раскрашивания» блоков с событиями в соответствии с их серьезностью, что потребует дальнейшего обязательного отслеживания;

— обеспечение целостности данных при их передаче в, из и в пределах блокчейна;

— независимость блокчейна от типа и количества источников данных – например, если они заменяются новыми СЗИ или их количество увеличивается, блокчейн продолжает работать;

— обязательное подтверждение подлинности источника данных, которому стороны могут доверять (только авторизованные и проверенные источники могут не анонимно передавать собранные данные; проверка осуществляется пирами);

— запись событий в режиме реального времени (включая, например, попытки доступа к относящимся к ИБ данным, влияющие на безопасность самого блокчейна) с полной историей событий, поддерживающей прослеживаемость и прозрачность (последнее также относится к неизменяемому ведению записей для любого события, происходящее в защищаемой сети).

Построенная таким образом *SIEM*-системы 3.0 с разработанным средством полностью соответствует воплощению концепции интеллектуальной безопасности, изображенной на рис. 45. Построение этой системы еще не окончено (в конце раздела приведен список открытых вопросов, над которыми работа еще продолжается), поскольку оно ведется автором исследования самостоятельно, и поэтому система пока не реализована. Кроме этого, для реализации требуется целый штат разработчиков, как это было со всеми известными в настоящее время *SIEM*-системами (типа *Splunk*, *IBM Qradar*, *LogRhythm*). Но уже понятна методика проведения оценки результативности (производительности) *SIEM*-системы 3.0 с новым элементом с точки зрения ее цели, системных ресурсов, реализуемости, полноты, последовательности функционирования,

однозначности получаемых результатов и проверяемости. Выбраны следующие основные показатели результативности, типичные для такого рода вычислительных систем: некорректные выходы системы в виде ложных положительных и отрицательных срабатываний, способность взаимодействовать с различными типами СЗИ и обновлять классификации инцидентов ИБ, частота потребности в обслуживании и модификации, пиковые режимы работы и работа в случае временного ограничения имеющихся ресурсов, время простоя и время ожидания, время отклика, потеря данных, удовлетворенность администратора и операторов *SIEM*-системы форматом, содержанием или своевременностью вывода результатов и т.д. В соответствии с лучшими практиками будет проведена проверка способности *SIEM*-системы 3.0 с основанным на блокчейне элементом противостоять типичным атакам (например, *DoS*-атакам, попыткам стирания информации о событиях, блокированию каналов передачи информации от СЗИ, атакам на сам блокчейн и т.д.).

Методикой проверки того, что проект с разработанным средством удовлетворяет требованиям к *SIEM*-системам и функционирует согласно их ожидаемому поведению, может быть выбрана *Z*-нотация [274], предложенная Ж.-П.Абриаль (J.RAbrial) в 1977 г. и признанная в 2002 г. формальным языком спецификации описания и моделирования программ и вычислительных систем (к которым может быть отнесена и *SIEM*-система) с помощью математических обозначений, используемых в аксиоматической теории множеств. Кстати, в самом стандарте [274] приведены примеры типов систем, которые могут быть определены с помощью *Z*-нотации, включая, среди прочего, системы защиты, такие как системы обработки транзакций (это и есть по сути *SIEM*-системы).

Другая возможность – применение поддерживаемого многочисленными инструментами *B*-метода, популярного в отраслевых проектах и системных приложениях, для которых важна защита [275]. Также созданный Ж.-П.Абриаль в 1980 г., *B*-метод поддерживает точные выражения свойств с точки зрения целей проектирования, требуемых спецификациями, и моделирует системы в среде их функционирования с акцентом на код программ. *B*-метод – более низкоуровневый, чем *Z*-нотация, и представляет собой набор, включающий специальный *B*-язык, дополнительные уточнения в процессе преобразования разработанной модели в виде абстрактной спецификации в машинный код, доказательства и соответствующие инструменты. *B*-язык также имеет две возможности, которых нет в *Z*-нотации, – это проверка согласованности (гарантирует, что совершаемые машиной операции не нарушают ее функционирование) и проверка уточнения (гарантирует, что каждая машина является допустимым уточнением предыдущей машины), что имеет важное значение для применения технологии блокчейна и ПО, работающего в режиме реального времени [276]. Именно поэтому, представляется, что в дальнейшем выбор должен быть сделан в пользу *B*-метода. Его применение позволит выявить потенциальную ог-

раниченность проекта *SIEM*-системы 3.0 с новым элементом, которая в дальнейшем при общении с разработчиками ПО системы будет устранена.

Наиболее важные направления перспективных исследований в продолжение к уже полученным результатам на пути к воплощению проекта *SIEM*-системы 3.0 с разработанным средством в жизнь требуют ответа на следующие вопросы. Каковы основные критерии и принципы, согласно которым из БДОРС будут выбираться события для создания одного блока блокчейна? Каково оптимальное количество узлов в блокчейне *SIEM*-системы 3.0, что зависит от размера ИТКС ОРГАНИЗАЦИИ, предоставляемых на ее основе услуг и количества событий, происходящих в ИТКС? Где и как разместить элемент *SIEM*-системы 3.0 наиболее оптимальным образом? Как организовать потоковую ИБ-аналитику для блоков, содержащих события, происходящие в ИТКС? Как спроектировать промежуточное ПО блокчейна для средства в составе *SIEM*-системы 3.0, что позволит персоналу ЦИУСБ наиболее результативно коррелировать события ИБ для помещения их в один блок? Как визуализировать блокчейн для наиболее качественно выявления связей событий и закономерностей в совместно анализируемых новых и исторических данных? Как предсказать появление событий ИБ в будущем? Этот список вопросов можно расширять для того, чтобы проект *SIEM*-системы 3.0 стал совершеннее.

В конце раздела можно заключить, что представленный подход позволяет не просто модифицировать *SIEM*-системы, а вывести их следующее поколение на качественно новый и более высокий уровень управления событиями ИБ для ИТКС ОРГАНИЗАЦИИ в ЦИУСБ. Созданная описанным способом *SIEM*-система 3.0 с разработанным средством блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС для типового ЦИУСБ ОРГАНИЗАЦИИ защитит ее информацию от компрометации и обеспечит выполнение требований специализированных стандартов серии 27000, посвященных идентификации, сбору и/или получению из различных источников, пометке, хранению, транспортировке и сохранению свидетельств инцидентов ИБ в цифровой форме [128-130, 182, 183]. Особенно это касается получения и сохранения собранных свидетельств инцидентов ИБ в неприкосновенности для поддержания их неоспоримости при обращении в правоохранительные органы.

5.6. Функциональная устойчивость типового Центра интеллектуального управления сетевой безопасностью в едином информационном пространстве организации

Анализ концептуальных подходов к понятию «устойчивость» показывает, что существует множество определений, свидетельствующих в пользу его неоднозначности. Военные подразумевают под ним способность сохранять боеспособность, терпя потери. В толковом словаре

русского языка Д.Н.Ушакова *устойчивость* – это отвлеченное существительное к слову «устойчивый» – не поддающийся, не подверженный колебаниям и изменениям, твердый, стойкий, надежный, не поддающийся влияниям. В физике *устойчивость* материала – его физическое свойство, благодаря которому он может вернуться к своей первоначальной форме или положению после деформации, не превышающей предел его упругости. *Помехоустойчивость* устройства – его способность выполнять свои функции без ошибок в условиях воздействия помех. В теории автоматического управления *устойчивость* характеризуется реакцией динамической системы на различные неизбежные возмущения (воздействия), а *устойчивость* системы автоматического управления при воздействии на неё случайных возмущений и помех изучается теорией управления стохастическими системами. Для организаций выделяют несколько различных по своей природе видов *устойчивости*: финансовая, экономическая, производственная, технологическая, организационная, кадровая, экологическая, правовая и т.д. Обобщая эти и другие определения, *устойчивость* можно представить как способность чего-либо бесконечно долго сохранять свои свойства (структуру, состояние, рабочие параметры и т.п.) в допустимых диапазонах под влиянием неблагоприятных внешних воздействий и возвращаться в установившийся режим (исходный или близкий к нему) после отклонения в результате возмущений [277].

Устойчивость бывает статической (неизменность структуры) и динамической (неизменность поведения). Она является фундаментальным качеством всех более или менее длительно существующих систем. Тогда объект описывается как *устойчивый*, если:

— физическое или логическое воздействие на объект допустимо в течение некоторого периода времени;

— объект должен быть в состоянии продолжать достижение поставленной цели/миссии при некотором воздействии на него (непрерывность деятельности в сложной, подверженной рискам среде с различными угрозами);

— объект должен быть в состоянии за некоторый разумный срок вернуться к «нормальному» состоянию (после аварийного восстановления).

Тогда *устойчивость системы* можно определить как ее способность оставаться относительно неизменной в течение определённого периода вопреки внешним и внутренним возмущениям и возвращаться к состоянию установившегося равновесия после снятия возмущения, нарушившего это равновесие [277]. При этом *устойчивость системы* к воздействиям определяется не их характером, а структурой самой системы, и бывает двух форм: пассивная у простых систем, не способных к акту решения, и активная (надежность, отказоустойчивость, живучесть и пр.) у сложных систем, целенаправленное поведение которых основано на акте решения – выборе из альтернатив предпочтительного для них состояния – цели.

Но отождествлять *устойчивость* и *стабильность* системы нельзя, поскольку часто первая

приобретается в процессе развития системы в сторону прогресса [278]. Это не только возможность предвидеть, осуществлять мониторинг и противостоять, реагировать и восстанавливаться, но и извлекать уроки и эволюционировать [279], совершенствуясь в неблагоприятных условиях, при стрессовых ситуациях и компьютерных атаках на ресурсы, необходимые для непрерывного выполнения бизнес-процессов и доступности предоставляемых услуг.

В рамках данного исследования от типового ЦИУСБ ОРГАНИЗАЦИИ требуется не просто его устойчивость как системы, а *функциональная устойчивость ЦИУСБ* в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций) – способность типового ЦИУСБ регулировать свое функционирование в ЕИП ОРГАНИЗАЦИИ с целью поддержания выполнения его бизнес-процессов при ожидаемых условиях и в условиях ужесточения требований, нарушений и инцидентов, угроз ИБ и непредвиденных обстоятельств (адаптировано на основе [23]). Это активная форма устойчивости для динамической системы – типового ЦИУСБ ОРГАНИЗАЦИИ.

Обеспечение функциональной устойчивости типового ЦИУСБ должно поддерживаться сохранением непрерывности его бизнес-процессов и их части в виде отдельных бизнес-операций и доступности ИТ-услуг и ресурсов пользователям, даже в условиях предсказуемой заранее деградации инфраструктуры и функциональных процессов, в том числе при воздействии различных дестабилизирующих воздействий и отказов внутри самого ЦИУСБ. Логически продолжая эту мысль, функциональную устойчивость типового ЦИУСБ можно рассматривать как такую его способность, при которой уровень риска нарушения функционирования и уровень риска доступности ИТ-услуг и ресурсов предсказуемы и приемлемы как для их пользователя, так и владельца. Причем, эта способность должна быть изначально встроены в проект типового ЦИУСБ, а не добавлена в виде отдельных функции, а все нарушения ИБ и инциденты ИБ должны быть контролируемые.

Функциональная устойчивость типового ЦИУСБ в ЕИП ОРГАНИЗАЦИИ после прекращения действия возмущения должна проявляться в двух режимах функционирования (адаптировано на основе [280]):

1) «в малом», когда с течением времени достаточно малое отклонение режима работы от исходного (установившегося) уменьшается и функционирование ЦИУСБ возвращается в исходное состояние;

2) «в большом», когда после прекращения действия возмущения при достаточно большом начальном отклонении функционирование ЦИУСБ возвращается в исходное состояние.

Управление функциональной устойчивостью типового ЦИУСБ как неотъемлемая часть всего процесса управления ЦИУСБ должно учитывать, что для достижения поставленной цели

его функционирования во время и после воздействия инцидента ИБ может потребоваться смена значений параметров, относящихся ко всем его бизнес-процессам (в отличие от частного случая управления – регулирования, заключающегося лишь в поддержании определенных параметров системы в заданных пределах).

В общем случае управление функциональной устойчивостью типового ЦИУСБ ОРГАНИЗАЦИИ базируется на управлении ИТ-операциями и предоставлением ИТ-услуг, управлении непрерывностью функционирования, управлении собственной ИБ ЦИУСБ и других составляющих этого процесса, например, управлении финансами, персоналом, коммуникациями и осведомленностью (рис. 52).



Рисунок 52 – Составляющие процесса управления функциональной устойчивостью типового ЦИУСБ ОРГАНИЗАЦИИ

Управление ИТ-операциями, непрерывностью функционирования и ИБ – это дополняющие и взаимодействующие между собой процессы, ориентированные на управление операционными рисками ЦИУСБ, и имеющие одну общую цель – улучшать и поддерживать функциональную устойчивость типового ЦИУСБ. При этом **риск нарушения функционирования ЦИУСБ, или операционный риск** (англ. *operational risk*), это риск убытка ОРГАНИЗАЦИИ в результате неадекватных или ошибочных внутренних процессов ЦИУСБ, действий его работников и систем или внешних событий (адаптировано на основе [281]). Одной из основных составляющих ИТКС, а, следовательно, и ЦИУСБ, является информационная составляющая (раздел 1.1.3). Следовательно, значительная часть операционных рисков типового ЦИУСБ, включая риск прерывания его деятельности, связана с информацией, а уровень и условия проявления этих рисков во многом определяются качеством ИТ-услуг (по подготовке, обработке, передаче, хранению и отображению информации), которые могут быть предоставлены с использованием ИКТ.

Непрерывность функционирования ЦИУСБ в ЕИП ОРГАНИЗАЦИИ – это стратегическая и тактическая способность типового ЦИУСБ планировать свою работу в случае инци-

дентов ИБ и нарушений его функционирования, направленная на обеспечение непрерывности бизнес-процессов на установленном приемлемом уровне. Логически продолжая приведенное определение, примем, что обеспечение непрерывности функционирования типового ЦИУСБ в ЕИП ОРГАНИЗАЦИИ будет являться обеспечением такой стратегической и тактической способности этой системы, предполагающее долгосрочное существование ЦИУСБ в ЕИП. В свою очередь управление непрерывностью функционирования типового ЦИУСБ в ЕИП является целостным системным процессом управления, предусматривающим идентификацию потенциальных нарушений ИБ и инцидентов ИБ и их воздействия на функционирование типового ЦИУСБ для принятия обоснованных решений по сохранению его бизнес-процессов. Такой вид управления создает основу для повышения функциональной устойчивости типового ЦИУСБ и направлен на реализацию таких типовых ответных мер против инцидентов ИБ, которые обеспечивают защиту функционирования ЦИУСБ. Тогда непрерывность функционирования типового ЦИУСБ в ЕИП ОРГАНИЗАЦИИ также можно определить как способность ЦИУСБ сохранять надежность его ресурсов, обеспечивающих непрерывность бизнес-процессов и доступность ИТ-услуг и самой информации пользователям, даже в условиях деградации инфраструктуры и функциональных процессов ЦИУСБ, в том числе при воздействии различных нарушений ИБ и инцидентов ИБ (адаптировано на основе [282]).

Пользователь при обращении к необходимым ему ресурсам и услугам ЦИУСБ в рамках своих полномочий должен получить доступ за приемлемое для него время. Для этого типовой ЦИУСБ для типовой ИТКС ОРГАНИЗАЦИИ должна быть системой высокой доступности (англ. *high availability*), что подразумевает обеспечение для нее повышенной отказоустойчивости (способности сохранять работоспособность при случайных выходах из строя или сбоях отдельных элементов ЦИУСБ), катастрофоустойчивости (способности ЦИУСБ сохранять критически важные ресурсы и продолжать выполнение своих функций, возможно с определенными ограничениями, в условиях деградации его архитектуры, вызванной уничтожением элементов и связей между ними в результате стихийных бедствий, техногенных аварий и катастроф, целенаправленного воздействия людей или групп людей) и достаточной информационной защищенности (определена в разделе 1.2.2) на заданную перспективу. Высокая доступность означает способность ЦИУСБ работать при существующих нагрузках и при их увеличении, а также противостоять отказам, вызванных, в том числе, уничтожением его компонентов и связей между ними, а уровень доступности обычно измеряется «девятками». Система высокой доступности с максимальным уровнем доступности, равным 99,999 %, допускает пять минут простоя в год и предназначена для практически бесперебойного предоставления ИТ-услуг. ОРГАНИЗАЦИЯ должна самостоятельно определить уровень доступности для своего ЦИУСБ.

Из рис. 52 ясно видно, что эффективность и результативность управления функциональ-

ной устойчивостью типового ЦИУСБ ОРГАНИЗАЦИИ напрямую зависит от процессов управления непрерывностью функционирования ЦИУСБ в ЕИП и управления его ИБ на основе СОИБ. Причем на рис. 52 эти два процесса показаны как независимые, хотя в реальности они могут пересекаться, поскольку некоторые угрозы и риски управления непрерывностью функционирования и управления ИБ могут быть одними и теми же. На основе проведенного анализа одинаковых рисков могут быть выработаны похожие требования к обеспечению непрерывности функционирования и ИБ, а в дальнейшем выбраны одинаковые процессы и меры обеспечения ИБ для похожих рисков.

В общем случае процесс управления непрерывностью функционирования типового ЦИУСБ ОРГАНИЗАЦИИ в ее ЕИП можно разделить на два генеральных направления его реализации (по аналогии с [106]):

- 1) обеспечение функциональной устойчивости ЦИУСБ и его бизнес-процессов, в результате чего происходит снижение вероятности наступления рискованных событий (инцидентов, нарушений, отказов и т.п.) на основе разработки и внедрения превентивных антикризисных мероприятий;

- 2) восстановление (продолжение) функционирования ЦИУСБ, включая бизнес-процессы, отдельные операции и ресурсы, после рискованных событий с последующей минимизацией и корректировкой их негативного влияния, если они уже произошли.

Наглядно процесс восстановления функциональной устойчивости типового ЦИУСБ после инцидента ИБ можно представить рис. 53. Важно заметить, что после инцидента ИБ не всегда сразу происходит резкое прекращение осуществления бизнес-процессов (как на рис. 53), поскольку он может порождать не только прямые, но и косвенные убытки.

Простейшими мерами обеспечения функциональной устойчивости типового ЦИУСБ являются разработка Плана обеспечения непрерывности функционирования, применение генераторов для резервного питания, использование более долговечных строительных материалов и т.п.

Система управления функциональной устойчивостью типового ЦИУСБ ОРГАНИЗАЦИИ предназначена для всесторонней поддержки соответствующего процесса управления и включает План и Программу управления, сам процесс, процедуры и практики управления, а также весь задействованный в этом процессе персонал (рис. 54) [277].

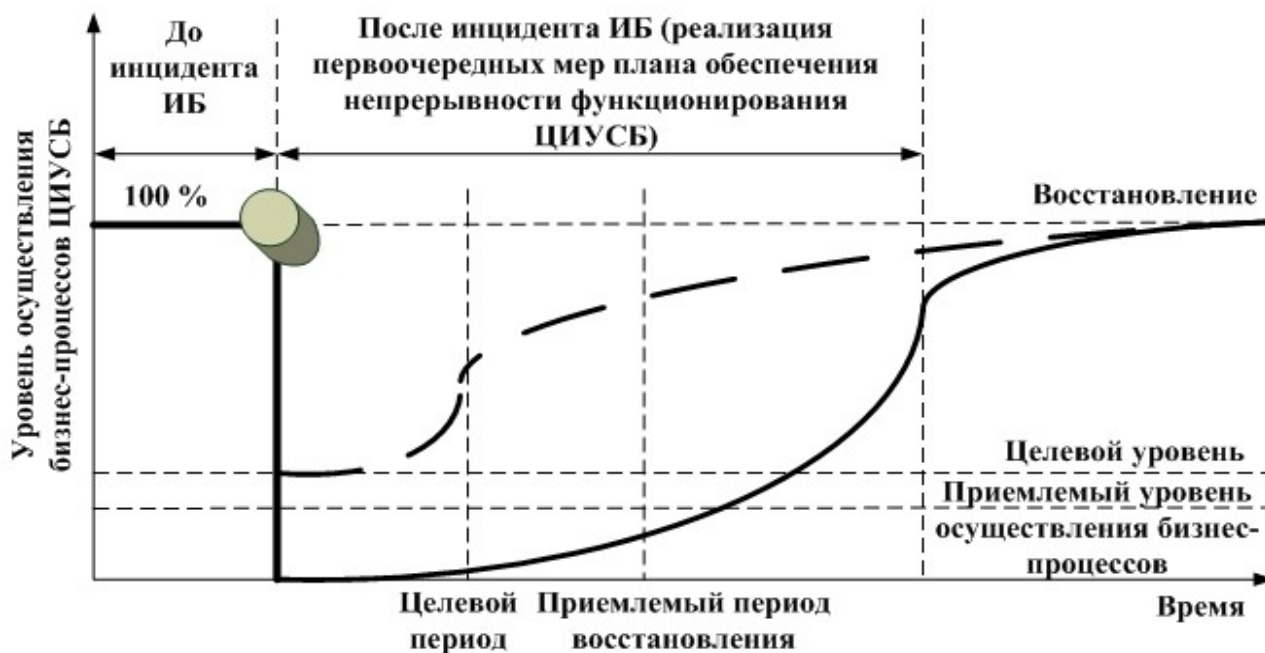


Рисунок 53 – Процесс восстановления функциональной устойчивости типового ЦИУСБ ОРГАНИЗАЦИИ после инцидента ИБ



Рисунок 54 – Основные элементы системы управления функциональной устойчивостью типового ЦИУСБ ОРГАНИЗАЦИИ

При эффективной реализации этой системы она способствует следующему:

- постоянному совершенствованию устойчивого функционирования ЦИУСБ и обеспечению стабильности в достижении его основных бизнес-целей;
- предоставлению отработанного метода восстановления способности ЦИУСБ предоставлять ресурсы и ИТ-услуги на установленном уровне в пределах согласованного времени после нарушения функционирования;
- обеспечению верифицируемой способности ЦИУСБ управлять нарушениями функционирования и защищать свои бизнес-процессы.

Таким образом, процесс управления функциональной устойчивостью типового ЦИУСБ в ЕИП ОРГАНИЗАЦИИ как комплексный процесс управления включает в себя, но не ограничивается, следующими основными мероприятиями:

- создание в рамках ЦИУСБ централизованной системы управления функциональной

устойчивостью, которая должна быть согласована с аналогичной системой и общей стратегией высшего уровня – для всей ОРГАНИЗАЦИИ в целом;

- соблюдение требований законодательства, нормативных и правовых актов, ведомственных и иных документов, регулирующих данные вопросы;

- идентификация, оценка и ранжирование по различным критериям рисков ИБ, с которыми может столкнуться ЦИУСБ с точки зрения вероятности возникновения, масштабов и вероятности возникновения последствий в краткосрочной и долгосрочной перспективах, включая выявление и присваивание приоритетов критически важным бизнес-процессам;

- выявление всех активов, вовлеченных в критически важные бизнес-процессы, и их ценности для устойчивого функционирования ЦИУСБ;

- выбор наиболее надежных ИКТ, способов и средств обработки информации, соответствующих бизнес-целям ЦИУСБ;

- выявление и исследование возможности реализации дополнительных к уже имеющимся предупреждающих и снижающих последствия нарушений ИБ и инцидентов ИБ процессов и мер обеспечения ИБ;

- определение достаточных финансовых, организационных, технических, людских и иных ресурсов, учитывающих требования по обеспечению функциональной устойчивости и способных обеспечить их на практике;

- выработка соответствующих планов, учитывающих эти требования, а также регулярное обновление и испытание реализованных/планируемых к реализации планов и процесса обеспечения функциональной устойчивости ЦИУСБ;

- установление ответственности за процесс обеспечения функциональной устойчивости ЦИУСБ;

- разработка процедур и форматов обмена информацией, касающейся прерывания функционирования ЦИУСБ;

- разработка системы оценки уровня функциональной устойчивости и восстановления ЦИУСБ после нарушений ИБ и инцидентов ИБ, являющейся основой получения результатов для совершенствования и эволюционирования ЦИУСБ за счет поддержки стратегических решений, наблюдения за тактикой и обеспечение его функциональной устойчивости.

Последний аспект особенно важен и требует отдельной проработки, поскольку типовой ЦИУСБ — достаточно сложная система, качество работы которой оценить не так-то просто. Подходить к оценке «в лоб» нерационально: при повышении качества обнаружения в ЦИУСБ количество обнаруженных инцидентов ИБ становится больше, поскольку раньше часть из них просто не была выявлена. Аналитики ЦИУСБ получают более совершенные и реализующие сложные аналитические методы инструменты, за счет чего среднее время расследования слож-

ного инцидента ИБ может возрастать. Но вместе с тем существенно возрастает и качество реализации всего ПУИИБ для ИТКС ОРГАНИЗАЦИИ.

При разработке системы оценок функциональной устойчивости для типового ЦИУСБ необходимо базироваться на следующих понятиях, выведенных на основе [176]:

— Атрибут – свойство или характеристика функциональной устойчивости ЦИУСБ, которые могут быть определены количественно или качественно вручную или автоматизированными средствами;

— Единица измерения – конкретная величина, определенная и принятая по соглашению, с которой сравниваются другие величины того же вида, чтобы выразить их значение относительно данной величины;

— Шкала – упорядоченная совокупность значений, непрерывная или дискретная, или совокупность категорий, на которые отображается атрибут меры измерения. Для каждой шкалы используются свои единицы измерения;

— Мера измерения – переменная, которой присваивается некоторое значение, полученное в результате измерения;

— Показатель (индикатор) функциональной устойчивости типового ЦИУСБ – мера измерения, дающая качественную или количественную оценку особых атрибутов – свойств или характеристик функциональной устойчивости ЦИУСБ, выведенных на основе аналитической модели относительно определенной информационной потребности. Показатели функциональной устойчивости ЦИУСБ являются основой для анализа и принятия решений по корректировке текущего уровня функциональной устойчивости ЦИУСБ;

— Метрика показателя функциональной устойчивости типового ЦИУСБ: количественное значение показателя функциональной устойчивости ЦИУСБ, полученное в результате применения метода измерения (логической последовательность операций оценки свойств и процессов функционирования ЦИУСБ относительно заданной шкалы) к объектам измерения.

В табл. 20 представлен начальный набор показателей функциональной устойчивости типового ЦИУСБ за принятый отчетный период (неделю, месяц, квартал или год) с указанием одного из трех классов – управленческие (У), организационные (О) и технические (Т), к которым они могут быть отнесены [171]. По мере совершенствования деятельности ОРГАНИЗАЦИИ по проведению оценок уровня функциональной устойчивости ее ЦИУСБ этот набор будет расширяться.

Таблица 20 – Начальный набор показателей функциональной устойчивости типового ЦИУСБ за принятый отчетный период

Функция ЦИУСБ	Ожидаемый обобщенный результат оценки	Показатели функциональной устойчивости ЦИУСБ за принятый отчетный период
Управление инцидентами ИБ	Насколько хорошо обнаруживаются, правильно идентифицируются, обрабатываются и устраняются последствия инцидентов ИБ.	Стоимость инцидента ИБ (У). Средняя стоимость инцидента ИБ (У). Средняя стоимость восстановления после инцидента ИБ (О). Среднее время до выявления инцидента ИБ (О). Количество инцидентов ИБ (Т). Среднее время между инцидентами ИБ (О). Среднее время восстановления после инцидента ИБ (О).
Управление уязвимостями	Насколько хорошо выявляются уязвимости посредством идентификации и устранения известных уязвимостей.	Зона действия сканеров анализа защищенности (Т). Процент систем, в которых нет известных серьезных уязвимостей (У). Среднее время устранения уязвимостей (О). Количество известных уязвимостей (Т). Средняя стоимость устранения уязвимости (О).
Управление обновлениями	Насколько хорошо удается поддерживать постоянное обновление систем.	Соблюдение политики установки обновлений (У). Зона действия установки обновлений (Т). Среднее время до обновления (О). Средняя стоимость обновления (О).
Управление конфигурациями	Каково состояние конфигураций систем организации.	Процент верных конфигураций (У). Зона действия управления конфигурациями (Т). Текущие настройки на отражение вредоносных кодов (Т).
Управление изменениями	Как изменения в конфигурациях систем влияют на ИБ организации.	Среднее время внесения изменений (О). Процент изменений с анализом ИБ (У). Процент изменений с исключениями ИБ (О).
Защита приложений	Можно ли положиться на защищенность используемых для осуществления деятельности в организации приложений.	Количество приложений (Т). Процент критичных приложений (Т). Зона действия оценки рисков ИБ (Т). Зона действия тестов по обеспечению ИБ (Т).
Финансы	Каков уровень и цели затрат на обеспечение ИБ.	Затраты на ИБ в процентном отношении к затратам на ИТ (У). Бюджетные ассигнования на ИБ (О).

На примере управления инцидентами ИБ в самом ЦИУСБ покажем, как можно рассчитывать указанные в таблице показатели.

— Стоимость инцидента ИБ, которая складывается из прямых потерь (стоимость уничтоженных активов и Т.П.) – ПП; стоимости простоя ЦИУСБ (стоимость возмещения расходов для бизнес-операций и стоимость потерь для ОРГАНИЗАЦИИ, непосредственно связанных с инцидентами ИБ в ЦИУСБ) – СП; стоимости удержания (усилия и стоимость; консультационные услуги) – СУ; стоимости восстановления (стоимость исследования и анализа инцидента ИБ; усилия, необходимые для восстановления и замены АО, ИС, ПО ЦИУСБ; стоимость замены перечисленного, консультационные услуги по замене или исследованию) – СЗ; и стоимости возмещения убытков (штрафы и другие денежные средства, выплачиваемые из-за нарушения контрактов или *SLA* ОРГАНИЗАЦИИ, возникших в результате инцидента ИБ в ЦИУСБ; стои-

мость непредоставления клиентам ИТКС услуг в результате инцидента ИБ в ЦИУСБ; стоимость связей с общественностью; стоимость раскрытия и уведомления; судебные издержки, штрафы и выплаты) – СВУ:

$$\text{ССИ} = \frac{\sum (\text{ПП} + \text{СП} + \text{СУ} + \text{СЗ} + \text{СВУ})}{\text{Общее количество инцидентов ИБ}}$$

— Средняя стоимость восстановления функциональной устойчивости ЦИУСБ после инцидента ИБ, которая равна усредненной по всем инцидентам ИБ суммарной стоимости:

$$\text{ССВПИ} = \frac{\sum (\text{Стоимость\_восстановления})}{\text{Общее количество инцидентов ИБ}}$$

— Среднее время до выявления инцидента ИБ за принятый отчетный период, которое должно с течением времени снижаться:

$$\text{СВВИ} = \frac{\sum (\text{Дата\_обнаружения} - \text{Дата\_происшествия})}{\text{Общее количество инцидентов ИБ}}$$

— Среднее время между инцидентами ИБ за принятый отчетный период, которое должно с течением времени увеличиваться и зависит от усредненного по количеству инцидентов ИБ суммарному времени между всеми двумя произошедшими друг за другом инцидентами ИБ:

$$\text{СВМИ} = \frac{\sum (\text{Дата\_происшествия}_n - \text{Дата\_происшествия}_{n-1})}{\text{Общее количество инцидентов ИБ}}$$

— Среднее время восстановления после инцидента ИБ за принятый отчетный период, которое должно с течением времени уменьшаться и зависит от усредненного по всем инцидентам ИБ суммарного временного интервала между датами всех происшествий и восстановлений после них:

$$\text{СВВПИ} = \frac{\sum (\text{Дата\_восстановления} - \text{Дата\_происшествия})}{\text{Общее количество инцидентов ИБ}}$$

Аналогичные формулы можно вывести и для других показателей и составить перечень атрибутов для них.

Данный раздел был бы не полон, если бы в нем не были упомянуты термин «киберустойчивость» (англ. *cyber resilience*) и соответствующие показатели киберустойчивости, которым в настоящее время посвящено множество публикаций. Комментарии по поводу приставки «кибер» в этом исследовании уже приводились (раздел 1.2.5) – главное, что здесь требуется повторить, это то, что кибербезопасность – это безопасность в киберпространстве. Отсюда следует несложный вывод, что киберустойчивость – это устойчивость в киберпространстве.

Разработкой показателей киберустойчивости и функциональной устойчивости занимались многие, например, *CERT* [283] (представлены списки показателей, разделенных по 26 процессам, таким как управление доступом, соответствие требованиям, управление мерами обес-

печения ИБ, управление персоналом, управление инцидентами, управление информацией и знаниями и т.п.), *ENISA* [284] (показатели устойчивости рассматриваются в двух областях – с точки зрения инцидентов (готовность к ним, предоставление услуг и восстановление) и с точки зрения обеспечения надежности, безопасности и работоспособности), *MITRE* [285] (показатели разделены по процессам – предотвращение/избежание, подготовка, продолжение, ограничение, восстановление, понимание, преобразование, реорганизация) и многие другие. Все разработанные этими организациями показатели могут быть пересмотрены применительно к функциональной устойчивости ЦИУСБ, поскольку показатели киберустойчивости – это лишь подмножество показателей более общей функциональной устойчивости ЦИУСБ ОРГАНИЗАЦИИ.

5.7. Вопросы кадрового обеспечения типового Центра интеллектуального управления сетевой безопасностью

В типовой ЦИУСБ, как ранее отмечалось в разделе 4.3.1 для ЦМБ, с организационной точки зрения должен входить персонал, состоящий в основном (без учета руководства ЦИУСБ) из операторов, работающих с текущими данными, и ИБ-аналитиков, которые выполняют их углубленный анализ и осуществляют «охоту за угрозами». Штат ЦИУСБ зависит от многих факторов, например, размера и сложности ИТКС ОРГАНИЗАЦИИ, количества ранее обнаруживаемых инцидентов ИБ, организационной модели ЦИУСБ, режима работы персонала, уровня автоматизации его деятельности, конечно, готовности ОРГАНИЗАЦИИ выделять соответствующий бюджет на поддержку функционирования своего ЦИУСБ. Вопросы, связанные с численностью штата ЦИУСБ, умышленно выведены из области данного исследования, посвященного более научным и концептуальным аспектам построения типового ЦИУСБ. Здесь основной акцент делается на профессиональную подготовку персонала, его компетенции.

Персонал типового ЦИУСБ по выполняемым ими функциям можно разделить на несколько групп, называемых в англоязычных публикациях «линиями» (англ. *tier*) [190]. Как показал анализ, обычно это четыре линии.

Операторы первой линии непрерывно контролируют всю входящую информацию и процессы ее регистрации, следят за очередью предупреждений об опасности, генерируемых СЗИ и другими системам типа *SIEM*-систем, и определяют срочность каждого предупреждения, а также производят оперативную несложную обработку той части информации, которая не может быть по каким-либо причинам обработана в автоматизированном режиме. Этот персонал также отслеживает работоспособность источников данных о событиях ИБ – сетевых сенсоров и агентов на конечных точках. Для этого в общем потоке всех собранных гетерогенными источниками данных, относящихся к событиям ИБ или предположительно связанным с ИБ, в соответст-

вии с установленными политиками и правилами выделяются те данные, которые свидетельствуют об инциденте ИБ. Глубокий анализ событий ИБ они не осуществляют и в своих действиях опираются на заранее разработанные сценарии реагирования (*playbooks*) – последовательность оперативных действий при обнаружении конкретного типа инцидента ИБ. Если на обработку события уходит более нескольких минут, то они передают (эскалируют) его на вторую линию – операторам более высокого уровня. Туда же оперативно – строго в течении установленного периода времени (например, 15 минут) – передаются сведения об инцидентах ИБ, для которых определен высокий уровень критичности. Также операторы первой линии могут управлять СЗИ и регулярно готовить отчеты. Поскольку их работа требует особого внимания и быстрой реакции, они работают посменно. Важное замечание – информация о подозрительных событиях должна передавать не только специалистам второй линии, но и между сменами, поскольку существует множество компьютерных атак, которые развивают часами, днями, а иногда и годами (как в случае с *APT*-атаками).

У операторов второй линии обычно больше опыта, поэтому они могут быстро найти причину обнаруженной проблемы, используя корреляционный анализ данных, полученных из различных источников, и оценить, какая часть ИТКС ОРГАНИЗАЦИИ подвергается компьютерной атаке. Они строго следуют разработанным процедурам по устранению этой проблемы и ее последствий (для них разработаны свои варианты *playbooks* – последовательность оперативных действий при реагировании на конкретный тип инцидента ИБ). Если это не удастся и причина проблемы не установлена, тогда они передают ее для дополнительного расследования на третью линию. Операторы второй линии способны обеспечивать поддержку внедрения новых аналитических методов обнаружения угроз ИБ.

Специалисты третьей линии – это эксперты-аналитики в области сетевой безопасности высшего уровня, способные понять уникальную ситуацию, применяя свои знания и опыт и сопоставляя различные события и факты, имеющие отношение к инциденту ИБ. Используя средства обнаружения угроз ИБ («охоты за угрозами»), они детально анализируют всю информацию, имеющуюся к этому моменту для расследования переданного им инцидента ИБ, и активно ищут уязвимости в ИТКС. Исследование одного инцидента может занять от нескольких минут до нескольких недель, поскольку часто требует сбора дополнительных сведений, связанных с инцидентом ИБ, и привлечения технических экспертов. Эксперты-аналитики осуществляют анализ ранее не происходивших и неизвестных событий ИБ и новых уязвимостей, опираясь на различные источники и исторические данные самой ОРГАНИЗАЦИИ, для чего у них должно быть четкое понимание внешнего и внутреннего контекста функционирования ИТКС. Исследуя инцидент ИБ, они могут выявить его характерные признаки и передавать их в соответствующие системы мониторинга ИБ и операторам первой линии – таким образом, эти эксперты активно

вовлечены в разработку, настройку и внедрение аналитики для обнаружения угроз ИБ. В их задачу входит восстановление последовательности всех событий, приведших к инциденту ИБ, а также подготовка рекомендаций по ликвидации его последствий и повышению общего уровня ИБ ИТКС. Кроме ИБ-аналитиков, к специалистам третьей линии также относятся аудиторы ИБ и специалисты, занимающиеся сбором свидетельств инцидентов ИБ в цифровой форме для их детального расследования и, при необходимости, передачи этой информации в правоохранительные органы.

Четвертая линия состоит из руководителей высшего звена и руководителей с большим опытом работы, которые несут ответственность за соблюдение всех применимых требований, политик и правил и координирует работу всего ЦИУСБ. Эта группа наблюдает за всей деятельностью персонала ЦИУСБ и выполняет административные функции, включающие в себя управление стратегий и тактикой функционирования ЦИУСБ, прием на работу, регулирование работы смен, управление бюджетом, необходимое обучение работников, а также оценку общих результатов функционирования ЦИУСБ и вклада в них отдельных работников. Особая роль четвертой линии проявляется и во время кризисных ситуаций, когда она служит связующим звеном между персоналом ЦИУСБ и остальной частью ОРГАНИЗАЦИИ. Кроме этого, на этой линии должно при необходимости осуществляться непрерывное взаимодействие, например, с ГосСОПКА и другими уполномоченными организациями.

Очень кратко описанные трудовые функции (ТФ) для всех четырех линий персонала типового ЦИУСБ должны быть в последствии уточнены и расширены в зависимости от потребностей конкретной ОРГАНИЗАЦИИ.

С публикацией в августе 2020 г. на сайте ФСТЭК России проекта ГОСТ Р, посвященного терминам и определениям в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирование на компьютерные инциденты [286], были перечислены следующие виды сотрудников центра ГосСОПКА – специалистов трех линий с указанием выполняемых ими ролей:

1) Первой – выполняющие роли с соответствующими ТФ:

— «специалист по взаимодействию с персоналом и пользователями» – прием сообщений персонала и пользователей информационных ресурсов и подготовка информации для предоставления в Национальный координационный центр по компьютерным инцидентам (НКЦКИ);

— «специалист по обнаружению компьютерных атак и инцидентов» – анализ событий ИБ, регистрация компьютерных атак и инцидентов ИБ;

— «специалист по обслуживанию средств центра ГосСОПКА» – обеспечение функционирования средств, размещаемых в центре ГосСОПКА, а также дополнительных средств защиты ИИ;

2) Второй – выполняющие роли:

— «специалист по оценке защищенности» – инвентаризация информационных ресурсов, выявление уязвимостей, анализ выявленных уязвимостей и угроз ИБ, установление соответствия принимаемых мер требованиям по обеспечению ИБ;

— «специалист по ликвидации последствий компьютерных инцидентов» – координация действий по реагированию на компьютерные инциденты и приведению ИИ в штатный режим работы;

— «специалист по установлению причин компьютерных инцидентов» – анализ причин компьютерных инцидентов, анализ последствий инцидентов и подготовку перечня компьютерных инцидентов для представления в НКЦКИ;

3) Третьей – выполняющие роли:

— «аналитик» – анализ информации, предоставляемой специалистами первой и второй линий; выявление и анализ угроз ИБ, прогнозирование их развития, разработка предложений по доработке нормативных и методических документов по вопросам защиты информации;

— «технический эксперт» – экспертная поддержка в соответствии со специализацией (вредоносное ПО, настройка СЗИ, применение специализированных технических средств, оценка защищенности и т.п.), формирование предложений по повышению уровня защищенности; разработку предложений по доработке нормативных и методических документов по вопросам защиты информации;

— «специалист» – нормативное правовое и методическое сопровождение деятельности центра ГосСОПКА;

— «руководитель» – управление деятельностью центра ГосСОПКА, взаимодействие с НКЦКИ, внесение изменений в соответствующие нормативные и методические документы.

15-летний опыт существования ЦМБ позволяет выделить такую тенденцию – в среднем его штат полностью обновляется за 6 лет, что ставит задачу поиска новых и развития имеющихся работников [287]. Это означает, что в настоящее время особенно актуальной является подготовка кадров для ЦИУСБ, причем как для его разработчиков, так и пользователей. Эта тема является очень обширной и в данном исследовании она затронута кратко, только под углом зрения подготовки персонала для типового ЦИУСБ.

Квалификационные характеристики персонала типового ЦИУСБ, относящегося к специалистами в области ИБ, могут быть представлены в виде набора компетенций. Компетенция традиционно определяется как совокупность наблюдаемых и измеримых знаний (З), навыков (Н) и умений (У) (вместе ЗНУ) (а также некоторых других атрибутов и опыта работы), которые способствуют повышению производительности труда работников ЦИУСБ и, в конечном счете, приводят к успешной деятельности ОРГАНИЗАЦИИ [288]. Знание – это узнавание фактов, ис-

тин и принципов, полученных в процессе традиционного обучения и/или опыта [288]. Навык – это развитая ловкость (сноровка) в осуществлении умственных операций или физических процессов, которые часто приобретаются посредством специализированного обучения; использование этих навыков приводит к успешной работе [288]. Умение – это способность выполнять физические или умственные действия, которые связаны с той или иной профессией [288]. Следовательно, в рамках данного исследования ЗНУ – это три неотъемлемых атрибута конкретной компетенции, которые необходимы для успешного осуществления деятельности описанных выше четырех групп персонала ЦИУСБ.

На протяжении многих лет во всем мире предпринимаются усилия по выработке общего подхода к необходимому объему знаний, навыков и умений специалистов в области ИБ, представляющему собой необходимый и достаточный набор требований к выпускникам высших учебных заведений и слушателям курсов повышения квалификации различных образовательных учреждений и центров, осуществляющих долгосрочную и краткосрочную подготовку специалистов. Первые попытки сформировать общую точку зрения по этому вопросу были приняты на Всемирных международных конференциях по образованию в области ИБ (англ. *World Conference on Information Security Education, WISE*) в конце 1990-х и начале 2000-х годов, которые с тех пор стали традиционными и проходят до сих пор. Примерно в то же время стали появляться, а потом обновляться и расширяться для новых ИТ предлагаемые различными организациями этой отрасли системы сертификации специалистов области ИБ, например, начального уровня (типа *CompTIA Security+* и *GIAC Security Essentials*) и более продвинутые, такие как *Certified Information Systems Security Professional (CISSP)*, *Certified Information Security Manager (CISM)* и *Certified Ethical Hacker (CEH)* [288].

До сегодняшнего дня так и не определены единые и признаваемые во всем мире компетенции специалистов в области ИБ. Сформировались три базовых подхода – американский, австралийский и европейский [53]:

— Американская точка зрения была сформулирована в документе «State Government Information Security Workforce Development Model. A Best Practice Model and Framework» [289] (Национальная правительственная модель развития кадров в области информационной безопасности. Модель и инфраструктура лучших практик), разработанном Национальным подразделением кибербезопасности Департамента национальной безопасности США (DHS/NCSD), и «National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework» [290] (Национальная инициатива по образованию в области кибербезопасности. Модель персонала в области кибербезопасности) Национального института стандартов и технологий (NIST);

— Офис информационного менеджмента при Правительстве Австралии (AGIMO) разработал документ «The Cyber Security Capability Framework & Mapping of ISM Roles» [291] (Мо-

дель умений в области кибербезопасности и карта ролей в области ИБ);

— Европейский подход впервые был изложен Европейской Комиссией в модели электронных компетенций, которая с 2019 г. представлена в документе «EN 16234-1:2019 e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all sectors – Part 1: Framework» (Общая европейская модель для профессионалов в области ИКТ во всех секторах), и в более специализированном для области ИБ международном стандарте ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals [292] (Информационная технология. Методы и средства обеспечения безопасности. Требования к компетенциям специалистов в области систем менеджмента ИБ).

Компетенции специалистов в области систем менеджмента ИБ (СМИБ) из ISO/IEC 27021:2017 [292] очень хорошо подходят для СУИБ ОРГАНИЗАЦИЙ, владеющих ИТКС. Все компетенции в стандарте (их 24) описаны с точки зрения содержания ТФ работника, обладающего определенными знаниями и навыками, и разделены на две категории [293]:

1) 12 общих компетенций в контексте деятельности ОРГАНИЗАЦИИ (а именно, лидерство; коммуникации; бизнес-стратегия и система менеджмента ИБ; управление структурой, культурой и деятельностью организации и заинтересованными сторонами; организация процессов и управление организационными изменениями; человеческие ресурсы; управление командами и отдельными работниками; управление рисками; управление ресурсами; архитектура ИС; управление проектами и имеющимися наработками; управление поставщиками; управление проблемами);

2) 12 компетенций в области управления ИБ, включая компетенции в области ИБ (а именно, управление ИБ и контекст деятельности ОРГАНИЗАЦИИ) и специфические для СМИБ компетенции, которые представлены в соответствии с последовательностью процессов – планирование (область действия СМИБ; управление и обработку рисков ИБ), эксплуатация (процедуры управления ИБ), поддержка (обучение и осведомленность в области ИБ; документация), оценка эффективности (мониторинг, измерение, анализ и оценка СМИБ; аудит СМИБ; анализ менеджмента) и улучшение (постоянное совершенствование; тенденции и разработки в области технологий).

Даже из простого перечисления компетенций стандарта очевидно, что штат типового ЦИУСБ должен обладать всеми этими обширными компетенциями в объемах, соответствующих их функциональным обязанностям.

Еще одно важное дополнение – в 2017 г. совместные усилия объединенной группы преподавателей из передовых университетов мира, осуществляющих образовательную деятельность в области кибербезопасности, включая и автора данного исследования, под эгидой Ассо-

циации вычислительной техники (*ACM*), Компьютерного общества *IEEE (IEEE CS)*, Специальной группы по безопасности Ассоциации информационных систем (*AIS SIGSEC*) и Рабочей группы Технического комитета по обучению ИБ Международной федерации по обработке информации (*IFIP WG 11.8*) увенчались успехом – был разработан документ «Cybersecurity Curricular Guideline» (CSEC 2017) (Руководство по учебному плану в области кибербезопасности). Основной фокус этого документа, к сожалению, сделан не на компетенции, а на содержание и базовые концепции учебных дисциплин, которые чаще всего изучаются в рамках направления «Кибербезопасность».

Объективно оценивая ситуацию в области подготовки кадров в области ИБ, сделаем вывод, что в России в единственной стране в мире уже давно создана целая система подготовки кадров в области ИБ, базирующаяся на Федеральных государственных образовательных стандартах (ФГОС) высшего образования (ВО) и профессиональных стандартах (ПС).

При подготовке специалистов для типового ЦИУСБ ОРГАНИЗАЦИИ необходимо исходить из того, что они должны обладать современными профессиональными компетенциями (ПК), требуемыми для решения конкретных профессиональных задач и реализации конкретных ТФ. Формирование ПК относится к задачам, решаемым существующей системой образования, нормативной базой которого является комплекс ФГОС высшего образования (ВО). В данном случае речь идет о ФГОС ВО, относящихся к Укрупненной группе специальностей и направлений подготовки (УГСНП) 10.00.00 «Информационная безопасность». При разработки ФГОС последнего поколения (ФГОС++) были сформулированы общепрофессиональные компетенции (ОПК) выпускников, прошедших обучение в рамках определенного ФГОС [294]. Эти ПК можно связать с положениями действующих в настоящее время ПС, относящихся к группе занятий (профессий) «Специалисты в области информационной безопасности» [295].

Анализ указанных выше ФГОС и ПС позволил установить связь объектов и предметов ТФ работника типового ЦИУСБ с определенными образовательными и профессиональными стандартами:

— ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность» (уровень – магистратура);

— ПС 06.032 Специалист по безопасности компьютерных систем и сетей (вид профессиональной деятельности: защита информации в компьютерных системах и сетях);

— ПС 06.033 Специалист по защите информации в автоматизированных системах (вид профессиональной деятельности: обеспечение безопасности информации в АС).

Конкретная программа магистратуры, готовящий работников типового ЦИУСБ в рамках образовательного стандарта, должна устанавливать следующие ОПК (выпускник должен быть):

— ОПК-1. Способен обосновывать требования к СОИБ и разрабатывать проект техниче-

ского задания на ее создание;

— ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения ИБ.

Программа магистратуры, рассчитанная на подготовку специалистов для типового ЦИУСБ, должна обеспечивать реализацию дисциплин, обозначенных в ФГОС 10.04.01 как базовые дисциплины профессионального модуля. Среди них можно выделить дисциплину, которой наиболее полно соответствует содержание ТФ работника типового ЦИУСБ – это «Технологии обеспечения информационной безопасности» (ТОИБ) – оригинальная дисциплина, разработанная автором данного исследования, и в настоящее время преподаваемая во всех учебных заведениях РФ, где ведется подготовка магистров по направлению «Информационная безопасность».

Проект примерной основной образовательной программы магистратуры по ФГОС ВО 10.04.01 устанавливает связь между дисциплиной ТОИБ и ОПК-1 и ОПК-2 путем формулирования индикаторов достижения (ИД) ОПК [296, 297]. Для дисциплины ТОИБ эти индикаторы будут следующими:

— для ОПК-1: ОПК-1.1.1 знать основы отечественных и зарубежных стандартов в области обеспечения ИБ; ОПК-1.2.1 уметь проектировать техническое задание на создание СОИБ; ОПК-1.3.1 владеть навыками участия в разработке СОИБ;

— для ОПК-2: ОПК-2.1.1 знать методы концептуального проектирования технологий обеспечения ИБ; ОПК-2.2.1 уметь выбирать и обосновывать применение методов решения задач обеспечения ИБ; ОПК-2.3.1 владеть навыками выполнения работы при разработке и эксплуатации систем и средств обеспечения ИБ.

Приведенные выше ИД ОПК с привязкой к дисциплине ТОИБ могут быть сопоставлены с обобщенными ТФ (ОТФ) и связанными с ними ТФ, приведенными в ПС 06.032 и ПС 06.033. При этом выделены только те ОТФ и ТФ, которые имеют отношение к ЦИУСБ.

Для дисциплины ТОИБ:

ПС–06–032: Специалист по безопасности компьютерных систем и сетей:

ОТФ–С: Оценивание уровня безопасности компьютерных систем и сетей:

ТФ–С/01.7: Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.

ТФ–С/02.7: Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей.

ОТФ–D: Разработка программно-аппаратных СЗИ компьютерных систем и сетей:

ТФ–D/01.8: Разработка требований к программно-аппаратным СЗИ компьютерных систем и сетей.

ТФ–D/02.8: Проектирование программно-аппаратных СЗИ компьютерных систем и сетей.

ТФ–D/03.8: Разработка и тестирование СЗИ компьютерных систем и сетей.

ТФ–D/04.8: Сопровождение разработки СЗИ компьютерных систем и сетей.

ПС–06-033: Специалист по защите информации в АС:

ОТФ–D: Разработка систем защиты информации АС:

ТФ–D/01.7: Тестирование систем защиты информации АС.

ТФ–D/02.7: Разработка проектных решений по защите информации в АС.

ТФ–D/03.7: Разработка эксплуатационной документации на системы защиты информации АС.

ТФ–D/04.7: Разработка программных и программно-аппаратных средств для систем защиты информации АС.

ОТФ–E: Формирование требований к защите информации в АС:

ТФ–E/01.8: Обоснование необходимости защиты информации в АС.

ТФ–E/02.8: Определение угроз безопасности информации, обрабатываемой АС.

ТФ–E/03.8: Разработка архитектуры системы защиты информации АС.

ТФ–E/04.8: Моделирование защищенных АС с целью анализа их уязвимостей и эффективности средств и способов защиты информации.

На этапе разработки рабочих планов конкретной магистерской программы и рабочих программ конкретных дисциплин должен быть расширен компетентностный подход путем формулирования ПК и соответствующих им ИД. Например, конкретизируем ПК для всех четырех линий работников типового ЦИУСБ:

1) персонал первой линии – процедура сортировки (англ. *triage*) предупреждений, обнаружение вторжений, основы информационной и сетевой безопасности, *SIEM*-системы, СЗИ и т.п.;

2) персонал второй линии – компетенции персонала первой линии, основы расследования инцидентов ИБ, сбор свидетельств инцидентов ИБ в цифровой форме в сети и на хостах, процедуры реагирования на инциденты ИБ, просмотр ЖРС, базовая оценка вредоносного ПО, ПО, использующее уязвимости (англ. *exploits*), основы *Threat Intelligence* и т.п.;

3) персонал третьей линии – компетенции персонала второй линии, глубокие знания в области сетей, конечных точек, расследования инцидентов ИБ, реверс-инжиниринг вредоносного ПО, специфическое ПО, используемое в ИТКС ОРГАНИЗАЦИИ, *Threat Intelligence*, «охота за угрозами», обнаружение аномалий, агрегирование и расширенный анализ данных, тесты на проникновение (англ. *Pen Testing*) и т.п.;

4) персонал четвертой линии – управление проектами, обучение управлению инцидентами ИБ, общие вопросы управления ИБ и т.п. Именно для персонала этой линии в полном объеме подходят компетенции, перечисленные в ISO/IEC 27021:2017 [292].

И, конечно, обучение персонала типового ЦИУСБ должно проводиться постоянно, для чего предназначены курсы повышения квалификации, проводимые различными учебными центрами. Это необходимо потому, что информационные, коммуникационные, сетевые технологии постоянно развиваются, также появляются новые технологии, что отражается на динамически изменяющейся среде функционирования ИТКС ОРГАНИЗАЦИИ и ЦИУСБ как ее неотъемлемой части.

5.8. Демонстрация выполнения требований к типовому Центру интеллектуального управления сетевой безопасностью

Обобщая представленные в данном исследовании результаты, продемонстрируем, что все сформулированные в разделе 4.7 общие и специальные требования, а также требования к обеспечению ИБ типового ЦИУСБ ОРГАНИЗАЦИИ в ходе данного исследования были выполнены. Далее будет процитировано (в более сжатом виде, чем в разделе 4.7) само требование и кратко показано как оно было учтено/реализовано в типовом ЦИУСБ, с указанием соответствующего раздела, где это подробно рассмотрено.

ТО1. Вся деятельность ЦИУСБ ОРГАНИЗАЦИИ должна быть выстроена и реализована согласно требованиям, изложенным в применимых нормативных, правовых, отраслевых и других документах – Исследование начато с определения нормативной и правовой базы (раздел 1.3). Все перечисленные источники многократно упоминаются по тексту исследования.

ТО2. ЦИУСБ должна представлять собой комплекс, позволяющий обеспечить автоматизацию ПУИИБ ОРГАНИЗАЦИИ, включая реагирование на инциденты ИБ, за счет централизованной обработки связанной с ИБ ИТКС информации, а также предоставляющий услуги и средства связи для персонала, вовлеченного в ПУИИБ – Функциональные подсистемы типового ЦИУСБ построены с учетом разработанного ПУИИБ (раздел 3.4) и централизованной ИБ-аналитики в отношении связанной с ИБ ИТКС информации, описанной в разделах 4.4 и 5.4.2.

ТО3. Единство и скоординированность функционирования ЦИУСБ с ИТКС ОРГАНИЗАЦИИ – Это требование выполняется за счет того, что типовой ЦИУСБ изначально строился как структурная единица, телекоммуникационно и информационно встроенная в ИТКС ОРГАНИЗАЦИИ, наделенная должными полномочиями и имеющая необходимые инструментальные средства и компетенции его персонала.

ТО4. ЦИУСБ должен быть системообразующим элементом СОИБ ОРГАНИЗАЦИИ на основе жесткой связи с ней, влиять на ее развитие и совершенствование – Типовой ЦИУСБ с самого начала исследования рассматривался как особая структура для управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ. В разделе 3.4.6 показано, что эта система управления

сетевой безопасностью входит как системообразующий элемент в общую СУИБ ОРГАНИЗАЦИИ. Поскольку процесс управления входит в обеспечение ИБ, а СУИБ входит в СОИБ, то и ЦИУСБ входит в СОИБ и является его системообразующим элементом для ЕИП ОРГАНИЗАЦИИ.

ТО5. Наличие необходимой организационной структуры и органа управления ЦИУСБ – В высокоуровневой функциональной архитектуре типового ЦИУСБ выделен уровень управления (раздел 5.4.1).

ТО6. Интеграция информационных и телекоммуникационных сетей, ресурсов и услуг ЦИУСБ в единую систему – Типовой ЦИУСБ как неотъемлемая часть ИТКС ОРГАНИЗАЦИИ обладает этим качеством по своей природе, поскольку как и ИТКС объединяет телекоммуникационную и информационную сети (раздел 1.1.3), а также за счет централизованного управления ЦИУСБ (уровень управления в разделе 5.4.1).

ТО7. Применение современных средств технического, программного, информационного, аналитического, организационного, документального обеспечения, функционально объединенных в ЦИУСБ – Типовой ЦИУСБ как сложный комплекс различных систем и подсистем, предназначенных для обеспечения его функциональной устойчивости, построен на принципе типизации современных, «лучших в своем классе» решений, выбираемых для его реализации и внедрения (раздел 5.2).

ТС1. Создание и непрерывное развитие ЦИУСБ как единой экосистемы – В главе 5 типовой ЦИУСБ все время представляется как сложная динамическая система взаимосвязанных элементов в ЕИП ОРГАНИЗАЦИИ. В основу его построения положен принцип эволюционности (раздел 5.2), который упоминается и при обсуждении вопросов обеспечения функциональной устойчивости типового ЦИУСБ (раздел 5.6).

ТС2. Управляемость ЦИУСБ с централизованной архитектурой и распределенной/ децентрализованной работой отдельных процессов при совмещении масштабируемости и эластичности сбора, хранения, первичной обработки и корреляции данных для его функционирования в изменяющейся среде осуществления деятельности ОРГАНИЗАЦИИ и при появлении новых угроз ИБ в ЕИП для ее ИТКС – Наличие централизованного управления в типовом ЦИУСБ на уровне управления обсуждается в разделе 5.4.1. Распределенное и часто распараллеленное исполнение различных процессов ПУИИБ, описанных в разделе 3.4, очевидно. К этому нужно добавить то, что процессы обеспечения собственной ИБ ЦИУСБ выполняются в разных зонах безопасности, выделенных в разделе 5.4.3. Принцип эластичности заложен в проект типового ЦИУСБ изначально (раздел 5.2) и соблюдается за счет внедрения в структуру типового ЦИУСБ современной системы хранения данных – озера данных (раздел 5.4.2). Процессы ИБ-аналитики в ЦИУСБ представлены в разделах 4.5.2 и 5.4.2, посвященным бизнес-логике функ-

ционирования ЦИУСБ и обработке больших данных в ЦИУСБ соответственно.

ТС3. Согласованность процессов, поддерживающих функционирование ЦИУСБ, со всеми передовыми практиками и применимыми к ИТКС ОРГАНИЗАЦИИ требованиями по обеспечению ИБ – Данное исследование начато с определения нормативной и правовой базы (раздел 1.3). Все перечисленные источники многократно упоминаются по тексту исследования. Лучшие практики учтены при выборе типовых «лучших в своем классе» решений (например, *NGFW*, *SOAR*-система) для реализации отдельных функций ЦИУСБ.

ТС4. Расширенная ИБ-аналитика и использование для нее как можно большего количества типов данных – Данное требование взято за основу изложения раздела 5.4.2.

ТС5. Адаптивное управление событиями ИБ в ИТКС, поддерживаемое за счет применения предсказательного определения возможных тенденций в области обеспечения ИБ в ЕИП ОРГАНИЗАЦИИ и типовых модульных и конфигурируемых СЗИ, сетевых устройств, протоколов, процессов и мер обеспечения сетевой безопасности – Для предсказательного определения возможных тенденций в области обеспечения ИБ в ЕИП конкретной ОРГАНИЗАЦИИ и соответствующего адаптивного управления событиями ИБ в ИТКС предлагается использовать системы *Threat Intelligence* (разделы 4.4 и 5.3.2), «охоту за угрозами» (раздел 5.3.2) и «песочницу» (раздел 5.4.3). Кроме этого, в бизнес-логике функционирования типового ЦИУСБ определен *TRI Vox*, решающий именно эти задачи (разделы 4.4. ЦИУСБ построен на принципе типизации решений, выбираемых для его реализации и внедрения (раздел 5.2).

ТС6. Функциональная устойчивость ЦИУСБ в штатном режиме, в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций – Определению функциональной устойчивости типового ЦИУСБ и управлению им посвящен раздел 5.6.

ТС7. Масштабируемость ЦИУСБ с точки зрения масштабируемости сбора и обработки огромного количества событий от различных гетерогенных внутренних и внешних по отношению к ИТКС источников, что все вместе определяет необходимость применения ИТ и использования продвинутых технологий для хранения больших данных – Данное требование взято за основу изложения раздела 5.4.2. Озеро с быстрыми данными составляет основу архитектуры обработки связанных с ИБ данных в типовом ЦИУСБ.

ТС8. Эластичность для распределенных и реализуемых в режиме реального/близкого к реальному времени агрегирования, пакетной и потоковой обработки и передачи гибридных относящихся к ИБ больших данных – Соблюдение этого требования обеспечивается предложенной бизнес-логикой функционирования типового ЦИУСБ, основанной на модульном характере используемых блоков, число которых можно наращивать (раздел 4.5.2), а процессы ИБ-аналитики относящихся к ИБ больших и быстрых данных рассмотрены в разделе 5.4.2.

ТС9. Гибкость при использовании необходимых методов и инструментов ИБ-аналитики таким образом, чтобы персонал ЦИУСБ мог использовать при обработке все доступные в тот момент данные (включая исторические за длительный период времени) и получать результаты, учитывающие разные точки зрения – Данное требование учтено при выборе озера данных в качестве системы хранения всех накопленных типовым ЦИУСБ относящихся к ИБ данных. Сами процессы ИБ-аналитики в отношении больших и быстрых данных рассмотрены в разделе 5.4.2.

ТС10. Собственная защищенность и надежность ЦИУСБ, включая защищенность его инфраструктуры, процессов обработки данных и самих связанных с ИБ больших данных – Данное требование взято за основу изложения раздела 5.4.3, в котором предложена зональная архитектура обеспечения ИБ в типовом ЦИУСБ.

ТС11. Прозрачность для руководства ОРГАНИЗАЦИИ всей деятельности ЦИУСБ для принятия своевременных управленческих решений – Руководство ОРГАНИЗАЦИИ, взаимодействуя с уровнем управления типового ЦИУСБ (разделе 5.4.1) и соответствующими работниками ЦИУСБ (раздел 5.7), регулярно готовящими отчетность по его функционированию, будет располагать всей необходимой информацией для принятия управленческих решений как в отношении ЦИУСБ, так и ИТКС как основы ЕИП ОРГАНИЗАЦИИ. Зональная архитектура обеспечения ИБ в типовом ЦИУСБ дает полную видимость всех областей функционирования ЦИУСБ и действий его персонала (раздел 5.4.3).

ТБ1. Целенаправленная и эшелонированная (многоуровневая) защита всех ресурсов и подсистем ЦИУСБ и ИТКС, основанная на системном методологическом подходе и реализации на каждом уровне соответствующих процессов и мер обеспечения ИБ и обеспечения независимости уровней друг от друга с точки зрения поддержания ИБ – Принцип эшелонированной защиты типового ЦИУСБ заложен изначально в его проект (раздел 5.2). Этому способствует зональная архитектура обеспечения ИБ в типовом ЦИУСБ с выделением четырех зон безопасности, а именно, демилитаризованной, доверенной, запретной и управления с соответствующими подзонами, представленная в разделе 5.4.3.

ТБ2. Прогнозируемость характера проблем и задач в области обеспечения ИБ ЦИУСБ – Для поддержания предсказательного определения возможных тенденций в области обеспечения ИБ во всем ЕИП конкретной ОРГАНИЗАЦИИ (включая ЦИУСБ) предлагается использовать системы *Threat Intelligence* (разделы 4.4 и 5.3.2), «охоту за угрозами» (раздел 5.3.2) и «песочницу» (раздел 5.4.3). Кроме этого, в бизнес-логике функционирования типового ЦИУСБ определен ТР1 Вох, решающий именно эти задачи (раздел 4.4).

ТБ3. Своевременность обнаружения проблем, влияющих на безопасность ЦИУСБ – Функциональные подсистемы типового ЦИУСБ построены с учетом разработанного в разделе 3.4 ПУИИБ и централизованной ИБ-аналитики в отношении связанной с ИБ ИТКС информа-

ции, описанной в разделах 4.4 и 5.4.2, позволят своевременно обнаруживать проблемы, прямо или косвенно относящиеся к ИБ и потенциально способные повлиять на успешное достижение ЦИУСБ целей его устойчивого функционирования.

ТБ4. Своевременность, адекватность угрозам ИБ и разумная достаточность защитных мер ЦИУСБ – На основе предложенной в главе 2 таксономии уязвимостей, угроз ИБ, сетевых атак и инцидентов ИБ сначала должны быть построены Модель угроз ИБ и Модель нарушителей ИБ и разработан реестр рисков ИБ, на основе чего осуществляется обоснованный выбор всех необходимых и достаточных защитных мер для подлежащих защите объектов типового ЦИУСБ. Меры и средства обеспечения собственной ИБ ЦИУСБ перечислены в разделе 5.4.3.

ТБ5. Результативность и эффективность защитных мер с учетом их постепенной деградации – Для определения показателей результативности и эффективности защитных мер (и функциональной устойчивости в целом) должна регулярно проводится оценка рисков ИБ ЦИУСБ с последующие их обработкой, предназначенной для сохранения приемлемых для ОРГАНИЗАЦИИ рисков ИБ ЦИУСБ. Этому способствует риск-ориентированный подход, выбранный в качестве принципа построения типового ЦИУСБ (раздел 5.2). Кроме этого, в основу построения типового ЦИУСБ положен принцип эволюционности, который позволит ЦИУСБ постоянно совершенствоваться, обновлять арсенал процессов и мер обеспечения ИБ (раздел 5.2).

ТБ6. Непрерывность процесса безопасного функционирования подсистемы обеспечения ИБ ЦИУСБ – Вопросы управления непрерывностью функционирования типового ЦИУСБ и его восстановления после нарушений и инцидентов ИБ рассмотрены в разделе 5.6.

ТБ7. Гибкость управления и применения защитных мер – обеспечение возможности варьировать уровень защищенности ЦИУСБ в зависимости от текущей ситуации и потребности ОРГАНИЗАЦИИ в ИБ в данный период времени – Принцип обеспечение гибкой настройки ЦИУСБ и управляемых мер и средств обеспечения сетевой безопасности на совместную работу при изменении нормативных, правовых и других документов и динамически изменяющихся условиях функционирования ИТКС заложен в проект типового ЦИУСБ (раздел 5.2). Он поддерживается бизнес-логикой функционирования типового ЦИУСБ, в которой для этих целей специально определен U Box, отвечающий за изменение конфигурационных настроек СЗИ (раздел 4.4).

ТБ8. Способность к интеграции и согласованность применения различных защитных мер – При разработке зональной архитектуры обеспечения ИБ в типовом ЦИУСБ для использования в разных зонах безопасности были выбраны такие типовые СЗИ, которые способны к согласованной работе (раздел 5.4.3). Один и тот же класс СЗИ должен быть установлен сразу в нескольких зонах. Модульность архитектуры способствует тому, что реализация новых мер в

работающий ЦИУСБ не нарушит процесса его нормального функционирования, при интеграции не возникнет критичных уязвимостей и все объекты защиты ЦИУСБ попадут в их область действия.

ТБ9. Наблюдаемость защитных мер – результат их применения будет явно наблюдаем (прозрачен) и может быть оценен – Объединяющая все процессы и меры обеспечения ИБ ЦИУСБ зона централизованного управления предназначена для решения именно этой задачи (раздел 5.4.3). Зональная архитектура обеспечения ИБ в типовом ЦИУСБ дает полную видимость всех областей функционирования ЦИУСБ.

ТБ10. Обязательность постоянного (мониторинг) и систематического периодического (аудит) контроля защитных мер с целью выяснения, насколько они выполняют возлагаемые на них функции защиты объектов ЦИУСБ – В зоне централизованного управления ИБ типового ЦИУСБ расположены системы мониторинга и аудита его СЗИ (раздел 5.4.3).

ТБ11. Мониторинг активности персонала и пользователей ЦИУСБ для своевременного выявления несанкционированных действий и ошибок – В зоне централизованного управления ИБ типового ЦИУСБ расположены системы мониторинга активности его персонала (в частности, *IAM*- и *DLP*-системы) (раздел 5.4.3). Зональная архитектура обеспечения ИБ в типовом ЦИУСБ дает полную видимость всех действий персонала ЦИУСБ.

ТБ12. Простота и управляемость защитных мер ЦИУСБ – Проект типового ЦИУСБ разработан как объединение ЦИБ и СОЦ (раздел 5.3.2), что как и раз и способствует выполнению характерных функций централизованного администрирования со стороны персонала СОЦ в составе ЦИУСБ. Простота управления обеспечивается использованием типовых решений с удобными и стандартизованными пользовательскими интерфейсами и развитыми средствами визуализации для проверки согласованности конфигураций СЗИ (например, САЗ).

ТБ13. Совершенствование обеспечения ИБ ЦИУСБ за счет периодической переоценки защитных мер и потребности в них – В основу обеспечения ИБ типового ЦИУСБ, как и для ЦИУСБ в целом, положены принципы эволюционности и использования риск-ориентированного подхода (раздел 5.2), реализация которых осуществляется на основе принятия решений по результатам оценки рисков ИБ, а также мониторинга и аудита ИБ ЦИУСБ.

ТБ14. Формирование режима безопасности ЦИУСБ – Реализация данного требования обеспечивается комплексом мер, направленных на обеспечение информированности (осведомленности) и лояльности персонала типового ЦИУСБ и его постоянное теоретическое и практическое обучение (раздел 5.7).

ТБ15. Кадровое обеспечение ЦИУСБ высококвалифицированным персоналом с необходимыми компетенциями в области управления сетевой безопасностью и инцидентами ИБ – Вопросу подготовки высококвалифицированного персонала для типового ЦИУСБ в части приоб-

речения ими компетенций в области ИБ и непрерывности деятельности посвящен раздел 5.7, а также раздел 6.5, в котором говорится о внедрении результатов исследования в образовательный процесс НИЯУ МИФИ и Федеральный УМО в области ИБ (раздел 6.6).

ТБ16. Разделение полномочий, распределение ролей и ответственности – Вопросы кадрового обеспечения типового ЦИУСБ в разделе 5.7 рассмотрены с точки зрения полномочий и соответствующих компетенций его работников, которые не должны позволять им единолично осуществлять выполнение критичных операций, не могли нарушить критически важный для ЦИУСБ процесс или создать уязвимости в обеспечении ИБ ЦИУСБ по сговору с нарушителем ИБ и т.п.

ТБ17. Использование отечественного и зарубежного опыта, стандартов и нормативных и правовых актов в построении подобных центров – Данное исследование начато с определения нормативной и правовой базы (раздел 1.3). Все перечисленные источники многократно упоминаются по тексту исследования.

Таким образом, показано, что поставленная задача построения типового ЦИУСБ как системообразующего элемента СОИБ и основа реализации ПУИИБ в рамках ЕИП для ИТКС ОРГАНИЗАЦИИ была решена в полном объеме.

Структурно-логическая схема проведенного исследования может быть представлена рис. 55, который показывает, как на основе отобранной нормативной и правовой базы, разработки глоссария и таксономии основных понятий теории обеспечения ИБ, четко специфицированного ПУИИБ для ИТКС, рассмотренных спецификаций инцидентов ИБ и вопросов подготовки персонала был прослежен путь эволюционного развития ГРИИБ, приведший сначала к появлению ЦМБ, осуществляющего только мониторинг инцидентов ИБ в компьютерных сетях с *SIEM*-системой 1.0 в качестве ядра, а потом ЦИБ с *SIEM*-системой 2.0, способного управлять этими инцидентами ИБ за счет использования ИБ-аналитики и обработки больших данных. В данном исследовании этот путь быть продолжен предложенным типовым ЦИУСБ за счет добавления функциональных возможностей СОЦ, озер данных и интеллектуальной обработки быстрых данных, а также создания проекта *SIEM*-системы 3.0 с элементом, в котором применены технологии блокчейна. Таким образом, предложен переход от мониторинга инцидентов ИБ (ЦМБ – «глаза мониторинга инцидентов ИБ») через управление инцидентами ИБ (ЦИБ – «мозг управления инцидентами ИБ с широко открытыми глазами») к обеспечению адаптивной упреждающей сетевой безопасности (ЦИУСБ – «быстрый мозг обеспечения адаптивной упреждающей сетевой безопасности с широко открытыми глазами и умелыми руками»).



Рисунок 55 – Структурно-логическая схема исследования

Представленная схема проведенного исследования наглядно демонстрирует преемственность полученных результатов по отношению к ранее существовавшим и их значимость для эволюционного обеспечения сетевой безопасности.

Выводы по главе 5

1. После пояснений, касающихся хронологии событий, связанных с разработкой типового ЦИУСБ, и состояния этого вопроса в отечественной и зарубежной науке, сделан вывод о том, что идея ЦИУСБ как объединения ЦИБ и СОЦ принадлежит автору данного исследования. Далее изложена разработанная методология построения типового ЦИУСБ ОРГАНИЗАЦИИ, что хорошо согласуется с циклом *PDCA*.

2. На основе сформулированных в разделе 4.7 требований в качестве основных и учитывая типичными требованиями к системам управления были определены принципы построения типового ЦИУСБ.

3. Сформулированы основные типовые цели функционирования типового ЦИУСБ в ОРГАНИЗАЦИИ, для достижения которых, расширения автономности управления инцидентами ИБ в рамках одной ОРГАНИЗАЦИИ и углубления знаний об уровне ИБ ее ИТКС предлагается объединить все преимущества ЦИБ и СОЦ с их уникальными и совместно применимыми инструментальными средствами управления сетью и ее сетевой безопасностью.

4. Проведен сравнительный анализ характеристик ЦИБ и СОЦ, показавший, что по СОЦ работает с данными о состоянии сети и ее отдельных элементов, что похоже на функционирование ЦИБ с тем различием, что последний имеет дело только с данными о событиях ИБ.

5. Обоснована объективная возможность объединения ЦИБ и СОЦ и указана главная

цель объединенного ЦИУСБ – предоставить ОРГАНИЗАЦИИ управляемую на основе интеллекта сетевую безопасность ИТКС, что даст возможность опережать возникающие проблемы в области ИБ за счет как можно более тесной интеграции со всеми бизнес-процессами в ОРГАНИЗАЦИИ. Перечислены получаемыми функциональные возможности ЦИУСБ для их организаций-владельцев и четыре ключевых бизнес-процесса, реализуемые в этих центрах. Образуя говоря, ЦИУСБ – это «быстрый мозг обеспечения адаптивной упреждающей сетевой безопасности с широко открытыми глазами и умелыми руками».

6. Установлены особенности визуализации информации об ИБ и то, какая информация подлежит визуализации в типовом ЦИУСБ информация об ИБ ИТКС ОРГАНИЗАЦИИ для принятия обоснованных решений по управлению ее сетевой безопасностью обобщенно по всей ИТКС или по отдельным событиям ИБ.

7. Руководствуясь лучшими практиками построения инфраструктур для сложных сетевых систем с точки зрения выполняемых на их основе бизнес-операций и упорядочения процессов и мер обеспечения ИБ, для типового ЦИУСБ выделено пять взаимосвязанных между собой функциональных инфраструктурных уровней. Сделан вывод, что инфраструктура защищенного ЦИУСБ должна соответствовать требованиям обеспечения его ИБ с разных точек зрения – АО, ПО, технической, организационной и т.д.

8. При управлении сетевой безопасностью чем больше в ЦИУСБ ОРГАНИЗАЦИИ собрано данных для анализа, тем более качественно можно установить важные корреляции, уменьшить количество ложных срабатываний, повысить доверие к обнаруживаемым нарушениям ИБ и сократить среднее время реагирования на инциденты ИБ. С точки зрения ИБ выделено четыре типа разнородных и представленных в разных форматах данных, с которыми работают системы ИБ-аналитики ЦИУСБ, типичными представителями которых являются *SIEM*- и *SOAR*-системы. Все они вместе доказывают наличие проблем ИТ больших данных, с которыми приходится сталкиваться в ЦИУСБ.

9. При применении пакетной, потоковой и гибридной обработки к большим относящимся к ИБ данным типовой ЦИУСБ синтезирует знания об ИБ ИТКС ОРГАНИЗАЦИИ. Представлен процесс получения таких знаний, а также объяснено как использовать ИБ-аналитику в работе ЦИУСБ именно с точки зрения ИТ больших данных.

10. Для обработки относящихся к ИБ данных в типовом ЦИУСБ предлагается использовать не просто ИТ больших данных, но более современные озера данных. Выделенные в работе характеристики озер данных полностью согласуются с требованиями к ЦИУСБ ОРГАНИЗАЦИИ, сформулированными в разделе 4.7 исследования. Таким образом, озеро данных является ключевым компонентом ИБ-аналитики типового ЦИУСБ ОРГАНИЗАЦИИ.

11. В настоящее время объемы связанных с ИБ данных – это одна из проблем, но еще

большая проблема – это скорость, с которой события ИБ случаются в ИТКС. Именно поэтому большинство связанных с ИБ данных, приходящих в типовой ЦИУСБ, можно рассматривать и как быстрые данные, требующие немедленной обработки «на лету» для принятия соответствующих решений и активации ответных действий. Делается вывод, что в типовом ЦИУСБ ОРГАНИЗАЦИИ необходимо создать озеро, рассчитанное на работу с большими «сырыми» данными, большая часть из которых является быстрыми данными.

12. Проведено сопоставление ранее разработанной бизнес-логики функционирования ЦИБ, наследуемой ЦИУСБ, и упрощенной архитектуры обработки данных в ЦИУСБ. Показано, что они полностью соответствуют друг другу.

13. Определены типы контекста, в рамках которого должна проводиться ИБ-аналитика относящихся к ИБ ИТКС ОРГАНИЗАЦИИ данных.

14. Проведено сравнение базовых возможностей традиционных подходов анализа относящихся к ИБ данных в ЦМБ и ИБ-аналитики в типовом ЦИУСБ ОРГАНИЗАЦИИ, которое показало существенные преимущества ИБ-аналитики для реализации упреждающего управления сетевой безопасностью ИТКС, имеющей в своем составе ЦИУСБ.

15. Построение типового ЦИУСБ ОРГАНИЗАЦИИ в виде встроенной части ИТКС, а также централизованной, многоуровневой системы на основе современных архитектур и решений, предполагает распределение обработки относящихся к ИБ данных с выделением зон их сбора в ИТКС и собственно обработки – первоначальной у мест сбора в ИТКС и окончательной с применением ИБ-аналитики в ЦИУСБ. Следовательно, определяющими принципами разработки архитектуры обеспечения ИБ типового ЦИУСБ являются изолированность его внутренних систем и сетей от ИТКС и жесткая регламентация доступа с постоянным анализом ресурсов и услуг ЦИУСБ, к которым было обращение.

16. Системный подход к обеспечению ИБ типового ЦИУСБ требует ее поддержки на каждом из семи уровней иерархии его ИИ. Важными также являются выработка требований по обеспечению ИБ на основе специально разработанных Модели угроз ИБ и Модели нарушителей ИБ и составления реестра рисков ИБ для ЦИУСБ, а также определение процедур регулярного контроля его уровня ИБ. При таком подходе обеспечение ИБ типового ЦИУСБ рассматривается как изначальный базис его построения, позволяющий за счет такого подхода сделать ИБ не переменным качеством ЦИУСБ ОРГАНИЗАЦИИ, объективно характеризующим его способность противостоять угрозам как внешнего, так и внутреннего характера.

17. Принципиальным элементом разработанной методологии построения типового ЦИУСБ ОРГАНИЗАЦИИ является построение его адекватных моделей и происходящих в нем процессов. Основой решения этой проблемы может явиться предложенная обобщенная модель процессов обеспечения ИБ в типовом ЦИУСБ ОРГАНИЗАЦИИ, для которой указано несколько

возможных модификаций. Показано, что с помощью этой модели можно решить задачи анализа, то есть определить значения показателей защищенности информации в ЦИУСБ, синтеза и управления обеспечением ИБ в ЦИУСБ. Оговорено, что результативность практического использования данной модели существенно зависит от представительности и адекватности исходных данных. Поэтому эта модель может применяться только в совокупности с неформальными методами анализа и прогнозирования.

18. К разработанной архитектуре обеспечения собственной ИБ типового ЦИУСБ ОРГАНИЗАЦИИ применен принцип зонирования с многоуровневой сегментацией, выполняемой МЭ. Планирование зон безопасности определяется типом данных, обрабатываемых в определенной зоне, типом доступа к этим данным и процессам, выполняемым в этой зоне. Зональная архитектура обеспечения ИБ ЦИУСБ включает в себя четыре зоны (с подзонами). Показаны основные преимущества выбранной зональной сегментации и управления ЦИУСБ и роль «песочницы» в нем. Построенный таким образом ЦИУСБ также дает полную видимость всех областей деятельности персонала ЦИУСБ, объединяющего группы ИТ-специалистов и ИБ-персонала ОРГАНИЗАЦИИ.

19. Для разработанной зональной архитектуры типового ЦИУСБ указаны применимые меры и средства обеспечения ИБ, предназначенные для защиты ЦИУСБ путем обеспечения защиты ее сетевой инфраструктуры, функций устройств, информационных ресурсов и данных, управления пользователями и т.д., с указанием их расположения в зонах безопасности. В дополнение к списку СЗИ приведен еще ряд существенных замечаний, касающихся мер обеспечения ИБ в ЦИУСБ ОРГАНИЗАЦИИ.

20. Определено понятие блокчейна, которое положено в основу разработки в составе *SIEM*-системы нового поколения (3.0) для типового ЦИУСБ средства блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ для обеспечения его целостности. Показано, как происходит процесс включения блока в блокчейн, и что из себя представляют транзакции, содержащие подозрительные и «чистые» события ИБ, происходящие в ИТКС ОРГАНИЗАЦИИ. Поскольку блокчейн обновляется каждый раз, когда приходит новый блок о новых событиях в ИТКС ОРГАНИЗАЦИИ, его размер будет очень быстро расти, а *SIEM*-система 3.0 будет работать все медленнее и медленнее, то предлагается сократить необходимые ресурсы и решить проблему масштабируемости блокчейна, используя идею метода свертки.

21. Определено основное отличие по сравнению с предыдущим поколением, заключающееся в том, что *SIEM*-система 3.0 полностью дублирует возможности *SIEM*-системы 2.0 в части анализа данных, но при этом новое средство дополнительно структурирует результаты работы последней и сохраняет их в неизменном виде в блокчейне для последующего расследования

инцидентов ИБ ИТКС ОРГАНИЗАЦИИ. Также показано, как технологии блокчейна расширяют функционал *SIEM*-систем 2.0, что полностью соответствует воплощению концепции интеллектуальной безопасности. Сделан вывод, что представленный подход позволяет не просто модифицировать *SIEM*-системы, а вывести их следующее поколение на качественно новый и более высокий уровень управления событиями ИБ для ИТКС ОРГАНИЗАЦИИ в ЦИУСБ.

22. Оговорено, что построение *SIEM*-системы 3.0 с новым средством еще окончено (в конце раздела приведен список открытых вопросов, работа над которыми еще ведется), поскольку оно ведется автором исследования в одиночку, и поэтому система пока не реализована. Но в настоящее время уже понятна методика проведения оценки результативности *SIEM*-системы 3.0 с новым средством, для чего были проанализированы два подхода: *Z*-нотация и *B*-метод, которому обосновано отдано предпочтение.

23. Введено понятие *функциональной устойчивости* типового ЦИУСБ в ЕИП ОРГАНИЗАЦИИ в штатном режиме, в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций. Это активная форма устойчивости для динамической системы – ЦИУСБ ОРГАНИЗАЦИИ – в двух режимах функционирования («в малом» и «в большом»), которая должна быть изначально встроена в проект ЦИУСБ, а не добавлена в виде отдельных функции. При этом все нарушения ИБ и инциденты ИБ должны быть контролируемыми. Определены обеспечение функциональной устойчивости ЦИУСБ и управление функциональной устойчивостью ЦИУСБ как неотъемлемая часть всего процесса управления ЦИУСБ. Для этого должна быть создана система управления функциональной устойчивостью ЦИУСБ ОРГАНИЗАЦИИ с соответствующими мерами обеспечения устойчивости.

24. Даны пояснения по непрерывности функционирования типового ЦИУСБ в ЕИП ОРГАНИЗАЦИИ и ее обеспечению и управлению и показано, что ЦИУСБ для ИТКС можно рассматривать как систему высокой доступности. Наглядно показан процесс восстановления функциональной устойчивости ЦИУСБ после инцидента ИБ. Перечислены основные мероприятия, осуществляемые в рамках процесса управления функциональной устойчивостью ЦИУСБ в ЕИП ОРГАНИЗАЦИИ.

25. Особо оговорена необходимость разработки системы оценки уровня функциональной устойчивости и восстановления ЦИУСБ после нарушений и инцидентов ИБ, являющейся основой получения результатов для совершенствования и эволюционирования ЦИУСБ за счет поддержки стратегических решений, наблюдения за тактикой и обеспечением его функциональной устойчивости. Представлен начальный набор показателей функциональной устойчивости типового ЦИУСБ и на примере управления инцидентами ИБ в самом ЦИУСБ показано, как можно рассчитывать указанные показатели.

26. Упомянуты публикации, например, *CERT*, *ENISA* и *MITRE*, посвященные разработанным этими организациями показателям, которые могут быть пересмотрены применительно к функциональной устойчивости ЦИУСБ, поскольку.

27. Определен примерный состав кадрового обеспечения типового ЦИУСБ, который обычно делится на четыре линии. В качестве примера приведены роли сотрудников ГосСОПКА. Для каждой линии указаны типовые трудовые функции персонала.

28. Кратко описан международный опыт разработки документов, устанавливающих компетенции профессионалов в области ИБ, а также рассмотрены возможности российской системы высшего образования в формулировании таких компетенций. Продемонстрировано, как это может быть применено для подготовки специалистов для типового ЦИУСБ.

29. В заключении главы показано, как в типовом ЦИУСБ реализованы все сформулированные к нему общие и специальные требования, а также требования по обеспечению его собственной ИБ, и приведена структурно-логическая схема проведенного исследования, наглядно демонстрирующая преемственность полученных результатов по отношению к ранее существовавшим и их значимость для эволюции обеспечения сетевой безопасности.

ГЛАВА 6. ВНЕДРЕНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

В главе приведено краткое описание внедрения результатов диссертационной работы при разработке СОИБ для Банка России (акт головного исполнителя работ – российской компании «ЕС-лизинг»), при создании решений для ЦИУСБ организаций в регионах Восточной Европы, Кавказа и Центральной Азии (акт головного исполнителя работ – компании Qualys), при модернизации Ситуационного центра Службы ИБ Газпромбанка, при реализации типового ЦИУСБ в НИЯУ МИФИ, включая подготовку высококвалифицированных специалистов для проектирования, внедрения, сопровождения и совершенствования ЦИУСБ, в практике деятельности ООО «ЛИНС-М» при разработке средств ИБ для Банка России и стандарта обеспечения ИБ для Банка ВТБ (ПАО), а также при разработке и внедрении нормативных правовых и учебно-методических документов, регулирующих высшее образования в области ИБ, в Федеральном Учебно-методическом объединении в системе высшего образования по укрупненной группе специальностей подготовки «Информационная безопасность».

6.1. Внедрение результатов в Ситуационном центре Газпромбанка

Банк ГПБ (АО), или Акционерное Общество «Газпромбанк», является одним из трех (по размеру активов) крупнейших универсальных финансовых институтов России, в капитале которого опосредованно участвует государство. Эта кредитная организация предоставляет широкий спектр банковских, финансовых, инвестиционных продуктов и услуг корпоративным и частным клиентам, финансовым институтам, институциональным и частным инвесторам, располагает развитой сетью филиалов и дочерних банков и занимает третье место среди банков Центральной и Восточной Европы. Банк ГПБ (АО) обслуживает предприятия и компании ключевых отраслей российской экономики, именно поэтому внедрение результатов диссертационного исследования именно в этой организации является важным показателем их практической значимости.

Ситуационный центр Службы ИБ Банка ГПБ (АО) (далее – Ситуационный центр), созданный в 2010 г. и являющийся одним из наиболее развитых в России, состоит из отдела мониторинга инцидентов ИБ, реализующего первую линию ЦМБ по всем инцидентам и вторую линию по техническим инцидентам, и отдела администрирования, предоставляющего технические средства и услуги для работы отдела мониторинга. Ситуационный центр осуществляет мониторинг как инфраструктуры ИБ (виртуальные частные сети, МЭ, СПВ и т.п.), так и видит полную картину ИТКС Банка и выступает как контроль качества предоставляемых ИТ-услуг. В основе работы центра *SIEM*-система ПО *HP ArcSight ESM*, которая взаимодействует с постоянно актуализируемой базой данных управления конфигурациями (англ. *Configuration Management Da-*

tabase, CMDB) и осуществляет сбор данных с различных ИТ-источников, их нормализацию, агрегирование и корреляцию событий с признаками инцидентов. Обработка инцидентов начинается со службы технической поддержки службы ИБ Ситуационного центра и далее поступает для более интеллектуальной обработки на систему *Security BI* (от *Business Intelligence*).

В 2016 г. после шести лет существования Ситуационного центра встала необходимость его модернизации и была проведена независимая оценка зрелости, которая помогла определить зоны потенциальных улучшений. Именно с этого времени кафедра «Информационная безопасность банковских систем» НИЯУ МИФИ начала активно сотрудничать с Банком ГПБ (АО) в формировании как целевой операционной модели усовершенствования Системы выявления и обработки инцидентов (СВОИ) Ситуационного центра, включая модернизацию ИТ-архитектуры, процессную модель, оценку и расчёты достаточной численности штата, так и выработки набора отдельных рекомендаций. В СВОИ функционирует подсистема обработки инцидентов ИБ (ПСО СВОИ), которая предназначена для автоматизации деятельности сотрудников Банка ГПБ (АО), связанной с управлением конфигурациями и событиями ИБ, обработкой выявленных при помощи СВОИ инцидентов ИБ (реагированием) в самом Ситуационном центре и в рамках платежного процесса (о которых нужно отчитываться в Банк России), а также деятельности по расследованию инцидентов ИБ и подготовке отчетности по результатам их расследования, включая подготовку обязательной отчетности по инцидентам для Банка России. Для ознакомления с работой ПСО СВОИ было проанализировано, как эта подсистема осуществляет автоматизацию процесса обработки и расследования инцидентов ИБ при помощи следующих функций:

- регистрация и последующая классификация инцидентов ИБ (подозрений на инциденты) в интерактивном режиме;
- ввод информации об этапах и результатах обработки инцидентов ИБ в интерактивном режиме;
- визуализация событий ИБ и объектов инцидентов ИБ и редактирование связей инцидентов ИБ с событиями ИБ и объектами инцидентов ИБ в интерактивном режиме;
- формирование и отправка персоналу СВОИ уведомлений при наступлении определенных событий, связанных с обработкой инцидентов ИБ;
- прием сообщений об инцидентах ИБ (подозрений на инциденты) и связанных с ними событиях ИБ из смежных подсистем СВОИ;
- автоматическая регистрация в БД инцидентов ИБ и событий ИБ по принятым из смежных подсистем СВОИ сообщениям;
- передача сообщений об этапах и результатах обработки инцидентов ИБ в смежные подсистемы СВОИ;

— добавление, редактирование и поиск статей базы знаний ИБ, содержащих описания решений инцидентов ИБ и прочую справочную и вспомогательную информацию;

— формирование отчетов по инцидентам ИБ, событиям ИБ и действиям сотрудников в рамках ПСО, сохранения отчетов в файл и печати отчетов.

После этого была определена основная цель внедрения результатов данного диссертационного исследования в Ситуационном центре как выработка рекомендаций по повышению результативности его функционирования. Так, в рамках расширения Ситуационного центра с учетом созданного в 2016 г. проекта развития функций реверс-инжиниринга Ситуационного центра было предложено при модернизации центра внедрить технологию «песочницы», а в сфере *Threat Intelligence* Ситуационный центр стал выступать как потребитель различных бесплатных и платных подписок на информацию об угрозах ИБ.

Для СВОИ Ситуационного центра совместно с сотрудниками Банка ГПБ (АО) были проанализированы настройки подсистемы сбора и анализа (ПСИА) головного офиса (ГО), проверена актуальность версий компонентов ПСиА ГО, проведена диагностика ПО *HP ArcSight ESM* и входящих в него компонентов, включая анализ журналов и ошибок ПО, настройки контента, конфигурации менеджера и БД, соответствие рекомендациям производителя по защите данных и т.п., проанализированы типовые собираемые события ИБ, включая анализ текущих настроек по фильтрации и агрегирования событий на коннекторах *HPE ArcSight SmartConnectors*, после чего были подготовлены рекомендации по дальнейшему развитию ПСиА ГО. Среди них, в частности, следующие (более специфические рекомендации здесь не приводятся в целях неразглашения конфиденциальной информации):

— произвести инвентаризацию ресурсов ИТКС, подлежащих защите, пересмотрев модели угроз и нарушителей ИБ;

— подключить интерфейсы удаленного управления серверов (*iLO*) в локальную сеть, что обеспечит возможность оперативной диагностики и решения возникающих проблем с оборудованием, и настроить отправку событий *iLO* по протоколу *syslog* в СВОИ;

— развернуть стандартный пакет мониторинга устройств сбора событий и коннекторов на базе пакета *System Monitoring*;

— произвести оптимизацию работы правил коннекторов, включая оптимизацию условий выборки и метода срабатывания, замену использования локальных переменных на глобальные, где применимо, и т.п.;

— провести инвентаризацию подключенных агентов сбора событий и удалить те, которые более не используются;

— распределить нагрузку между всеми серверами агентов;

— перейти на более быстрые диски, например, *Solid-State Drive (SSD)*, поскольку СВОИ

расширяется, и количество собираемых событий растет;

- использовать системы резервного копирования, включая периодическое выполнение тестового восстановления из резервных копий;

- в регионах установить экспресс-редакцию *SIEM*-системы и оттуда в ГО пересылаются не «сырые», а уже отфильтрованные данные, для чего на высоконагруженных и кеширующих коннекторах применить фильтрацию и агрегирование;

- произвести анализ событий, поступающих от источников с наибольшим количеством событий, на предмет использования их ресурсами СВОИ; оставить только необходимые, к остальным применить правила фильтрации на коннекторах;

- использовать ресурс *Trends*, что позволит снизить нагрузку на БД Системы за счет разбиения одного запроса к БД за продолжительный промежуток времени на несколько таких же запросов, но за меньший промежуток (например, запрос на выборку за неделю может быть заменен на семь запросов, которые будут выполнены в наименее нагруженный период, каждый из них выбирает информацию за один день);

- провести оптимизацию работы ресурса *Active Channel*, например, использовать фильтры с наиболее частотными условиями выборки вместо указания их в условиях выборки в самом *Active Channel*, формировать условия выборки согласно определенным правилам и использовать необходимый временной промежуток для построения *Active Channel* (использование временной метки *Attacked Time*);

- применять политику использования централизованного хранения высокочастотных условий выборок, используя ресурсы системы *Filters*;

- проанализировать условия срабатываний правил, которые создают кейсы, и произвести их переработку и оптимизацию с указанием исключений из работы правила;

- организовать получение инцидентов ИБ, передаваемых в подсистему мониторинга СВОИ из ПСО СВОИ и из ПСиА СВОИ через интеграционную шину СВОИ посредством сообщений в универсальном формате обмена СВОИ;

- добавить возможности поиска решений по закрытым инцидентам ИБ и более активно использовать шаблоны инцидентов ИБ, что можно автоматизировать при помощи написания соответствующего скрипта;

- внедрить технологию централизованного сбора событий *Microsoft Windows Event Forwarding* для реализации сбора локальных событий со всех узлов – серверов и рабочих станций – ОС *Windows* с помощью *Windows Remote Management (WinRM)* и их пересылки на основе протокола *http/https*. При этом мониторинг событий в ОС *Windows* выполняется удаленно. Сбор событий осуществляется с использованием агентов *SmartConnector for Microsoft Windows Event Log – Native*, которые устанавливаются на сервере коннекторов. Для работы с журналом собы-

тий *Eventlog*-агент использует интерфейс *Microsoft API*. Агент выполняет сбор событий из журналов *HardwareEvents* сервера *Event Collector*. Для организации доступа в домене создается учетная запись с правами «Пользователь домена» (рекомендуемое имя – *arcsight*), которая добавляется в группу безопасности *Event Log Readers*;

— использование средства мониторинга состояния работоспособности компонент *HP ArcSight* на базе ПО *SOC Prime* – системы анализа работы *SIEM*-системы с обязательным маскированием конфиденциальной информации в обрабатываемых данных, автоматическим оповещением о таких событиях как, остановка или сбой в работе любого из компонентов, подключенного к мониторингу; критическая ошибка, которая может привести к непредвиденной остановке работы компонентов; потеря сетевого соединения между компонентами или между компонентами и источниками журналов регистрации событий и т.п. и автоматической выдачей рекомендаций по устранению критических ошибок, которые влияют или могут влиять на работу компонентов *SIEM*-системы;

— отключить те ресурсы Системы, которые не используются.

Таким образом, для развития Ситуационного центра были внедрены следующие результаты диссертационного исследования:

— методология и принципы построения ЦИУСБ как современного решения, предназначенного для управления нарушениями и инцидентами ИБ и таким образом снижающего операционные риски для ИТКС АО;

— построение ЦИУСБ с точки зрения обеспечения его функциональной устойчивости, реализованная, в частности, за счет использования предложенных диссертантом решений для конкретной исторически сложившейся среды функционирования ИТКС Банка:

1) системы анализа аномального трафика на базе решения *Cisco StealthWatch*, которая с помощью *Netflow* и других телеметрических данных, полученных из существующей крупномасштабной ИТКС, позволяет контролировать сетевое взаимодействие компонентов ИТКС Банка и выявлять в них *DDoS*-атаки, *APT*-атаки, различные аномалии и вредоносную активность для ускорения и более точного обнаружения угроз ИБ, реагирования на инциденты ИБ и проведения их расследований;

2) системы выявления уязвимостей на базе решения *SkyBox Vulnerability Control*, которая обеспечивает непрерывное управление и приоритезацию выявленных уязвимостей и моделирование атак при эксплуатации каждой найденной уязвимости при полной видимости ИТКС Банка;

3) системы выявления аномального поведения пользователей и устройств в ИТКС на базе решения *Exabeam*, относящегося к классу *UEBA* и позволяющего создавать профили работы пользователя, а также обнаруживать злоупотребления правами доступа на основе построения

моделей поведения пользователей и групп;

4) многоуровневой защиты почтового канала, включающей спам-фильтр, почтовый антивирус, средство защиты от атак «нулевого дня» и *PT MultiScanner* (многовендорный антивирус на базе решения компании *Positive Technologies*);

5) *NGFW* на базе решения *CheckPoint* — виртуальных комплексов ПО, устанавливаемых на аппаратные решения компании *Check Point* и осуществляющих сложную фильтрацию сетевого трафика и разграничение доступа пользователей и сервисов ИТКС Банка.

Результирующая схема после модернизации СВОИ в виде СВОИ 2.0 представлена на рис. 56 (схема предоставлена Ситуационным центром Службы ИБ Банка ГПБ (АО)).

Акт о внедрении материалов диссертационного исследования в Банке ГПБ (АО) приведен в Приложении А.

6.2. Внедрение результатов в Банке России

В создании информационно-телекоммуникационной системы (ИТС) Банка России активное участие принимала российская компания ЗАО «ЕС-лизинг». Основанная в 1994 г. на базе Научно-исследовательского центра электронной вычислительной техники (НИЦЭВТ), она специализируется в области разработки программных и аппаратных СВТ, являясь бизнес-партнером IBM, и создания прикладных программных продуктов в области ИТ по заказам российских и зарубежных компаний и организаций. Среди заказчиков ЗАО «ЕС-лизинг» – ОАО «Российские железные дороги», ПАО «Газпром», Министерство сельского хозяйства России, Министерство цифрового развития, связи и массовых коммуникаций РФ (Минкомсвязи) и многие другие.

Начиная с 2002 г. в интересах Банка России ЗАО «ЕС-лизинг» были созданы типовые проекты вычислительных центров регионального уровня, Система Консолидации Серверов и Данных (СКСД), спроектированы на принципах консолидации, высокой доступности, катастрофоустойчивости и обеспечения ИБ Коллективные Центры Обработки Информации (КЦОИ), а также спроектированы и внедрены Системы Автоматизированного Тестирования (САТ) и СОИБ.

Исходные данные для определения области внедрения результатов диссертационного исследования были предоставлены Департаментом информатизации и телекоммуникаций (ДИТ) России и информационно-вычислительными подразделениями Банка России – Центром информационных технологий (ЦИТ), Межрегиональным центром информатизации (МЦИ) и Технологическим центром (ТЦ) «Нудоль» Банка России.

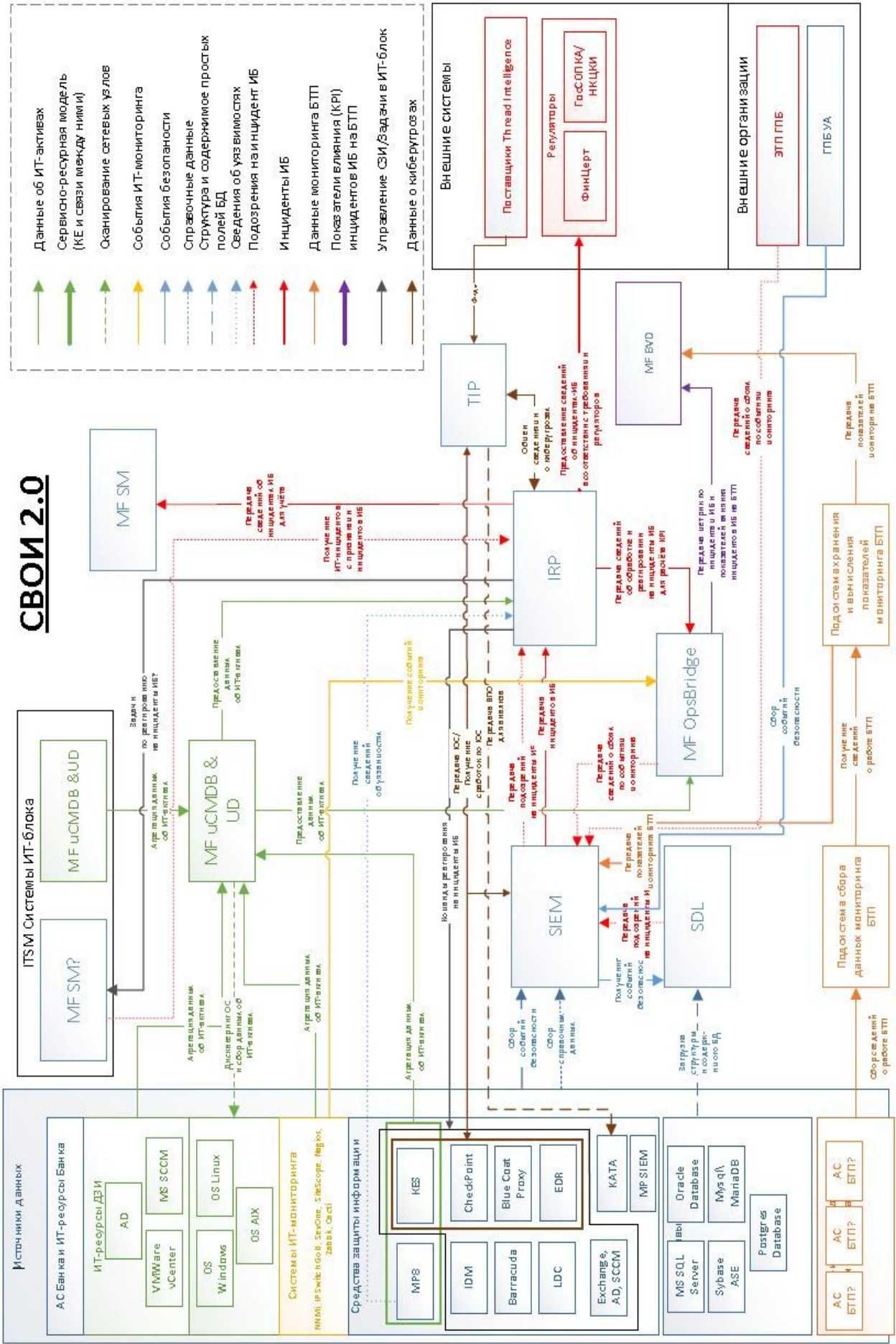


Рисунок 56 – Модернизированная СВОИ 2.0 Банка ГПБ (АО)

В связи с ростом сложности применяемых технологий и архитектуры ИТС Банка России, его потребностей в оперативности предоставления защищенных сервисов ИТС и объемов обрабатываемой и передаваемой по ИТС информации, требующей обеспечения ИБ, а также необходимостью минимизации рисков, связанных с применением ИКТ, стало необходимым внедрение результатов диссертационного исследования в проектно-конструкторскую деятельность ЗАО «ЕС-лизинг» в интересах Банка России при разработке СОИБ ИТС, которое осуществлялось по двум основным направлениям, а именно:

1) общесистемного проектирования центров управления инцидентами ИБ для ЦОД заказчиков на базе типового ЦИУСБ как комплексного системотехнического решения, обеспечивающего снижение операционных рисков при развертывании современных средств обеспечения сетевой безопасности в зонах безопасности ЦИУСБ, ориентированных на создание комплексной СОИБ ИТКС заказчиков;

2) реализации концепции функциональной устойчивости ЦИУСБ, заложенной в сам проект типового ЦИУСБ и реализованной для ИТКС заказчиков, в частности, за счет использования следующих конкретных решений в зонах безопасности ЦИУСБ:

— аппаратные МЭ с отслеживанием состояния соединений и глубоким анализом протоколов прикладного уровня *Cisco ASA (Adaptive Security Appliance)* компании Cisco Systems;

— многофункциональная система управления доступом к корпоративной сети на базе *Cisco ISE (Identity Services Engine)*, связывающая систему хранения данных о пользователях (типа *Microsoft Active Directory*, LDAP-сервера, активных каталогов почтового сервера и т.п.) и сеть;

— система мониторинга сетевыми устройствами *Cisco Prime Infrastructure*, из единого центра управляющая локальными и беспроводными сетями, в частности, контролирующая состояние сети и обеспечивающая гарантированный доступ ко всем приложениям, оптимизируя работу конечных пользователей;

— ПО *HP Network Automation* компании Hewlett-Packard, предоставляющего в режиме реального времени информацию об управляемой ИТКС, возможность автоматизированного управления и внесения изменений в конфигурации сетей, построенных на оборудовании различных производителей;

— платформа для операционной аналитики *Splunk Enterprise* компании Splunk, осуществляющая поиск, отслеживание, анализ (с учетом исторических данных и корреляции сложных событий) и визуализацию данных для последующего принятия бизнес-решений за счет анализа транзакции пользователей, их поведения и поведение устройств, а также создания настраиваемых интерактивных панелей мониторинга для отслеживания инцидентов ИБ, уровней обслуживания и других ключевых показателей производительности;

— российская *DLP*-система *InfoWatch Traffic Monitor*, предотвращающая утечки конфиденциальной информации на основе полноценного анализа содержимого информационных потоков (собранных по сети и с агентов), с компонентой *InfoWatch Device Monitor*, отвечающей за управление агентами;

— почтовый шлюз *hMail Server* под платформу *Windows*, включающий в себя инструменты администрирования и резервного копирования и производящий авторизацию пользователей через *Active Directory*;

— файловый шлюз *Vaultize* одноименной компании, являющийся единой централизованной платформой для контроля и управления доступом к данным, имеющей *DLP*-коннектор, ограничивающей возможности получателя документа с учетом геолокации, количества открытий и времени доступности защищенного документа и т.п.;

— российское решение для централизованного управления комплексной системой защиты *Kaspersky Security Center*, предоставляющее администратору доступ к детальной информации об уровне безопасности корпоративной сети и позволяющее гибко настраивать все компоненты системы защиты для нее, включая облачные, физические и виртуальные машины, а также мобильные устройства.

В рамках Договора № Л201711 от 2017 г. между ЗАО «ЕС-лизинг» и Банком России при участии диссертанта осуществлялась разработка специализированной подсистемы управления и мониторинга средствами защиты информации от НСД КЦОИ-2. Эта подсистема является одной из основных в составе СОИБ ИТС. Ранее определяющим принципом построения СОИБ в ИТС была определена реализация многоуровневой защиты информации, на каждом уровне которой были предложены различные средства обеспечения ИБ. При этом уровни в соответствии с моделью взаимодействия открытых систем *OSI/ISO* устанавливались таким образом, чтобы они были независимы друг от друга с точки зрения поддержания ИБ. Инфраструктура иерархической СОИБ ИТС с набором необходимых подсистемы (межсетевого экранирования (создавалась в 2009 г.), защиты от НСД и вредоносного ПО, защиты прикладного уровня, защиты коммуникаций и т.п.) разрабатывалась как специализированный комплекс организационных, технических, криптографических и технологических мероприятий и средств, обеспечивающих ИБ информации на всех этапах жизненного цикла ИТС. Основы построения СОИБ ИТКС Банка России, включающие в себя системный подход, средства и уровни обеспечения ИБ ИТС БР представлены на рис. 57. Как видно, важной составляющей были определены процедуры контроля (в том числе мониторинга ИБ), регулярное проведение которых позволяло бы адекватным образом реагировать на постоянные изменения, происходящие во внешних и внутренних угрозах ИБ ИТС.

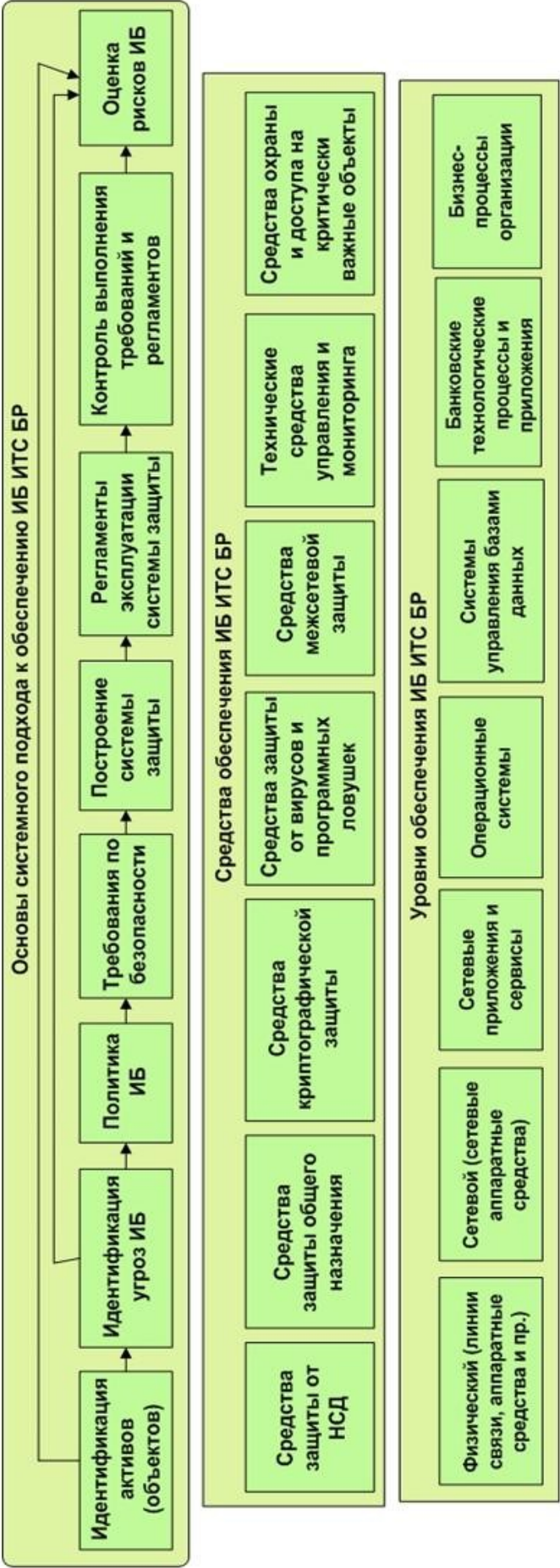


Рисунок 57 – Основы построения СОИБ ИТС Банка России

На этой же основе в 2011 г. в рамках Договора № 00-7-044-0475 между Банком России и НИЯУ МИФИ был разработан тренинговый модуль «Информационно-телекоммуникационная системы Банка России. Структура, составные части, функции, задачи» (ТМ ИТС БР), который предназначен для руководящих работников Банка России, специалистов и разработчиков отдельных систем (сетей) и подсистем для формирования общего представления об ИТС при создании, модернизации и совершенствовании средств информатизации, а также в качестве вспомогательного средства информационного обеспечения для повышения квалификации специалистов региональных учреждений и организаций. Основной целью создания ТМ ИТС, размещенного в Автоматизированной тренинговой системе (АТС), являлось повышение эффективности использования и совершенствования ИТС БР за счет формирования у пользователей ТМ ИТС компетенций в области организации функционирования ИТС БР. Использование ТМ ИТС сократило временные и материальные затраты на тренинговую подготовку (переподготовку) специалистов структурных подразделений на рабочих местах по единой, унифицированной для Банка России, дистанционной технологии.

В 2018 г. ЗАО «ЕС-лизинг» открыла Центр компетенции по технологии IBM Big Data, в 2019 г. выступила партнером восьмого делового форума Big Data 2019, что иллюстрирует ее вовлеченность в такое направление деятельности как применение аналитики больших данных. В Центре компетенции решаются такие задачи, как хранение и обработка больших данных, объем которых не позволяет эффективно управлять ими с помощью реляционных БД, работа с неструктурированной информацией (текстами на естественном языке, изображениями и видео), а также анализ больших данных для построения отчетов, создания и внедрения прогнозных моделей. Основная цель анализа больших относящихся к ИБ ИТКС данных – помочь руководству компании принимать более взвешенные решения в области обеспечения ИБ, позволяя анализировать огромные объемы данных из гетерогенных источников, которые не могут быть использованы обычными программами бизнес-аналитики (BI). А основная задача обработки таких больших данных, включая неструктурированные, заключается в выявлении повторяющихся бизнес-моделей при эффективном хранении данных и обеспечение управляемости при распределенной обработке в режиме реального времени, что в случае несоблюдения может повлечь привлечение к ответственности, если требуемая информация не может быть представлена в случае аудита ИБ или судебного разбирательства. Данные вопросы также рассматривались в рамках диссертационного исследования, и поэтому третьим направлением внедрения результатов диссертационного исследования в проектно-конструкторскую деятельность ЗАО «ЕС-лизинг» в интересах его заказчиков было использование в проектах для заказчиков разработанной диссертантом архитектуры хранения больших относящихся к ИБ ИТКС данных в виде «озер данных», рассчитанной и на работу с быстрыми данными, что требуется для интеллекту-

ального анализа в определенном контексте всех имеющихся в распоряжении заказчиков «сырых» и исторических данных о событиях ИБ в их ИТКС и реализации упреждающего подхода для предотвращения инцидентов в ИТКС, нарушающих устойчивое и защищенное функционирование ЦИУСБ, а, значит, и ИТКС организации.

При внедрении результатов своего исследования в ЗАО «ЕС-лизинг» диссертантом были пересмотрена разработанная архитектура хранения больших относящихся к ИБ ИТКС данных, представленная в [180], и в нее были внесены уточняющие дополнения и изменения, касающиеся процессов обработки больших и быстрых данных, что нашло отражение на обновленной схеме рис. 44. Акт головного исполнителя работ – ЗАО «ЕС-лизинг» – о внедрении материалов диссертационного исследования приведен в Приложении Б.

6.3. Внедрение результатов в компании Qualys

Основания в 1999 г. компания Qualys является одним из ведущих поставщиков облачных решений для обеспечения ИБ и контролю соблюдения требований по обеспечению ИБ, услугами которой пользуются более 5500 клиентов в 85 странах мира. Продукты платформы *QualysGuard* этой компании осуществляют автоматизацию всего спектра задач аудита ИБ и контроль защищенности ИТ-систем и веб-приложений. Кафедра «Информационная безопасность банковских систем» НИЯУ МИФИ имеет давние партнерские отношения с компанией Qualys, которые начались с того, что в 2014 г. диссертант прошла обучение по продуктам платформы *QualysGuard*, подтвержденное соответствующими сертификатами. Позже результаты ее диссертационной работы были внедрены в проектно-конструкторскую деятельность компании Qualys в регионах Восточной Европы, Кавказа и Центральной Азии при разработке и реализации проектов для ряда организаций-заказчиков (названия организаций не разглашаются в соответствии с условиями сотрудничества с этими организациями), а именно:

— зональная архитектура обеспечения ИБ ЦИУСБ с эшелонированной защитой и жесткой регламентацией доступа к ресурсам и услугам различных зон безопасности, которая была реализована с использованием, кроме прочего, облачного МЭ *QualysGuard Web Application Firewall (WAF)*, осуществляющего защиту веб-приложений в режиме реального времени за счет блокировки соответствующих атак на веб-сайты заказчиков, а также повышающего производительность веб-сайтов за счет применения кэширования, сжатия и оптимизации контента, а также решения *QualysGuard® Policy Compliance (PC)*, уменьшающего риск реальных внешних и внутренних угроз ИБ и в то же время предоставляющего свидетельства соответствия требованиям регуляторов по обеспечению ИБ и выполнения требований политик ИБ заказчика, подтверждая это документально соответствующими отчетами;

— размещение «песочницы» в ДМЗ ЦИУСБ для исследования подозрительного ПО от непроверенных третьих лиц, пользователей, веб-сайтов и т.д., поступающих в ИТКС заказчика из внешних открытых сетей, на основе применения сервиса обнаружения вредоносного ПО *QualysGuard® Malware Detection Service (MDS) Enterprise Edition*, осуществляющего регулярное сканирование с автоматическим оповещением об обнаружении заражения или подозрения на заражение;

— развертывание в зонах безопасности ЦИУСБ современных средств обеспечения сетевой безопасности, ориентированных на создание комплексной СОИБ ИТКС заказчиков, включая облачный сканер анализа защищенности *QualysGuard® Web Application Scanning (WAS)*, идентифицирующий с низким процентом ложных срабатываний уязвимости веб-приложений, приводящие, например, к атакам типа «отказ в обслуживании», *SQL*-инъекции, межсайтовый скриптинг (*XSS*), перенаправление *URL* и т.п., а также средство управления уязвимостями в масштабах предприятия *QualysGuard® Vulnerability Management (VM)*, в том числе обнаруживающее и отображающее активы и оценивающее уязвимости с точки зрения бизнес-рисков.

Такой вариант реализации ЦИУСБ с использованием ряда СЗИ в виде аутсорсинговых решений типа «ПО как услуга» (англ. *Software-as-a-Service, SaaS*) как раз подходит заказчикам, у которых в силу разных обстоятельств не достаточно возможностей для их размещения или самостоятельного поддержания.

Акт головного исполнителя работ – компании Qualys – о внедрении материалов диссертационного исследования приведен в Приложении В.

6.4. Реализация типового ЦИУСБ в НИЯУ МИФИ

Для проверки работоспособности и совершенствования концепции ЦИУСБ в Институте кибернетических интеллектуальных систем (ИИКС) НИЯУ МИФИ в 2016 г. было начато внедрение Учебно-научного центра «Интеллект в управлении сетевой безопасностью» (УНЦ) в составе трех учебно-научных лабораторий – «Предотвращение утечки конфиденциальной информации», «Межсетевые экраны нового поколения» и «Управление информацией и событиями безопасности» (рис. 56). Сначала была развернута первая лаборатория, созданная вокруг *DLP*-системы компании «СёрчИнформ» [51]. Через два года была оснащена вторая лаборатория на базе *Palo Alto NGFW* [50]. В настоящее время ведется создание третьей лаборатории с «СёрчИнформ SIEM» в качестве ее ядра, что было временно остановлено в связи с возникшими обстоятельствами – пандемией коронавируса. При этом активно использовались лучшие практики и рекомендации, например, компаний *MITRE*, *SANS* и *Cisco* по созданию центров мониторинга кибербезопасности [190, 203].

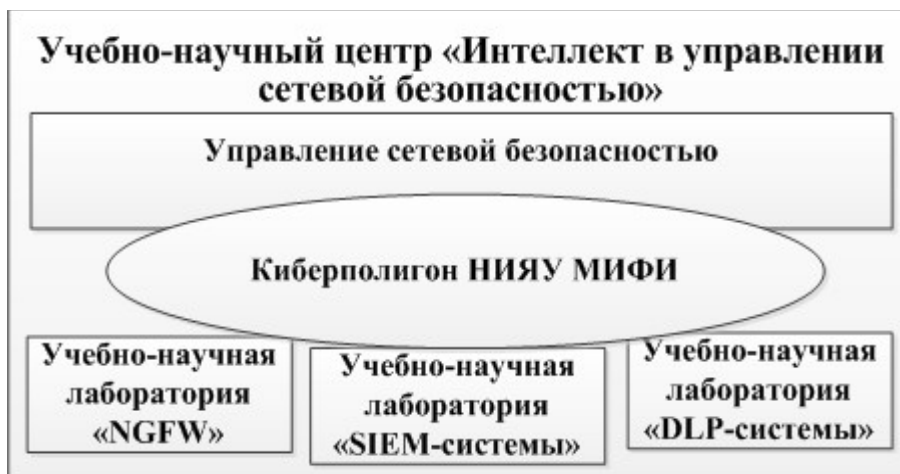


Рисунок 56 – Структура Учебно-научного центра «Интеллект в управлении сетевой безопасностью» НИЯУ МИФИ

Среди полезных уроков, которые были полученных во время разворачивания УНЦ, особо нужно отметить, например, такие: «Важно правильно организовать сбор и хранение данных», «Эффективность СЗИ зависит от качества и объема данных», «Агрегирование «сырых» данных позволяет выйти из положения при отсутствии единого стандарта данных», «СЗИ и средства управления сетью не взаимозаменяемы, а дополняют друг друга», «День на установку СЗИ, год на его настройку под конкретную среду», «Использование любого нового СЗИ порождает новые процессы, которыми нужно грамотно управлять» и многие другие.

При реализации УНЦ обеспечение его собственной ИБ было поставлено в центр внимания [50, 51]. На основе комплексного анализа уровня ИБ компьютерной сети ИИКС и, в частности, кафедры «Информационная безопасность банковских систем», что включало изучение ЖРС СЗИ, использование САЗ и пр. С использованием общих подходов инвентаризации и категорирования информационных активов в качестве начальных этапов оценки рисков ИБ в первую очередь были определены все информационные ресурсы, подлежащие защите в рамках будущего УНЦ. Это конфиденциальные данные, используемые в типичной сети учебного заведения, например, служебная информация ограниченного распространения, конфиденциальная информация, связанная с деятельностью самого центра, персональные данные его сотрудников и обучающихся, учебные и тестовые материалы, защищенные авторским правом, ключевая информация, учетные данные, пароли и т.д. После этого были написаны две обобщенные модели ИБ для УНЦ: Модель угроз ИБ и Модель нарушителей ИБ. Далее на этой основе были разработаны политики ИБ и соответствующие процедуры и регламенты, включая следующие области их действия: использование действующих СЗИ и мер обеспечения ИБ», организация мониторинга ИБ и аудита ИБ, обработка события ИБ и инцидентов ИБ, управление уязвимостями, управление конфигурационными настройками и их изменениями, регистрация активности

пользователей, фильтрация входящего и исходящего трафика, защита от компьютерных вирусов и несанкционированного изменения ПО, контроль использования портов компьютеров УНЦ, защита от *DoS*-атак, защита от несанкционированного сканирования.

Далее началось разворачивание самого УНЦ с учетом начальных требований, перечисленных выше. Появление УНЦ позволило на провести апробацию предлагаемых в данном исследовании архитектурных решений и показало их состоятельность для обеспечения ИБ и функциональной устойчивости ИТКС ИИКС НИЯУ МИФИ. Кроме этого, на более высоком качественном уровне стали проводиться учебные занятия и научные исследования (в рамках практик и выполнения выпускных квалификационных работ) студентов по созданию систем управления сетевой безопасностью ИТКС, методам результативного управления сетевой безопасностью ИТКС на основе применения интеллектуальных подходов, использованию технологии больших данных для обработки связанной с ИБ ИТКС информации, исследованию вопросов совместимости средств обеспечения сетевой безопасности и выработки рекомендаций по решению возникающих в связи с этим проблем, а также оценке защищенности ИТКС. В качестве примера приведем несколько названий выпускных квалификационных работ (ВКР) магистров и дипломных работ специалистов, выполненных под руководством диссертанта и имеющих большое научное и практическое значение:

— «Обеспечение информационной безопасности и непрерывности функционирования информационной системы <Организации> на основе использования межсетевого экрана следующего поколения»;

— «Разработка архитектуры защищенного территориально распределенного интранета <Организации> с использованием нескольких демилитаризованных зон»;

— «Разработка моделей угроз и частных политик обеспечения информационной безопасности для интранета <Организации>, использующего межсетевые экраны для построения виртуальных частных сетей»;

— «Разработка контрольных мероприятий внутреннего аудита информационной безопасности для оценки защищенности интранета <Организации>, использующего межсетевой экран»;

— «Разработка тестов на проникновение для оценки защищенности интранета <Организации>, использующего межсетевой экран следующего поколения»;

— «Разработка документального обеспечения для использования межсетевого экрана типа *WAF* при обеспечении информационной безопасности и непрерывности функционирования веб-сайта <Организации>»;

— «Использование межсетевых экранов для защиты *IoT*»;

— «Исследование вопросов применения нейронных сетей для усовершенствования технологии межсетевого экранирования»;

— «Исследование вопросов применения глубокого обучения для усовершенствования технологии межсетевого экранирования».

Также была реализована бизнес-логика функционирования УНЦ, которая была успешно протестирована после в реальной сетевой среде – интранете кафедры. Ядро системы представляет собой программный модуль, написанный на *Visual Basic*, который реализует описанную логику и объединяет вместе все системные элементы (такие как пользовательский интерфейс, хранилище данных, модуль аутентификации, модуль установки параметров ПО, модуль конфигурации СЗИ, аналитический модуль и т.д.).

В настоящее время на базе УНЦ разрабатывается проект развертывания киберполигона (рис. 54). В инфраструктуре УНЦ он является четвертой виртуальной лабораторией, в некотором смысле объединяющей три уже созданных лаборатории и взаимодействующей со средствами управления сетевой безопасностью УНЦ. Зональная архитектура обеспечения ИБ ЦИУСБ как раз хорошо подходит под деление УНЦ на разные зоны безопасности. В рамках киберполигона обучающиеся получают следующие основные профессиональные компетенции (ПК): развитие навыков обнаружения компьютерных атак; развитие навыков расследования инцидентов ИБ; развитие навыка оценки ИБ элементов сетей; развитие навыков взаимодействия между отделами организации; разработка рекомендаций по нейтрализации компьютерных атак; разработка мер профилактики компьютерных атак. Таким образом, студенты, прошедшие практическую подготовку на киберполигоне, приобретут основные знания и навыки (так называемые *Hard Skills*), а именно знания технологий атаки и защиты, знания и умения использовать необходимые СЗИ и другие инструментальные средства, а также другие навыки (называемые *Soft Skills*), включая навыки работы в команде, умение взаимодействия с другими членами групп реагирования и мониторинга и навыки управления временем выполнения поставленных задач. Перечисление АО и ПО, составляющего основу киберполигона, намеренно опущено, поскольку оно пока окончательно не закуплено в связи с известными мировыми трудностями. (Статья о киберполигоне, написанная диссертантом в соавторстве, принята к печати, но пока не опубликована.)

Современное обучение высококвалифицированных специалистов базируется на так называемом компетентностном подходе, когда результат обучения формулируется в виде перечня ПК, которые должен приобрести обучающийся и которые должны определить его способность применять знания, умения, навыки и личностные качества для успешной деятельности в определенной области [294-296]. Согласно такому подходу штат типового ЦИУСБ должен быть укомплектован специалистами с соответствующей подготовкой и определенными квалифика-

ционными характеристиками и ПК, демонстрирующими их способность поддерживать функционирование ЦИУСБ и выполнять конкретную работу в сфере управления сетевой безопасностью ИТКС. Еще более важно подготовить высококвалифицированных специалистов для проектирования, внедрения и совершенствования ЦИУСБ на всех стадиях их жизненного цикла, а не только его сопровождения. В 2015 г. на кафедре «Информационная безопасность банковских систем» ИИКС НИЯУ МИФИ в рамках направления «Информационная безопасность» была начата подготовка магистров по образовательной программе «Обеспечение непрерывности и информационной безопасности бизнеса». Анализ существовавших к тому времени учебных программ показал отсутствие в России и в мире тоже аналогичной программы, хотя уже с конца 1990-х годов стало очевидным, что для успешной деятельности любой организации необходимо, чтобы ее работники владели знаниями в двух взаимозависимых областях – обеспечение ИБ и непрерывности бизнеса (НБ). Причем уже тогда были и сейчас в еще большей степени востребованы профессионалы, обладающие интегрированными знаниями, умениями и навыками. Также необходимо было учесть, что длительная подготовка кадров с высшим образованием не могла обеспечить требуемую адаптацию содержания обучения к динамично изменяемой области профессиональной деятельности, к которой относится обеспечение ИБ и НБ (например, в отношении появления новых угроз, возникновении новых ИКТ и т.п.).

В связи с этим в НИЯУ МИФИ в 2010-2012 гг. была разработана выше названная образовательная программа [42, 43, 298]. Причина создания программы, предназначенной для подготовки именно магистров, объясняется следующими факторами:

- малая длительность обучения (два года), что очень важно в условиях острой нехватки профессионалов данного направления;
- вариативность формирования учебного плана – до 50 % учебного времени изучаются учебные дисциплины, формируемые самим образовательным учреждением и непосредственно относящиеся к области профессиональной деятельности – обеспечению ИБ и НБ;
- гибкость реализации учебного плана – до 15 % учебного времени занимают так называемые «дисциплины по выбору», которые обучающийся выбирает самостоятельно;
- практическая направленность обучения – до 25 % учебного времени отдано прохождению различных практик, выполнению научно-исследовательской работы и подготовке выпускной квалификационной работы.

Область профессиональной деятельности выпускников магистерской программы определена как сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением непрерывности и ИБ основных бизнес-процессов организаций, в условиях существования угроз в информационной сфере. Это полностью согласуется с тематикой диссертационного исследования.

Объекты профессиональной деятельности выпускника магистерской программы – это информационные ресурсы и ИТ, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие основные бизнес-процессы организации, а также технологии обеспечения непрерывности и ИБ основных бизнес-процессов организации. Вывод о полном соответствии с тематикой диссертационного исследования очевиден.

Виды профессиональной деятельности выпускника также соответствуют данной тематике (раздел 5.7):

— организационно-управленческая – персонал четвертой линии – решение в том числе следующих задач профессиональной деятельности: участие в работах по созданию СУИБ, разработка проектов методических и нормативных документов, предложений и мероприятий по обеспечению непрерывности и ИБ ИТКС ОРГАНИЗАЦИИ, организация и контроль реализации контрольных мероприятий по оценке эффективности СОИБ, организация работ по совершенствованию, модернизации и унификации СОИБ в соответствии с нормативными актами и требованиями и т.п.;

— научно-аналитическая и проектная – персонал третьей линии – решение в том числе следующих задач профессиональной деятельности: системный анализ прикладных областей использования ИТКС ОРГАНИЗАЦИИ, выявление угроз («охота за грозами») и оценка уязвимостей ИС ИТКС, разработка требований и критериев обеспечения непрерывности и ИБ ИТКС, концептуальное проектирование систем и комплексов средств для ИТКС, обоснование выбора функциональной структуры, принципов организации технического, программного и информационного обеспечения систем, средств и технологий обеспечения непрерывности и ИБ для ИТКС, адаптация в конкретной ИТКС современных методов обеспечения непрерывности и ИБ на основе отечественных и международных стандартов и т.п.;

— контрольно-аналитическая – персонал первой и второй линий – решение в том числе следующих задач профессиональной деятельности: документирование контрольно-аналитических мероприятий, разработка планов проведения контрольно-аналитических мероприятий; контроль эффективности применяемых мер обеспечения непрерывности и ИБ ИТКС ОРГАНИЗАЦИИ, реализация программ аудита ИБ СОИБ и т.д.

Отметим, что данное деление обосновывает достаточность трех линий для персонала типового ЦИУСБ, как это предложено в проекте ГОСТ Р [286].

Освоение магистерской программы направлено на формирование у выпускников способности, среди прочего, принимать участие в разработке, эксплуатации и совершенствовании СОИБ и СУИБ для ИТКС ОРГАНИЗАЦИИ, включая подготовку соответствующей документации, планировать и организовывать исследование объектов защиты, на практике применять

стандарты, относящиеся к обеспечению ИБ и НБ, проводить оценку рисков с целью обеспечения ИБ и НБ, участвовать в проектировании и эксплуатации системы управления инцидентами ИБ организации, проводить инструментальный мониторинг ИБ ИТКС ОРГАНИЗАЦИИ и многое другое.

Эти ПК формируются при реализации конкретного учебного плана, среди основных учебных дисциплин которого можно выделить авторские курсы автора диссертационного исследования, а именно «Технологии обеспечения информационной безопасности объектов» (преподается с 2015 г., первоначально под названием «Информационная безопасность открытых систем. Часть 1. Угрозы, уязвимости, атаки и подходы к защите»), «Защищенные информационные системы» (преподается с 2015 г. первоначально под названием «Информационная безопасность открытых систем. Часть 2. Средства защиты в сетях»), «Основы управления рисками» (преподается с 2015 г.), «Основы управления инцидентами» (преподается с 2015 г.) и «Оценка защищенности информационных технологий» (преподается с 2015 г.).

Для каждой из названных учебных дисциплин разработан комплект учебно-методических материалов, которые можно рассматривать как типовые. В поддержку лекций были написаны учебники и учебные пособия, получившие грифы Министерства образования и науки РФ и УМО по образованию в области ИБ (например, [55, 132, 134-137, 139, 168, 171, 172]). Для учебника на английском языке в поддержку летних школ для студентов Европейского сообщества под названием «Интенсивная программа «Безопасность информационных и коммуникационных технологий» (англ. *Intensive Programme on Information and Communication Technologies Security, IPICS*) была в соавторстве написана глава, посвященная безопасности сетей [138].

Кроме материалов для лекционных занятий и контрольных мероприятий, в комплекты входят учебно-методические рекомендации для проведения лабораторных работ по соответствующим курсам, также разработанных при непосредственном участии автора диссертационного исследования, а именно:

— Учебная дисциплина «Защищенные информационные системы»:

1) Лабораторная работа «Изучение уязвимостей систем, приводящих к атакам *SQL-injection*», цель которой – ознакомление с уязвимостями, способствующими реализации *SQL*-инъекций, и понимания методов ее предотвращения;

2) Лабораторная работа «Изучение уязвимостей систем, приводящих к атакам *XSS*», цель которой – ознакомление с уязвимостями, способствующими реализации *XSS*-атак, и понимания методов ее предотвращения;

3) Лабораторная работа «Изучение уязвимостей систем, приводящих к атакам *MiTM*», цель которой – ознакомление с уязвимостями, способствующими реализации *MiTM*-атак, и по-

нимания методов ее предотвращения [299];

— Учебная дисциплина «Технологии обеспечения информационной безопасности объектов»: Лабораторная работа «Изучение межсетевых экранов следующего поколения», цель которой – развитие у студентов навыков настройки параметров *NGFW*, а также ознакомления с его базовым функционалом по защите от сетевых атак [51];

— Учебная дисциплина «Основы управления инцидентами»: Лабораторная работа «Компьютерная криминалистика для расследования инцидентов ИБ», цель которой – получение студентами следующих навыков: использование инструментов управления инцидентами ИБ и организация ПУИИБ, в частности, сбор и анализ информация по инцидентам ИБ для определения последующего реагирования, а также разработка проектов организационных и распорядительных документов для СУИИБ [52].

В настоящее время в условиях пандемии начата работа по переводу первых трех лабораторных работ в дистанционный режим выполнения с использованием средств виртуальной реальности (англ. *Virtual Reality*) (статья на данную тему готовится) и разработки построения на базе ИИКС киберполигона, основная цель которого – помочь будущим специалистам сформировать системно-целостное видение проблем обеспечения ИБ, получить представление о сценариях и средствах распространённых атак и научиться результативно им противодействовать.

В 2019 г. выше описанная программа была существенно обновлена и для нее разработаны новые учебные дисциплины: «Центры управления сетевой безопасностью», «Интеллект в управлении сетевой безопасностью», «Аудит информационной безопасности», «Управление рисками информационной безопасности» и «Управление инцидентами информационной безопасности». Набор на новую программу уже состоялся и интерес к ней абитуриентов был очень высок, что доказывает конкурс – более 7 заявлений на одно место.

Именно в рамках образовательной программы «Обеспечение непрерывности и информационной безопасности бизнеса» представляется объективно возможной подготовка персонала для ЦИУСБ. Кроме нее в НИЯУ МИФИ реализуются еще четыре магистерские программы: «Безопасность данных и криптография», «Информационно-аналитическое обеспечение финансового мониторинга», «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» и «Теоретическая и практическая криптография», что позволяет готовить персонал для всех четырех (или трех) линий ЦИУСБ.

Материалы диссертационного исследования (в частности, основы построения ЦИУСБ, разработанный ПУИИБ, таксономия базовых понятий ИБ) были также использованы при подготовке аспирантов ИИКС НИЯУ МИФИ по направлению 10.06.01 «Информационная безопасность», программа «Методы и системы защиты информации, информационная безопасность» в учебных дисциплинах «Интеллект в управлении сетевой безопасностью» и «Методы и системы

защиты информации, информационная безопасность».

Кроме этого, они использовались при научном руководстве выпускными квалификационными и научно-исследовательскими работами, производственными и преддипломными практиками студентов кафедры «Информационная безопасность банковских систем», начиная с 2007/2008 учебного года и по настоящее время.

Акт о внедрении материалов диссертационного исследования в НИЯУ МИФИ приведен в Приложении Г.

6.5. Внедрение результатов в компании «ЛИНС-М»

ООО «ЛИНС-М», созданная в 2000 г. как исследовательская лаборатория, в настоящее время является известным системным интегратором в области ИБ, обладающим большим опытом создания территориально распределенных корпоративных вычислительных сетей различного масштаба, а также разработки и внедрения СОИБ в соответствии с особенностями функционирования объекта защиты и нормативных требований по обеспечению его ИБ.

В 2011-2012 гг. в рамках договоров между ООО «ЛИНС-М» и Банком России при разработке средств ИБ для Банка России, в частности, разрабатывалась подсистема межсетевого экранирования с соответствующим комплексом организационно-технических мер, необходимых для выполнения действующих требований по обеспечению ИБ с использованием МЭ, и документами – регламентами, руководствами, инструкциями, в чем участвовал диссертант. Таким образом, следующие результаты диссертационного исследования были внедрены в практику деятельности ООО «ЛИНС-М» в этих целях:

— информационно-аналитические материалы, полученные в результате исследования ЦУБ, и практические рекомендации по архитектурным улучшениям имеющихся центров в ЦИУСБ.

В рамках договора № 2017-01-4 от 2017 г. «Разработка корпоративного стандарта по обеспечению информационной безопасности» между ООО «ЛИНС-М» и Банком ВТБ (ПАО) в интересах последнего разрабатывался комплект различных документов верхнего уровня, описывающие принципы и подходы к обеспечению ИБ в целом, а также отдельные концептуальные документы и положения, необходимые для реализации политики ИБ, то есть были внедрены следующие результаты диссертационного исследования:

— рекомендации по разработке документального обеспечения функционирования ЦИУСБ;

— таксономия базовых понятий ИБ, а именно «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», которая используется при разработке Модели угроз ИБ, Модели нарушителей ИБ и Плана реагирования на инциденты ИБ;

— реестр рисков ИБ для ИТКС, построенный на основе Моделей угроз ИБ и Моделей

нарушителей ИБ.

Акт о внедрении материалов диссертационного исследования в ООО «ЛИНС-М» приведен в Приложении Д.

6.6. Внедрение в Федеральном Учебно-методическом объединении в системе высшего - образования по укрупненной группе специальностей направления подготовки - «Информационная безопасность»

Основные положения диссертационного исследования были использованы при разработке и внедрены Федеральным Учебно-методическим объединением (УМО) в системе высшего образования по укрупненной группе специальностей направления подготовки (УГСНП) «Информационная безопасность» в содержание ряда нормативных правовых и учебно-методических документов, а именно:

1) ФГОС по направлению высшего образования (в редакции 3 и 3+) по направлению 10.04.01 «Информационная безопасность» – уровень магистратуры, по направлению 10.03.01 «Информационная безопасность» – уровень бакалавриата, включая требования к результатам освоения программ, содержанию профессиональных задач, решаемых выпускником, требования к структуре программ, в части определения обязательных дисциплин «Защищенные информационные системы», «Управление информационной безопасностью», «Основы управления информационной безопасностью», требования к материально-техническому обеспечению, в части определения состава оборудования лабораторий в области технологий обеспечения ИБ и защищенных ИС;

2) примерные учебные планы подготовки магистров по направлению 10.04.01 «Информационная безопасность», бакалавров по направлению 10.03.01 «Информационная безопасность» и специалистов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» в части обоснования включения дисциплин (объемы их изучения, результаты обучения, дидактика дисциплины): Защищенные информационные системы», «Управление информационной безопасностью», «Основы управления информационной безопасностью», «Безопасность вычислительных сетей», а также дисциплин специализации «Информационная безопасность автоматизированных банковских систем». Примерные учебные планы по реализации ФГОС ВПО были утверждены на Пленуме УМО ИБ 20.10.2012. Примерные учебные планы по реализации ФГОС ВО (редакция 3+) были утверждены на XXI Пленуме УМО ИБ в мае 2017 г.;

3) примерные учебные программы дисциплин «Защищенные информационные системы» и «Управление информационной безопасностью», включенные в примерные учебные планы подготовки магистров по направлению 10.04.01 «Информационная безопасность» в качестве

обязательных. В содержание данных дисциплин включены теоретические положения и результаты диссертационного исследования. Примерные учебные программы дисциплин по реализации ФГОС ВО (редакция 3+) были утверждены на XXI Пленуме УМО ИБ в мае 2017 г.;

4) рекомендованные для учебного процесса в образовательных организациях изданные в соавторстве учебные издания, в которых использованы результаты диссертационного исследования, включая учебники «Информационная безопасность открытых систем» в двух томах с грифом Минобрнауки РФ [55], серия учебных пособий «Вопросы управления информационной безопасностью» в составе пяти книг [132, 168, 171, 172] и учебное пособие «Межсетевые экраны» с грифом УМО.

Акт о внедрении результатов диссертационного исследования в Федеральном УМО в системе высшего образования по УГСНП «Информационная безопасность» приведен в Приложении Ж.

Выводы по главе 6

Практическое применение результатов исследований, внедренных в промышленную эксплуатацию, состояло в следующем:

1) при модернизации Ситуационного центра Службы ИБ Банка ГПБ (АО):

— методология и принципы построения ЦИУСБ как современного решения, предназначенного для управления нарушениями и инцидентами ИБ и таким образом снижающего операционные риски для ИТКС АО;

— построение ЦИУСБ с точки зрения обеспечения его функциональной устойчивости, реализованная, в частности, за счет использования предложенных диссертантом решений для конкретной исторически сложившейся среды функционирования ИТКС Банка, включая использование следующих решений: система анализа аномального трафика на базе решения *Cisco StealthWatch*, система выявления уязвимостей на базе решения *SkyBox Vulnerability Control*, система выявления аномального поведения пользователей и устройств в ИТКС на базе решения *Exabeam*, многоуровневой защиты почтового канала, включающей спам-фильтр, почтовый антивирус, средство защиты от атак «нулевого дня» и *PT MultiScanner* и *NGFW* на базе решения *CheckPoint*;

2) в проектно-конструкторской деятельности российской компании «ЕС-лизинг» при разработке СОИБ для Банка России:

— общесистемное проектирование центров управления инцидентами ИБ для ЦОД заказчиков на базе типового ЦИУСБ как комплексного системотехнического решения, обеспечивающего снижение операционных рисков при развертывании современных средств обеспечения

сетевой безопасности в зонах безопасности ЦИУСБ, ориентированных на создание комплексной СОИБ ИТКС заказчиков;

— реализация концепции устойчивого функционирования ЦИУСБ, заложенной в сам проект типового ЦИУСБ и реализованной для ИТКС заказчиков, в частности, за счет использования следующих конкретных решений в зонах безопасности ЦИУСБ: аппаратные МЭ с отслеживанием состояния соединений и глубоким анализом протоколов прикладного уровня *Cisco ASA (Adaptive Security Appliance)*, многофункциональная система управления доступом к корпоративной сети на базе *Cisco ISE (Identity Services Engine)*, система мониторинга сетевыми устройствами *Cisco Prime Infrastructure*, ПО *HP Network Automation*, платформа для операционной аналитики *Splunk Enterprise*, российская DLP-система *InfoWatch Traffic Monitor* с компонентой *InfoWatch Device Monitor*, почтовый шлюз *hMail Server* под платформу *Windows*, файловый шлюз *Vaultize* и российское решение для централизованного управления комплексной системой защиты *Kaspersky Security Center*;

— архитектура хранения больших относящихся к ИБ ИТКС данных в виде «озер данных», рассчитанная и на работу с быстрыми данными, что требуется для интеллектуального анализа в определенном контексте всех имеющихся в распоряжении заказчиков «сырых» и исторических данных о событиях ИБ в их ИТКС и реализации проактивного подхода для предотвращения инцидентов в ИТКС, нарушающих устойчивое и защищенное функционирование ЦИУСБ, а, значит, и ИТКС организации;

3) в проектно-конструкторской деятельности компании Qualys в регионах Восточной Европы, Кавказа и Центральной Азии при создании решений для ЦУБ организаций:

— зональная архитектура обеспечения ИБ ЦИУСБ с эшелонированной защитой и жесткой регламентацией доступа к ресурсам и услугам различных зон безопасности, внедренная у заказчиков компании;

— размещение «песочницы» в ДМЗ ЦИУСБ для исследования подозрительного ПО от непроверенных третьих лиц, пользователей, веб-сайтов и т.д., поступающих в ИТКС заказчика из внешних открытых сетей;

— развертывание в зонах безопасности ЦИУСБ современных средств обеспечения сетевой безопасности (включая сканеры анализа защищенности Qualys), ориентированных на создание комплексной СОИБ ИТКС;

4) при реализации типового ЦИУСБ в НИЯУ МИФИ:

— методология и принципы построения Учебно-научного центра «Интеллект в управлении сетевой безопасностью» на базе Института интеллектуальных кибернетических систем (ИИКС) в составе трех учебно-научных лабораторий – «Предотвращение утечки конфиденциальной информации» (на базе DLP-системы компании «СёрчИнформ»), «Межсетевые экраны

нового поколения» (на базе *Palo Alto NGFW*) и «Управление информацией и событиями безопасности» (на базе «*СёрчИнформ SIEM*»), что позволило на более высоком качественном уровне проводить учебные занятия и научные исследования по созданию систем управления сетевой безопасностью ИТКС, методам эффективного управления сетевой безопасностью ИТКС на основе применения интеллектуальных подходов, использованию технологии больших данных для обработки связанной с сетевой безопасностью информации, исследованию вопросов совместимости средств обеспечения сетевой безопасности и выработки рекомендаций по решению возникающих в связи с этим проблем, а также оценке защищенности ИТКС;

— архитектурные решения, предлагаемые в качестве основы построения учебно-научного центра, показавшие свою состоятельность в рамках функционирования ИТКС ИИКС;

— при проведении лекционных и практических занятий и разработке учебно-методических комплексов для преподаваемых учебных дисциплин по направлению 10.04.01 «Информационная безопасность», программа подготовки магистров «Обеспечение непрерывности и информационной безопасности бизнеса»: основы построения ЦИУСБ, разработанный ПУИИБ и таксономия базовых понятий ИБ и по направлению 10.06.01 «Информационная безопасность», программа подготовки аспирантов «Методы и системы защиты информации, информационная безопасность»: основы построения ЦИУСБ, разработанный ПУИИБ, таксономия базовых понятий ИБ;

— при подготовке и публикации серии учебных пособий и учебников, которые получили грифы Министерства образования и науки РФ и Учебно-методического объединения вузов России по образованию в области ИБ и в настоящее время используются при преподавании дисциплин в качестве обязательной учебной литературы;

— при выполнении ряда выпускных квалификационных и научно-исследовательских работ, производственной и преддипломной практик студентов кафедры «Информационная безопасность банковских систем»;

5) в практику деятельности ООО «ЛИНС-М» при разработке средств ИБ для Банка России и стандарта обеспечения ИБ для Банка ВТБ (ПАО):

— информационно-аналитические материалы, полученные в результате исследования ЦУБ, и практические рекомендации по архитектурным улучшениям имеющихся центров в ЦИУСБ;

— рекомендации по разработке документального обеспечения функционирования ЦИУСБ;

— таксономия базовых понятий ИБ, а именно «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», которая используется при разработке Модели угроз ИБ, Модели нарушителей ИБ и Плана реагирования на инциденты ИБ;

— реестр рисков ИБ для ИТКС, построенный на основе Моделей угроз ИБ и Моделей нарушителей ИБ;

б) при разработке Федеральным УМО в системе высшего образования по УГСНП «Информационная безопасность» содержания ряда нормативных правовых и учебно-методических документов, а именно:

— ФГОС по направлению высшего образования (в редакции 3 и 3+) по направлению 10.04.01 «Информационная безопасность» – уровень магистратуры, по направлению 10.03.01 «Информационная безопасность» – уровень бакалавриата, включая требования к результатам освоения программ, содержанию профессиональных задач, решаемых выпускником, требования к структуре программ, в части определения обязательных дисциплин «Защищенные информационные системы», «Управление информационной безопасностью», «Основы управления информационной безопасностью», требования к материально-техническому обеспечению, в части определения состава оборудования лабораторий в области технологий обеспечения ИБ и защищенных ИС;

— примерные учебные планы подготовки магистров по направлению 10.04.01 «Информационная безопасность», бакалавров по направлению 10.03.01 «Информационная безопасность» и специалистов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» в части обоснования включения дисциплин (объемы их изучения, результаты обучения, дидактика дисциплины): Защищенные информационные системы», «Управление информационной безопасностью», «Основы управления информационной безопасностью», «Безопасность вычислительных сетей», а также дисциплин специализации «Информационная безопасность автоматизированных банковских систем»;

— примерные учебные программы дисциплин «Защищенные информационные системы» и «Управление информационной безопасностью», включенные в примерные учебные планы подготовки магистров по направлению 10.04.01 «Информационная безопасность» в качестве обязательных. В содержание данных дисциплин включены теоретические положения и результаты диссертационного исследования;

— рекомендованные для учебного процесса в образовательных организациях изданные в соавторстве учебные издания, в которых использованы результаты диссертационного исследования, включая учебники «Информационная безопасность открытых систем» в двух томах с грифом Минобрнауки РФ, серия учебных пособий «Вопросы управления информационной безопасностью» в составе пяти книг и учебное пособие «Межсетевые экраны» с грифом УМО;

Внедрение всех результатов подтверждено соответствующими актами.

ЗАКЛЮЧЕНИЕ

В ходе проведения диссертационного исследования диссертантом достигнута поставленная цель, а именно разработана научно обоснованная методология и принципы построения специализированного структурного элемента ИТКС – типового ЦИУСБ в составе СОИБ ИТКС, призванного осуществлять упреждающее управление сетевой безопасностью ИТКС на всех стадиях жизненного цикла ее информационных ресурсов за счет прогнозирования развития событий в области ИБ ИТКС и применения в ЦИУСБ для достижений этих целей интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных. При этом все процессы обеспечения ИБ с применением ЦИУСБ в ИТКС ОРГАНИЗАЦИИ будут работать наиболее результативно только в том случае, когда операционные (текущие), тактические (в ближайшей перспективе) и стратегические (в отдаленной перспективе) задачи обеспечения ИБ ИТКС будут четко определены и будут решаться на взаимоподдерживающей основе в рамках СОИБ ИТКС.

Диссертантом получены следующие *научные результаты*.

1. Обосновано включение в ИТКС (объект КИИ) нового специализированного структурного элемента – ЦИУСБ, предназначенного для упреждающего управления сетевой безопасностью ИТКС на всех стадиях ее жизненного цикла как системообразующего элемента СОИБ ЕИП ОРГАНИЗАЦИИ (субъект КИИ).

2. Разработаны научно обоснованная методология и принципы построения типового ЦИУСБ с применением интеллектуальных подходов (включая корреляционный, контекстный, поведенческий и структурный анализ) обработки больших относящихся к ИБ данных для упреждающего управления сетевой безопасностью ИТКС.

3. Проведена научно обоснованная структуризации понятий информационной защищенности ИТКС и описания внутреннего и внешнего контекста деятельности ОРГАНИЗАЦИИ как единая таксономия, необходимая для конкретизации требований к ЦИУСБ, которая позволила получить научную систематизацию и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей (базовых понятий ИБ: «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»).

4. На основе обобщения опыта построения ИТКС с централизованной обработкой и хранением больших объемов данных разработаны основные принципы и базовые архитектурные решения построения перспективных ЦИУСБ для объектов КИИ в условиях Российской Федерации, а также необходимое расширение оригинальной бизнес-логики их функционирования при управлении инцидентами ИБ в ИТКС ОРГАНИЗАЦИИ.

5. Для обеспечения целостности накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ в составе рекомендуемой в качестве ядра ЦИУСБ SIEM-системы 3.0

обосновано и спроектировано средство блокирования попыток компрометации с применением технологий блокчейна.

6. Для реализации в ЦИУСБ ОРГАНИЗАЦИИ детально разработаны и формализованы с применением расширенного метода составления карт (с добавлением табличного описания) основные взаимосвязанные процессы управления инцидентами ИБ ИТКС.

7. Для типового ЦИУСБ при реализации ИБ-аналитики и синтеза новых знаний об ИБ ИТКС ОРГАНИЗАЦИИ для ее упреждающей защиты обосновано использование концепции озер данных при организации хранения и обработки в режиме реального времени связанных с ИБ ИТКС данных.

8. Уточнена и существенно расширена по сравнению с используемой временная шкала появления технологий и средств обеспечения сетевой безопасности, что позволяет наглядно отслеживать эволюцию существующих и своевременно фиксировать появление новых технологий и средств.

9. Разработан глоссарий взаимосогласованных терминов предметной области обеспечения сетевой безопасности, отвечающий существующей нормативной и правовой базам и расширяющий терминологию ГОСТ Р ИСО/МЭК 27033-1-2011.

10. Практические внедрения полученных результатов научных исследований подтвердили их достоверность и результативность.

Теоретическая значимость полученных результатов исследования заключается в следующем:

1. Обоснована необходимость совершенствования современных подходов к обеспечению ИБ современных сетей, которые не справляются с обработкой всех поступающих из гетерогенных источников данных о многочисленных и усложнившихся компьютерных атаках для реагирования в режиме жесткого реального времени на инциденты ИБ в ЕИП ОРГАНИЗАЦИИ.

2. Разработаны научно обоснованная методология и принципы построения типового ЦИУСБ ОРГАНИЗАЦИИ как объединения ЦИБ и СОЦ, что вносит значительный теоретический вклад в подходы к обеспечению сетевой безопасности ИТКС объектов КИИ, поскольку они направлены на решение проблемы совершенствования технического и организационного обеспечения сетевой безопасности в условиях угроз ИБ при одновременной интенсификации использования ИКТ в России.

3. Разработана таксономия как научная систематизация и совокупность классификаций сложноорганизованных иерархически взаимосвязанных сущностей, базовых понятий ИБ, а именно «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», которая вносит существенный вклад в развитие теории ИБ, к настоящему времени до конца пока не сформировавшейся в качестве самостоятельной теории.

4. Разработана обобщенная модель процессов функционирования типового ЦИУСБ, которая может быть использована не только применительно к ЦИУСБ, но и к ИТКС ОРГАНИЗАЦИИ, и в рамках этой модели сформулированы задачи анализа, то есть определить значения показателей защищенности информации в ЦИУСБ, синтеза и управления обеспечением ИБ в ЦИУСБ.

5. Для типового ЦИУСБ разработана архитектура хранения и обработки в режиме жесткого и мягкого реального времени больших и быстрых относящихся к ИБ ИТКС данных, основанная на использовании озер данных и ориентированная на применение в ЦИУСБ предложенного в рамках исследования процесса ИБ-аналитики и синтеза новых знаний об информационной защищенности ИТКС ОРГАНИЗАЦИИ для ее упреждающей защиты.

6. С применением расширенного (с добавлением табличного описания) метода составления карт процессов разработаны и формализованы основные взаимосвязанные процессы в рамках управления инцидентами ИБ ИТКС.

7. Представлен обзор основных возможностей ИБ-аналитики и выделены преимущества ее использования при решении задач управления инцидентами ИБ ИТКС ОРГАНИЗАЦИИ.

8. Обоснована необходимость разработки *SIEM*-системы нового поколения для использования в типовом ЦИУСБ и с применением технологий блокчейна со сверткой в составе *SIEM*-системы 3.0 разработано средство блокирования попыток компрометации массива накапливаемых в ЦИУСБ свидетельств инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ.

9. Разработан глоссарий взаимосогласованных терминов предметной области обеспечения сетевой безопасности, который может стать основой для дальнейшего расширения.

10. Разработана структурно-логическая схема проведенного исследования, наглядно показывающая преемственность полученных результатов по отношению к ранее существовавшим и их значимость для эволюции методов и средств обеспечения сетевой безопасности.

Практическая значимость полученных результатов исследования, созданных диссертантом и внедренных в промышленную эксплуатацию, заключается в следующем:

1. Построен типовой ЦИУСБ, описана методология его построения и рассмотрены вопросы ее использования при реализации ПУИИБ, что готово к доработке под конкретный внешний и внутренний контекст любой организации, владеющий ИТКС и желающий результативно управлять инцидентами ИБ в ИТКС.

2. Предложены вербальные описания ключевых типовых признаков (индикаторов), характеризующих типичные действия злоумышленника и свидетельствующих об удаленных сетевых атаках на ИТКС ОРГАНИЗАЦИИ, которые могут быть положены в основу разработки индикаторов компрометации (*IoC*) для источников *Threat Intelligence*.

3. В связи с отсутствием в международной и отечественной нормативных базах четких

рекомендаций по разработке реестра (классификатора) рисков ИБ, предложены вид реестра рисков ИБ для ИТКС, построенный на основе Модели угроз ИБ и Модели нарушителей ИБ, и примерная типовая структура частной Политики ИБ для элемента ИТКС ОРГАНИЗАЦИИ.

4. Приведены примеры постоянной и временной информации, подлежащей сбору при расследовании инцидентов ИБ в ИТКС ОРГАНИЗАЦИИ.

5. Установлены особенности визуализации информации об ИБ и то, какая информация об ИБ ИТКС ОРГАНИЗАЦИИ подлежит визуализации в ЦИУСБ для принятия обоснованных решений по управлению сетевой безопасностью обобщенно по всей ИТКС или по отдельным событиям ИБ.

6. Определены типы контекста, в рамках которого должна проводиться ИБ-аналитика относящихся к ИБ ИТКС ОРГАНИЗАЦИИ данных.

7. Для зональной архитектуры ЦИУСБ указаны применимые меры и средства обеспечения ИБ, предназначенные для защиты ЦИУСБ путем обеспечения защиты его сетевой инфраструктуры, функций устройств, информационных ресурсов и данных, управления пользователями и т.д., с указанием их расположения в зонах безопасности ЦИУСБ.

8. Введено понятие функциональной устойчивости ЦИУСБ в ЕИП ОРГАНИЗАЦИИ в штатном режиме, в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций как активной формы устойчивости для динамической системы, что должно быть изначально встроено в проект ЦИУСБ, как и система оценки уровня функциональной устойчивости и восстановления ЦИУСБ после нарушений и инцидентов ИБ (для нее приведен начальный набор показателей), а также перечислены основные мероприятия, осуществляемые в рамках процесса управления функциональной устойчивостью ЦИУСБ в ЕИП ОРГАНИЗАЦИИ.

9. Определен примерный состав кадрового обеспечения типового ЦИУСБ, который обычно делится на три-четыре линии. Для каждой линии указаны типовые трудовые функции персонала и их профессиональные компетенции.

10. Кратко описан международный опыт разработки документов, устанавливающих компетенции профессионалов в области ИБ, а также рассмотрены возможности российской системы высшего образования в формулировании таких компетенций. Кратко продемонстрировано, как это может быть применено при подготовке специалистов для типового ЦИУСБ.

11. Результаты диссертации использовались для разработки уникальной в России и мире образовательной программы подготовки магистров под названием «Обеспечение непрерывности и информационной безопасности бизнеса» в рамках направления подготовки 10.04.01 «Информационная безопасность».

12. Практические внедрения полученных результатов научных исследований подтверди-

ли их достоверность и результативность.

Результаты диссертационной работы использованы при разработке СОИБ для Банка России (акт головного исполнителя работ – российской компании «ЕС-лизинг»), при создании решений для ЦИУСБ организаций в регионах Восточной Европы, Кавказа и Центральной Азии (акт головного исполнителя работ – компании Qualys), при модернизации Ситуационного центра Службы ИБ Газпромбанка, при реализации типового ЦИУСБ в НИЯУ МИФИ, включая подготовку высококвалифицированных специалистов для проектирования, внедрения, сопровождения и совершенствования ЦИУСБ, в практике деятельности ООО «ЛИНС-М» при разработке средств ИБ для Банка России и стандарта обеспечения ИБ для Банка ВТБ (ПАО), а также при разработке и внедрении нормативных правовых и учебно-методических документов в Федеральном Учебно-методическом объединении в системе высшего образования по укрупненной группе специальностей направления подготовки «Информационная безопасность». Внедрение результатов подтверждается соответствующими актами.

Перечисленные внедрения доказывают несомненную практическую значимость для индустрии в целом и финансовой индустрии в частности разработанного в диссертационном исследовании типового ЦИУСБ, основными функциональными возможностями которого для его организации-владельца являются следующие:

- централизованное управление инцидентами ИБ в ИТКС ОРГАНИЗАЦИИ и полная ситуационная осведомленность в режиме реального времени с «бесшовной» интеграцией и комплексным отслеживанием контролируемых объектов и процессов ИТКС с ведением единой БД активов и визуализацией текущей ситуации в «едином окне» с различными информационными панелями, предназначенными для администрирования и принятия оперативных и стратегических решений в области ИБ;

- интеграция непрерывного мониторинга всей сетевой активности (связываемой с объектами, а не IP-адресами) и выполнения требований по обеспечению ИБ с автоматизированным контролем за производительностью и доступностью всех элементов ИТКС, приоритизацией предупреждений об опасности от СЗИ, оповещением и уведомлениями соответствующего персонала и всех причастных сторон, отчетностью и единой службой технической поддержки;

- централизованное управление и аудит конфигурационных настроек сетевых устройств и СЗИ, БД, архивов и т.п., включая отслеживание их изменений, отображаемых в привязке к изменению мер обеспечения ИБ и нарушению требований ОРГАНИЗАЦИИ;

- быстрое обнаружение событий ИБ и сокращение времени скоординированного реагирования на инциденты ИБ посредством автоматического устранения ошибок, обновления и активизации необходимых мер обеспечения ИБ;

- автоматизированный сбор данных, включая сбор событий и информационных пото-

ков, агрегирование и корреляцию посредством автоматизации и расширенной (как с точки зрения сети, так и ИБ) аналитика, с целью извлечения из них большего смысла и получения максимальной пользы из больших данных, связанных с ИБ, доступных ЦИУСБ, в частности при исследовании инцидентов ИБ, включая сохранение всего трафика, реконструкцию пакетов, восстановление сеансов пользователей и т.д.

Таким образом, в диссертационном исследовании решена научная проблема, имеющая важное значение для создания функционально устойчивой и защищенной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств России и заключающаяся в научно обоснованном рациональном выборе конкретных методов, принципов, способов и средств построения того главного, от чего в первую очередь зависит достижение информационной защищенности информационных ресурсов ИТКС, и изложены научно обоснованные технические, технологические и кадровые решения, внедрение которых вносит значительный вклад в развитие страны и научной области обеспечения сетевой безопасности.

Пути дальнейшего развития идей исследования диссертант видит в следующем:

1. На основе полученных результатов исследования предоставить техническому комитету ТК362 материалы для разработки в рамках серии ISO 27000 международного стандарта, посвященного ЦУБ.
2. Обратиться к техническому комитету ТК362 с просьбой восстановить работу над международным стандартом ISO/IEC 27044, посвященным *SIEM*-системам.
3. Разработать образовательный стандарт, предназначенный для подготовки специалистов в области управления сетевой безопасностью, к которым относятся и кадры для ЦИУСБ.
4. Расширить ЦИУСБ, реализованный в НИЯУ МИФИ, в части более активного проведения на его базе научных исследований.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АС	Автоматизированная система
АО	Аппаратное обеспечение
БД	База данных
БДОРС	База данных ожидающих решения событий
ВО	Высшее образование
ВЧС	Виртуальная частная сеть
ГО	Головной офис
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации
ГРИИБ	Группа реагирования на инциденты информационной безопасности
ДМЗ	Демилитаризованная зона
ЖРС	Журнал регистрации событий
ЕИП	Единое информационное пространство
ИД	Индикаторы достижения
ИИ	Информационная инфраструктура
ИКТ	Информационно-коммуникационные технологии
ИС	Информационная система
ИТ	Информационные технологии
ИТИ	Информационно-телекоммуникационная инфраструктура
ИТКС	Информационно-телекоммуникационная сеть
ИТС	Информационно-телекоммуникационная система
КИИ	Критическая информационная инфраструктура
КЦОИ	Коллективный центр обработки информации
МИФИ	Московский инженерно-физический институт
МЭ	Межсетевой экран
НБ	Непрерывность бизнеса
НИЯУ МИФИ	Национальный исследовательский ядерный университет МИФИ
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
НСД	Несанкционированный доступ
ОПК	Общепрофессиональные компетенции
ОС	Операционная система
ОТФ	Обобщенные трудовые функции

ПК	Профессиональные компетенции
ПО	Программное обеспечение
ПС	Профессиональные стандарты
ПСиА	Подсистема сбора и анализа
ПУИИБ	Процесс управления инцидентами информационной безопасности
РФ	Российская Федерация
СAB3	Средства антивирусной защиты
САЗ	Сканер анализа защищенности
СВОИ	Система выявления и обработки инцидентов
СВТ	Средства вычислительной техники
СЗИ	Средства защиты информации
СКЗИ	Средства криптографической защиты информации
СМИ	Средства массовой информации
СМИБ	Система менеджмента информационной безопасности
СОИА	Среда обработки информационного актива
СОВ	Система обнаружения вторжений
СОИ	Система обработки информации
СОИБ	Система обеспечения информационной безопасности
СОЦ	Сетевой операционный центр
СПВ	Система предотвращения вторжений
СУБД	Система управления базами данных
СУИБ	Система управления информационной безопасностью
ТМ	Тренинговый модуль
ТОИБ	Технологии обеспечения информационной безопасности
ТС	Технологическая система
ТФ	Трудовые функции
УГСНП	Укрупненная группа специальностей и направлений подготовки
ФГОС	Федеральные государственные образовательные стандарты
ЦИБ	Центр интеллектуальной безопасности
ЦИУСБ	Центр интеллектуального управления сетевой безопасностью
ЦМБ	Центр мониторинга безопасности
ЦУБ	Центр управления безопасностью
<i>ACL</i>	<i>Access Control List</i> – Список контроля доступа
<i>AST</i>	<i>Application security testing</i> – Тестирование безопасности приложений

<i>CASB</i>	<i>Cloud Access Security Broker</i> – Брокер безопасности облачного доступа
<i>CGI</i>	<i>Common Gateway Interface</i> – Общий интерфейс шлюза
<i>DCAP</i>	<i>Data-Centric Audit and Protection</i> – Аудит и защита, ориентированные на данные
<i>DDoS</i>	<i>Distributed Denial of Service</i> – Распределенный отказ в обслуживании
<i>DLP</i>	<i>Data Loss Prevention</i> – Предотвращение утечки данных
<i>DMZ</i>	<i>Demilitarized Zone</i> – Демилитаризованная зона
<i>DNS</i>	<i>Domain Name System</i> – Система доменных имен
<i>DoS</i>	<i>Denial of Service</i> – Отказ в обслуживании
<i>DPI</i>	<i>Deep Packet Inspection</i> – Глубокая (всесторонняя) инспекция пакетов
<i>EM</i>	<i>Employee Monitoring</i> – Мониторинг сотрудников
<i>ETDR/EDR</i>	<i>Endpoint Threat Detection and Response/Endpoint Detection and Response</i> – Обнаружение и реагирование на угрозы для конечных точек
<i>FCI</i>	<i>Full Content Inspection</i> – Полная инспекция контента (содержания)
<i>FTP</i>	<i>File Transfer Protocol</i> – Протокол передачи файлов
<i>HTTP</i>	<i>HyperText Transfer Protocol</i> — Протокол передачи гипертекста
<i>HTTPS</i>	<i>HyperText Transfer Protocol Secure</i> — Защищенный протокол передачи гипертекста
<i>IDS</i>	<i>Intrusion Detection System</i> – Система обнаружения вторжений
<i>IoT</i>	<i>Internet of Things</i> – Интернет вещей
<i>IPS</i>	<i>Intrusion Prevention System</i> – Система предотвращения вторжений
<i>MiTM</i>	<i>Man-in-the-Middle</i> – Атака «третий по середине»
<i>NGFW</i>	<i>Next-Generation Firewall</i> – Межсетевой экран следующего поколения
<i>NGIPS</i>	<i>Next-Generation Intrusion Prevention System</i> – Система предотвращения вторжений нового поколения
<i>NOC</i>	<i>Network Operations Center</i> – Центр управления сетью
<i>NTA</i>	<i>Network traffic analysis</i> – Анализ сетевого трафика
<i>OC</i>	<i>Outbound Control</i> – Контроль исходящих коммуникаций
<i>PAM</i>	<i>Privileged Access Management</i> – Управление привилегированным доступом
<i>SLA</i>	<i>Service Level Agreement</i> – Соглашение об уровне услуг
<i>SOAR</i>	<i>Security Orchestration, and Automated Response</i> – Оркестровка безопасности и автоматическое реагирование или <i>Security Operations, Analytics and Reporting</i> – Действия, аналитика и отчетность по безопасности

<i>SPI</i>	<i>Stateful Packet Inspection</i> – Инспекция пакетов на основе состояний
<i>SSL</i>	<i>Secure Sockets Layer</i> – уровень защищенных сокетов
<i>SUBA</i>	<i>Security User Behavior Analytics</i> – Анализ безопасности поведения пользователей
<i>SWG</i>	<i>Secure Web Gateway</i> – Шлюзы безопасности веб-среды
<i>URL</i>	<i>Uniform Resource Locator</i> – Унифицированный указатель ресурсов
<i>UTM</i>	<i>Unified Threat Management</i> – Унифицированное управление угрозами
<i>UEBA/UBA</i>	<i>User and Entity Behavior Analytics/User Behavior Analytics</i> – Анализ поведения пользователей и сущностей
<i>VPN</i>	<i>Virtual Private Network</i> – Виртуальная частная сеть
<i>WAF</i>	<i>Web Application Firewall</i> – Межсетевой экран уровня веб-приложений
<i>XML</i>	<i>eXtensible Markup Language</i> — Расширяемый язык разметки
<i>XSS</i>	<i>Cross-Site Scripting</i> – Межсайтовый скриптинг

СЛОВАРЬ ТЕРМИНОВ

1 Автоматизированная система (АС) (англ. *automated system*): система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. Примечания: 1. В зависимости от вида деятельности выделяют, например, следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др. 2. В зависимости от вида управляемого объекта (процесса) АСУ делят, например, на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д. (ГОСТ 34.003-90 [109]).

2 Агрегирование: процесс объединения однородных и повторяющихся данных о событиях ИБ в ИТКС ОРГАНИЗАЦИИ.

3 Активы организации (англ. *assets*): все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении. Примечание – К активам организации могут относиться: информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение); ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие); процессы (технологические, информационные и пр.); выпускаемая продукция и/или оказываемые услуги (ГОСТ Р 53114-2008 [22]).

4 Атака (англ. *attack*): попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования (ГОСТ Р ИСО/МЭК 27000-2012 [117], ISO/IEC 27000:2018 [123]).

5 Аутентификация отправителя данных: подтверждение того, что отправитель полученных данных соответствует заявленному (ГОСТ Р ИСО 7498-2-99 [119]).

6 Аутентификация равноправного логического объекта: подтверждение того, что равноправный логический объект в какой-либо ассоциации (установлении соединения, от англ. *association*) является заявленным логическим объектом (ГОСТ Р ИСО 7498-2-99 [119]).

7 База данных (БД): упорядоченный набор структурированной информации или данных, которые обычно хранятся в электронном виде в компьютерной системе. БД обычно управляется системой управления БД (СУБД).

8 Безопасность информации [данных] (англ. *information [data] security*): состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность (ГОСТ Р 50922-2006 [111]).

9 Безопасность критической информационной инфраструктуры (безопасность

КИИ): состояние защищенности КИИ, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак (статья 2, 149-ФЗ [6]).

10 Безопасность сети или сетевая безопасность (англ. *network security*) в дополнение к безопасности информации, передаваемой по линиям связи, затрагивает безопасность устройств, безопасность деятельности по управлению данными устройствами, приложениями/услугами и конечными пользователями (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

11 Бизнес-процесс: множество из одной или нескольких упорядоченных во времени, логически связанных и завершенных видов деятельности, в совокупности поддерживающих деятельность организации и реализующих ее политику, направленную на достижение поставленных целей [170].

12 Блокчейн (англ. *blockchain*): особый тип защищенной синхронизированной между его пользователями распределенной структуры данных – БД, которая без главного администратора и централизованного хранилища данных поддерживает постоянно расширяющийся список (в виде последовательной цепочки) нередактируемых блоков/записей и устанавливает правила работы с транзакциями/событиями, записываемыми в блоках и привязанными таким образом к ним (в отличие от обычных БД, в которых правила часто устанавливаются для всей БД или приложения) [160, 267, 268]. В свою очередь, блок (как структурированные данные с заголовком) будет содержать информацию о последовательности подтвержденных и проверенных транзакций – произошедших в хронологическом порядке имеющих отношение к ИБ ИТКС ОРГАНИЗАЦИИ событий, то есть стадий одного инцидента ИБ.

13 Большие данные (англ. *big data*): массивы данных такого объема и структуры, которые превышают возможности традиционных программных инструментов (БД, ПО) по сбору, хранению и обработке данных за приемлемое время и тем более превышают возможности их восприятия человеком. При этом данные могут быть структурированными, слабоструктурированными и неструктурированными, что не позволяет результативно управлять ими и обрабатывать традиционным образом [41].

14 Ведение контрольных журналов (англ. *audit logging*): фиксирование данных о событиях, связанных с ИБ, в целях проверки, анализа и постоянного мониторинга (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]). Иначе этот процесс можно назвать **логированием**, понимая под ним процесс автоматической записи с настраиваемой степенью детализации сведений о происходящих в ИТКС и ее подсистемах событиях в специальные журналы (файлы, базы данных) регистрации.

15 Виртуальная локальная вычислительная сеть (англ. *Virtual Local Area Network, VLAN*): независимая сеть, созданная с логической точки зрения внутри физической сети (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

16 Виртуальная частная сеть (англ. *Virtual Private Network, VPN*): логическая выделенная сеть передачи данных, построенная на базе сети общего пользования (публичной сети) и обеспечивающая их конфиденциальность, целостность и аутентичность за счет использования туннелирования, криптографии и других функций безопасности [55].

17 Вторжение (англ. *intrusion*): несанкционированный доступ (НСД) к сети или подсоединенной к сети системе, то есть преднамеренный или случайный НСД к информационной системе (ИС), включая злонамеренную деятельность против ИС или несанкционированное использование ресурсов в ИС (ГОСТ Р ИСО/МЭК 27033-3-2014 [108]).

18 Высокая доступность (англ. *high availability*) ЦИУСБ ОРГАНИЗАЦИИ: обеспечение для ЦИУСБ повышенной отказоустойчивости, катастрофоустойчивости и информационной защищенности на заданную перспективу. Она означает способность ЦИУСБ работать при существующих нагрузках и при их увеличении, а также противостоять отказам, вызванным, в том числе, уничтожением его компонентов и связей между ними, а уровень доступности обычно измеряется «девятками».

19 Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации (ГосСОПКА): единый централизованный территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, и федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования системы (Указ Президента РФ № К 1274 [25]).

20 Группа реагирования на инциденты информационной безопасности (ГРИИБ) (англ. *IS incident response team*): Команда квалифицированных и доверенных сотрудников организации, которая обрабатывает инциденты в течение их жизненного цикла. Примечание – CERT (Computer Emergency Response Team, Группа реагирования на компьютерные инциденты) и CSIRT (*Computer Security Incident Response Team*, Группа реагирования на инциденты компьютерной безопасности) являются часто используемыми синонимами ГРИИБ (ISO/IEC 27035-1:2016 [68]).

21 Данные (англ. *data*): информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека (ГОСТ 15971-90 [104]).

22 Демилитаризованная зона (ДМЗ) (англ. *Demilitarized Zone, DMZ*): пограничный сегмент сети (также известный как защищенная подсеть), выполняющий функции «нейтральной зоны» между сетями (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

23 Деятельность: набор действий, спроектированный с целью получения определенного

результата [300].

24 Домен безопасности (англ. *security domain*): совокупность активов и ресурсов, подчиняющихся единой политике безопасности (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

25 Допустимый риск информационной безопасности (допустимый риск ИБ): риск ИБ, предполагаемый ущерб от которого ОРГАНИЗАЦИЯ в данное время и в данной ситуации готова принять (ГОСТ Р ИСО/МЭК 27005-2010 [107]).

26 Достоверность (англ. *reliability*): свойство соответствия предусмотренному поведению и результатам (ГОСТ Р ИСО/МЭК 27000-2012 [117]).

27 Доступность (англ. *availability*): свойство быть доступным и готовым к использованию по запросу авторизованного субъекта (ГОСТ Р ИСО/МЭК 27000-2012 [117]).

28 Доступность информационной системы (ИС): свойство, характеризующее возможность за приемлемое время получить от ИС требуемую информационную услугу [63].

29 Единое информационное пространство (ЕИП): совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворение их информационных потребностей». Оно включает в себя следующее: 1) информационные ресурсы, содержащие данные, сведения и знания, зафиксированные на соответствующих носителях информации; 2) информационную инфраструктуру в составе: организационные структуры, обеспечивающие функционирование и развитие ЕИП, в частности, сбор, обработку, хранение, распространение, поиск и передачу информации; средства информационного взаимодействия его участников, в том числе программно-технические средства и организационно-нормативные документы, обеспечивающие доступ к информационным ресурсам на основе соответствующих ИТ (Решение Президента РФ № Пр-1694 [67]).

30 Журнал регистрации событий (англ. *log file, audit trail, audit log*) **информационно-телекоммуникационной сети организации:** имеющая отношение к ИБ ИТКС хронологическая автоматически создаваемая с настраиваемой степенью детализации запись/набор записей в файл/БД событий, происходящих с каким-то контролируемым объектом (или в рамках какого-то процесса) ИТКС, с указанием ее источника, документально подтверждающая последовательность действий, сопровождающих конкретную операцию, процедуру, работу программы, событие и т.п.

31 Защитные меры (англ. *security measures*): действия, процессы, процедуры и средства, способные обеспечить ИБ при возникновении угрозы ИБ, уменьшить уязвимость, ограничить воздействие инцидента ИБ, обнаружить инциденты и облегчить восстановление затронутых объектов [172].

32 Знания об угрозах ИБ (англ. *Threat Intelligence*): основанные на фактических данных знания, содержащие такую проверенную, определенным образом обогащенную и значимую информацию о существующей или возникающей угрозе ИБ как признаки, по которым можно распознать потенциальную угрозу (например, IP-адреса и домены, связанные с преступной активностью, сигнатуры вредоносного ПО, имена файлов и пользователей, адреса электронной почты, описание деятельности АРТ-группировок и применяемые ими инструменты), средства ее реализации, индикаторы, последствия и действенные рекомендации [81, 151].

33 Значимый объект критической информационной инфраструктуры (значимый объект КИИ): объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ (статья 2, 149-ФЗ [6]).

34 Зоны (или контуры) безопасности Центра интеллектуального управления сетевой безопасностью (зоны безопасности ЦИУСБ): абстрактные выделенные в инфраструктуре ЦИУСБ части, имеющие установленные границы и связанные между собой разрешенными потоками управляющих данных и данных об ИБ ИТКС ОРГАНИЗАЦИИ [254]. В одной зоне (или подзоне) безопасности ЦИУСБ находится совокупность объектов защиты, используемая для реализации бизнес-процессов и (или) технологических процессов ЦИУСБ одинаковой степени критичности (важности), для которой применяется единая политика (режим) защиты информации (единый набор требований к обеспечению ИБ информации) (адаптировано на основе [144]).

35 Индикатор компрометации (англ. *Indicator of Compromise, IoC*): артефакты как описанные специалистами признаки, отражающие наблюдаемые события, действия, объекты и т.п. в сети, ОС, СУБД, приложении, на рабочей станции, сервере и т.п., которые с высокой степенью вероятности указывают на предпринимаемую или уже состоявшуюся атаку. Они используются для описания того, что атака, возможно, уже произошла или может произойти прямо сейчас или в будущем, то есть для обнаружения попыток проникновения в компьютерные системы на ранних стадиях и первичной оценки возможного ущерба. Примеры *IoC*: адреса командных серверов ботнетов (англ. *botnet*, от *robot network*), электронные адреса рассыльщиков фишинговых писем и спама, сигнатуры вирусов, хэш-суммы вредоносных файлов.

36 Инструментальные средства аудита (англ. *audit tools*): автоматизированные инструментальные средства, помогающие анализировать содержание журналов событий (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

37 Интеллектуальная безопасность или ИБ-аналитика (англ. *Security Intelligence* или *Information Security Intelligence*): Сбор, нормализация и анализ в режиме реального времени данных, генерируемых пользователями, приложениями и инфраструктурой, которые влияют на ИТ-безопасность и состояние рисков организации [217].

38 Интерфейс (англ. *interface*): совокупность средств и правил, обеспечивающих взаи-

модействие устройств вычислительной машины или системы обработки информации и (или) программ (ГОСТ 15971-90 [104]). Разнотипные системы и сервисы различных уровней взаимодействуют между собой через интерфейсы, а однотипные сервисы одного уровня – по протоколам.

39 Интранет (англ. *intranet*): частная компьютерная сеть, использующая интернет-протоколы и возможность сетевого соединения для безопасного коллективного использования части информации или операций организации ее сотрудниками (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

40 Информационная безопасность (ИБ) (англ. *information security*): защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность (ГОСТ Р ИСО/МЭК 27002-2012 [106]). По аналогии с началом определения ИБ Российской Федерации из «Доктрины информационной безопасности Российской Федерации» [2] ИБ – состояние защищенности информации, обрабатываемой средствами вычислительной техники (СВТ) или автоматизированной системы (АС), от внутренних или внешних угроз: от нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также ее незаконного тиражирования, которые приводят к материальному или моральному ущербу владельца или пользователя информации.

41 Информационная безопасность информационно-телекоммуникационной сети организации (ИБ ИТС организации): состояние защищенности технологических систем ОРГАНИЗАЦИИ, предназначенных для обработки и передачи по линиям связи информации, доступ к которой осуществляется с использованием современных ИТ, СВТ и средств связи, включающее безопасность информационных ресурсов и предоставляемых услуг и обеспечивающее функциональную устойчивость ИТКС в штатном режиме и в условиях угроз ИБ в ЕИП ОРГАНИЗАЦИИ. Защищенность достигается обеспечением совокупности свойств ИБ – конфиденциальности, целостности, доступности, подлинности, подотчетности, неотказуемости и достоверности, приоритетность которых определяется значимостью информации для интересов (целей) организации.

42 Информационная безопасность организации (ИБ организации): состояние защищенности интересов организации в условиях угроз в информационной сфере. Примечание – Защищенность достигается обеспечением совокупности свойств информационной безопасности – конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации (ГОСТ Р 53114-2008 [22]).

43 Информационная защищенность информационно-телекоммуникационной сети организации (информационная защищенность ИТКС организации): такая ее способность, при которой в едином информационном пространстве (ЕИП) ОРГАНИЗАЦИИ создана адекватная защищенная среда ее функционирования, обеспечивающая необходимый уровень ИБ для получения (поиска и сбора), обработки, хранения, распространения (передачи и предоставления) и уничтожения информации. При этом уровень риска нарушения осуществления деятельности ОРГАНИЗАЦИИ с использованием ИТКС и уровень риска нарушения всех свойств ИБ информационных активов ИТКС на всех стадиях их жизненного цикла приемлемы как для их пользователя, так и владельца.

44 Информационная инфраструктура (ИИ) (англ. *information infrastructure*): система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. Примечание. ИИ включает в себя совокупность информационных центров, банков данных и знаний, систем связи и обеспечивает доступ потребителей к информационным ресурсам (СТО БР ИББС-1.0-2014 [65]).

45 Информационная система (ИС) (англ. *information system*): организационно упорядоченная совокупность информационных ресурсов и ИТ, реализующих информационные процессы в традиционном или автоматизированном режиме с использованием технических средств для удовлетворения информационных потребностей пользователей [63]. С точки зрения пользователя (потребителя предоставляемых услуг) ИС – сложная система, включающая всю совокупность аппаратного, системного и прикладного программного обеспечения и методов их организации, обеспечивающая информационную деятельность пользователей и предназначенная для решения каких-либо конкретных прикладных задач предприятия. Эта система организует хранение и манипулирование информацией о предметной области (ГОСТ 34.321-96 [59]). Система обработки информации (СОИ) предоставляет ИС средства для решения этих задач, то есть поддерживает приложения. Предприятие создает свою ИС на основе СОИ.

46 Информационная сфера: совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений (СТО БР ИББС-1.0-2014 [65]).

47 Информационно-коммуникационная технология (ИКТ) (англ. *Information and Communication Technology, ICT*): информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники (СВТ) и средств телекоммуникации (ГОСТ Р 52653-2006 [113]).

48 Информационно-телекоммуникационная инфраструктура (ИТИ): сложная пространственно распределенная технологическая система организационных структур, предназна-

ченная для создания безопасных, простых и надежных сервисов и обеспечивающая функционирование и развитие информационного пространства и средств информационного взаимодействия (адаптировано на основе [5]).

49 Информационно-телекоммуникационная сеть (ИТКС): технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (СВТ) (статья 2, 149-ФЗ [6]).

50 Информационно-телекоммуникационная система (ИТС): сложная иерархическая пространственно распределенная автоматизированная система (АС), обеспечивающая информатизацию функциональной деятельности и предоставляющая информационные и телекоммуникационные сервисы (услуги) пользователям с применением современных информационных технологий (ИТ), средств вычислительной техники (СВТ) и связи (адаптировано на основе [5]).

51 Информационные технологии (ИТ) (англ. *information technology, IT*): ресурсы, используемые для получения, обработки, хранения и распространения информации. Примечание – Это понятие также включает понятие "коммуникационные технологии" и составной термин "информационно-коммуникационные технологии" (ИКТ) (ГОСТ Р ИСО/МЭК 38500-2017 [118]). Реализация ИТ базируется на следующих средствах ИТ: математических как совокупности моделей разного уровня: от моделей принятия решений до частных моделей отдельных информационных процессов; технических, включающих разнообразные средства вычислительной техники (СВТ) и специализированные устройства на их основе – сети, автоматизированные рабочие места, оргтехника и т.д.; алгоритмических как алгоритмов реализации математических средств (моделей) посредством программного обеспечения, операционных систем и т.п.; информационных, включающих банки и базы данных, базы знаний и др.; методических, имеющих вид описаний, инструкций и другой документации по использованию ИТ для решения задач бизнеса.

52 Информационный актив (англ. *information asset*): информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации; находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме (СТО БР ИББС-1.0-2014 [65]).

53 Информационный процесс: процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации (ГОСТ Р 53114-2008 [22]).

54 Информационный ресурс: информационный актив организации, который используется или потребляется в процессе выполнения некоторой деятельности, и используемая для его обработки информационная инфраструктура (адаптировано на основе СТО БР ИББС-1.0-2014 [65]).

55 Информация: сведения о лицах, предметах, фактах, событиях, явлениях и процессах

независимо от формы их представления (ГОСТ Р 50922-96 [111]).

56 Инфраструктура: комплекс взаимосвязанных обслуживающих структур, составляющих основу для решения проблемы (задачи) (СТО БР ИББС-1.0-2014 [65]).

57 Инфраструктура центра интеллектуального управления сетевой безопасностью (инфраструктура ЦИУСБ) организации: специализированный комплекс современных организационных, технических, аппаратно-программных, технологических и других мероприятий и средств, который обеспечивает ИБ информации ИТКС и самой ЦИУСБ на всех стадиях их жизненного цикла.

58 Инцидент информационной безопасности (инцидент ИБ) (англ. *information security incident, IS incident*): появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операций и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации (ISO/IEC 27035-1:2016 [69]).

59 Источник угрозы ИБ: субъект (физическое лицо, материальный объект или физическое явление), использующий уязвимости для реализации угроз ИБ.

60 ИТ-оборудование (сетевое, телекоммуникационное оборудование): технические средства (устройства, оборудование), используемые для построения сетей (систем) передачи данных (телекоммуникационных сетей). Например, активное телекоммуникационное оборудование: маршрутизатор, коммутатор, концентратор, мост, репитер (повторитель), сетевой адаптер, модем, сетевой трансивер, медиаконвертер, принт-сервер и т.п., и пассивное телекоммуникационное оборудование, не получающее питание от электрической сети или других источников : розетки, кабели и кабель-каналы, вилки, патчкорды, коннекторы, телекоммуникационные шкафы, монтажные шкафы, стойки, кабельные органайзеры и т.д. (адаптировано на основе ГОСТ Р 51513-99 [62] и [63]).

61 ИТ-услуги (услуги информационных технологий или услуги ИТ) (англ. *IT services*): совокупность функциональных возможностей информационных и, возможно, неинформационных технологий, предоставляемая конечным пользователям в качестве услуги. Примечание – Примерами услуг ИТ могут служить передача сообщений, бизнес-приложения, сервисы файлов и печати, сетевые сервисы и т.д. (ГОСТ Р 53114-2008 [22]).

62 Канал связи (передачи данных) (англ. *(tele)communication channel*): часть сети, связывающая между собой каждую пару ее конечных терминалов и состоящая из технических средств передачи и приема данных, включая линию связи, а также средств программного обеспечения и протоколов. В зависимости от характера, принципа построения, назначения и использования различают каналы проводной, оптоволоконной, радио, телефонной, телеграфной, компьютерной, аналоговой, цифровой, дуплексной (двухсторонней) связи и т.д. [301].

63 Катастрофоустойчивость ЦИУСБ ОРГАНИЗАЦИИ: способность ЦИУСБ сохранять критически важные ресурсы и продолжать выполнение своих функций, возможно с определенными ограничениями, в условиях деградации его архитектуры, вызванной уничтожением элементов и связей между ними в результате стихийных бедствий, техногенных аварий и катастроф, целенаправленного воздействия людей или групп людей.

64 Кибербезопасность (англ. *cyber security*): сохранение конфиденциальности, целостности, доступности и других важных свойств активов пользователей и организаций типа подлинности, подотчетности, неотказуемости и достоверности в киберпространстве (ISO/IEC 27032:2012 [101]).

65 Киберпространство (англ. *cyber space*): комплекс среды и, как следствие в результате взаимодействия людей, программного обеспечения (ПО) и услуг в Интернете с помощью технологии устройств и сетей, подключенных к ней, которых не существует в любой физической форме (ISO/IEC 27032:2012 [101]).

66 Кластер: объединение нескольких однородных элементов, которое может рассматриваться как самостоятельная единица, обладающая определенными свойствами (ГОСТ Р 57429-2017 [302]).

67 Коммутатор (англ. *switch*): устройство, обеспечивающее соединение сетевых устройств посредством внутренних механизмов коммутации, с технологией коммутации, обычно реализованной на втором или третьем уровне эталонной модели взаимодействия открытых систем *OSI/ISO*. Примечание – Коммутаторы отличаются от других соединительных устройств локальной сети (например, концентраторов), так как используемая в коммутаторах технология устанавливает соединения на основе «точка – точка» (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

68 Комплекс средств автоматизации (КСА): совокупность взаимосогласованных компонентов и комплексов программного, технического и информационного обеспечения, разрабатываемая, изготавливаемая и поставляемая как продукция производственно-технического назначения, или совокупность всех компонентов автоматизированной системы, за исключением людей [63].

69 Компьютерная атака (англ. *computer attack*): целенаправленное воздействие программных и (или) аппаратно-программных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации (статья 2, 187-ФЗ [7]).

70 Конфиденциальность (англ. *confidentiality*): свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов (ГОСТ Р ИСО/МЭК 27000-2012 [117]).

71 Концентратор (англ. *hub*): сетевое устройство, которое функционирует на первом уровне эталонной модели взаимодействия открытых систем *OSI/ISO*. Примечание – Сетевые концентраторы не являются интеллектуальными устройствами, они обеспечивают только точки физического соединения для сетевых систем или ресурсов (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

72 Корреляция событий информационной безопасности (корреляция событий ИБ): процесс выявления событий ИБ, имеющих логическую связь и потенциально значимых для выявления возможных нарушений ИБ.

73 Критическая информационная инфраструктура (КИИ): объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов (статья 2, 149-ФЗ [6]).

74 Линия связи (англ. *(tele)communication link, circuit*): физическая среда, по которой осуществляется передача данных между терминалами сети. В зависимости от ее характера, принципа построения, назначения и использования различают линии проводной, оптоволоконной, радио-, телефонной, телеграфной, компьютерной и др. видов связи [301].

75 Логирование или ведение контрольных журналов (англ. *logging*): процесс автоматической записи с настраиваемой степенью детализации сведений о происходящих в ИТКС и ее подсистемах событиях в специальные журналы (файлы, базы данных) регистрации. Это фиксирование данных о событиях, связанных с ИБ, в целях проверки, анализа и постоянного мониторинга (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

76 Маршрутизатор (англ. *router*): сетевое устройство, используемое для установления и управления потоками данных между различными сетями путем выбора трактов или маршрутов на основе механизмов и алгоритмов протоколов маршрутизации. Примечания. 1 Сети сами могут быть основаны на разных протоколах. 2 Информация о маршрутизации хранится в таблице маршрутизации (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

77 Масштабируемость: способность к увеличению/уменьшению производительности и затрат в ответ на изменения в потребностях АО, приложений, систем обработки данных и т.п. [224].

78 Межсетевой экран (МЭ) (англ. *firewall*): программные и программно-технические средства, реализующие функции контроля и фильтрации в соответствии с заданными правилами проходящих через них информационных потоков и используемые в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа (Информационное сообщение № 240/24/1986 [103]).

79 Межсетевой экран уровня веб-сервера (тип «Г»): межсетевой экран, применяемый

на сервере, обслуживающем сайты, веб-сервисы и веб-приложения, или на физической границе сегмента таких серверов (сервера) (Информационное сообщение № 240/24/1986 [103]).

80 Межсетевой экран уровня логических границ сети (тип «Б»): межсетевой экран, применяемый на логической границе (периметре) информационной системы (ИС) или между логическими границами сегментов ИС (Информационное сообщение № 240/24/1986 [103]).

81 Межсетевой экран уровня промышленной сети (тип «Д»): межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами (Информационное сообщение № 240/24/1986 [103]).

82 Межсетевой экран уровня сети (тип «А»): межсетевой экран, применяемый на физической границе (периметре) информационной системы (ИС) или между физическими границами сегментов ИС (Информационное сообщение № 240/24/1986 [103]).

83 Межсетевой экран уровня узла (тип «В»): межсетевой экран, применяемый на узле (хосте) информационной системы (ИС) (Информационное сообщение № 240/24/1986 [103]).

84 Мера обеспечения информационной безопасности (мера обеспечения ИБ), ранее мера и средство контроля и управления ИБ (англ. *control*): средство менеджмента риска, включающее в себя политики, процедуры, рекомендации, инструкции или организационные структуры, которые могут быть административного, технического, управленческого или правового характера. Примечание – Термин «мера и средство контроля и управления» также используется как синоним терминов «защитная мера» (англ. *safeguard*) или «контрмера» (англ. *countermeasure*) (ГОСТ Р ИСО/МЭК 27002-2012 [106]).

85 Модели зрелости центра управления безопасностью (модель зрелости ЦУБ): модель оценки процессов управления сетевой безопасностью ИТКС ОРГАНИЗАЦИИ в ее ЦУБ.

86 Модель угроз информационной безопасности (модель угроз ИБ): описание источников угроз ИБ; уязвимостей, используемых источниками угроз ИБ; объектов, пригодных для реализации угрозы ИБ; методов реализации угроз ИБ; типов возможной потери (например, конфиденциальности, целостности, доступности ИА); масштабов потенциального ущерба (СТО БР ИББС-1.0-2014 [65]).

87 Модель нарушителя информационной безопасности (модель нарушителя ИБ): описание и классификацию нарушителей ИБ, включая определение их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей (СТО БР ИББС-1.0-2014 [65]).

88 Мониторинг информационной безопасности и контроль защитных мер (мониторинг ИБ): процесс постоянного (непрерывного) наблюдения за регистрируемыми событиями, влияющими на обеспечение ИБ, а также сбор, анализ и обобщение результатов наблю-

дений [171].

89 Мониторинг информационной безопасности и контроль защитных мер ИТКС организации (мониторинг ИБ ИТКС организации): процесс постоянного (непрерывного) наблюдения за регистрируемыми событиями, влияющими на обеспечение ИБ ИТКС организации, а также сбор, анализ и обобщение результатов наблюдений (адаптировано на основе [171]).

90 Надежность (англ. *reliability*): свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования. Примечание. Надежность является комплексным свойством, которое в зависимости от назначения объекта и условий его применения может включать безотказность, долговечность, ремонтпригодность и сохраняемость или определенные сочетания этих свойств (ГОСТ 27.002-89 [303]).

91 Нарушитель (англ. *attacker*): любое лицо, преднамеренно использующее уязвимости технических и нетехнических мер и средств контроля и управления безопасностью с целью захвата или компрометации информационных систем (ИС) и сетей, или снижения доступности ресурсов ИС и сетевых ресурсов для законных пользователей (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

92 Национальный координационный центр по компьютерным инцидентам (НКЦКИ): составная часть сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, задачей которого является обеспечение координации деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (Приказ № 366 [102]).

93 Неотказуемость (англ. *non-repudiation*): способность удостоверить имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение (ГОСТ Р ИСО/МЭК 27000-2012 [117]).

94 Несанкционированный доступ (НСД): доступ к информации или к ресурсам автоматизированной ИС, осуществляемый с нарушением установленных прав и (или) правил доступа (ГОСТ Р 53114-2008 [22]).

95 Непрерывность функционирования центра интеллектуального управления сетевой безопасностью в едином информационном пространстве организации (непрерывность функционирования ЦИУСБ в ЕИП ОРГАНИЗАЦИИ): стратегическая и тактическая способность ЦИУСБ планировать свою работу в случае инцидентов ИБ и нарушений его функционирования, направленная на обеспечение непрерывности бизнес-процессов на установленном

приемлемом уровне.

96 Нормализация данных: приведение получаемых от различных источников данных к формату, необходимому для дальнейшей их обработки и хранения.

97 Обеспечение информационной безопасности (обеспечение ИБ): осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления (Указ Президента РФ № 646 [2]).

98 Обеспечение информационной безопасности информационно-телекоммуникационной системы: деятельность, направленная на реализацию мер по защите информационных ресурсов информационно-телекоммуникационной системы от несанкционированного доступа (НСД), случайного или преднамеренного вмешательства в нормальное использование или попыток их разрушения [63].

99 Обеспечение информационной безопасности информационно-телекоммуникационной сети (обеспечение ИБ ИТКС): деятельность, направленная на реализацию мер по защите ИТКС от компьютерных атак и представляемая сложным процессом, состоящим из множества подпроцессов поддержания безопасного (защищенного) состояния всех ее элементов в отдельности (информационных ресурсов) и ИТКС в целом (объединяющей информационной инфраструктуры) как основы обеспечения ИБ ЕИП ОРГАНИЗАЦИИ.

100 Обеспечение сетевой безопасности информационно-телекоммуникационной сети (обеспечение сетевой безопасности ИТКС): деятельность, направленная на обеспечение безопасности устройств ИТКС, обеспечение безопасности управления этими устройствами, приложениями, предоставляемыми услугами и конечными пользователями, в дополнение к обеспечению безопасности информации, передаваемой по линиям связи ИТКС.

101 Обнаружение вторжений (англ. *intrusion detection*): формальный процесс обнаружения вторжений, обычно характеризующийся сбором сведений об аномальном характере использования, а также о том, какая уязвимость была использована и каким образом, включая то, когда и как это произошло (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

102 Обработка инцидента (англ. *incident handling*): Действия по выявлению, отчетности, оценке, реагированию, решению и извлечению опыта из инцидентов ИБ (ISO/IEC 27035-1:2016 [68]).

103 Обработка рисков информационной безопасности (обработка рисков ИБ) (англ. *IS risk treatment*): общий процесс идентификации, анализа и оценивания риска ИБ [132].

104 Объект защиты информации: информация или носитель информации, или инфор-

мационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 50922-2006 [111]).

105 Объект управления: система (организация, коллектив и т.п.), на которую направлены все виды управленческого воздействия с целью ее совершенствования, повышения качества функций и задач, успешного достижения запланированной цели (целей) [172].

106 Объекты критической информационной инфраструктуры (объекты КИИ): информационные системы (ИС), информационно-телекоммуникационные сети (ИТС), автоматизированные системы управления (АСУ) субъектов КИИ (статья 2, 149-ФЗ [6]).

107 Озеро данных (англ. *data lakes*): масштабируемое хранилище огромного количества необработанных данных в исходном формате («как есть»), пока они не понадобятся, промежуточных и конечных результатов их обработки, а также система обработки, которая может принимать данные независимо от их структуры.

108 Операционная устойчивость (англ. *operational resilience*): способность системы регулировать функционирование с целью поддержания выполнения операций при ожидаемых условиях и при ужесточении требований, нарушениях и непредвиденных обстоятельствах [23].

109 Операционный риск (англ. *operational risk*), **или риск нарушения функционирования ЦИУСБ:** риск убытка организации в результате неадекватных или ошибочных внутренних процессов ЦИУСБ, действий его работников и систем или внешних событий (адаптировано на основе [278]).

110 Остаточный риск информационной безопасности (остаточный риск ИБ) (англ. *IS residual risk*): риск ИБ, остающийся после обработки риска ИБ [132].

111 Отказ в обслуживании (англ. *denial of service; DoS*): прекращение санкционированного доступа к ресурсам системы или задержка операций и функций системы, приводящее в итоге к потере доступности для авторизованных пользователей (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

112 Отказоустойчивость (англ. *failure-related durability*): свойство образца в целом и (или) его функциональных систем и составных частей, характеризующее способность обеспечивать завершение цикла применения по назначению в ожидаемых условиях эксплуатации при возможных отказах без неприемлемого вреда лицам или имуществу, за исключением вреда, предусмотренного целевым назначением образца (ГОСТ Р 56112-2014 [304]).

113 Отказоустойчивость системы: способность функционировать даже после того, как появилось определенное число неисправностей или событий более низкого уровня, приводящих к отказу системы (ГОСТ Р 27.302-2009 [305]).

114 Отказоустойчивость ЦИУСБ ОРГАНИЗАЦИИ: способность сохранять работоспособность при случайных выходах из строя или сбоях отдельных элементов ЦИУСБ.

115 Отчетность (ресурсов ИС) (англ. *accountability*): состояние ресурсов ИС, при котором обеспечиваются идентификация и регистрация действий с ними (Р 50.1.056-2005 [122]).

116 «Охота за угрозами» (англ. *Threat Hunting*): постоянная упреждающая и интерактивная деятельность, заключающаяся в поиске, обнаружении, локализации и анализе угроз, которые обходят существующие превентивные СЗИ [87].

117 Оценка рисков информационной безопасности (оценка рисков ИБ) (англ. *IS risk assessment*): оценка угроз ИБ, их последствий, уязвимостей информации и средств ее обработки, а также вероятности их возникновения [132].

118 Пакет (англ. *packet*): объект, содержащий четко определенный блок байтов, состоящий из заголовка, данных и необязательного трейлера (концевика, от англ. *trailer*), который может передаваться по сетям или по телефонным линиям (ISO/IEC 27033-4:2014 [126]).

119 Периметр сети (англ. *network perimeter*): физическая или логическая подсеть, которая содержит и предоставляет внешние сервисы организации для публичной сети (ISO/IEC 27033-4:2014 [126]).

120 Песочница (англ. *sandbox*): замкнутая среда предварительного выполнения программ или изолированный карантин (специфический пример виртуализации), используемый для тестирования подозрительного ПО путем его запуска в выделенной области памяти, имитирующей программную среду функционирования, и анализа его дальнейшего поведения.

121 Подлинность (англ. *authenticity*): свойство, гарантирующее, что субъект или ресурс идентичен заявленному (ГОСТ Р ИСО/МЭК 27000-2012 [117]).

122 Подотчетность (англ. *accountability*): ответственность субъекта за его действия и решения (ГОСТ Р ИСО/МЭК 27000-2012 [117]).

123 Политика безопасности (информации в организации): совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности (ГОСТ Р 50922-2006 [111]).

124 Политика безопасности информационно-коммуникационных технологий (политика безопасности ИКТ) или Политика безопасности информационно-телекоммуникационных технологий (англ. *ICT security policy*): правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию (ГОСТ Р ИСО/МЭК 13335-1-2006 [174]).

125 Политика информационной безопасности (организации) (Политика ИБ (организации)) (англ. *information security policy*): формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопас-

ности, которыми руководствуется организация в своей деятельности. Примечание – Политики должны содержать: предмет, основные цели и задачи политики безопасности; условия применения политики безопасности и возможные ограничения; описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом; права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации; порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности (ГОСТ Р 53114-2008 [22]).

126 Политика обеспечения сетевой безопасности или политика сетевой безопасности (англ. *network security policy*): совокупность положений, правил и практических приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как должна обеспечиваться защита ее сетевой инфраструктуры и сервисов (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

127 Порт (англ. *port*): конечная точка соединения. Примечание – В контексте Интернет-протокола порт представляет собой конечную точку логического канала *TCP*- или *UDP*-соединения. Протоколы приложений на основе *TCP* или *UDP* обычно имеют назначенные по умолчанию номера портов, например, порт 80 для *HTTP* (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

128 Правила фильтрации: перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных), и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций (Информационное сообщение № 240/24/1986 [103]).

129 Предотвращение вторжений (англ. *intrusion prevention*): формальный процесс активного реагирования с целью предотвращения вторжений (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

130 Предупреждение об опасности или сигнал тревоги (англ. *alert or alarm*): “немедленное” оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие аварии, сбоя или человеческой ошибки (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

131 Протокол передачи данных: набор правил и соглашений, определяющих содержание, формат, параметры времени, последовательность и проверку ошибок в сообщениях, которыми обмениваются сетевые устройства (ГОСТ Р 54619-2011 [115]).

132 Протокол: свод правил и форматов, определяющих взаимодействие объектов одноименных (одинаковых) уровней различных систем или совокупность правил, регламентирующих формат и процедуры обмена информацией между двумя или несколькими независимыми

устройствами или процессами [63]. Разнотипные системы и сервисы различных уровней взаимодействуют между собой через интерфейсы, а однотипные сервисы одного уровня – по протоколам.

133 Процесс: совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующая входы в выходы и требующая для этого определенных ресурсов и управляющих воздействий (управления) [172].

134 Процессный подход: систематическая идентификация и управление применяемых организацией бизнес-процессов и особенно взаимодействия таких процессов [172].

135 Расследование информационной безопасности (англ. *information security investigation*): Проведение экспертизы, анализа и обработка результатов анализа, которые способствуют пониманию инцидента ИБ (ISO/IEC 27035-1:2016 [68]).

136 Реагирование на инцидент (англ. *incident response*): Действия, предпринятые для смягчения или устранения инцидента ИБ, включая меры, принятые для защиты и восстановления нормальных рабочих режимов эксплуатации информационной системы и информации, хранящейся в ней (ISO/IEC 27035-1:2016 [68]).

137 Результативность (продуктивность) процесса: степень реализации запланированной деятельности и достижения запланированных результатов [171].

138 Ресурс: актив организации, который используется или потребляется в процессе выполнения некоторой деятельности (СТО БР ИББС-1.0-2014 [65]).

139 Риск (англ. *risk*): следствие влияния неопределенности на достижение поставленных целей. Примечания – 1. Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное). 2. Цели могут быть различными по содержанию (в области экономики, здоровья, экологии и т.п.) и назначению (стратегические, общеорганизационные, относящиеся к разработке проекта, конкретной продукции и процессу). 3. Риск часто характеризуют путем описания возможного события и его последствий или их сочетания. 4. Риск часто представляют в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности. 5. Неопределенность — это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей (ГОСТ Р ИСО 31000-2019 [116]).

140 Риск нарушения ИБ (риск ИБ): потенциальная возможность использования уязвимостей актива/группы активов конкретной угрозой ИБ для причинения ущерба организации. Измеряется исходя из комбинации вероятности события и его последствия (РС БР ИББС-2.2-2009 [66]).

141 Сервис: группа компонентов (функциональных блоков, модулей) системы, которая предоставляет другим группам (блокам, модулям) некоторый законченный в функциональном

отношении пакет услуг, доступных через специфицированные интерфейсы, и сам может пользоваться услугами других модулей через соответствующие интерфейсы. Компоненты могут взаимодействовать между собой сложным образом, чаще всего образуя иерархическую или уровневую структуру. При этом однотипные сервисы одного уровня взаимодействуют между собой по протоколам, а разнотипные и сервисы различных уровней – через интерфейсы [55].

142 Сетевая атака (англ. *network attack*): компьютерная атака с использованием протоколов межсетевого взаимодействия (Р 50.1.053-2005 [121], Р 50.1.056-2005 [122], ГОСТ Р 51275-2006 [112]).

143 Сетевая безопасность или безопасность сети (англ. *network security*) в дополнение к безопасности информации, передаваемой по линиям связи, затрагивает безопасность устройств, безопасность деятельности по управлению данными устройствами, приложениями/услугами и конечными пользователями (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

144 Сетевая безопасность информационно-телекоммуникационной сети или сетевая безопасность ИТКС: безопасность устройств ИТКС, безопасность деятельности по управлению этими устройствами, приложениями, предоставляемыми услугами и конечными пользователями, в дополнение к безопасности информации, передаваемой по линиям связи ИТКС (адаптировано на основе ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

145 Сетевое (ИТ-, телекоммуникационное) оборудование: технические средства (устройства, оборудование), используемые для построения сетей (систем) передачи данных (телекоммуникационных сетей). Например, активное телекоммуникационное оборудование: маршрутизатор, коммутатор, концентратор, мост, репитер (повторитель), сетевой адаптер, модем, сетевой трансивер, медиаконвертер, принт-сервер и т.п., и пассивное телекоммуникационное оборудование, не получающее питание от электрической сети или других источников : розетки, кабели и кабель-каналы, вилки, патчкорды, коннекторы, телекоммуникационные шкафы, монтажные шкафы, стойки, кабельные органайзеры и т.д. (адаптировано на основе ГОСТ Р 51513-99 [62] и [63]).

146 Сетевой анализатор пакетов или сниффер (англ. *network analyzer or network sniffer*): устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика. Примечание – До проведения анализа информационного потока информация должна быть собрана определенным образом, например, путем использования сетевого анализатора пакетов (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

147 Сетевой мониторинг (англ. *network monitoring*): процесс постоянного наблюдения и проверки зафиксированных данных о сетевой деятельности и операциях, включая контрольные журналы и оповещения об опасности, и связанный с этим анализ (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

148 Сеть связи: технологическая система, включающая в себя средства связи и линии связи и предназначенная для электросвязи или почтовой связи (ГОСТ Р 53801-2010 [114]).

149 Сигнал тревоги или предупреждение об опасности (англ. *alert or alarm*): “немедленное” оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие аварии, сбоя или человеческой ошибки (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

150 Система информационных технологий (система ИТ) и тождественная по смыслу система информационно-коммуникационных технологий (система ИКТ) (англ. *information and communication technology system, ICTS*): совокупность телекоммуникационного (включая сетевое) оборудования, аппаратных и программных средств и систем обработки информации, предназначенных для комплексного управления бизнес-процессами организации с применением средств вычислительной техники (СВТ) и телекоммуникаций (адаптировано на основе ГОСТ Р ИСО/МЭК 27031-2012 [306] и ГОСТ Р 52653-2006 [113]).

151 Система обработки информации (СОИ) (англ. *information processing system*): совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации (ГОСТ 15971-90 [103]). СОИ – это техническая основа, на которой строится информационная система (ИС). СОИ предоставляется ИС средства для решения организации, то есть обеспечивает поддержку информационной деятельности пользователей. Термин используется, когда ИС рассматривается с точки зрения конструктора, проектировщика, программиста.

152 Система: множество (совокупность) элементов (объектов) любой, в том числе различной физической, природы и информационных объектов, взаимодействующих между собой для достижения общей цели и обладающее системным свойством/свойствами, которое не имеет ни один из элементов множества и ни одно из подмножеств элементов при любом способе членения (адаптировано на основе СТО БР ИББС-1.0-2014 [65]).

153 Система обеспечения информационной безопасности (СОИБ) организации: система поддержания состояния защищенности единого информационного пространства (информационных активов, информационных процессов, ИТ-услуг, хранилищ информации, средств обработки и передачи информации и т.п.) организации. СОИБ состоит из системы управления ИБ (СУИБ) и мер обеспечения ИБ. СОИБ включает в себя организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы, меры и средства и ресурсы, необходимые для обеспечения ИБ организации.

154 Система обнаружения вторжений (англ. *Intrusion Detection System, IDS*): специализированная система, используемая для идентификации того факта, что была предпринята попытка вторжения, вторжение происходит или произошло, а также для возможного реагирования

на вторжение в информационные системы и сети (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

155 Система предотвращения вторжений (англ. *Intrusion Prevention System, IPS*): вид систем обнаружения вторжений, специально предназначенных для обеспечения активной возможности реагирования (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

156 Система предотвращения утечки конфиденциальной информации (DLP-система): специализированная система, предназначенная для предотвращения неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами (ГОСТ Р 53114-2008 [22]).

157 Система управления информационной безопасностью информационно-телекоммуникационной сети (СУИБ ИТКС) организации: часть общей системы управления организации, основанная на риск-ориентированном подходе (на оценке бизнес-рисков и рисков ИБ в частности), предназначенная для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ, и включающая организационную структуру, политику, планирование действий, роли и обязанности, установившийся порядок, процедуры, процессы, меры обеспечения ИБ и ресурсное обеспечение для эффективного управления ИБ ИТКС [172].

158 Системный подход: методологическое направление исследования объекта как системы с разных сторон, комплексно, в совокупности отношений и связей между его элементами [172].

159 Системы телекоммуникационной инфраструктуры: комплекс технических средств, обеспечивающих безопасную передачу сообщений с заданными параметрами на любые расстояния.

160 Снижение/уменьшение риска информационной безопасности (англ. *IS risk reduction*): действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском ИБ [132].

161 Сниффер или сетевой анализатор пакетов (англ. *network analyzer or network sniffer*): устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика. Примечание – До проведения анализа информационного потока информация должна быть собрана определенным образом, например, путем использования сетевого анализатора пакетов (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

162 Событие информационной безопасности (событие ИБ) (англ. *information security event, IS event*): идентифицированное появление определенного состояния актива организации (системы, сервиса или сети), указывающего на возможное нарушение Политики ИБ или нару-

шения в работе средств защиты или неспособность защитной меры обеспечить адекватную защиту информационного актива, либо возникновение ранее неизвестной ситуации, которая может иметь отношение к ИБ (адаптировано на основе ISO/IEC 27035-1:2016 [68]).

163 Соединение (электросвязи): установленное в результате вызова или предварительно установленное взаимодействие между средствами электросвязи, позволяющее пользователю передавать и/или принимать информацию (ГОСТ Р 53801-2010 [114]).

164 Спуффинг (англ. *spoofing*): маскировка под легального пользователя или сетевой ресурс (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

165 Среда обработки информационного актива (СОИА): среда использования и (или) эксплуатации информационного актива, в которой осуществляется получение (поиск и сбор), обработка, хранение, распространение (передача и предоставление) и уничтожение информации (РС БР ИББС-2.2-2009 [66]).

166 Средства вычислительной техники (СВТ): совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (ГОСТ Р 50739-95 [110]).

167 Средство антивирусной защиты (САЗ): программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации (Профили защиты средств антивирусной защиты [307]).

168 Стратегия информационной безопасности организации (стратегия ИБ организации): официально принятая руководством организации система взглядов на проблему обеспечения ее ИБ, методы и средства защиты жизненно важных интересов организации в информационной сфере, включая ИБ ИТКС организации. Эта система взглядов определяет цели, задачи, принципы и основные направления обеспечения ИБ организации и обеспечивается взаимовязываемыми правовыми, организационными, аппаратно-программными, техническими и иными мерами обеспечения ИБ и в качестве обратной связи основывается на постоянном анализе защищенности ИТКС организации средствами мониторинга ИБ для выявления и последующего устранения уязвимостей, угроз ИБ и уже состоявшихся инцидентов ИБ с прослеживанием динамики их развития и недопущения их проявления в будущем.

169 Субъект управления: лицо, группа лиц или специально созданный орган, являющийся носителем управленческого воздействия на объект (управляемую систему), осуществляющий деятельность, направленную на сохранение качественной специфики, обеспечение его нормального функционирования и успешное движение к заданной цели [172].

170 Субъекты критической информационной инфраструктуры (субъекты КИИ):

государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (ИС), информационно-телекоммуникационные сети (ИТС), автоматизированные системы управления (АСУ), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей (статья 2, 149-ФЗ [6]).

171 Телекоммуникационная инфраструктура: совокупность систем, формирующие каналы передачи данных по радиолиниям, волоконно-оптическим и электрическими кабелям. Она может включать вычислительные и мультисервисные сети, системы пакетной *IP*- и классической телефонии, комплексы оперативной и диспетчерской связи, беспроводные и проводные решения доступа к информации (включая интернет), инфраструктуру центров обработки данных (ЦОД), центры обработки вызовов, видеоконференцсвязь и т.п.

172 Телекоммуникационная система: совокупность технических и программных средств, обеспечивающая передачу информации на значительные расстояния с использованием коммутируемых и выделенных линий или специальных каналов связи [5].

173 Телекоммуникационное (ИТ-, сетевое) оборудование: технические средства (устройства, оборудование), используемые для построения сетей (систем) передачи данных (телекоммуникационных сетей). Например, активное телекоммуникационное оборудование: маршрутизатор, коммутатор, концентратор, мост, репитер (повторитель), сетевой адаптер, модем, сетевой трансивер, медиаконвертер, принт-сервер и т.п., и пассивное телекоммуникационное оборудование, не получающее питание от электрической сети или других источников: розетки, кабели и кабель-каналы, вилки, патчкорды, коннекторы, телекоммуникационные шкафы, монтажные шкафы, стойки, кабельные органайзеры и т.д. (адаптировано на основе ГОСТ Р 51513-99 [62] и [63]).

174 Технологическая система (ТС): совокупность функционально взаимосвязанных средств технологического оснащения, предметов производства и исполнителей для выполнения в регламентированных условиях производства заданных технологических процессов или операций. Примечания: 1. К предметам производства относятся: материал, заготовка, полуфабрикат и изделие, находящиеся в соответствии с выполняемым технологическим процессом в стадии хранения, транспортирования, формообразования, обработки, сборки, ремонта, контроля и испытаний. 2. К регламентированным условиям производства относятся: регулярность поступ-

ления предметов производства, параметры энергоснабжения, параметры окружающей среды и др. 3. Следует различать четыре иерархических уровня технологических систем: технологические системы операций, технологические системы процессов, технологические системы производственных подразделений и технологические системы предприятий (ГОСТ 27.004-85 [56]).

175 Туннель (англ. *tunnel*): канал передачи данных между сетевыми устройствами, который устанавливается через существующую сетевую инфраструктуру. Примечание – Туннели могут устанавливаться путем использования таких технических приемов, как протокольная инкапсуляция, коммутация на основе меток или виртуальный канал (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

176 Угроза (англ. *threat*): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ Р 50922-2006 [111]).

177 Угроза нарушения информационной безопасности организации (угроза ИБ организации): совокупность факторов и условий, создающих опасность нарушения ИБ организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации. Примечания: 1. Формой реализации (проявления) угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств ИБ объекта(ов) защиты организации. 2. Угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы (ГОСТ Р 53114-2008 [22]).

178 Угроза нарушения информационной безопасности информационно-телекоммуникационной сети организации (угроза ИБ ИТКС организации): совокупность факторов и условий, создающих опасность нарушения ИБ ИТКС организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для нее. Формой реализации (проявления) угрозы ИБ является наступление одного или нескольких взаимосвязанных событий ИБ и инцидентов ИБ, приводящего(их) к нарушению свойств ИБ объекта(ов) ИТКС организации (адаптировано на основе ГОСТ Р 53114-2008 [22]).

179 Удаленный доступ (англ. *remote access*): процесс получения доступа к сетевым ресурсам из другой сети или с терминала, не являющегося постоянно соединенным физически или логически с сетью, к которой он получает доступ (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

180 Удаленный пользователь (англ. *remote user*): пользователь, находящийся на объекте (площадке, филиале), отличном от того, на котором размещаются используемые сетевые ресурсы (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

181 Управление инцидентами информационной безопасности (управление инцидентами ИБ): состоящий из ряда подпроцессов процесс, на вход которого поступают данные, полученные в результате сбора и протоколирования затрагивающих ИС событий ИБ, а на вы-

ходе – информация о причинах произошедшего инцидента ИБ, нанесенном организации ущербе и мерах, которые необходимо принять для того, чтобы инцидент ИБ не повторился вновь [168].

182 Управление рисками информационной безопасности (управление рисками ИБ) (англ. *IS risk management*): скоординированная непрерывная деятельность по руководству и управлению организацией в отношении рисков ИБ на основе политики управления рисками ИБ и плана обработки рисков ИБ, обычно включающие в себя установление контекста управления рисками ИБ, оценку, обработку, принятие, мониторинг, пересмотр и коммуникацию рисков ИБ [132].

183 Управление информационной безопасностью информационно-телекоммуникационной сети организации (ИБ ИТКС организации): циклический процесс, который состоит из совокупности целенаправленных действий, осуществляемых для достижения заявленных бизнес-целей организации посредством обеспечения информационной защищенности ее ИТКС как основы единого информационного пространства (ЕИП) в условиях угроз ИБ в информационной сфере [172].

184 Управление сетевой безопасностью информационно-телекоммуникационной сети организации (управление сетевой безопасностью ИТКС организации): циклический процесс, который состоит из совокупности целенаправленных действий, осуществляемых для управления безопасностью устройств ИТКС, используемых приложений, предоставляемых услуг и конечных пользователей, в дополнение к управлению безопасностью информации, передаваемой по линиям связи ИТКС, в целях безопасного, надежного и устойчивого функционирования ИТКС ОРГАНИЗАЦИИ в течение всего ее жизненного цикла.

185 Услуга; сервис (англ. *service*): результат деятельности исполнителя по удовлетворению потребности потребителя. Примечание – В качестве исполнителя (потребителя) услуги может выступать организация, физическое лицо или процесс (ГОСТ Р 53114-2008 [22]).

186 Услуги информационных технологий (услуги ИТ или ИТ-услуги) (англ. *IT services*): совокупность функциональных возможностей информационных и, возможно, неинформационных технологий, предоставляемая конечным пользователям в качестве услуги. Примечание – Примерами услуг ИТ могут служить передача сообщений, бизнес-приложения, сервисы файлов и печати, сетевые сервисы и т.д. (ГОСТ Р 53114-2008 [22]).

187 Уязвимость (англ. *vulnerability*): уязвимость (информационной системы) – свойство ИС, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Примечания – 1. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в ИС. 2. Если уязвимость соответствует угрозе, то существует риск (ГОСТ Р 50922-2006 [111]).

188 Уязвимость «нулевого дня» (англ. *0day, zero day*): уязвимость, которая становится

известной до момента выпуска разработчиком компонента информационной системы соответствующих мер защиты информации, исправлений недостатков или соответствующих обновлений (ГОСТ Р 56545-2015 [142]).

189 «Фи́ды» (англ. *Threat Intelligence Feeds*) **или потоки информации**: непрерывные потоки структурированных постоянно обновляемых знаний об угрозах ИБ, полученных в результате применения ИБ-аналитики к исходным собранным данным и передаваемым организациям-подписчикам чаще всего из внешних источников. К ним относятся бесплатные и платные каналы информации о *IoC*, бюллетени, внутренняя разведывательная информация организаций и их стратегических партнеров, информация известных в данной области компаний (типа *SANS*) и закрытых сообществ обмена информацией, относящиеся к конкретным отраслям или приоритетным областям.

190 Фильтрация (англ. *filtering*): процесс приема или отклонения потоков данных в сети в соответствии с определенными критериями (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]). Это выборка данных из всех данных по определенным критериям.

191 Функциональная устойчивость (от англ. *operational resilience*) центра интеллектуального управления сетевой безопасностью в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций): способность ЦИУСБ регулировать свое функционирование в ЕИП ОРГАНИЗАЦИИ с целью поддержания выполнения его бизнес-процессов при ожидаемых условиях и в условиях ужесточения требований, нарушений, угроз ИБ и непредвиденных обстоятельств (адаптировано на основе [23]).

192 Хост или узел (англ. *host*): компьютер или другое устройство, подключенное к интранету/интернету и имеющее уникальный адрес.

193 Хост-бастион (англ. *bastion host*): специальный хост с усиленной операционной системой (ОС), который используется для перехвата пакетов, входящих или исходящих из сети, и системы, к которой обычно должен подключаться любой посторонний, чтобы получить доступ к сервису или системе, которая находится в МЭ организации (ISO/IEC 27033-4:2014 [126]).

194 Целостность (англ. *integrity*): свойство сохранения правильности и полноты активов (ГОСТ Р ИСО/МЭК 27000-2012 [117]).

195 Целостность информации: состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право (Р 50.1.056-2005 [121]).

196 Цель защиты информации: заранее намеченный результат защиты информации. Примечание – Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непред-

намеренного воздействия на информацию (ГОСТ Р 50922-2006 [111]).

197 Циклическая модель или цикл *PDCA*: от англ. *Plan-Do-Check-Act* – «планируй – выполняй – проверяй – действуй».

198 Цифровая информация (англ. *digital information*): информация, представленная в виде последовательности цифр и доступная для получения (поиска и сбора), обработки, хранения, распространения (передачи и предоставления) и уничтожения с помощью технических устройств в результате применения информационных технологий (ИТ).

199 Шлюз безопасности (англ. *security gateway*): точка соединения между сетями, между сегментами сетей или между программными приложениями в различных доменах безопасности, предназначенная для защиты сети в соответствии с существующей политикой безопасности (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

200 Экранирование: функция межсетевого экрана, позволяющая поддерживать безопасность объектов внутреннего информационного пространства, игнорируя несанкционированные запросы из внешнего информационного пространства (Информационное сообщение № 240/24/1986 [103]).

201 Экстранет (англ. *extranet*): расширение интранета организации, особенно через инфраструктуру общедоступной сети, делающее возможным совместное использование ресурсов организацией, другими организациями и лицами, с которыми она имеет дело, с предоставлением ограниченного доступа к своей интранет (ГОСТ Р ИСО/МЭК 27033-1-2011 [60]).

202 Эластичность: способность системы с течением времени увеличивать нагрузку на свои текущие и дополнительные динамически и автоматически добавляемые по требованию вычислительные ресурсы [224].

203 Эффективность (англ. *efficiency*) **процесса:** экономическая категория, показывающая соотношение между достигнутым результатом (характеристикой результативности) и использованными затратами-ресурсами (время, финансы и т.д.), обеспечившим его получение [171].

204 Эффективность управления информационной безопасностью информационно-телекоммуникационной сети организации (эффективность управления ИБ ИТКС организации): экономическая категория, отражающая вклад управленческой деятельности в отношении обеспечения ИБ ИТКС в конечный результат – уровень ИБ ИТКС и определяемая степенью реализации целей ОРГАНИЗАЦИИ в области обеспечения ИБ ИТКС и ее интегрального показателя – прибыли [171].

205 Эффективность системы управления информационной безопасностью информационно-телекоммуникационной сети организации (эффективность СУИБ ИТКС организации): соотношение между достигнутым уровнем ИБ ИТКС, полученным при управлении ИБ ИТКС на основе СУИБ, и использованными ресурсами, обеспечившим его получение [171].

СПИСОК ЛИТЕРАТУРЫ

1. Okinawa Charter on Global Information Society [Электронный ресурс]: Веб-сайт / MOFA. – 2000. – Режим доступа: <https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html> (дата обращения: 17.09.2020).
2. Доктрина информационной безопасности Российской Федерации // Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 // СЗ РФ, 12.12.2016, № 50. – М., 2000. [Указом Президента Российской Федерации от 05.12.2016 № 646 настоящая Доктрина признана утратившей силу]
3. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года [Указ Президента Российской Федерации от 7 мая 2018 г. № 204] [Электронный ресурс]: Веб-сайт / Президент России. – 2018. – Режим доступа: <http://kremlin.ru/acts/bank/43027> (дата обращения: 17.09.2020).
4. Паспорт национального проекта. Национальная программа «Цифровая экономика Российской Федерации» [утв. решением президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 г.] [Электронный ресурс]: Веб-сайт / Правительство России. – 2018. Режим доступа: https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (дата обращения: 17.09.2020).
5. Руководство по организации эксплуатации информационно-телекоммуникационной системы Банка России: [в 2 томах]. [Электронный ресурс]. – М.: АС «Сфинкс», 2008. – № НМД-4. – 1 электрон, опт. диск (CD-ROM).
6. Об информации, информационных технологиях и о защите информации [федер. закон от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой 8 июля 2006 г.; одобрен Советом Федерации 14 июля 2006 г.]. – 2006. – 88 с.
7. О безопасности критической информационной инфраструктуры Российской Федерации [федер. закон от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой 12 июля 2017 г.; одобрен Советом Федерации 19 июля 2017 г.]. – 2017. – 20 с.
8. TOP 10 2019 Attacks [Электронный ресурс]: Веб-сайт / HACKMAGGEDON. – Hackmageddon, 2020. – Режим доступа: <https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/> (дата обращения: 17.09.2020).
9. Verizon. Data breach report highlights how unsecured cloud storage opens door to attacks. [Электронный ресурс]: Веб-сайт / ZDNET. – Verizon, 2020. – Режим доступа: <https://www.zdnet.com/article/verizons-data-breach-report-highlights-how-unsecured-cloud-storage-opens-door-to-attacks/> (дата обращения: 17.09.2020).

10. Лукацкий, А.В. Ситуационные центры по информационной безопасности / А.В.Лукацкий // Журнал «Information Security/Информационная безопасность». – 2005. – № 2. – С. 28-30.
11. Построение центра мониторинга и управления безопасностью Cisco. Архитектура, процессы и результаты [Электронный ресурс]: Веб-сайт / EURECA. – 2006. – Режим доступа: <http://www.eureca.ru/edu/study/cisco/library/download.php?type=pdf&att=SOC.pdf> (дата обращения: 17.09.2020).
12. Лукацкий А. Как построить Security Operations Center (SOC) Архитектура, требования, методология и процессы [Электронный ресурс]: Веб-сайт / CISCO / А.Лукацкий. – Cisco, 2007. – Режим доступа: https://www.cisco.com/c/dam/global/ru_ua/assets/expo2007/present/soc_alukatsk_1.pdf (дата обращения: 17.09.2020).
13. Волков К. Практический опыт построения системы централизованного мониторинга ИБ в банковской организации на базе решений Oracle [Электронный ресурс]: Веб-сайт / THEPRESENTATION / К.Волков. – М.: ЛИНС-М, 2008. – Режим доступа: <https://thepresentation.ru/uncategorized/lins-m> (дата обращения: 17.09.2020).
14. Романов, В.В. Ситуационные центры в решении проблем информационной безопасности / В.В.Романов // Журнал «InformationSecurity / Информационная безопасность». – 2006. – № 3, 4. – С. 28.
15. ГОСТ Р «Защита информации. Мониторинг информационной безопасности. Общие положения». Проект [Электронный ресурс]: Веб-сайт / ФСТЭК России. – Режим доступа: <https://fstec.ru/tk-362/standarty-tk362/303-proekty/1896-proekt-natsionalnogo-standarta-gost-r-4> (дата обращения: 17.09.2020).
16. ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации». Проект [Электронный ресурс]: Веб-сайт / ФСТЭК России. – Режим доступа: <https://fstec.ru/tk-362/standarty-tk362/303-proekty/1895-proekt-natsionalnogo-standarta-gost-r-3> (дата обращения: 17.09.2020).
17. Cost of a Data Breach Report 2019 [Электронный ресурс]: Веб-сайт / ALL-ABOUT-SECURITY. – Ponemon Institute, 2019. – Режим доступа: https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf (дата обращения: 17.09.2020).
18. 2018 Insider Threat Report [Электронный ресурс]: Веб-сайт / CROWDRESEARCHPARTNERS. – Crowd Research Partners, 2018. – Режим доступа: <https://crowdresearchpartners.com/insider-threat-report/> (дата обращения: 17.09.2020).
19. 2019 Insider Threat Report: Executive Summary [Электронный ресурс]: Веб-сайт / VERIZON. – Verizon, 2019. – Режим доступа: <https://enterprise.verizon.com/resources/>

executivebriefs/insider-threat-report-executive-summary.pdf (дата обращения: 17.09.2020).

20. Website hacking statistics of 2020 [Электронный ресурс]: Веб-сайт / WEBARXSECURITY. – 2020. – Режим доступа: <https://www.webarxsecurity.com/website-hacking-statistics-2018-february/> (дата обращения: 17.09.2020).

21. Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [постановление Правительства РФ от 8 февраля 2018 г. № 127]. – 2018. – 21 с.

22. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Введ. 2009-10-01. – М.: Стандартинформ, 2009. – 20 с.

23. Nemeth C.P. Resilience Engineering Perspectives: Preparation and Restoration in Human Systems / C.P.Nemeth, E.Hollnagel, S.Dekker. – UK: Ashgate Publishing, 2009. – Vol. 2. – 241 p.

24. Бессонов Л.А. Теоретические основы электротехники. Электрические цепи / Л.А.Бессонов. – 9-е изд. перераб. и доп. – М.: «Высшая школа», 1996. – 638 с.

25. О Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [указ Президента РФ от 12 декабря 2014 г. № К 1274]. – 2014. – 8 с.

26. Соловьев С.В. Методическое обеспечение обоснования требований к информационно-аналитическому комплексу межведомственной системы контроля состояния технической защиты информации: дис. ... канд. техн. наук: 05.13.19 / Соловьев Сергей Вениаминович. – Воронеж, 2002. – 142 с.

27. Ламонов А.В. Исследование механизмов блокирования информации в компьютерных системах органов государственного и муниципального управления в интересах выявления противоправных действий в сфере компьютерной информации: дис. ... канд. юр. наук: 05.13.19 / Ламонов Андрей Владимирович. – Воронеж, 2006. – 192 с.

28. Лукашин А.А. Система защиты информационного взаимодействия в среде облачных вычислений: автореф. дис. ... канд. техн. наук: 05.13.19 / Лукашин Алексей Андреевич. – СПб., 2012. – 17 с.

29. Попов В.М. Методика управления рисками в системе неразрушающего контроля безопасности почтовой корреспонденции на предприятии-адресате: дис. ... канд. техн. наук: 05.13.19 / Попов Владимир Михайлович. – М., 2012. – 145 с.

30. Глухов А.П. Модели и методы риск-ориентированного управления информационной безопасностью железнодорожной транспортной системы: дис. ... докт. техн. наук: 05.13.19 / Глухов Александр Петрович. – СПб., 2017. – 423 с.

31. Калинин М.В. Адаптивное управление безопасностью информационных систем на основе логического моделирования: дис. ... докт. техн. наук: 05.13.19 / Калинин Максим Олегович. – СПб., 2010. – 308 с.
32. Исаев А.С. Метод и модель управления информационной безопасностью на основе динамических экспертных систем поддержки принятия решений. дис. ... канд. техн. наук: 05.13.19 / Исаев Александр Сергеевич. – СПб., 2015. – 187 с.
33. Цыганков А.С. Адаптивное управление межсетевым экранированием информационно-телекоммуникационных сетей на этапе обнаружения вторжений: дис. ... канд. техн. наук: 05.13.19 / Цыганков Александр Сергеевич. – Оренбург, 2008. – 138 с.
34. Ушаков Д.В. Развитие принципов функционирования систем обнаружения сетевых вторжений на основе модели защищенной распределенной системы: дис. ... канд. техн. наук: 05.13.19 / Ушаков Дмитрий Вячеславович. – М., 2005. – 175 с.
35. Лаврова Д.С. Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции: дис. ... докт. техн. наук: 05.13.19 / Лаврова Дарья Сергеевна. – СПб., 2019. – 303 с.
36. Машкина И.В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий: автореф. дис. ... докт. техн. наук: 05.13.19 / Машкина Ирина Владимировна. – Уфа, 2009. – 346 с.
37. Демидов Р.А. Выявление угроз нарушения информационной безопасности в сетях с динамической топологией с использованием методов глубокого обучения: дис. ... канд. техн. наук: 05.13.19 / Демидов Роман Алексеевич. – СПб., 2018. – 143 с.
38. Карайчев Г.В. Разработка и исследование метода весовых функций для решения задач интеллектуального анализа данных при выявлении аномальной сетевой активности: дис. ... канд. техн. наук: 05.13.19 / Каравайчев Глеб Викторович. – Ростов-на-Дону, 2011. – 153 с.
39. Шелудько И.А. Разработка и исследование системы оперативного сетевого мониторинга событий безопасности: дисс. ... канд. техн. наук: 05.13.19 / Шелудько Игорь Александрович. – Таганрог, 2004. – 179 с.
40. Ковалев Д.О. Выявление нарушений информационной безопасности по данным мониторинга информационно-телекоммуникационных сетей: дис. ... канд. техн. наук: 05.13.19 / Ковалев Дмитрий Олегович. – М., 2011. – 170 с.
41. Miloslavskaya, N. Information Security Maintenance Issues for Big Security-Related Data / N.Miloslavskaya, M.Senatorov, A.Tolstoy, S.Zapechnikov // Proceedings of 2014 International Conference on Future Internet of Things and Cloud FiCloud 2014. International Symposium on Big Data Research and Innovation (BigR&I 2014) (Barcelona (Spain), 27-29 August 2014). – 2014. – Pp. 361-366. DOI: 10.1109/ FiCloud.2014.64.

42. Miloslavskaya, N. «Business Continuity and Information Security Maintenance» Masters' Training Program / N.Miloslavskaya, M.Senatorov, A.Tolstoy, S.Zapechnikov // In: Ronald C. Dodge Jr., Lynn Fitcher (Eds.): Information Assurance and Security Education and Training – WISE 8, Auckland, New Zealand, 2013, WISE 7, Lucerne Switzerland, 2011, and WISE 6, Bento Gonçalves, RS, Brasil, 2009, Revised Selected Papers // Advances in Information and Communication Technology.– Springer, 2013. – Vol. 406. – Pp. 95-102. DOI: 10.1007/978-3-642-39377-8_10.

43. Будзко, В.И. Новое направление подготовки профессионалов: магистры в области обеспечения непрерывности и информационной безопасности бизнеса / В.И.Будзко, С.В.Запечников, Н.Г.Милославская, М.Ю.Сенаторов, А.И.Толстой // Системы высокой доступности. – 2012. – Том 8, вып.1. – С. 71-73.

44. Милославская, Н.Г. Вопросы практического применения технологий блокчейна/ Н.Г.Милославская, В.И.Будзко // Безопасность информационных технологий. – 2018. – Том 26, № 1. – С. 36-45.

45. Miloslavskaya, N. Taxonomy for Unsecure Big Data Processing in Security Operations Centers / N.Miloslavskaya, A.Tolstoy, S.Zapechnikov // Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016) (Vienna (Austria). 22-24 August 2016). – 2016. – Pp. 154-159. DOI: 10.1109/W-FiCloud.2016.42.

46. Malyuk, A. Information Security Theory Development / A.Malyuk, N.Miloslavskaya // Proceedings of the 7th International Conference on Security of Information and Networks (SIN2014) (Glasgow (UK), 9-11 September 2014). – ACM New York, 2014. – Pp. 52-55. DOI: 10.1145/2659651.2659659.

47. Kostina, A. Information Security Incident Management / A.Kostina, N.Miloslavskaya, A.Tolstoy // Proceedings of the 3rd International Conference on Internet Technologies and Applications (Wrexham (UK), 8-11 September 2009). – 2009. – Pp. 27-34.

48. Miloslavskaya, N. Information Visualisation in Information Security Management for Enterprises's Information Infrastructure / N.Miloslavskaya, A.Tolstoy, A.Birjukov // Scientific Visualisation. – Moscow, MEPhI, 2014. – Vol. 6, № 2. – Pp. 74-91.

49. Miloslavskaya, N. Application of Big Data, Fast Data and Data Lake Concepts to Information Security Issues / N.Miloslavskaya, A.Tolstoy // Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016) (Vienna (Austria), 22-24 August 2016). – 2016. – Pp. 148-153. DOI: 10.1109/W-FiCloud.2016.41.

50. Miloslavskaya, N. «Network Security Intelligence» Educational and Research Center / N.Miloslavskaya, A.Tolstoy, A.Migalin // In: Bishop M., Fitcher L., Miloslavskaya N., Theocharidou

M. (eds) Information Security Education for a Global Digital Society. WISE 2017 // Advances in Information and Communication Technology. – Springer, 2017. – Vol. 503. – Pp. 157-168. DOI: 10.1007/978-3-319-58553-6_14.

51. Miloslavskaya, N. DLP as an Integral Part of Network Security Intelligence Center / N.Miloslavskaya, V.Morozov, A.Tolstoy, D.Khassan // Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud (FiCloud2017) (Prague (Czech Republic), 21-23 August 2017). – 2017. – Pp. 297-304. DOI 10.1109/FiCloud.2017.15.

52. Miloslavskaya, N. Developing Hands-On Laboratory Works for the «Information Security Incident Management» Discipline / N.Miloslavskaya, A.Tolstoy // In: Drevin L., Theocharidou M. (eds) Information Security Education – Towards a Cybersecure Society. WISE 2018 // Advances in Information and Communication Technology. – Springer, 2018. – Vol 531. – Pp. 28-39. DOI: 10.1007/978-3-319-99734-6_3.

53. Miloslavskaya, N. State-Level Views on Professional Competencies in the Field of IoT and Cloud Information Security / N.Miloslavskaya, A.Tolstoy // Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Intercloud and IoT (ICI 2016) (Vienna (Austria), 22-24 August 2016). – 2016. – Pp. 83-90. DOI: 10.1109/W-FiCloud.2016.31.

54. Morozov, V. Technical to Psychological Aspects Ratio in the Specialized Information Security Training Content / V.Morozov, N.Miloslavskaya // In: Samsonovich A., Klimov V. (eds) Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019 // Procedia Computer Science, 2020. – Pp. 90-95. DOI: 10.1016/j.procs.2020.02.119.

55. Информационная безопасность открытых систем. Учебник с грифом Министерства образования РФ. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В.Запечников, Н.Г.Милославская, А.И.Толстой, Д.В.Ушаков. – М., Горячая Линия-Телеком, 2006. – 536 с.

56. ГОСТ 27.004-85 Надежность в технике (ССНТ). Системы технологические. Термины и определения. – Введ. 1986-07-01. – М., Гос. комитет СССР по стандартам, 1986. – 9 с.

57. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – Введ. 1996-01-01. – М., Гос. стандарт РФ, 1995. – 8 с.

58. Сенаторов М.Ю. Информационно-телекоммуникационная система Банка России / М.Ю.Сенаторов. – М.: Аякс-Пресс, 2008. – 176 с.

59. ГОСТ 34.321-96 Информационные технологии (ИТ). Система стандартов по базам данных. Эталонная модель управления данными. – Введ. 2001-07-01. – Минск, Межгосударст-

венный Совет по стандартизации, метрологии и сертификации, 2001. – 27 с.

60. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. – Введ. 2012-01-01. – М., Стандартиформ, 2012. – 73 с.

61. Летелкин, Н.В. Об определении признаков и понятия «информационно-телекоммуникационная сеть» в отечественном уголовном законодательстве / Н.В.Летелкин // Вопросы российского и международного права. – 2018. – Том 8, вып. 3А. – С. 216-221.

62. ГОСТ Р 51513-99 Совместимость технических средств электромагнитная. Оборудование распределительных сетей приемных систем телевидения и радиовещания. Нормы электромагнитных помех, требования помехоустойчивости и методы испытаний. – Введ. 2001-07-01. – М., Госстандарт России, 1999. – 15 с.

63. Сборник терминов и определений, применяемых в ИТС Банка России [Электронный ресурс]. – Москва, АС «Сфинкс», 2004. – № 2491. – 1 электрон, опт. диск (CD-ROM).

64. Шинкаренко, А.Ф. Особенности подходов к построению ИТКС / А.Ф.Шинкаренко // Современные тенденции технических наук: материалы III Междунар. науч. конф. (г. Казань, октябрь 2014 г.). – Казань: Бук, 2014. – С. 19-21.

65. СТО БР ИББС-1.0-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – Введ. 2014-06-01. – М., 2014. – 101 с.

66. РС БР ИББС-2.2-2009 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. – Введ. 2010-01-01. – М., 2009. – 23 с.

67. Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов [одобрена решением Президента РФ от 23 ноября 1995 г. № Пр-1694] [Электронный ресурс]: Веб-сайт / NSR. – 1995. – Режим доступа: http://www.nsc.ru/win/laws/russ_kon.htm (дата обращения 17.09.2020).

68. ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. – 21 p.

69. Conrad C. Next Generation Security. Slideshow [Электронный ресурс]: Веб-сайт / SLIDESHARE / C.Conrad. – 2013. – Режим доступа: <https://www.slideshare.net/neoma329/next-generationsecurity> (дата обращения 17.09.2020).

70. Mayhew S. History of Biometrics [Электронный ресурс]: Веб-сайт / BIOMETRICUPDATE / S.Mayhew. – 2018. – Режим доступа: <https://www.biometricupdate.com/201802/history-of-biometrics-2> (дата обращения 17.09.2020).

71. MIT Kerberos Documentation [Электронный ресурс]: Веб-сайт / MIT. – MIT, 1985. –

Режим доступа: <https://web.mit.edu/kerberos/krb5-latest/doc/> (дата обращений 17.09.2020).

72. Denning, D. Requirements and Model for IDES – A Real-Time Intrusion-Detection Expert System, Final Report / D.Denning, P.Neumann. – SRI International, 1985. – 70 p.

73. Bradford A. What was the very first antivirus package? [Электронный ресурс]: Веб-сайт / TOPTENREVIEWS / A.Bradford. – 2020. – Режим доступа: <https://www.toptenreviews.com/what-was-the-first-antivirus-software> (дата обращений 17.09.2020).

74. Liska A. Building an Intelligence-Led Security Program / A.Liska. – Syngress, 2014. – 200 p.

75. Practical VoIP Security / T.Porter, J.Kanclirz, A.Zmolek, A.Rosela. – Syngress, 2006. – 564 p.

76. Vacca J.R. Computer and Information Security Handbook / J.R.Vacca. – Elsevier, 2017. – 1280 p.

77. Pirc J. The Evolution of Intrusion Detection/Prevention: Then, Now and the Future [Электронный ресурс]: Веб-сайт / SECUREWORKS / J.Pirc. – 2017. – Режим доступа: <https://www.secureworks.com/blog/the-evolution-of-intrusion-detection-prevention> (дата обращений 17.09.2020).

78. Ландергрэн П. VPN следующего поколения [Электронный ресурс]: Веб-сайт / OSP / П.Ландергрэн. – 2001. – № 22. – Режим доступа: <https://www.osp.ru/cw/2001/22/42169/> (дата обращений 17.09.2020).

79. Web Application Firewall (WAF) [Электронный ресурс]: Веб-сайт / PENTASECURITY. – Режим доступа: <https://www.pentasecurity.com/product/waf/web-application-firewall/> (дата обращений 17.09.2020).

80. Worldwide Threat Management Security Appliances 2004–2008 Forecast and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance Report [Электронный ресурс]: Веб-сайт / YUMPU. – IDC, 2004. – Режим доступа: <https://www.yumpu.com/en/document/view/21075686/worldwide-threat-management-security-appliances-fortinet> (дата обращений 17.09.2020).

81. Cook I. Intelligence Led Corporate Security Programs Why a Business Needs to Setup a Cyber Threat Analysis Unit [Электронный ресурс]: Веб-сайт / FIRST/ I.Cook. – 2004. – Режим доступа: <https://www.first.org/resources/papers/conference2004/c14.pdf> (дата обращений 17.09.2020).].

82. Perkins E.L. Consider Identity and Access Management as a Process, Not a Technology [Электронный ресурс]: Веб-сайт / NETWORKINGPS / E.L.Perkins, A.Allan. – Gartner, 2005. – Режим доступа: https://www.networkingps.com/white_papers/Identity%20Access%20Management%20Process.pdf (дата обращений 17.09.2020).

83. What is Security Information and Event Management? [Электронный ресурс]: Веб-сайт / ibm.com. – IBM. – Режим доступа: <https://www.ibm.com/security/security-intelligence> (дата обра-

щений 17.09.2020).

84. Kanagasingham P. [Электронный ресурс]: Веб-сайт / SANS / P.Kanagasingham. – SANS Institute, 2008. – Режим доступа: <https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883> (дата обращения 17.09.2020).

85. What is patch management [Электронный ресурс]: Веб-сайт / GFI. – GFI Software. – Режим доступа: <https://www.gfi.com/patch-management> (дата обращения 17.09.2020).

86. 2010/2011 CSI Computer Crime and Security Survey [Электронный ресурс]: Веб-сайт / ETSMTL. – CSI, 2011. – Режим доступа: <https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf> (дата обращения 17.09.2020).

87. The origin of Threat Hunting [Электронный ресурс]: Веб-сайт / BLOGPOST. – 2017. – Режим доступа: <https://taosecurity.blogspot.com/2017/03/the-origin-of-threat-hunting.html> (дата обращения 17.09.2020).

88. Chuvakin A. Named: Endpoint Threat Detection & Response [Электронный ресурс]: Веб-сайт / GARTNER / A.Chuvakin. – Gartner, 2013. – Режим доступа: <https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/> (дата обращения 17.09.2020).

89. Market Guide for User and Entity Behavior Analytics [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner. 2015. – Режим доступа: <https://www.gartner.com/en/documents/3134524/market-guide-for-user-and-entity-behavior-analytics> (дата обращения 17.09.2020).

90. Security Orchestration, Automation And Response (SOAR). Gartner Glossary [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner, 2017. – Режим доступа: <https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar> (дата обращения 17.09.2020).

91. Market Guide for Data-Centric Audit and Protection [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner, 2017. – Режим доступа: <https://www.gartner.com/en/documents/3645326/market-guide-for-data-centric-audit-and-protection> (дата обращения 17.09.2020).

92. 2019 Gartner Market Guide for Network Traffic Analysis [Электронный ресурс]: Веб-сайт / EXTRAHOP. – Gartner, 2019. – Режим доступа: <https://www.extrahop.com/lp/gartner-nta-market-guide/> (дата обращения 17.09.2020).

93. Manage the risk of privileged access management [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner, 2020. – Режим доступа: <https://www.gartner.com/en/conferences/emea/identity-access-management-uk/agenda/featured-topics/topic-privileged-access-management> (дата обращения 17.09.2020).

94. Magic Quadrant for Cloud Access Security Brokers [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner, 2017. – Режим доступа: <https://www.gartner.com/en/documents/3834266/magic-quadrant-for-cloud-access-security-brokers> (дата обращения 17.09.2020).

95. What Is Employee Engagement? [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner, 2018. – Режим доступа: <https://www.gartner.com/smarterwithgartner/what-is-employee-engagement/> (дата обращения 17.09.2020).
96. What Is XDR? [Электронный ресурс]: Веб-сайт / PALO ALTO. – Palo Alto. – Режим доступа: <https://www.paloaltonetworks.com/cyberpedia/what-is-xdr> (дата обращения 17.09.2020).
97. ICT Security Measures used by enterprises. EU-27.2019 [Электронный ресурс]: Веб-сайт / EUROPA. – EU, 2019. – Режим доступа: https://ec.europa.eu/eurostat/statistics-explained/images/5/5d/ICT_security_measures_used_by_enterprises%2C_EU-27%2C_2019_%28%25_enterprises%29.png (дата обращения 17.09.2020).
98. Сбербанк отчитался о спасении от хакеров ₽32 млрд вкладчиков [Электронный ресурс]: Веб-сайт / RBC. – 2018. – Режим доступа: <https://www.rbc.ru/finances/29/11/2018/5bffa4499a79470bc3de89aa> (дата обращения: 17.09.2020).
99. Chuvakin A. On Large-scale SIEM Architecture [Электронный ресурс]: Веб-сайт / GARTNER / A.Chuvakin. – 2012. – Режим доступа: <http://blogs.gartner.com/anton-chuvakin/2012/07/25/on-large-scale-siem-architecture/>. (дата обращения: 17.09.2020).
100. Miloslavskaya, N. A. IoTBlockSIEM for Information Security Incident Management in the Internet of Things Ecosystem / N.Miloslavskaya, A.Tolstoy // Cluster Computing. – Springer, 2020. DOI: <https://doi.org/10.1007/s10586-020-03110-5>.
101. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. – 50 p.
102. О Национальном координационном центре по компьютерным инцидентам [приказ Федеральной Службы Безопасности РФ от 24 июля 2018 г. № 366]. – 2018. – 9 с.
103. Информационное сообщение об утверждении требований к межсетевым экранам от 28.04.2016 № 240/24/1986. – ФСТЭК России, 2016. – 4 с.
104. ГОСТ 15971-90 Системы обработки информации. Термины и определения. – Введ. 1992-01-01. – М., Гос. комитет СССР по управлению качеством, 1991. – 14 с.
105. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. – Введ. 2008-02-01. – М., Стандартинформ, 2008. – 31 с.
106. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Введ. 2014-01-01. – М., Стандартинформ, 2014. – 106 с.
107. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Введ. 2011-12-01. – М., Стандартинформ, 2011. – 51 с.

108. ГОСТ Р ИСО/МЭК 27033-3-2014 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. – Введ. 2015-11-01. – М., Стандартинформ, 2015. – 40 с.

109. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. – Введ. 1992-01-01. – М., Стандартинформ, 2009. – 16 с.

110. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – Введ. 1996-01-01. – М., Стандартинформ, 2006. – 8 с.

111. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. – Введ. 2008-02-01. – М., Стандартинформ, 2008. – 12 с.

112. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – Введ. 2008-02-01. – М., Стандартинформ, 2008. – 11 с.

113. ГОСТ Р 52653-2006 Информационно-коммуникационные технологии в образовании. Термины и определения. – Введ. 2008-07-01. – М., Стандартинформ, 2008. – 12 с.

114. ГОСТ Р 53801-2010 Связь федеральная. Термины и определения. – Введ. 2011-07-01. – М., Стандартинформ, 2011. – 32 с.

115. ГОСТ Р 54619-2011 Глобальная навигационная спутниковая система. Система экстренного реагирования при авариях. Протоколы обмена данными автомобильной системы/устройства вызова экстренных оперативных служб с инфраструктурой системы экстренного реагирования при авариях. – Введ. 2012-09-01. – М., Стандартинформ, 2012. – 67 с.

116. ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и руководство. – Введ. 2020-03-01. – М., Стандартинформ, 2020. – 19 с.

117. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. – Введ. 2013-12-01. – М., Стандартинформ, 2014. – 22 с.

118. ГОСТ Р ИСО/МЭК 38500-2017 Информационные технологии (ИТ). Стратегическое управление ИТ в организации. – Введ. 2018-09-01. – М., Стандартинформ, 2017. – 16 с.

119. ГОСТ Р ИСО 7498-2-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. – Введ. 2000-01-01. – М., Госстандарт России, 2000. – 39 с.

120. ГОСТ Р ИСО/МЭК 9594-8-98 Информационная технология (ИТ). Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации. – Введ. 1999-01-01. – М., Гос-

стандарт России, 1998. – 32 с.

121. Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. – Введ. 2006-01-01. – М., Стандартинформ, 2005. – 16 с.

122. Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. – Введ. 2006-06-01. – М., Стандартинформ, 2006. – 20 с.

123. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. – 27 p.

124. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. – 23 p.

125. ISO/IEC 27033-2:2012 Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security. – 28 p.

126. ISO/IEC 27033-4:2014 Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways. – 22 p.

127. ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. – 57 p.

128. ISO/IEC 27041:2015 Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method. – 18 p.

129. ISO/IEC 27042:2015 Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence. – 14 p.

130. ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes. – 30 p.

131. NIST Special Publication 800-61. Revision 2. 2012. Computer Security Incident Handling Guide.

132. Милославская Н.Г. Управление рисками информационной безопасности. Учебное пособие для вузов с грифом УМО. В 5 книгах. Книга 2 / Н.Г.Милославская, А.И.Толстой, М.Ю.Сенаторов. – 2-е изд. испр. – М., Горячая Линия-Телеком. – 2014. – 130 с. – (Серия «Вопросы управления информационной безопасностью»)

133. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Введ. 2013-12-01. – М., Стандартинформ, 2014. – 56 с.

134. Уязвимость и методы защиты в глобальной сети Internet. Учебное пособие / Н.Г.Милославская, Ю.А.Тимофеев, А.И.Толстой. – М., МИФИ, 1997. – 236 с.

135. Интрасети: доступ в Internet, защита. Учебное пособие для вузов с грифом Министерства образования РФ / Н.Г.Милославская, А.И.Толстой. – М., ЮНИТИ-ДАНА, 2000. – 527 с.

136. Интрасети: обнаружение вторжений. Учебное пособие для вузов с грифом Министерства образования РФ / Н.Г.Милославская, А.И.Толстой. – М., ЮНИТИ-ДАНА, 2001. – 587 с.
137. Основы информационной безопасности автоматизированных банковских систем. Учебное пособие / А.П.Курило, Н.Г.Милославская, С.Ф.Михайлов, А.И.Толстой. – М., МИФИ, 2001. – 100 с.
138. Securing Information and Communication Systems: Principles, Technologies, and Applications // Chapter 8: Network Security / S.Katsikas, N.Miloslavskaya. – Artech House, 2008. – Pp. 139-170.
139. Милославская Н.Г. Сетевые атаки на открытые системы на примере интранета: учебное пособие для вузов с грифом УМО / Н.Г.Милославская. – М., МИФИ, 2012. – 64 с.
140. Miloslavskaya, N. Taxonomy for Unsecure Digital Information Processing / N.Miloslavskaya, A.Tolstoy, S.Zapechnikov // Proceedings of the 3rd International Conference on Digital Information Processing, Data Mining and Wireless Communications (DIPDMWC2016) (Moscow (Russia), 6-8 July 2016. – 2016 – Pp. 81-86. DOI: 10.1109/DIPDMWC.2016.7529368.
141. Miloslavskaya N. Remote Attacks Taxonomy and their Key Verbal Indicators / N.Miloslavskaya // Proceedings of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures (BICA 2017) (Moscow (Russia), 1-6 August 2017) // Procedia Computer Science, 2018. – Vol. 123. – Pp. 278-284. DOI: 10.1016/j.procs.2018.01.043.
142. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. – Введ. 2016-04-01. – М., Стандартинформ, 2018. – 12 с.
143. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. – Введ. 2016-04-01. – М., Стандартинформ, 2015. – 12 с.
144. ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия. – Введ. 2018-09-01. – М., Стандартинформ, 2018. – 28 с.
145. Регламент включения информации об уязвимостях ПО и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России [методический документ: утвержден ФСТЭК России 26 июня 2018 г.] [Электронный ресурс]: Веб-сайт / ФСТЭК России. – ФСТЭК России, 2018. – Режим доступа: <https://fstec.ru/component/attachments/download/1956> (дата обращения 17.09.2020).
146. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [утверждена зам. Директора ФСТЭК России 14 февраля 2008 г.] [Электронный ресурс]: Веб-сайт / fstec.ru. – ФСТЭК России, 2008. – Режим доступа: <https://fstec.ru/component/attachments/download/290> (дата обращения

17.09.2020).

147. Octave [Электронный ресурс]: Веб-сайт / EUROPA. – Режим доступа: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html (дата обращений 17.09.2020).

148. Harmonized Threat and Risk Assessment (TRA) Methodology [Электронный ресурс]: Веб-сайт / GC. – 2007. – Режим доступа: <https://cyber.gc.ca/sites/default/files/publications/tra-emr-1-e.pdf> (дата обращений 17.09.2020).

149. Вихорев С.В. Классификация угроз информационной безопасности [Электронный ресурс]: Веб-сайт / ELVIS / С.В.Вихорев. – 2001. – Режим доступа: <https://elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf> (дата обращений 17.09.2020).

150. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [утверждена зам. директора ФСТЭК России, 15.02.2008] [Электронный ресурс]: Веб-сайт / ФСТЭК России. – ФСТЭК России, 2008. – Режим доступа: <https://fstec.ru/component/attachments/download/289> (дата обращений 17.09.2020).

151. Reviews for Security Threat Intelligence Products and Services Market [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner, 2020. – Режим доступа: [https://www.gartner.com/reviews/market/security-threat-intelligence-services#:~:text=%22Threat%20intelligence%22%20\(TI\),to%20that%20menace%20or%20hazard](https://www.gartner.com/reviews/market/security-threat-intelligence-services#:~:text=%22Threat%20intelligence%22%20(TI),to%20that%20menace%20or%20hazard) (дата обращений 17.09.2020).

152. Zaytsev, A. Analysis of Research on Specific Insider Information Security Threats / A.Zaytsev, A.Malyuk, N.Miloslavskaya // In: A. Rocha et al. (eds.), Recent Advances in Information Systems and Technologies // Advances in Intelligent Systems and Computing. – Springer, 2017. – Vol. 570. – Pp. 725-735. DOI 10.1007/978-3-319-56538-5_73.

153. Graham R. What is a typical intrusion scenario? FAQ: Network Intrusion Detection Systems. 2000. [Электронный ресурс]: Веб-сайт / LINUXSECURITY / R.Graham. – Режим доступа: http://www.linuxsecurity.com/resource_files/intrusion_detection/network-intrusion-detection.html (дата обращений 17.09.2020).

154. Olzak T. The five phases of a successful network penetration. 2008. [Электронный ресурс]: Веб-сайт / TECHREPUBLIC / T.Olzak. – Режим доступа: <http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/> (дата обращений 17.09.2020).

155. Hutchins E.M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains [Электронный ресурс]: Веб-сайт / LOCKHEEDMARTIN / E.M.Hutchins, M.J.Cloppert, R.M.Amin. – Lockheed Martin, 2010. – Режим доступа: <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf> (дата обращений 17.09.2020).

156. ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) [Электронный ресурс]: Веб-сайт / MITRE. – MITRE. – Режим доступа: <https://attack.mitre.org/> (дата обращения 17.09.2020).
157. Common Attack Pattern Enumeration and Classification [Электронный ресурс]: Веб-сайт / MITRE. – MITRE. – Режим доступа: <https://capec.mitre.org/> (дата обращения 17.09.2020).
158. Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (Версия 2.3). – Банк России. – Режим доступа: http://cbr.ru/StaticHtml/File/14408/inforegl_23.pdf (дата обращения 17.09.2020).
159. Miloslavskaya, N. Stream Data Analytics for Network Attacks' Prediction / N.Miloslavskaya // In: Samsonovich A., Klimov V. (eds) Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019 // Procedia Computer Science. – 2020. – Pp. 57-62. DOI: 10.1016/j.procs.2020.02.114.
160. Miloslavskaya, N. Designing Blockchain-based SIEM 3.0 System / N.Miloslavskaya // Information and Computer Security (UK). – Emerald Publishing, 2018. – Vol. 26, Iss. 4. – Pp. 491-512. DOI: 10.1108/ICS-10-2017-0075.
161. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Введ. – М., Стандартинформ, 2007.
162. ГОСТ Р 57580.1–2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – Введ. 2018-01-01. – М., Стандартинформ, 2017. – 67 с.
163. РС БР ИББС-2.5-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности. – Введ. 2014-06-01. – М., 2014. – 29 с.
164. СТО БР ИББС-1.3-2016 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств. – Введ. 2017-01-01. – М., 2017. – 49 с.
165. Государственный стандарт Республики Узбекистан «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы управления инцидентами (ISO/IEC 27035-1:2016, MOD) [Электронный ресурс]: Веб-сайт / TACE. – 2019. – Режим доступа: https://tace.uz/docs/OzDSt_27035_2019_1.pdf (дата обращения 17.09.2020).
166. Государственный стандарт Республики Узбекистан «Информационная технология.

Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2 Руководящие указания по планированию и подготовке к реагированию на инциденты (ISO/IEC 27035-2:2016, MOD) [Электронный ресурс]: Веб-сайт / TACE. – 2019. – Режим доступа: https://tace.uz/docs/OzDSt_27035_2019_2.pdf (дата обращения 17.09.2020).

167. CMU/SEI-2004-TR-015 Defining incident management processes for CISRT: A Work in Progress. Technical Report / C.J.Alberts, A.J.Dorofee, G.Killcrece, R.Ruefle, M.Zajicek. – Carnegie Mellon University, 2004. – 249 p.

168. Милославская Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов с грифом УМО. В 5 книгах. Книга 3 / Н.Г.Милославская, А.И.Толстой, М.Ю.Сенаторов. – 2-е изд. испр. – М., Горячая Линия-Телеком. – 2016. – 170 с. – (Серия «Вопросы управления информационной безопасностью»)

169. ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь (с Поправкой). – Введ. 2015-11-01. – М., Стандартиформ, 2015. – 53 с.

170. Аудит информационной безопасности / Под ред. А. П. Курило. – М.: БДЦ-Пресс, 2006. – 304 с.

171. Милославская Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов с грифом УМО. В 5 книгах. Книга 5 / Н.Г.Милославская, А.И.Толстой, М.Ю.Сенаторов. – 2-е изд. испр. – М., Горячая Линия-Телеком. – 2014. – 166 с. – (Серия «Вопросы управления информационной безопасностью»)

172. Курило А.П. Основы управления информационной безопасностью. Учебное пособие для вузов с грифом УМО. В 5 книгах. Книга 1 / А.П.Курило, Н.Г.Милославская, А.И.Толстой, М.Ю.Сенаторов. – 2-е изд. испр. – М., Горячая Линия-Телеком. – 2016. – 244 с. – (Серия «Вопросы управления информационной безопасностью»)

173. ГОСТ Р 51901.23-2012 Менеджмент риска. Реестр риска. Руководство по оценке риска опасных событий для включения в реестр риска. – Введ. 2-13-12-01. – М., Стандартиформ, 2014. – 35 с.

174. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий (с Поправкой). – Введ. 2007-08-01. – М., Стандартиформ, 2007. – 23 с.

175. Kurilo, A.P. Information Security Specialist Training for the Banking Sphere / A.P.Kurilo, N.G.Miloslavskaya, A.I.Tolstoy // Proceedings of the 5th World Conference on Information Security Education WISE5 (West Point (USA), 19-21 June 2007). – US Military Academy, 2007. – Pp. 87-93.

176. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. – Введ.

2012-01-01. – М., Стандартинформ, 2012. – 61 с.

177. Милославская, Н.Г. Визуализация процессов управления информационной безопасностью / Н.Г.Милославская, А.И.Толстой // Научная визуализация. – 2017. – Том 9, № 5. – С. 117-136.

178. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий. – Введ. 2007-09-01. – М., Стандартинформ, 2007. – 49 с.

179. Evolution of the Modern SIEM [Электронный ресурс]: Веб-сайт / SUVOCONSULTING. – Q1 Labs, 2011. – Режим доступа: <http://protect.suvoconsulting.de/files/2013/02/SIEM-Evolution.pdf> (дата обращения 17.09.2020).

180. Miloslavskaya, N. Security Intelligence Centers for Big Data Processing / N.Miloslavskaya // Proceedings of 2017 5th International Conference on Future Internet of Things and Cloud Workshops. The 4th International Symposium on Big Data Research and Innovation (BigR&I-2017) (Prague (Czech Republic), 21-23 August 2017). – 2017. Pp. 7-13. DOI 10.1109/W-FiCloud.2017.7.

181. Милославская, Н.Г. Актуальные вопросы использования технологии больших данных в мониторинге информационной безопасности сети / Н.Г.Милославская, А.Т.Махмудова // Безопасность информационных технологий. – 2015. – Том 22, № 2. – С.118-124.

182. ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. – 38 p.

183. ГОСТ Р ИСО/МЭК 27037-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. – Введ. 2015-11-01. – М., Стандартинформ, 2014. – 47 с.

184. CMU/SEI-2003-TR-001 State of Practice of Computer Security Incident Response Teams (CSIRTs). Technical report / G.Killcrece, K.P.Kossakowski, R.Ruefle, M.Zajicek. – Carnegie Mellon Software Engineering Institute, 2003. – 293 p.

185. Burdach M. Forensic Analysis of a Live Linux System [Электронный ресурс]: Веб-сайт / symantec.com / M.Burdach. – Режим доступа: <http://www.symantec.com/connect/articles/forensic-analysis-live-linux-system-pt-1> (дата обращения 17.09.2020).

186. Костина, А.Б. Разработка процесса управления инцидентами информационной безопасности в соответствии с требованиями международных стандартов / А.Б.Костина, Н.Г.Милославская // Безопасность информационных технологий. – 2008. – Том 14, № 4. – С. 109-116.

187. IT Security Compliance Management Design Guide with IBM Tivoli Security Information

and Event Manager. 2nd edition [Электронный ресурс]: Веб-сайт / IBM. – IBM Corporation, 2010. – Режим доступа: <http://www.redbooks.ibm.com/redbooks/pdfs/sg247530.pdf> (дата обращения 17.09.2020).

188. Miloslavskaya, N. Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers / N.Miloslavskaya // In: Samsonovich A., Klimov V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017 // Advances in Intelligent Systems and Computing. – Springer, 2018. – Vol 636. – Pp. 282-288. DOI: 10.1007/978-3-319-63940-6_40.

189. Security Information and Event Management (SIEM) Implementation / D.Miller, S.Harris, A.Harper, S.VanDyke. – McGraw-Hill, 2010. – 464 p.

190. Zimmerman C. Ten Strategies of a World-Class Cybersecurity Operations Center [Электронный ресурс]: Веб-сайт / MITRE / C.Zimmerman. – MITRE, 2014. – Режим доступа: <https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf> (дата обращения 17.09.2020).

191. Security information and event management (SIEM) [Электронный ресурс]: Веб-сайт / TECHTARGET. – Techtarget, 2014. – Режим доступа: <http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM> (дата обращения 17.09.2020).

192. Scarfone K. Introduction to SIEM services and products [Электронный ресурс]: Веб-сайт / TECHTARGET / K.Scarfone. – 2015. – Режим доступа: <http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products> (дата обращения 17.09.2020).

193. Handbook for Computer Security Incident Response Teams (CSIRTs) [Электронный ресурс]: Веб-сайт / CMU / M.J.West-Brown, D.Stikvoort, K.-P.Kossakowski, G.Killcrece, R.Ruefle, M.Zajicekm. – 2003. – Режим доступа: <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305> (дата обращения 23.03.2016).

194. Bace R.G. Intrusion Detection / R.G.Bace. – Indianapolis: Macmillan Technical Publishing, 2000. – 368 p.

195. Van Wyk K.R. Incident Response / K.R. Van Wyk, R. Forno. – Sebastopol, CA: O'Reilly Media, Inc., 2001. – 240 p.

196. Schultz E.E. Incident Response: A Strategic Guide to Handling System and Network Security Breaches / E.E.Schultz, R.Shumway. – Sams, 2001. – 408 p.

197. Northcutt S. Network Intrusion Detection / S.Northcutt. – 3rd Edition. – Indianapolis: New Riders Publishing, 2002. – 512 p.

198. Spitzner L. Honeypots: Tracking Hackers / L.Spitzner. – Addison-Wesley Professional, 2002. – 480 p.

199. Prosise C. Incident Response and Computer Forensics / C.Prosise, K.Mandia, M.Pepe. –

2nd Edition. – McGraw-Hill/Osborne, 2003. – 507 p.

200. Bejtlich R. The Tao of Network Security Monitoring: Beyond Intrusion Detection / R.Bejtlich. – Boston, MA: Pearson Education, 2005. – 832 p.

201. Bejtlich R. Extrusion Detection: Security Monitoring for Internal Intrusions / R.Bejtlich. - Addison-Wesley Professional, 2005. – 416 p.

202. Bidou R. Security Operation Center Concepts & Implementation [Электронный ресурс]: Веб-сайт / IV2-TECHNOLOGIES / R.Bidou. – 2005.- Режим доступа: <http://iv2-technologies.com/~rbidou/SOCCConceptAndImplementation.pdf> (дата обращений 17.09.2020).

203. Security Operations Center: Building, Operating, and Maintaining your SOC [Электронный ресурс]: Веб-сайт / CISCO. – Cisco Press, 2015. – Режим доступа: https://supportforums.cisco.com/sites/default/files/security_operations_center_9780134052014_ch_1_final__0.pdf (дата обращений 17.09.2020).

204. Fry C. Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks / C.Fry, M.Nystrom. – Cambridge: O'Reilly, 2009. – 246 p.

205. Rajnovic D. Computer Incident Response and Product Security / D.Rajnovic. – Indianapolis, Cisco Press, 2011. – 256 p.

206. Sanders C. Applied Network Security Monitoring: Collection, Detection, and Analysis / C.Sanders, J.Smith. – Boston, MA: Syngress, 2013. – 496 p.

207. Bejtlich R. Practice of Network Security Monitoring / R.Bejtlich. – San Francisco, CA: No Starch Press, 2013. – 376 p.

208. Security Operations Center [Электронный ресурс]: Веб-сайт / resources.infosecinstitute.com. – 2015. – Режим доступа: <http://resources.infosecinstitute.com/security-operations-center/> (дата обращений 17.09.2020).

209. Chuvakin A. Can You Do a SIEM-less SOC? [Электронный ресурс]: Веб-сайт / GARTNER / A.Chuvakin. – 2018. – Режим доступа: <https://blogs.gartner.com/anton-chuvakin/2018/06/26/can-you-do-a-siem-less-soc/> (дата обращений 17.09.2020).

210. Miloslavskaya, N. Security Operations Centers for Information Security Incident Management / N.Miloslavskaya // Proceedings of the 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016) (Vienna (Austria), 22-24 August 2016). – 2016. Pp. 131-138. DOI: 10.1109/FiCloud.2016.26.

211. Милославская, Н.Г. Центры управления информационной безопасностью / Н.Г.Милославская // Безопасность информационных технологий. – 2016. – Том 23, № 4. – С. 38-51.

212. Ковалев, Д.О. Адаптивная защита автоматизированной банковской системы при помощи операционного центра информационное безопасности / Д.О.Ковалев, Н.Г.Милославская // Безопасность информационных технологий. – 2010. – Том 17, № 1. – С. 76-78.

213. Miloslavskaya, N. Information Security Management in SOC's and SIC's / N.Miloslavskaya // Journal of Intelligent & Fussy Systems. – IOS Press (Netherlands), 2018. – Vol. 35, № 3. – Pp. 2637-2647. DOI:10.3233/JIFS-169615.
214. 2015 Data Breach Investigation Report [Электронный ресурс]: Веб-сайт / IDAHO. – Verizon, 2015. – Режим доступа: https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/data-breach-investigation-report_2015.pdf (дата обращения: 17.09.2020).
215. Miloslavskaya, N. SOC- and SIC-Based Information Security Monitoring / N.Miloslavskaya // In: A. Rocha et al. (eds.), Recent Advances in Information Systems and Technologies // Advances in Intelligent Systems and Computing. – Springer, 2017. – Vol. 570. – Pp. 364-374. DOI 10.1007/978-3-319-56538-5_37.
216. Милославская, Н.Г. Information Security Intelligence – основа современного управления информационной безопасностью / Н.Г.Милославская, А.И.Толстой // Безопасность информационных технологий. – 2013. – Том 20, № 4. – С. 88-96.
217. Burnham J. What Is Security Intelligence and Why Does It Matter Today? [Электронный ресурс]: Веб-сайт / SECURITYINTELLIGENCE / J.Burnham. – 2011. – Режим доступа: <https://securityintelligence.com/what-is-security-intelligence-and-why-does-it-matter-today/> (дата обращения: 17.09.2020).
218. IT Executive Guide to Security Intelligence. Transitioning from Log Management and SIEM to Security Intelligence. Whitepaper [Электронный ресурс]: Веб-сайт / DATABREACHTODAY. – Q1 Labs, 2012. – Режим доступа: <http://www.databreachtoday.com/whitepapers/executive-guide-to-security-intelligence-transitioning-from-siem-to-w-554> (дата обращения: 17.09.2020).
219. Ackoff, R.L. From Data to Wisdom / R.L.Ackoff // Journal of Applies Systems Analysis. – 1989. – Vol. 16. – Pp. 3-9.
220. SOC vs. SIC: The Difference of an Intelligence Driven Defense® Solution. A White Paper [Электронный ресурс]: Веб-сайт / ITSECURITYNEWS. – Lockheed Martin Corporation, 2015. – Режим доступа: <https://www.itsecuritynews.info/soc-vs-sic-the-difference-of-an-intelligence-driven-defense-solution/> (дата обращения: 17.09.2020).
221. Лебедев П. Сбербанк обезопасит себя с помощью искусственного интеллекта [Электронный ресурс]: Веб-сайт / CNEWS / П.Лебедев. – 2016. – Режим доступа: https://banks.cnews.ru/news/top/2016-06-10_sberbank_obezopasit_sebya_s_pomoshchyu_iskusstvennogo (дата обращения: 17.09.2020).
222. Бодрик А. Обзор рынка Security GRC в России [Электронный ресурс]: Веб-сайт / ANTI-MALWARE / А.Бодрик. – 2017. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/Security_GRC_in_Russia (дата обращения: 17.09.2020).

223. ГОСТ Р ИСО/МЭК 33004-2017 Информационная технология. Оценка процесса. Требования к эталонным моделям процесса, моделям оценки процесса и моделям зрелости. – Введ. 2018-01-01. – М., Стандартиформ, 2017. – 12 с.
224. ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса. – Введ. 2011-09-01. – М., Стандартиформ, 2011. – 124 с.
225. BPM Maturity Model Identifies Six Phases for Successful BPM Adoption [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner, 2006. – Режим доступа: <https://www.gartner.com/en/documents/497289/bpm-maturity-model-identifies-six-phases-for-successful-b> (дата обращения: 17.09.2020).
226. Open Information Security Management Maturity Model (O-ISM3), Version 2.0 [Электронный ресурс]: Веб-сайт / OPEN GROUP. – Open Group, 2017. – Режим доступа: <https://publications.opengroup.org/c17b> (дата обращения: 17.09.2020).
227. Милославская, Н.Г. Обзор моделей зрелости процессов управления информационной безопасностью / Н.Г.Милославская, Р.А.Сагиров // Безопасность информационных технологий. – 2015. – Том 22, № 2. – С. 119-125.
228. Anderson B. Building, Maturing and Rocking a Security Operations Center [Электронный ресурс]: Веб-сайт / SANS / B.Anderson. – Режим доступа: https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Building-Maturing-and-Rocking-a-Security-Operations-Center-Brandie-Anderson.pdf (дата обращения: 17.09.2020).
229. Majority of SOCs are below optimal maturity levels. 9th annual (ISC)2 Security Congress [Электронный ресурс]: Веб-сайт / HELPNETSECURITY. – (ISC)2, 2017. – Режим доступа: <https://www.helpnetsecurity.com/2017/01/18/soc-maturity-levels/> (дата обращения: 17.09.2020).
231. Ghosh A. To level up your SOC game, take one logical step at a time [Электронный ресурс]: Веб-сайт / ACCENTURE / A.Ghosh. – 2020. – Режим доступа: <https://www.accenture.com/us-en/blogs/level-up-soc-game-take-one-logical-step-time> дата обращения: 17.09.2020).
231. Miloslavskaya, N. Network Security Intelligence Center as a combination of SIC and NOC / N.Miloslavskaya // Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society) // Procedia Computer Science. – 2018. – Vol. 145. – Pp. 354-358. DOI: 10.1016/j.procs.2018.11.084.
232. IT Glossary [Электронный ресурс]: Веб-сайт / GARTNER. – Gartner. – Режим доступа: <https://blogs.gartner.com/it-glossary/operational-resilience/> (дата обращения: 17.09.2020).
233. Kecskemeti G. Developing Interoperable and Federated Cloud Architecture / G.Kecskemeti, A.Kertecz, Z.Nemeth. – IGI Global, 2016. – P. 4.
234. Cyber Security: Security Operations Center (SOC) vs. Network Operations Center (NOC)

[Электронный ресурс]: Веб-сайт / INTELLECTUALPOINT. – 2016. – Режим доступа: <https://www.intellectualpoint.com/blog/cyber-security-security-operations-center-soc-vs-network-operations-center-noc/> (дата обращения: 17.09.2020).

235. The Difference between the Security Operations Center (SOC) & Network Operations Center (NOC) [Электронный ресурс]: Веб-сайт / INCIDENTRESPONSE. – 2017. – Режим доступа: <https://www.incidentresponse.com/the-different-between-the-security-operations-center-soc-network-operations-center-noc/#:~:text=The%20NOC%20handles%20incidents%20and,a%20way%20that%20reduces%20downtime.&text=The%20SOC%20focuses%20on%20%E2%80%9Cin telligent,with%20naturally%20occurring%20system%20events> (дата обращения: 17.09.2020).

236. Miloslavskaya, N. Developing a Network Security Intelligence Center / N.Miloslavskaya // Postproceedings of the 9th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2018 (Ninth Annual Meeting of the BICA Society) // Procedia Computer Science. – 2018. – Vol. 145. – Pp. 359-364. DOI: 10.1016/j.procs.2018.11.085.

237. Network operations center (NOC) [Электронный ресурс]: Веб-сайт / TECHTARGET. – Режим доступа: <http://searchnetworking.techtarget.com/definition/network-operations-center> (дата обращения: 17.09.2020).

238. What Is a Network Operations Center (NOC)? [Электронный ресурс]: Веб-сайт / CONTINUUM. – Режим доступа: <http://www.continuum.net/msp-resources/mspedia/what-is-a-network-operations-center-noc> (дата обращения: 17.09.2020).

239. McCauley G. Network vs Security Operation Centers | Comparing NOC vs SOC. [Электронный ресурс]: Веб-сайт / EXTNOС / G.McCauley. – 2020. – Режим доступа: <https://www.extnoc.com/blog/network-vs-security-operation-centers-comparing-noc-vs-soc/> (дата обращения: 17.09.2020).

240. Bhardwaj R. NOC vs SOC – Detailed comparison & difference between NOC & SOC. [Электронный ресурс]: Веб-сайт / IPWITHEASE / R.Bhardwaj. – 2020. – Режим доступа: <https://ipwithease.com/noc-vs-soc/> (дата обращения: 17.09.2020) (дата обращения: 17.09.2020).

241. Glick B. Information security is a big data issue [Электронный ресурс]: Веб-сайт / COMPUTERWEEKLY. – 2013. – Режим доступа: <http://www.computerweekly.com/feature/Information-security-is-a-big-data-issue> (дата обращения: 17.09.2020).

242. Wood P. How to tackle big data from a security point of view [Электронный ресурс]: Веб-сайт / COMPUTERWEEKLY / P.Wood. – 2013. – Режим доступа: <http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view> (дата обращения: 17.09.2020).

243. Guarino A. Digital Forensics as a Big Data Challenge // ISSE 2013 Securing Electronic Business Processes. – Springer Fachmedien Wiesbaden, 2013. – Pp. 197-203.

244. Hornbeck R.L. Batch Versus Streaming: Differentiating Between Tactical and Strategic Big Data Analytics [Электронный ресурс]: Веб-сайт / BLOGPOST / R.L.Hornbeck. – 2013. – Режим доступа: <http://datatactics.blogspot.ru/2013/02/batch-versus-streaming-differentiating.html> (дата обращения: 17.09.2020).
245. Casado R. The three generations of Big Data processing [Электронный ресурс]: Веб-сайт / ACADEMIA / R.Casado. – 2013. – Режим доступа: http://www.academia.edu/7179455/The_three_generations_of_Big_Data_processing (дата обращения: 17.09.2020).
246. Marz N. Big Data: Principles and best practices of scalable real-time data systems / N.Marz, J.Warren. Manning Publication, 2015. – 328 p.
247. Han J. Data Mining: Concepts and Techniques / J. Han, M. Kamber. – 2nd Edition. – Elsevier, 2006. – 743 p.
248. Dua S. Data Mining and Machine Learning in Cybersecurity / S.Dua, X.Du. – Auerbach Publications, 2011. – 256 p.
249. Dixon J. Pentaho, Hadoop, and Data Lakes [Электронный ресурс]: Веб-сайт / jamesdixon.wordpress.com / J.Dixon. – 2010. – Режим доступа: <https://jamesdixon.wordpress.com/2010/10/14/pentaho-hadoop-and-data-lakes/> (дата обращения: 17.09.2020).
250. McClure T. Yesterday's unified storage is today's enterprise data lake [Электронный ресурс]: Веб-сайт / TECHTARGET / T.McClure. – 2014. – Режим доступа: <https://searchstorage.techtarget.com/opinion/Yesterdays-unified-storage-is-todays-enterprise-data-lake> (дата обращения: 17.09.2020).
251. Laskowski N. Data lake governance: A big data do or die [Электронный ресурс]: Веб-сайт / TECHTARGET / N.Laskowski. – 2016. – Режим доступа: <https://searchcio.techtarget.com/feature/Data-lake-governance-A-big-data-do-or-die> (дата обращения: 17.09.2020).
252. Shalom N. The next big thing in big data: fast data [Электронный ресурс]: Веб-сайт / VENTUREBEAT / N.Shalom. – 2014. – Режим доступа: <http://venturebeat.com/2014/06/25/the-next-big-disruption-in-big-data/> (дата обращения: 17.09.2020).
253. Betts R. Fast Data: Smart and at Scale / R. Betts, J. Hugg. – O'Reilly, 2015. – 487 p.
254. Miloslavskaya, N. Security Zone Infrastructure for Network Security Intelligence Centers / N.Miloslavskaya // In: Samsonovich A., Klimov V. (eds) Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2019 // Procedia Computer Science. – 2020. – Pp. 51-56. DOI: 10.1016/j.procs.2020.02.113.
255. Sandboxes Explained: How They're Already Protecting You and How to Sandbox Any Program [Электронный ресурс]: Веб-сайт / HOWTOGEEK. – 2013. – Режим доступа: <http://www.howtogeek.com/169139/sandboxes-explained-how-theyre-already-protecting-you-and-how-to-sandbox-any-program/> (дата обращения: 17.09.2020).

256. Exposing the Unknown: How Sandboxing Technology Fights Modern Threats. White Paper [Электронный ресурс]: Веб-сайт / INFORSECURITY MAGAZINE. – 2016. – Режим доступа: <https://www.infosecurity-magazine.com/white-papers/sandboxing-technology-fights/> (дата обращения: 17.09.2020).

257. Chen J., DeWitt D., Tian F., Wang Y. NiagaraCQ: a Scalable Continuous Query System for Internet Databases. In Proceedings of SIGMOD'00, Dallas, Texas, 2000. Pp. 379–390.

258. Olston, C. Adaptive Filters for Continuous Queries over Distributed Data Streams / C.Olston, J.Jiang, J.Widom // Proceedings of SIGMOD'03. – San Diego, California, 2003. – Pp. 563–574.

259. Govindan, R. Computing Aggregates for Monitoring Wireless Sensor Networks / R.Govindan, D.Estrin. // Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications. – 2003. – Pp. 139–148.

260. Oliveira S.R.M. Privacy preservation when sharing data for clustering / S.R.M.Oliveira, O.R. Zaïane // Proceedings of the International Workshop on Secure Data Management in a Connected World (Toronto (Canada), August 2004). – 2004. – Pp. 67–82.

261. Liu, K. An attacker's view of distance preserving maps for privacy preserving data mining / K.Liu, C.Giannella, H.Kargupta // Proceedings of PKDD'06 (Berlin (Germany), September 2006. – 2006. – Pp. 297–308.

262. Haarslev, V. On the scalability of description logic instance retrieval / V.Haarslev, R.Möller // Journal of Automated Reasoning. – Springer, 2008. – Vol. 41. – Pp. 99–142.

263. Lyon L. Load Testing in a Big Data Environment [Электронный ресурс]: Веб-сайт / DATABASEJOURNAL / L.Lyon. – 2014. – Режим доступа: <https://www.databasejournal.com/features/db2/load-testing-in-a-big-data-environment.html#:~:text=Load%20testing%20involves%20simulating%20a,and%20a%20full%2D-sized%20database.> (дата обращения: 17.09.2020).

264. Miloslavskaya, N. Survey of Big Data Information Security / N. Miloslavskaya, A.Makhmudova // Proceedings of 2016 4th International Conference on Future Internet of Things and Cloud Workshops. The 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016) (Vienna (Austria), 22–24 August 2016). – 2016. – Pp. 133–138. DOI: 10.1109/W-FiCloud.2016.38.

265. Махмудова, А.Т. Обзор вопросов обеспечения информационной безопасности больших данных / А.Т.Махмудова, Н.Г.Милославская // Безопасность информационных технологий. – 2016. – Том 23, № 2. – С.82–88.

266. Запечников, С.В. Проблемы обеспечения информационной безопасности больших данных / С.В.Запечников, Н.Г.Милославская, М.Ю.Сенаторов, А.И.Толстой // Безопасность информационных технологий. – 2014. – Том 21, № 3. – С. 161–167.

267. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]: Веб-сайт / NAKAMOTO INSTITUTE / S.Nakamoto. – 2018. – Режим доступа: <https://nakamotoinstitute.org/literature/> (дата обращения: 17.09.2020).
268. Miloslavskaya, N. Chapter 7. Blockchain Application for IoT Security Management / N.Miloslavskaya, A.Tolstoy, V.Budzko V., M.Das M // In: Essentials of Blockchain Technology. – CRC Press, Taylor & Francis Group (USA), 2019. – Pp. 141-168. DOI: 10.1201/9780429674457-7.
269. NISTIR 8202 Blockchain Technology Overview [Электронный ресурс]: Веб-сайт / NIST / D.Yaga, P.Mell, N.Roby, K.Scarfone. – 2018. – Режим доступа: <https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf> (дата обращения: 17.09.2020).
270. ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary. – 10 p.
271. Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World [Электронный ресурс]: Веб-сайт / ACCENTURE. – Accenture, 2016. – Режим доступа: https://www.accenture.com/t20160927T033514Z__w_/us-en/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf (дата обращения: 17.09.2020).
272. Cocheo S. A blockchain you can edit? [Электронный ресурс]: Веб-сайт / BANKINGEXCHANGE / S.Cocheo. – 2016. – Режим доступа: <http://www.bankingexchange.com/technology-channel/item/6492-a-blockchain-you-can-edit> (дата обращения: 17.09.2020).
273. Krawczyk H. Chameleon Hashing and Signatures [Электронный ресурс]: Веб-сайт / IACR / H.Krawczyk, T.Rabin. – 1997. – Режим доступа: <https://eprint.iacr.org/1998/010.ps> (дата обращения: 17.09.2020).
274. ISO/IEC 13568:2002/Cor 1:2007 Information technology — Z formal specification notation — Syntax, type system and semantics. – 189 p.
275. Lano K. The B Language and Method: A Guide to Practical Formal Development / K.Lano. – Springer-Verlag New York, Inc. Secaucus (USA). – 1996. – 240 p.
276. Leuschel M. The ProB animator and model checker for B – a tool description. [Электронный ресурс]: Веб-сайт / SOTON / M.Leuschel, M.Butler. – 2003. – Режим доступа: http://users.ecs.soton.ac.uk/mal/systems/prob_tooldescription.pdf (дата обращения: 17.09.2020).
277. Милославская, Н.Г. Понятие устойчивости организации инфраструктуры финансового рынка в условиях угроз кибербезопасности / Н.Г.Милославская, С.А.Толстая // Безопасность информационных технологий. – 2015. – Том 22. № 4. – С. 75-85.
278. Фетисов Г.Г. Устойчивость банковской системы и методология ее оценки / Г.Г.Фетисов. – М.: Экономика, 2003. – 400 с., с. 44.
279. Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques [Электронный ресурс]: Веб-сайт / MITRE. – MITRE, 2015. – Режим доступа: <http://www.mitre.org/sites/default/files/publications/pr->

15-1334-cyber-resiliency-engineering-aid-framework-update.pdf (дата обращения: 17.09.2020).

280. Бессонов Л.А. Теоретические основы электротехники. Электрические цепи / Л.А.Бессонов. – Изд. 9-е, перераб. и доп. – М.: «Высшая школа», 1996. – 638 с.

281. Operational risk – Revisions to the simpler approaches – consultative document. Basel Committee on Banking Supervision [Электронный ресурс]: Веб-сайт / BIS. – 2014. – Режим доступа: <https://www.bis.org/publ/bcbs291.pdf> (дата обращения: 17.09.2020).

282. Егоров, Б.М. Основные направления обеспечения непрерывности функционирования информационно-телекоммуникационных систем высокой доступности / Б.М.Егоров, М.Ю.Сенаторов, Е.В.Фролков, С.Я.Нагибин // Безопасность информационных технологий. – 2014. – Том 21, № 4. – С. 12-17.

283. CERT® Resilience Management Model, Version 1.2 / R.A.Caralli, J.H.Allen, D.W.White, L.R.Young, N.Mehravari, P.D.Curtis. – CERT, 2016. – 860 p.

284. Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report [Электронный ресурс]: Веб-сайт / ENISA. – ENISA, 2011. – Режим доступа: <https://www.enisa.europa.eu/publications/metrics-tech-report> (дата обращения: 17.09.2020).

285. Bodeau D.J. Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. [Электронный ресурс]: Веб-сайт / MITRE / D.J.Bodeau, R.D.Graubart, R.M.McQuaid, J.Woodill. – MITRE, 2018. – Режим доступа: <https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf> (дата обращения: 17.09.2020).

286. ГОСТ Р «Защита информации. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты. Термины и определения». Проект. [Электронный ресурс]: Веб-сайт / fstec.ru. – Режим доступа: <https://fstec.ru/component/attachments/download/2770> (дата обращения: 17.09.2020).

287. Янкин А. SOC: кадры решают все / А.С.Янкин // Журнал «Information Security/Информационная безопасность» [Электронный ресурс]: Веб-сайт / ITSEC. – 2016. – № 1. – Режим доступа: <http://lib.itsec.ru/articles2/Oborandteh/soc-kadry-reshayut-vse> (дата обращения: 17.09.2020).

288. Милославская, Н.Г. Подготовка специалистов по информационной безопасности: международный опыт / Н.Г.Милославская // Безопасность информационных технологий. – 2008. – Том 15, № 4. – С. 33-42.

289. State Government Information Security Workforce Development Model. A Best Practice Model and Framework. Final Version 1.0 [Электронный ресурс]: Веб-сайт / US-CERT. – US, 2010. – Режим доступа: <https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework> (дата обращения: 17.09.2020).

290. The U.S. National Cybersecurity Workforce Framework [Электронный ресурс]: Веб-

сайт / DHS. – Режим доступа: <https://www.dhs.gov/national-cybersecurity-workforce-framework> (дата обращения: 17.09.2020).

291. The Cyber Security Capability Framework & Mapping of ISM Roles. Final Report [Электронный ресурс]: Веб-сайт / DHS. – Australian Government Information Management Office, 2010. – Режим доступа: <https://www.yumpu.com/en/document/read/43006585/cyber-security-capability-framework-mapping-of-ism-roles-agimo> (дата обращения: 17.09.2020).

292. ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals. – 21 p.

293. Милославская, Н.Г. Компетентностные требования стандартов ISO/IEC к профессионалам в области информационной безопасности / Н.Г.Милославская, А.И.Толстой // Безопасность информационных технологий. – 2017. – Том 24, № 4. – С. 6-18.

294. Методические материалы XXII Пленума ФУМО ВО ИБ. Проекты ФГОС ВО 3++ УГСНП 10.00.00 «Информационная безопасность» (Краснодар, 2–7 октября 2018 г.) / Разраб.: Е.Б.Белов и др. – Краснодар: Издательский Дом – Юг, 2018. – 140 с.

295. Научно-методические и нормативные материалы XX пленума ФУМО ВО ИБ. Сборник профессиональных стандартов по группе занятий (профессий) «Специалисты в области информационной безопасности» (Москва, 23-28 ноября 2016 г.). – М., 2016. – 198 с.

296. Методические материалы XXIII Пленума ФУМО ВО ИБ. Часть 1. Проекты примерных основных образовательных программ бакалавриата и магистратуры (по ФГОС ВО 3++) УГСНП 10.00.00 «Информационная безопасность» (Ставрополь, 1-5 октября 2019 г.). – Ставрополь, 2019. – 52 с.

297. Подготовка магистров по направлению 10.04.01: Рабочие учебные планы и Компетентностные модели [Электронный ресурс]: Веб-сайт / mephi.ru. – Режим доступа: <http://www.mephi.ru> (дата обращения: 17.09.2020).

298. Запечников, С.В. Подготовка магистров по программе «Обеспечение непрерывности и информационной безопасности бизнеса» / С.В.Запечников, Н.Г.Милославская, М.Ю.Сенаторов, А.И.Толстой // Безопасность информационных технологий. – 2012. – Том 19, № 2. – С. 108-115.

299. Саттаров, А.Б. Учебно-лабораторный комплекс по изучению атак типа «человек по середине» и способов защиты от них / А.Б.Саттаров, Н.Г.Милославская // Безопасность информационных технологий. – 2018. – Том, № 4. – С. 63-74.

300. Правила проведения работ при создании автоматизированных систем в Банке России [Электронный ресурс]. – Москва, АС «Сфинкс», 2010. – № НМД-6. – 1 электрон, опт. диск (CD-ROM).

301. Воройский Ф.С. Информатика. Новый систематизированный толковый словарь /

Ф.С.Воройский. – М., ФИЗМАТЛИТ, 2003. – 760 с.

302. ГОСТ Р 57429-2017 Судебная компьютерно-техническая экспертиза. Термины и определения. – Введ. 2017-09-01. – М., Стандартиформ, 2017. – 12 с.

303. ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения. – Введ. 1990-07-01. – М., Гос. комитет СССР по стандартам, 1989. – 24 с.

304. ГОСТ Р 56112-2014 Интегрированная логистическая поддержка экспортируемой продукции военного назначения. Общие требования к комплексным программам обеспечения эксплуатационно-технических характеристик. – Введ. 2015-09-01. – М., Стандартиформ, 2015. – 23 с.

305. ГОСТ Р 27.302-2009 Надежность в технике. Анализ дерева неисправностей. – Введ. 2010-09-01. – М., Стандартиформ, 2012. – 27 с.

306. ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. – Введ. 2014-01-01. – М., Стандартиформ, 2014. – 38 с.

307. Методический документ. Профили защиты средств антивирусной защиты [Электронный ресурс]: Веб-сайт / ФСТЭК России. – ФСТЭК России, 2012. – Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/120-normativnye-dokumenty/470-metodicheskie-dokumenty-utverzhdeny-fstek-rossii-3-fevralya-2012-g-2> (дата обращения: 17.09.2020).

СПИСОК ИЛЛЮСТРАТИВНОГО МАТЕРИАЛА

Таблицы

- Таблица 1 – Эволюция технологий и средств обеспечения сетевой безопасности
- Таблица 2 – Системная классификация уязвимостей элементов ИТКС
- Таблица 3 – Системная классификация угроз ИБ ИТКС
- Таблица 4 – Системная классификация сетевых атак на ИТКС и ее элементы
- Таблица 5 – Системная классификация инцидентов ИБ ИТКС
- Таблица 6 – Эволюция подходов к управлению сетевой безопасностью
- Таблица 7 – Содержание деятельности в рамках ПУИИБ для ИТКС ОРГАНИЗАЦИИ
- Таблица 8 – Описание обобщенного процесса «Обнаружение, оповещение и обработка сообщений об уязвимостях, событиях ИБ и инцидентах»
- Таблица 9 – Описание процесса «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ»
- Таблица 10 – Диаграмма процесса «Реагирование на инциденты ИБ – Первоначальные действия»
- Таблица 11 – Описание процесса «Реагирование на инциденты ИБ – Продолжение»
- Таблица 12 – Описание процесса «Анализ инцидентов ИБ»
- Таблица 13 – Описание процесса «Расследование инцидентов ИБ»
- Таблица 14 – Сравнительный анализ систем для управления ЖРС и SIEM-систем
- Таблица 15 – Системная классификация ЦМБ для внедрения в ИТКС ОРГАНИЗАЦИИ
- Таблица 16 – Сравнительный анализ характеристик трех видов ЦУБ – ЦМБ, ЦИБ и разрабатываемого ЦИУСБ
- Таблица 17 – Сравнительный анализ характеристик СОЦ и ЦИБ
- Таблица 18 – Сравнение традиционных подходов анализа данных в ЦМБ и ИБ-аналитики в ЦИУСБ ОРГАНИЗАЦИИ
- Таблица 19 – Примеры относящихся и не относящихся к ИБ событий в ОРГАНИЗАЦИИ А
- Таблица 20 – Начальный набор показателей устойчивого функционирования типового ЦИУСБ за принятый отчетный период

Рисунки

- Рисунок 1 – Типовая схема распределенной сети организации
- Рисунок 2 – Виды сетевых соединений
- Рисунок 3 – Упрощенная иерархическая модель телекоммуникационной сети
- Рисунок 4 – Логическая структура ИТКС ОРГАНИЗАЦИИ

Рисунок 5 – Возрастание сложности атак при снижении общего уровня знаний злоумышленников

Рисунок 6 – Задачи защиты информационного взаимодействия в ИТКС ОРГАНИЗАЦИИ

Рисунок 7 – Использование средств обеспечения сетевой безопасности в 2009-2010 гг.

Рисунок 8 – Использование мер обеспечения безопасности ИКТ в 2019 г. на предприятиях стран Европейского сообщества [98]

Рисунок 9 – Соотношение понятий ИБ и сетевой безопасности согласно ISO/IEC 27032:2012 [102]

Рисунок 10 – Нормативная и правовая база исследования

Рисунок 11 – Взаимосвязь базовых понятий ИБ

Рисунок 12 – Взаимосвязь базовых понятий ИБ

Рисунок 13 – Взаимосвязь базовых понятий ИБ

Рисунок 14 – Системная классификация уязвимостей в информационной сфере ИТКС ОРГАНИЗАЦИИ

Рисунок 15 – Системная классификация угроз ИБ ИТКС ОРГАНИЗАЦИИ

Рисунок 16 – Системная классификация сетевых атак на ИТКС ОРГАНИЗАЦИИ и ее элементы

Рисунок 17 – Системная классификация инцидентов ИБ ИТКС ОРГАНИЗАЦИИ

Рисунок 18 – Иллюстрация понятия «процесс»

Рисунок 19 – Взаимосвязь понятий результативности и эффективности процессов

Рисунок 20 – Взаимосвязь деятельности ОРГАНИЗАЦИИ по обеспечению ИБ ИТКС и ее основной деятельности в ЕИП

Рисунок 21 – Упрощенная модель процесса обеспечения ИБ ИТКС

Рисунок 22 – Место Политики ИБ ИТКС в системе документов ОРГАНИЗАЦИИ

Рисунок 23 – Уровни управления ИБ ИТКС ОРГАНИЗАЦИИ

Рисунок 24 – Схема управления ИБ ИТКС ОРГАНИЗАЦИИ

Рисунок 25 – Высокоуровневое представление процесса управления ИБ ИТКС

Рисунок 26 – Иллюстрация понятия СУИБ ИТКС ОРГАНИЗАЦИИ

Рисунок 27 – Циклическая модель рассмотрения процессов управления ИБ в рамках СУИБ ИТКС

Рисунок 28 – Содержание подпроцессов цикла PDCA применительно к процессам СУИБ ИТКС ОРГАНИЗАЦИИ

Рисунок 29 – Взаимосвязь процессов мониторинга ИБ и аудита ИБ для ИТКС

Рисунок 30 – Взаимосвязь процессов мониторинга ИБ и управления инцидентами ИБ для ИТКС ОРГАНИЗАЦИИ

Рисунок 31 – Деятельность в рамках процесса управления инцидентами ИБ для ИТКС

Рисунок 32 – Деятельность в рамках процесса управления инцидентами ИБ для ИТКС

Рисунок 33 – Высокоуровневая диаграмма процесса управления инцидентами ИБ для ИТКС ОРГАНИЗАЦИИ

Рисунок 34 – Диаграмма обобщенного процесса «Обнаружение и оповещение об уязвимостях, событиях ИБ и инцидентах ИБ»

Рисунок 35 – Диаграмма процесса «Обработка сообщений об уязвимостях, событиях ИБ и инцидентах ИБ»

Рисунок 36 – Диаграмма процесса «Реагирование на инциденты ИБ – Первоначальные действия»

Рисунок 37 – Диаграмма процесса «Реагирование на инциденты ИБ – Продолжение»

Рисунок 38 – Диаграмма процесса «Анализ инцидентов ИБ»

Рисунок 39 – Диаграмма процесса «Расследование инцидентов ИБ»

Рисунок 40 – Место ЦИУСБ среди систем в области ИБ ОРГАНИЗАЦИИ

Рисунок 41 – Типичная архитектура *SIEM*-системы

Рисунок 42 – Схема, иллюстрирующая бизнес-логику функционирования ЦИБ

Рисунок 43 – Многоуровневая функциональная инфраструктура типового ЦИУСБ

Рисунок 44 – Процесс получения знаний об ИБ ИТКС ОРГАНИЗАЦИИ в ЦИУСБ

Рисунок 45 – Процесс использования ИБ-аналитики в ЦИУСБ ОРГАНИЗАЦИИ с точки зрения ИТ больших данных

Рисунок 46 – Упрощенная архитектура обработки данных в ЦИУСБ ОРГАНИЗАЦИИ

Рисунок 47 – Обобщенная модель процессов обеспечения ИБ в ЦИУСБ ОРГАНИЗАЦИИ

Рисунок 48 – Высокоуровневая схема расположения зон безопасности типового ЦИУСБ

Рисунок 49 – Зональная архитектура обеспечения ИБ ЦИУСБ ОРГАНИЗАЦИИ

Рисунок 50 – Пример включения блока в блокчейн

Рисунок 51 – Пример формирования блока для включения в блокчейн

Рисунок 52 – Составляющие процесса управления устойчивостью функционирования типового ЦИУСБ ОРГАНИЗАЦИИ

Рисунок 53 – Процесс восстановления устойчивого функционирования типового ЦИУСБ ОРГАНИЗАЦИИ после инцидента ИБ

Рисунок 54 – Основные элементы системы управления устойчивостью функционирования типового ЦИУСБ ОРГАНИЗАЦИИ

Рисунок 55 – Структурно-логическая схема исследования

Рисунок 56 – Модернизированная СВОИ 2.0 Банка ГПБ (АО)

Рисунок 57 – Основы построения СОИБ ИТС Банка России

ПРИЛОЖЕНИЯ

АКТ О ВНЕДРЕНИИ в Банке ГПБ (АО)

УТВЕРЖДАЮ

Вице-Президент - начальник
Департамента мониторинга
информационной безопасности
Банка ГПБ (АО)



А.В. Бабкин

АКТ

**о внедрении результатов диссертационной работы
Милославской Натальи Георгиевны на тему
«Построение центров управления сетевой безопасностью в информационно-
телекоммуникационных сетях» в Банке ГПБ (АО)**

Мы, нижеподписавшиеся, заместитель начальника Департамента – начальник Управления контроля защищенности информационных ресурсов Горбачев Е.В., начальник Управления менеджмента инцидентов информационной безопасности Зенин Н.А. и начальник Управления обеспечения непрерывности процессов мониторинга информационной безопасности Филатов В.В., составили настоящий акт в том, что следующие результаты диссертационной работы к.т.н, доцента НИЯУ МИФИ Милославской Н.Г. на тему «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях» были использованы в проектно-конструкторской деятельности и внедрены при усовершенствовании имеющегося в Банке ГПБ (АО) (далее – Банк) центре, а именно:

- методология и принципы построения центра управления сетевой безопасностью как современного решения, предназначенного для управления нарушениями и инцидентами информационной безопасности (ИБ) и таким образом снижающего операционные риски для информационно-телекоммуникационной сети Банка;
- построение центра управления сетевой безопасностью с точки зрения обеспечения его устойчивого функционирования, реализованная, в частности, за счет использования следующих решений:
 - Системы выявления и обработки инцидентов на базе решения Micro Focus ArcSight Security Information and Event Management, которая позволяет осуществлять сбор, агрегацию, корреляцию событий информационной безопасности и выявлять на базе них инциденты информационной безопасности;
 - Системы анализа аномального трафика на базе решения Cisco StealthWatch, которая позволяет обеспечить контроль сетевого взаимодействия компонентов сети Банка и выявлять в них аномалии и вредоносную активность;

- Системы построения векторов атак на базе решения SkyBox Vulnerability Control, которая позволяет обеспечить приоритизацию выявленных уязвимостей и моделирование атак на ИТ-инфраструктуру Банка;
- Системы выявления аномального поведения пользователей в ИТ-инфраструктуре на базе решения Exabeam, что позволяет обеспечить выявление подозрительных действий пользователей сети;
- многоуровневой защиты почтового канала, включающей спам-фильтр, почтовый антивирус, средство защиты от атак «нулевого дня» и Мультисканер (многовендорный антивирус на базе решения Positive Technologies);
- межсетевые экраны на базе решения CheckPoint, которые позволяют обеспечить сетевое разграничение доступа пользователей и сервисов.

Внедрение указанных результатов диссертационного исследования Милославской Н.Г. доказывает их большую практическую значимость при построении центров управления сетевой безопасностью крупных компаний.

Настоящий акт составлен в трех экземплярах.

 / Горбачев Е.В./

 / Зенин Н.А./

 / Филатов В.В./

АКТ О ВНЕДРЕНИИ в ЗАО «ЕС-лизинг»

«УТВЕРЖДАЮ»

Генеральный директор
ЗАО «ЕС-Лизинг», д.т.н., проф.
Шмид А.В./
«3» марта 2020 г.

АКТ

о внедрении результатов диссертационной работы Милославской Натальи Георгиевны на тему «Построение центров управления сетевой безопасностью в информационно- телекоммуникационных сетях» в ЗАО «ЕС-Лизинг»

Мы, нижеподписавшиеся,

Технический директор, д.т.н., проф. Позин Б.А., Заместитель генерального директора Зайцев А.С. и руководитель отдела защиты информации Клоповский Г.В.,

составили настоящий акт в том, что результаты диссертационной работы доцента НИЯУ МИФИ, к.т.н, доцента Милославской Натальи Георгиевны на тему «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях»

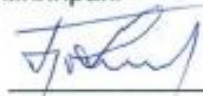
были внедрены в проектно-конструкторскую деятельность компании, а именно:

- общесистемное проектирование типового центра интеллектуального управления сетевой безопасностью (ЦИУСБ) как комплексного системотехнического решения, обеспечивающего снижение операционных рисков при развертывание современных средств обеспечения сетевой безопасности в зонах безопасности ЦИУСБ, ориентированных на создание комплексной системы обеспечения информационной безопасности (ИБ) информационно-телекоммуникационных сетей (ИТКС) заказчиков;
- концепция устойчивого функционирования ЦИУСБ, заложенная в сам проект типового ЦИУСБ и реализованная, в частности, за счет использования следующих конкретных решений в зонах безопасности ЦИУСБ: Cisco ASA, Cisco ISE, Cisco Prime Infrastructure, HPE Network Automation, Splunk Enterprise, InfoWatch Traffic Monitor, InfoWatch Device Monitor, почтовый шлюз hMail Server, файловый шлюз Vaultize, Kaspersky Security Center;
- архитектура хранения больших относящихся к ИБ ИТКС данных в виде «озер данных», рассчитанная и на работу с быстрыми данными, что требуется для интеллектуального анализа в определенном контексте всех имеющихся в распоряжении заказчиков «сырых» и исторических данных о событиях ИБ в их ИТКС и реализации проактивного подхода для предотвращения инцидентов в

ИТКС, нарушающих устойчивое и защищенное функционирование ЦИУСБ, а, значит, и ИТКС организации.

Внедрение перечисленных результатов диссертационного исследования Милославской Н.Г. демонстрирует их высокую практическую значимость, а также на практике позволяет доказать их большую научную ценность, что способствует обеспечению отказоустойчивости, высокой доступности и информационной защищенности ЦИУСБ в штатном режиме и в условиях угроз ИБ (в условиях направленных на него компьютерных атак, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций).

Настоящий акт составлен в трех экземплярах.

 / Позин Б.А./

 / Зайцев А.С./

 / Клоповский Г.В./

АКТ О ВНЕДРЕНИИ в компании «Qualys GmbH»



Qualys.
Continuous Security

«УТВЕРЖДАЮ»
Управляющий Директор
Qualys GmbH
П. В. Сотников /
«06» декабря 2019 г.

АКТ
о внедрении результатов диссертационной работы
Милославской Натальи Георгиевны на тему
«Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях»

Комиссия компании «Qualys GmbH» в составе Управляющего Директора Сотникова П.В., Менеджера по безопасности Чибисова Н.С. и Менеджера Черезова К.С. составила настоящий акт о том, что результаты диссертационной работы к.т.н, доцента Милославской Натальи Георгиевны на тему «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях» были внедрены в проектно-конструкторскую деятельность компании, а именно:

- зональная архитектура обеспечения информационной безопасности центров интеллектуального управления сетевой безопасностью (ЦИУСБ) с эшелонированной защитой и жесткой регламентацией доступа к ресурсам и услугам различных зон безопасности, внедренная у заказчиков компании;
- размещение «песочницы» в демилитаризованной зоне ЦИУСБ для исследования подозрительного ПО от непроверенных третьих лиц, пользователей, веб-сайтов и т.д., поступающих в информационно-телекоммуникационную сеть заказчика из внешних открытых сетей;
- развертывание в зонах безопасности ЦИУСБ современных средств обеспечения сетевой безопасности (включая сканеры анализа защищенности Qualys), ориентированных на создание комплексной системы обеспечения информационной безопасности информационно-телекоммуникационных сетей заказчиков.

Внедрение перечисленных результатов свидетельствует о высокой практической значимости результатов, полученных Милославской Н.Г. при проведении диссертационного исследования, и позволяет практически доказать их научную ценность при реализации упреждающего подхода к управлению сетевой безопасностью информационно-телекоммуникационных сетей различных организаций.

Настоящий акт составлен в трех экземплярах.

_____/ Сотников П.В./

_____/ Чибисов Н.С./

_____/ Черезов К.С./

Qualys, Inc.
919 E Hillsdale Blvd, 4th Floor, Foster City, CA 94404 USA
T 650 801 6100 F 650 801 6101 www.qualys.com

АКТ О ВНЕДРЕНИИ в НИЯУ МИФИ



«УТВЕРЖДАЮ»

Проректор НИЯУ МИФИ

/ Каргин Н.И. /

«11» / 02 2020 г.

АКТ ВНЕДРЕНИЯ

материалов диссертационной работы Милославской Натальи Георгиевны на тему
«Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях», представленной на соискание ученой степени доктора технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Мы, нижеподписавшиеся, Каргин Николай Иванович, проректор, Климов Валентин Вячеславович, зам. директора ИИКС, Толстой Александр Иванович, и.о.зав. каф. 44, составили настоящий АКТ ВНЕДРЕНИЯ материалов диссертационной работы к.т.н, доцента Милославской Натальи Георгиевны о том, что в НИЯУ МИФИ были внедрены следующие результаты исследования:

–методология и принципы построения Учебно-научного центра «Интеллект в управлении сетевой безопасностью», которая была реализована на базе Института интеллектуальных кибернетических систем (ИИКС) в 2016 г. в составе трех учебно-научных лабораторий – «Предотвращение утечки конфиденциальной информации» (на базе DLP-системы компании «СёрчИнформ»), «Межсетевые экраны нового поколения» (на базе Palo Alto NGFW) и «Управление информацией и событиями безопасности» (на базе «СёрчИнформ SIEM»), что позволило на более высоком качественном уровне проводить учебные занятия и научные исследования по созданию систем управления сетевой безопасностью информационно-телекоммуникационных сетей (ИТКС), методам эффективного управления сетевой безопасностью ИТКС на основе применения интеллектуальных подходов, использованию технологии больших данных для обработки связанной с сетевой безопасностью информации, исследованию вопросов совместимости средств обеспечения сетевой безопасности и выработки рекомендаций по решению возникающих в связи с этим проблем, а также оценке защищенности ИТКС;

–архитектурные решения, предлагаемые в качестве основы построения учебно-научного центра, показавшие свою состоятельность в рамках функционирования ИТКС ИИКС.

Настоящий акт составлен в трех экземплярах.

Председатель комиссии:

_____/ Каргин Н.И. /

Члены комиссии:

_____/ Климов В.В. /
 _____/ Толстой А.И. /

АКТ О ВНЕДРЕНИИ в ООО «ЛИНС-М»



ООО «ЛИНС-М»

115409, г. Москва, шоссе Каширское,
дом 70, корпус 3, эт 2, каб 14

Тел. +7 (495) 109-90-00

УТВЕРЖДАЮ

Генеральный директор



Дата 07.09.2022

А К Т

о внедрении результатов докторской диссертационной работы
Милославской Натальи Георгиевны на тему
«Построение центров управления сетевой безопасностью
в информационно-телекоммуникационных сетях»

Комиссия в составе:

председатель – Никитин Александр Владимирович, генеральный директор ООО
«ЛИНС-М»,

члены комиссии:

Митричева Наталья Ильинична – Руководитель проектного офиса,

Власов Александр Валерьевич – Ведущий инженер 1-ой категории,

Мерзляков Александр Игоревич – Руководитель проектов,

составили настоящий акт о том, что результаты диссертационной работы
Милославской Натальи Георгиевны «Построение центров управления сетевой
безопасностью в информационно-телекоммуникационных сетях», представленной
на соискание ученой степени доктора технических наук по специальности 05.13.19
«Методы и системы защиты информации, информационная безопасность», а
именно:

- информационно-аналитические материалы, полученные в результате исследования центров управления безопасностью, и практические рекомендации по архитектурным улучшениям имеющихся центров в Центрах интеллектуального управления сетевой безопасностью (ЦИУСБ);

- рекомендации по разработке документального обеспечения функционирования ЦИУСБ;
- таксономия базовых понятий ИБ, а именно «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», которая используется при разработке Модели угроз ИБ, Модели нарушителей ИБ и Плана реагирования на инциденты ИБ;
- реестр рисков ИБ для информационно-телекоммуникационной сети (ИТКС), построенный на основе Моделей угроз ИБ и Моделей нарушителей ИБ;

внедрены в практику деятельности Общества с ограниченной ответственностью «ЛИНС-М» (ООО «ЛИНС-М»).

Разработанная в рамках диссертационной работы методика проектирования типового ЦИУСБ используется при проектировании ЦИУСБ для ИТКС заказчиков.

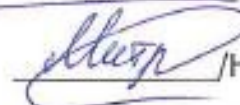
Следует отметить высокий научный и практический уровень результатов диссертационного исследования Милославской Н.Г. Большинство из них носят универсальный характер и могут быть эффективно применены для поддержки принятия решений по обеспечению ИБ ИТКС и реализации упреждающей защиты для них.

Настоящий акт составлен в трех экземплярах.

Председатель комиссии

 /А.В. Никитин/

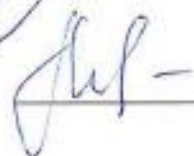
Члены комиссии:

 /Н.И. Митричева/

Члены комиссии:

 /А.В. Власов/

Члены комиссии

 /А.И. Мерзляков/

АКТ О ВНЕДРЕНИИ в Федеральном УМО в СВО по УГСНП «ИБ»

**ФЕДЕРАЛЬНОЕ УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЪЕДИНЕНИЕ
В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ ПО УКРУПНЕННОЙ ГРУППЕ
СПЕЦИАЛЬНОСТЕЙ И НАПРАВЛЕНИЙ ПОДГОТОВКИ
10.00.00 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**



№ 336/103 - УМО от 11.09.2020

УТВЕРЖДАЮ

Председатель Федерального УМО в
системе высшего образования по УГСНП
«Информационная безопасность»



А.Б. Пичкур

«14» сентября 2020 г.

АКТ

о внедрении результатов диссертационной работы Милославской Н.Г. на тему
«Построение центров управления сетевой безопасностью в информационно-
телекоммуникационных сетях»

Комиссия в составе:

председателя – председателя УМС по специальности «Компьютерная безопасность» к.т.н., доцента Макаренкова С.А.

членов комиссии – председателя УМС по специальности «Информационная безопасность телекоммуникационных систем» д.т.н., профессора Шалимова И.А.; заместителя председателя УМС по специальности «Компьютерная безопасность» д.ф.-м.н., профессора Черемушкина А.В.

составила настоящий акт о том, что основные положения диссертационного исследования доцента НИЯУ МИФИ, к.т.н., доцента Милославской Натальи Георгиевны на тему «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях» были использованы при разработке и внедрены в содержание следующих нормативных правовых и учебно-методических документов, регулирующих высшее образование в области информационной безопасности:

1. Федеральные государственные образовательные стандарты (ФГОС) высшего образования (в ред. 3 и 3+) по направлению 10.04.01 «Информационная безопасность» – уровня магистратуры (утверждены приказами Минобрнауки России от 28.10.2009 года № 497, от 1.12.2016 года № 1513), ФГОС по направлению 10.03.01 «Информационная безопасность» – уровня бакалавр (утверждены приказами Минобрнауки России от 28.10.2009 г. № 426, от 1.12.2016 года № 1515), а именно: требования к результатам освоения программы бакалавриата и магистратуры, содержанию профессиональных задач, решаемых выпускником; требования к структуре программы магистратуры и бакалавриата, в части определения обязательных дисциплин «Защищенные информационные системы»,

«Управление информационной безопасностью», «Основы управления информационной безопасностью»; требования к материально-техническому обеспечению, в части определения состава оборудования лабораторий в области технологий обеспечения информационной безопасностью и защищенных информационных систем.

2. Примерные учебные планы подготовки магистров по направлению 10.04.01 «Информационная безопасность», бакалавров по направлению 10.03.01 «Информационная безопасность» и специалистов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» в части обоснования включения дисциплин (объемы их изучения, результаты обучения, дидактика дисциплины): Основы управления информационной безопасностью, Управление информационной безопасностью, Защищенные информационные системы, Управление информационной безопасностью, Безопасность вычислительных сетей, а также дисциплин специализации «Информационная безопасность автоматизированных банковских систем». Примерные учебные планы по реализации ФГОС ВПО утверждены на Пленуме УМО ИБ 20 октября 2012 года, примерные учебные планы по реализации ФГОС ВО (ред. 3+) утверждены на XXI Пленуме УМО ИБ 20-24 мая 2017 года.

3. Примерные учебные программы дисциплин «Управление информационной безопасностью» и «Защищенные информационные системы», включенные в примерный учебный план подготовки магистров по направлению 10.04.01 «Информационная безопасность» в качестве обязательных. В содержание данных дисциплин включены теоретические положения и результаты диссертационного исследования. Примерные учебные программы дисциплин по реализации ФГОС ВО (ред. 3+) утверждены на XXI Пленуме УМО ИБ 20-24 мая 2017 года.

4. Кроме этого, в соавторстве Милославской Н.Г. были изданы учебные издания, рекомендованные для учебного процесса в образовательных организациях, в которых использованы результаты диссертационного исследования:

– учебники «Информационная безопасность открытых систем. Том 1: Угрозы, уязвимости, атаки и подходы к защите и Том 2. Средства защиты в сетях» с грифом Министерства образования и науки РФ «Допущено Министерством образования и науки РФ в качестве учебника для студентов высших учебных заведений, обучающихся по специальности 075500 (090105) – «Комплексное обеспечение информационной безопасности автоматизированных систем»;

– серия учебных пособий «Вопросы управления информационной безопасностью» в составе пяти книг с грифом Учебно-методического объединения вузов России по образованию в области информационной безопасности «Допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 – «Информационная безопасность» (уровень – магистр)»:

Книга 1: Основы управления информационной безопасностью. Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. М.: Горячая линия–Телеком, 2014 (второе издание). 244 с.

Книга 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. М.: Горячая линия–Телеком, 2014 (второе издание). 130 с.

Книга 3: Управление инцидентами информационной безопасности и непрерывностью бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. М.: Горячая линия–Телеком, 2014 (второе издание). 170 с.

Книга 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. М.: Горячая линия–Телеком, 2014 (второе издание). 214 с.

Книга 5: Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. М.: Горячая линия–Телеком, 2014 (второе издание). 166 с.

– Учебное пособие: Межсетевые экраны. Учебное пособие для вузов/ Н.Г. Милославская, А.И. Толстой. М.: Горячая линия–Телеком, 2020. 157 с. Рекомендовано Федеральным учебно-методическим объединением в системе высшего образования по УГСНП «Информационная безопасность» для студентов, обучающихся по направлению подготовки 10.04.01 «Информационная безопасность» и по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Настоящий акт составлен в трех экземплярах.

Председатель комиссии:
председатель УМС по специальности
«Компьютерная безопасность»

к.т.н., доцент



С.А. Макаренков

Члены комиссии:

председатель УМС по специальности
«Информационная безопасность
телекоммуникационных систем»

д.т.н., профессор



И.А. Шалимов

заместитель председателя УМС по специальности
«Компьютерная безопасность»

д.ф.-м.н., профессор



А.В. Черемушкин