ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
доктора военных наук, профессора
Лося Владимира Павловича
на диссертацию Милославской Натальи Георгиевны
на тему: «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях», представленную на соискание учёной степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы исследования определяется противоречием между, с одной стороны, невозможностью избежать осуществляемых искушенными злоумышленниками усложняющихся за счет применения новейших информационно-коммуникационных технологий (ИКТ) компьютерных атак на информационно-телекоммуникационные сети (ИТКС) организаций – субъектов критической информационной инфраструктуры (КИИ) Российской Федерации (РФ), и с другой стороны, использованием в этих условиях для обеспечения на одинаково высоком уровне информационной защищенности и, следовательно, функциональной устойчивости современных ИТКС устаревших стратегий и систем обеспечения информационной безопасности (СОИБ), основанных на принципе реагирования, а не упреждения угроз и инцидентов информационной безопасности (ИБ), и, как следствие, обеспечивающих недостаточный уровень ИБ ИТКС. Одна из остро стоящих научных проблем – формирование научной основы обеспечения сетевой безопасности 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 едином информационном пространстве (ЕИП) ОРГАНИЗАЦИИ.

Диссертация Милославской Н.Г. посвящена решению названной научной проблемы, имеющей важное значение для создания функционально устойчивой и защищенной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для организаций РФ. Эта проблема является новой и пока еще не имеет удовлетворительно разработанного научно-методического базиса. В этих условиях следует признать диссертационную работу Милославской Н.Г. весьма актуальной.

Содержание работы по главам. Диссертационная работа Милославской Н.Г. состоит из введения, шести глав, заключения, словаря терминов, списка литературы и шести приложений.

Во введении содержится краткий историко-содержательный экскурс решаемой научной проблемы, обоснована актуальность темы диссертации, сформулирована цель исследования, определен круг решаемых задач, обозначены общие подходы к достижению поставленной цели, а также приведены основные результаты, выносимые на защиту, показана их роль и сформулирована научная новизна.

В главе 1 с целью постановки научной проблемы диссертационного исследования и определения его границ на основе критического анализа положения дел по исследуемому вопросу выбирается и описывается объект исследования –

типовая ИТКС ОРГАНИЗАЦИИ, вводятся используемые в работе термины, устанавливаются особенности текущего состояния обеспечения ИБ информационных ресурсов ИТКС в условиях существования угроз ИБ в ЕИП ОРГАНИЗАЦИИ, определяется нормативная и правовая база, положенная в основу исследования, а также формулируются цель и задачи исследования.

В главе 2 для ИТКС разрабатывается таксономия взаимосвязанных понятий ИБ, таких как «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ», необходимых для упорядочивания знаний об информационной защищенности ИТКС, написания адекватных Стратегии и Политик ИБ и обоснования разработки системы и выбора методов и средств обеспечения ИБ для ИТКС ОРГАНИЗАЦИИ, что напрямую зависит от полноты и качества разработанной таксономии и представленных классификаций.

В главе 3 для ИТКС определяются понятия процесса, его результативности и эффективности, обеспечения ИБ, информационной защищенности и др., после чего детально описываются процессы обеспечения и управления ИБ, показывается их взаимная связь и даются определения обеспечения и управления сетевой безопасностью ИТКС, анализируется эволюция основных подходов к управлению сетевой безопасностью, перечисляются основные процессы проверки ИБ с особым вниманием к процессу мониторинга ИБ ИТКС как основы выявления событий и инцидентов ИБ в рамках функционирования центра интеллектуального управления сетевой безопасностью (ЦИУСБ) ОРГАНИЗАЦИИ. Далее подробно разрабатывается являющийся основой деятельности ЦИУСБ процесс управления инцидентами ИБ для ИТКС с детальным представлением карт его процессов и их описанием и показывается место разрабатываемого ЦИУСБ среди систем обеспечения и управления ИБ ОРГАНИЗАЦИИ в качестве фундамента системы управления инцидентами ИБ ИТКС.

В главе 4 подробно рассматривается SIEM-система как основа построения ЦИУСБ, поясняется концепция интеллектуальной безопасности, положенная в основу ЦИУСБ, анализируются два вида центров – предшественников ЦИУСБ, разрабатывается расширенная по сравнению с оригинальной бизнес-логика функционирования типового ЦИУСБ, показываются различные модели зрелости ЦУБ, на основе чего формулируются общие и специальные требования, а также требования по обеспечению собственной ИБ ЦИУСБ.

В главе 5 излагается разработанная автором методология построения типового ЦИУСБ ОРГАНИЗАЦИИ, после чего формулируются принципы его построения, представляются функциональные возможности для централизованного управления ИБ ИТКС и рассматриваются вопросы визуализации информации для принятия решений по управлению инцидентами ИБ в ИТКС. С учетом требований, изложенных в главе 4, для ЦИУСБ разрабатываются три архитектуры – функциональная, обработки больших и быстрых относящихся к ИБ ИТКС данных и обеспечения собственной ИБ – и проект SIEM-системы 3.0 с новым элементом, построенным с применением технологий блокчейна. Далее рассматриваются вопросы кадрового обеспечения и функциональной устойчивости ЦИУСБ в штатном режиме и в условиях угроз ИБ в ЕИП ОРГАНИЗАЦИИ и демонстрируется выполнение в разработанном типовом ЦИУСБ сформулированных в главе 4 требований.

В главе 6 приводится описание внедрения результатов диссертационной работы в Газпромбанке, российских компаниях «ЕС-лизинг» и «ЛИНС-М», зарубежной компании Qualys в регионах Восточной Европы, Кавказа и Центральной Азии, в НИЯУ МИФИ и Федеральном Учебно-методическом объединении в системе высшего образования по укрупненной группе специальностей подготовки «Информационная безопасность».

Заключение отражает основные выводы и результаты диссертационного исследования, намечает пути продолжения исследования.

Словарь терминов содержит обоснованно отобранные, уточненные и введенные автором термины, относящиеся к области сетевой безопасности.

Список литературы включает 307 источников, из которых 165 отечественных и 142 зарубежных авторов.

В шести приложениях приведены копии актов о внедрении и использовании результатов исследования.

В целом диссертация написана в хорошем литературном стиле и достаточно полно иллюстрирована. Выводы по каждой главе и работе в целом адекватно отражают полученные результаты.

Достоверность и новизна результатов диссертации. Достоверность результатов диссертации подтверждается использованием утвержденных в установленном порядке российских ГОСТов и международных стандартов, анализом большого объёма фактического материала, сравнением полученных автором результатов с другими известными методами и их критической оценкой, а также практическим внедрением полученных результатов научных исследований.

Основным научным результатом работы следует считать научно обоснованную методологию и принципы 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. Полученный комплекс результатов характеризуется существенной научной новизной, которая состоит в следующем:

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

— 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;

— проведена научно обоснованная структуризации базовых смысловых понятий ИБ 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 этих иерархически

взаимосвязанных таких сущностей, как «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»;

— разработаны основные принципы и базовые архитектурные решения построения перспективных ЦИУСБ для объектов КИИ РФ, а также необходимое расширение оригинальной бизнес-логики их функционирования при управлении инцидентами ИБ в ИТКС;

— обосновано и спроектировано средство блокирования попыток компрометации свидетельств инцидентов ИБ в ИТКС с применением технологий блокчейна;

— детально разработаны и формализованы с применением расширенного метода составления карт (с добавлением табличного описания) основные взаимосвязанные процессы управления инцидентами ИБ ИТКС, реализуемые в ЦИУСБ;

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

— уточнена и существенно расширена по сравнению с используемой временная шкала появления технологий и средств обеспечения сетевой безопасности, наглядно демонстрирующая эволюцию существующих и своевременно фиксировать появление новых технологий и средств;

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

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации. Исследование опиралось на общенаучные (анализ и синтез, сравнение и обобщение, научная абстракция, формальная логика) и специальные (системный, структурный и функциональный анализы, графические, экспертные методы, моделирование и т.д.) методы научного познания явлений и процессов, российские ГОСТы и международные стандарты, материалы научно-практических конференций и публикаций в периодической печати, а также лучшие практики в области обеспечения ИБ, что доказывает высокую степень их обоснованности.

Подтверждение опубликования основных результатов диссертации в научной печати. Основные результаты диссертационной работы прошли апробацию на конференциях всероссийского и международного уровня. Они с достаточной полнотой и соблюдем принципа научной преемственности с предшествующими работами по данной проблематике изложены в 56 печатных работах, в их числе в 21 публикации в изданиях, рекомендованных ВАК для опубликования основных научных результатов диссертаций на соискание ученой степени доктора наук. Большинство печатных работ с изложением методологии и принципов построения ЦИУСБ опубликовано соискателем без соавторов. В тех случаях, когда в диссертации использованы результаты работ, выполненных в соавторстве, автор обозначил свой личный вклад. Таким образом, можно заключить, что основные результаты и выводы диссертации строго обоснованы, являются новыми и получены автором самостоятельно. Особо следует отметить тот

факт, что автор свои исследования продолжает, о чем свидетельствует выходящие в 2021 г. монография и учебное пособие по теме диссертации.

Ценность для науки и практики результатов работы. Теоретическая ценность работы заключается в том, что в ней впервые обоснована необходимость совершенствования современных подходов к обеспечению ИБ современных сетей и предпринята попытка разработки для этих целей 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 за счет применения в ЦИУСБ интеллектуальных подходов обработки больших относящихся к ИБ ИТКС данных и на этой основе прогнозирования развития событий в области ИБ ИТКС. Для построения типового ЦИУСБ разработаны основные теоретические положения в виде ряда необходимых моделей, таксономий, процессов и архитектур, что вносит существенный вклад в развитие теории обеспечения ИБ.

Полученные в диссертационной работе Милославской Н.Г. результаты имеют существенную практическую ценность. Она заключается в разработке научно-методической базы создания типового ЦИУСБ, который может быть взят за основу при его внедрении в конкретной организации, учитывая ее специфику и внешний и внутренний контекст ведения деятельности.

Полученные в работе результаты создают значительный задел для продолжения и развития теоретических и прикладных исследований в сфере обеспечения сетевой безопасности в распределенных компьютерных системах.

Замечания по работе. В работе можно отметить ряд недостатков:

1. Подпункты «Новизна полученных результатов..» и «Теоретическая и практическая значимость» (Введение) по содержанию и формулировкам во многом схожи с изложением полученных результатов и целями работы.

2. Включение в систему такого дополнительного элемента как ЦИУСБ ОРГАНИЗАЦИИ изменяет свойства всей системы. Однако в диссертации не приводятся требования, предъявляемые к ЦИУСБ, чтобы этот новый элемент в системе не был более уязвимым, чем исходная система (Глава 3)?

3. Для формируемой стратегии обеспечения сетевой безопасности в типовом ЦИУСБ (Глава 5) могли бы быть указаны параметры, позволяющие регулировать информационную защищенность ИТКС, к которой применяется данная стратегия.

4. Некоторые превосходные степени прилагательных (например, «наиболее», «значительно») в тексте диссертации излишни.

Отмеченные недостатки, однако, относятся лишь к отдельным научным положениям и выводам диссертации и не являются определяющими при оценке значимости исследования в целом.

Соответствие содержания автореферата основным положениям диссертации. Автореферат достаточно полно и адекватно отражает основные результаты диссертации.

Соответствие диссертации требованиям, предъявляемым к диссертациям на соискание ученой степени доктора наук. Считаю, что диссертация Милославской Н.Г. представляет собою завершенную и целостную научно-квалификационную

работу, в которой на основании выполненных автором исследований разработаны методология и принципы построения типового ЦИУСБ для субъектов КИИ, 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. Тема диссертации полностью соответствует действующему паспорту специальности 05.13.19 – методы и системы защиты информации, информационная безопасность. Содержание диссертации соответствует отрасли наук, по которой присуждается ученая степень, – «технические науки».

Заключение по работе. Таким образом, диссертация Милославской Н.Г. оформлена согласно ГОСТ Р 7.0.11-2011, полностью соответствует критериям, установленным «Положением о порядке присуждения учёных степеней» для диссертаций на соискание учёной степени доктора наук, а ее автор, Милославская Наталья Георгиевна, достойна присуждения ей ученой степени доктора технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
Лось Владимир Павлович
РТУ МИРЭА, Центр исследования проблем кадрового обеспечения
отрасли информационной безопасности, директор
Президент Ассоциации защиты информации,
профессор, доктор военных наук, 20.01.03 – «Оперативное искусство в целом, по видам Вооруженных Сил, родам войск и специальным войскам», 20.02.12 – Военная кибернетика (в настоящее время - Системный анализ, исследование операций, моделирование боевых действий и систем военного назначения, компьютерные технологии в военном деле)
Тел. +7(903)740-32-61, email: los-vladimir@yandex.ru

_____Лось Владимир Павлович
«18» января 2021 г.

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» (РТУ МИРЭА)
119454, г. Москва, Пр-т Вернадского, д. 78
+7 (499) 215-65-65, rector@mirea.ru

Подпись руки Лось В.П.
УДОСТОВЕРЯЮ:
Начальник
Управления кадров
М.М. Буханова