

Федеральное государственное бюджетное образовательное
учреждение высшего образования
МИРЭА – Российский технологический университет

На правах рукописи

Магомедов Шамиль Гасангусейнович

**Методы и модели построения масштабируемой архитектуры
системы контроля доступа к вычислительным сервисам**

Специальность 05.13.15 — Вычислительные машины,
комплексы и компьютерные сети

Диссертация

на соискание ученой степени доктора технических наук

Научный консультант

доктор военных наук, профессор

Лось Владимир Павлович

Москва – 2022

Оглавление

Список сокращений	6
ВВЕДЕНИЕ	7
Глава 1. ОБЗОР ПОДХОДОВ К ПОСТРОЕНИЮ АРХИТЕКТУР И ИСПОЛЬЗУЕМЫХ ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ДОСТУПА К ВЫЧИСЛИТЕЛЬНЫМ СЕРВИСАМ	22
1.1. Аналитический обзор типовых подходов к построению архитектур вычислительных комплексов.....	22
1.2. Основные требования к архитектуре систем управления и контроля информационных систем.....	37
1.3. Анализ защищенных вычислительных архитектур.....	43
1.4. Системные факторы влияния на процесс контроля доступа	49
1.5. Современные перспективы развития технологий контроля доступа ...	53
1.6. Особенности защищенного обмена данными в области здравоохранения.....	66
1.7. Особенности защищенного обмена данными в области образования .	75
Выводы по главе.....	81
Глава 2. РАЗРАБОТКА МНОГОУРОВНЕВОЙ МАСШТАБИРУЕМОЙ АРХИТЕКТУРЫ КОНТРОЛЯ ДОСТУПА	83
2.1. Анализ современных концепций построения систем контроля доступа к информационным ресурсам.....	83
2.2. Формирование политик защищенности доступа к вычислительным комплексам.....	96
2.3. Модель обеспечения гарантированного качества предоставления сервисов при организации контроля доступа	102
2.4. Особенности использования методов моделирования в системах контроля доступа	112

2.5. Технологии построения и развития SIEM-систем.....	120
2.6. Анализ требований и условий проектирования архитектуры контроля доступа.....	127
2.7. Разработка четырехуровневой архитектуры системы контроля доступа.....	133
2.8. Разработка аппаратного уровня архитектуры системы контроля доступа.....	135
Выводы по главе.....	137
Глава 3. ОБЛАЧНАЯ ИНФРАСТРУКТУРА ОБРАБОТКИ ДАННЫХ СИСТЕМ КОНТРОЛЯ ДОСТУПА	139
3.1. Методика построения облачной инфраструктуры	139
3.2. Формирование сетевых функций виртуальной облачной инфраструктуры	141
3.2.1. Разработка виртуальной инфраструктуры для систем, использующих протокол DICOM	141
3.2.2. Разработка виртуальной инфраструктуры для систем, использующих протокол HTTP и для реализации UBA-системы	152
3.3. Построение виртуальной инфраструктуры	163
Выводы по главе.....	169
Глава 4. МЕТОД ОЦЕНКИ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ ДЛЯ КОМПОНЕНТОВ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА	170
4.1. Метод оценки ресурсной эффективности для оценки	170
4.2. Технология реализации имитационного виртуального стенда для оценки вычислительных ресурсов.....	173
Выводы по главе.....	183

Глава 5. СОВЕРШЕНСТВОВАНИЕ КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ РЕАКЦИЙ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С ЭЛЕМЕНТАМИ ИНТЕРФЕЙСА	185
5.1. Архитектура SIEM-систем с модулем анализа реакций пользователей	185
5.2. Экспериментальные исследования.....	188
5.3. Метод анализа реакций пользователей для контроля доступа и технология реализации модуля анализа данных	196
Выводы по главе.....	200
Глава 6. ПОСТРОЕНИЕ МНОГОУРОВНЕВОЙ АРХИТЕКТУРЫ ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ ДЛЯ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ДОСТУПА К СЕРВИСАМ ЗДРАВООХРАНЕНИЯ	201
6.1. Анализ программно-аппаратного обеспечения цифровой среды здравоохранения.....	201
6.1.1. Схема взаимодействия объектов медицинской инфраструктуры	203
6.1.2. Наиболее вероятные угрозы для медицинских учреждений	209
6.2. Анализ уязвимости инфраструктуры медицинских цифровых систем.....	215
6.3. Экспериментальный стенд для оценки ресурсоэффективности систем контроля доступа	223
6.4. Рекомендации к построению безопасной цифровой среды медицинского учреждения	236
Выводы по главе.....	243

Глава 7. ПОСТРОЕНИЕ МНОГОУРОВНЕВОЙ АРХИТЕКТУРЫ ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ ДЛЯ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ДОСТУПА К СЕРВИСАМ УЧРЕЖДЕНИЙ ВЫСШЕГО ОБРАЗОВАНИЯ	244
7.1. Типовая архитектура распределенных вычислительных комплексов для вычислительных сервисов сферы образования.....	244
7.2. Система анализа поведения пользователей (UBA)	249
7.3. Система сетевого анализа трафика на основе поведения пользователей	253
7.4. Описание тестового стенда с многоуровневым контролем доступа ..	258
Выводы по главе.....	274
ЗАКЛЮЧЕНИЕ	276
ЛИТЕРАТУРА	278
ПРИЛОЖЕНИЕ 1	310

Список сокращений

IDS	— intrusion detection system
PACS	— picture archiving and communication system
RBR	— rule based reasoning
SEM	— security event management
SIEM	— security information and event management
SIM	— security information management
UBA	— user behavior analytics
UEBA	— user and entity behavior analytics
QoS	— Qulity of Service
БД	— база данных
БК	— вычислительный комплекс
ВР	— время реакции
ВС	— вычислительные сервисы
ИБ	— информационная безопасность
ИС	— информационных систем
КД	— контроль доступа
МИС	— медицинская информационная система
ПО	— программное обеспечение
ППД	— полномочная политика доступа
ПСП	— пассивные средства противодействия
РПД	— дискреционное управления доступом
СДО	— система дистанционного обучения
СП	— средства противодействия
СХД	— системы хранения данных
ТЗ	— техническое задание
ЦП	— цифровые порталы

ВВЕДЕНИЕ

Актуальность исследования. В настоящее время все больше государственных [1], медицинских [2], банковских [3], образовательных [4] и прочих услуг переносится в цифровую среду [5]. Активное развитие цифровизации [6, 7] определило ее массовое проникновение во все сферы жизни и деятельности [8]. Экономические отношения и отношения людей с государственными органами принимают форму взаимодействия с вычислительными сервисами по компьютерным сетям [9–11]. Основным инструментом цифровой среды становятся веб-сервисы (или цифровые порталы, вычислительные сервисы, далее — ВС) или специализированные приложения, подключенные к общедоступным сетям [12].

В развивающейся цифровой среде разработчики ВС стоят перед решением противоречия: с одной стороны — вычислительный сервис должен быть максимально доступен, платформонезависим, удобен и прост в использовании (желательно, например, в «один клик»); с другой — предоставляемые услуги связаны с большим количеством персональных, медицинских, банковских и прочих конфиденциальных данных, защита которых требует значительного дополнительного контроля, верификации пользователя [13]. Для обеспечения защищенного контроля доступа (КД) [14] используются технологии информационной безопасности. Подключение внешних модулей к вычислительному комплексу, обслуживающему ВС, требует учета вычислительных ресурсов, определения точек интеграции компонентов контроля доступа [15].

Системы КД являются частью информационных систем, обеспечивающих ВС, в тоже время КД представляют собой отдельные компоненты, под управление КД выделяется часть инфраструктуры, виртуальные и физические ресурсы ВК, то есть система КД — это самостоятельный объект со своими задачами проектирования и конфигурирования [16]. Системы

КД могут развиваться отдельно от собственно технологий, обеспечивающих предоставление ВС: могут добавляться реализации новых концепций КД; может обновляться и изменяться программное, аппаратное обеспечение, не затрагивая при этом основных функциональных возможностей ВС. Все вышесказанное делает актуальной задачу проведения теоретических, экспериментальных, структурных, программно-аппаратных исследований по разработке принципов и решений по построению новых и совершенствованию существующих средств защищенного доступа к ВС на основе построения масштабируемой архитектуры системы КД, обеспечивающих функционирование многопользовательских ВК.

В ВС имеется ряд специфических задач, связанных с КД: передача паролей и средств контроля сторонним лицам; защита от перехвата паролей программными средствами; выявление ситуаций, в которых пользователь, прошедший все способы верификации, оставил систему активной (сознательно или случайно), а другой пользователь стал взаимодействовать с ВС и др., требующие постоянного подтверждения личности пользователя в процессе взаимодействия [17]. В банковских антифрод-системах [18, 19] используется система анализа подозрительных операций; в системах с повышенной конфиденциальностью используются средства, анализирующие поведение пользователя. Включение компонентов анализа поведения пользователя [20–21] и других потенциальных современных технологий должно быть обеспечено масштабируемостью архитектуры КД.

Таким образом, разработка методов и моделей построения масштабируемой архитектуры контроля доступа к вычислительным сервисам на основе совершенствования существующих средств защиты информации и обеспечения информационной безопасности, является актуальной задачей, имеющей важное значение для развития защищенной современной цифровой среды.

Научная проблема. Системы КД к информационным ресурсам развиваются параллельно с самими информационными системами: чем больше функций, разных категорий доступа к данным, тем сложнее становится контроль. Это определяет проблему построения такого организационно-технологического решения, которое позволяло бы наращивать мощности и совершенствование технологий информационной безопасности в рамках общей вычислительной архитектуры и инфраструктуры. Особенно важным контроль доступа является для веб-сервисов, порталов, предоставляющих доступ по компьютерным сетям общего пользования. В этих случаях добавляется необходимость постоянной верификации пользователя, защиты от несанкционированного доступа со стороны субъектов и программных систем. Системы контроля в соответствии с новыми технологиями должны иметь возможность совершенствования КД и системы предупреждения киберугроз. Таким образом, в настоящее время стоит проблема, требующая научных теоретических и экспериментальных исследований по разработке принципов, методов и моделей построения архитектуры контроля доступа к ВС, обеспечивающей интеграцию технологий передачи, хранения, мониторинга, идентификации и аутентификации пользователей и субъектов информационных процессов.

Состояние проблемы. В настоящее время развиваются системы КД, основанные на концепции SIEM (Security information and event management) [23–25], которая объединяет мониторинг событий в реальном времени и управление информационной безопасностью. Существуют коммерческие решения SIEM-систем: QRadar IBM [26], Arc Sight HP [27], Symantec Security Services [28], FortiSIEM и др. [24]. Разработке SIEM-систем, выявлению источников угроз и механизмов их выявления посвящено значительное количество современных исследований: в распределенных системах [29–32] (И.В. Котенко, И.Б. Саенко, А.В. Степашкина, L. Kufel, L. Coppolino, S. D’Antonio, N. Kheir, M. Frigault и др.); для блоки-

ровки вредоносного трафика с устройств IoT [25, 31] (Н.Г. Милославская, B. Al-Duwairi, R. Fahmawi и др.); интеллектуальной обработке данных из нескольких источников [33, 34] (J. Lee, J. Kim, N. Moukafih, G. Orhanou, S. El Hajji и др.); использование методов классификации событий [35] (J.C. Sancho; A. Caro, A. Walker, J. Svacina, A.S.M. Kayes, R. Kalaria, M. Islam и др.) и многие другие [36, 37] исследования.

Для веб-сервисов одним из способов является использование role-based access control (RBAC) [38], где каждая точка входа связана с набором ролей пользователя. Различные исследовательские группы разработали контекстно-зависимые подходы и структуры управления доступом, которые различаются своими контекстными моделями, моделями политик и возможностями рассуждений [39]. Было предложено несколько моделей управления доступом на основе ролей [40–43], включающих в политики динамически изменяющиеся контекстные условия (например, информацию, ориентированную на местоположение пользователя и ресурсы). Подобно пространственному и временному подходам [44, 45], эти контекстно-зависимые подходы в основном зависят от предметной области и принимают во внимание определенные типы контекстных условий. Контекстно-зависимый подход к управлению доступом на основе ролей был разработан [22, 46] для облегчения управления доступом к ресурсам данных на основе широкого диапазона контекстных условий.

Перспективным направлением многопользовательских сервисов является анализ КД на основе шаблонов поведения — технологии UBA (анализ поведения пользователей, User behavior analytics) [20, 46–49]. Предложены разные варианты развития UBA: использование интеллектуальных технологий, применение встраиваемых динамических моделей в интернет-приложения [50] (В.В. Миронов и соавторы); ситуационные и прецедентные модели (K. Csaba, H.B. Péter, X. Xi, T. Zhang и др.) и т. п. [48, 49]. Современные психологические исследования выявили достоверность данных

по исследованию реакций, полученных с использованием веб-интерфейсов с данными, полученными в лабораторных условиях [51], что позволяет признать целесообразным использовать психомоторные реакции.

В настоящее время SIEM и UBA рассматриваются как дополняющие друг друга концепции. Причем исследования происходят в аспектах информационной безопасности. При внедрении их в практику выясняется ряд нерешенных задач, связанных с возможностью интеграции вычислительных комплексов, масштабируемости, ресурсоэффективности, точек подключения систем мониторинга, выбора способов и места для хранения вспомогательных данных, направления и анализа потоков данных и прочих вопросов, относящихся к архитектуре, структуре и технологиям вычислительных комплексов.

Типовая архитектура внедряемых систем КД включает в себя следующие уровни: сетевой; систем хранения; инфраструктуры приложений; систем управления; систем безопасности. Такой подход обеспечивает решение задач безопасности без учета ресурсных затрат и способов обработки данных КД, что затрудняет внедрение. Работы по масштабируемой архитектуре комплексов обеспечения сетевой безопасности [16] (О.Ю. Гузев, И.В. Чижов) определяют следующий состав: аппаратная платформа, виртуальные машины, программный гипервизор, средства управления вычислительной инфраструктурой, средства управления коммутацией сетевого трафика, средства коммутации сетевого трафика. Однако этот подход нацелен на конкретные технологии реализации анализа сетевого трафика и управления виртуальными ресурсами, не вводя методологические принципы построения архитектуры КД, что не дает возможность учесть совершенствование технологий и масштабируемость.

Таким образом, все вышеперечисленные результаты дают предпосылки для проведения теоретических и экспериментальных исследований по

разработке принципов, методов и моделей построения масштабируемой архитектуры КД для обеспечения защищенного доступа к ВС.

Цель: разработка принципов, методов и моделей построения масштабируемой архитектуры контроля управлением доступа, обеспечивающей интеграцию технологий передачи, хранения, мониторинга, идентификации и аутентификации пользователей и субъектов информационных процессов доступа к вычислительным сервисам по компьютерным сетям.

Задачи:

1. Обзор подходов информационной безопасности к построению архитектур и используемых технологий обеспечения разграничения и контроля доступа к ВС.
2. Анализ общих моделей ВС и выявление особенностей интеграции технологий КД.
3. Исследование особенностей архитектуры и технологии построения SIEM и UBA-систем.
4. Формирование комплекса методов и моделей построения многоуровневой масштабируемой архитектуры КД.
5. Разработка методики проектирования инфраструктуры виртуальных ресурсов КД.
6. Разработка метода оценки ресурсных затрат при внедрении технологий КД.
7. Разработка ресурсоэффективного метода КД для анализа поведения пользователей.
8. Разработка методик учета прикладных аспектов при разработке архитектуры КД.
9. Внедрение результатов.

Объект исследования: программно-аппаратные средства защиты информации в информационных системах, обеспечивающих предоставление вычислительных сервисов по общедоступным компьютерным сетям.

Предмет исследования: архитектуры, технологии реализации КД, включающие системы идентификации и аутентификации пользователей и субъектов информационных процессов, связанных с действиями устройств и пользователей при взаимодействии с вычислительными сервисами.

Методы исследования: методы создания новых и совершенствования существующих средств защиты информации и обеспечения информационной безопасности информационных систем; организации защиты специальной обработки данных, хранения и ввода-вывода информации, обработки информации, многопроцессорных и многомашинных систем; модели противодействия угрозам нарушения информационной безопасности информационных систем.

Научная новизна:

1. Сформулированы принципы и модели построения архитектуры системы КД как подсистемы программно-аппаратного вычислительного комплекса, имеющей собственные задачи: сбор, передачу, хранение и обработку данных о действиях пользователей и программных систем, методы, ресурсы и технологии обработки которых независимы от используемых для предоставления ВС. Таким образом, система КД требует собственных вычислительных ресурсов, при этом должны быть соблюдены технико-экономические ограничения. Предложенный подход позволяет сформулировать ряд задач, являющихся типовыми для рассматриваемого класса объектов: определить состав системы сбора данных, содержащих информацию о доступе к ВС; сформировать виртуальную инфраструктуру для обработки данных КД; определить состав и технико-экономические требования к вычислительным ресурсам для компонентов анализа данных системы КД.

2. Разработана четырехуровневая масштабируемая архитектура системы контроля доступа, интегрируемая в вычислительные комплексы, обеспечивающие защиту взаимодействия пользователей с ВС. Архитекту-

ра включает комплекс понятий и свойств системы КД, реализованных в ее элементах, взаимосвязи компонентов, основанных на реализации функций КД. Масштабируемость архитектуры определяется наличием четырех уровней, на каждом из уровней определен специфический класс задач, который может быть реализован разными вариантами технологических решений, что позволяет внедрять различные технологии КД: SIEM, UBA и др.

3. Разработана методика построения облачной инфраструктуры, обеспечивающей решение задач КД. Сформированы принципы решения задач сбора и перенаправления специализированных данных о доступе к ВС, для которых требуется с использованием облачных технологий виртуализировать ресурсы с целью обеспечения параллельного решения задач КД с основными функциями ВС.

4. Разработаны модель и метод анализа затрат вычислительных ресурсов для реализации систем контроля доступа на основе подхода, использующего имитационные виртуальные стенды в условиях заданных характеристик эксплуатации.

5. Предложен метод контроля доступа на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса на основе анализа времени ответа на контрольные вопросы. Предложенный метод дополняет и совершенствует существующие методы верификации пользователей при доступе в ВС.

6. Разработаны методики учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычислительных комплексов (на примере медицинских и образовательных услуг).

7. Разработаны принципы и информационные модели проектирования архитектуры системы КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза.

Достоверность и обоснованность научных результатов и рекомендаций, приведенных в диссертационной работе, основаны на корректном использовании архитектурных, структурных, логических и программно-аппаратных методов создания систем защиты информации, на применении вычислительно надежных моделей, проведении экспериментальных исследований, а также апробации и обсуждении результатов на международных научных конференциях и семинарах, публикациях результатов в рецензируемых отечественных и международных изданиях.

Теоретическая и практическая значимость исследования. Внедрение.

Результаты работы использованы при выполнении работ по грантам и договорам:

1) государственный контракт № 087/ГК на выполнение работ (оказание услуг) для государственных нужд «Создание цифровой образовательной среды и разработка (доработка) ЭОР для учителей школ за рубежом», проводимый в рамках Национальной программы «Цифровая экономика Российской Федерации» утвержденной президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16;

2) соглашение о предоставлении из федерального бюджета субсидии в соответствии с абзацем вторым пункта 1 статьи 77.1 Бюджетного кодекса Российской Федерации (внутренний номер 08-01/X4354/706) № 075-02-2019-2358 от 20.11.2019, «Проектирование интеграционной платформы непрерывного образования»;

3) соглашение о предоставлении из федерального бюджета субсидии в соответствии с абзацем вторым пункта 1 статьи 77.1 Бюджетного кодекса Российской Федерации (внутренний номер 08-04/X4354/706) № 075-02-2020-1583 от 06 апреля 2020 года, «Разработка и реализация мер по выделению грантов аспирантам и молодым ученым и проведению научно-

образовательных и проектных мероприятий в области информационной безопасности для задач цифровой экономики»;

4) договор № 308ГРНТИС5/42860-3 от 30.10.2018 г. по выполнению проекта «Развитие системы поддержки принятия врачебных решений на основе международных баз данных по доказательной медицине и в соответствии с Национальными клиническими рекомендациями и Стандартами оказания медицинской помощи в Российской Федерации, в том числе для наблюдения за больными с профессиональными заболеваниями и с высоким риском их развития и для профилактики и лечения возраст-зависимых патологических процессов и заболеваний».

Результаты работы использованы в РТУ МИРЭА, Федеральном бюро медико-социальной экспертизы Министерства труда и социальной защиты Российской Федерации, ФГУП «НПО «Техномаш», ООО «Непрерывные технологии», ООО «Коллектив Интеллидженс Системс», ФГУП «НТЦ «Орион».

Апробация. Основные положения и результаты исследования, составляющие содержание диссертации, докладывались и обсуждались на Futuristic Trends in Networks and Computing Technologies (FTNCT-2020) (Таганрог, 13–15.10.2020); Научно-практической конференции «Цифровые аналитические инструменты и прикладные программы в образовании» (Москва, РАО, 27.10.2020); Big Data & AI Conference 2020 (Москва, 17–18.09.2020); II Всероссийской научно-технической конференции «Состояние и перспективы развития современной науки по направлению «Информационная безопасность» (Анапа, 19–20.03.2020); V региональной научной конференции «Прикладные исследования и технологии» ART2018 (Москва, 15–16.07.2018); XXVII научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт Петербург, 24–26.09.2018); III Всероссийской научно-практической конференции «Информационные технологии в экономике и управлении» (Ма-

хачкала, 29–30.11.2018); Межвузовской школе-семинаре «Задачи системного анализа, управления и обработки информации» (Москва, МТИ, 2017, 2019); LXVI Международной научно-практической конференции «Технические науки — от теории к практике» (Новосибирск, 2017); Всероссийской научно-практической конференции «Актуальные проблемы науки и практики в предпринимательстве» (24.03.2017); XX Международной научно-практической конференции «Теории и практика современной науки» (22.03.2017); V Международной научно-практической электронной конференции «Социально-антропологические проблемы информационного общества» (10.03.2017); VI Международной научно-практической электронной конференции «Современные научные исследования: актуальные теории и концепции» (10.04.2017); XV Международной научно-практической конференции «Научный поиск в современном мире» (31.04.2017); XIII Международной научно-практической конференция «Теоретические и практические проблемы развития современной науки» (31.03.2017).

Положения, выносимые на защиту.

1. Принципы и модели построения архитектуры системы КД, как подсистемы программно-аппаратного вычислительного комплекса, имеющей собственные данные, цели, задачи и технологии реализации, отличные от ВС. Отличие от альтернативных подходов связано с возможностью параллельной разработки, поэтапного внедрения, возможностью замены или расширения элементов системы КД, что можно реализовать, с одной стороны — независимо, с другой — используя требования и условия эксплуатации. Построение КД, разработанного в соответствии с предложенными принципами, позволяет провести обоснованную оценку вычислительных ресурсов, что даст возможность сократить затраты на внедрение КД, обеспечить миграцию на новые технологии, возможность поэтапного внедрения отдельных компонентов КД.

2. Четырехуровневая масштабируемая архитектура системы КД, интегрируемая в вычислительную среду ВС, обеспечивающая защищенный доступ: 1) программно-аппаратный уровень, включающий средства, обеспечивающие КД; 2) уровень виртуальной инфраструктуры обработки данных системы КД; 3) уровень физических ресурсов для обработки данных КД; 4) уровень компонентов анализа данных. Четырехуровневость обеспечивает интуитивно понятную декомпозицию задач, решение которых может быть осуществлено специалистами разных квалификаций, а также совершенствование методов и моделей на каждом уровне независимо от других уровней архитектуры. Архитектура может быть реализована разными вариантами технологических решений.

3. Методика построения облачной инфраструктуры, обеспечивающей решение задач КД. Методика основана на принципе сбора и перенаправления специализированных данных о доступе к ВС, выделении прав защищенного доступа, основанного на выявлении серверных ролей. Облачная инфраструктура, в отличие от иных решений, позволяет обеспечить миграцию системы КД.

4. Метод и модель ресурсного анализа реализации элементов системы КД на основе имитационных исследований. Особенностью метода является повышение эффективности использования логирования сеансов доступа, позволяющее получить экспериментальные оценки скорости обработки, объемов и ширины каналов и др. характеристик ресурсов, требуемых для модулей КД.

5. Новый метод и соответствующая система КД на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса на основе анализа времени ответа на контрольные вопросы. Предложенный метод дополняет и совершенствует существующие методы верификации пользователей при доступе в ВС. Метод позволяет учитывать персональные реакции только на основе времени ответа на контрольные

вопросы, что позволяет существенно сократить затраты ресурсов для оперативного анализа.

6. Методики учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычислительных комплексов на примере медицинских и образовательных услуг. Предложенные методики направлены на сокращение затрат вычислительных ресурсов, обеспечивающих заданный уровень защищенности взаимодействия пользователей с вычислительными сервисами.

7. Разработаны принципы и информационные модели проектирования архитектуры системы КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза в условиях защищенной цифровой образовательной среды. Использование разработанных методов и моделей КД способствует повышению защищенности образовательных ресурсов от несанкционированного доступа.

Соответствие паспорту специальности.

Область исследования соответствует пп.: «1. Разработка научных основ создания вычислительных машин, комплексов и компьютерных сетей, исследования общих свойств и принципов функционирования вычислительных машин, комплексов и компьютерных сетей», поскольку результаты работы направлены на формирование вычислительных комплексов, в архитектуру которых включены системы контроля доступа; «2. Теоретический анализ и экспериментальное исследование функционирования вычислительных машин, комплексов и компьютерных сетей с целью улучшения их технико-экономических и эксплуатационных характеристик», что соответствует проведенным исследованиям, направленным на экспериментальную оценку ресурсных затрат при включении в комплексы многоуровневого контроля доступа; «5. Разработка научных методов и алгоритмов создания структур и топологий компьютерных сетей, сетевых протоколов и служб передачи данных в компьютерных сетях, взаимодействия компью-

терных сетей, построенных с использованием различных телекоммуникационных технологий, мобильных и специальных компьютерных сетей, защиты компьютерных сетей и приложений» соответствует рассматриваемому объекту исследования — защищенному доступу к вычислительным сервисам на основе многопользовательских веб-сервисов или мобильным приложениям.

Публикации по теме диссертации. Основные результаты диссертационного исследования опубликованы в 51 работе, из них: 14 — в изданиях, включенных в перечень рецензируемых журналов, рекомендованных ВАК по специальности 05.13.15; 20 — индексируемых в Web of Science/Scopus (включая квартиль Q1/Q2); 9 свидетельств о регистрации РИД.

Личный вклад соискателя в получение результатов, изложенных в диссертации. Все результаты и положения, составляющие основные результаты, выносимые на защиту, получены автором. Работ, выполненных без соавторов — 14. В работах, опубликованных в соавторстве, личный вклад состоит в разработке архитектуры вычислительных комплексов, средств контроля доступа, методик контроля доступа на основе технологий SIEM и UBA.

Структура и объем. Диссертация состоит из семи глав, введения, заключения, приложений, изложена на 309 с. текста, библиографический список содержит 249 источников.

В первой главе проведен анализ современных вычислительных инфраструктур, систем и комплексов, обеспечивающих поддержку и контроль доступа в информационной среде цифровых услуг. Сформулированы актуальные направления исследований по разработке архитектур контроля доступа в вычислительных комплексах, функционирующих в цифровой среде.

Во второй главе сформулированы задача проектирования архитектуры контроля доступа, требования к составу средств контроля доступа; разра-

ботана (в условиях заданных технико-экономических характеристик) четырехуровневая архитектура контроля доступа к вычислительному комплексу, предоставляющему веб-сервисы.

В третьей главе рассмотрены вопросы построения уровня облачной инфраструктуры архитектуры КД, изложена методика распределения виртуальных вычислительных ресурсов и сетевого взаимодействия, рассмотрен пример инфраструктуры для КД при сетевом взаимодействии на примере протокола DICOM.

В четвертой главе предложена методика экспериментального оценивания, требуемого для резервирования количества вычислительных ресурсов при проектировании системы КД.

В пятой главе предложен метод контроля доступа на основе использования психологических реакций, которые могут быть измерены при работе с интерфейсами; метод экспериментально проверен на большой выборке; разработана методика использования реакций в системах КД.

В шестой главе описывается система КД к ВС медицинского учреждения, которая подразумевает как базовую защиту периметра с помощью межсетевых экранов и правил доступа, реализуемых в сетевом оборудовании, так и компоненты защиты архива DICOM и сервера приложений.

В седьмой главе описывается система КД к ВС учреждений образования, которая подразумевает как базовую защиту периметра с помощью межсетевых экранов и правил доступа, реализуемых в сетевом оборудовании, так и компоненты защиты серверов СДО (тестирование студентов, личные кабинеты пользователей), включая анализ пользовательской активности.

Глава 1. ОБЗОР ПОДХОДОВ К ПОСТРОЕНИЮ АРХИТЕКТУР И ИСПОЛЬЗУЕМЫХ ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ДОСТУПА К ВЫЧИСЛИТЕЛЬНЫМ СЕРВИСАМ

В главе проведен анализ современных вычислительных инфраструктур, систем и комплексов, обеспечивающих поддержку и контроль доступа в информационной среде цифровых услуг

1.1. Аналитический обзор типовых подходов к построению архитектур вычислительных комплексов

При разработке вычислительных комплексов (ВК), создаваемых с целью обеспечения потребностей вычислительных сервисов (ВС) достаточно часто возникает следующая ситуация: цели разработки ВК, поставленные первоначально, не достигнуты, а сам процесс создания обходится слишком дорого (это касается трудовых, материальных и временных затрат), причем это положение становится очевидным на поздних этапах разработки или даже эксплуатации ВС. Чаще всего проблемы такого рода появляются в связи с тем, что цели разработки ВК не были четко поставлены, и, кроме того, отсутствовали подходы к проектированию, разработке, внедрению, использованию и развитию ВС.

В процессе работы над большими сложными проектами следует использовать комплексные подходы к разработке, которые дают возможность контролировать ситуацию и управлять значительным количеством модулей, входящих в состав разрабатываемых ВК, при этом принимая во внимание различные организационные роли.

Архитектурный подход к построению ВК представляет собой комплекс мероприятий, выполнение которых дает возможность увеличить эф-

фективность, управляемость, масштабируемость, а также безопасность реализуемых вычислительных комплексов. Архитектурой информационной системы называется совокупность описаний всех частей ВК, а также взаимодействий между ними.

В современных отечественных и зарубежных источниках по тематике проектирования автоматизированных и информационных систем достаточно часто применяется понятие «архитектура системы» [52–54], при этом оно интерпретируется разными способами. Например, стандарт ANSI \ IEEE 1471-2000 [55, 56] Института инженеров электротехники и электроники определяет такие элементы архитектуры, как схемы, представления, среды, обоснования, заинтересованные стороны и т. д. (рис. 1.1).

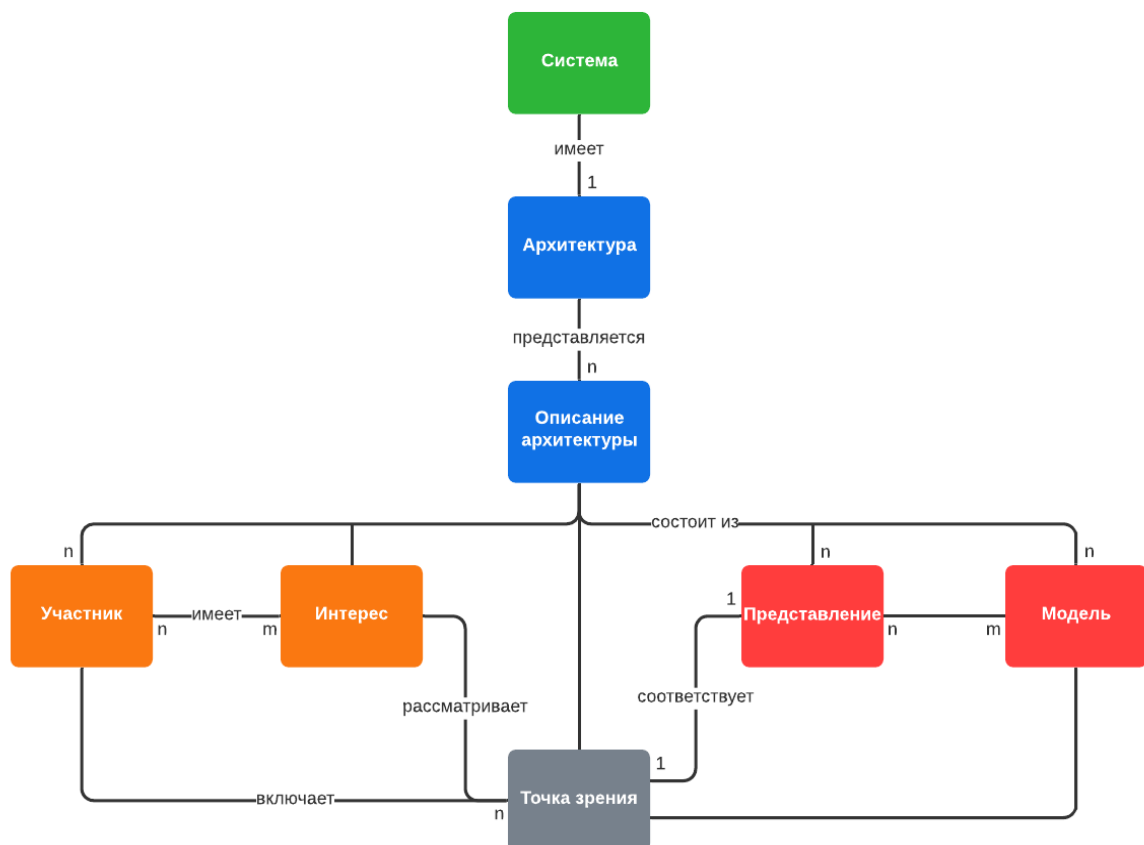


Рисунок 1.1 — Рамочная модель разработки архитектуры системы
в соответствии со стандартом IEEE 1471-2000

В соответствии с этим положением, архитектура ВК может рассматриваться по-разному в зависимости от существующих представлениями заинтересованных лиц.

Само понятие архитектуры ВК [57, 58] можно изучать с различных сторон. Возможно рассмотрение понятий «системная архитектура» (System Architecture) и «программная архитектура» (Software Architecture). В зависимости от контекста архитектура ВК, технологическая архитектура информационной системы (ИС) или архитектура продукта (группы продуктов), выпускаемого этой организацией, может быть названа «системной архитектурой».

Описание и проектирование архитектуры ВК имеет много общего с описанием архитектуры ВС. Однако следует отметить, что архитектура программных систем является самостоятельной сферой знаний, которая исследуется в большом количестве публикаций [53, 59, 60]. В зависимости от контекста термин «программная архитектура» может использоваться для описания архитектуры взаимодействия компонентов в составе ИС организации (архитектура приложений); архитектуры взаимодействия классов в рамках приложения или архитектуры программных модулей. Перечисленные виды архитектуры можно рассматривать с разных точек зрения, а также с разным масштабированием. Можно выделить следующие способы представления программной архитектуры:

- концептуальный — представлены компоненты и их функциональность, причем достаточно неформальным языком. Чаще всего это описание используется при обсуждении с руководством, бизнес-менеджерами, а также непосредственными пользователями (каким функционалом должна обладать система);
- логический — представлены правила взаимодействия компонентов, а также интерфейсы и протоколы. Этот уровень обеспечивает наиболее эффективное выполнение параллельной разработки;

- физическая реализация — согласование с типами используемого оборудования, определенными параметрами среды (например, операционными системами — ОС), узлами размещения. Стандарт ANSI/IEEE 1471-2000 достаточно схематично описывает модель создания архитектуры. Однако различные виды архитектур являются необходимыми при представлении основ архитектурного подхода.

Согласно стандарту ГОСТ 33.320-96 «Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы» [61] архитектура ИС состоит из: внешней схемы (внешние интерфейсы); внутренней схемы (пользовательский интерфейс); концептуальной схемы (содержимое базы данных, в т. ч. перечень возможных действий); информационного процессора, информационной базы. Исследуем данные понятия более подробно:

- внешняя схема — информация о формах внешнего представления для допустимых наборов предложений (формы соответствуют запросам пользователей) и специфике их использования;
- внутренняя схема — сведения о формах внутреннего представления для возможных наборов предложений и специфике их использования;
- концептуальная схема — перечень высказываний, необходимых для решения задач в конкретной области;
- информационная база — перечень предложений, соответствующих высказываниям (согласованным с концептуальной схемой, а также между собой), которые не являются обязательными;
- информационный процессор — в ответ на команду выполняет действие над информационной базой и/или концептуальной схемой.

На этапах разработки автоматизированной системы (АС), которые определены в ГОСТ [62], синтез структуры разрабатываемой системы яв-

ляется необходимым уже во время создания концепции АС. Позднее такая необходимость возникает на этапе формирования ТЗ на разработку системы. Обычно архитектуру и структуру АС на данных этапах отождествляют.

Необходимо отметить, что зарубежные стандарты содержат значительное количество подходов к определению архитектуры системы [57, 60, 63–70].

Понятия «информационная система» и «автоматизированная информационная система» представлены в большом числе стандартов (и российских, и зарубежных), а также в публикациях на данную тематику и нормативной документации. Эти определения соответствуют перечисленным аспектам понятия «автоматизированная информационная система»:

- целевой — сбор, хранение, обработка, поиск, накопление и распространение информации в разных сферах деятельности;
- структурный — компоненты системы: пользователи, информационные, аппаратные и программные компоненты, а также документация объединяются в комплексы;
- функциональный — информационная технология представляет собой набор взаимосвязанных функций, задач и процедур, которые могут быть реализованы в автоматическом или интерактивном режимах.

По мнению авторов [59], эволюция архитектуры ИС обусловлена необходимостью определения требований, предъявляемых к архитектурам организаций, а также внедрением архитектурного подхода в управление организацией. Главные фундаментальные положения разработки архитектуры предприятия утверждены в стандарте ISO 15704 [64]. Данный стандарт регламентирует построение методологий и архитектур организации (Enterprise-reference Architectures and Methodologies) [71]. Разработанный и

введенный в действие в 2006 г. ISO 19439 «Enterprise integration — Framework for enterprise modelling» [72] базируется на основных принципах ISO 15704.

В стандарт ISO 15704 были включены в 2005 г. «Дополнительные представления с точки зрения пользователя» (Additional views for user concerns). Назначение стандарта ISO 15704 — это решение таких задач, как создание предприятия, реструктуризация и изменения, связанные с его развитием. Стандарт ориентирован и на пользователей, и на технологии, в нем сделан акцент на неизбежности применения комплексного подхода к построению автоматизированной системы. Основой стандарта служит подход, отличающийся от общепринятых стандартов и методик в области информационных технологий: центр внимания — это сама организация, рассматриваемая как многогранный, сложный объект [73].

Следует отметить, что ISO 15704 выделяет два типа архитектур предприятия: «3.2. архитектура: Описание (модель) основной компоновки и взаимодействия частей системы (будь то физический или абстрактный объект, или сущность). Существует только два типа архитектур, имеющих отношение к интеграции предприятий:

- системные архитектуры (архитектуры «типа 1»). Их действие распространяется на проектирование системы, например, на компьютеризованную систему, которая является компонентом системы интеграции предприятия;
- стандартные проекты предприятия (архитектуры «типа 2»). Их действие распространяется на организацию разработки и реализации проекта, например, интеграцию предприятия или иную программу развития».

В стандарте, в первую очередь, рассматриваются требования, которые предъявляются к архитектурам типа 2 («референсные архитектуры и методологии»).

В [53] отмечается, что результатом анализа материала из разных источников является вывод о том, что понятия «структура системы» и «архитектура системы» достаточно часто являются тождественными. В то же время в понятии «архитектура системы» подчеркивается многосторонний, сложный характер объекта. Варианты определения понятия «архитектура системы», которые используются наиболее часто, можно увидеть в той же работе.

Отечественные стандарты и нормативные документы [61, 62, 74, 75] не содержат определения термина «архитектура системы», а также не применяют его. Однако эти документы определяют:

- элементы ИС: пользователи, технические средства, средства автоматизации;
- входящие в состав ИС структуры: функциональная, техническая, организационная, программная и информационная;
- виды обеспечения ИС: программное, информационное, техническое, организационное, методическое, математическое и др.;
- необходимость выделения структуры функциональных систем и подсистем информационной системы, а также создания набора функций с заданными параметрами и задач, решаемых ИС.

Стандарт Control Objectives for Information and related Technology (CobiT).

В CobiT не встречается понятие «архитектура системы» [65]. Однако в этом стандарте определено и используется такое понятие, как «ИТ-архитектура» — интегрированный фреймворк для развития существующих

и разработки новых ИТ, который способствует достижению организацией поставленных целей.

Кроме того, в данном стандарте определяется и используется понятие «ИТ-ресурсы», которое обозначает компоненты ИС.

В соответствии с фреймворком в CobiT выделяют такие ИТ-ресурсы, как:

- приложения — автоматизированные пользовательские системы, в состав которых входят процедуры обработки данных, запускаемые пользователями;
- информация — это данные (вводимые, выводимые, обрабатываемые, хранимые) в форме, необходимой организации;
- инфраструктура — это технология и объекты инфраструктуры (аппаратные комплексы, СУБД, операционные системы, сетевые и мультимедиа технологии и т. д, а также среда, где они существуют);
- сотрудники — это персонал, выполняющий планирование, организацию, реализацию, доставку, поддержку, оценку, контроль сервисов и систем. Персонал может быть разделен на внутренний, внешний, работающий на договорной основе.

Стандарт ISO 15704:2000, Industrial automation systems — Requirements for enterprise-reference architectures and methodologies [64].

В этом документе архитектура системы представлена как модель расположения и связей между собой элементов системы (концептуальных и физических объектов).

Стандарт ANSI/IEEE Std 1471-2000, Recommended Practice for Architectural Description of Software-Intensive Systems [55].

Согласно этому стандарту, архитектура является фундаментальной организацией системы, которая реализована в ее составляющих, связях

между ними, связях с окружением и принципах управления проектированием и развитием ИС.

Unified Modeling Language (UML) Specification [68].

Под архитектурой понимается организационная структура и поведение системы, которое с ней связано. Рекурсивно архитектуру можно представить таким образом:

- компоненты, которые взаимодействуют с помощью интерфейсов;
- связи между компонентами;
- условия, необходимые для взаимодействия структур системы.

Методология организации процессов разработки ПО Rational Unified Process [76] определяет архитектуру программной системы как структуру или организацию взаимодействий основных составляющих с помощью интерфейсов с более мелкими составляющими и интерфейсами.

Эта методология представляет архитектуру программной системы как множество, которое состоит из точек зрения, соответствующих главным элементам:

- Use-Cases View (варианты использования) — структура возможных вариантов использования системы;
- Logical View (логическое представление) — классификация элементов и подсистем, входящих в систему;
- Implementation View (представление реализации) — структура программной реализации;
- Process View (представление процессов) — объединение процессов и подсистем;
- Deployment View (представление развертывания) — соответствие элементов ПС техническим средствам.

Согласно The Zachman Institute for Framework Advancement [63], архитектура организации (или архитектура ИС) может быть реализована в

виде структурированной совокупности моделей («Framework for information systems architecture», «The Zachman Framework»), в соответствии с разным пониманием структуры организации лицами, участвующими в ее появлении и развитии (собственника, менеджеров, проектировщика, пользователей и др.). Разные представления об организации выделены в соответствии с разными сторонами предприятия — функции, организация, структура данных, сетевая инфраструктура, мотивация и т. д.

В [77] детально исследуются наиболее популярные подходы к определению архитектуры АИС (Meta Group, TOGAF Gartner, и др.). На основе исследования можно выделить следующие компоненты архитектуры:

Основные компоненты:

- бизнес-архитектура — совокупность всех бизнес-процессов предприятия и связей между ними;
- архитектура данных — совокупность всех данных, необходимых для осуществления бизнес-процессов предприятия;
- архитектура приложений — описание ПС, необходимых для осуществления бизнес-процессов предприятия и управления данными;
- технологическая архитектура — информация о аппаратном и программном обеспечении для разработки среды, в которой будут работать ПС.

Дополнительные компоненты:

- архитектура интеграции — инфраструктура, необходимая при интеграции ПС и данных;
- архитектура сервисов общего назначения — общие средства обеспечения ИБ, электронная почта и др.;

- архитектура управления и эксплуатации ИТ — структуры процессов, поддерживающих инфраструктуру и ПС;
- архитектура безопасности.

Для управления развитием и функционированием госучреждений и предприятий с помощью информационных технологий в США применяется общий подход к управлению процессом информатизации структур федеральной власти и госучреждений, который носит название Federal Enterprise Architecture (FEA) [70].

Этот подход основан на совокупности взаимосвязанных моделей, соответствующих всем аспектам организации, включая ее информационную систему: структуру и функции деятельности, структуру информации, структуру программных и аппаратных средств.

Согласно [78–80], на развитие архитектур крупномасштабных распределенных информационных систем повлияло в т. ч. внедрение проектов создания «электронного правительства». В определенный момент времени значительное число методов и моделей архитектур, которые были разработаны для этого проекта, стали применяться негосударственными организациями.

В развитии архитектурного подхода заметную роль сыграло создание FEA. В этой методологии реализованы федеративные принципы архитектуры — централизованное руководство и децентрализованное планирование в процессе разработки архитектур организаций и информационных систем. Отличительные черты FEA — это полноценный состав, принцип сегментного подхода, а также развитие обобщенной схемы и референсных моделей.

Компоненты FEA:

- стимулы (деловые, технические) и направление развития архитектуры (включая видение, цели, объекты);

- основные принципы, руководящие материалы, стандарты, глоссарий;
- архитектурные референсные модели;
- имеющаяся и целевая архитектуры;
- переходные процессы, среди которых планы перехода к целевой архитектуре, мониторинг и управление реализацией проектов;
- сегментный подход для отдельных сфер деятельности;
- хранилище для централизованного накопления всех видов архитектурных компонентов для последующего распределенного использования.

Принцип сегментного подхода позволяет сделать более быстрым практическое внедрение архитектуры, особенно в крупных многоотраслевых организациях, поскольку дает возможность в определенной мере автономно функционировать в пределах конкретного сегмента, гарантируя сохранение общих ресурсов и стандартов взаимодействия систем сегментов, а также уменьшение затрат.

К числу достоинств FEA следует отнести описанные в ней справочные модели (reference models):

- справочная модель эффективности (данные о затрачиваемых ресурсах, эффективность методов достижения целей, уровень достижения целей и др.);
- модель функций и сервисов деятельности (классификация задач, решаемых программными средствами и др.);
- модель прикладных ИТ-сервисов общего назначения (описание состава используемых прикладных ИС);
- модель базовых технических ИТ-сервисов и стандартов;
- модель описания данных и информации.

Справочные модели можно считать каталогами «идеальных» компонентов архитектуры, большинство из них не обладает спецификой инструментов ЭП и может применяться в любых проблемных областях. Справочную модель прикладных ИТ-сервисов общего назначения, например, можно использовать на этапе планирования разработок программных средств почти в любой организации.

На настоящий момент разработано и используется значительное число методологий в области создания архитектуры организации. В то же время заметная часть организаций при описании своей деятельности ограничивается следующими аспектами: цели, организационная структура, бизнес-процессы, ИС, ключевые показатели результативности, документы, компетенция и полномочия персонала.

Эти аспекты представлены в актуальных методологиях, описывающих архитектуру организации. Однако основная проблема, с которой сталкивается большое число организаций — это осуществление перехода от реальных бизнес-процессов к средствам автоматизации. Поэтому для многих организаций, которые занимаются описанием бизнес-процессов, актуальна задача перехода от норм и моделей бизнес-процессов к построению архитектуры ВК.

В данный момент в процессе передачи информации от бизнес-аналитиков к ИТ-специалистам существует определенный информационный пробел. Следует отметить, что при внедрении «тяжелых» систем с определенным функционалом (транзакции, структуры данных и др.) проблемы с взаимодействием можно преодолеть, передавая модели бизнес-процессов непосредственно персоналу, занимающемуся внедрением систем. В ситуациях, когда речь идет о системах-конструкторах или собственных разработках, такого процесса передачи будет недостаточно.

Если брать за основу бизнес-процессы, то необходимо выявить структуру данных, перечень возможных операций, состав отдельных мо-

дулей системы, интерфейс и т. д. При этом следует учитывать рекомендации перечисленных выше методологий архитектуры, в т. ч. The Open Group Architecture Framework (TOGAF).

Этот подход поможет решить актуальные проблемы, связанные с тем, что достаточно часто описание и развитие бизнес-процессов организации реализуют подразделения по совершенствованию бизнес-процессов или функциональные подразделения. Эти требования предъявляются ИТ-специалистами, то есть, требования, которые предъявляются к информационному сопровождению бизнес-процессов, должны быть четко сформулированы и представлены бизнес-специалистам и ИТ-специалистам.

Большая часть разработчиков ПО для определения требований к ИС применяет методологию UML, которая не является полностью совместимой с процессным подходом. Данную ситуацию усложняет наличие разных языков описаний: бизнес-специалисты для этого используют процессные модели, а разработчики применяют UML-модели.

Для устранения такого разрыва необходимо делать описание архитектуры организации более широким, при этом уделяя отдельное внимание архитектуре процессов и, принимая во внимание необходимость одинакового подхода к описанию архитектуры и для бизнес-аналитиков, и для ИТ-служб организации.

Ставя своей целью перейти к представлению ИТ-архитектуры от архитектуры бизнес-процессов, надо более четко представить предметную область. Представление архитектуры данных, фундаментом которой являются информация и документация бизнес-процессов, будет первым шагом. Далее создаются архитектура приложений и архитектура технологий.

В процессе работы над созданием архитектуры данных следует сначала выявить главные сущности, а после добавить к ним информацию, полученную из описания бизнес-процессов. Используя модель «сущность – связь» (Entity Relationship Model, ERM) [81] все данные можно структури-

ровать, определив при этом структуры таблиц БД. Это позволяет формализовать структуру данных организации на основании реальных бизнес-процессов, при этом вся информация будет представлена в форме, понятной для ИТ-персонала.

После этого от архитектуры бизнес-процессов и архитектуры данных можно перейти к разработке архитектуры приложений. Первоначально выявляются классы ИС, подлежащие автоматизации, выявляются отдельные модули, которые являются компонентами конкретных ИС.

В процессе проектирования архитектуры приложений модель процессов верхнего уровня (укрупненное представление бизнес-процессов организации) является основной. Компоненты этой модели — это основные типы ИС, которые представляются позже в виде моделей отдельных модулей ИС и др. Необходимо учитывать, что решить задачу создания архитектуры приложений можно, лишь принимая во внимание ее связь с бизнес-процессами.

Модели требований к информационной системе образуют самостоятельную предметную область, которая оказывает влияние на разрабатываемую архитектуру приложений. Можно говорить, что модели требований к ИС являются целевым функционалом ИТ-решения, выявленным с помощью ключевых характеристик, и обладают структурой, согласованной с существующими бизнес-процессами организациями и/или подразделениями. Создаваемая архитектура планируется с учетом выполнения этих требований и моделей бизнес-процессов, которые имеют место в организации. Кроме того, основываясь на связи архитектуры бизнес-процессов с архитектурой приложений, возможно создать «карту сопровождения процессов посредством ИС».

После создания архитектуры приложений разрабатывается архитектура технологий [7], включающая в себя составляющие ИТ-инфраструктуры:

серверное и сетевое оборудование, прочие устройства, используемые для работы приложений.

В работе, в соответствии с ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011 «Системная и программная инженерия. Описание архитектуры» [82], под архитектурой ВК понимается «комплекс основных понятий, специфики системы, реализованной в ее компонентах, их взаимосвязях и принципах ее проекта и развития». Согласно стандарту, «архитектура характеризуется: набором системных компонентов или элементов; каким образом устроены элементы системы или как они связаны между собой; принципами организации системы или проекта; правилами, которые влияют на развитие системы в течение жизненного цикла».

Под масштабируемостью архитектуры КД понимается возможность увеличения используемых технологических принципов и наращивания дополнительных ресурсов ВК без структурных изменений основных узлов комплекса.

1.2. Основные требования к архитектуре систем управления и контроля информационных систем

Задача управления информационными системами в настоящее время играет все более важную роль среди задач управления. Эту задачу можно представить в качестве упорядоченной схемы связей и процессов выбора направлений дальнейшего развития и методов управления в области ИКТ. Управление ИС соединяет структурно все информационные процессы, ресурсы и информацию, способствуя разработке стратегий и достижению поставленных целей.

Большинство организаций в настоящее время уже вложило значительные объемы денежных средств в информатизацию своей деятельности

и продолжает направлять ресурсы на развитие информационных технологий. Однако следует отметить распространенную зависимость от используемых ИС, часто являющихся «слабым звеном» в ситуациях, когда в них пытаются включить электронное взаимодействие отдельных ведомств, предоставление ВС в электронном виде, и прочие компоненты электронного документооборота.

Вопросы, связанные с созданием архитектуры, раньше обсуждались в области использования ИС, но в настоящий момент очевидно, что системный подход нужен не только при разработке ИТ-архитектуры, но и при построении архитектуры ВК в целом. Разработка архитектуры ВК, которая обеспечивает полное представление основных элементов ВС и связей между ними, требует особого внимания.

Если рассматривать идеальный случай, то архитектура ВК должна быть фундаментом для определения структуры деятельности (целей ВС, структуры, реализуемых процессов и др.); информации, используемой ВС (документов, данных и др.). Помимо этого, необходимым свойством архитектуры ВК является адаптивность для обеспечения быстрого и эффективного управления изменениями согласно запросам внешней среды.

Одна из распространенных проблем — это большое число информационных систем, с которыми взаимодействует ВС. Поначалу использование различных информационных систем, которые иногда дублируют функции друг друга, не является проблемой [83]. Но дублирование функций, неопределенности со временем и способами доставки электронных документов и данных является критическими. Кроме того, существует проблема «лоскутной» разработки ПО [84]. Обычно при автоматизации используется функциональный подход к управлению, что способствует возникновению независимо функционирующих систем, которые решают свои задачи.

При аудите внедрения ВС можно заметить, что в случае наличия большого числа функций чаще всего нет сквозной автоматизации бизнес-процесса. Примером подобной ситуации может служить следующий: документ распечатывается из одной ИС и передается его на бумажном носителе в другое подразделение, где он заново переводится в цифровой формат и после этого регистрируется в ИС, что является неэффективным решением.

Следующая важная проблема — нехватка качественного документирования применяемых решений в сфере ИТ. Осуществленные разработчиками или внедренные готовые решения должны быть сопровождаемы документацией на каждом этапе создания и эксплуатации. Иначе возникнет «черный ящик», которым никто не может управлять. Существует значительное число примеров того, что только из-за некачественного документирования ИС ее использование прекращалось, и начиналась разработка или внедрение новых решений.

Следует выделить главную проблему автоматизации бизнес-процессов в ВС — разрыв между бизнес-процессами, которые реально существуют и средствами их автоматизации. Одна из наиболее частых проблем — это недовольство пользователей ИС, которое может быть связано с трудностями использования, недостатками в работе ВС, сложностями при корректировке. Анализируя эти проблемы, можно отметить, что выполняемые в реальности бизнес-процессы и применяемая система часто несогласованы. И такой разрыв будет лишь увеличиваться. Следует начинать согласование требований бизнес-процессов и основных пользователей с функционалом ИС еще при ее выборе и продолжать непрерывно до окончания ее применения.

Для обеспечения успешной деятельности ВС необходимо четкое понимание того, можно ли считать управление информацией:

- успешным для достижения поставленных предприятием целей;

- гибким для обеспечения адаптации и обучения к текущим и потенциальным изменениям;

- помогающим избежать рисков, которым подвергается предприятие;

- умеющим видеть возможности и использовать их.

Система управления ВС должна обладать следующими качествами:

- центр приложения основных действий по управлению ВС должен сохраняться таким образом, чтобы цели, поставленные организацией, совпадали с целями ИТ-инфраструктуры в течение всего времени работы;

- координировать процесс для определения масштаба и диапазона области действия;

- сохранять уровень, рекомендованный лучшими практиками управления ИС, а также информационными технологиями, отвечать актуальным стандартам;

- использовать общепринятый язык, а также термины, ясные для заинтересованных лиц;

- соблюдать нормативные требования, заданные корпоративными стандартами и ИТ-контролем.

Что касается информации, то она должна соответствовать бизнес-требованиям, которые предъявляются к информации. Чаще всего используют следующие требования:

- результативность — информация имеет отношение к конкретным бизнес-процессам, представлена вовремя в корректной форме;

- эффективность — информация предоставляется с соблюдением требования оптимального использования ресурсов;

- конфиденциальность — защита информации;

- целостность определяют полнота, достоверность и корректность информации согласно конкретным задачам бизнеса;

- доступность информации для бизнес-процессов и административных процессов. Здесь же следует указать защиту ресурсов и возможностей, которые они предоставляют;

- согласованность — соответствие законодательным и нормативным актам, другим документам, регламентирующим деятельность предприятия, а также внутренней политике предприятия;

- надежность — предоставление руководству предприятия информации, необходимой для управления, а также реализации самого процесса управления.

Разработка стратегии развития архитектуры ВК должна быть основана на актуальных и достоверных данных о состоянии ИТ-инфраструктуры и бизнес-архитектуры, а также стратегии развития [85]. При создании стратегии развития ВС необходимо принимать во внимание актуальные для данной ситуации ограничения: временные, технические, материальные и др., а также результаты анализа уровня корпоративной культуры. Большую часть данной информации можно получить при проведении постоянного мониторинга архитектуры АП.

Разработку плана стратегического развития архитектуры ВС необходимо проводить согласованно со стратегией развития ИТ-инфраструктуры ВК. Разрабатываемая стратегия должна обеспечивать уровень сервисов, достаточный для введения новых бизнес-процессов и функционирования приложений, которые их сопровождают. Необходимо учитывать, насколько реальной является возможность интегрировать инновации в сфере ИТ: искусственный интеллект, облачные и туманные технологии и т. д., использование которых существенно повлияет на развитие ИТ-инфраструктуры [6, 78–80].

Следовательно, разработку стратегии развития архитектуры ВС нельзя рассматривать отдельно от управления приложениями и данными в актуальном состоянии архитектуры, а также от специфики эксплуатации ИТ-

инфраструктуры ВК. При создании стратегии обязательным является применение универсальных методов и инструментов, которые позволяют решить данную задачу. В первую очередь, в числе этих методов следует указать архитектурные фреймворки (TOGAF, фреймворк Захмана) и методологии проектирования ИС (в т. ч. MSF — методология проектирования [86], разработки и внедрения ПО; RUP — методология создания ИС и ПО). Основой этих инструментов является сервисный процессный подход, они признаны лучшими практиками сопровождения ИТ-инфраструктуры предприятия. Широко распространенными и применяемыми в настоящий момент являются руководства библиотеки ITIL, где описана совокупность процессов, которые используются для реализации подхода ITSM (Information Technology Service Management) [87], созданного в соответствии с потребностями организации с использованием оптимального сочетания трудовых ресурсов, информационных технологий и др.

Наиболее часто используемая на практике открытая модель — ITIL/ITSM. Помимо нее часто применяют методологию Microsoft Operations Framework (MOF) — это библиотека документов, имеющая своей основой идеологию ITIL [88]. Входящие в состав этой библиотеки «рекомендованные практики» — это обобщение практического опыта сопровождения ИТ-инфраструктуры компанией Microsoft с учетом анализа реализованных проектов и особенностей использования ИТ-решений компании в процессе разработки технологической архитектуры. Кроме того, для решения данной задачи значимыми являются методологии и инструменты разработки бизнес-архитектуры, т. к. именно бизнес-архитектура служит основой для создания универсальных требований, предъявляемых к архитектуре ИС.

В процессе разработки стратегического плана развития архитектуры ВС следует принимать во внимание и текущие информационные запросы, и потенциальные направления развития в области ИКТ. Кроме того, при

осуществлении аудита и мониторинга архитектуры можно выявить недостаточно сильные стороны технологической архитектуры, негативно влияющие на развитие архитектуры ВК. Эти потенциальные риски необходимо принимать во внимание при создании стратегии построения и развития архитектуры ВК.

Завершая анализ проблем управления ИТ-инфраструктурой ВК, основой которого является архитектурная модель управления, можно прийти к следующему выводу: разработка такой модели делает возможным поставить в соответствие подходящую ИТ-инфраструктуру постоянно меняющимся запросам цифровой среды. Взаимодействие ее ресурсов с другими компонентами модели гарантирует поддержку всех процессов управления. Архитектурная модель, основой которой являются современные методики создания ИС, информационные технологии и средства обмена данными, в настоящий момент представляет собой наиболее важное средство для синхронизации задач цифрового общества и архитектуры ИС.

1.3. Анализ защищенных вычислительных архитектур

Подходы к созданию, использованию и взаимодействию защищенных информационных ресурсов имеют следующую специфику [89, 90]:

- значительное количество отдельных информационных ресурсов разного рода, которые представляют собой массивы информации (структурированные и неструктурированные);
- несогласованность периодов времени, в которые актуализируются имеющиеся информационные ресурсы.

В общий контур максимальной конфигурации включены 3 отдельные контура (см. рис. 1.2):

- контур открытых защищенных информационных ресурсов (О-контур);

- контур конфиденциальных защищенных информационных ресурсов (К-контур);
- контур закрытых защищенных информационных ресурсов (З-контур или С-контур).

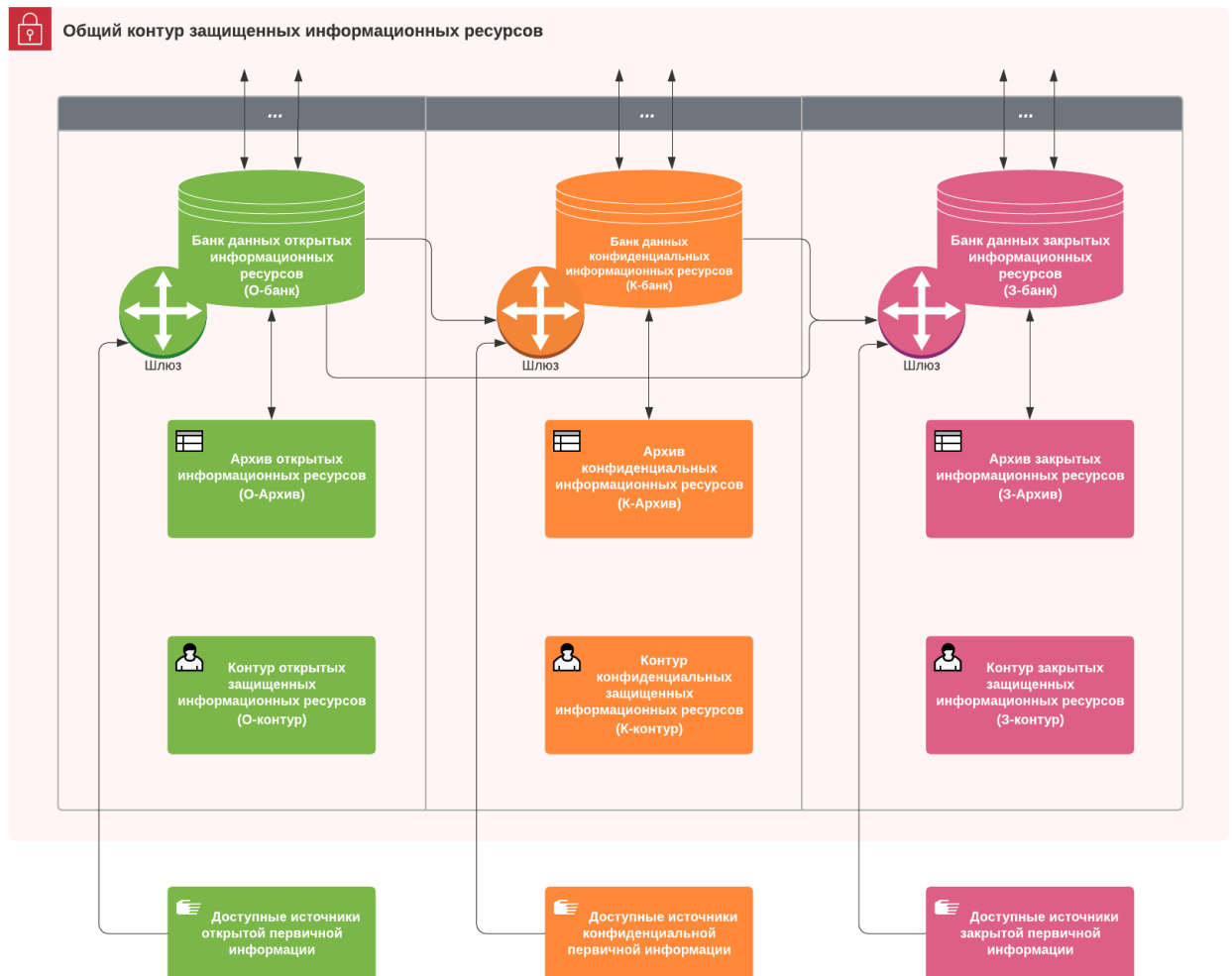


Рисунок 1.2 — Обобщенная модель создания и взаимодействия защищенных информационных ресурсов

Также, в случае необходимости можно использовать общий контур сокращенного состава, который включает не более двух автономных контуров из тех, что представлены выше.

Каждый из контуров включает в себя:

- банк данных (О-банк, К-банк, З-банк) — упорядоченная совокупность данных, свод всей информации, необходимой для информационного взаимодействия и коллективного использования пользователями. Создание банка данных происходит с использованием разных систем хранения и передачи информации;

- архив информации (О-архив, К-архив, З-архив);

- однонаправленные шлюзы, которые обеспечивают однонаправленную передачу информации (например, информация передается из источников первичной открытой информации в О-контур или из О-контура в К-контур; из К-контура в З-контур).

Информационное взаимодействие общих контуров защищенных информационных ресурсов происходит через описанные выше банки данных (при этом учитываются права на доступ, используются согласованные регламенты):

- защищенные информационные ресурсы отдельного Участника/Участников;

- защищенные информационные ресурсы отдельного Участника с прочими информационными ресурсами во время взаимодействия внутри информационной инфраструктуры Участника;

- защищенные информационные ресурсы отдельного Участника с информационными ресурсами прочих структур.

В действительности создание общего контура защищенных информационных ресурсов необходимо осуществлять, взяв за основу единую ИС в защищенном исполнении, соответствующую требованиям, предъявляемым к проектированию защищенных архитектур ВК. Использование при этом типового интерфейса/интерфейсов информационного взаимодействия и типовых регламентов является крайне важным.

Использование единых подходов и обеспечение стандартизации системотехнических решений необходимо для потенциального Участника в процессе создания защищенной вычислительной архитектуры [91–93]. Эти требования дают возможность создать цельное видение системы, ее архитектуры; создать язык, чтобы определить и описать ее; выявить возможность согласованности и результативного взаимодействия составляющих/подсистем внутри единой системы.

Что касается непосредственной реализации, то единая техническая политика должна включать в себя стандарты, обязательные для исполнителей работ и всех структурных подразделений Участника. Целью этой политики должны быть согласованность при выборе решений и предотвращение несогласованных действий по улучшению составляющих будущей защищенной архитектуры.

Актуальная информационная структура, включающая в себя информационные, телекоммуникационные и вычислительные средства, является разнородной программно-аппаратной средой, в которой используются различные программные и аппаратные ресурсы [94, 95]. Естественно, что частой проблемой является вопрос совместимости в данной среде (взаимодействие систем, защищенность и масштабируемость систем, переносимость приложений от одной платформы к другой).

Международные стандарты определяют среду, обладающую этими качествами, как среду открытой системы, описывающую функциональную специфику ИС, необходимую для того, чтобы обеспечить совместимость и переносимость приложений в разнородных сетях, которые связывают программные и аппаратные платформы разного типа.

Применение согласованного профиля стандартов ко всем программно-аппаратным комплексам обеспечивает открытость среды. Поскольку существует значительное число стандартов в сфере ИТ и, в связи с возникновением новых технологий, оно увеличивается, следует отметить, что обеспе-

чение открытости является достаточно непростой задачей. Кроме того, необходимо учитывать специфику каждого из Участников будущей защищенной вычислительной архитектуры.

В процессе работы над обеспечением открытости ИС одним из этапов является разработка методики формирования профилей — обязательной части каждой информационной инфраструктуры. Профилем среды открытой системы является выбранная определенным образом совокупность базовых стандартов и указываемых в них опций, с помощью которых для отдельных областей приложений или классов определяют на языке требований к функционалу, интерфейсов, форматов данных, протоколов особенности функционирования приложений в процессе их взаимодействия.

В последнее время опыт проектирования профилей накапливался быстрыми темпами, появилось представление о содержании профилей, их процессах жизненного цикла, что оказало огромное положительное влияние на содержание отечественных стандартов, принимая во внимание имеющийся опыт и материалы в области разработки международных стандартов. Преимуществами использования профилей открытой системы можно назвать:

- отсутствие зависимости от поставщика;
- обеспечение функциональной совместимости и интеграции;
- обеспечение связи между основной деятельностью предприятия и используемыми ИТ;
- предоставление всесторонней и наглядной информации о результатах деятельности предприятия;
- возможность сопровождения и поддержки любых технологических образцов;
- обеспечение создание структуры инвестиций, наиболее эффективной при вложении в ИТ.

Рекомендации по стандартизации, которые разработаны согласно требованиям IEEE Std 1003.23-98 «Руководство по проектированию профилей среды открытой системы организации-пользователя» [96], являются наиболее подходящими для применения в этом случае.

С учетом требований стандарта IEEE 1003.23-98 разработан и введен в действие российский нормативный документ Р 50.1.041-2002 «Рекомендации по стандартизации. Информационные технологии. Руководство по проектированию профилей среды открытой системы организации-пользователя» [97]. Эти рекомендации созданы для проектировщиков, пользователей, заказчиков, специалистов по внедрению и использованию сложных ИС при разработке профилей среды открытой системы организации, устанавливающих требования организаций к телекоммуникациям и обработке информации.

На выбор подхода к проектированию профилей среды открытых систем может влиять целый ряд факторов (в т. ч. функции, задачи, процессы, которые характеризуют данную организацию). Рекомендации, представленные в этом документе, не включают в себя полные сведения для разработки профиля; они регламентируют методологию выбора стандартов и порядок проектирования профилей для организации-пользователя. В процессе практического использования рекомендации необходимо дополнить технологиями создания профилей среды открытых систем, которые учитывают специфику отдельной организации.

Расширением отдельных этапов формулирования требований проектирования профиля с учетом связи между стратегией основной сферы деятельности конкретной организации-пользователя, запросами к функциональности ЕИС и процессом проектирования профиля является общая модель создания профиля среды открытых систем организации.

1.4. Системные факторы влияния на процесс контроля доступа

Для проведения эффективной политики КД необходимо выделить множество всех значимых угроз, воздействий и влияний. Такие факторы, которые могут оказать влияние на КД, назовем *факторами влияния*.

Факторы влияния условно можно разделить на три вида: 1) факторы влияния, непосредственно оказывающие негативное воздействие на процесс КД, — это угрозы и атаки, то есть реализованные угрозы; 2) факторы влияния, оказывающие опосредованное негативное воздействие на процесс КД; 3) факторы влияния, оказывающие позитивное воздействие на процесс КД.

Сформируем перечень возможных воздействий со стороны каждого компонента всех участвующих в процессе КД сущностей и их взаимосвязи.

Субъекты доступа являются источниками наиболее опасных и наиболее негативных массовых воздействий на процесс КД; в частности, они являются источниками злоумышленных действий — считается, что не менее 70% атак реализуются с участием персонала объекта защиты. Имеется много различных методик и перечней возможных угроз. Наиболее важным и представительным из подобных перечней является список угроз, связанных с защитой персональных данных, который приведен на сайте ФСТЭК [91, 92]. И хотя он привязан к защите персональных данных, этот перечень почти целиком может использоваться и при анализе угроз по требованиям, выходящим за рамки защиты персональных данных [98]. Более того, это перечень включает также угрозы, исходящие от других компонентов [99].

Кроме угроз, со стороны субъектов могут быть и следующие воздействия на процесс КД:

1. Безответственное и даже негативное отношение субъекта доступа к процедурам, связанным с обеспечением ИБ.
2. Настойчивые попытки использования субъектами доступа на рабочем месте несанкционированных программно-аппаратных средств, обосновывая это необходимостью для качественного выполнения возложенных обязанностей.
3. Рекомендации и предложения со стороны субъектов доступа по совершенствованию процесса КД.
4. Спонсорская и иная поддержка и помощь со стороны субъектов доступа системы обработки данных на объекте защиты, включая систему обеспечения ИБ и подсистему КД.

Следующим компонентом являются объекты доступа, то есть информационные системы и программно-аппаратные средства, представляющие интерес для субъектов доступа разного типа, включая процессы обработки данных. Они также могут являться источниками негативных воздействий, в частности угроз ИБ. Возможный их перечень применительно к персональным данным приведен в приложении. Среди других типов воздействий со стороны объектов доступа отметим следующие:

1. Достаточно велико время обработки данных на объекте допуска.
2. Неспособность правильно выполнять объектом доступа свои функциональные задачи: отказ системы (устройства), сбой, выход из строя, дефекты архитектуры или программной (аппаратной) реализации системы (устройства).
3. Высокий уровень адаптируемости (живучести) объекта доступа (программно-информационной системы или устройства), не отраженный в типовой документации.

4. Широкий спектр программных средств, с которыми объект доступа способен активно взаимодействовать.

Среди факторов влияния, связанных с системой обработки данных, кроме угроз, которые приведены в приложении, укажем также на следующие факторы влияния.

1. Проблемы взаимодействия различных информационных систем или аппаратных средств, связанные с недостаточной и даже низкой совместимостью их.

2. Большой и разнообразный набор программных средств, часто взаимозаменяемых, используемых в системе обработки данных.

3. Использование хорошо зарекомендовавших себя программно-аппаратных средств в системе обработки данных.

4. Жесткая регламентация и минимизация взаимодействия системы обработки данных с внешними объектами и системами, особенно с мало-знакомыми.

Система обеспечения информационной безопасности наряду с угрозами может находиться также под воздействием следующих факторов:

1. Текучесть кадров, вызванная наличием на рынке более привлекательных возможностей, прежде всего, по оплате труда.

2. Недостаточный объем средств для совершенствования и обновления средств защиты с учетом роста возможностей совершения злоумышленных действий.

3. Наличие документов аттестации системы обеспечения ИБ по требованиям информационной безопасности (в частности, по защите персональных данных).

4. Налаженное взаимодействие с службами информационной безопасности других организаций, имеющих эффективные системы обеспечения ИБ либо высокий уровень компетентности в сфере ИБ.

Внешнее окружение является одним из главных источников угроз наряду с субъектами доступа. Большой состав подобных угроз приведен в приложении. В качестве факторов косвенного влияния на процесс КД выделим также следующие факторы.

1. Относительно высокий уровень криминогенности в зоне расположения объекта защиты.
2. Большой объем внешнего трафика объекта защиты с внешним миром.
3. Наличие контактов и совместных обсуждений с дружественными и компетентными интернет-партнерами.
4. Понимание важности проблемы обеспечения ИБ на объекте защиты и поддержка со стороны местных органов власти, силовых органов.

Объекту защиты подчинены все службы обеспечения безопасности, то есть руководство объекта защиты обеспечивает функционирование и контролирует результаты работы систем безопасности. Объект защиты, несмотря на то, что все процессы обеспечения ИБ нацелены на поддержание наиболее благоприятных условий его функционирования, также является потенциальным источником угроз. Кроме того, выделим следующие факторы влияния, связанные с объектом защиты [100].

1. Недостаточный уровень информационного взаимодействия объекта защиты с системой обработки данных и с системой обеспечения ИБ.
2. Наличие ряда слабостей и уязвимостей в политике информационной безопасности, принятых под давлением представителей объекта защиты под предлогом обеспечения более благоприятных условий для его функционирования.
3. Наличие тесного взаимодействия систем обеспечения ИБ со службой физической защиты объекта.
4. Обеспечение требуемого уровня финансовой поддержки системы ИБ со стороны объекта защиты.

Система КД также потенциально является источником нетипового воздействия на процесс КД.

1. Недостаточный уровень использования технических средств контроля доступа, включая контроль перемещения по территории объекта защиты.
2. Устаревание средств контроля доступа с течением времени и отсутствие их адекватного обновления.
3. Отсутствие должного контроля работы персонала системы КД.
4. Полное взаимодействие системы КД с другими службами организации.

Таким образом, основу перечня факторов влияния составляет перечень всех актуальных угроз. Отметим, что приведенный перечень факторов влияния может уточняться и расширяться по мере анализа конкретной организации, систем обработки данных и обеспечения ВС. Полученный перечень позволяет повысить эффективность системы КД на основе более адекватного управления процессами КД.

1.5. Современные перспективы развития технологий контроля доступа

Программные средства Security information and event management (SIEM) — управление событиями информационной безопасности стали доступными для приобретения примерно в 1997 г. [32, 36, 101]. Их функционал позволял уменьшить количество «ложных срабатываний» систем обнаружения сетевых вторжений (IDS — intrusion detection system), которые угрожали системам IDS.

Как и множество других продуктов, SIEM-системы были результатом эволюции и слияния систем Security Event Management (SEM) и Security

Information Management (SIM) [24]. Работа программных продуктов SEM происходит практически в реальном времени, осуществляя мониторинг, сбор и корреляцию событий, формирование предупреждающей информации. Системы SIM исследуют собранную информацию с точки зрения статистики, отклонений от «нормы» и др. О SIEM-системах идет речь, в случае, когда возможности SEM и SIM объединяются в одном программном продукте. Учитывая это, можно расшифровать и перевести аббревиатуру SIEM, как «система сбора и корреляции событий». Следует учитывать, что как самостоятельное решение (standalone) SIEM-системы нельзя рассматривать, они не могут предотвратить ситуации нарушения информационной безопасности. Суть SIEM-систем сформулирована в их названии — это анализ информации, которая поступает из разных источников (IDS, DLP, межсетевые экраны, антивирусы и др.), и, после этого, определение особенностей отклонений от норм по критериям, заданным заранее. Однако достоинств у SIEM-систем достаточно. Главной задачей SIEM-систем является сбор заданной информации разного рода и обнаружение в ней предупреждений о нарушении информационной безопасности и инцидентов высокого уровня [23, 29, 33, 35, 101]. Обычно для достижения этих целей используются методы нормализации, фильтрации, агрегации и корреляции событий. Но при увеличении сложности проводимых атак (к примеру, целевые атаки), защищаемых объектов (в т. ч. киберфизических систем) и применяемых технологий, используемые методы и подходы иногда не могут обеспечить необходимую степень защищенности. На эту тенденцию негативно влияет также возрастающий объем данных, обрабатывать которые все более затруднительно. В SIEM-средствах защиты главная роль отводится процессу корреляции данных, который направлен, главным образом, на выявление причинно-следственных связей между событиями, поступающими на обработку. Процесс корреляции данных дает возможность обнаружить вредоносные и аномальные активности, определить источник

и цели атаки, а также выявить многошаговые атаки [102, 103]. В настоящее время существует значительное количество методов и подходов, которые применяются в процессе корреляции, однако наиболее широко используемым является правило-ориентированный метод [104, 105].

Согласно [28, 106], программный продукт Symantec Security Information Manager применяет для выявления угроз безопасности подход, в рамках которого происходит классификация проблем и угроз безопасности и принимается во внимание способ атаки, целевые ресурсы и уровень воздействия инцидента.

Модуль анализа данных продукта Symantec SIM использует правила, в основе которых лежат шаблоны. Правило может включать в себя несколько более простых правил, применяемых в стандартных ситуациях. В итоге процедура обслуживания и разработки правил, которые способны охватить несколько условий, становится заметно более простой [106]. Такой подход дает возможность достичь анализа, осуществляемого с высокой скоростью — до 30000 событий за 1 секунду.

В реальном времени производится сбор и анализ событий, который выполняется с учетом заданных правил путем соотнесения потока нормализованных событий. При выявлении события/группы событий, соответствующих правилу корреляции, формируется заключение, которое или инициирует появление нового инцидента или автоматически привязано к существующему инциденту. Заключение появляются вместе с небольшими описаниями, которые дают возможность понять ситуацию в системе без подробного чтения логов. К предлагаемому разработчиком (Symantec) описанию конкретных действий по ликвидации угрозы можно добавить предписания и рекомендации, которые приняты в конкретной компании.

Подводя итоги, можно заключить, что программный продукт Symantec SIM также имеет своей основой применение правил корреляции, которые, несмотря на то что именуются «интеллектуальными», не обеспе-

чивают выявления новых атак, неизвестных ранее. Кроме того, это решение опять же ориентировано на обработку событий, уже произошедших. Этот продукт можно теоретически считать лучше адаптированным к системам ЦП и ВС в силу того, что компоненты, собирающие события с наблюдаемых объектов (коллекторы) делятся на два типа: те, что работают на оборудовании Symantec SIM и те, что работают на прочих компьютерах.

Программный продукт MaxPatrol (разработчик — Positive Technologies) обладает следующей спецификой:

1) симптоматика:

- представление событий в форме, доступной пользователю;
- присвоение тегов событиям;
- дополнение риск-метриками (в т. ч. суммарной риск-метрикой);
- разбиение событий на классы;

2) особенности корреляции:

- выполняется внутри серии/последовательности событий;
- корреляция осуществляется на основе правил;
- историческая корреляция;
- использование функций;
- применение блоков симптоматики;
- возможность добавления пользовательских правил.

3) сетевой сенсор:

- выявление угроз при исследовании трафика (вредоносное ПО, уязвимости программных средств и попытки их использования);
- исследование протоколов (нестандартные порты, команды, туннели, сведения об авторизации, обертки);
- перехват файлов во время передачи (scap, md5/sha);
- flow-заголовки трафика для формирования связей;

- мониторинг Secure Sockets Layer (SSL) сертификатов;
- разработка правил политики межзонного взаимодействия;

4) аналитика:

- агрегаты веса по объектам (IP, username, Host, uid, port и т. д.);
- источники данных (FQDN, MD5/SHA, IP, URL, email);
- построение взаимозависимостей между отдельными объектами;
- историческая корреляция;
- создание взаимосвязей между процессом и пользователем, пользователем и машиной, пользователем и логинами и т. д.;
- выявление угроз с помощью накопленной информации;
- выявление аномалий («CRC этого процесса ранее не встречалось», «такой ситуации еще не возникало» и т. д.);
- формирование отчетной документации.

Главный акцент в процессе поиска инцидентов приходится на метод корреляции на основе заданных правил. Кроме того, решение дает возможность дополнять уже существующие правила своими. Также интересной для рассмотрения является историческая корреляция, которая, видимо, позволяет реализовывать изучение инцидентов и создание векторов атак для пополнения базы знаний. Еще следует отметить, что в рассмотренных программных продуктах уделяется внимание различным весовым коэффициентам и метрикам, что дает возможность предполагать наличие расширенной функциональности корреляции. Формирование взаимосвязей ориентировано, главным образом, на сущность пользователя: процесс — пользователь, пользователь — машина, пользователь — логины.

Несмотря на значительные возможности, которыми обладают представленные SIEM-продукты, их масштабируемость и гибкость, они не мо-

гут гарантировать полностью обеспечение безопасности ЦП и ВС ввиду следующих особенностей:

- 1) ориентация на работу с событиями, которые описаны правилами и зафиксированы в журналах;
- 2) применение в качестве основного инструмента метода корреляции на основе заданных правил. Это решение достаточно субъективно и делает необходимым постоянное дополнение перечня правил, что не всегда осуществимо в случае крупномасштабных систем;
- 3) нет ориентированности на специфику поведения пользователей.

Актуальные тенденции в области безопасности предполагают концентрацию внимания на человеке и его поведении, поскольку именно человек — главный источник нарушений, угроз, инцидентов и рисков. На настоящий момент не существует унифицированного наименования для решений, позволяющих анализировать поведение пользователей. Например, компания Gartner использует название User and Entity Behavior Analytics (UEBA). Похожие названия носят продукты компаний Gurukul, Forcepoint, Securonix и Fortscale. Разработчики из Splunk, DNIF, HP ArcSight (HPE/MicroFocus), IBM и персонал IDC применяют название User Behavior Analytics (UBA) для своих программных продуктов [22, 47].

Прочие компании, работающие на этом рынке, делают упор не только на анализируемых объектах, сущностях (Entity) или пользователях (User), но также на целях анализа. Например, Microsoft и Exabeam пользуются терминами Advanced Threat Analytics или Advanced Analytics. Сотрудники компании Forrester используют название Security User Behavior Analytics (SUBA) для класса решений для поведенческого анализа, делая при этом упор на обеспечение безопасности. Иногда компании используют свои названия для продуктов, зачастую достаточно образные: Risk Fabric (компания Bay Dynamics), Enterprise Immune System (компания Darktrace) [107].

Что касается российских решений в этой области, то можно отметить наличие продуктов класса UEBA/UBA/SUBA, которые часто характеризуются смешанным подходом: система UBA (входит в DLP) от Zecurion; ProfileCenter от SearchInform; Prediction класса UEBA, предлагаемый компанией InfoWatch.

Общепринятые базовые функции первых UBA-решений:

- 1) мониторинг и анализ поведения человека;
- 2) детектирование отклонений в поведении и расстановка их приоритетов, обеспечивающая своевременную реакцию на самые значительные и широко распространенные изменения.

С течением времени подход к базовому пониманию функционала UBA-продуктов изменился в плане добавления новых функций. Ниже представлены основные из них.

- 1) Способность накапливать данные в ходе работы или применять данные, накопленные раньше;
- 2) Применяя методы, определенные заранее, выявлять характерное постоянное поведение исследуемых объектов (это касается и людей и программных/аппаратных средств). Чтобы провести этот анализ, необходимы источники различных данных в течение значительного периода для того чтобы была возможность выявить характерное для человека или сущности поведение и его рамки, выход за которые принимается за отклонение от нормального состояния. Подходы в UBA-решениях могут быть различными в соответствии с применяемыми методами анализа.
- 3) Способность выявлять аномальное или нетипичное поведение объекта. Существует точка зрения, что детектирование UBA помогает выявить значительные нарушения, плохо определяемые с помощью традиционных средств систем безопасности [21, 47].

4) Полученные результаты ранжируются. Достаточно часто системы информационной безопасности обладают слишком высокой чувствительностью ко всем изменениям, что порождает значительное число предупреждений, поэтому службы безопасности не могут разобрать и детально расследовать их все. UBA-решения могут консолидировать все предупреждения, оценить риски и передавать пользователю информацию только о наиболее значимых отклонениях. Это приводит к увеличению результативности работы персонала ИБ, поскольку число ложных срабатываний уменьшается (рис. 1.3).

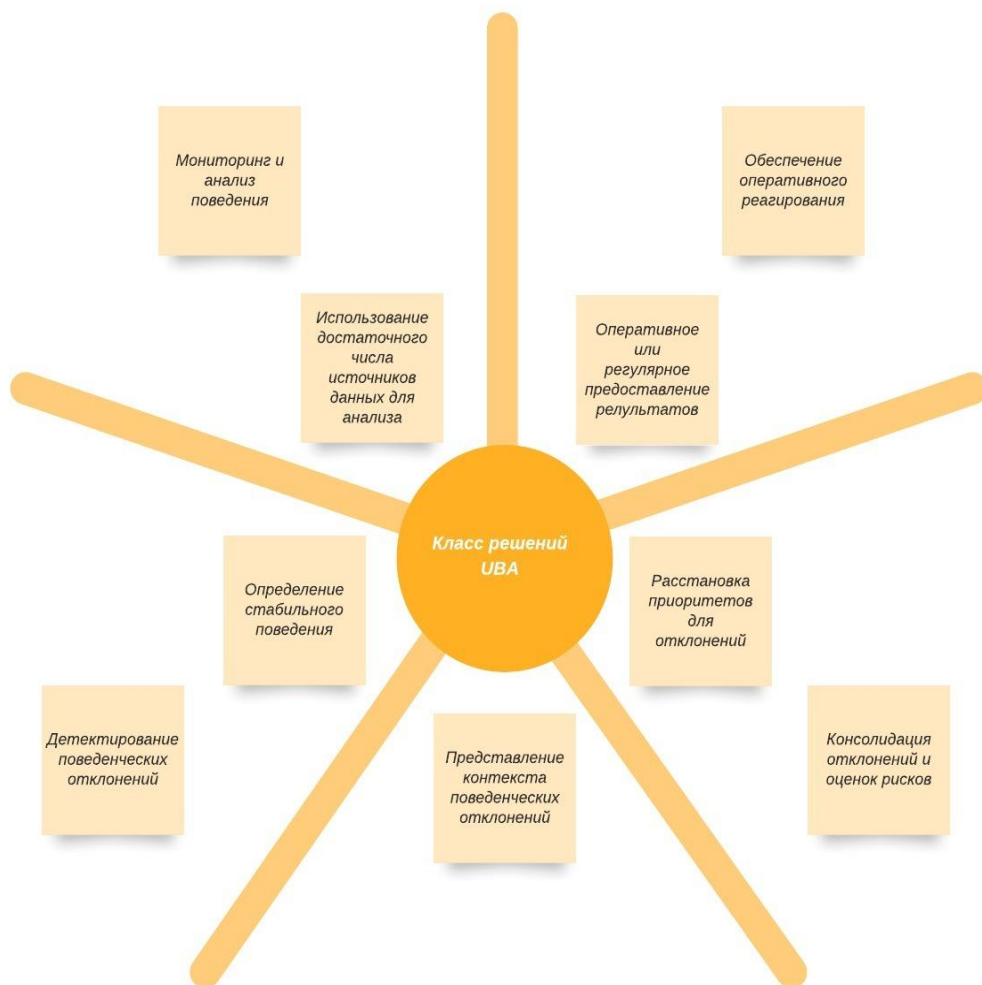


Рисунок 1.3 — Основные функции решений класса UBA

Кроме того, иногда в источниках [15, 20, 48] указываются следующие функции, наличие которых желательно в актуальных решениях UBA:

- применение встроенных моделей поведения объекта;
- уведомление пользователя о выявлении отклонений в поведении;
- возможность гибкого поиска в ходе расследований;
- создание отчетов о результатах анализа;
- применение временной шкалы с целью исследования полученных результатов в течение некоторого времени;
- ретроспективный анализ данных, накопленных ранее, с целью выявления отклонений в поведении в предыдущие периоды.

Более подробную информацию о решениях UBA можно увидеть в сравнительной таблице UBA на сайте ROI4CIO [108].

Вычисления в тех масштабах, в которых они осуществляются сейчас, становятся выполнимыми в связи с тем, что создаются все более сложные устройства и программная инфраструктура, сопровождающие пользователя в окружающем мире. Эти системы должны обладать свойством независимой адаптации к переменам в контексте и поведении пользователя, безотказно функционируя при его минимальном вмешательстве. Значит, эти системы должны обладать возможностью обучения по действиям пользователя, а также данным, которые вводятся. При этом необходимое условие доступности для пользователя приводит к требованиям предсказуемости, способности объяснения своих действий и предоставления возможности пользователям распознавать и корректировать знания, полученные системой. Все это приводит нас к методам, использующим логические правила при рассуждениях и представлении знаний. При этом необходимой будет определенная статическая предварительная обработка информации с датчиков, но несмотря на это, такой подход имеет заметные преимущества при принятии базового логического формализма — простого и модульного

исполнения с использованием принципиальных представлений времени и пространства [109] и структур политик [110].

Следует отметить, что исследование норм поведения пользователя с применением индуктивных рассуждений приводит к появлению некоторых проблем. Необходима постепенность обучения. Т.к. примеры поведения объектов добавляются непрерывно, то система должна предусматривать периодическое обновление правил и полученных знаний. Кроме того, необходим учет временных аспектов для изучения устойчивости и изменений с течением времени, а также исключения из правил, изученных ранее. Поэтому система должна быть приспособлена к немонотонным рассуждениям [39]. Она должна использовать частичные данные, соблюдая тщательный контроль самого процесса рассуждения для удовлетворения требованиям предвзятости поиска (в т. ч. минимизации изменений, которые вносятся в исходную теорию) и пользовательского языка.

Анализ экспертных мнений [111, 112], выявил направления с наибольшим потенциалом роста, которые будут способствовать технологическим решениям КД, в частности наиболее быстро развивающейся концепции SIEM:

- автоматизация ответа на киберинциденты;
- развитие экспертизы в сфере управления системой;
- добавление нового функционала SIEM за счет методов мониторинга поведения объектов UBA;
- применение облачных вычислений в качестве источника информации и предоставление информации в рамках модели «as a service»;
- анализ ситуации на конечных узлах и анализа трафика.

В течение последних 15 лет под SIEM понимают инструмент для сбора информации с различных систем и средств корреляции, при этом исследование полученных массивов данных подразумевает только корреляционный анализ.

Для того чтобы повысить уровень мониторинга событий безопасности необходимо выявить: правила, по которым будет происходить нормализация; пакеты с правилами выявления угроз; методы настройки источников данных; методику активации источников; содержание правил детектирования; рекомендации для ситуаций срабатывания правил. В настоящий момент доля покрытия SIEM-технологии равна 50–60%, что же касается качества реализации, то оно составляет 3 балла (среднее) [111].

Другим трендом потенциального развития SIEM-решений является автоматизация ответа на инциденты. Исходя из результатов опроса, проведенного Positive Technologies, одна четвертая часть всех опрошенных специалистов в сфере ИБ работает в SIEM-системе каждый день 2–4 часа. Самыми трудозатратными задачами были названы: анализ инцидентов (назвали 52% участников опроса) и обработка ложных срабатываний — внесение изменений в правила корреляции (58%). Настройка источников данных, а также мониторинг их работоспособности занимают значительное количество времени по мнению 30% специалистов. Такая ситуация способствует эволюции SIEM-решений в сторону программных решений Security orchestration and automated response (SOAR), решающих вопросы автоматического реагирования и оркестрации систем безопасности. Для этой технологии покрытие примерно равно 60–70%, уровень качества реализации, по мнению экспертов, равен 3.

В качестве третьего направления для развития SIEM следует указать взаимопроникновение технологий анализа логов (SIEM-решения), анализа сетевого трафика (Network Traffic Analysis, NTA-решения), а также анализа ситуации на конечных узлах (Endpoint Detection & Response, EDR-решения). В отсутствие возможностей, предоставляемых EDR-системами и детального анализа трафика, мониторинг нельзя считать полным. Анализ сетевого трафика в ближайшие годы будет являться обязательной процедурой при проведении SIEM, анализ ситуации на конечных узлах станет

опциональной возможностью функционала. Для этой технологии доля покрытия равна 60–70%, а качество ее реализации эксперты Positive Technologies считают равным 2 баллам.

Четвертой тенденцией можно назвать добавление возможностей UEBA-решений (механизмов анализа поведения объектов) к инструментам SIEM, что даст возможность получения полной картины ситуации в инфраструктуре на едином экране. Принципиальная разница между UEBA и SIEM заключается в том, что средства UEBA разрабатывают модели поведения, а SIEM-решение является неким конструктором, собирающим логи. В алгоритмах поиска и изучения инцидентов могут использоваться разные подходы: машинное обучение, глубокое обучение, статистический анализ и т. д. Эти подходы дают оператору информацию о том, какие объекты ведут себя нетипичным для них образом и почему такое поведение нехарактерно для них. Доля покрытия этой технологии составляет 70–80%. Уровень качества реализации соответствует 4 баллам.

Следующий тренд в развитии SIEM связан с использованием облачных технологий. Исследование, которое провела компания Enterprise Strategy Group в 2019 г. по заказу Intel Corp. и Dell Technologies, показало, что 64% организаций планировали увеличение затрат на публичные облачные платформы в сравнении с предыдущим годом. Эта тенденция стимулирует вендоров к добавлению наиболее широко используемых платформ (Google Cloud Platform, Microsoft Azure, Amazon Web Services) в перечень поддерживаемых источников SIEM. Кроме того, вендоры начинают сами предлагать системы SIEM посредством подхода «as a service», дополняя способы развертывания, настройки и управления системой SIEM (облачных, виртуальных устройств — virtual appliance). Согласно мнению экспертов, покрытие технологии равно 60–70%, качество реализации равно 3 баллам.

По мнению [111] (рис. 1.4), некоторые из этих тенденций уже сейчас проявляются в определенной степени, другие из них станут актуальными в течение 1–3 лет. Эти технологии улучшают уровень качества работы с системами SIEM и дают возможность снизить нагрузку на операторов, осуществляющих мониторинг и реагирующих на инциденты.

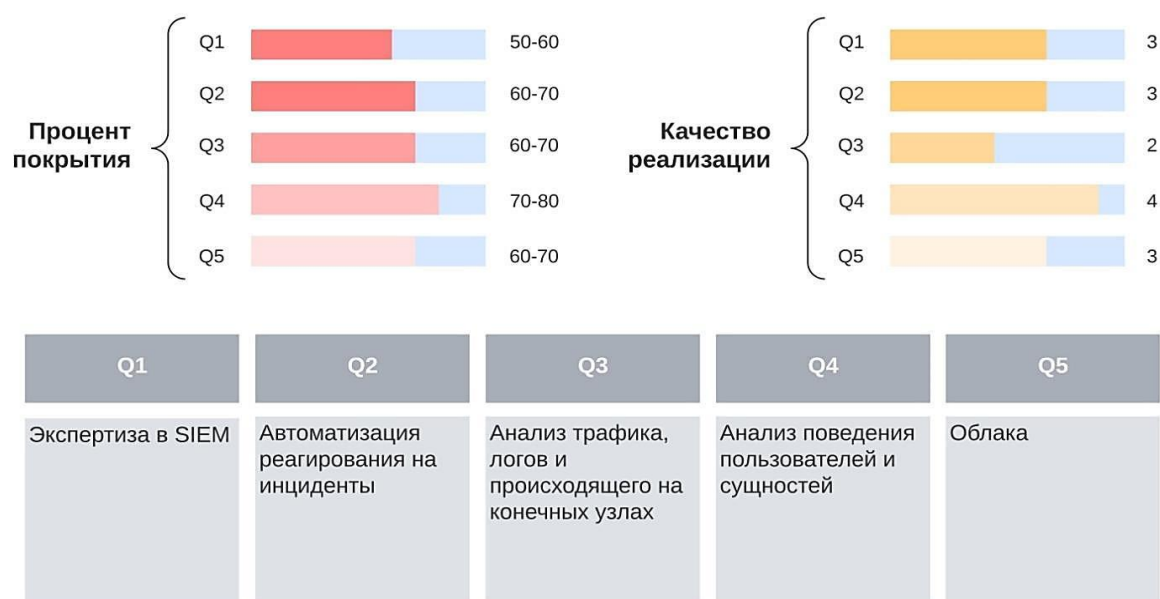


Рисунок 1.4 — Тренды развития SIEM-систем (оценки качества реализации: 1 — реализовано плохо; 2 — качество реализации ниже среднего; 3 — качество реализации среднее; 4 — качество реализации выше среднего; 5 — реализовано хорошо)

Представленная информация является экспертной оценкой компании Positive Technologies. Тенденции являются актуальными для компаний-лидеров на рынке SIEM (число компаний-лидеров было определено с помощью информации, предоставленной IDC).

1.6. Особенности защищенного обмена данными в области здравоохранения

Каждое государство по-своему пытается защитить себя от злоумышленников [113], и чаще всего на это тратятся значительные финансовые ресурсы. Однако эти ресурсы расходуются, главным образом, на безопасность в финансовой и промышленной отраслях, а сфере здравоохранения не уделяется достаточного внимания, что в корне неверно, поскольку кроме денежных средств, ущербу могут подвергнуться здоровье и даже жизнь людей. Вмешательство в медицинское оборудование в процессе операции может быть причиной потери здоровья или жизни пациента.

Различные государства по-разному пытаются решить вопрос разработки единых международных стандартов для обмена медицинскими данными. Это объясняет значительное число таких стандартов: ASC X12, ASTM, IEEE/MEDIX, HL7, NCPDP, DICOM и прочие [114]. Обычно эти документы именуют по названиям комитетов/групп и других некоммерческих организаций, принимавших участие в их разработке.

Группы по созданию стандартов специализируются на отдельных направлениях, например, ASTM E31.11 разрабатывает стандарты обмена данными лабораторных тестов; ACR/NEMA DICOM создает стандарты, связанные с передачей изображений; ASC X12N отвечает за внешние стандарты обмена электронными документами; IEEE P1157 (MEDIX) создает стандарты обмена медицинскими данными и т. п.

Медицинские учреждения, где уровень информационной напряженности очень высок по множеству причин (сезонные заболевания; срочные госпитализации; значительный поток пациентов и др.) — это один из объектов, где проблемы информационной безопасности требуют особого внимания. Информация о пациентах поступает в учреждение здравоохранения

непрерывно, причем фиксируется и на бумажных носителях, и в разнообразных информационных системах (электронная регистратура, диагностические системы — компьютерная томография, магнитно-резонансная томография, УЗИ и т. д.).

Уже в течение нескольких лет данные пациентов переходят с бумажных носителей в специальную электронную инфраструктуру. В настоящий момент эта информация находится в разных информационных системах, которые функционируют с использованием различных сетей, среди которых есть подключенные к внешней сети, использующие различные протоколы, специализированные медицинские системы и т. д. [115–117]. Следует отметить, что достаточно часто к ресурсам, которые обрабатывают данные пациентов, есть внешний доступ и, в целом, безопасности сетевой инфраструктуры медицинских учреждений не уделяется должного внимания. В электронной регистратуре находятся сведения о здоровье пациентов, являющиеся персональными данными, и это не только ФИО и контактная информация, но и более важные данные. Что касается диагностических устройств, то они используют аппаратные средства и методы обработки информации, сравнимые с промышленными устройствами в автоматизированных системах управления технологическими процессами [91].

В настоящее время известны многие случаи массовых атак на ИС медицинских учреждений. Также есть информация о возможных к реализации летальных атаках, целью которых является медицинское оборудование, функционирующее в лабораторных условиях.

Проблема безопасности медицинских данных является значительно более серьезной, чем это может показаться. Ситуация в мире, связанная с пандемией COVID-19, подтверждает это. Крах фондового рынка 2020 года, прекращение работы огромного числа предприятий; остановка авиасообщения между различными странами и регионами; большие потери в туристической отрасли, составляющие, согласно оценке руководителя WTTC

(Всемирный совет по туризму и путешествиям). Предварительно оценивается, что мировая экономика в целом недосчитается нескольких триллионов долларов.

В этот период были зафиксированы случаи проникновения злоумышленниками в информационные системы медучреждения с целью распространения ложной информации о наличии новых, более тяжелых, случаев заболевания COVID-19.

Закрытие границ между государствами, вынужденная изоляция граждан, спекуляция на товарах первой необходимости привели к тому, что используемые раньше способы кражи персональных данных граждан и их последующая продажа уже не так актуальны и примитивны в реализации, как сейчас, с использованием ВС.

Независимо от целей, которые ставят перед собой злоумышленники (это может быть адресная атака на конкретных людей или вымогательство денег у руководителей медучреждений), пациенты медицинских учреждений могут подвергнуться опасности. Быстрое обнаружение искаженной информации (например, при повторном обследовании или с помощью проведения других анализов) тоже не всегда полностью решает проблему, т. к. возможна приостановка работы медицинского учреждения в связи с тем, что необходимо перепроверить всю информацию, которая хранится в информационной системе данного учреждения.

По данным CDC (Центры по контролю и профилактике заболеваний США) среди причин смерти третье место в США занимают врачебные ошибки. Правильное диагностирование зависит не только от квалификации лечащего врача, но и от правильности сведений, которые поступают с медицинского оборудования и хранятся на серверах медицинских учреждений, которые могут быть целью злоумышленников и подвергаться их атакам.

Ниже приведены мнения экспертов в сфере ИБ, а также сведения из авторитетных международных источников относительно уровня защиты в секторе здравоохранения:

В отчете исследовательской компании Cybersecurity Ventures представлены данные о том, что в период 2017–2021 гг. число атак Ransomware на организации сферы здравоохранения, выросло вчетверо. К 2022 году это количество увеличится пятикратно [118].

Согласно данным выпуска ежегодного издания HIMSS Cybersecurity Survey (2020 г.) [119] около 60% персонала больниц и ИТ-специалистов, работающих в медицинских учреждениях, заявляют, что наибольшее число информационных проникновений происходит через электронную почту. Это касается случаев фишинга и других видов интернет-мошенничества [120].

По информации из HIPAA Journal число случаев мошенничества с использованием электронной почты в сфере здравоохранения за 2 года возросло на 473% [121].

По данным Health IT Security 24% людей, работающих в здравоохранении США никогда не принимали участие в тренингах повышения грамотности в сфере кибербезопасности. Тренинги такого типа ориентированы на помощь обучающимся в обнаружении и реагировании на фишинговые атаки, составляющие свыше 90% атак [122].

По данным [123], только 4–7% ИТ-бюджета системы здравоохранения расходуется на обеспечение кибербезопасности. В то же время, например, на финансовую отрасль приходится около 15%.

ИТ Gartner, исследовательская и консалтинговая компания, предполагает, что к 2022 г. свыше 25% кибератак в организациях, связанных с медициной, будут реализованы с помощью Интернета вещей (IoT): беспроводных и имплантируемых медицинских приборов (IMD) с беспроводным подключением (кардиостимуляторы, имплантируемые кардиовертеры-

дефибрилляторы (ICD), нейростимуляторы, инсулиновые помпы, и т. д.) [124].

В среднем каждое медицинское устройство имеет более 6 уязвимостей. При этом у 60% всех медицинских устройств заканчивается срок службы и нет возможности обновления [125].

Приведенные выше примеры являются лишь немногими из огромного числа и свидетельствуют о существовании проблемы в информационной безопасности медицинского сектора. Следует также отметить, что сфера здравоохранения в США планирует потратить свыше 65 млрд долл. США на продукцию и услуги по кибербезопасности в период 2017–2021 гг., а РФ предполагает потратить в течение этого периода на обеспечение информационной безопасности (во всех сферах) лишь 28 млрд руб. [126].

Недостаточно серьезное отношение к проблемам защиты информации в сфере здравоохранения может повлечь за собой значительный материальный ущерб, а иногда привести и к трагическим последствиям. Вот некоторые примеры.

В 2016 г. Пресвитерианский медицинский центр Голливуда (Калифорния, США) остановил свою работу на 4 дня из-за действий злоумышленников, которым было заплачено 17000 долл. США [127].

Атака вредоносной программы WannaCry в 2017 г. парализовала деятельность нескольких сотен медицинских учреждений Великобритании; привела к отмене тысяч операций, а также к массовому переводу неотложных больных из медицинских центров, подвергшихся атаке [128].

Ученые Израиля в 2019 г. нашли уязвимость в системах защиты медицинского оборудования. Используя эту уязвимость, можно искажать снимки, полученные с помощью КТ и МРТ, что может ввести в заблуждение лечащих докторов и привести к неправильному диагностированию [129].

Анализ протоколов, которые используются при работе с медицинским оборудованием, изучение их защищенности, поиск решений минимизирующих риски ИБ, с помощью создания многоуровневой архитектуры распределенных вычислительных структур, обеспечивающей безопасный контроль доступа по вычислительным сетям, а также анализ специализированных приложений в сфере здравоохранения — все это является актуальными задачами на настоящий момент.

Наиболее значимыми стандартами в сфере медицинской информатики можно назвать: Digital Imaging and Communications in Medicine (DICOM), Health Level 7, RCC, SNOMED CT [114].

Современные медицинские учреждения — это крупные экосистемы, включающие в себя значительное число устройств сетевой инфраструктуры, разнообразного оборудования, а также системы, в т. ч. взаимодействующие с внешней средой. Медицинские данные обладают большой чувствительностью к изменениям, постороннее вмешательство является серьезной угрозой жизни и здоровью людей. Для того, чтобы увидеть возможные уязвимости работы информационной инфраструктуры медицинского учреждения нет необходимости иметь какие-либо особые навыки. Для соблюдения конфиденциальности данных пациентов необходимо обеспечение безопасности медицинских данных на всех этапах работы с информацией [130]. При этом по-прежнему должны выполняться требования доступности и стабильности оказания медицинских услуг [131]. Обязательность выполнения всех этих требований приводит к следующему выводу: компании-разработчики медицинских систем и сами медицинские учреждения должны реализовать совокупность необходимых мероприятий, обеспечивающих требуемую степень защиты пациентов и информационных систем медицинских учреждений.

Поскольку человеческая жизнь является наивысшей ценностью, все мероприятия по обеспечению безопасности данных в медицинских инфор-

мационных системах (МИС) направлены на обеспечение сохранности жизни и здоровья пациентов [132, 133]. Опасная ситуация может возникнуть из-за действий злоумышленника, получившего доступ к сети учреждения посредством эксплуатации уязвимостей внешнего периметра и/или излишне пермиссивных политик доступа внутри локальной вычислительной сети [134]. Злоумышленник может не только испортить или сфабриковать медицинские изображения в архиве, но и нанести вред пациенту и учреждению, завладев учетными записями пользователей МИС (особенный интерес представляют учетные данные врачей), и корректируя курс лечения пациента по своему усмотрению. Меры КД [135] позволяют обезопасить пациентов и врачей от неверных диагнозов и последствий неподходящего лечения: защита данных в архивах DICOM позволяет исключить влияние поврежденных или поддельных медицинских изображений на решения, принимаемые врачом-диагностом; анализ пользовательской активности позволяет выявить неординарное и опасное поведение пользователей МИС, ассоциированное с деструктивным вмешательством в деятельность врачей [136].

Существует ряд актуальных развивающихся направлений в области контроля доступа данных медицинского характера.

Входящие данные должны соответствовать требованиям стандарта DICOM. Проверка выполнения этого требования должна осуществляться на стороне сервера (DICOM Server) или посредством механизма фильтрации, функционирующего как внешний интерфейс (frontend) сервера [137]. На этом этапе речь идет о Information Objects Definition (IOD). Следует отметить, что предложение представлять IOD с помощью формального языка не является новым [138]. Например, это реализовано в программном продукте dcm4che [139, 140].

Водяные знаки на медицинских изображениях. В [141] предложен способ нанесения водяных знаков, в основе которого лежит свойство обра-

тимости водяного знака. Этот метод позволяет аутентифицировать и обеспечивать самовосстановление изображения с помощью выделения интересующей (Region of interest) и не интересующей (Region of not interest) областей изображения. После этого первая область встраивается во вторую, а значит все возможные изменения в изображении могут быть выявлены, а изображение может автоматически корректироваться к исходному состоянию посредством извлечения 1-й области из 2-й. В [142] описан подход к обеспечению безопасности с использованием аутентификации пациента, при этом контроль целостности данных и соблюдение конфиденциальности происходят с использованием водяного знака, обладающего свойством обратимости. Контроль целостности данных происходит с помощью вычисления значения хеш-функции MD5. Свойство обратимости обеспечивает сжатый R–S-вектор, который вычисляется из изображения. Сам водяной знак создается с использованием значения уникального номера пациента, хеш-функции и сжатого R–S-вектора. Водяной знак шифруется с помощью Advanced Encryption Standard и встраивается в медицинские изображения.

Шифрование DICOM-изображений. В источнике [143] представлен метод, обеспечивающий конфиденциальность, контроль целостности и подлинности данных названия и пикселей DICOM-изображений — это механизм, включающий в себя шифрование и формирование подписи, а затем расшифровку и проверку подписи. В [144] представлены два различных метода, позволяющих обеспечить безопасность данных, находящихся в облачных хранилищах — это Rijndael (алгоритм шифрования, применяемый для конфиденциальных данных) и расширяемый протокол аутентификации. Авторы в своей работе [145] представляют безопасный способ хранения медицинских изображений в облачных структурах и их передачи. Этот способ включает в себя применение гибридного шифрования, т. е. сочетания симметричного и асимметричного алгоритмов шифрования. Предложенный авторами подход включает в себя отдельные процедуры:

- 1) хеширование заголовка файлов DICOM с использованием алгоритма хеширования SHA-3;
- 2) шифрование с помощью блочного алгоритма XTEA пикселей, содержащих результат, полученный на предыдущем этапе.

Применение искусственного интеллекта для обнаружения злонамеренной фальсификации медицинских данных. Мирский и др. [146] предложили атаку на сеть PACS, позволяющую изменять конфиденциальные файлы трехмерных изображений с использованием глубокого обучения. Они предложили модель GAN, помогающую добавлять или удалять паттерны, связанные с раком легких, при редактировании 3D-снимков компьютерной томографии. Авторы также упоминают использование цифровых подписей [121, 147] как лучший способ противостоять таким атакам. Они отмечают, что такая функция реализована в реальных системах PACS, но часто не настроена должным образом. Поэтому общий подход с контролируемой областью [148] считается более надежным в обнаружении взлома.

Использование коммерческих SIEM-решений является распространенной практикой для медицинских учреждений, поскольку техническая поддержка часто играет решающую роль. Одно из лидирующих решений, давно существующих на рынке, — IBM QRadar [26]: позволяет технологическим партнерам IBM разрабатывать расширения, называемые QRadar Applications [149], среди которых есть и нативный IBM QRadar User Behavior Analytics application [150]; а также имеет механизмы поддержания высокой доступности. К сожалению, не удалось найти расширений для интеллектуального анализа DICOM-трафика. Среди неоспоримых архитектурных достоинств QRadar стоит отметить кластер компонентов DataNode, каждый узел в котором добавляет пространства и вычислительных ресурсов [150]. Механизм высокой доступности полагается на присутствие первичного и вторичного аналитических хостов, при этом вторичная роль является резервной, постоянно синхронизируемой с первичной.

Другое распространенное решение от AT&T Cybersecurity, согласно исследованию Gartner [124], — USM Appliance [151] также содержит модули UBA, но не позволяет разработку сторонних расширений — разрешены только нативные плагины, разбирающие события с применением регулярных выражений [152]. Механизм поддержки высокой доступности полагается на пассивную копию установки (slave) [153].

1.7. Особенности защищенного обмена данными в области образования

В условиях современного цифрового общества КД система обучения и доступа к образовательным ресурсам имеет важное значение [154], что было продемонстрировано анализом функционирования образовательной цифровой среды в период эпидемий коронавирусной инфекции COVID-19.

В настоящее время внедрение информационных технологий позволяет учреждениям в сфере высшего образования усилить свои конкурентные преимущества за счет перехода к новой бизнес-стратегии, отвечающей современным тенденциям и реализующей поставленные руководством задачи. С учетом последствий пандемии COVID-19 образовательным учреждениям пришлось перейти на формат дистанционного обучения. Это привело к тому, что применение ИТ и актуальных образовательных технологий в учебном процессе в настоящее время обладает сильным влиянием на развитие сферы образования. Огромное количество программ информатизации в образовательной сфере направлено на модернизацию ИТ-инфраструктуры образовательных учреждений, обновление лабораторного оборудования, и в целом глобальную информатизацию, которая позволяла бы результативно управлять организацией, оказывать образовательные и информационные услуги обучающимся, преподавателям, научным работ-

никам и персоналу, в т. ч. с применением современных дистанционных технологий. Это накладывает определенные условия на деятельность образовательных учреждений — ИТ-инфраструктура должна быть современной, безопасной и масштабируемой. Это будет фундаментом для создания, внедрения и функционирования информационных систем в образовательной сфере.

ИТ-инфраструктура сервисов в сфере образования — это совокупность программных, аппаратных, телекоммуникационных ресурсов и продуктов, служащих для решения задач обучения и профессиональной деятельности, которые стоят перед обучающимися, преподавателями, научными работниками и другим персоналом.

Стратегия развития ИТ-инфраструктуры организации — это один из основополагающих элементов ИТ-стратегии организации. В стратегию развития ИТ-инфраструктуры закладываются требования к обеспечению результативного выполнения ИТ-процессов, связанных с оказанием информационных услуг в соответствии с принятыми бизнес-требованиями. Кроме того, эта стратегия включает в себя проект перехода от актуальной архитектуры организации к архитектуре, построенной с учетом функционирования дистанционных образовательных технологий.

К ИТ-инфраструктуре сервисов образования предъявляются следующие требования:

Гарантированный контроль доступа.

ИТ-инфраструктура сервиса образования должна обеспечивать управление правами доступа пользователей, т. е. разграничивать доступ пользователей к информационным ресурсам, основываясь на правилах разграничения доступа, заданных в ИС, и следить за выполнением данных правил.

Процесс проектирования ИТ-инфраструктуры включает в себя: 1) реализуемые модели управления доступом — мандатная, дискреционная, не-

дискреционная; 2) возможные типы доступа — просмотр, изменение, выполнение, создание; 3) правила разграничения доступа. Могут быть привязаны к спискам, ролям, меткам безопасности, значениям атрибутов и др.

Кроме того, при проектировании устанавливаются показатели качества (доступности информации) в соответствии с матрицей доступа (разрешительной системой) к обрабатываемой информации. В штатном режиме функционирования ИТ-инфраструктуры обеспечивается авторизованный доступ пользователей, с определенными показателями качества.

Надежность.

Надежностью является следующая характеристика ИТ-инфраструктуры — поддерживать постоянными (в установленных границах) значения показателей способности функционирования в заданных режимах и при определенных условиях использования.

Для того, чтобы гарантировать надежность ИТ-инфраструктуры обычно используют стандартные протоколы работы оборудования, применяют резервное копирование. Для решения отдельных прикладных задач могут применяться технические средства и программно-аппаратные структуры более узкой направленности.

Безопасность.

Безопасность в данном случае представляет собой успешное и своевременное выявление и реагирование на попытки несанкционированного доступа к информации, а также прочих действий, направленные на ИС и/или информацию. Эти действия совершаются злоумышленниками для получения доступа к информации, внесения в нее изменений, уничтожения и изменения доступа.

Инфраструктура образовательного учреждения включает в себя значительное число связанных между собой элементов, безопасность которых необходимо обеспечить:

- система дистанционного обучения;

- система по учету обучающихся;
- система учета помещений и оборудования;
- система контроля и управления доступом;
- система бухгалтерского учета;
- система для организации и проведения видеоконференций и т. д.

Защита среды виртуализации

Для обеспечения защиты среды виртуализации следует исключить возможность несанкционированного доступа к данным, которые обрабатываются в виртуальной инфраструктуре, а также к ее элементам. Также должна быть исключена возможность воздействия на информацию и элементы виртуальной инфраструктуры, среди которых: средства управления, гипервизоры, системы хранения и обработки данных, сетевое оборудование, гостевые ОС, системы репликации данных, терминальное оборудование, системы резервного копирования и восстановления данных.

Масштабируемость.

Масштабируемость дает возможность оперативного внесения поправок в ИТ-инфраструктуру для адаптации к актуальному состоянию внутренней и внешней среды образовательного учреждения. Сфера образования достаточно динамична, зачастую необходимы срочные коррективы для внесения изменений в бизнес-процессы, а также создание и внедрение дополнительных информационных систем в существующую инфраструктуру.

Масштабируемость — это обеспечение возможности увеличения количества и объема составляющих элементов с учетом сохранения установленных характеристик функционирования инфраструктуры. ИТ-инфраструктура образовательного учреждения должна отвечать требованию наличия возможности внедрения в сжатые сроки необходимых сервисов, т. е. должна развиваться с опережением, с учетом будущих тенденций.

Результативность использования ресурсов.

Принимая во внимание стоимость ПО и оборудования и учитывая тот факт, что значительная часть затрат образовательного учреждения приходится на поддержку ИТ-инфраструктуры (а не на ее создание), актуальным является требование оптимальной стоимости содержания ИТ-инфраструктуры. Следует отметить, что в действительности имеют место не случаи лишних трат, но наоборот — попытки необоснованного уменьшения затрат на поддержку ИТ-инфраструктуры, которые часто влекут за собой неблагоприятные последствия.

Данные требования важно постоянно поддерживать и обновлять с учетом развития современных ИТ стандартов.

Если приводить аналогию сервисов образования с циклом Деминга [155], то можно их представить так, как показано на рис. 1.5.

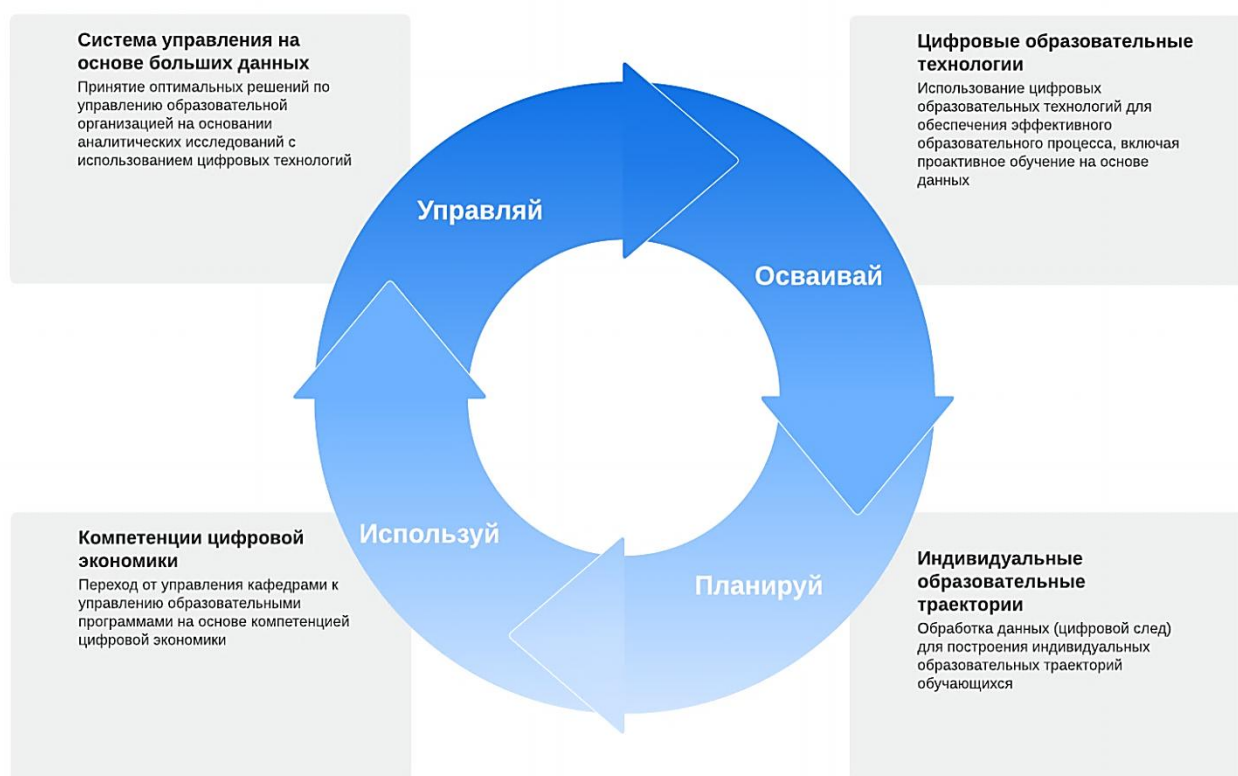


Рисунок 1.5 — Критерии оценивания качества ИТ-инфраструктуры ВК

Использование стратегического подхода к созданию ИТ-инфраструктуры организации включает в себя как непрерывный мониторинг и исследование внешней среды, так и основательное изучение, и наблюдение за ИТ-процессами организации, что возможно осуществить, используя готовые программные продукты.

Создание и развитие образовательной, инновационной и научной инфраструктуры, которая предоставляет все условия для того, чтобы каждый учащийся и сотрудник мог наиболее успешно реализовать свой образовательный, профессиональный и личностный потенциал, — это одна из важнейших задач развития информационной образовательной среды.

Угрозами ИТ-инфраструктуре образовательного учреждения могут быть взлом файерволов; рассылка электронных сообщений, содержащих вредоносные вложения; попытки несанкционированного доступа к информации и т. д. Число способов атаки на информацию, хранящуюся в ИС организации, увеличивается, появляются новые механизмы, используемые злоумышленниками.

ИТ-инфраструктура организации должна обеспечивать непрерывное осуществление мониторинга верификации пользователей, защищать информационную образовательную среду организации, причем пользователю должна быть предоставлена возможность в течение достаточного времени оставаться в сеансе доступа к определенному ресурсу. Для контроля за этой ситуацией в сфере образования актуальным является использование технологий UBA [47].

UBA-системы направлены на сбор данных, необходимых для построения моделей машинного обучения, позволяющих обнаруживать паттерны аномальной активности в плотном журнале событий, который часто рассматривается как поток больших данных [12, 140, 156–158]. При этом модели направлены на выделение шаблонов нормальной и подозрительной активности, построение профилей событий.

Существует большое разнообразие подходов к моделированию.

- 1) Модели, основанные на немонотонном обучении, позволяющие выполнять пересмотр правил поведения пользователя (например, в [39] используется аппарат индуктивного логического программирования для обучения модели на примерах).
- 2) Модели ожидаемого пользовательского поведения (в [159] предложен алгоритм, который принимает запрос доступа в качестве входных данных и использует отношения между сеансами, ролями, командами вместе с различными ограничениями на действия и поведение, чтобы найти подходящую политику управления доступом для принятия решения о контроле доступа).
- 3) Модели обнаружения злонамеренного поведения в средах SIEM (например, в [50] проведен анализ наборов данных [160, 161]).
- 4) Логические, ситуационные, статистические и другие модели также применимы для анализа поведения пользователей.

Выводы по главе

Проведенный анализ современных вычислительных инфраструктур, систем и комплексов, обеспечивающих поддержку и контроль доступа в информационной среде цифровых услуг, показал актуальность следующих направлений по разработке архитектур контроля доступа в вычислительных комплексах, функционирующих в цифровой среде:

- разработка многоуровневой масштабируемой архитектуры контроля доступа;
- построение аппаратного обеспечения для контроля доступа;

- построение облачной инфраструктуры обработки данных контроля доступа;
- разработка методики оценки вычислительных ресурсов для компонентов системы контроля доступа;
- совершенствование контроля доступа на основе использования реакций пользователей при работе с элементами интерфейса;
- построение многоуровневой архитектуры распределенных вычислительных комплексов для обеспечения защищенного контроля доступа по компьютерным сетям для сервисов образования и здравоохранения.

Глава 2. РАЗРАБОТКА МНОГОУРОВНЕВОЙ МАСШТАБИРУЕМОЙ АРХИТЕКТУРЫ КОНТРОЛЯ ДОСТУПА

В главе сформулированы задача проектирования архитектуры контроля доступа, требования к составу средств контроля доступа; разработана четырехуровневая архитектура контроля доступа к вычислительному комплексу, предоставляющему веб-сервисы с учетом заданных технико-экономических характеристик.

2.1. Анализ современных концепций построения систем контроля доступа к информационным ресурсам

Современная система доступа к ВС включает большое количество средств контроля, идентификации и верификации пользователей (рис. 2.1).

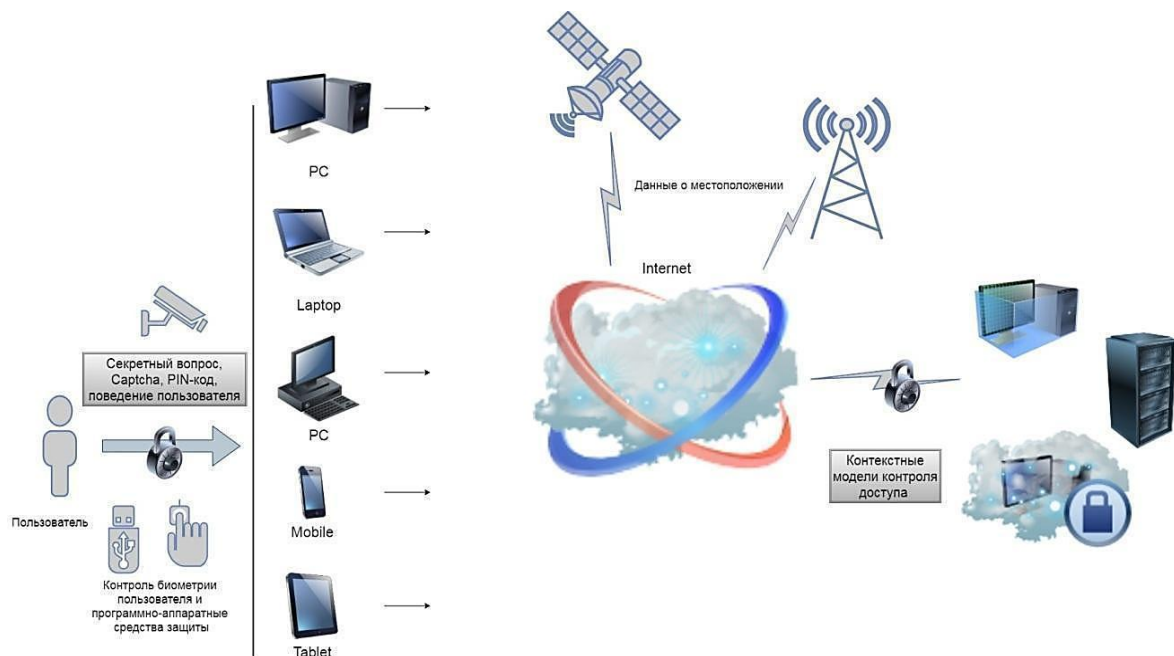


Рисунок 2.1 — Архитектура вычислительного комплекса
с многоуровневым контролем доступа

Требования к обеспечению контроля доступа и условия функционирования могут быть сформулированы следующим образом [11, 140, 162]. ВК с системой с защищенного контроля доступа к ВС по компьютерным сетям обеспечивает возможность доступа с любого устройства, используемого пользователем. При этом происходит идентификация пользователя с использованием различных средств биометрии (например, отпечаток пальца, встроенные или внешние камеры), в процессе доступа используются программные средства верификации (секретный вопрос, PIN-коды, Captcha). В настоящее время развиваются системы, связанные с анализом поведения пользователей (например, реакции пользователей на вопросы доступа или поведенческие модели). Элементом контроля доступа является учет локации пользователя, эти данные могут быть сравнены с данными в профиле пользователя. Для доступа к сервисам существует уровень контроля доступа, обеспечиваемый контекстными моделями. Такими моделями могут быть политики, построение моделей по журналам событий, соответствующим группам пользователей, а также специализированные методики, относящиеся к предметной области сервиса — медицинские, банковские, образовательные, имеющие свои специализированные протоколы и особенности доступа. На уровне вычислительных ресурсов [163] — серверов, виртуальных машин, баз данных, осуществляется аппаратный контроль доступа [164].

Таким образом, содержательно процесс доступа к ВС описывается отношением некоторой группы субъектов к заданной совокупности ресурсов, к которым эти субъекты желают занять доступ.

Для описания, формализации, анализа или синтеза системы КД необходимо, прежде всего, описать три основных его компонента [165, 166]:

- субъектов, участвующих в системе КД,
- ресурсы
- и объекты, являющиеся предметом интересов субъектов.

Отметим, что в процессе КД ставится задача обеспечения сохранности всех необходимых свойств (или, обобщенно ВС) данных ограниченного доступа [167].

Под субъектом понимается не только физическое или юридическое лицо, которое желает воспользоваться определенным программно-аппаратным или информационным ресурсом в информационной системе, но и информационные процессы, программно-аппаратные средства, которые могут получить доступ к ВС. Таким образом, под субъектом понимается любой объект или процесс, который может совершить определенное действие в информационной системе с использованием процессорных устройств системы. Примеры субъектов программно-аппаратного типа: операционная система, антивирусные и сетевые средства, информационные системы конкретного назначения (редакторы, СУБД, системы электронного документооборота, системы для обслуживания бизнес-процессов (например, 1С), и т.п.

Под объектом, осуществляющим доступ, понимаются любые поименованные элементы информационной системы, к которым может получить доступ хотя бы одно из процессорных устройств: информационные системы, периферийное и сетевое оборудование, файлы, носители информации, внешние устройства разного назначения. Более того, одни объекты доступа могут являться частью других объектов доступа (если они поименованы и доступны для процессоров); например, флешка и файлы, записанные на ней, являются объектами доступа, таковыми же являются база данных и отдельные записи, содержащиеся в ней, межсетевой экран и отдельные его параметры, доступные для процессоров.

Доступ описывает непосредственно набор тех действий, которые может совершать данный субъект над данным объектом [168]. Таким образом, доступ привязан к паре «субъект-объект» и представляет собой набор разрешенных (санкционированных) действий, которые может совершать

субъект над объектом. Основными видами доступов являются чтение и запись данных. Многие другие виды действий с данными могут с некоторой степенью условности приведены к этим видам доступа. Например, удаление файла может рассматриваться как запись пустых данных в файл — в этом случае пустой файл отождествляется с удаленным файлом, что в целом не всегда корректно. Далее, добавление данных в файл может быть отождествлено с записью данных [169]. Однако, если данные структурированы (например, в базах данных), то подобное добавление требует предварительного формирования структурного скелета новой записи, что уже не укладывается в схему просто записи данных в файл. Поэтому к перечисленным видам действий, которые могут входить в доступ, добавляются также удаление объекта (файла, устройства из перечня и т.п.), добавление объекта (записи, устройства), активации объекта (запуска программы, включение технического устройства), модификация (замена), блокирование, контроль права собственности (включая авторизацию, подтверждение авторства или авторских прав). В состав возможных видов доступа могут включены и другие более специфические действия [170].

Процесс формирования и реализации доступов для каждой пары «субъект-объект» из заданных перечней субъектов и объектов, а также порядок изменения этих доступов в процессе функционирования информационной системы и составляет основное содержание политики управления доступом. В настоящее время выделяют три основных способа построения системы КД: 1) дискреционный; б) мандатный; в) ролевой. Рассмотрим каждый из перечисленных видов более подробно.

1. Дискреционное управление доступом (Discretionary Access Control DAC), или разграничительная политика доступа (РПД) – политика КД, при которой процедура предоставления/не предоставления доступа опирается на характеристики непосредственно объектов доступа. Каждый из объектов доступа наделен рядом характеристик, прежде всего, уровнем

секретности, его ценностью — при равных уровнях секретности ценность объекта, в том числе стоимость, возможные потери, связанные с нарушением его сервисов безопасности, могут быть разные. Значения указанных характеристик обычно устанавливаются владельцем объекта. То есть изначально предполагается, что каждый объект имеет своего владельца (собственника). Собственник имеет все права доступа к объекту, в том числе обычно имеет право передавать часть или все права на данный объект (программную систему, техническое устройство, информационную базу и т. п.) другим субъектам, в частности продавать, предоставлять в аренду или в разовое использование.

При РПД объектами контроля, на основе анализа которых и принимаются управленческие решения, являются непосредственно объекты обработки данных. Поэтому, наиболее простой способ задания РПД заключается в перечислении для каждой пары «субъект-объект» предоставленные права доступа с сопутствующими условиями и ограничениями. Это перечисление может быть представлено в виде матрицы, строки которой соответствуют субъектам системы, а столбцы — объектам доступа; на пересечении перечисляются разрешенные виды доступов с сопутствующими ограничениями. Описанная матрица называется матрицей доступа. Таким образом, любая РПД задается матрицей доступа, которая однозначно определяет данную конкретную РПД, и принцип доступа, лежащий в основе РПД, может быть сформулирован следующим образом: разрешено только то, что записано в матрице доступа. Данная процедура доступа реализует запретительный принцип доступа, когда разрешено только то, что записано, а все остальное запрещено — в отличие от разрешительного принципа доступа, когда перечисляется все, что запрещено, а все остальное считается разрешенным.

Концепция построения РПД, имеющая по своей сути более чем двухтысячелетнюю историю как составная часть систем физической охраны и

безопасности объектов защиты, применительно к системам обработки данных имеет ряд существенных недостатков. Прежде всего, данная политика КД, вообще говоря, не обеспечивает гарантий безопасности в будущем даже при самом тщательном соблюдении всех требований политики ИБ — имеются конкретные примеры РПД, в которых доказано отсутствие гарантий безопасности.

Вторым существенным недостатком данной политики, особенно значимым, является отсутствие защиты от атак с помощью программных закладок типа троянского коня [171]. Поясним сказанное на примере. Пусть в системе имеется два пользователя U_1 и U_2 , причем U_2 является злоумышленником. Объектами защиты являются три информационно-программных объекта O_1 , O_2 и O_3 , где объект O_1 содержит закрытые данные, которые недоступны пользователю U_2 , объект O_2 содержит данные ограниченного пользования, доступные обоим пользователям, причем уровень секретности объекта O_2 не ниже уровня секретности O_1 , объект O_3 является общедоступным.

Для несанкционированного получения данных из объекта O_1 пользователь U_2 может поступить следующим образом. Запустив объект O_3 по своим идентификационным данным, пользователь U_2 может записать в него троянскую программу, которая бы позволила выполнить следующие действия: O_3 при одновременной работе с O_2 (ее тоже может запустить U_2) записывает в O_2 программу, которая бы перекачала определенные данные из O_1 в O_2 в момент, когда обе программы будут одновременно работать (будут запущены пользователем U_1), что на практике рано или поздно происходит. Затем троянская программа перекачает эти данные из O_1 в O_2 , откуда злоумышленник U_2 сможет скопировать эти данные. Отметим, что утечка информации произошла без формального нарушения правил доступа. Практическая реализация описанного канала утечки на основе троянской программы требует дальнейших уточнений.

Таким образом, дискреционная политика доступа в ее классическом виде, являясь наиболее простой в реализации и распространенной (практически все известные программные продукты опираются на РПД), имеет ряд принципиальных недостатков, не позволяющих полноценно опираться на эту политику. В то же время отказаться от этой политики невозможно ввиду характера ее реализации — даже в составе мандатной и ролевой политик управления доступом заложены возможности дискреционного доступа. Следовательно, необходимо усовершенствовать механизмы реализации РПД так, чтобы максимально обесценить негативные элементы этой политики. При этом, конечно, абсолютных гарантий безопасности не достигнется, поскольку, как показал анализ данной политики [172], обеспечение гарантий безопасности в будущем, вообще говоря, недостижимо, если объектами управления доступом являются объекты обработки данных. В связи с этим, применительно к РПД часто не ставятся задачи обеспечения условия абсолютной гарантированности защиты в будущем, а задачи обеспечения гарантированности с вероятностью, не ниже заданной (обеспечения гарантированного качества, Quality-of-Service, QoS).

2. Мандатное управление доступом (MandatoryAccessControl — MAC), или полномочная политика доступа (ППД) — политика КД, при которой процедура предоставления/непредоставления доступа опирается на характеристики не объектов доступа, а информационных потоков, возникающих между объектами и субъектами системы. Иными словами, при осуществлении доступа происходит перемещение информации между субъектом и объектом доступа — это перемещение называется информационным потоком. Всем объектам и всем субъектам приписываются метки, обозначающие их уровень секретности или уровень доступа соответственно. Тогда принцип доступа в рамках ППД может быть сформулирован следующим образом: разрешены только те потоки, которые не приводят к информационному потоку от более секретного объекта или субъекта

к менее секретному объекту или субъекту; при равных уровнях секретности все потоки разрешены. Таким образом, мандатное управление доступом опирается на запретительный принцип доступа, в отличие от дискреционного управления доступом.

Рассмотрим теперь более детально, в чем состоит разница между данными двумя политиками КД. Вначале рассмотрим два базовых вида доступа: чтение и запись. При чтении информационный поток направлен от объекта к субъекту; поэтому поток будет разрешенным, если уровень секретности объекта не ниже уровня доступа объекта, что совпадает с правилом разрешенного доступа в РПД. Таким образом, применительно к чтению правила доступа для обеих политик (РПД и ППД) совпадают. При реализации доступа «запись» информационный поток направлен от субъекта к объекту; поэтому уровень доступа субъекта должен быть не ниже уровня секретности объекта. Однако при дискреционной политике, если уровень доступа субъекта ниже уровня секретности объекта, то доступ по записи также запрещен. Таким образом, применительно к доступу «запись» правила доступа в РПД и в ППД противоположны. К действиям типа «запись» сводятся и другие важные виды доступа: добавление данных, изменение, уничтожение. Таким образом, во всех перечисленных доступах правила доступа в РПД и ППД противоположны.

Описанное правило и позволяет избежать возникновения канала утечки информации, описанного выше при анализе недостатков РПД. Именно для того, чтобы в рамках ППД троянская программа, записанная в O_2 , могла прочитать закрытые данные из объекта O_1 и затем записать в O_2 , необходимо, чтобы текущие уровни секретности объектов O_1 и O_2 совпадали. Но если пользователь U_2 имеет право читать данные из O_2 , то, в силу требований ППД, его уровень доступа (по чтению) не ниже уровня секретности объекта O_2 (а значит, и O_1), и в этом случае U_2 может считать данные непосредственно из O_1 . Следовательно, U_2 не имеет права считывания дан-

ных из O_2 , и проведенная работа по организации канала утечки с использованием объекта O_2 оказывается бессмысленной, не позволяя пользователю U_2 прочитать данные из O_2 .

При использовании ППД возникает ряд проблем. Рассмотрим две наиболее важные из них. Как следует из описания правила доступа по записи, если уровень доступа субъекта выше уровня секретности объекта, то субъект не может записать данные в объект. Например, руководитель, если уровень доступа у него выше, чем у подчиненного, не сможет переслать никакой информации своему подчиненному — ситуация, в некотором смысле несовместимая с логикой управления коллективом сотрудников. Для решения данной проблемы в ППД введено еще одно понятие — понятие текущего уровня секретности объекта и текущего права доступа. Если необходимо записать информацию от более секретного объекта в менее секретный, то предварительно на время записи уровни секретности обоих объектов выравниваются до некоторого промежуточного уровня, который и называется текущим, — это уже позволяет произвести требуемую запись данных.

Еще одна проблема в ППД: политика мандатного управления, как видно из приведенного описания, сложнее политики дискреционного управления доступом. Если произойдет сбой работы самой системы мандатного управления доступом, то будет заблокирована вся система обработки данных. Во избежание подобной ситуации в ППД для узкой категории пользователей, включающей администраторов информационной безопасности, вводится возможность прямого вмешательства в процедуру управления доступом, что является, по существу, дискреционным управлением доступом. Таким образом, при реализации ППД не удалось пока избавиться от РПД.

Наиболее известной моделью, реализующей ППД, является модель Белла–Лападула, впервые представленная в «Оранжевой книге». (стандарт

«Критерии безопасности компьютерных систем», Trusted computer system evaluation criteria — TCSEI, разработанный Министерством обороны США в 1983 г. Этот документ более известен под неформальным названием «Оранжевая книга»). В рамках модели все перечисленные выше варианты мандатного доступа реализованы. Для модели Белла–Лападула доказано, что при соблюдении в течение сколь угодно большого промежутка времени всех требований ППД, в будущем никогда не произойдет злоумышленного проникновения в систему, то есть выполняется условие гарантированной безопасности. Это существенное достоинство ППД по сравнению с РПД, которая не дает подобных гарантий.

При РПД объектами контроля, на основе анализа которых и принимаются управленческие решения, являются, наряду с субъектами и объектами, информационные потоки между всеми парами объектов и субъектов, прежде всего, их направления. Поэтому мандатную политику можно задавать с помощью функций секретности (для объектов) и доступа (для субъектов), описывающих указанные показатели для каждого объекта и субъекта в текущий момент времени. Тогда процедура реализации ППД заключается для каждой пары «объект-субъект» и каждого вида доступа значений указанных функций.

Мандатное управление доступом позволяет обеспечить гарантированное выполнение политики безопасности. Основные недостатки: структурная простота существующих моделей, опирающихся на ППД, что часто не позволяет «уложить» требования по обеспечению безопасности в рамки данной модели. Кроме того, для достаточно сложных систем объем работы по назначению и последующему контролю прав доступа оказывается настолько большим, что реализовать его вручную становится практически невозможным.

Таким образом, мандатное управление доступом, решая одну из основных проблем процесса обеспечения ИБ — проблему гарантированно-

сти защиты в будущем, пока не находит столь широкого применения по сравнению с дискреционной политикой ввиду простоты моделей, в рамках которых доказана гарантированность — эти модели не учитывают специфические требования реальных объектов защиты. Поэтому в настоящее время ППД часто используется как дополнительная процедура к РПД. Например, в известной СУБД в основной системе используется РПД, а мандатное управление доступом предлагается в составе дополнительного пакета программных модулей.

3. Ролевая политика управления доступом (РлПД) опирается на приписывание ролей всем субъектам, которые задают допустимые рамки возможных действий субъекта. Роль — это определенный набор разрешенных/запрещенных действий, которые могут быть организованы как на основе дискреционной, так и на основе мандатной политики. Более того, в настоящее время создаются модели ролевого доступа, в которых роли привязаны также к текущим параметрам систем обработки данных и безопасности, то есть набор возможных действий в рамках роли может увеличиваться или сужаться в зависимости от состояния системы, что является еще одним важным достоинством РлПД. Таким образом, объектами контроля в рамках РПД являются роли. Перечислим достоинства и недостатки РлПД по сравнению с РПД и ППД. Выделим вначале достоинства.

Роль может динамически изменяться, разрешаться или запрещаться в зависимости от текущего состояния системы, что позволяет значимо повысить эффективность управления доступом и тем самым, эффективность обеспечения ИБ.

Одной из серьезных проблем при практической реализации РПД и ППД, особенно для больших систем, является сложность задания и контроля прав доступа для каждой пары «субъект-объект». Для решения этой проблемы в рамках РПД и ППД часто создают группы пользователей, наделяя правами группу и приписывая каждого пользователя к некоторой

группе. Однако при этом взаимодействие внутри групп требует отдельного внимания, поскольку пользователи одного уровня прав могут иметь индивидуальные требования по доступам. В ролевой же политике доступа выбирается либо формируется типовой набор ролей, в которых все возможные проблемы взаимодействия максимально устранены. Задание политики управления доступом на основе ролей в целом требует существенно меньших усилий, чем задание прав доступа на основе РПД и ППД.

Организация процесса управления доступом на основе ролей позволяет формировать разные сценарии процесса обеспечения ИБ, в которых может быть зафиксирована определенная последовательность активизации ролей, допустимое совмещение ролей (в смысле совместной реализации их в один и тот же момент), в том числе с учетом запущенных приложений.

Ролевое управление доступом активно применяется во многих важных приложениях: системах управления базами данных, системах электронного документооборота. Поэтому использование РлПД в рамках операционной системы может являться гармоничным дополнением к ролевой политике в рамках этих приложений, что позволяет более полно охватить все возможные особенности доступа к ресурсам системы.

Наборы ролей позволяют намного более адекватнее, чем РПД и ППД, охватить все особенности систем обработки данных и требований по политике безопасности.

Основным недостатком РлПД является отсутствие доказательства выполнения свойства гарантированности выполнения требований политики управления доступом в будущем. Это связано со сложностью формализованных моделей, описывающих политику ролевого доступа; например, в [173] описанию формализованной модели посвящены две главы монографии. Анализ столь сложных моделей в ручном режиме практически невозможен. К сожалению, существующие методы автоматического анализа подобных моделей пока малоэффективны. Примером автоматического

анализа подобных моделей являются подход, основанный на использовании методов темпоральной логики [174.

Проведем анализ — рассмотрим три наиболее распространенные системы КД, давая их общую характеристику, исследуя достоинства и недостатки. Выявлено, что наиболее распространенная из них — РПД является и наиболее важной, поскольку остальные две включают элементы РПД. Непосредственно РПД имеет ряд серьезных недостатков, которые создают благоприятные возможности для злонамеренных атак. Поэтому необходимо усовершенствовать систему РПД элементами, которые бы повысили эффективность защиты на основе РПД. Опишем некоторые возможные способы повышения эффективности.

Прежде всего, целесообразно использовать все три политики КД в сочетании и даже в совокупности. РПД и ППД могут использоваться параллельно, и доступ будет разрешен, если он разрешен по обоим политикам управления доступом. Наиболее сложным элементом данной системы является контроль доступа по операции записи и подобным ей операциям, которые, как было указано выше, противоположны по своим правилам. Для операции записи анализ доступа должен проводиться по текущим уровням секретности объектов и доступа субъектов. Тогда проблем с доступом по обоим политиками не возникает, поскольку при выравнивании уровней секретности и доступа уровень доступа субъекта всегда должен либо оставаться без изменения, либо понижаться (не увеличиваться). Таким образом, сочетание и совместное использование РПД и ППД возможно. Применительно к РлПД укажем, что в рамках каждой роли по отдельным правам доступа может использоваться как РПД, так и ППД и даже их совокупность. Таким образом, возможно совместное использование всех трех политик управления доступом, что позволит существенно повысить эффективность системы обеспечения защищенности ВК.

2.2. Формирование политик защищенности доступа к вычислительным комплексам

Процесс обеспечения защищенного доступа на конкретном ВК складывается из ряда направлений обеспечения ИБ, каждое из которых в настоящее время принято представлять как одну из политик доступа (ПД). Под политикой обеспечения защищенного доступа понимается организованная совокупность средств, методов и мероприятий, нацеленная на решение задач, связанных с обеспечением защиты доступа к ВС.

В настоящее время выделяют много разных видов частных политик [175]. Сформируем набор ПД, обеспечивающих защищенный КД.

1. Политика системы менеджмента информационной безопасности.
2. Политика предоставления и контроля доступа к ВС (политика управления доступом).
3. Политика разграничения доступа.
4. Политика чистого стола и чистого экрана.
5. Политика неразрешенного программного обеспечения.
6. Политика, касающаяся получения файлов программного обеспечения из внешних сетей или через них.
7. Политика использования мобильных устройств и носителей информации (политика, касающаяся мобильного кода).
8. Политика резервного копирования.
9. Политика, касающаяся обмена информацией между организациями.
10. Политика, касающаяся допустимого использования электронных средств связи.
11. Политика сохранения записей (политика обезличивания данных).
12. Политика использования сетевых служб.
13. Политика, касающаяся мобильных вычислений и связи.
14. Политика дистанционной работы.

15. Политика использования криптографического контроля (политика использования криптографических средств).
16. Политика соответствия.
17. Политика лицензирования программного обеспечения.
18. Политика учета, хранения и уничтожения электронных и бумажных носителей (Политика удаления программного обеспечения).
19. Политика защиты и секретности данных.
20. Политика протоколирования и аудита.
21. Политика контроля целостности.
22. Политика экранирования.
23. Политика анализа защищенности.
24. Политика обеспечения отказоустойчивости.
25. Политика обеспечения безопасного восстановления.
26. Политика туннелирования.
27. Политика восстановления.
28. Политика физической защиты информационных систем.
29. Политика администрирования.
30. Политика идентификации и аутентификации.
31. Политика работы пользователя.
32. Политика антивирусного контроля.
33. Политика проведения ремонта, настройки, модификации технических средств, входящих в состав автоматизированных (информационных) систем обработки конфиденциальной информации.
34. Политика организации парольной защиты.
35. Политика резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных.
36. Политика учетных записей
37. Политика защиты АРМ
38. Политика защиты от утечки по техническим каналам.

По этим более специальным требованиям состав частных ПД может быть более конкретизированным и ограниченным. Например, применительно к защите персональных данных наряду с общей ПД выделяют в качестве основных следующие виды частных политик (ниже приведены их номера в соответствии с приведенным перечнем), которые и являются предметом анализа при аттестации автоматизированных (информационных) систем обработки конфиденциальной информации по требованиям безопасности обработки персональных данных: 15, 18, 29, 31 – 35.

Среди перечисленных ПД одной из наиболее важных является политика КД. Это связано с тем, что почти любое опасное злонамеренное действие обычно предполагает несанкционированное проникновение «вглубь» зоны, где находится интересующий злоумышленника информационный ресурс, то есть предполагает несанкционированные действия (НСД). Более того, первый в мире стандарт по информационной безопасности (известный как «Оранжевая книга») опирается на следующую аксиому безопасности [177, с.9]: «...what it really means to call a computer system "secure." ...secure systems will control ... access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information.» — «...что такое безопасная компьютерная система. ...в безопасных системах должен контролироваться доступ к информации таким образом, что только правильно идентифицированные субъекты или процессы, действующие от их имени, будут иметь доступ на чтение, запись, создание или уничтожение информации». Таким образом, безопасная система (по «Оранжевой книге») — это система, управляющая доступом к информации таким образом, что только авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию. Кратко данное положение означает, что все проблемы обеспечения информационной безопасности описываются доступом **субъектов к объектам**.

Данное положение было принято большинством ведущих специалистов по информационной безопасности во всем мире и повторено в стандартах и нормативных документах других стран [178, 179]. В действительности, данное положение не является корректным, поскольку, как видно из приведенного выше перечня 38 частных политик безопасности, контроль доступа — это только одна из частных политик (хотя и наиболее важная), и поэтому она в принципе не может заменить все остальные виды частных политик; например, проблемы, связанные с побочными электромагнитными излучениями и наводками (ПЭМИН), не могут быть естественным образом уложены в рамки контроля доступа. Отметим, однако, что многие другие частные политики действительно нацелены на поддержку политики управления доступом, и, прежде всего, политика учетных записей, политика идентификации и аутентификации, политика парольной защиты и др.

Международным аналогом Оранжевой книги является стандарт ISO/IEC 15408, опубликованный в 2005 году. Этот стандарт ратифицировали множество стран, включая Россию.

Однако, несмотря на указанные аргументы, проблема контроля доступа (к информационным ресурсам, объектам и системам обработки данных, другим компонентам системы обработки данных) является ключевой в процессе обеспечения информационной безопасности (ИБ), и большинство других частных политик в значительной степени нацелены на эффективную поддержку системы контроля и управления доступом.

Применительно к информационной среде вместо сочетания «контроль доступа» используется понятие «разграничение доступа». Однако для того, чтобы охватить все проблемы, связанные с доступом, в рамках единого подхода, как к информационной среде, так и к физической среде используется сочетание «контроль и управление доступом» (КД) — данная фраза достаточно точно передает содержание процедуры доступа. Укажем, что контроль доступа представляет собой выполнение всех предписанных

действий и мероприятий, связанных с обеспечением доступа в соответствии с заданной политикой КУД, а управление предполагает наличие механизмов адекватного реагирования на ситуации, связанные с возможным нарушением процедуры доступа, которые не были предусмотрены в выбранной политике КД. Например, актуальными стали угрозы, которые ранее таковыми не являлись и поэтому не были охвачены политикой информационной безопасности.

Опишем более детально содержание политики контроля и управления доступом (КД). Назначение: политика КД определяет правила предоставления сотрудникам доступа к защищаемым ВС.

Основные положения политики КД следующие. К работе с информационным ресурсом ограниченного доступа допускаются пользователи, ознакомленные с правилами работы с этим ресурсом и наделенные ответственностью за нарушение указанных правил. Каждому сотруднику Организации, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в информационной системе (ИС). В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими субъектам при работе с ВС и того же имени пользователя («группового имени») запрещено.

Для полноты определения необходимо описать основные действия (процедуры), которые могут совершаться с учетными записями (УЗ). Основными являются следующие процедуры: 1) создание УЗ; 2) удаление УЗ; 3) продление УЗ; 4) внесение изменений в УЗ; 5) хранение документов, на основе которых были выполнены определенные действия с УЗ.

Процедура создания УЗ, то есть регистрации пользователя, а также продления срока действия УЗ или внесения изменений пользователя инициируется заявкой. В заявке необходимо наличие идентифицирующей ин-

формации лица, подавшего заявку, и основание для выполнения соответствующего действия с УЗ. Заявка должна быть верифицирована руководителем структурного подразделения, наделенного полномочиями на предоставление подобной заявки на основе принятой политики безопасности. Заявка согласуется с администратором информационной в том числе и по регламентным ограничениям для данной УЗ. Исполнителем заявки является системный администратор. По окончании регистрации УЗ в заявке делается отметка о выполнении задания за подписями исполнителей.

При наступлении момента прекращения срока действия полномочий пользователя УЗ должна немедленно блокироваться. В заявке наряду с идентифицирующей информацией приводится основание, порождающее необходимость прекращения срока действия полномочий пользователя. Заявка согласуется с системой ИБ и передается на исполнение системному администратору.

Все исполненные заявки передаются ответственному сотруднику архива на основе установленной процедуры и хранятся в архиве в течение периода времени, зафиксированного в политике информационной безопасности. Копии исполненных заявок хранятся у системного администратора для выполнения определенных действий в аварийных и нетиповых ситуациях, а также в контрольных целях.

Применительно к системам обработки данных проблема контроля доступа сводится, прежде всего, к контролю доступа к различным информационным системам: операционной системе, базам данных, системе электронного документооборота и др., к техническим средствам обработки данных и к другим объектам систем обработки данных ВС. Наиболее важной из информационных систем с точки зрения обеспечения ИБ является операционная система, установленная на компьютерных системах объекта защиты, а также на других корпоративных средствах связи обработки данных — прежде всего, на мобильных устройствах связи.

В последние десятилетия данная проблема еще более обострилась в связи с интенсивным развитием интернета, что привело к появлению большого числа новых видов угроз — сетевых угроз. Эти виды угроз оказались существенно более опасными, что породило большой всплеск в развитии различных средств и механизмов сетевой защиты компьютерных систем. Политическая общественность многих стран остро ставит вопрос об обеспечении полного государственного контроля над сетевыми трафиками национального уровня, разработке своих программно-аппаратных средств обработки данных.

Таким образом, объектами доступа, представляющими интерес для злоумышленных действий, являются информационные системы объекта защиты, технические средства обработки данных, а также непосредственно процессы обработки данных.

2.3. Модель обеспечения гарантированного качества предоставления сервисов при организации контроля доступа

Для эффективности системы обеспечения КД в качестве целевых показателей предлагается использовать стохастические методы — использование величины, равной сумме среднего значения этого фактора и его среднеквадратического отклонения. Данный подход позволяет оценить средние ожидаемые значения оцениваемых характеристик, значения которых должны лежать в диапазоне, заданном технико-экономическими требованиями к условиям функционирования системы, то есть обеспечивать гарантированное значение качества обслуживания (Quality-of-Service, QoS) [180].

Среди различных направлений повышения эффективности процесса обеспечения контроля доступа важное место занимают различные методы,

связанные с созданием проблем и препятствий несанкционированному доступу и обеспечением целостности ВК [181]. Средства, обеспечивающие повышение эффективности контроля доступа к ВК, назовем средствами противодействия (СП) [100]. Эти средства могут включать аппаратные, программные, организационные средства, обеспечивающие целостность и контроль доступа к данным, вычислительным ресурсам и объектам инфраструктуры ВК. Каждое из этих действий и мероприятий характеризуется определенными затратами на создание и поддержку в работоспособном состоянии, с одной стороны, а, с другой, определенной вероятностью (коэффициентом) воспрепятствования злоумышленному действию [182]. Встает задача выбора состава СП, который бы в наибольшей степени уменьшал вероятность возможного перерастания угрозы целостности или несанкционированного доступа в противоправные действия с ВК.

Под управлением понимается такое воздействие на показатели ВК, результатом которого будут запланированные (желаемые) изменения показателей эффективности в течение заданного регламентного периода времени.

В процессе реализации управления ВК необходимо также решить ряд сопутствующих задач:

1. Оценить степень и характер влияния показателей отдельных ВК и их определенной совокупности на показатели угроз.
2. Оценить требуемые объемы затраты средств на предполагаемые изменения показателей ВК.
3. Сформировать процедуру выбора наиболее приемлемого варианта в систему управления ВК.
4. Сформировать конкретные механизмы вложения средств в реализацию выбранного варианта управления ВК.
5. Оценить эффективность и результативность выбранного варианта управления ВК как по текущим и конечным результатам, так и непосред-

ственно по показателям процесса реализации выбранных элементов управляющих воздействий.

Построим формальную модель для взаимосвязи показателей ВК и показателей угроз с учетом объемов ресурсов, используемых для повышения уровня показателей ВК. Для этого сформулируем ряд положений.

1. Для более адекватной оценки влияния средств противодействия на изменения стабильности функционирования ВК в целом, целесообразно *дифференцировать* на классы и уровни вычислительной архитектуры.

2. Особенностью влияния на целостность и надежность ВК является перманентный, долговременный характер негативного влияния, так как практически все показатели нарушения целостности формируются в результате *кумулятивного* (суммарного) *накопления* воздействий и условий.

3. Одним из важных технологических показателей, характеризующих взаимосвязь и взаимозависимость между различными парами показателей в системе управления ВК, является *коэффициент эластичности*, показывающий, на сколько процентов изменится данный показатель угроз при увеличении значения заданного показателя ВК на 1% при заданном конкретном значении показателя ВК. В рассматриваемом случае коэффициент эластичности характеризует, на сколько процентов увеличиваются значения вероятности перерастания угрозы в опасную ситуацию и величины возможного ущерба при увеличении величины конкретного показателя заданного СП на 1%. Коэффициент эластичности описывает уменьшение вероятности возможного несанкционированного проникновения в систему при использовании заданного ВК с заданными параметрами и затраты на указанное ВК в течение регламентного промежутка времени.

Применительно ко многим показателям ВК есть определенные основания считать, что коэффициент эластичности не является константой, а описывается очень медленно убывающей функцией [183], что обусловлено, в частности, тем, что, начиная с некоторого уровня, наступает ситуация

«насыщения» для конкретной угрозы пассивными средствами противодействия, когда дальнейшее совершенствование ПСП оказывает все меньшее влияние на показатели.

Построим стохастическую модель [183]. Наряду со значением коэффициента эластичности, равного константе, также рассматривается случай, когда коэффициент эластичности $e(x)$ зависимости между конкретными показателями угроз и средств противодействия задается функцией вида: $e(x) = a - b(\ln(c + x))^{-\alpha}$, которая при подходящем выборе всех параметров принимает только положительные значения и очень медленно убывает при $x \rightarrow \infty$, где x — текущее значение рассматриваемого показателя средств противодействия; а $a > 0$, $b \geq 0$, $c \geq 0$ и $\alpha > 0$. Тогда, если $p(x)$ есть абсолютное значение рассматриваемого показателя угроз (вероятности ее реализации), то, исходя из определения эластичности, можно записать следующее равенство:

$$e(x) = \left(\frac{dp(x)}{p(x)} \right) / \left(\frac{dx}{x} \right) = a - b(\ln(c + x))^{-\alpha},$$

откуда получаем следующее дифференциальное уравнение с разделяющимися переменными для нахождения $p(x)$:

$$\frac{dp(x)}{p(x)} = \left(a - b \frac{1}{(\ln(c + x))^\alpha} \right) \frac{dx}{x}.$$

Отсюда после интегрирования обеих частей получаем соотношение:

$$\ln p(x) = a \int_0^x \frac{dx}{x} - b \int_0^x \frac{1}{(\ln(c + x))^\alpha} \frac{dx}{x} \quad \text{и}$$

$$p(x) = x^a \exp \left\{ -b \int_0^x \frac{1}{(\ln(c + x))^\alpha} \frac{dx}{x} \right\}.$$

При больших значениях x константа c становится несущественной: $\ln(x + c) \sim \ln x$.

Тогда

$$\int_0^x \frac{1}{(\ln(c+x))^\alpha} \frac{dx}{x} \sim \int_\tau^x \frac{1}{(\ln x)^\alpha} \frac{dx}{x} = \int_\tau^x \frac{d \ln x}{(\ln x)^\alpha} \sim \frac{(\ln x)^{1-\alpha}}{1-\alpha} + K_0, \text{ если } \alpha \neq 1,$$

и аналогично

$$\int_0^x \frac{1}{(\ln(c+x))^\alpha} \frac{dx}{x} \sim \ln \ln x + K_0, \text{ если } \alpha = 1,$$

где $\tau > 1$ — любая константа, K_0 — константа. С учетом последних соотношений примем ($\alpha \geq 0$):

$$p(x) = p(x, \alpha) = \begin{cases} K x^a \exp(-B(\ln(x+\tau))^{1-\alpha}), & \text{если } \alpha \neq 1, \\ K x^a (\ln(x+\tau))^{-b}, & \text{если } \alpha = 1. \end{cases} \quad (2.1)$$

Здесь коэффициент τ обеспечивает конечность и положительность функции $p(x)$ при малых значениях x ; $K = \exp(K_0)$; $B = b(1-\alpha)^{-1}$. Коэффициент K определяет абсолютное значение функции $p(x)$, являясь также масштабным коэффициентом, то есть зависит от единицы (шкалы) измерения. Параметр a определяет характер поведения функции $p(x)$ при больших значениях x , а также одновременно с параметром b определяет степень чувствительности $p(x)$ по отношению к изменению значения x , т. е. значения соответствующего показателя ВК. Наконец, параметр α описывает степень замедления «отдачи», т. е. уменьшения величины роста показателя угрозы при увеличении значения показателя ПСП. Задача оценки значений этих параметров обсуждается ниже.

Заметим, что при $\alpha = 1$ и $b = 0$ эластичность $e(x)$ постоянна и зависимость изменения абсолютной величины данного показателя угроз от рассматриваемого показателя ПСП линейна.

4. Для каждого уровня архитектуры ВК *типичны* свои функции $p(x)$, описывающие зависимость показателей угроз от объема затраченных ресурсов, вкладываемых в повышение показателей ВК.

Приведенные выше соотношения необходимы, прежде всего, для решения задачи *управления качеством обеспечения контроля доступа* с целью обеспечения снижения показателей угроз [99, 166]. Для решения последней задачи необходимо сформировать целевую функцию, которая должна характеризовать величину, на которую уменьшатся показатели угрозы при конкретном варианте распределения средств на повышение показателей ВК для различных видов ВК, а также дать формализованное описание задачи. Опишем возможную постановку задачи распределения средств на совершенствование СП с целью снижения показателей угроз.

Пусть для данного конкретного вида ВК, имеющего номер k , на повышение значение его i -го показателя средств противодействия необходимо затратить ресурсы в объеме $x_i(k)$; $p_j(\bar{x}(k)) = p_{ij}(\bar{x}(k); k)$ — изменение j -го показателя угроз при вложении ресурсов в объеме $x_i = x_i(k)$ в повышение значения j -го показателя k -го вида ПСП и $\bar{x}(k) = (x_1(k); x_2(k); \dots; x_{20}(k))$; S — общий объем ресурсов, выделенных на повышение угроз путем изменения показателей качества разных видов продукции. Тогда значение j -го показателя угроз L_j после реализации вложенных средств равно ($j = \overline{1, M}$):

$$L_j(x_i(k), i = \overline{1, M}, k = \overline{1; K_{np}}) = \sum_{k=1}^{K_{np}} p_j(\bar{x}(k), k),$$

где K_{np} — общее число видов ВК, приведенное в перечне видов ВК. В этом случае в качестве целевой функции можно взять функцию:

$$\begin{aligned} L(x_i(k), i = \overline{1; M}, k = \overline{1; K_{np}}) = \\ = \sum_{j=1}^M v_j L_j(x_i(k), i = \overline{1; M}, k = \overline{1; K_{np}}) = \sum_{j=1}^M \sum_{k=1}^{K_{np}} v_j p_j(\bar{x}(k), k), \end{aligned} \quad (2.2)$$

где v_j — оценка степени важности j -го показателя угроз в системе всех угроз объекту защиты.

При этом выполнены следующие дополнительные ограничения:

$$\sum_{i=1}^M \sum_{k=1}^{K_{np}} x_i(k) \leq S, \quad x_i(k) \geq 0 \quad \text{для всех } i \text{ и } k \quad (2.3)$$

Таким образом, решение задачи нахождения максимального значения функции $L()$, приведенной в (2.2), при условии выполнения ограничения (2.3) позволит найти оптимальный вариант распределения ресурсов для снижения показателей угроз путем повышения эффективности ВК.

Существующие процедуры и методики оценки показателей информационной безопасности обычно опираются либо на усредненные значения исходных характеристик, определяющих состояние информационной безопасности на объекте защиты, либо на их экстремальные значения — особенно, в случае критических систем безопасности. В первом случае получающиеся при этом конечные оценки показателей безопасности носят усредненный характер. При использовании усредненных оценок данный подход может не обеспечивать адекватности поведения системы защиты в случае возможности появления больших всплесков значений отдельных факторов, способных оказать значимое влияние на процессы возникновения атак и противодействия им — назовем эти факторы сопутствующими. При использовании экстремальных показателей часто конечные оценки показателей безопасности могут быть слишком избыточными, порождая необходимость значительных дополнительных затрат, которые практически мало влияют на изменение уровня обеспечения безопасности. Назовем используемые значения рассматриваемых показателей целевыми, поскольку они предназначены и востребованы в качестве параметров, которые используются в процессе анализа состояния системы безопасности и формирования политики безопасности, при выборе варианта совершенствования системы безопасности, построении интегральных характеристик систем обеспечения информационной безопасности, при оптимизации структуры

построения и технологии функционирования системы безопасности. Таким образом, оба подхода (на основе средних и экстремальных значений) к выбору целевых показателей имеют серьезные недостатки. В первом случае происходит недооценка уровня опасности при определенных реально возможных значениях факторов, влияющих на безопасность и имеющих значительные отклонения от средних значений, а во втором случае — избыточность и связанные с ней дополнительные затраты, причем эти затраты тем значимее, чем больше разница между средними и экстремальными значениями показателей, характеризующих факторы.

С точки зрения эффективности системы обеспечения информационной безопасности целесообразно использовать адаптивные оценки отдельных факторов, если имеется такая возможность [184, 185]. Если же нет возможности адаптивно оценить требуемые целевые параметры для сопутствующих факторов (например, ввиду большого числа этих факторов), то в качестве целевых показателей предлагается использовать для каждого из требуемых параметров в случае абсолютных их значений, по аналогии с методами стохастической оптимизации, величины, равные сумме среднего значения этого фактора и его среднеквадратического отклонения. Приведем соответствующие соотношения. Пусть p — оцениваемый целевой параметр системы, имеющий абсолютное измерение (например, средняя величина промежутка времени до ближайшей атаки на ВК, величина ожидаемого ущерба); $p_1, p_2, \dots, p_n$ — набор статистических наблюдений либо экспертных данных по параметру p , где n — число наблюдений или экспертных оценок. Тогда средние значения $p_{\text{ср}}$ целевого показателя p_i , его экстремальное значение $p_{\text{э}}$ равны соответственно

$$p_{\text{ср}} = \frac{1}{n} \sum_{i=1}^n p_i, \quad p_{\text{э}} = \max\{p_i; 1 \leq i \leq n\}.$$

Вместо $p_{\text{ср}}$ и $p_{\text{э}}$ предлагается использовать значение $p_{\text{г}}$, которое в определенной степени дает гарантию учета и значительной части всплесков значений параметра p :

$$p_{\text{г}} = p_{\text{ср}} + \sigma_p, \sigma_p = \sqrt{\frac{1}{n} \sum_{i=1}^n (p_i - p_{\text{ср}})^2}. \quad (2.4)$$

В случае же использования относительных (безразмерных) показателей (например, вероятности $p_{\text{усп}}$ успешного противодействия атаки либо желаемого изменения сопутствующего фактора в течение заданного регламентного промежутка времени T) указанный подход при использовании соотношений (2.4) неприемлем, поскольку при определенных значениях значений p_i значение вероятности $p_{\text{усп}}$ может оказаться больше единицы. Для получения в случае относительных целевых показателей оценки, аналогичной (1), можно поступить следующим образом (продемонстрируем процедуру на пример одного из наиболее важных показателей — вероятности $p_{\text{усп}}$). Часто при оценке вероятности $p_{\text{усп}}$ предполагают, что имеет место следующая зависимость указанной вероятности от интенсивности λ_p атак:

$$p_{\text{усп}} = C(\lambda_p, T) \cdot \exp\{-K(\lambda_p, T)\lambda_p T\}, \quad (2.5)$$

где $C(\lambda_p, T)$, $K(\lambda_p, T)$ — некоторые ограниченные функции. Так как при отсутствии атак (то есть при $\lambda_p = 0$) очевидно $p_{\text{усп}} = 1$, то из (2.5) вытекает $C(\lambda_p, T) = 1$. Далее, хотя функция $K(\lambda_p, T)$, вообще говоря, не является константой — она зависит от параметров конкретных средств противодействия, используемых в системе, часто при проведении общего анализа системы, не привязанного к конкретным средствам противодействия, принимают $K(\lambda_p, T) = K$ постоянным. Отметим, что K характеризует степень эффективности использования имеющихся средств противодействия ата-

кам на информационные ресурсы или другие ценности на основе использования имеющихся в системе безопасности средств противодействия. Тогда, предполагая, что соотношение (2.5) справедливо для каждого отдельного наблюдения $p_i (i = \overline{1; n})$, из (2.5) получаем соотношение:

$$\lambda_{p,i} = -\frac{1}{KT} \ln(p_i).$$

По аналогии с (2.4), заменяя текущие интенсивности $\lambda_{p,i}$ их гарантированными оценками $\lambda_{p,\Gamma} = \overline{\lambda_p} + \sigma_\lambda$, получаем следующую гарантированную оценку p_Γ для вероятности успешного противодействия атакам:

$$p_\Gamma = \exp\{-K\lambda_{p,\Gamma}T\}, \lambda_{p,\Gamma} = \overline{\lambda_p} + \sigma_\lambda, \\ \overline{\lambda_p} = \frac{1}{n} \sum_{i=1}^n \lambda_{p,i}, \sigma_\lambda = \sqrt{\frac{1}{n} \sum_{i=1}^n (\lambda_{p,i} - \overline{\lambda_p})^2}. \quad (2.6)$$

Отметим, в оценках (2.5) и (2.6) для увеличения доли атак, которые успешно нейтрализованы с помощью имеющихся средств противодействия, значения вторых слагаемых σ_p и σ_λ могут быть увеличены путем введения множителей больших единицы, то есть использования слагаемых $\mu\sigma_p$ и $\mu\sigma_\lambda$, $\mu > 1$ — константа. В частности, при $\mu = 3$ и предположении о нормальном законе распределения оценок p_i по закону «трех сигм» для нормального закона, выводим, что для 99,7% всех атак значения вероятностей успешного противодействия этим атакам будут меньше p_Γ .

2.4. Особенности использования методов моделирования в системах контроля доступа

Рассмотрим методы математического обеспечения гарантированного качества КД. При решении задач анализа, каковыми являются и рассматриваемые задачи гарантий, могут быть использованы логико-аналитические, эмпирико-статистические или экспертные методы. Эмпирико-статистические методы опираются на опыт практического использования или эксплуатации системы (в нашем случае — системы КД). Однако даже при очень длительном и большом опыте работы системы безопасности нет абсолютных гарантий того, что в какой-то момент не будет найден новый метод преодоления системы КД. Поэтому, эмпирико-статистические методы не могут являться основой получения гарантий безопасности в будущем. Еще менее убедительны экспертные методы в задаче получения гарантий безопасности. Поэтому, единственным способом, позволяющим обеспечить получение гарантий безопасности в будущем, является использование логико-аналитических методов. Сам метод получения гарантий представляет собой строгое математическое доказательство того, что в рамках некоторой формализованной модели, описывающей политику КД, при соблюдении требований этой политики в каждый момент времени не будут нарушены правила и требования, установленные в системе КД. Таким образом, для получения гарантий безопасности по выполнению требований политики КД в любой момент времени в будущем необходимо формирование политики КД на основе формализованной модели, в рамках которой доказана невозможность несанкционированного преодоления системы КД в любой момент в будущем при условии, что все требования заложенные в формализованную модель и в построенную на ее основе политику КД выполняются.

В рамках субъектно-объектного подхода к построению системы КД, о котором говорилось в разделе 2.1, были выделены три основных компонента:

- множество субъектов S , которые могут получить доступ к программно-аппаратным ресурсам системы обработки данных;
- множество объектов O системы обработки данных (информационных ресурсов и данных, программных средств, аппаратно-технических устройств), которые могут являться предметом действий хотя бы одного субъекта из S ;
- множество прав доступа $D = \{d(s,o)\}$ (то есть набор видов доступа) для каждой пары (s, o) , $s \in S$, $o \in O$, причем каждое из этих прав может иметь временные ограничения; например, может быть запрещено чтение определенных данных в нерабочее и отпускное время.

Отметим, что множества S и O , вообще говоря, пересекаются. Например, некоторая исполняемая программа может запускаться или модифицироваться другим приложением (в частности, троянской или вирусной программой)

Таким образом, формализованная модель субъектно-объектной модели в своей минимальной конфигурации представляет собой тройку множеств $\{S, O, D\}$. Конкретный формализованный язык описания компонентов может быть самый разный [173, 174]: теория графов (модель «Take-Grand»), вероятностные (модель информационных потоков), теории автоматов (автоматная модель), и т. д.

Однако формализованное описание процесса доступа на основе модели $\{S, O, D\}$ во многих случаях затруднительно, прежде всего, ввиду того, что описание каждой связи из D является достаточно громоздким — необходимо перечислить все условия реализации этой связи и все ограни-

чения, которые с ней связаны. Поэтому целесообразно детализировать формализованную модель следующим образом. Примем, что D описывает только перечень видов доступа для каждой пары «объект-субъект». Далее, добавим в модель множества R, C для каждой пары «объект-субъект»; то есть $R = \{R(s, o)\}$ и $C = \{C(s, o)\}$, где для субъекта s и объекта o выражения $R(s, o)$ и $C(s, o)$ содержат перечисление ограничений и условий доступа субъекта s к объекту o соответственно. Здесь под ограничением понимается требование, которое накладывается на процесс доступа к данным изначально (по времени доступа, по рабочим станциям и IP-адресам, по рабочим возможностям), а условие – это ограничения на процесс доступа к данным, которые зависят непосредственно от процесса обработки данных и которые могут вызвать изменение возможностей доступа субъекта к объекту уже в процессе обработки. Условия могут быть привязаны к внешним условиям на текущий момент работы, к состоянию системы обработки данных и системы обеспечения ИБ.

Наконец, представляет интерес также указание на тот набор действий A (методов, способов и технологий), которые могут применяться в системе для установления и изменения возможностей доступа субъекта к объекту, причем состав этих действий может быть привязан также индивидуально к каждой паре «субъект-объект» (например, действие «блокировать процесс» применимо не ко всем возможным процессам или физическим субъектам. Особенно важен этот набор в процессе проектирования или модификации системы КД. Мы предполагаем, что A не зависит от субъектов и объектов, к которым конкретные действия применяются. Отметим, что множество A включает, в частности, возможные методы, способы и технологии противодействия угрозам и атакам.

Таким образом, исходя из вышесказанного, формализованная модель доступа M может быть представлена в виде набора из пяти компонентов: $M = \{S, O, D, R, C, A\}$. Конкретное содержание каждого из компонентов

модели привязано к конкретному объекту защиты и требованиям по ИБ, а также к принятой политике безопасности, если таковая есть на объекте защиты. Содержание и наполнение первых пяти компонентов модели в целом не вызывает проблем. Более подробно рассмотрим содержание последнего компонента — множества действий А.

Для систематизации всех возможных действий выделим, прежде всего, показатели систематизации. Имеется большой набор возможных показателей классификации; в работе предлагаются следующие четыре как наиболее важные с точки зрения КД.

1. *Класс средств, к которому принадлежит данное действие.* Класс определяется типом средств и связанных с ними действий, которые относительно похожи для всех средств и действий из одного класса.

Выделяют следующие классы средств по обеспечению информационной безопасности, в том числе и КД:

- 1) программные;
- 2) аппаратные;
- 3) организационные;
- 4) технические;
- 5) правовые;
- 6) криптографические;
- 7) инженерные;
- 8) морально-этические.

Некоторые пояснения:

- а) различие аппаратных и технических средств состоит в том, что аппаратные средства функционируют только тогда, когда работает система обработки данных (например, платы контроля доступа), а технические функционируют всегда вне зависимости от того, работает или нет система обработки данных;

- б) поскольку в настоящее время граница между программными и аппаратными средствами достаточно относительная (аппаратные средства могут быть реализованы программно и, наоборот, многие программные средства допускают аппаратную реализацию), то часто их объединяют в одну группу программно-аппаратных средств;
- в) организационные средства занимают промежуточное положение между техническими и правовыми средствами, поэтому их часто объединяют в один класс либо с техническими (и говорят об организационно-технических средствах), либо с правовыми (и говорят об организационно-правовых средствах).

2. Среда действия.

Различают следующие основные среды воздействия на процесс КД:

- 1) информационная среда (посредством глобальных и локальных сетей, рабочих станций);
- 2) физические средства, например, посредством хищения или повреждения средств обработки и носителей информации;
- 3) электромагнитные средства, связанные с утечкой информации;
- 4) правовая среда, связанная, прежде всего, с изменениями прав собственности на определенные данные.

3. Режим воздействия.

Принципиально различают два основных режима воздействия:

- 1) оперативный режим, когда воздействие фактора происходит непосредственно в процессе функционирования системы обработки данных;
- 2) плановый режим, когда воздействие фактора может произойти в будущем и поэтому предпринимаются определенные превентивные действия для предотвращения (или, наоборот, усиления) этого воздействия или уменьшения (увеличения) последствий и результатов воздействия фактора.

Планируемый режим часто делят на следующие более частные режимы с учетом временных промежутков реализации превентивных мер:

- а) стратегический;
- б) долгосрочный;
- в) среднесрочный;
- г) краткосрочный;
- е) годовой;
- ж) квартальный;
- з) месячный;
- и) недельный;
- к) дневной;
- л) текущий.

Отметим, что разница между стратегическим и долгосрочным режимами может быть лаконично выражена в следующей фразе: стратегический режим — это взгляд из будущего в настоящее, а долгосрочный — это взгляд из настоящего в будущее.

4. Характер действий по ее нацеленности.

Выделим следующие виды действий по их характеру в процессе КД:

- 1) авторизация субъекта/объекта в системе КД, то есть предъявление пользователем своих индивидуальных атрибутов для получения доступа и проверка системой наличия этих атрибутов в списке субъектов;
- 2) идентификация — проверка наличия у субъекта атрибутов, подтверждающих (или доказывающих в случае аутентификации) в соответствие атрибутов авторизации непосредственно субъекту, которому принадлежат эти атрибуты;
- 3) регламентирование — установление определенных ограничений для вида из разрешенных видов доступа по процедуре доступа субъекта к объекту;

- 4) контролирование — ведение контроля работы субъекта в системе по заданному фиксированному набору характеристик;
- 5) сопровождение — непрерывное отслеживание работы субъекта в системе обработки данных;
- 6) ограничение — установление определенных требований, связанных с процессом работы субъекта в системе обработки данных;
- 7) разделение и разграничение — определение порядка доступа субъектов к ресурсам системы обработки данных и ограничение возможностей их работы в системе с целью максимально полного изолирования процессов, связанных с работой пользователей в системе обработки данных;
- 8) обнаружение несанкционированных действий — выявление событий, сущностей или состояний, нарушающих установленные требования и ограничения по обработке данных;
- 9) информирование — передача информации заданному установленному составу субъектов в соответствии с установленным политикой безопасности регламентом (прежде всего, оповещение всех ответственных лиц в случае возникновения нестандартных, в частности, чрезвычайных ситуаций или событий;
- 10) локализация зоны проявления негативного воздействия — выявление возможной зоны нахождения источника негативного воздействия (шпионской программы, злоумышленника и т.п.) и максимально возможное ограничение взаимодействия всех процессов в системе обработки данных с теми из них, которые активизированы в этой зоне;
- 11) изолирование источника негативного воздействия (в частности, злоумышленника) — создание препятствий для субъектов и процессов, находящихся в зоне локализации, по проникновению в ча-

сти системы обработки данных, находящихся вне зоны локализации;

- 12) блокирование — создание условий в системе обработки данных, при которых источник негативного воздействия не имеет возможности совершать сколько-нибудь значимые действия в системе обработки данных;
- 13) нейтрализация источника негативного воздействия — проведение действий и мероприятий, после завершения которых источник негативного воздействия окажется неспособным совершать какие-либо действия;
- 14) прекращение работы системы обработки данных или ее отдельных компонентов — немедленное завершение процессов в системе обработки данных (например, в случае наличия серьезных оснований для предположения о злоумышленном проникновении в систему либо при возникновении чрезвычайных ситуаций);
- 15) проверка состояния компонентов — перманентный (то есть с заданной периодичностью либо на основе заданной процедуры проверки) контроль и аудит состояния всех компонентов системы обработки данных и системы обеспечения информационной безопасности;
- 16) журнализация — ведение журнала, в котором записываются все события, происходящие в системе обработки данных в процессе работы системы, по заданной совокупности параметров и в соответствии с установленным форматом;
- 17) анализ — формирование перечня проблем и задач по обеспечению ИБ, подлежащих решению, на основе изучения и осмысления всех источников, отражающих процессы обработки данных и обеспечения информационной безопасности в системе (в частности, журналов событий и обеспечения ИБ);

- 18) сигнализация — активизация технических и программно-аппаратных средств немедленного оповещения всех лиц в зоне контроля при возникновении опасных ситуаций.

Сочетание отдельных значений каждого из перечисленных четырех параметров порождает одно из возможных действий или мероприятий, требующих комплексного обеспечения доступа, где под словом «комплексный» понимается наличие в системе механизмов реализации действий для любой возможной ситуации, связанной с нарушением установленного режима обработки данных.

2.5. Технологии построения и развития SIEM-систем

Теоретически работу SIEM-системы можно описать достаточно просто: сбор информации; предварительный анализ (в случае опасности появляется предупреждение); размещение информации в базах данных; анализ поведения с учетом предыдущих наблюдений (появляется предупреждение). Что же касается практики, то система функционирует посредством следующих составляющих:

- агенты (собирают из различных ресурсов информацию);
- серверы-коллекторы (накапливают информацию, собранную агентами);
- сервер баз данных (осуществляет хранение информации);
- сервер-коррелятор (анализирует информацию).

На вход SIEM-системы может подаваться практически произвольная информация, важна форма ее подачи. Агенты, собирающие данные, — это некоторая программа, собирающая локально журналы событий и передающая, если это возможно, журналы на сервер. Чтобы «прочитать» источники данных, агенты применяют коллекторы — это библиотеки для понима-

ния информации в конкретных журналах или в системе. Коллекторы имеют большое значение, поскольку в разных источниках одно событие может именоваться по-разному. Именно коллекторы дают возможность собрать и понять эти события.

В том случае, если у источника нет коллектора, то можно пытаться отправлять события как SYSLOG (если источник умеет делать это), но здесь возможно возникновение «проблемы синонимов» и необходимости создавать дополнительный обработчик для сведения информации к единому формату.

Помимо этого, возможен удаленный сбор информации с использованием соединения по протоколам FTP, RPC, SMB/CIFS. Но в таком случае не исключено возникновение проблем с перегруженностью сети, поскольку некоторые системы не дают возможности передачи только последних записей, а передают журнал полностью,

Источники информации, которые могут использовать SIEM-системы:

- Access Control и Authentication — используются для мониторинга контроля доступа к ИС и применения привилегий;
- IDS/IPS-системы — получают сведения о кибератаках, изменениях доступа к устройствам и конфигурации;
- DLP-системы — используются для получения сведений о попытках нарушения прав доступа и инсайдерских утечках данных;
- антивирусное ПО — формирует сообщения о работоспособности программных средств, изменении политик и конфигураций, базах данных, вредоносном ПО;
- межсетевые экраны — предоставляют сведения о вредоносном коде, атаках и т. д.;
- сетевое активное оборудование — применяется для учета сетевого трафика и контроля доступа;

- журналы событий рабочих станций и серверного оборудования — используются с целью контроля доступа, соответствия политике информационной безопасности, а также обеспечения непрерывности;
- сканеры защищенности (уязвимостей) — сбор информации об инвентаризации сервисов, ИТ-активов, ПО, уязвимостей, предоставление полученных данных, а также топологической структуры;
- системы веб-фильтрации — аккумулируют и предоставляют информацию о посещении персоналом организации запрещенных или подозрительных веб-сайтов;
- системы инвентаризации и Asset-Management — предоставление информации для контроля ИТ-активов в инфраструктуре и обнаружения новых активов.

После получения информации SIEM-система может выполнить ее анализ с помощью математических и статистических методов. При этом, в качестве отправной точки используются правила, заданные вручную. Например, событие «login failed», произошедшее только один раз, не вызывает опасений. Но если это событие для одной и той же учетной записи повторяется не меньше трех раз, то это может указывать на попытки подобрать пароль.

В простейшем случае в SIEM-системах правила представлены в формате Rule Based Reasoning (RBR) и включают в себя некоторую совокупность условий, счетчики, триггеры, возможные сценарии. К примеру, эти правила могут выявить мошенничество в случае удаленности друг от друга двух последних местоположений использования платежного средства за небольшой временной интервал: если в 20.00 банковской картой оплачивали покупку в супермаркете в Твери, а через полчаса с этой карты снимают крупную сумму в Париже, то мошенничество очевидно.

Обобщенная схема применения входных данных при процессе корреляции в SIEM-средствах приведена на рис. 2.2.

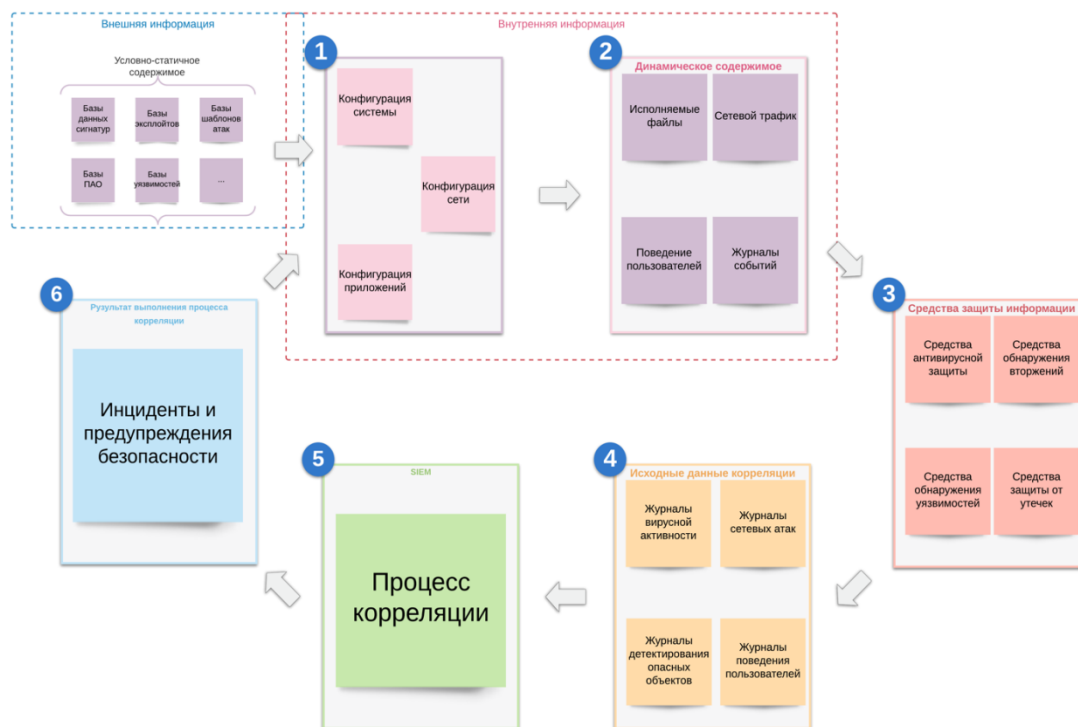


Рисунок 2.2 — Обобщенная схема процесса корреляции в SIEM

Среди возможностей SIEM-систем следует перечислить способность к выявлению: крупных вирусных атак; вирусных заражений; атак во внешнем и внутреннем сетевых периметрах; уязвимостей; сбоев и ошибок в работе ИС; ошибок конфигурации в ИС и средствах защиты; попыток несанкционированного доступа к информации; случаев мошенничества.

Корреляцию событий понимают как поиск общих атрибутов у событий и, на основе этого, объединение событий в кластеры. В SIEM-системах корреляция событий является процессом исследования большого числа событий, после чего некоторые из событий отбрасываются. Далее анализируется отношение типа «причина — эффект» для оставшихся событий с выделением сигналов о тревоге из набора связанных событий или идентификацией события, которое стало причиной появления неисправности.

В SIEM-системах корреляция событий реализована и для обнаружения инцидентов безопасности, и для их исследования, так, чтобы в дальнейшем была возможность восстановления порядка действий злоумышленника, инициирующего инцидент и расширения базы знаний информацией о событиях, вызывающих инцидент безопасности или о новых векторах атак. Этот подход дает возможность в последующем выявлять атаки уже на ранних стадиях, что влияет положительно на уровень безопасности. Существует подход [25] к разделению существующих методов корреляции на: сигнатурные (для определения инцидентов задаются правила); бессигнатурные (используется обучение SIEM-продукта на некоторых наборах данных).

Наиболее широко распространены следующие методы корреляции [25, 27, 35, 186]:

- статистический (statistical correlation);
- построение корреляционной матрицы;
- метод моделирования;
- корреляция с помощью заданных правил (rule-based);
- байесовский подход;
- использование нейронных сетей;
- построение графа зависимостей.

Статистический метод является бессигнатурным методом, при реализации которого вычисляется степень статистической связи между событиями.

Использование метода корреляционной матрицы предполагает, что по матрице событий выявляется соответствующий вектор. В матрице событий содержится информация о степени связей между событиями: вектору событий ($P1$, $P2$) соответствует определенное числовое значение, которое находится в этой матрице на пересечении строки $P1$ и столбца $P2$ [98, 187]. Предположим, что события $E2$ и $E3$ — причины проблемы $P1$;

проблема $P2$ является следствием $E1$ и $E2$; событие $E2$ влечет за собой проблему $P3$; события $E1, E2, E3$ — причины возникновения $P4$. Соответствующая матрица корреляции будет иметь вид (рис. 2.3):

	$P1$	$P2$	$P3$	$P4$
$E1$	0	1	0	1
$E2$	1	1	1	1
$E3$	1	0	0	1

Рисунок 2.3 — Пример матрицы корреляции

Если есть зависимость появления события от причины, то в соответствующей ячейке матрицы находится единица, в противном случае — ноль. Если появляются два события, то выбирают вектор, имеющий наименьшее расстояние Хэмминга. В [188] указано, что такой вид корреляции — это достаточно быстрый для применения метод, который обладает значительной устойчивостью к помехам и потерянными событиями. Для генерации проблемных векторов могут быть использованы обучающие наборы данных. В то же время этот метод не принимает во внимание данные о свойствах событий и о времени их генерации, т. е. для анализа используется неполное представление ситуации.

При реализации метода моделирования используются виртуальные интеллектуальные модели, которые программно представляют существующие объекты предметной области в системе. Для физических и логических объектов разного рода используются соответствующие типы моделей, которые являются шаблонами для создания моделей существующих объектов. Все типы моделей включают в себя набор атрибутов, поведений и

отношений. При моделировании реальные объекты распознаются и моделируются, при этом характеристики моделей заполняются реальными данными. После этого в режиме реального времени проводится мониторинг, в процессе которого происходит взаимодействие моделей в соответствии с заранее заданными правилами поведения с целью решения задачи корреляции событий [188].

Метод корреляции с помощью заданных правил основан на обнаружении связей между событиями с использованием predetermined правил, которые, чаще всего задают отношения «условие — действие». Среди достоинств этого метода следует назвать простоту, расширяемость и высокую надежность выявления инцидентов. Недостатки данного метода — это отсутствие возможности автоматического обучения на опыте его использования, а также возможная субъективность правил, которые задает человек.

При использовании байесовского подхода с помощью формулы Байеса, вычисляют вероятность появления некоторого события при условии, что имели место прочие события, взаимосвязанные с данным.

Применение метода, использующего нейронные сети, предусматривает выявление аномалий с использованием результатов обучения сети.

Метод, основанный на построении графа, формирует граф на основе обнаруженных зависимостей, связывающих системные компоненты. Далее граф применяют для обнаружения причины появления инцидента. Этот метод дает возможность выявить вероятную причину появления события, при этом анализ начинается в узлах, где произошли начальные события, а потом происходит поиск узлов, влияющих на появление начальных событий. В случае применения этого подхода при появлении множественных проблем в краткий интервал времени не всегда существует возможность определения всех первопричин событий.

2.6. Анализ требований и условий проектирования архитектуры контроля доступа

Анализ конфигурации вычислительных комплексов показывает, что повышение эффективности функционирования ВК может быть достигнуто за счет встраивания в архитектуру систем контроля доступа на всех уровнях передачи данных. Использование внешних систем и внешних контуров контроля доступа не гарантирует защиту от утечки данных вне встроеного контура на программном или аппаратном уровне. Применение таких систем требует больших ресурсов за счет дополнительных программных модулей и их стыковок с программно-аппаратным обеспечением вычислительных сервисов.

Например, в архитектуре ВК, реализующей многоуровневый контроль доступа на основе концепции SIEM, необходимо реализовать сбор и хранение событий. Сведения о состоянии различных элементов доступа к сервисам и управлению событиями фиксируются обработчиками событий, распределенными по сети на всех уровнях. Каждый из обработчиков событий напрямую подключен к одному или нескольким источникам событий. Каждый из обработчиков событий имеет набор правил. При обработке событий от локально подключенных источников событий применяется набор правил. При обнаружении нарушения контроля доступа безопасности обработчик событий выдает предупреждение системы безопасности.

В общем виде архитектуру технологии SIEM можно представить в следующем виде. Метод реализуется ВК, предоставляющим веб-сервисы и подключенным к глобальной сети. Реализуемый метод контроля доступа включает преобразование правил SIEM в формальные представления. С точки зрения программной реализации необходимо обеспечить преобразование информации о доступе и обработать формальное представление правил управления событиями (SIEM) при их развертывании в сети обработчиков событий. Программно в сети обработчиков событий реализуется развертывание оптимизированных правил SIEM.

Из рассмотренных примеров видно [16, 32, 189], что системы КД являются частью ВК, обеспечивающего компьютерные сервисы. В то же время КД представляют собой отдельные компоненты, под управление КД выделяются часть инфраструктуры, виртуальные и физические ресурсы ВК. Это позволяет рассматривать архитектуру КД как самостоятельный объект, хотя и являющийся частью всего ВК, но со своими задачами проектирования и конфигурирования. Системы КД могут развиваться отдельно от собственно технологий, обеспечивающих предоставление ВС, могут добавляться реализации новых концепций КД, обновляться и изменяться программное, аппаратное обеспечение, не затрагивая основных функциональных возможностей ВС. Вместе с тем КД нельзя рассматривать вне контекста всего ВК — системные связи между всем ВК и подсистемой КД должны быть учтены на уровне технико-экономических характеристик ВК и функциональными возможностями, реализуемыми ВС в цифровой среде.

Таким образом, можно сформулировать **концепцию проектирования архитектуры КД** [11]: проектирование архитектуры КД является самостоятельной задачей, прямо не зависящей от основных задач и методов их решения в рамках исходного ВК, представляющего ВС в цифровой среде. Иными словами, являясь частью ВК по предоставлению ВС, система КД решает собственные задачи: собирает данные о доступе с тех же устройств, от тех же пользователей, но не относящиеся к предоставлению ВС, передает данные по тем же каналам, обрабатывает и хранит на тех же вычислительных ресурсах ВК собственные данные о доступе. Технологии обработки данных, миграция на новые технологии [180], не влекут за собой изменение основных функций ВС в цифровой среде. Вместе с тем внедрение КД должно удовлетворять технико-экономическим требованиям, предъявляемым к ВК. Это позволяет выделить задачу архитектуры КД как самостоятельную задачу вычислительных комплексов, машин и компьютерных сетей.

Задача построения архитектуры КД может быть сформулирована как проектирование архитектуры КД как самостоятельной подсистемы ВК, имеющей собственные задачи, такие как сбор, передача, хранение и обработка данных о действиях пользователей, методы, ресурсы и технологии обработки, которые независимы от используемых для предоставления ВС, но требуют собственные вычислительные ресурсы в составе ВК, при этом должны быть соблюдены технико-экономические требования к ВК.

Предложенный подход позволяет сформулировать ряд задач, являющихся типовыми для рассматриваемого класса объектов: определить систему сбора данных, сформировать виртуальную инфраструктуру для обработки данных КД, определить состав и технико-экономические требования к вычислительным ресурсам, требуемым для решения задач КД, определить состав и требуемые ресурсы для компонентов анализа данных КД [11, 13, 163, 190, 191].

Анализ требований и условий позволяет сформировать общую структуру подсистемы КД. Аппаратное обеспечение содержит виртуальные машины, сервера, систему хранения данных, сетевые устройства для доступа клиентов к предоставляемым ВС. Программное обеспечение, интегрированное в состав информационного обеспечения сервисов и управления доступом и обработке данных, реализует следующие функции: фиксирование, передачу и хранение данных о доступе пользователей к вычислительным сервисам; генерацию правил и прогноз значений (оценка вероятных значений) маркеров поведения пользователей в соответствии с заданными политиками защищенного доступа, сравнение полученных показателей с шаблонными персонифицированными значениями.

Пример КД для вычислительных сервисов [192] приведен на рис. 2.4.

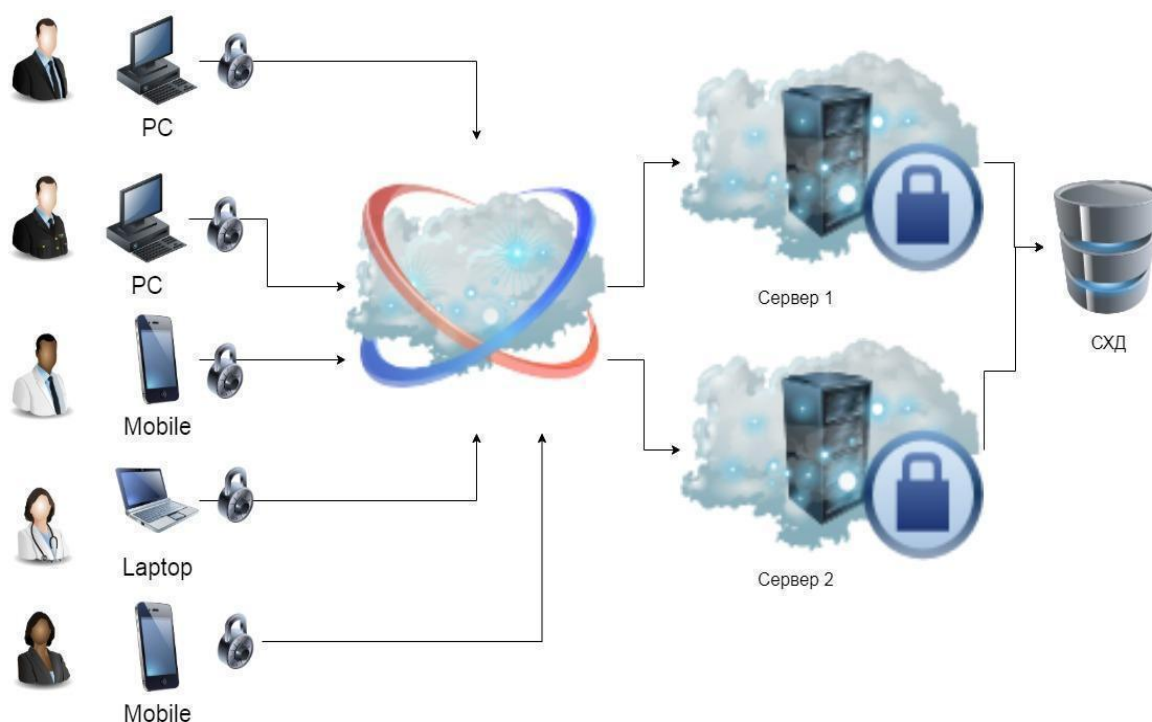


Рисунок 2.4 — Пример защищенного ВК для доступа к сервисам

ВК представляет собой [11, 193] сеть компьютеров, систем обработки данных и других устройств. ВК обработки сетевых данных содержит сеть, которая является средой, используемой для обеспечения каналов связи между компьютерами, системами обработки данных и прочими устройствами. Сеть может включать в себя соединения, такие как, например, проводные линии связи, каналы беспроводной связи и оптоволоконные кабели.

В показанном на рис. 2.4 примере серверы вместе с системой хранения данных (СХД) подключены к сети. Серверы могут предоставлять клиенту одну или несколько услуг, таких как, например, финансовые услуги, банковские услуги, правительственные услуги, образовательные услуги, услуги бронирования, услуги передачи данных в реальном времени, игровые услуги, услуги поиска и т. п. Кроме того, каждый из серверов включает в себя информацию о безопасности и диспетчер событий. Диспетчер со-

бытий отслеживает, регистрирует и объединяет соответствующие данные о событиях в соответствии с вычислительными услугами. Собранная информация служит основой для выявления отклонений от нормы и принятие соответствующих мер. Когда информация от диспетчера событий обнаруживают потенциальную проблему, то генерируется сообщение об инциденте безопасности на основе анализа и формируется команда другим элементам управления безопасностью, чтобы остановить процесс подозрительной активности, соответствующей предоставляемой услуге ВС. Менеджер событий может быть основан на правилах статистической корреляции для установления взаимосвязей между записями журнала событий безопасности. Диспетчер событий может также включать компоненты анализа поведения пользователей и компоненты управления.

Сервера могут отправлять инциденты безопасности на облачные ресурсы для дальнейшего анализа приложением когнитивного машинного обучения на основе идентифицированных характеристик инцидентов безопасности, обнаруженных во время локального анализа с помощью информации безопасности и диспетчера событий. Идентифицированные характеристики могут быть: наблюдаемое событие связано с инцидентом безопасности; наблюдаемое событие имеет оценку риска безопасности выше порогового значения; наблюдаемое событие определяется антивирусами как вредоносное ПО.

Диспетчер событий идентифицирует риски и угрозы безопасности, например, несанкционированные доступы к серверам и СХД. База инцидентов безопасности должна содержать инциденты неправомерного использования конфиденциальной информации, хранящейся на серверах ВК. Это может быть конфиденциальная информация, такая как номера кредитных карт, номера банковских счетов, финансовые записи, медицинские записи — любая информация, включающая конфиденциальные или персональные данные.

Клиентскими устройствами, с помощью которых пользователи подключаются через общедоступные сети к веб-сервисам, могут быть сетевые компьютеры, портативные компьютеры, карманные компьютеры, смартфоны, умные часы, умные телевизоры, игровые устройства и т. д. Пользователь клиентского устройства также может выполнять непреднамеренную или преднамеренную злонамеренную активность в отношении услуги, предоставляемой серверами.

СХД — это сетевое запоминающее устройство, способное хранить любой тип данных в структурированном и неструктурированном формате, кроме того, хранилище может хранить одну или несколько баз данных инцидентов безопасности, содержащих множество инцидентов безопасности, вместе с их соответствующими описаниями, весами источников, уровнями величин. СХД может хранить другие типы данных, например данные аутентификации или учетных данных, которые могут включать в себя имена пользователей, пароли и биометрические данные, связанные с пользователями, такими как, например, системные администраторы и аналитики безопасности.

Архитектура сетевой системы обработки данных может включать в себя любое количество дополнительных серверов, клиентов, запоминающих устройств и других устройств [163, 194, 195]. Программный код, расположенный в сетевой системе обработки данных, может загружаться в компьютер или другое устройство обработки данных для использования ВС [196–198]. Например, программный код может храниться на сервере и загружаться на клиент по сети в браузер пользовательского устройства [12].

2.7. Разработка четырехуровневой архитектуры системы контроля доступа

Разработана *четырёхуровневая масштабируемая архитектура контроля доступа пользователей в вычислительном комплексе, обеспечивающем доступ пользователей к ВС через компьютерные сети* [11].

На рис. 2.5 изображены уровни системы контроля доступа к данным ВК, предоставляющего ВС по сетям.



Рисунок 2.5 — Масштабируемая 4-уровневая архитектура системы КД

Программно-аппаратный уровень ВК включает в себя: аппаратные компоненты (в т. ч.: мейнфреймы, серверы, блейд-серверы, устройства хранения, сетевые компоненты [163]); системное и программное обеспечение ВК, а также программно-аппаратное обеспечение клиентского приложения и веб-сервисы, доступные через браузеры клиентских устройств.

Уровень виртуальной вычислительной инфраструктуры [163] обеспечивает взаимодействие виртуальных серверов, виртуальной памяти, виртуальных сетей, виртуальных приложений и операционных систем, виртуальных клиентов; управление сетевым взаимодействием клиентских запросов с ВК.

Уровень физических ресурсов включает: распределение вычислительных ресурсов ВК, которые используются для выполнения задач КД в облачной среде; специализированное ПО; доступ к среде пользователей и системных администраторов; а также управление системой хранения данных.

Уровень компонентов анализа данных КД включает конкретное программно-математическое обеспечение, которое реализует обработку и анализ данных, анализ инцидентов безопасности.

Разработанная архитектура позволяет заменять или расширять элементы на каждом из выделенных ресурсов без изменения общей структуры (т. е. обеспечивается масштабируемость).

Каждый уровень может быть рассмотрен отдельно как комплекс задач. Каждому уровню соответствует свой набор технологий, компонентов, что может быть реализовано отдельными компонентами или разработками отдельных команд ИТ-специалистов и специалистов по обработке данных.

Каждому уровню архитектуры соответствуют этапы разработки системы КД:

- 1) определение состава параметров, которые могут быть получены о действиях пользователей, способы их сбора и передачи;

- 2) формирование виртуальной вычислительной инфраструктуры, требуемой для решения задач обработки информации КД;
- 3) оценка параметров вычислительных ресурсов;
- 4) разработка компонентов анализа информации.

Предложенная архитектура позволяет заменять или расширять элементы на каждом из выделенных ресурсов без изменения общей структуры и определяет этапы задач по разработке и внедрению, тем самым обеспечивая масштабируемость и технологическое развитие системы.

2.8. Разработка аппаратного уровня архитектуры системы контроля доступа

На рис. 2.6 изображена архитектура серверной системы обработки данных (1 уровень архитектуры). Система предоставляет доступ клиентским устройствам к данным и услугам через веб-сервисы. Система обработки данных включает в себя структуру связи, которая обеспечивает связь между процессорным блоком, памятью, постоянным хранилищем, блоком коммуникационного оборудования.

В системах хранения данных, представляющих собой совокупность серверного оборудования и СХД, содержатся компоненты, реализующие контроль доступа к ВК. В систему КД включены следующие компоненты:

- база инцидентов, содержащая информацию о возможных вариантах поведения системы и/или пользователя при несанкционированном доступе или угрозам целостности данных или компонентам ВК;

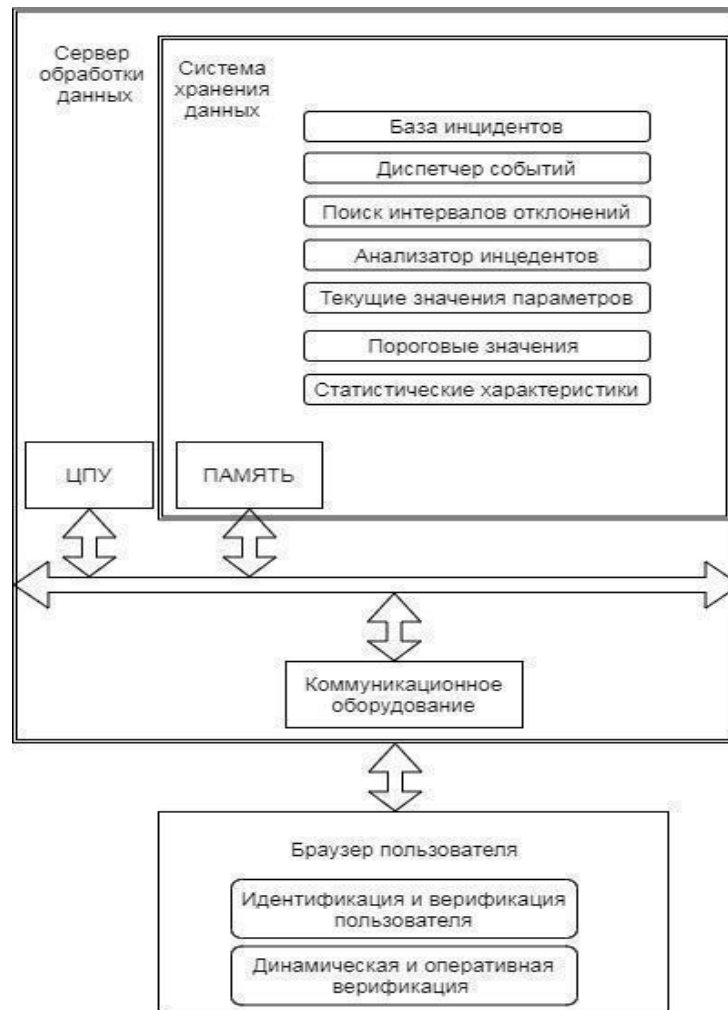


Рисунок 2.6 — Аппаратный уровень КД

- диспетчер событий — может быть отдельным аппаратным модулем, или программно-аппаратным модулем, отвечающим за фиксирование событий безопасности и контроле доступа через сети;
- анализатор инцидентов — программный модуль, обеспечивающий оперативный контроль доступа на основе анализа событий;
- модуль сравнения полученных значений параметров доступа и характеристик событий с заданными моделями или пороговыми значениями;

- текущие значения параметров, характеризующие контроль доступа пользователей, сбор статистических данных;
- пороговые значения — база значений, характеризующих события, при которых следует обеспечивать программные или аппаратные сценарии защиты, блокировки пользователя, повторной верификации и т. д., а также возможные варианты перерасчета пороговых значений;
- статистические характеристики — модуль, хранящий и вычисляющий значения статистических параметров конкретных пользователей, групп пользователей и других параметров, используемых при анализе инцидентов.

Выводы по главе

На основе анализа условий и характеристик систем КД сформулирована концепция и задача проектирования архитектуры КД как подсистемы ВК, имеющей собственные цели, задачи и технологии реализации. Отличие от альтернативных подходов связано с возможностью параллельной разработки, поэтапного внедрения, возможностью замены или расширения элементов КД, что можно делать, с одной стороны — независимо, с другой — используя требования и условия эксплуатации, предъявляемые ко всему ВК.

Для эффективности системы обеспечения КД в качестве целевого показателя предложена стохастическая модель, позволяющая оценить средние ожидаемые значения оцениваемых характеристик, которые должны лежать в диапазонах, заданных технико-экономическими требованиями, т. е. обеспечить гарантированное значение качества обслуживания.

Разработана четырехуровневая масштабируемая архитектура КД, интегрируемая в вычислительные комплексы, обеспечивающие взаимодействие пользователей с ВС: 1) программно-аппаратный уровень ВК, включающий средства, обеспечивающие КД; 2) уровень виртуальной инфраструктуры обработки данных КД; 3) уровень физических ресурсов для обработки данных КД; 4) уровень компонентов анализа данных.

Данная архитектура позволяет заменять или расширять элементы на каждом из выделенных ресурсов без изменения общей структуры и определяет этапы задач по разработке и внедрению.

Глава 3. ОБЛАЧНАЯ ИНФРАСТРУКТУРА ОБРАБОТКИ ДАННЫХ СИСТЕМ КОНТРОЛЯ ДОСТУПА

Рассмотрены вопросы построения уровня облачной инфраструктуры архитектуры КД, изложена методика распределения виртуальных вычислительных ресурсов и сетевого взаимодействия, приведен примеры инфраструктуры для системы КД при сетевом взаимодействии.

3.1. Методика построения облачной инфраструктуры

Предлагается структура уровня виртуальных вычислительных сервисов КД, включающая сетевой фильтр для проверки подлинности данных и легальности пользовательского поведения, обеспечивающая возможность анализа наборов архивных данных и входящих потоков больших данных, а также управления предупреждениями. Структура уровня виртуальной инфраструктуры разработанной архитектуры КД позволяет упростить процесс обновления и разработки КД.

Использование облачной инфраструктуры обеспечивает горизонтальную масштабируемость и отказоустойчивость.

Сформулированы базовые принципы и технологии, на основе которых предлагается строить второй уровень архитектуры КД.

1) Применение технологий виртуализации сетевых функций (NFV) [199]. В задачи каждой виртуальной машины входит обработка сетевого трафика данных КД, поступающих от пользователей ВС с программно-аппаратного обеспечения ВК, и передача обработанного трафика или служебной информации в систему хранения данных или модулям обработки данных [16].

2) Выделение серверных ролей виртуальным ресурсам. Для серверных ролей, работающих под управлением операционной системы с гипервизором, необходимо определить набор входных параметров, поступающих от программно-аппаратного уровня архитектуры КД, а также определить конкретные задачи КД.

3) Масштабирование виртуальной инфраструктуры как ее свойство. Это означает, что изменение объема обрабатываемого трафика может привести к изменению вычислительных ресурсов, но не должно требовать изменения программного обеспечения виртуальных машин.

4) Универсальность модели облачной инфраструктуры по отношению к серверному оборудованию. Разработка уровня виртуальных машин архитектуры КД должна быть универсальна, не быть ориентированной на специфику используемого оборудования. Изменение типа оборудования, состав технико-экономических требований определяют конфигурацию, количество, но не структуру и обмен данных между виртуальными машинами.

На основе предложенных принципов разработана *методика построения облачной инфраструктуры* для систем КД [11, 200, 201]:

1. Определение состава и потока данных КД.
2. Выделение серверных ролей виртуальных машин (ВМ).
3. Выбор ПО, реализующего функции серверных ролей.
4. Определение состава ВМ, обеспечивающих решение задач КД.
5. Разработка информационной модели обмена данных между ВМ.
6. Разработка облачной инфраструктуры.
7. Конфигурирование инфраструктуры.
8. Экспериментальная оценка ресурсной эффективности.

Ниже рассмотрены примеры применения методики для задачи анализа данных, передаваемых по протоколу DICOM и для UBA-системы.

3.2. Формирование сетевых функций виртуальной облачной инфраструктуры

3.2.1. Разработка виртуальной инфраструктуры для систем, использующих протокол DICOM

В качестве примера уровня виртуальных ресурсов рассмотрены сетевые функции анализа трафика, передаваемого с использованием протокола DICOM, который применяется в системе здравоохранения.

Наиболее распространенным медицинским протоколом является протокол DICOM [202]. Данные, передаваемые посредством этого протокола, будут рассматриваться в контексте корректности с медицинской точки зрения, чтобы минимизировать возможный вред от поддельных файлов DICOM [140]. Для достижения приемлемой точности на практике учитываются следующие аспекты: корректность периодичности и корректность самих данных изображения (временного ряда) для рассматриваемой модальности, а также легальность пользовательского поведения. В работе предлагается архитектура информационной системы и интегрированный в нее сетевой фильтр для проверки подлинности данных в архиве DICOM и легальности пользовательского поведения, обеспечивающий возможности анализа и управления предупреждениями. Структура предлагаемой системы предназначена как для работы с наборами архивных данных, так и для выполнения анализа входящих потоков больших данных [203, 204]. Компоненты программного обеспечения работают в кластере, что обеспечивает горизонтальную масштабируемость и отказоустойчивость.

Рассмотрим ряды данных с периодически отправляемыми в архив отсчетами (измерениями). Они могут генерироваться не только стационарным оборудованием, но и носимыми устройствами, такими как биомедицинские датчики ЭКГ. Аппаратные средства предоставляют данные по за-

просу программного обеспечения, которое обычно выполняет периодические запросы и отправляет данные в облако [205–207]. Если периодичность входящего потока данных нарушена, высока вероятность атаки, если при этом простая потеря сетевого соединения не имеет места. Ниже описывается предлагаемая модель корректности периодичности для входящих потоков данных. Она позволяет иметь некоторое отклонение от фиксированной величины периодичности для моделирования редких проблем с сетевым подключением.

Обозначим $X = \{X_1, X_2, \dots, X_1^r, X_2^r, \dots, X_n^r, \dots, X_1^d, X_2^d, \dots, X_m^d, \dots\}$ — временной ряд рассматриваемой модальности. В нем выделены две части: контрольная часть (отсчеты обозначены как $X_\bullet^r$) и часть для анализа (отсчеты обозначены как $X_\bullet^d$). Отсчеты $X_1, X_2, \dots$, предшествующие контрольной части, представляют собой архивные данные, которые не рассматриваются для построения модели.

Пусть $time(X_\bullet^r)$ — функция, возвращающая отметку времени отсчета $X_\bullet^r$, переданного в качестве аргумента.

Пусть $t_i^r = time(X_{i+1}^r) - time(X_i^r), i = 1, \dots, n - 1$ — временной интервал для двух отсчетов в контрольной части.

Тогда средний временной интервал для контрольной части $(1/n - 1) \sum_{i=1}^{n-1} t_i^r$ должен принадлежать $[T^r - \Delta^r; T^r + \Delta^r]$, где T^r — ожидаемый период, Δ^r — допустимое изменение ожидаемого периода. Обе величины задаются определяемыми пользователем внешними параметрами, представленными в виде положительных значений даты и времени.

Рассмотрим $t_j^d = time(X_{j+1}^d) - time(X_j^d), j = 1, \dots, m - 1$ как временной интервал двух отсчетов в анализируемой части. Среднее значение

$(1/m - 1) \sum_{j=1}^{m-1} t_j^d$ также должно принадлежать $[T^r - \Delta^r; T^r + \Delta^r]$ и должно выполняться

$$\forall j \in \{1, 2, \dots, m\} \left(k_l \min_{i=1,2,\dots,n} (t_i^r) \leq t_j^d \leq k_u \max_{i=1,2,\dots,n} (t_i^r) \right),$$

чтобы период анализируемой части считался корректным, где k_l и k_u — определяемые пользователем внешние параметры, представленные положительными действительными значениями.

Нарушение целостности может подразумевать не только отправку поддельных данных с нарушением периодичности, но и повреждение изображений, уже записанных в PACS. Второй аспект, который мы учитываем, — это подлинность самих медицинских данных [114]. Для различных модальностей разработаны специальные методы и алгоритмы [140, 208–213], позволяющие проводить анализ файлов и оценивать возможность несанкционированное изменение медицинских данных с правильной временной меткой.

Анализ содержимого файлов DICOM. Сетевой анализатор (кластер) предназначен для перехвата DICOM-трафика [140, 202, 214] и автономного анализа поступающих серий данных наблюдаемых пациентов. Программные компоненты низкого уровня полагаются на функциональность `libpcap` для захвата трафика с сетевых интерфейсов на машинах Linux. Все функции Linux и возможности `libpcap` для простоты обозначены как компонент `LinuxKernel` на представленных UML-диаграммах.

Диаграмма классов на рис. 3.1 иллюстрирует анатомию компонентов анализа трафика, имеющего отношение к медицинским данным.

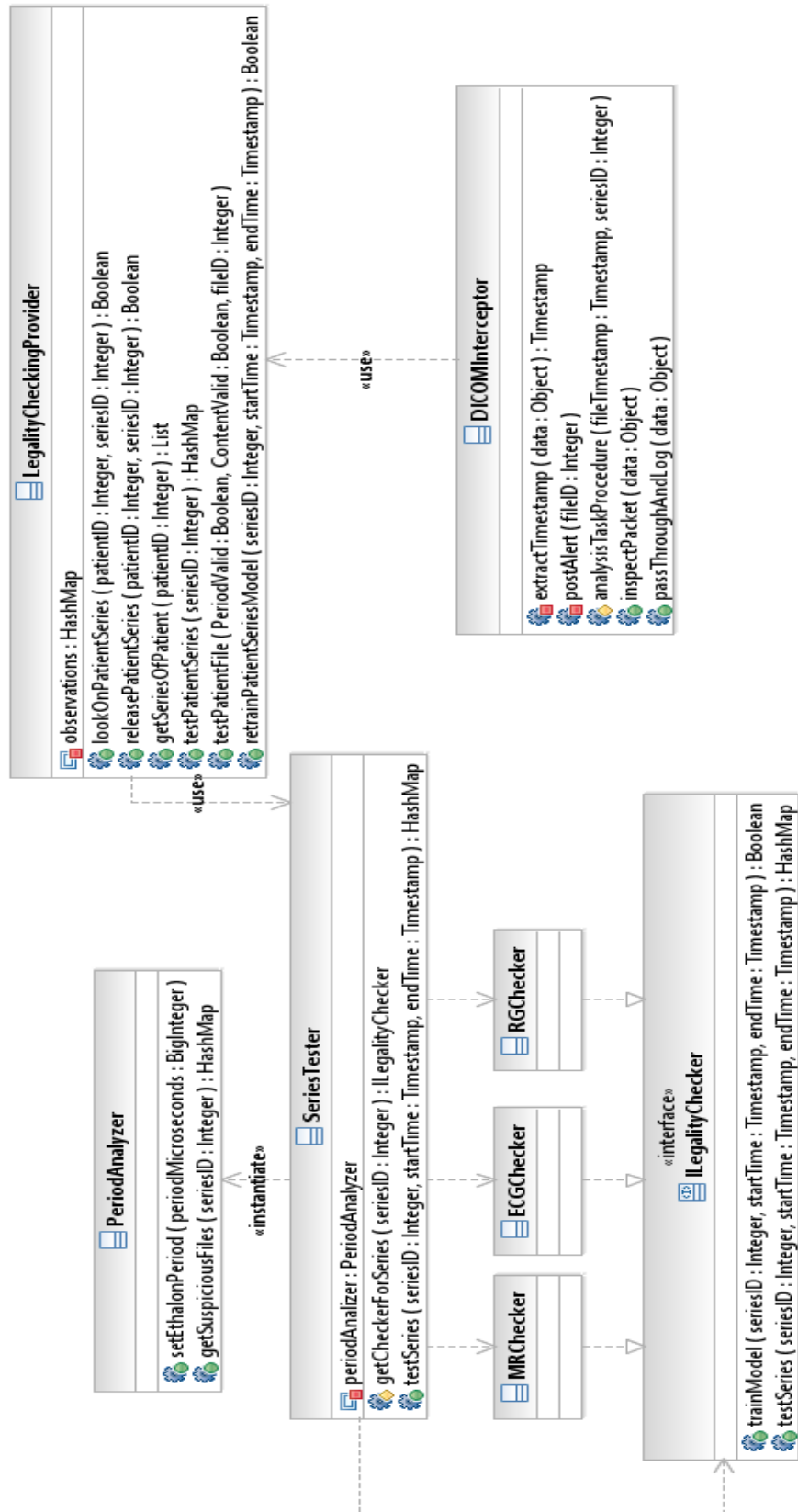


Рисунок 3.1 — Диаграмма классов анализатора медицинских данных

1. Класс DICOMInterceptor (табл. 3.1) предназначен для анализа пакетов DICOM и запуска проверки содержимого. Это основной класс, взаимодействующий с LinuxKernel.

Таблица 3.1 — Класс DICOMInterceptor

inspectPacket	1. Извлекает метку времени из пакета данных. 2. Если данные являются действительным файлом DICOM с меткой времени, запускает задачу анализа асинхронно
passThroughAndLog	Пропускает пакет дальше и регистрирует это событие
extractTimestamp	Извлекает метку времени из файла DICOM
postAlert	Публикует оповещение для указанного файла DICOM
analysisTaskProceduce	1. Ожидает появления файла с указанной меткой времени в архиве DICOM. 2. Запускает анализ этого файла. 3. Если есть нарушения, публикует предупреждения

2. Класс LegalityCheckingProvider (табл. 3.2) предназначен для управления конфигурацией и обеспечения функции проверки для компонента анализа содержимого файлов DICOM (DICOMAnalyzer).

3. Класс SeriesTester (табл. 3.3) загружает и использует различные плагины для проверки корректности данных для различных модальностей (типов серий данных). Он также использует экземпляр PeriodAnalyzer для проверки периодичности входящих данных.

Таблица 3.2 — Класс `LegalityCheckingProvider`

<code>retrainPatientSeriesModel</code>	Переобучить модель машинного обучения для указанной серии с указанным интервалом данных для обучения
<code>testPatientSeries</code>	Возвращает ассоциативный массив с идентификаторами отсчетов в качестве ключей и их корректностью в виде значений <code><boolean, boolean></code> . Первое логическое значение в кортеже — это корректность периодичности, второе логическое значение в кортеже — корректность содержимого
<code>testPatientFile</code>	Возвращает корректность периодичности и содержимого для отдельного указанного файла пациента
<code>getSeriesOfPatient</code>	Возвращает идентификаторы наблюдаемых серий для пациента
<code>releasePatientSeries</code>	Удалить серию пациента из списка наблюдений
<code>lookOnPatientSeries</code>	Добавить серию пациента в список наблюдений
<code>observations</code>	Ассоциативный массив с идентификаторами пациентов в качестве ключей и списками идентификаторов серий в качестве значений

Таблица 3.3. — Класс `SeriesTester`

<code>testSeries</code>	Возвращает ассоциативный массив с идентификаторами отсчетов в качестве ключей и их корректностью в виде значений <code><boolean, boolean></code> . Первое логическое значение в кортеже — это корректность периодичности, второе логическое значение в кортеже — корректность содержимого
<code>getCheckerForSeries</code>	Получить точку входа в соответствующем плагине для указанной серии данных
<code>periodAnalyzer</code>	Экземпляр <code>PeriodAnalyzer</code>

4. Класс `PeriodAnalyzer` (табл. 3.4) предназначен для анализа периодичности поступления данных.

Таблица 3.4 — Класс `PeriodAnalyzer`

<code>setEthalonPeriod</code>	Устанавливает значение периода, с которым проверяется соответствие для временного ряда
<code>getSuspiciousFiles</code>	Возвращает ассоциативный массив с идентификаторами отсчетов в качестве ключей, и корректностью отсчетов в виде логических значений

5. `ILegalityChecker` (табл. 3.5) — это общий интерфейс, который должен реализовывать каждый плагин проверки для любой модальности.

Таблица 3.5 — Класс `ILegalityChecker`

<code>trainModel</code>	Обучить модель машинного обучения для указанной серии с указанным интервалом данных для обучения
<code>testSeries</code>	Возвращает ассоциативный массив с идентификаторами отсчетов в качестве ключей, и корректностью отсчетов в виде логических значений

6. `MRChecker` — это плагин проверки модальности MR, реализующий интерфейс `ILegalityChecker`.

7. `RGChecker` — это плагин проверки модальности RG, реализующий интерфейс `ILegalityChecker`.

8. `ECGChecker` — это плагин для проверки модальности ЭКГ, реализующий интерфейс `ILegalityChecker`.

Все классы, кроме классов проверки корректности для разных модальностей (`MRChecker`, `RGChecker`, `ECGChecker`), реализованы в компоненте `DICOMAnalyzer`. Классы проверки корректности для разных модальностей реализованы в отдельных компонентах. Диаграмма компонен-

тов на рис. 3.2 иллюстрирует взаимосвязь компонентов в системе и ПО, с которым она работает.

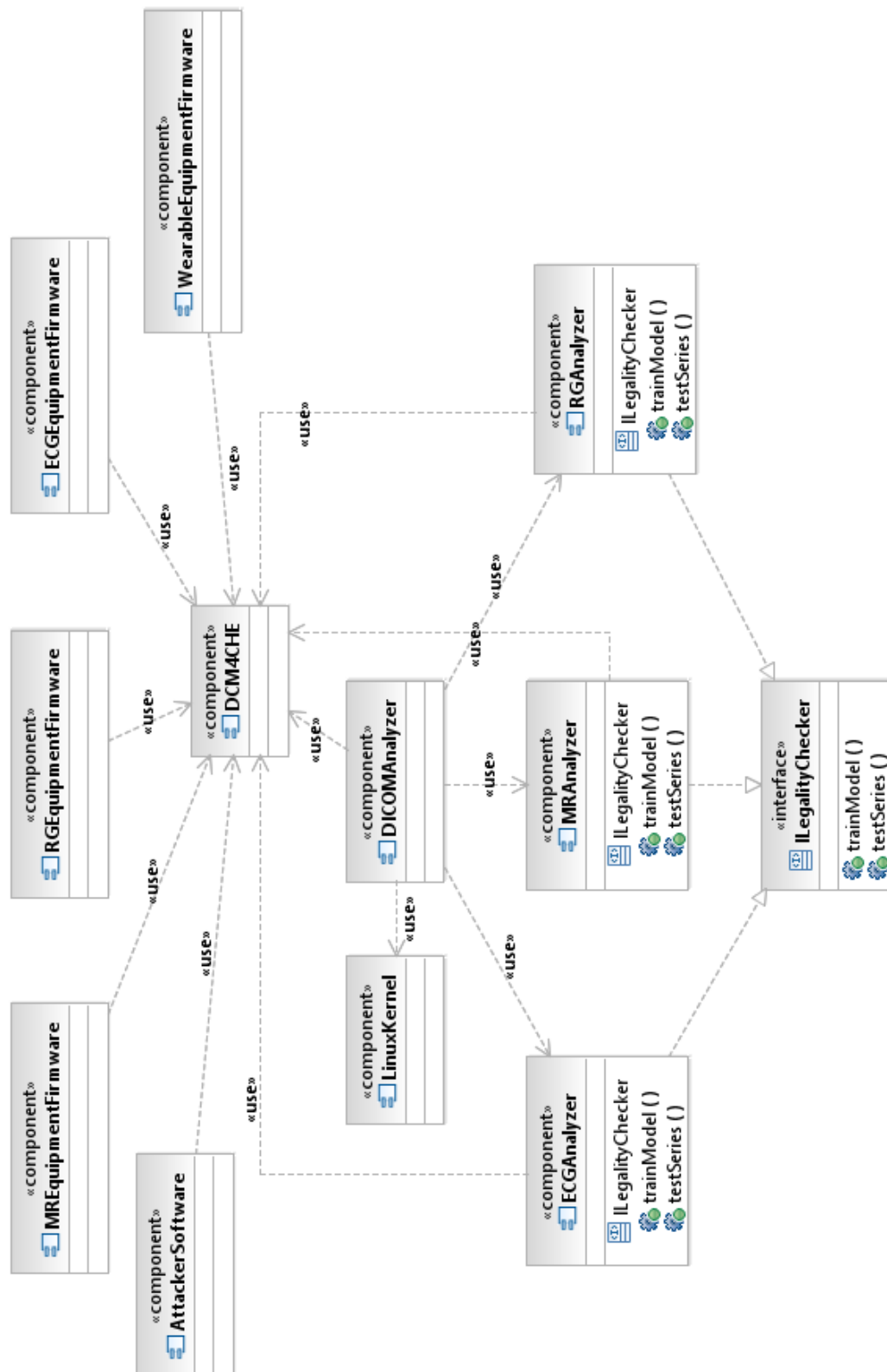


Рисунок 3.2 — Диаграмма компонентов анализатора медицинских данных

Источником данных являются различные медицинские программно-аппаратные комплексы и носимые приборы, на диаграмме компонентов фигурирует обозначение их микропрограммы

- MREquipmentFirmware,
- RGEquipmentFirmware,
- ECGEquipmentFirmware,
- WearableEquipmentFirmware.

Также повлиять на наполнение архива может деятельность ПО злоумышленника — на диаграмме компонентов отражено как AttackersSoftware, использующее dcm4che [215] наряду с медицинским оборудованием.

DICOMAnalyzer, MRAnalyzer, ECGAnalyzer, RGAnalyzer (и другие компоненты проверки корректности для разных модальностей) должны быть упакованы как отдельные артефакты (с такими же именами, рис. 3.3). Все они должны быть развернуты на узле LegalityAnalysisBackend. Эти узлы должны быть кластеризованы для обеспечения высокой доступности. Входящий трафик, предназначенный для PACS, просматривается на узле TCPInterceptorFrontend и направляется для анализа на узлы LegalityAnalysisBackend с балансировкой по алгоритму round-robin. Важно, что dcm4che, предоставляющий функциональность архива DICOM, и PostgreSQL, предоставляющий для него базу данных, должны быть развернуты на отдельных узлах DICOMArchive и DICOMArchiveDatabase соответственно.

Диаграмма деятельности на рис. 3.4 иллюстрирует процесс проверки и анализа пакетов DICOM в системе на аналитическом кластере.

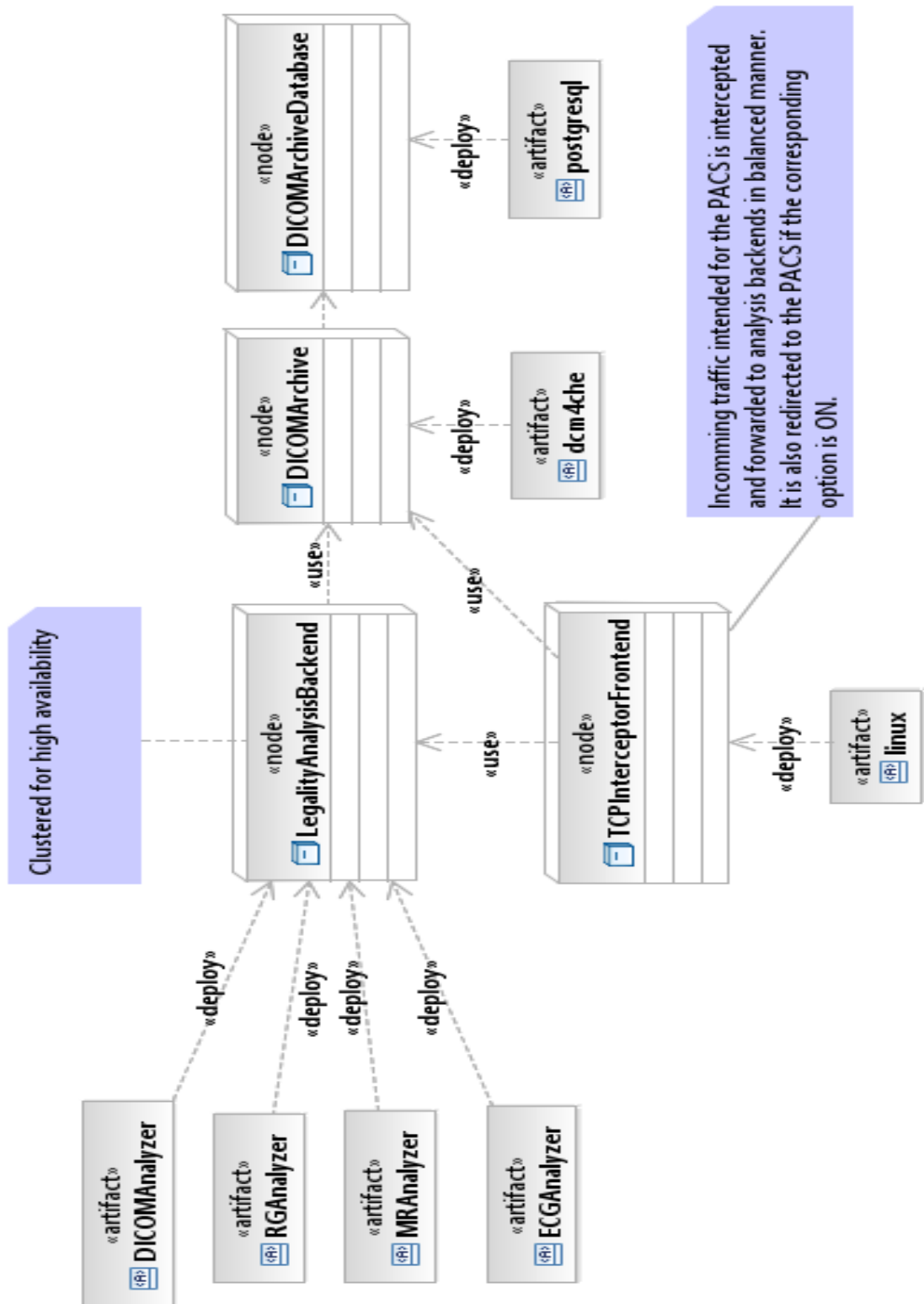


Рисунок 3.3 — Диаграмма развертывания анализатора медицинских данных

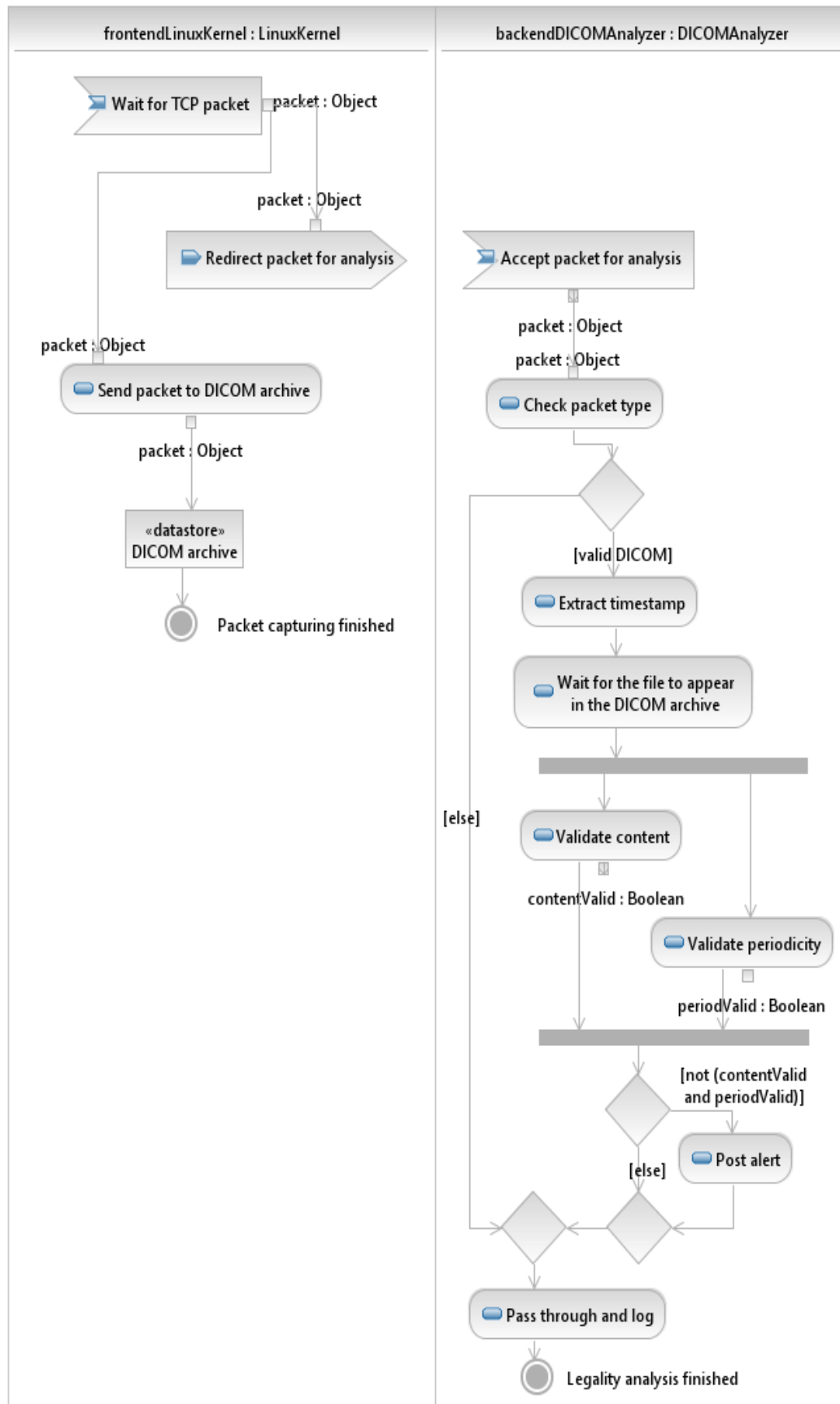


Рисунок 3.4 — Анализ входящих файлов DICOM

Процесс, показанный на диаграмме, предполагает, что модель для наблюдения за рядами уже обучена. Могут быть проанализированы только действительные пакеты DICOM. Когда пакет прибывает в ядро Linux на узле TCPInterceptorFrontend, он перенаправляется для анализа на один из узлов LegalityAnalysisBackend, где он проверяется, и из него извлекается значение временной метки (компонент DICOMAnalyzer). Если проверяемый пакет является допустимым пакетом DICOM, то процедура анализа выполняется асинхронно. Происходит ожидание, пока файл DICOM не появится в архиве DICOM, и тогда начинается анализ на предмет корректности периодичности и содержимого с помощью экземпляров PeriodAnalyzer и [Modality]Checker. Выбор для анализа содержимого возложен на метод getCheckerForSeries класса SeriesTester. При возникновении подозрений вызывается метод postAlert, который может нести требуемую функциональность оповещения об опасностях и дополнительного журналирования событий. Сетевая активность журналируется (passThroughAndLog).

3.2.2. Разработка виртуальной инфраструктуры для систем, использующих протокол HTTP и для реализации UBA-системы

Сетевой анализатор (кластер) предназначен для обработки HTTP-трафика и автономного анализа поступающих событий, индуцируемых пользователями. Примеры интерфейсов для системы здравоохранения: личный кабинет рентгенолога, личный кабинет специалиста по ЭКГ, личный кабинет анестезиолога. Программные компоненты низкого уровня полагаются на функциональность mitmproxy для захвата трафика, предназначенного для веб-сервера МИС. Все функции Linux для простоты обозначены как компонент LinuxKernel на представленных UML-диаграммах.

Диаграмма классов на рис. 3.5 иллюстрирует анатомию компонентов анализа пользовательского поведения.

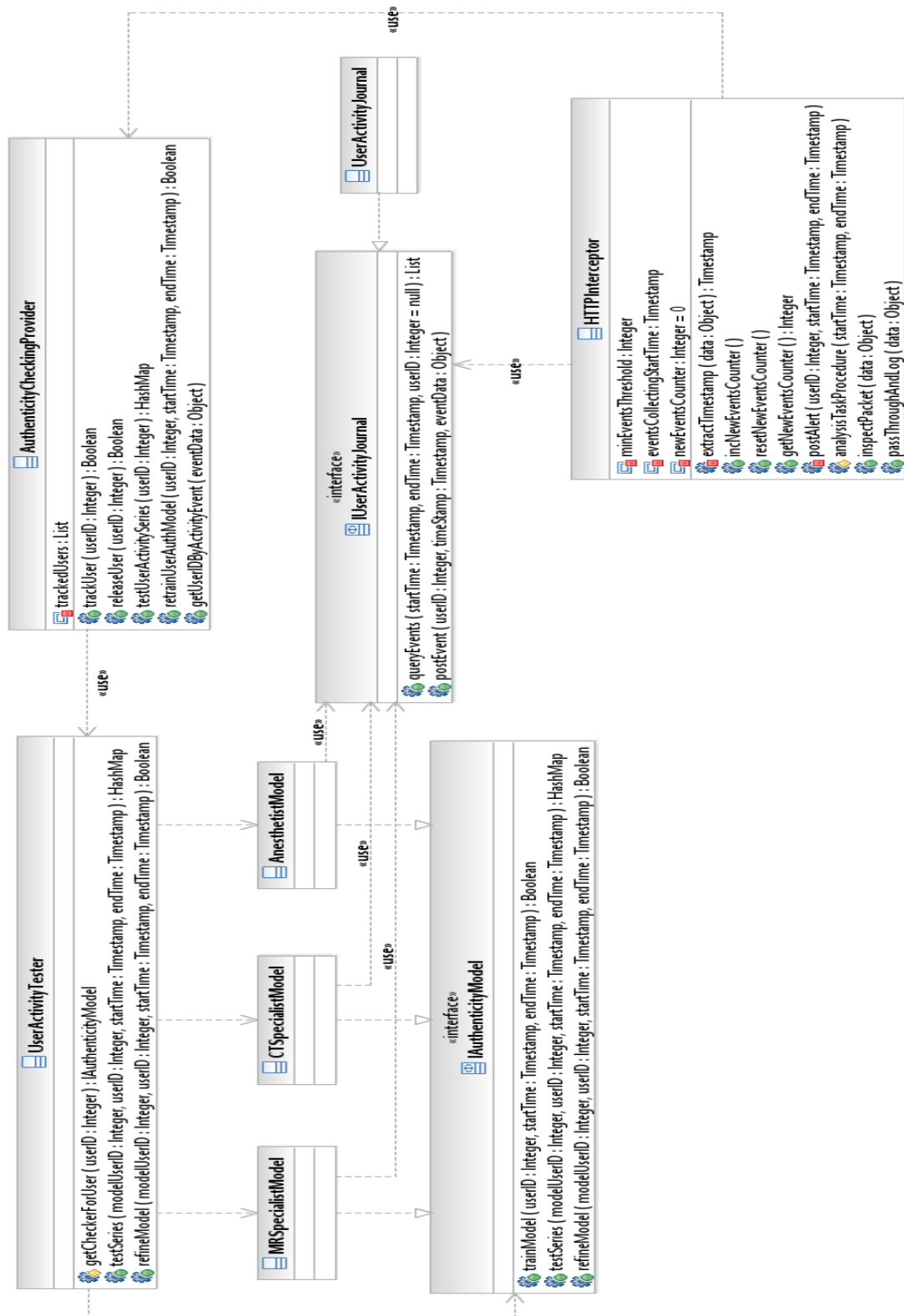


Рисунок 3.5 — Диаграмма классов анализатора медицинских данных

1. Класс `HTTPInterceptor` (табл. 3.6) предназначен для анализа пакетов HTTP и запуска проверки содержимого. Это основной класс, взаимодействующий с `mitmproxy`.

Таблица. 3.6 — Класс `HTTPInterceptor`

<code>minEventsThreshold</code>	Минимальный порог количества новых событий для начала анализа
<code>eventsCollectingStartTime</code>	Отметка времени начала сбора новых событий
<code>newEventsCounter</code>	Счетчик новых входящих событий активности пользователей для дальнейшего анализа
<code>extractTimestamp</code>	Извлекает отметку времени из заголовков HTTP
<code>incNewEventsCounter</code>	Увеличивает счетчик новых событий активности пользователя
<code>resetNewEventsCounter</code>	Сбрасывает счетчик новых событий активности пользователя на ноль. Устанавливает время начала сбора событий на текущее время
<code>getNewEventsCounter</code>	Возвращает значение счетчика новых событий активности пользователя
<code>postAlert</code>	Публикует оповещение для указанного интервала времени активности пользователя
<code>analysisTaskProcedure</code>	1. Запускает анализ новых событий. 2. Если есть подозрения, то выкладывает оповещения
<code>inspectPacket</code>	1. Извлекает метку времени из пакета данных. 2. Если данные действительны HTTP с действием пользователя, увеличивает счетчик новых событий, и если он достигает <code>minEventsThresholds</code> , запускает задачу анализа асинхронно
<code>passThroughAndLog</code>	Пропускает пакет дальше и регистрирует это событие

2. Класс `UserActivityJournal` предназначен для управления журналом пользовательской активности и предоставления данных аналитическим компонентам.

3. `IUserActivityJournal` (табл. 3.7) — интерфейс для работы с журналом пользовательской активности.

Таблица 3.7 — Класс `IUserActivityJournal`

<code>queryEvents</code>	Запросить события из журнала за указанный интервал времени для пользователя с указанным идентификатором
<code>postEvent</code>	Записать данные о событии в журнал с указанием отметки времени и идентификатора пользователя

4. Класс `AuthenticityCheckingProvider` (табл. 3.8) предназначен для управления конфигурацией и обеспечения функции проверки соответствия для компонента анализа поведения пользователей (`HTTPAnalyzer`).

Таблица 3.8 — `AuthenticityCheckingProvider`

<code>trackedUsers</code>	Список идентификаторов отслеживаемых пользователей
<code>trackUser</code>	Добавить пользователя, идентифицированного по <code>userID</code> , в список отслеживания. Истина возвращается, если соответствующий плагин модели поведения доступен и запись еще не добавлена
<code>releaseUser</code>	Больше не отслеживать пользователя, идентифицированного с помощью <code>userID</code> . Истина возвращается, если запись существует в списке отслеживания

Таблица. 3.8 — Окончание

testUserActivitySeries	Возвращает ассоциативный массив с отметками времени событий в качестве ключей и оценкой их подлинности в виде логических значений. Источник модели машинного обучения автоматически определяется идентификатором пользователя
retrainUserAuthModel	Переобучить модель машинного обучения для указанного пользователя с заданным интервалом данных для обучения
getUserIDByActivityEvent	Возвращает идентификатор пользователя по событию его активности

5. Класс UserActivityTester (табл. 3.9) загружает и использует различные плагины для проверки подлинности пользовательской активности для различных специалистов.

Таблица 3.9 — Класс UserActivityTester

getCheckerForUser	Получить точку входа в соответствующем плагине для указанной модели поведения пользователя
testSeries	Возвращает ассоциативный массив с отметками времени событий в качестве ключей и оценкой их подлинности в виде логических значений. Источник модели машинного обучения определяется пользователем, идентифицированным с помощью modelUserID, тестовые данные определяются активностью пользователя, идентифицированного с помощью userID. Если пользователи, идентифицированные с помощью modelUserID и userID, имеют несовместимые типы моделей машинного обучения, возникает исключение

Таблица. 3.9 — Окончание

refineModel	Уточнить модель поведения (модель машинного обучения) для пользователя, идентифицированного с помощью modelUserID, с помощью данных, связанных с активностью пользователя, идентифицированного с помощью userID. Если пользователи, идентифицированные с помощью modelUserID и userID, имеют несовместимые типы моделей машинного обучения, возникает исключение

6. IAuthenticityModel (табл. 3.10) — это общий интерфейс, который должен реализовывать каждый плагин проверки поведения для любой врачебной специализации.

Таблица. 3.10 — Класс IAuthenticityModel

trainModel	Обучить модель машинного обучения для пользователя, идентифицируемого userID, с указанным интервалом данных для обучения. Модель сохраняется в другом месте для использования в методах testSeries и refineModel
testSeries	Возвращает ассоциативный массив с отметками времени событий в качестве ключей и их оценкой в виде логических значений. Истина — достоверно, Ложь — незаконно. Используемая модель машинного обучения связана с пользователем, идентифицированным по modelUserID, ряды данных определяются активностью пользователя, идентифицированного по userID. Пользователи, идентифицированные по modelUserID и userID, должны быть связаны с одним и тем же типом модели машинного обучения
refineModel	Уточнить модель поведения для пользователя, идентифицированного с помощью modelUserID, с данными, связанными с активностью пользователя, идентифицированного с помощью userID. Пользователи, идентифицированные по modelUserID и userID, должны быть связаны с одним и тем же типом модели машинного обучения

7. `MRSpecialistModel` — это плагин проверки поведения специалиста модальности MR, реализующий интерфейс `IAuthenticityModel`.

8. `CTSpecialistModel` — это плагин проверки поведения специалиста модальности CT, реализующий интерфейс `IAuthenticityModel`.

9. `AnesthetistModel` — это плагин проверки поведения специалиста-анестезиолога, реализующий интерфейс `IAuthenticityModel`.

Все классы, кроме классов проверки поведения для различных врачебных специализаций (`MRSpecialistModel`, `CTSpecialistModel`, `AnesthetistModel`), реализованы в компоненте `HTTPAnalyzer`. Классы проверки поведения для различных врачебных специализаций реализованы в отдельных компонентах. Диаграмма компонентов на рис. 3.6 иллюстрирует взаимосвязь компонентов в системе и другого программного обеспечения, с которым она работает, например сервера приложений, предоставляющего функциональность интерфейсов личных кабинетов специалистов. Источником событий для последнего являются различные клиентские устройства специалистов с веб-браузером. Также повлиять на состояние сервера приложений может деятельность ПО злоумышленника (на диаграмме компонентов отражено как `AttackerHTTPClient`, использующее веб-сервер наряду с браузерами специалистов).

`HTTPAnalyzer`, `MRSpecialistValidator`, `CTSpecialistValidator`, `AnesthetistValidator` (и другие компоненты проверки пользовательского поведения для различных врачебных специализаций) должны быть упакованы как отдельные артефакты (с соответственными именами, рис. 3.7). Все они должны быть развернуты на узле `BehaviorAnalysisBackend`. Эти узлы должны быть кластеризованы для обеспечения высокой доступности. Входящий трафик, предназначенный для сервера приложений, просматривается на узле `HTTPInterceptorFrontend` и направляется для анализа на узлы `BehaviorAnalysisBackend` с балансировкой по алгоритму `round-robin`. Функциональность журнала пользовательской активности может быть предо-

ставлена компонентом rsyslog, который развертывается на отдельном узле JournalBackend. Сервер приложений, предоставляющий функциональность личных кабинетов специалистов, должен быть развернут на отдельном узле WebServer.

Разработана методика проверки и анализа трафика (пакетов HTTP) в системе КД на аналитическом кластере с учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных ВК, см. диаграмму на рис. 3.8.

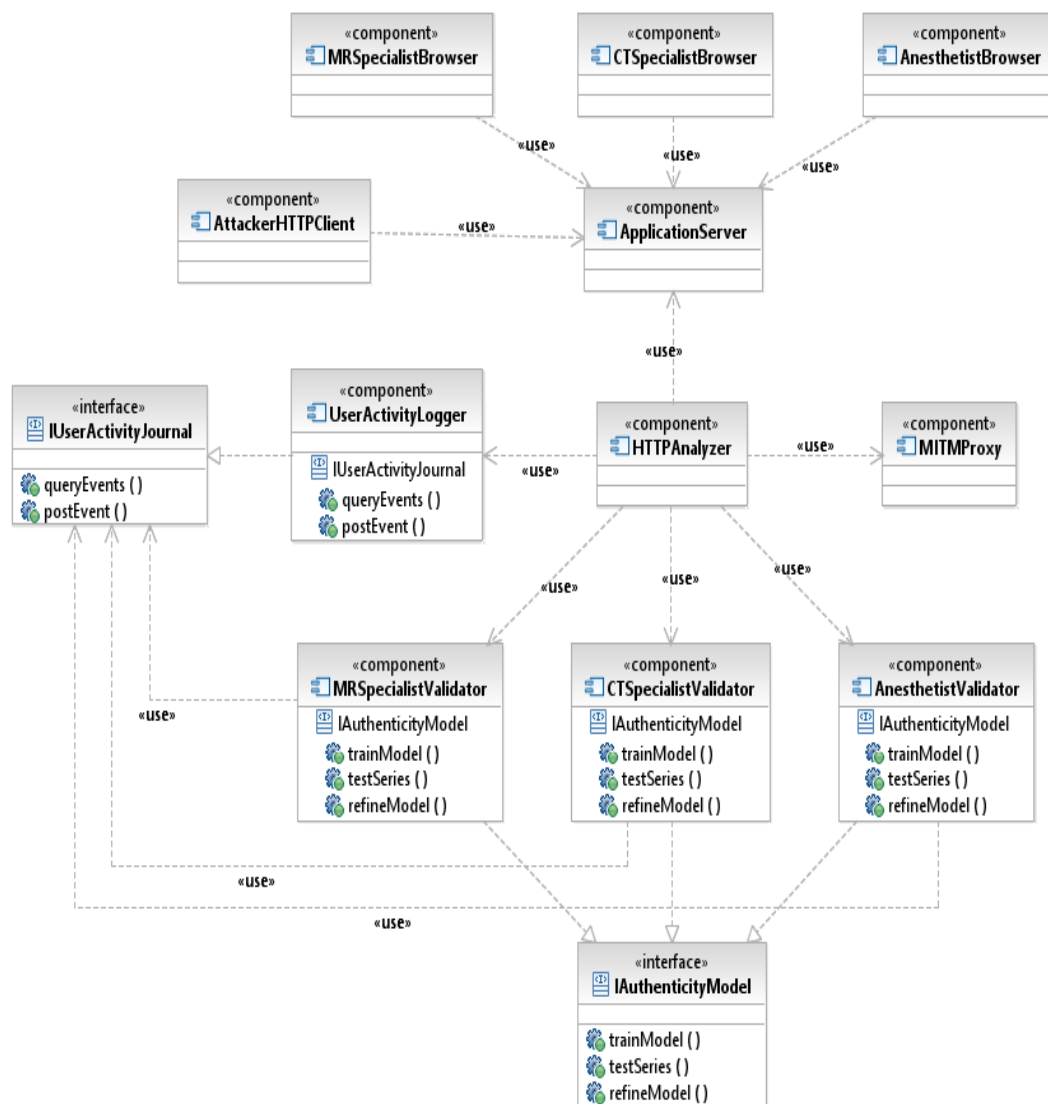


Рисунок 3.6 — Диаграмма компонентов анализатора
пользовательского поведения

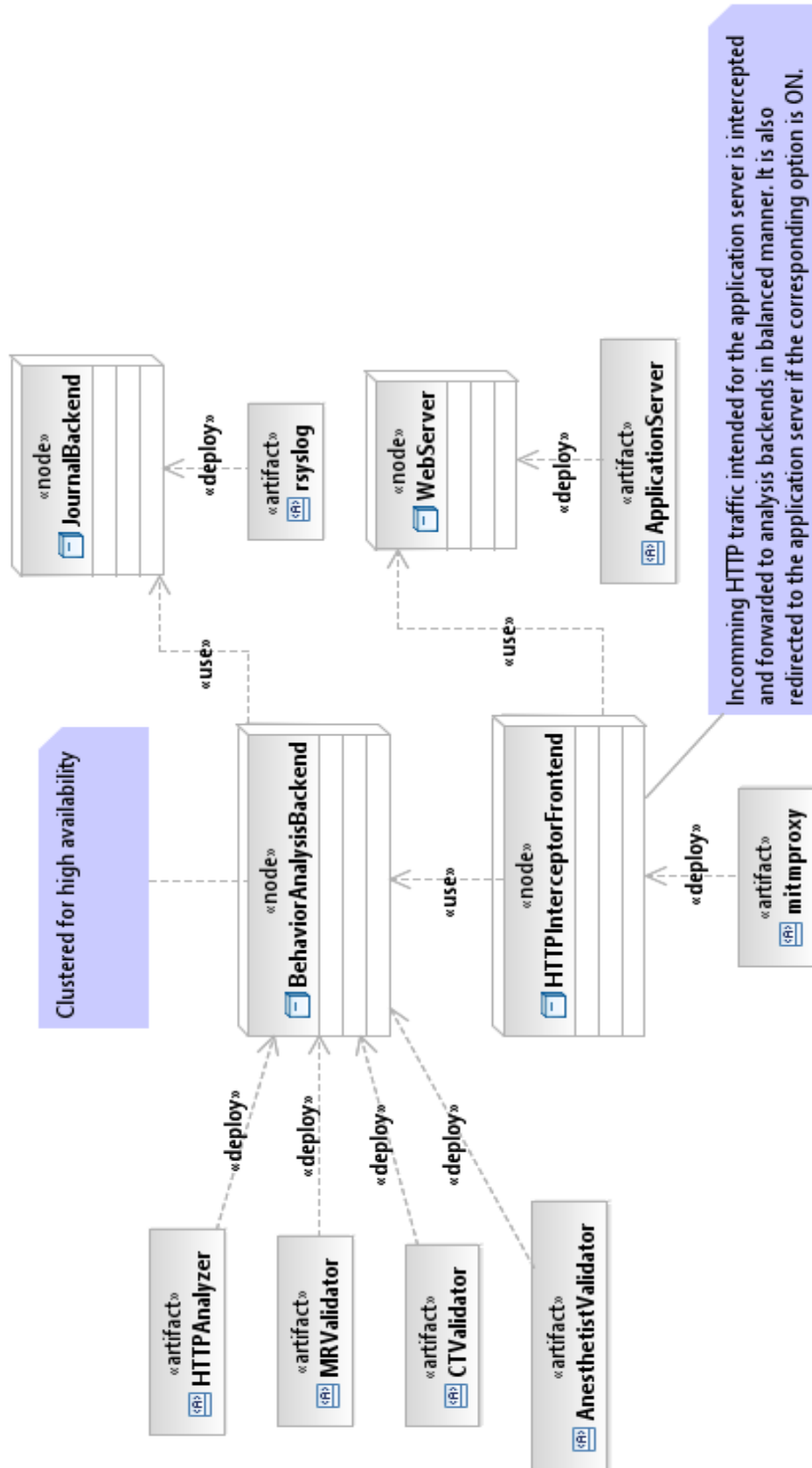


Рисунок 3.7 — Диаграмма развертывания анализатора
пользовательского поведения

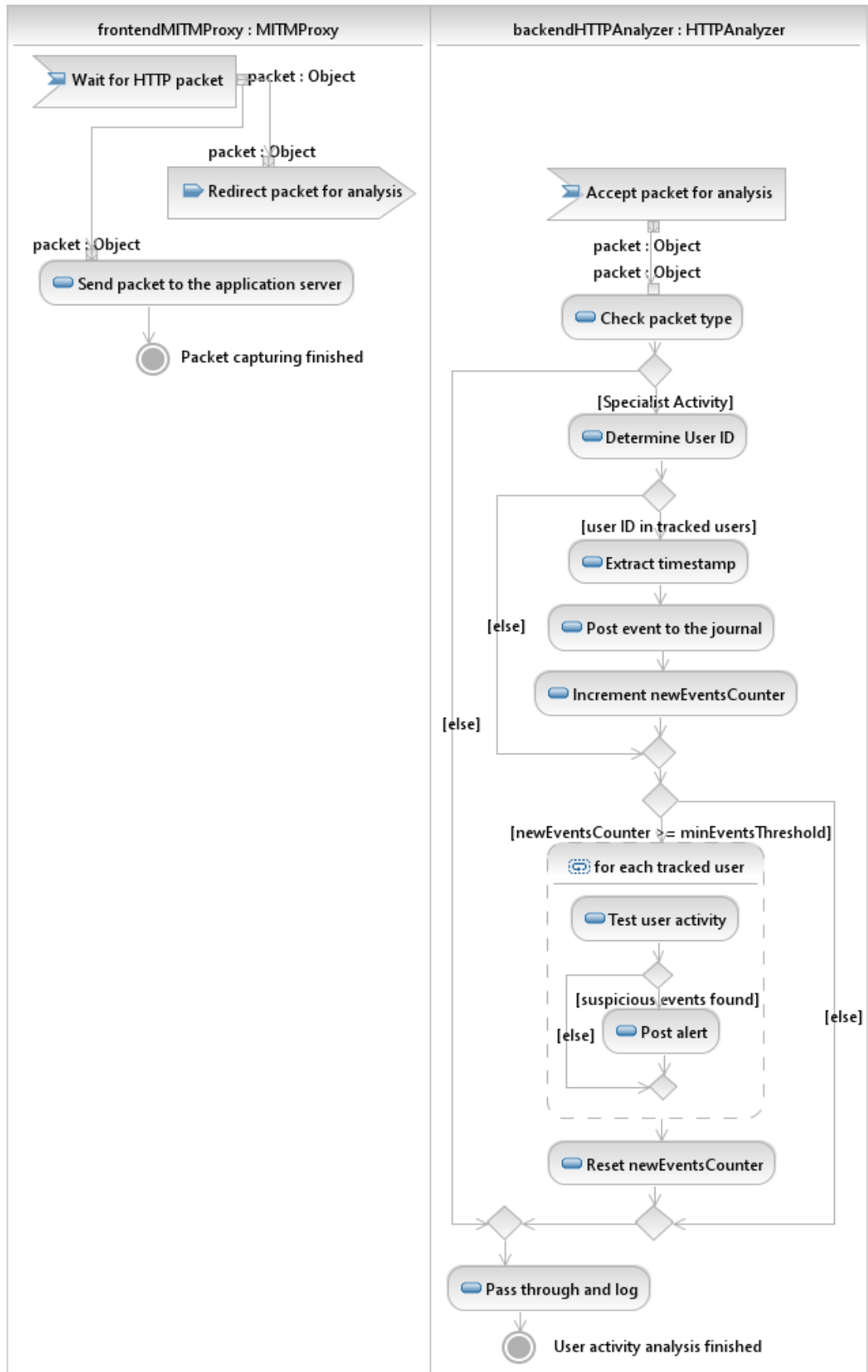


Рисунок 3.8 — Методика анализ пользовательской активности

Процесс, показанный на диаграмме, предполагает, что модели поведения специалистов уже обучены (обучение было инициировано вручную или автоматически с помощью средств планирования). Могут быть проанализированы только действительные пакеты HTTP, несущие данные об активности специалиста. Когда пакет прибывает в прокси mitmпроху на узле HTTPInterceptorFrontend, он перенаправляется для анализа на один из узлов BehaviorAnalysisBackend, где он проверяется, и из него извлекается значение временной метки (компонент HTTPAnalyzer). Если проверяемый пакет является допустимым пакетом HTTP, ассоциированным с активностью специалиста, происходит следующее: выясняется идентификатор пользователя, и в случае, если пользователь отслеживается, то событие регистрируется в журнале и инкрементируется счетчик новых входящих событий. Если минимальный порог количества новых входящих событий достигнут, то процедура их анализа запускается асинхронно. Ей передается временной интервал сбора событий (начало — `eventsCollectingStartTime`, конец — временная отметка последнего входящего события). Начинается анализ на предмет подлинности пользовательской активности с помощью `[Modality]SpecialistModel`, сбрасывается счетчик новых входящих событий до нуля, и фиксируется текущее время как новая отметка начала регистрации событий. Какую программу проверки выбрать для анализа событий, решает метод `getCheckerForUser` класса `UserActivityTester`. При возникновении подозрений вызывается метод `postAlert`, который может нести требуемую функциональность оповещения об опасностях и дополнительного журналирования событий. Во всех случаях сетевая активность журналируется (`passThroughAndLog`).

3.3. Построение виртуальной инфраструктуры

Функционирование описанных компонентов можно обеспечить в среде виртуальных машин, что поможет улучшить отказоустойчивость за счет механизмов миграции ВМ, активируемых при отказе физических серверов, а также уменьшить накладные расходы, связанные с администрированием серверных систем. Рекомендуемое распределение компонентов по виртуальным машинам приведено в таблицах 3.11 и 3.12, описывающих серверные роли, выполняемые ВМ. Функционирование всех ВМ предполагается под управлением ОС Linux x64, выбор конкретного дистрибутива определяется рекомендациями разработчиков разворачиваемого ПО.

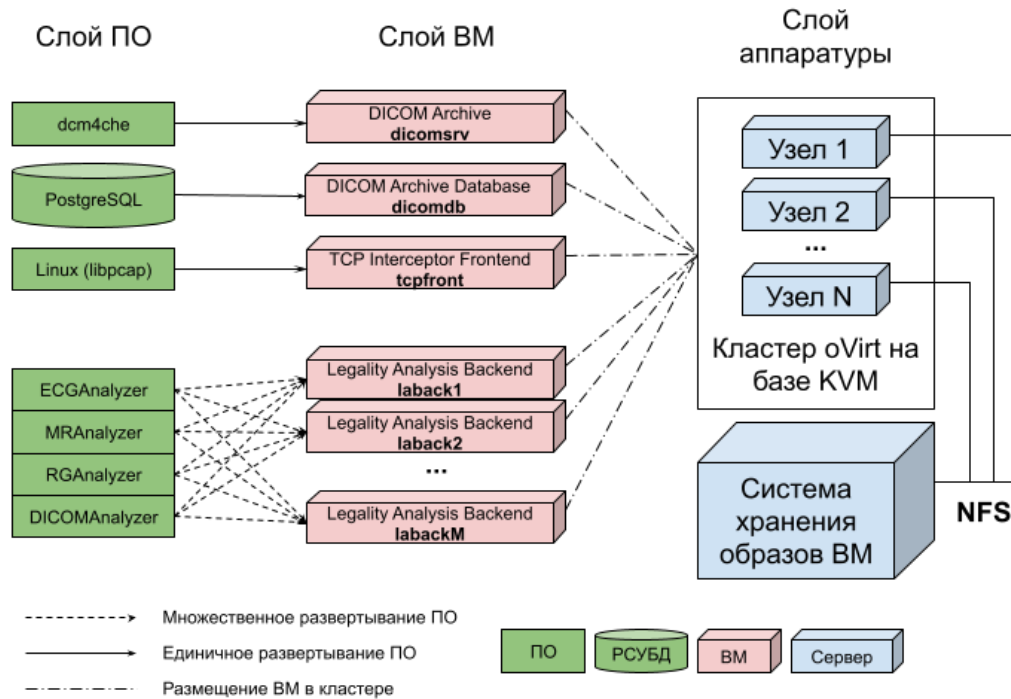
Таблица 3.11 — Серверные роли виртуальных машин (кластер для проверки корректности содержимого в архиве DICOM)

Имя ВМ	Серверная роль ВМ	Компоненты ПО	Описание ВМ
dicomsvr	DICOM Archive	dcm4che	Архив DICOM, содержащий медицинские данные. Является защищаемым объектом
dicomdb	DICOM Archive Database	PostgreSQL	База данных архива DICOM, необходимая для его функционирования
tcpfront	TCP Interceptor Frontend	Linux (libpcap)	Входящий трафик, предназначенный для PACS, просматривается на TCPInterceptorFrontend и направляется для анализа на узлы LegalityAnalysisBackend с балансировкой по алгоритму round-robin
laback1, ..., labackM	Legality Analysis Backend	DICOMAnalyzer RGAnalyzer MRAnalyzer ECGAnalyzer	Содержит компонент анализа содержимого файлов DICOM (DICOMAnalyzer), а также плагины проверки корректности медицинских данных для каждой модальности (RG, MR, ECG)

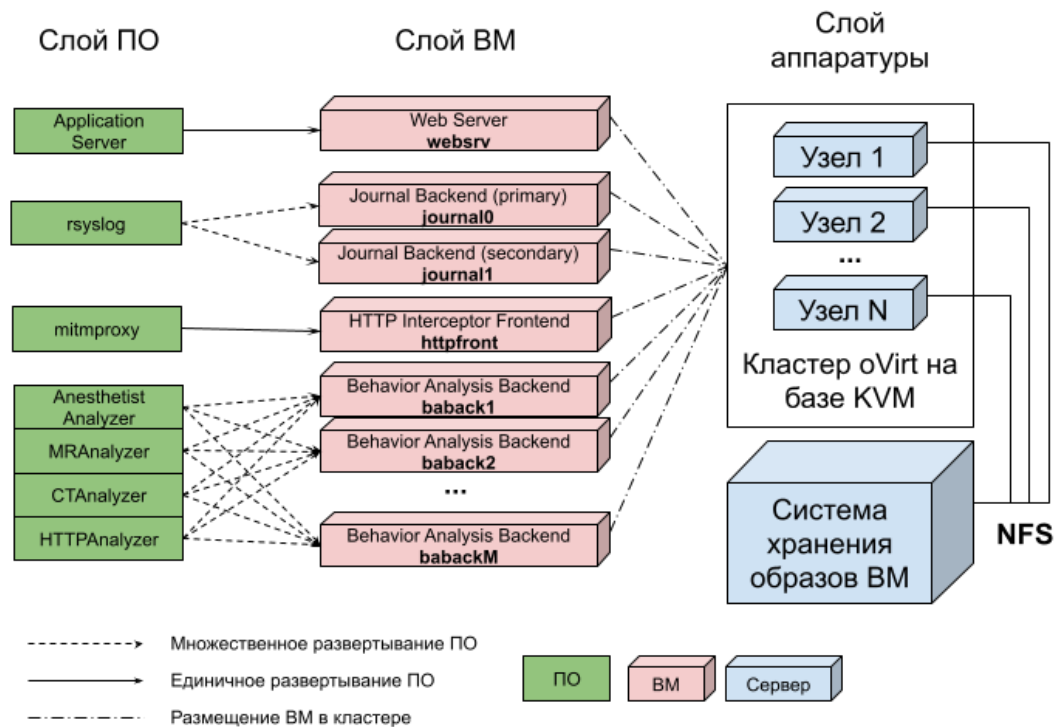
Таблица 3.12 — Серверные роли виртуальных машин (кластер для проверки корректности пользовательского поведения UBA)

Имя VM	Серверная роль VM	Компоненты ПО	Описание VM
websrv	Web Server	ApplicationServer	Сервер приложений МИС. Является защищаемым объектом
journal0	Journal Backend (primary)	rsyslog	Журнал пользовательских действий. Отказоустойчивость обеспечивается наличием первичного и вторичного экземпляров rsyslog [218]. При отказе первичного экземпляра данные направляются на вторичный. При возвращении первичного экземпляра, он вновь начинает принимать данные
journal1	Journal Backend (secondary)	rsyslog	
httpfront	HTTP Interceptor Frontend	mitmproxy	Входящий трафик, предназначенный для сервера приложений, просматривается на узле HTTPInterceptorFrontend и направляется для анализа на узлы BehaviorAnalysisBackend с балансировкой по алгоритму round-robin
baback1, ..., babackM	Behavior Analysis Backend	HTTPAnalyzer MRAnalyzer CTAnalyzer AnesthetistAnalyzer	Содержит компонент анализа поведения пользователей (HTTPAnalyzer), а также плагины проверки корректности пользовательского поведения для различных врачебных специализаций (CT, MR, Anesthetist)

На рис. 3.9 представлена схема развертывания кластеров проверки целостности архива DICOM (а) и UBA-системы (б) для уровня виртуализации. Отказоустойчивость кластеров обеспечивается за счет множественности экземпляров серверных ролей Legality Analysis Backend и Behavior Analysis Backend.



а) схема развертывания кластера проверки целостности архива DICOM



б) схема развертывания кластера анализа пользовательского поведения

Рисунок 3.9 — Развертывание виртуальных машин и ПО

На рис. 3.10 проиллюстрировано место сетевых анализаторов (кластеров) в типичной сетевой инфраструктуре медицинского учреждения.

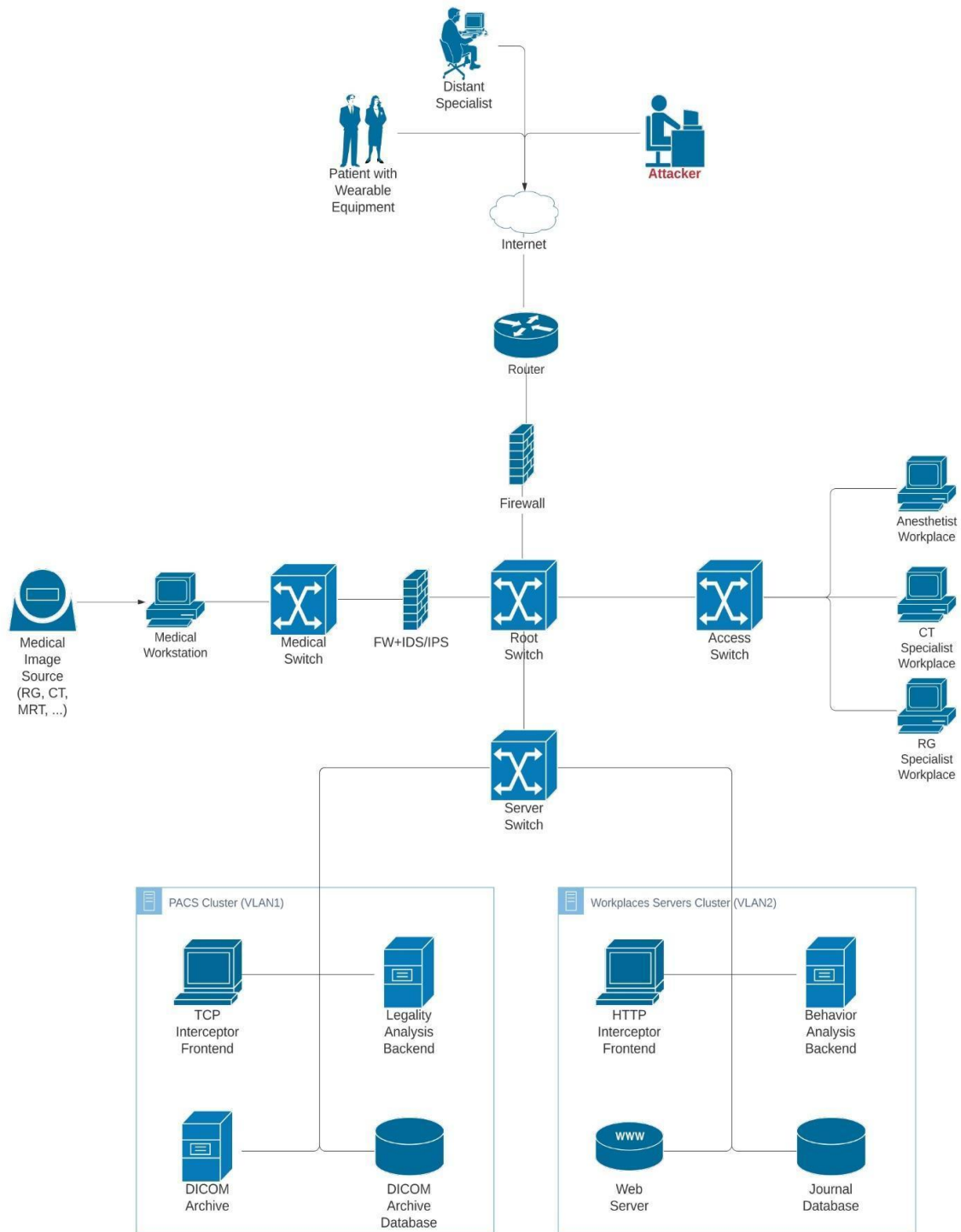


Рисунок 3.10 — Сетевая инфраструктура с анализом трафика

1. Новые серверные роли TCP Interceptor Frontend, Legality Analysis Backend вместе с существующими DICOM Archive и DICOM Archive Database формируют кластер PACS, для которого целесообразно выделение отдельного VLAN1. Трафик, который ранее направлялся на DICOM Archive, должен быть направлен на TCP Interceptor Frontend. После прохождения через Legality Analysis Backend он будет направлен на DICOM Archive автоматически — таково поведение по умолчанию. Последний аспект регулируется отдельной опцией, чтобы дать возможность альтернативного развертывания аналитического кластера: трафик, направляющийся непосредственно на DICOM Archive, может быть продублирован на TCP Interceptor Frontend с помощью зеркалирования портов на управляемом коммутаторе. В этом случае направление пакетов от Legality Analysis Backend к DICOM Archive было бы избыточно, а потому должно быть отключено.

2. Новые серверные роли HTTP Interceptor Frontend, Behavior Analysis Backend, Journal Backend вместе с существующим Web Server формируют кластер Workplaces Servers Cluster, для которого целесообразно выделение отдельного VLAN2. Трафик, который ранее направлялся на Web Server, должен быть направлен на HTTP Interceptor Frontend. После прохождения через Behavior Analysis Backend он автоматически будет направлен на Web Server — это его поведение по умолчанию. Последний аспект регулируется отдельной опцией, чтобы дать возможность альтернативного развертывания аналитического кластера: трафик, направляющийся непосредственно на Web Server, может быть продублирован на HTTP Interceptor Frontend с помощью зеркалирования портов на управляемом коммутаторе. В этом случае направление пакетов от Behavior Analysis Backend к Web Server было бы избыточно, а потому должно быть отключено.

3. Правила маршрутизации трафика, в том числе и между VLAN, должны быть разработаны с учетом специфики расположения рабочих

мест специалистов и не должны быть чрезмерно пермиссивными в целях уменьшения поверхности сетевой атаки.

Архив DICOM, серверы приложений, а также предложенные компоненты их защиты, формируют централизованную систему, предназначенную для развертывания в рамках локальной вычислительной сети медицинского учреждения [211, 214]. Базы данных, необходимые для функционирования защищаемых компонентов (DICOM Archive Database и прочие БД веб-приложений МИС), а также журнал пользовательской активности (JournalBackend) не могут быть вынесены за пределы периметра ЛВС, поскольку требуют соединения с низкими временными задержками. Они содержат все медицинские данные, приходящие в учреждение и генерируемые в нем, и являющиеся предметом интереса настоящей работы. Система имеет децентрализованные подсистемы аналитических кластеров для обеспечения горизонтальной масштабируемости и улучшения отказоустойчивости.

Первичный запуск системных функций требует участия медицинского специалиста. Медицинские данные пациента в архиве DICOM, равно как и данные активности пользователя МИС, будут подвергаться анализу только в том случае, если для соответствующего пациента или пользователя включено отслеживание в системе. При этом ассоциированные модели машинного обучения должны быть инициализированы на обучающей выборке регулярных легальных данных, задаваемой временным интервалом (классы `LegalityCheckingProvider` и `AuthenticityCheckingProvider`). После этого поведение системы сводится к непрерывному автоматическому анализу входящих потоков больших данных и выдаче предупреждений в случае обнаружения нежелательной активности — подозрительных DICOM-файлов или опасных пользовательских действий.

Выводы по главе

Предложенная архитектура аналитических кластеров предназначена для улучшения функциональности сред SIEM, развернутых в больницах. Она разработана специально, чтобы обеспечить интеграцию проверки самих медицинских данных и аналитики поведения пользователей для проверки деятельности медицинских специалистов.

Разработанная облачная инфраструктура как уровень архитектуры системы КД позволяет обеспечить повышение защищенности конфиденциальных данных, а также позволяет масштабировать ПО с помощью новых анализаторов и новых эффективных методов.

Программная реализация предложенных архитектурных принципов может лечь в основу фреймворка, предназначенного для сбора и анализа медицинских данных на предмет их подлинности, а также данных пользовательского поведения на предмет их легальности. Наличие подобного инструментария позволит исследователям, работающим в любом из указанных направлений, упростить задачи сбора данных и проведения экспериментов при отладке моделей машинного обучения.

Предложена архитектура системы, готовой к обработке больших данных при автономной проверке корректности медицинских записей в архивах DICOM, а также легальности пользовательского поведения. Условие отказоустойчивости — это наличие кластеризованных экземпляров компонентов DICOMAnalyzer и HTTPAnalyzer, развернутых на разных физических машинах с наличием или отсутствием уровня виртуализации или контейнеризации. Аналитические плагины должны развертываться с такой же избыточностью.

Глава 4. МЕТОДИКА ОЦЕНКИ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ ДЛЯ КОМПОНЕНТОВ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

В главе предложена метод экспериментального оценивания требуемого для резервирования количества вычислительных ресурсов при проектировании системы КД.

4.1. Метод оценки ресурсной эффективности для оценки

Эффективность использования ресурсов можно анализировать с помощью таких подходов, как анализ сложности алгоритмов и бенчмаркинг. Первый может предоставить информацию о производительности отдельных частей алгоритма программного обеспечения во времени, но вряд ли применим для анализа сложных программных систем. Второй — хорошо известный подход к анализу эффективности использования ресурсов программного обеспечения, однако он не учитывает специфику вычислительной инфраструктуры и планируемый объем запросов данных. Для решения поставленных задач необходимо построить модель и разработать методику, основанную на использовании экспериментальных оценок в среде [217], имитирующей функционирование ВК в заданных условиях и ограничениях.

Задачу оценки ресурсной эффективности компонентов архитектуры КД можно сформулировать следующим образом [218].

Пусть заданы технико-экономические характеристики функционирования ВК, представляющие собой набор заданных желаемых диапазонов

значений при заданном уровне обслуживания QoS, и планируемую форму и интенсивность запросов к ВС.

Тогда для пользовательских запросов $x \in X$ к ВС с системой КД с архитектурой V , для компонента Z_k с допустимыми технико-экономическими характеристиками, может быть задано отображение:

$$Z_k \subset V : x \xrightarrow{\Phi} R_k \in \mathbb{R}^n, \quad k = \overline{1, q},$$

где R_i — n -мерный вектор измеряемых вычислительных ресурсов. Отображение Φ является таким, что по наблюдаемому процессу X параметры R_i измеримы.

Отображение Φ в условиях виртуальности ресурсов может быть получено путем построения экспериментального стенда по технологии «инфраструктура как код», то есть получено в результате испытаний конфигурации Z_k при имитационном моделировании входного потока X . Иными словами отображение Φ представляет собой программно-конфигурационный код, содержащий виртуальную инфраструктуру, с входным сигналом в форме потока X и измеряемым скалярным выходом вектора измеряемых значений характеристик.

Для построения X может быть использовано имитационное моделирование. В ряде работ [219–221], посвященных построению математических моделей процессов веб-порталов, показано, что стохастические процессы, описывающие доступ пользователей, могут быть идентифицированы на основе типовых запросов. Для построения моделей трафика динамические модели используются широко. Существует направление, связанное с генерацией хаотического сигнала [222–225], имитирующего протокол TCP/IP. Для оценки ресурсов нет необходимости строить точные прогнозные модели процессов, поскольку искомые значения запасов вычислительных ресурсов зависят только от диапазона и интенсивности процессов, что может быть реализовано имитационным моделированием случайной величины с

заданной функцией распределения [226, 227]. В случае, если технико-экономические характеристики не сужают сильно канал, целесообразно использовать бета- или гамма-распределение, для узких каналов — распределение с «тяжелыми хвостами».

Разработан *метод анализа затрат вычислительных ресурсов* [219] для реализации систем контроля доступа, на основе подхода, использующего виртуальные стенды, обеспечивающие имитационную среду использования ВК на каждом уровне КД. Метод состоит из 7 шагов:

1. Построение типового запроса пользователя.
2. Создание виртуального экспериментального стенда, имитирующего среду использования компонентов архитектуры.
3. Программная реализация виртуальной инфраструктуры исследуемого компонента архитектуры в форме кода.
4. Формирование случайного сигнала с заданным законом распределения на основе типовых запросов пользователей.
5. Получение оценок значений ресурсов, требуемых для использования системы контроля доступа.
6. В случае решения задачи выбора вариантов реализации средств КД, выбор вариантов, имеющих меньшие ресурсные затраты.
7. Формирование архитектуры вычислительного комплекса с учетом полученных значений затрат вычислительных ресурсов.

Предложенные модель и метод [219] позволяют экспериментально решать задачи построения компромиссных решений: может быть решена задача выбора количества ресурсов, требуемых для полного внедрения КД, либо сокращать количество используемых модулей в условиях ограниченности ресурсов, заданных технико-экономическими требованиями к ВК, другие задачи, связанные с ограничением ресурсов, количества пользователей или допустимых внедрений элементов КД без затрат на дополнительные средства КД.

4.2. Технология реализации имитационного виртуального стенда для оценки вычислительных ресурсов

Технология реализации предложенного метода состоит в использовании виртуальных стендов, обеспечивающих имитационную среду использования ВК. Такой подход позволяет учитывать особенности современной цифровой среды и учитывать технико-экономические требования, предъявляемые к ВК.

Рассмотрим, например, задачу оценки вычислительных затрат при записи событий в БД при работе с веб-сервисами по компьютерным сетям с логированием действий пользователей.

Предполагается, что запись действий пользователей будет осуществляться в журнал событий. Для каждого устройства предлагается вести свою запись журнала действий, из-за разных видов интерфейсов, меняющихся в зависимости от типа устройства. Пусть каждое действие в журнале событий включает следующие данные:

- идентификатор пользователя;
- устройство (идентификатор конкретного устройства);
- действие (уникальное название или идентификатор, чтобы не путать действия; если одно и то же действие может запустить разные кнопки, то и идентификатор действий тоже должен быть разным);
- время совершенного действия.

Для проведения экспериментальных исследований будем использовать следующие данные: объём исходного файла с данными составляет 450 МБ; файл содержит 12000 записей ResearchSubject и 55458 записей ResearchResult; данные представлены в слабоструктурированном формате JSON [231].

Перед началом эксперимента создаются 3 виртуальные машины (ВМ) (Client, Server, Database) с заданными характеристиками. Для повторных экспериментов, если они были созданы ранее, предварительно удаляются существующие ВМ для обеспечения чистоты эксперимента между повторениями. Структура экспериментального стенда приведена на рис. 4.1 и в табл. 4.1.

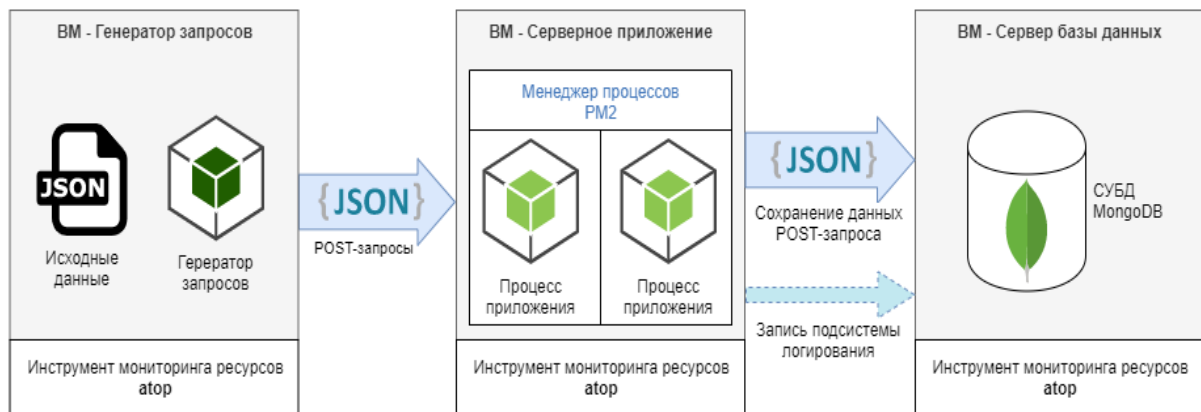


Рисунок 4.1 — Схема эксперимента

Таблица 4.1 — Параметры виртуальных машин

	Количество ядер ЦПУ (шт)	Объем ОЗУ (Мб)	Максимально разрешенная загрузка ядер ЦПУ (%)	Пропускная способность подсистемы ввода-вывода (Мб)
Client	4	8192	100	—
Server	2	2048	100	—
Database (MongoDB)	2	2048	50	25

После создания ВМ, установки и запуска серверного ПО и СУБД начинается сам эксперимент. Исходные данные загружаются в оперативную память ВМ Client. После их полной загрузки начинается отправка данных с заданными параметрами.

На первом этапе эксперимента производится отправка POST-запросов к серверу на сохранение записей ResearchSubject. На втором этапе эксперимента производится отправка POST-запросов к серверу на сохранение записей ResearchResult. В обоих случаях каждый POST-запрос содержит информацию только об одной записи. Таким образом, число запросов соответствует количеству исходных записей данных. Для логирования к запросу добавляется код, приведенный на рис. 4.2.

```
Model.afterRemote('**', (ctx, modelInstance) => {
  const params = ctx.req.body.data || ctx.req.body;
  const { id, researchSubjectId } = params;
  const userId = researchSubjectId || id;
  if (!userId) {
    return Promise.resolve();
  }
  return Model.app.models.ResearchSubject.findById(userId)
    .then((researchSubject) => {
      Model.app.models.ActionLog.logEvent(modelInstance, ctx, userId,
!!researchSubject);
    });
});
```

Рисунок 4.2 — Исходный код алгоритма логирования запросов к серверному ПО

Эксперимент производится с двумя различными конфигурациями серверного ПО. В первом случае производится только сохранение данных (см. примеры записей данных на рис. 4.3, 4.4). Во второй конфигурации добавлен программный код (рис. 4.5), осуществляющий логирование каждого запроса, полученного серверным ПО. При этом на каждый поступивший запрос в базе данных создается дополнительная запись, общий вид которой представлен на рис. 4.4. Эти записи создаются после выполнения каждого POST-запроса.

```
{
  "_id": ObjectId("5dce6295ef49df9ad703df17"),
  "sessionId":
"cPbEMLwbr16DH2ySQWELHoUSHpZ3faAqVrp59jvKQWEES0E4N6Ue2m
0BYnTDaWlH",
  "login": "abcd1234541104000",
  "researcherId": ObjectId("5db81cb3db867f7f119baabb"),
  "alias": "abcd00001",
  "privateResearchSampleId": "5dce608e83d1929b0423aaaa",
  "createdAt": "2019-11-15T08:32:21.370Z",
  "updatedAt": "2019-11-28T10:43:50.744Z"
}
```

Рисунок 4.3 — Пример записи ResearchSubject

```
{
  "_id": ObjectId("5dd90de7c383bff471725ac9"),
  "embeddedPsychotestId": "5dce5d89ef49df9ad703db2a",
  "embeddedPsychotestIndex": 4,
  "data": {
    "answers": [
      // Multiple Objects
    ],
    "scales": [
      // Multiple Objects
    ],
    "metadata": {
      "platformOs": "Windows 10 64-bit",
      "userAgent": "Mozilla/4.0 (Windows NT 10.0; Win64; x64) Ap-
pleWebKit/536.36 (KHTML, like Gecko) Chrome/63.0.3282.140 Safari/536.36
Edge/17.17763",
      "platformDescription": "Microsoft Edge 17.17763 on Windows 10 64-
bit",
      "startTime": "2019-11-23T10:43:06.095Z",
      "endTime": "2019-11-23T10:44:19.021Z"
    }
  },
  "researcherId": ObjectId("5db81cb3db867f7f119baabb"),
  "researchSampleId": ObjectId("5dce608e83d1929b0423aaaa"),
  "researchSubjectId": ObjectId("5dce6295ef49df9ad703df1b"),
  "createdAt": "2019-11-23T10:45:59.107Z",
  "updatedAt": "2019-11-23T10:45:59.107Z"
}
```

Рисунок 4.4 — Пример записи ResearchResult

```
{
  "_id": ObjectId("5fc8e399f50a5851737b43af"),
  "userId": "5dce6295ef49df9ad703df17",
  "exists": true,
  "method": "POST",
  "request": "ResearchSubject.create",
  "createdAt": ISODate("2020-12-03T13:09:44.173Z"),
  "updatedAt": ISODate("2020-12-03T13:09:44.173Z")
}
```

Рисунок 4.5 — Пример записи ActionLog

Сбор данных об используемых ресурсах осуществляется с помощью утилиты Atop с интервалом в 1 секунду.

Отправка запросов осуществляется в 4 потока, до 10 одновременных запросов.

Задержка между отправками пакетов по 10 запросов равна 300 мс, а задержка между этапами эксперимента — 60 с.

Максимальное ожидание ответа от сервера — 10 с.

Код выполняется с использованием Node.JS версии 12.x.

Серверное ПО запущено под управлением менеджера процессов PM2 со следующими параметрами:

```
pm2 start /vagrant/application/index.js --node-args="--
```

```
max_old_space_size=1024" -i max --restart-delay=5 --max-restarts=1000
```

Это означает, что объем выделенной для процесса ОЗУ не превышает 1024 МБ, количество параллельно работающих процессов равно числу ядер ЦПУ (т. е. 2).

Задержка перед повторным запуском процесса в случае отказа 5 с.

Максимальное число перезапуска процесса — 1000 раз.

Код выполняется с использованием Node.JS версии 12.x.

Установлена MongoDB версии 3.2.

Содержание основного конфигурационного файла (mongod.conf):

storage:

dbPath: /var/lib/mongodb

journal:

enabled: true

systemLog:

destination: file

logAppend: true

path: /var/log/mongodb/mongod.log

net:

port: 27017

bindIp: 0.0.0.0

processManagement:

timeZoneInfo: /usr/share/zoneinfo

Диаграмма последовательностей для эксперимента для оценки ресурсной эффективности записи действий пользователей в журнал событий приведена на рис. 4.6.

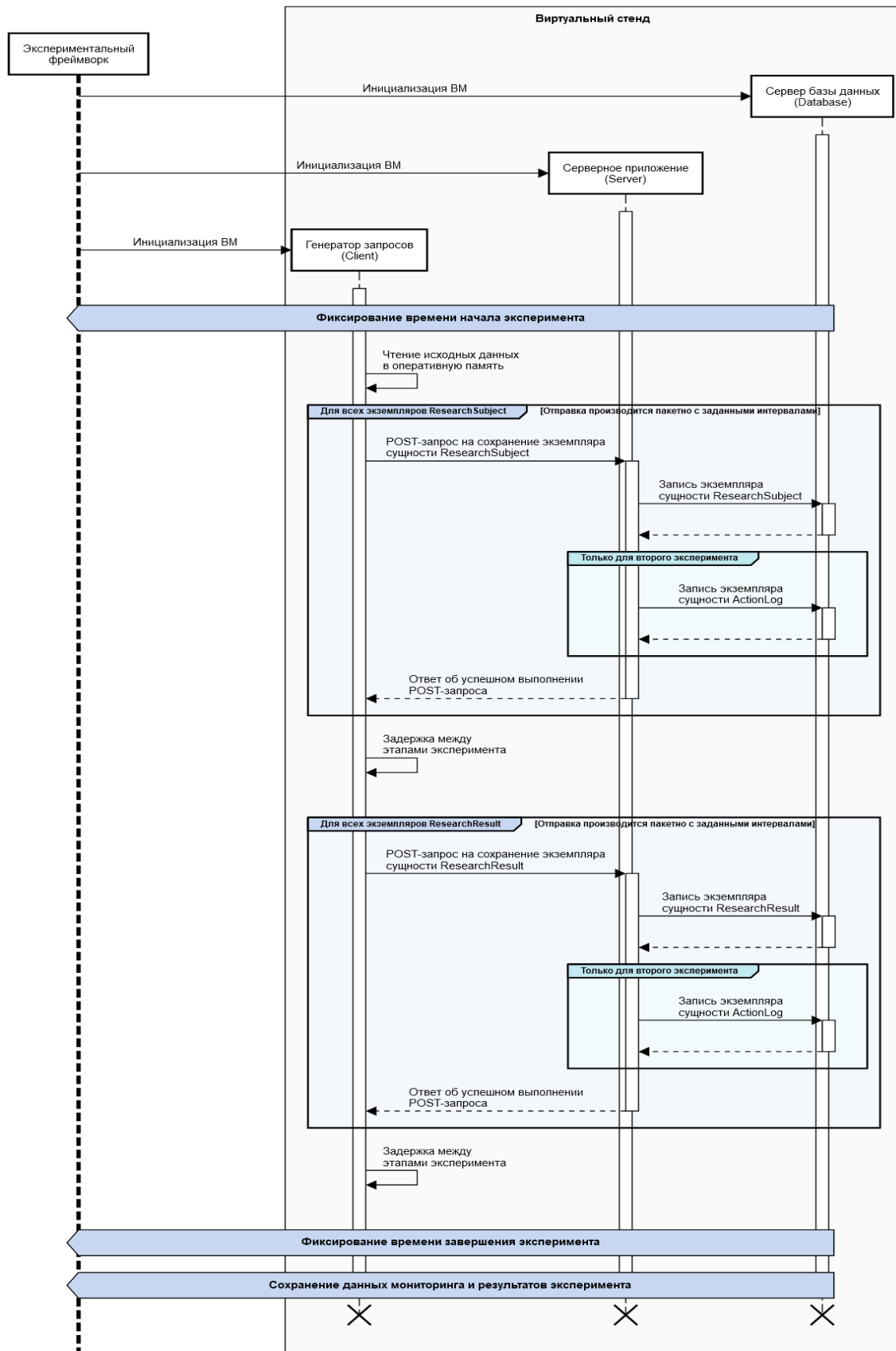


Рисунок 4.6 — Диаграмма последовательностей эксперимента

Результаты вычислительного эксперимента приведены на рис. 4.7–4.15 и табл. 4.2.

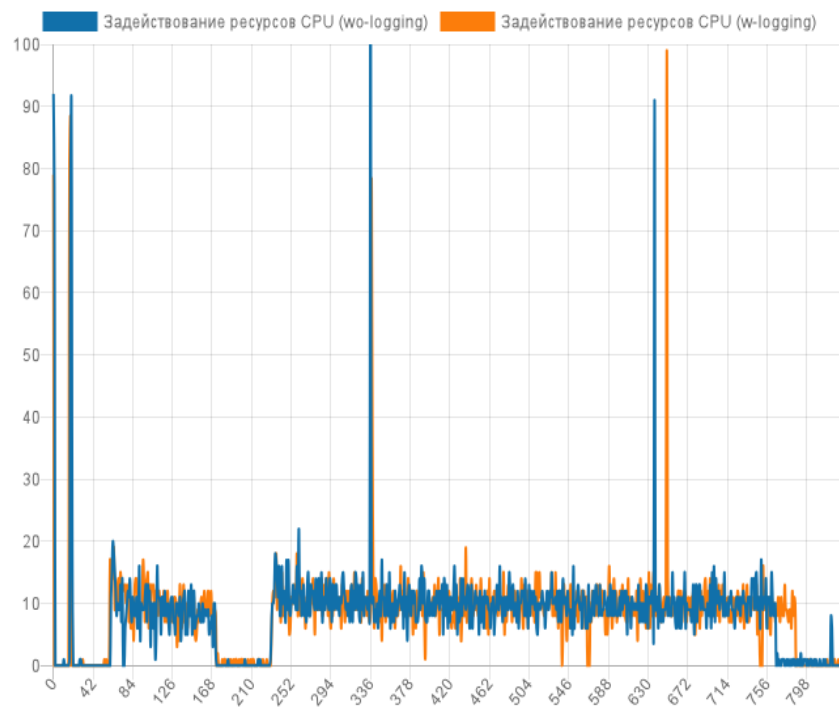


Рисунок 4.7 — Используемые ресурсы СПУ VM Client, %

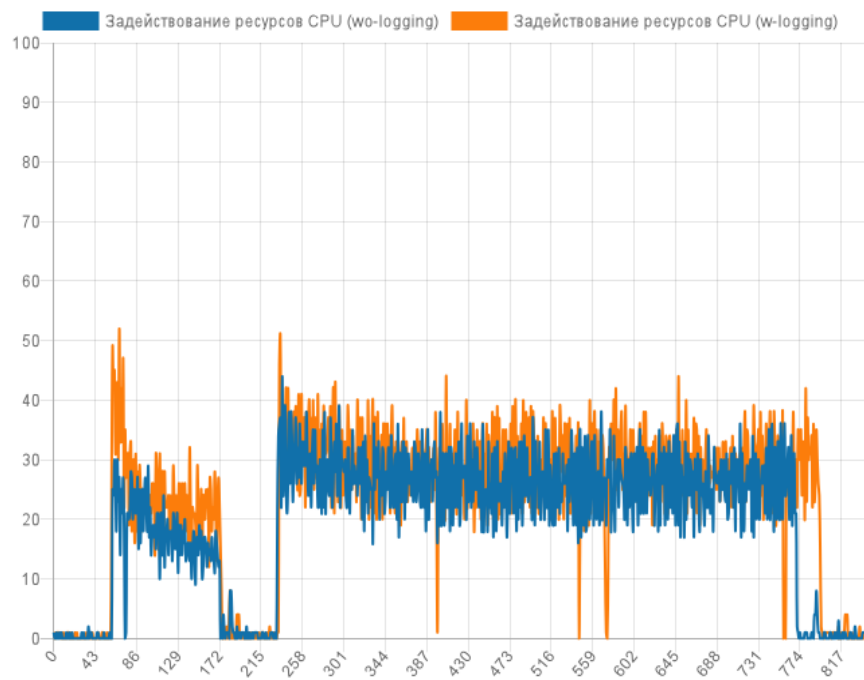


Рисунок 4.8 — Используемые ресурсы СПУ VM Server, %

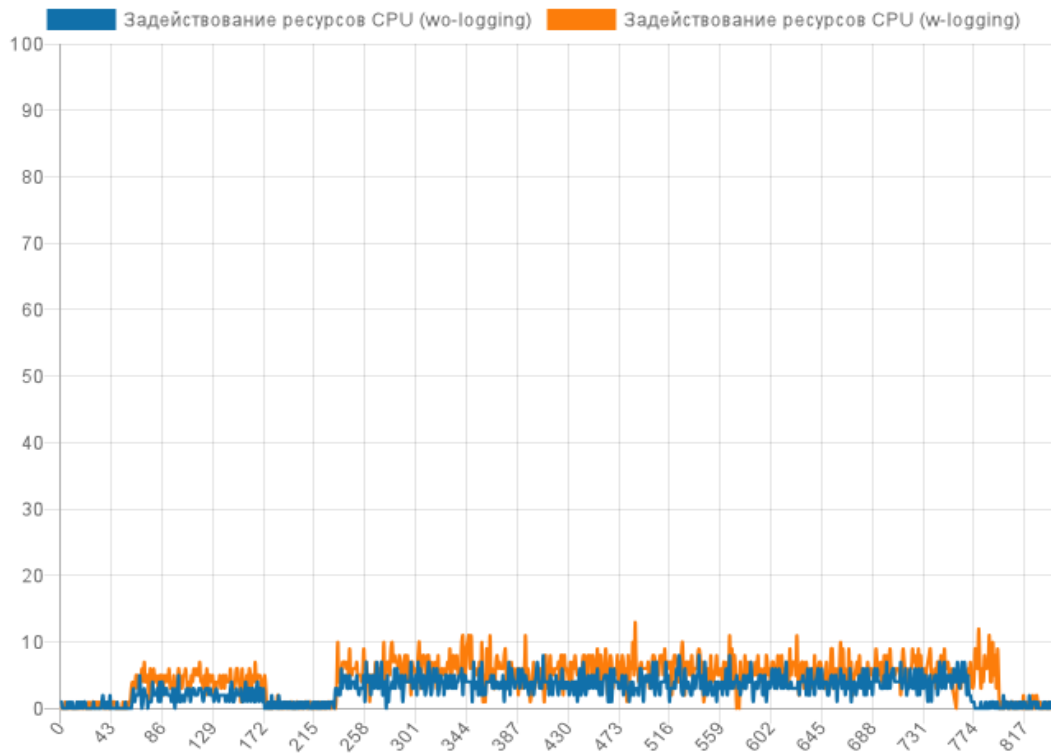


Рисунок 4.9 — Используемые ресурсы ЦПУ VM MongoDB, %

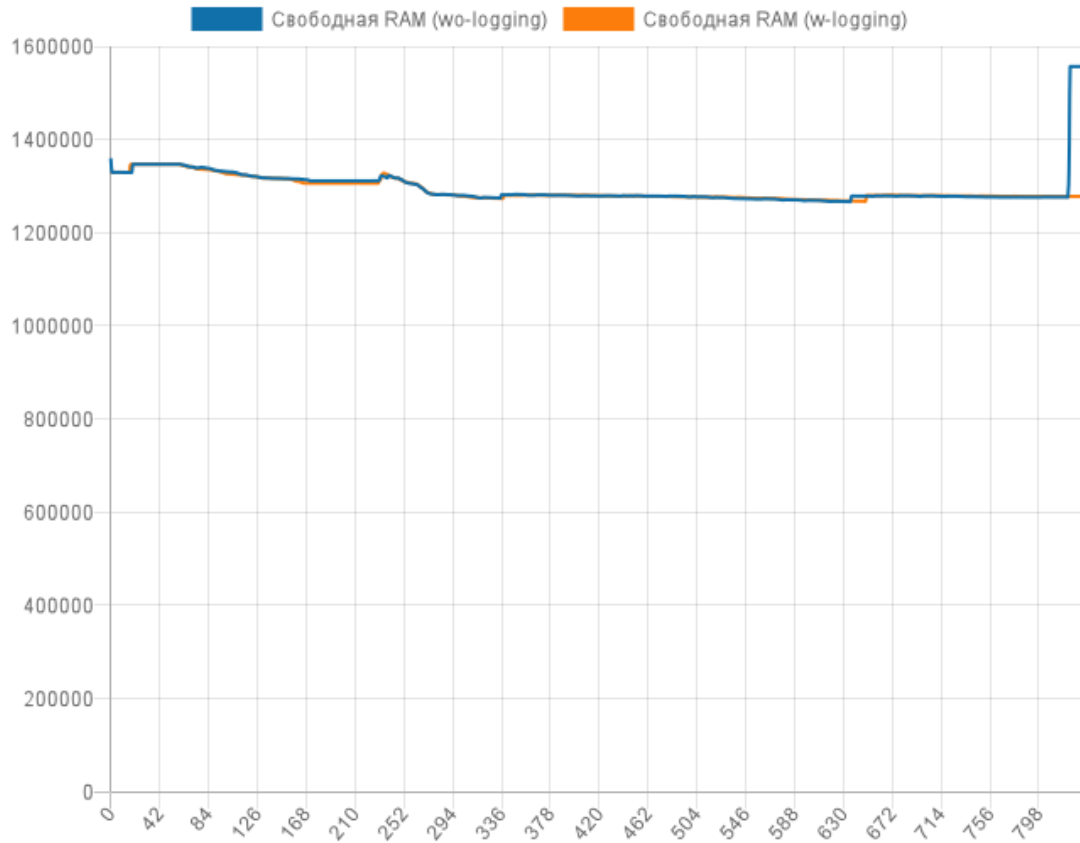


Рисунок 4.10 — Используемые ресурсы памяти VM Client, Мб

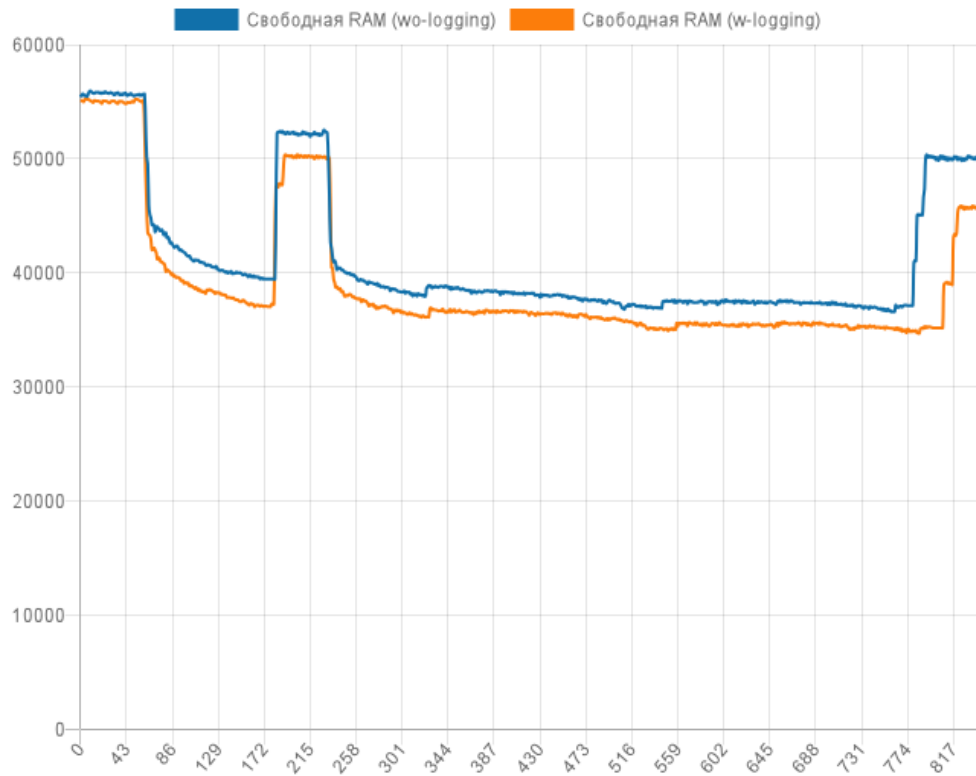


Рисунок 4.11 — Используемые ресурсы памяти VM Server, Мб

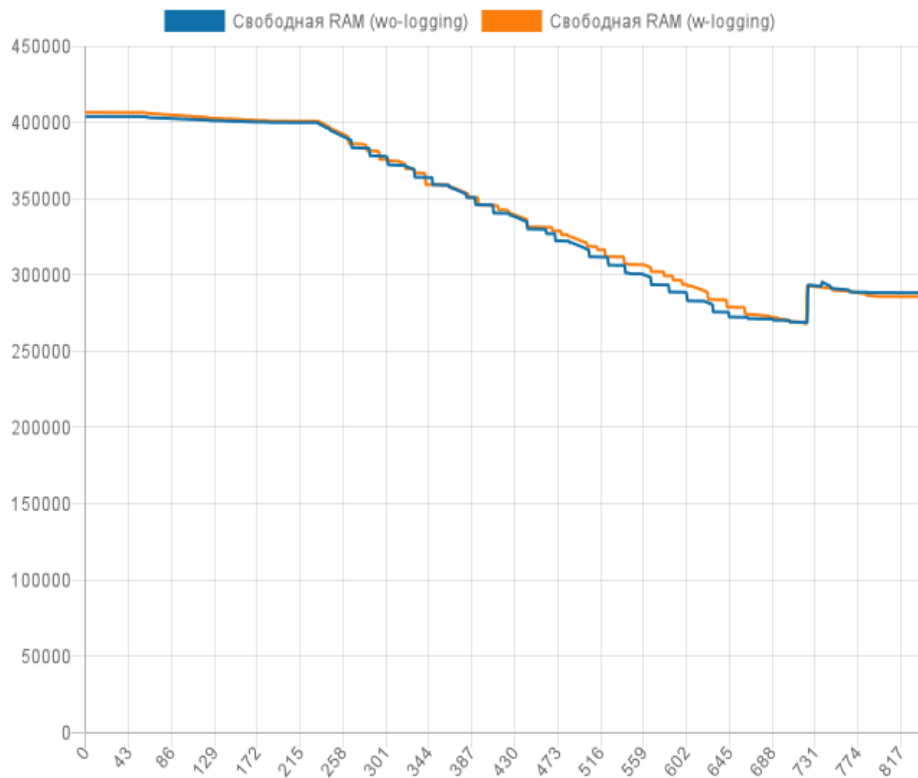


Рисунок 4.12 — Используемые ресурсы памяти VM MongoDB, Мб

Таблица 4.2 — Показатели ресурсных затрат
на логирование действий пользователей

Ресурсный показатель	Значение без использования логирования	Значение с использованием логирования	Разница в %
ЦПУ VM client	7.49	7.21	3.3
ЦПУ VM server	19.71	22.23	12.7
ЦПУ VM mongodb	2.85	3.37	52.9
Память VM client	1296827.18	1295665.40	0.08
Память VM server	41344.79	39146.05	5,32
Память VM mongodb	340911.11	341359.78	0,13

Таким образом, для рассматриваемого примера экспериментально установлено, что использование логирования действий пользователей существенно влияет только на загрузку процессоров Server и сервера Mongodb, незначительно увеличивает загрузку памяти сервера. Внедрение контроля доступа с логированием требует внесение соответствующих запасов ресурсов в ВК.

Выводы по главе

Сформулирована задача оценки ресурсной эффективности компонентов архитектуры КД в условиях заданных технико-экономических характеристик функционирования ВК, представляющих собой набор заданных желаемых диапазонов значений при заданном уровне обслуживания QoS и планируемой интенсивности запросов к ВС.

Предложено искомое отображение входных параметров в характеристики вычислительных ресурсов получить путем построения экспериментального стенда по технологии «инфраструктура как код», то есть получить в результате натурных испытаний конфигурации при имитационном моделировании входного потока.

Разработан метод анализа затрат вычислительных ресурсов для реализации систем контроля доступа, на основе подхода, использующего стенды на виртуальных машинах для создания имитационной вычислительной среды использования ВК на каждом уровне КД.

Рассмотрены вопросы технологической реализации метода для задачи оценки вычислительных затрат при записи событий в слабоструктурированной БД при работе с вычислительными сервисами по компьютерным сетям с логированием действий пользователей.

Глава 5. СОВЕРШЕНСТВОВАНИЕ КОНТРОЛЯ ДОСТУПА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ РЕАКЦИЙ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С ЭЛЕМЕНТАМИ ИНТЕРФЕЙСА

Предложен метод контроля доступа на основе использования психологических реакций, которые могут быть измерены при работе с интерфейсами; метод экспериментально проверен на большой выборке; разработана методика использования реакций в системах КД.

5.1. Архитектура SIEM-систем с модулем анализа реакций пользователей

В рамках концепции архитектур SIEM-систем в условиях больших данных [37, 228] использование технологий анализа поведения пользователей (User behavior analytics, UBA) [47] получает распространение. Решения UBA изучают шаблоны человеческого поведения, а затем применяют алгоритмы обнаружения аномалий этих шаблонов. Например в [20], когда злоумышленник в сети компании может использовать украденные учетные данные для незаметного сбора конфиденциальных данных. Такое поведение трудно обнаружить, если оно не вызывает предупреждение о нарушении доступа или утечке данных.

Альтернативой многоуровневой технологии является использование встраиваемых динамических моделей в интернет-приложения [229]. В работе предлагается подход с разработанной структурой, включающий ситуационные модели и интерпретатор. Модель содержит заданные конечные наборы состояний, переходов и правил, определяющих переходы. Интерпретатор отслеживает и сохраняет текущие состояния модели, проверяя условия переходов. Известен подход [48], включающий получение харак-

теристик действий пользователя (логин пользователя, движение мыши, среднее время между нажатием клавиши мыши и началом движения курсора, скорость набора текста и др.). Подобные исследования интересны, но носят ограниченный характер — для многопользовательских систем получение, передача, хранение и обработка данных вычислительно очень затратны. Кроме того, использование манипулятора мыши для анализа реакций сложно реализуемо — задержки сильно зависят от производителя и от поверхности, на которой в данный момент работает пользователь. Кроме того, веб-интерфейсы подразумевают использование их на разных устройствах, в том числе с сенсорными экранами.

Существуют подходы к КД, связанные с анализом всех параметров действий пользователя (движение мыши, среднее время между нажатием клавиши мыши и началом движения курсора, скорость набора текста и др.). Подобные исследования носят ограниченный характер — для многопользовательских систем получение, передача, хранение и обработка всех движений курсора мыши вычислительно затратны, зависят от используемого оборудования, версий программного обеспечения. Современные психологические исследования [230, 231] выявили достоверность данных по исследованию реакций, полученных с использованием веб-интерфейсов. Эти результаты дают основание для разработки информационной технологии построения архитектуры многоуровневого КД, использующего в качестве дополнительного идентификатора пользователя время реакций при работе с элементами интерфейса (время реакции — период времени от внешнего стимула до соответствующей реакцией индивидуума; оценка времени реакции — это один из важных методов изучения скорости обработки информации центральной нервной системой человеком и скоординированной реакции периферических движений).

На рис. 5.1 представлена ситуация, когда «Пользователь 1» ввел все необходимые данные для доступа, однако он может быть заменен другим

пользователем, как с рабочего места «Пользователя 1», так и из другого места. Если в системе отсутствуют блоки, связанные с поведением пользователя и его местонахождением, «Пользователь 2» может осуществлять доступ к данным.

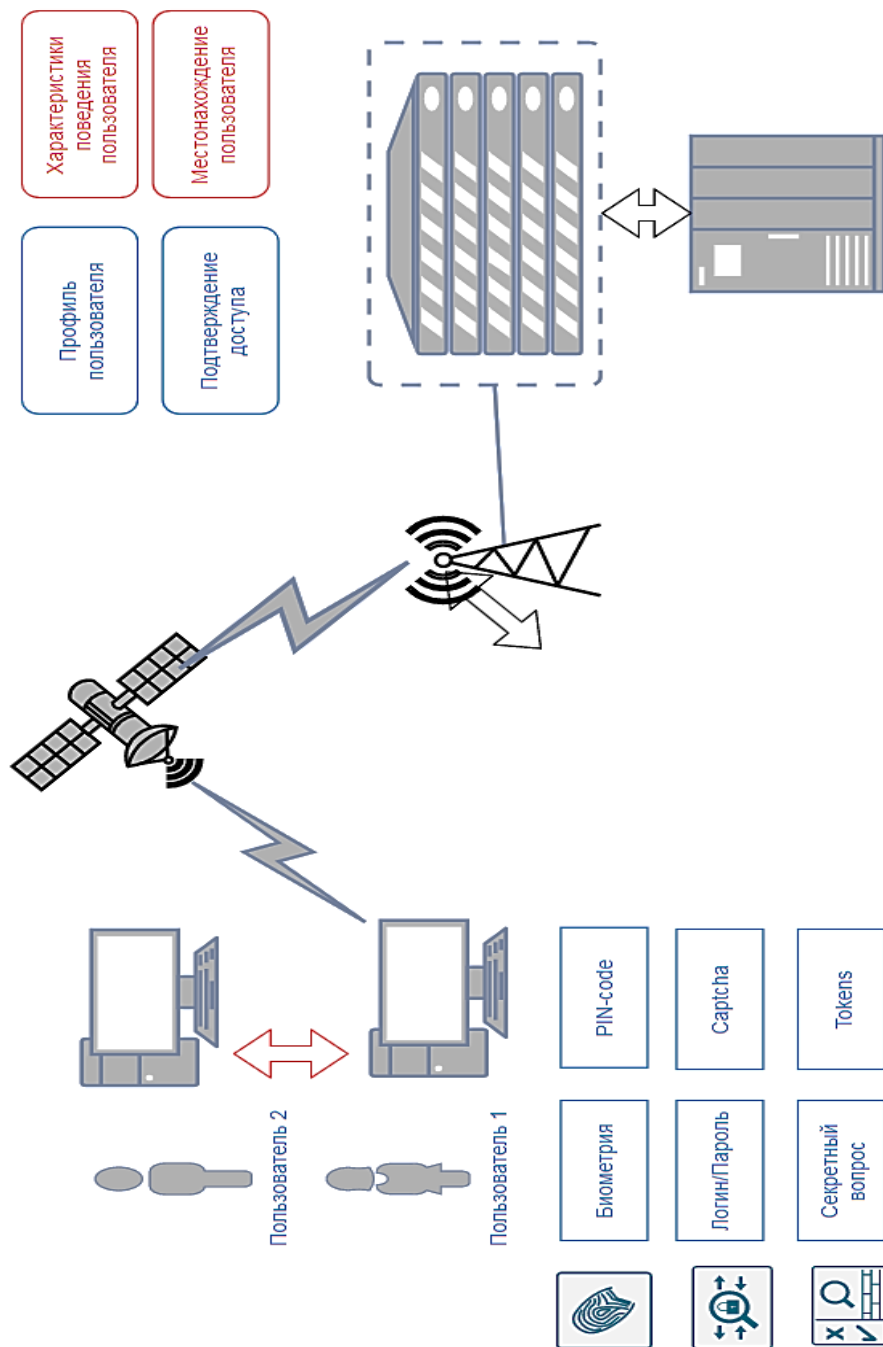


Рисунок 5.1 — Пример системы с контролем доступа

Таким образом, предлагается разработать на уровне анализа данных КД метод, использующий в качестве дополнительного идентификатора пользователя время реакций при работе с элементами интерфейса. При этом сбор данных будет осуществляться встроенными программными средствами, а элементы интерфейса будут передаваться в систему.

5.2. Экспериментальные исследования

Исследования проводились с помощью цифровой платформы DigitalPsyTools [12]. Система является одновременно цифровой платформой с веб-интерфейсом и инструментом психодиагностики, используемым для популяционных исследований в системе образования. В ВС в элементы интерфейса встроены платформонезависимые функции оценки когнитивных реакций.

Между приложением внешнего стимула и соответствующей двигательной реакцией на стимул существует определенный период времени, называемый временем реакции (ВР). Оценка этого времени — один из важных методов изучения скорости обработки когнитивной информации человеком и скоординированной реакции периферических движений. Время реакции определяется как интервал времени между предъявлением стимула и появлением у испытуемого соответствующей произвольной реакции.

На время реакции влияют многие факторы, такие как пол, возраст, физическое состояние, утомляемость, состояние здоровья и т. п. Увеличенное время реакции означает снижение производительности. Время показа является временем от начала показа страницы, на которой можно сделать действие, до времени на момент, когда пользователь осуществил какое-либо действие в интерфейсе. Иными словами, ВР — это время от появле-

ния стимула до нажатия кнопки (на основании психологических терминов).

Время реакции пользователя для конкретного действия можно разделить на:

- минимальное ВР (минимальная латентность ответа);
- максимальное ВР (максимальная латентность ответа);
- усредненное ВР (усредненная латентность ответа).

Для анализа использованы реакции 23 102 студентов при ответе на 4 вопроса:

1. Основа обучения (выбор из трех вариантов: бюджетная/контрактная/целевая).
2. Вы поступили на ту специальность, которую хотели? (Да/Нет).
3. Укажите профиль Вашего образования (выбор из четырех вариантов: технический/гуманитарный/естественнонаучный/нет профиля).
4. Программа обучения (выбор из четырех вариантов: бакалавриат/магистратура/специалитет/аспирантура).

Анкета организована в виде веб-интерфейса. После получения архив с опросом на устройстве клиента распаковывается и загружается в браузер. В каждом элементе опроса фиксируется ответ и время реакции в миллисекундах (с момента загрузки до выбора ответа и нажатии кнопки «далее»), т. е. время, за которое пользователь прочитал вопрос, выбрал нужный вариант и нажал кнопку «далее». Объемный опрос включал когнитивные тесты, поэтому пользователь был заинтересован перейти на следующую страницу. Данные передавались в платформу после окончания всего опроса, либо после закрытия пользователем веб-страницы. Это гарантировало невмешательство сетей в оценку времени реакции.

Также были собраны сведения об используемых операционных системах и браузерах при проведении опроса [20]. Эти сведения отображены на рис. 5.2 и рис. 5.3.

Гипотеза заключалась в том, что время реакции на разные ответы с разными элементами интерфейса различается [192]. Гипотеза анализа данных о времени реакции заключалась в возможности определения зависимости в реакциях пользователей при работе с элементами интерфейса при ответе на заданный вопрос, а также в возможности определения индивидуальных психомоторных реакций при работе с интерфейсом.

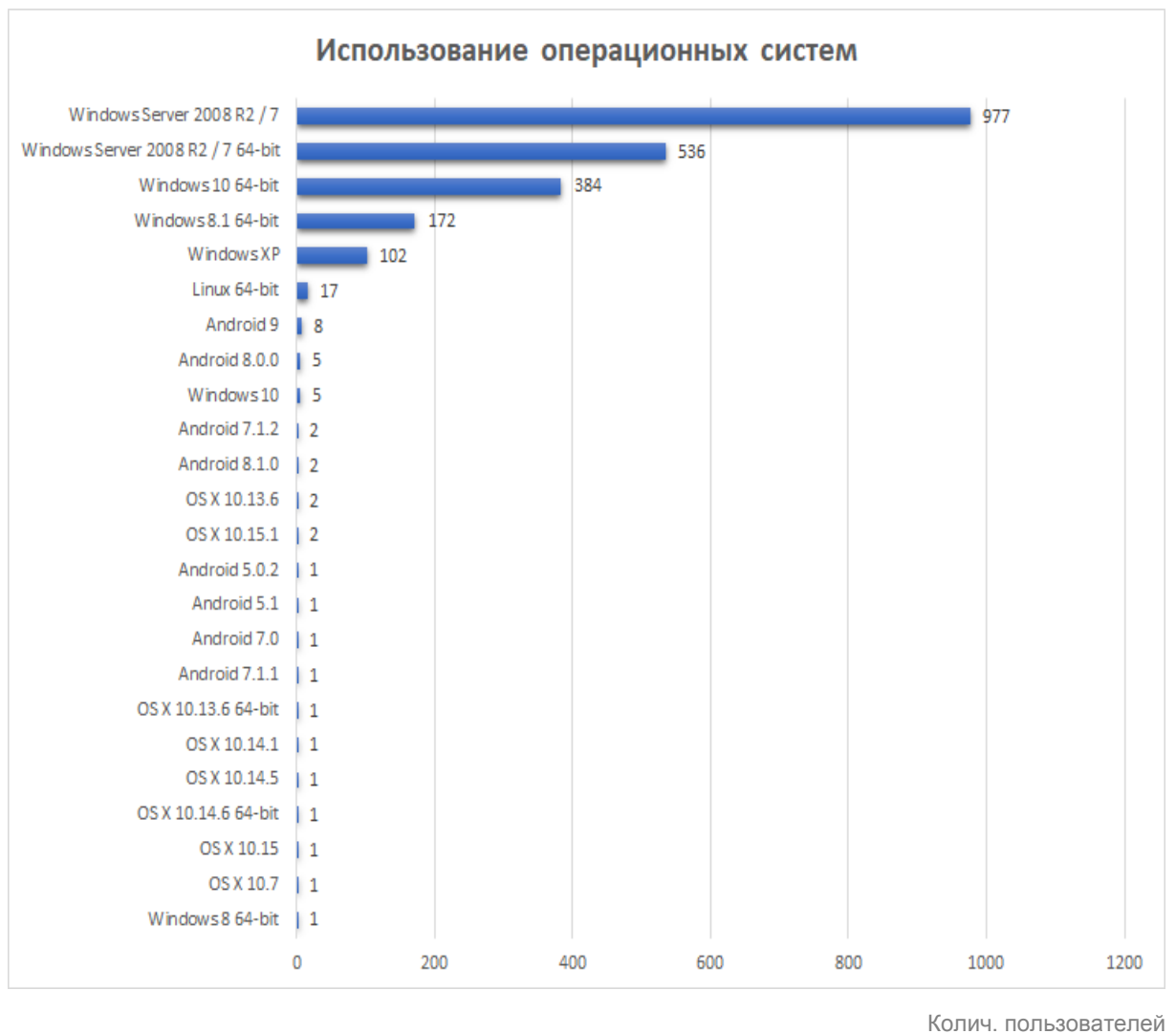


Рисунок 5.2 — Операционные системы, используемые пользователями

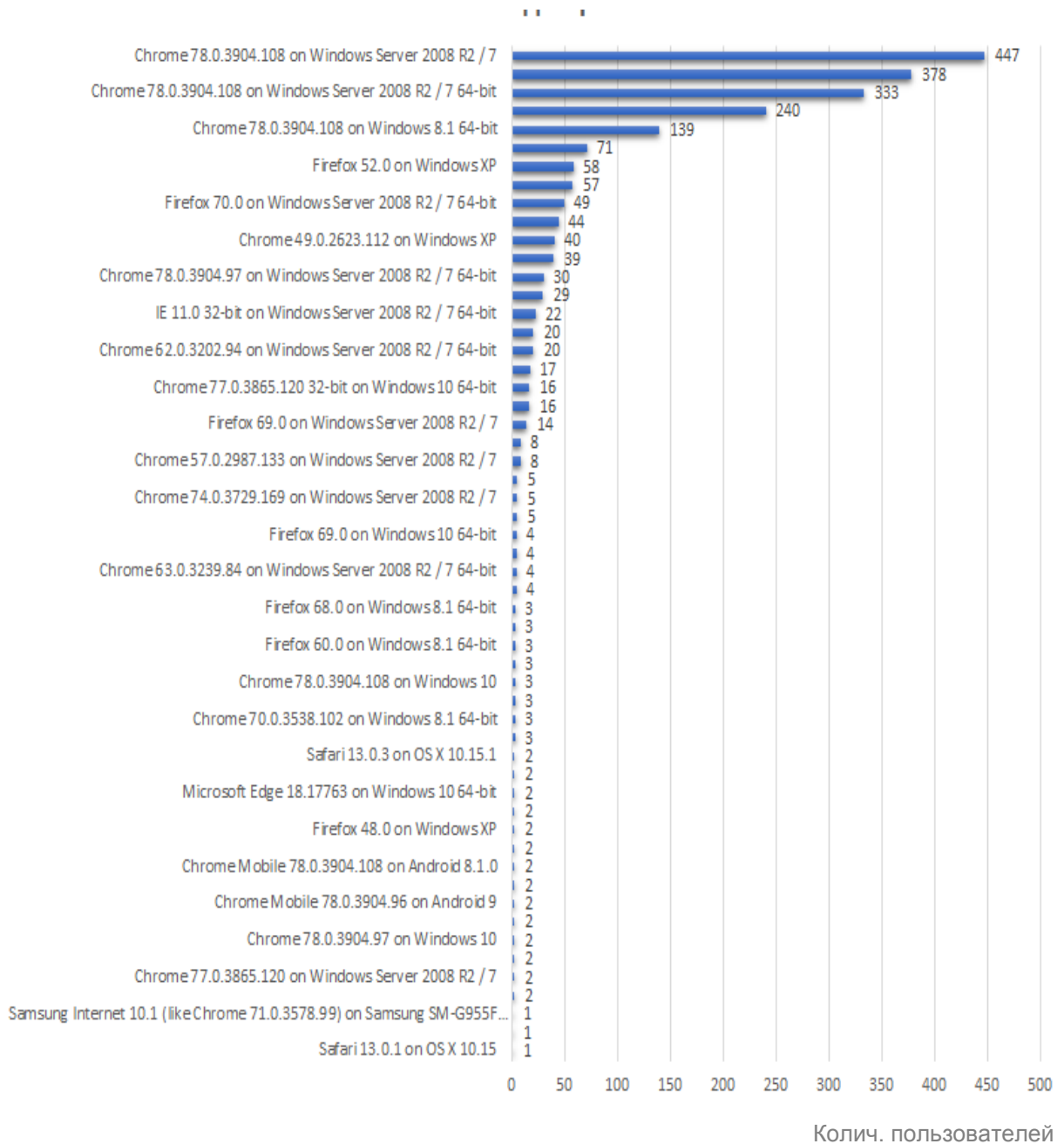


Рисунок 5.3 — Типы и версии браузеров, используемых в опросе

Проведен эксперимент, в котором участвовали студенты 20 различных вузов, в ходе которого в рамках когнитивных исследований, среди прочего, были заданы следующие три вопроса:

1. Учебная программа (на выбор четыре варианта: бакалавриат/магистратура/специалитет/аспирантура).

2. Основа обучения (выбор из трех вариантов: бюджет/контракт/целевое обучение).

3. Укажите профиль вашего образования (на выбор четыре варианта: техническое/гуманитарное/естественнонаучное/без профиля).

Вопросы 1, 2 задавались в начале взаимодействия с платформой, вопрос 3 — примерно через час после проведения различных когнитивных тестов.

Общее количество респондентов, принявших участие в исследовании, равнялось 23 102. Записи, содержащие пустые ответы или время реакции менее 2 секунд, были удалены из набора данных. Остальные 22 357 записей были нормализованы, рассчитаны средние значения для каждого вопроса. Был создан новый набор данных, содержащий отклонение от среднего времени реакции для каждого студента по каждому вопросу. Гистограммы экспериментальных данных по каждому вопросу приведены на рис. 5.4. Анализ гистограмм на основе методов психометрики подтверждает корректность психологического исследования.

Для качественной оценки отклонений времени реакции введена шкала, делящая отклонения на 4 квантили в порядке возрастания. Таким образом, у каждого из 22357 студентов была упорядоченная триада типа (1, 2, 4), представляющая их относительно отклонений времени реакции на вопросы 1–3. Границы квантилей показаны в табл. 5.1

Количественный анализ данных отклонений времени реакции показал достоверную корреляцию между отклонениями при ответах на вопросы 1–3. Коэффициенты корреляции представлены в табл. 5.2.

При изучении взаимосвязи отклонений времени реакции для трех вопросов 1–3 был проведен тест Вальда (табл. 5.3) [13], демонстрирующий значительную линейную взаимосвязь между отклонениями.

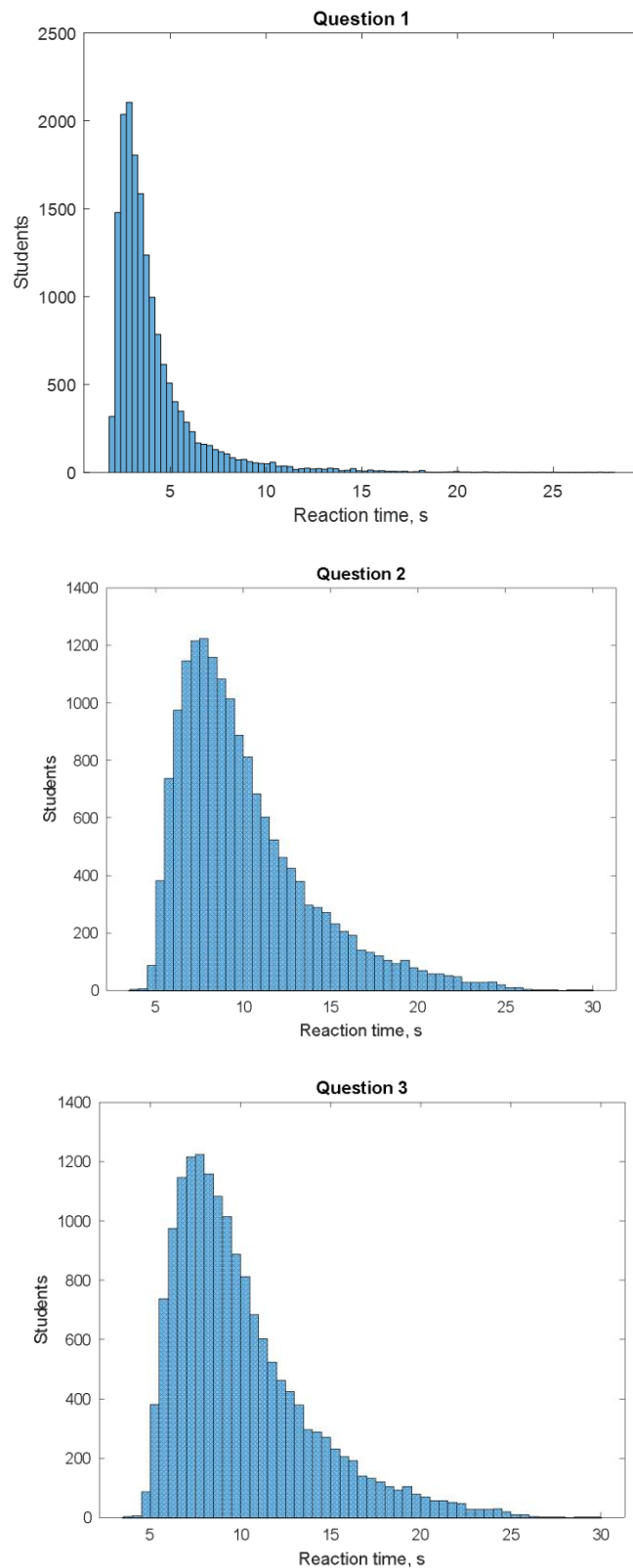


Рисунок 5.4 — Гистограммы нормализованного времени реакции пользователей при ответе на вопросы 1–3

Таблица 5.1 — Границы квартилей отклонений времени реакции

	Квартиль 1	Квартиль 2	Квартиль 3	Квартиль 4
Вопрос 1				
Нижняя граница	0	0.0056	0.0063	0.0068
Верхняя граница	0.0055	0.0062	0.0067	1
Вопрос 2				
Нижняя граница	0	0.0053	0.0071	0.0082
Верхняя граница	0.0052	0.007	0.0081	1
Вопрос 3				
Нижняя граница	0	0.0075	0.011	0.014
Верхняя граница	0.0074	0.0109	0.013	1

Таблица 5.2 — Коэффициенты корреляции отклонений времени реакции студентов на вопросы 1–3 (аргументы 1–3 обозначают номер вопроса)

R (1,2)	R (1,3)	R (2,3)
0.9298	0.8039	0.8376

Таблица 5.3 — Статистика теста Вальда

Вид модели	Статистика Вальда	Критическое значение
$D_1 = \beta_0 + \beta_1 D_2 + \beta_2 D_3 + \varepsilon$	145 320	4.9915
$D_1 = \beta_0 + \beta_1 D_2 + \varepsilon$	142 700	3.8415
$D_1 = \beta_0 + \beta_2 D_3 + \varepsilon$	40 854	3.8415
$D_2 = \beta_0 + \beta_1 D_1 + \beta_2 D_3 + \varepsilon$	176 340	4.9915
$D_2 = \beta_0 + \beta_2 D_3 + \varepsilon$	52 547	3.8415
$D_3 = \beta_0 + \beta_1 D_1 + \beta_2 D_2 + \varepsilon$	53 735	4.9915

Уровень значимости равен 0,05; $\beta_1, \beta_2, \beta_3$ — постоянные значения; ε — нормально распределенная ошибка с $M = 0, \sigma^2 = 1$.

В ходе качественного анализа было обнаружено, что 17 002 студентов (76%) принадлежали к одному квартилю по всем трем вопросам или не более чем один их квартиль находился рядом с двумя другими.

Из полученных гистограмм и приведенных результатов видно, что, несмотря на изменение времени реакций по всем данным реакции у большинства пользователей остались неизменными. Для прогнозирования реакций были проверены возможности построения регрессионных зависимостей, проведен тест Вальда. Получено, что зависимости могут быть построены, что демонстрирует допустимость построения достоверных прогнозных значений реакций пользователей. Это имеет важное значение для рассматриваемой задачи контроля. Например, для проверки того, работает ли с системой верифицированный пользователь, задается секретный вопрос или иной простой вопрос с анкетными данными. Анализ реакции пользователя по ответу на этот вопрос является также персональной информацией. Система КД может сравнить прогнозируемое значение с полученным. Тест Вальда показал, что значимыми могут быть простые модели, то есть проверка и расчет прогноза не потребуют значительного количества вычислительных ресурсов для сбора и передачи данных.

Для ВС предлагается встроить в системы КД и верификации вспомогательные индикаторы использования элементов интерфейса — время реакции (ВР) при выполнении определенных, заранее зафиксированных действий. Это позволит использовать только персональные реакции, исключив ситуации смены пользователя в одном сеансе работы. Также возможно определение пользователя при использовании чужих паролей для входа в систему.

5.3. Метод анализа реакций пользователей для контроля доступа и технология реализации модуля анализа данных

Предлагается в системы контроля доступа и верификации встроить вспомогательные индикаторы использования элементов интерфейса — ВР при выполнении определенных, заранее зафиксированных действий. Это позволит использовать только персональные реакции, исключив ситуации смены пользователя в одном сеансе работы. Также возможно определение пользователя при использовании чужих паролей для входа в систему. Возможные ситуации с изменением реакций из-за текущего психоэмоционального состояния требуют проведения дополнительных подтверждений личности пользователя. Так, в случаях, например болезни или снижения концентрации пользователя в системы с критическим доступом допуск пользователя может быть проверен специальными службами.

На основе гипотез и проверенных экспериментальных исследований можно сформулировать метод контроля доступа, основанный на реакциях пользователей. Метод состоит в следующем [13, 162]:

1. В интерфейс ВС встраивается или периодически подключается специализированный интерфейс с заданными анкетными вопросами или иными простыми вопросами.

2. На основе хранящихся данных о скорости реакции этого пользователя при работе с элементами интерфейса строится прогнозная модель о реакции.

3. Прогнозные значения сравниваются с полученными.

4. Если полученный экспериментальный результат входит в состав другого квартиля от ожидаемого значения, то запускаются механизмы идентификации пользователя, требующие персонального подтверждения.

5. Если результаты совпадают (попадают в один квартиль), то пользователь считается верифицированным.

В общем виде разрабатываемую технологию [162] можно представить в следующем виде.

1. Технология реализуется вычислительным комплексом (ВК). ВК может предоставлять клиенту одну или несколько услуг.

2. ВК включает компьютерные сети, системы управления передачей данных, т. е. среду, используемую для обеспечения каналов связи между компьютерами, системами обработки данных и другими устройствами. Сеть может включать в себя соединения в виде проводных линий связи и каналов беспроводной связи.

3. ВК могут отправлять инциденты безопасности на облачную платформу для дальнейшего анализа приложением машинного обучения на основе идентифицированных характеристик инцидентов безопасности, обнаруженных во время локального анализа с помощью модуля безопасности и диспетчера событий. Идентифицированные характеристики могут включать, например, информацию о том, что наблюдаемые параметры имеют оценку риска безопасности выше порогового значения.

4. В ВК создается постоянное хранилище информации о безопасности и менеджер событий, который может быть аппаратным компонентом или комбинацией аппаратных и программных компонентов. Менеджер информации и событий безопасности управляет процессом выбора только определенных инцидентов безопасности для локального и удаленного анализа.

5. Интервал оценки психомоторных реакций пользователя представляет собой заранее определенный интервал времени, на основе которого формируются инциденты безопасности.

Таким образом, элементы интерфейса вместе со встроенными реакциями передаются в ВК, анализируются на уровне доступа [162] (рис. 5.5).

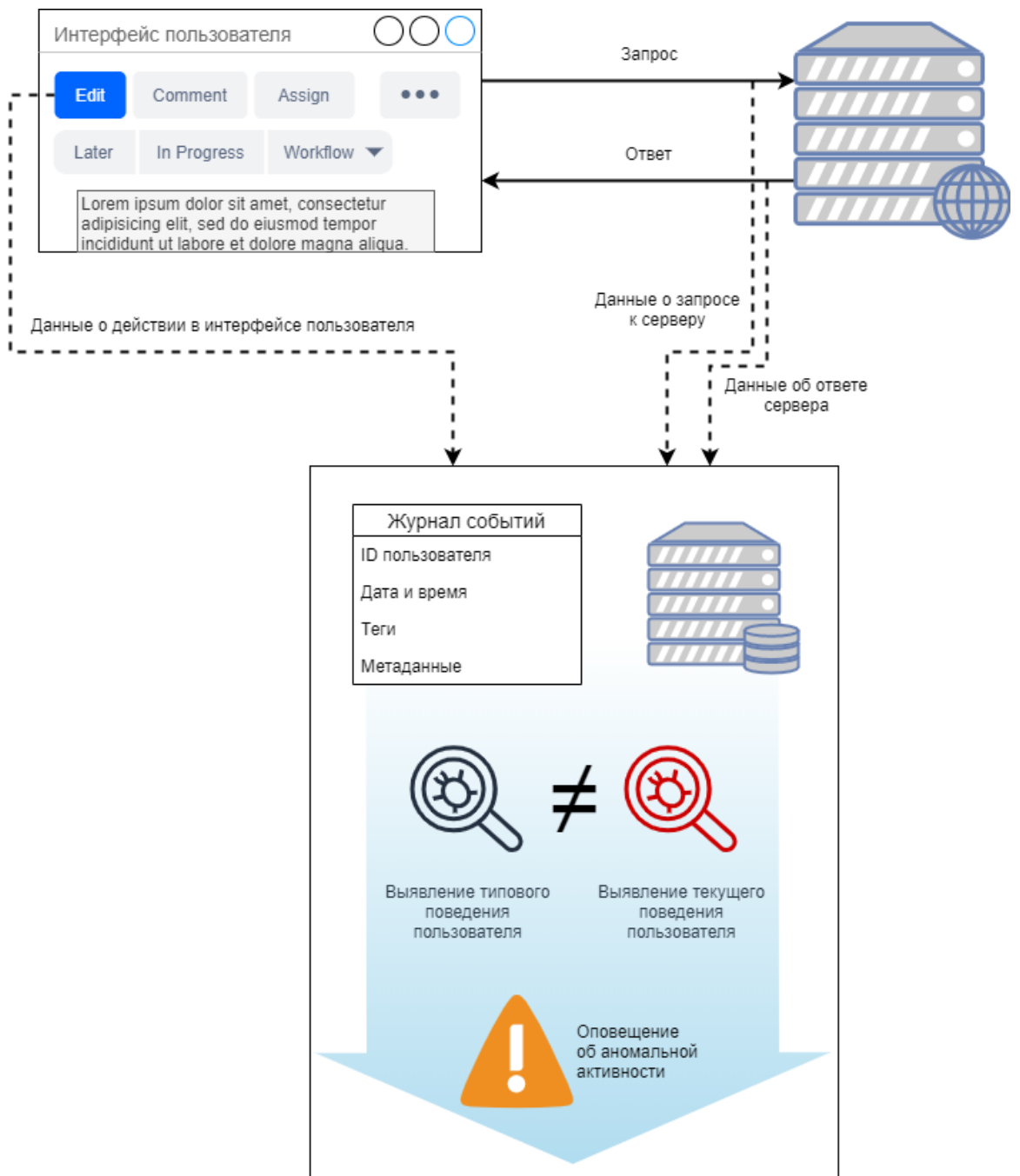


Рисунок 5.5 — Уровень анализа действий пользователя в архитектуре ВК

Концептуальная схема взаимодействия уровня управления и серверной части приведена на рис. 5.6.

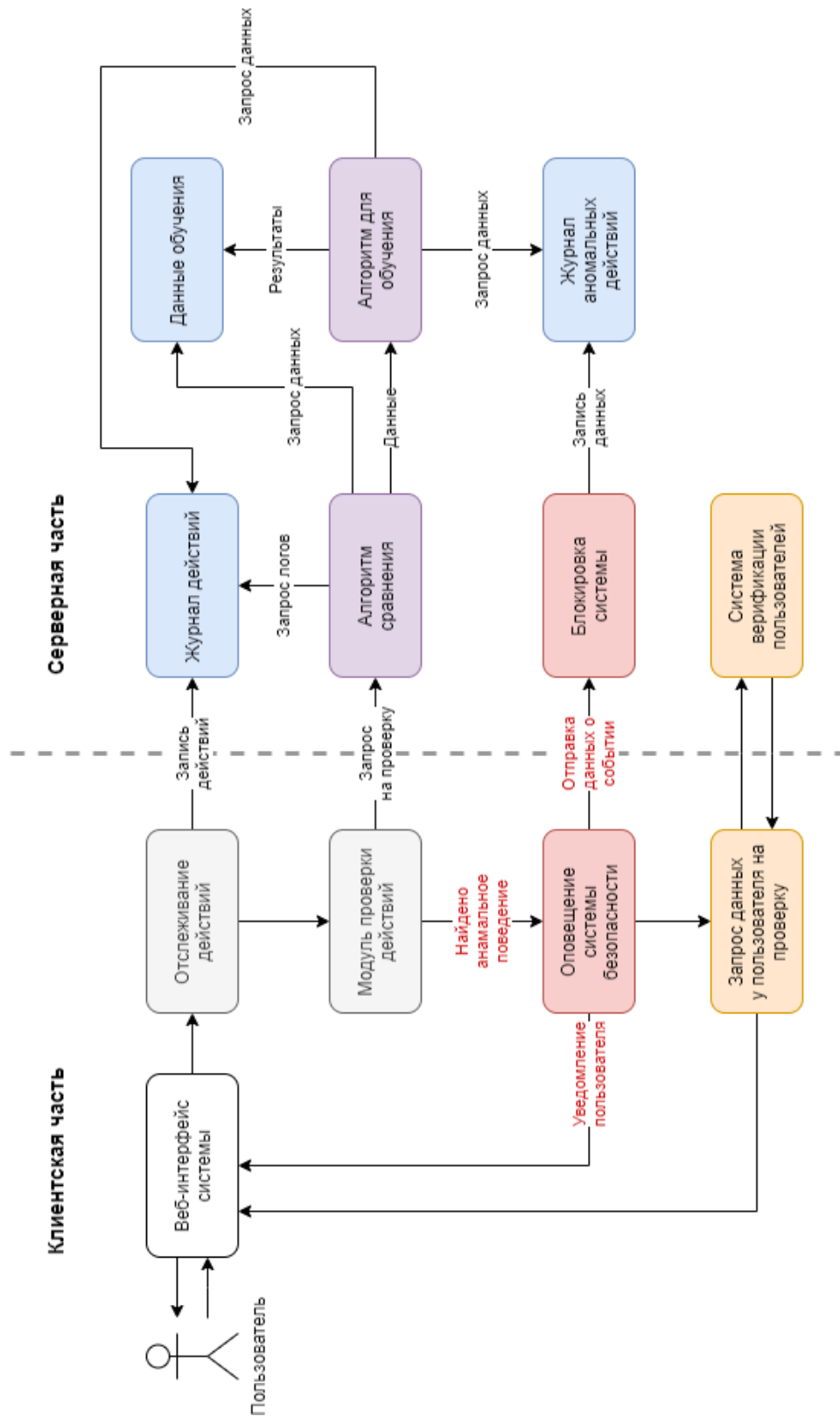


Рисунок 5.6 — Технология взаимодействия уровня управления с клиентскими интерфейсами

В процессе работы пользователя с интерфейсом системы необходимо проверять условия переходов на основе ранее совершенных наборов действий, записанных в журнал событий.

Разработано технологическое решение, которое может быть реализовано в широком спектре цифровых платформ — банковских, медицинских, образовательных и др.

В качестве развития разработанного подхода представляется актуальным использование инструментов искусственного интеллекта для выявления скрытых зависимостей в данных, полученных с базы логирования пользователей и выявления их наиболее вероятных действий.

Выводы по главе

Разработаны метод и соответствующая система контроля доступа на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса на основе анализа времени ответа на контрольные вопросы. Метод позволяет учитывать персональные реакции на основе только времени ответа на контрольные вопросы, что позволяет существенно сократить затраты ресурсов и объемы передаваемых данных, по сравнению с решениями, учитывающими все действия пользователей при взаимодействии с интерфейсом.

Приведенные результаты экспериментальных исследований показали, что анализ психомоторных реакций пользователей может быть использован как модуль анализа КД, при этом исследуемая характеристика пользователя может быть измерена без перегрузок каналов связи и независимо от используемого типа устройств, предложено время реакции.

Глава 6. ПОСТРОЕНИЕ МНОГОУРОВНЕВОЙ АРХИТЕКТУРЫ ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ ДЛЯ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ДОСТУПА К СЕРВИСАМ ЗДРАВООХРАНЕНИЯ

Защита сети медицинского учреждения подразумевает как базовую защиту периметра с помощью межсетевых экранов и правил доступа, реализуемых в сетевом оборудовании, так и предлагаемые в настоящей работе компоненты защиты архива DICOM и сервера приложений, предполагающие анализ пользовательской активности. Таким образом, защита технических объектов инфраструктуры медицинского учреждения обеспечивает защищенность жизни и здоровья пациентов, профессиональной репутации специалистов в частности и учреждения в целом.

6.1. Анализ программно-аппаратного обеспечения цифровой среды здравоохранения

Системные сбои, а также действия злоумышленников, которые впоследствии могут навредить учреждению, относятся к ИТ-инфраструктуре организации. Каждое вредоносное действие может осуществляться где угодно и когда угодно. Для получения необходимых подробных данных смоделируем инфраструктуру медицинского учреждения [164].

Современные диагностические устройства могут подключаться к локальной сети организации или же могут быть подключены к рабочим станциям с помощью, например, USB-соединения, нередко используются и беспроводные соединения. Довольно часто медицинское оборудование об-

работывает данные (например, снимки пациента), которые также могут представлять интерес для злоумышленника.

Для моделирования угроз медицинского учреждения рассмотрим схему сети типовой инфраструктуры на рис. 6.1.

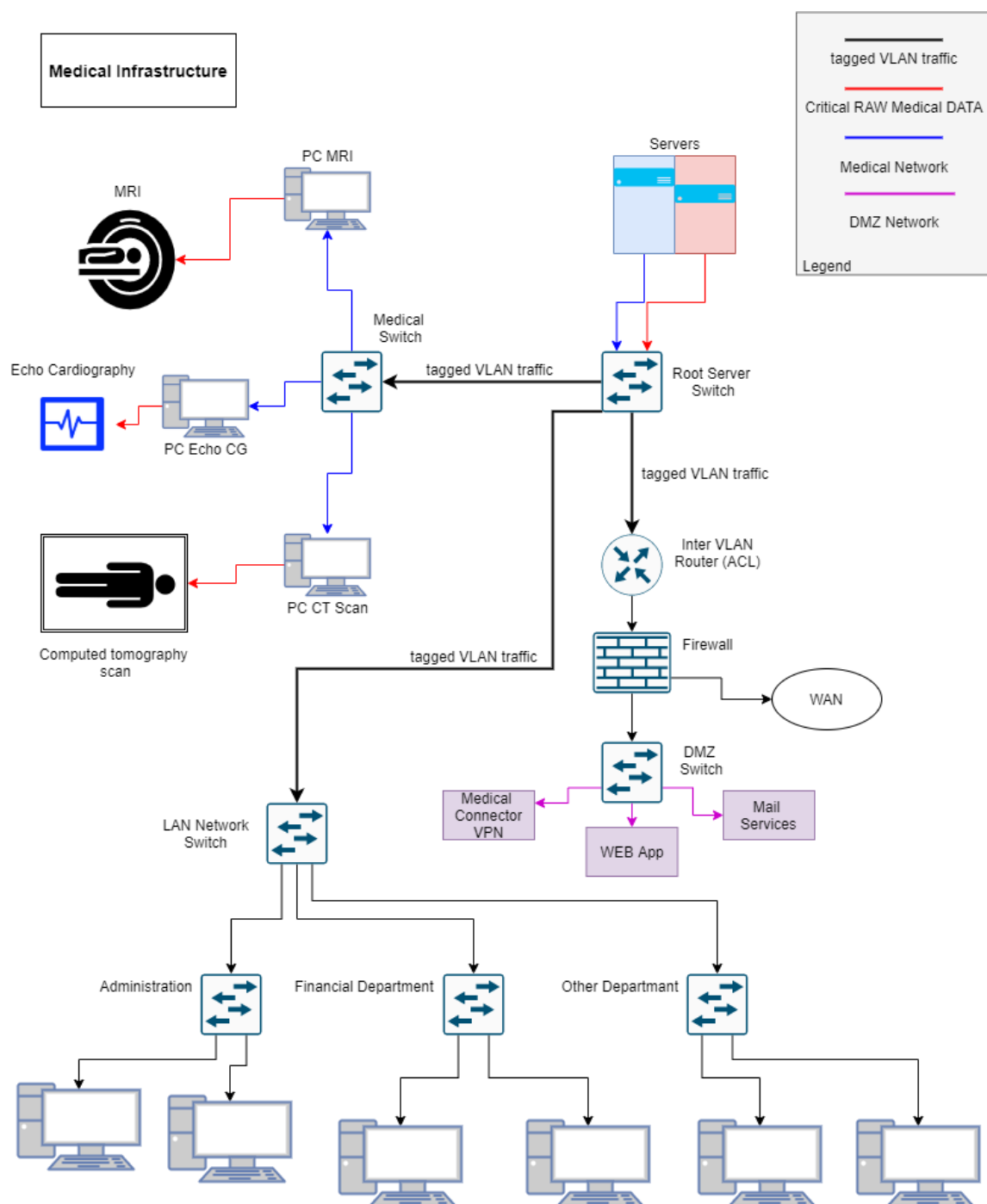


Рисунок 6.1 — Схема типовой инфраструктуры медицинского учреждения

6.1.1. Схема взаимодействия объектов медицинской инфраструктуры

Любая инфраструктура представляет совокупность взаимодействующих систем. В случае организации здравоохранения можно выделить 3 функциональные системы: система медицинского оборудования, система взаимодействия административного персонала, а также сервисные системы обслуживания оборудования.

Одной из самых критически важных систем медицинской организации является ее медицинская инфраструктура. На рис. 6.2 представлена медицинская инфраструктура.

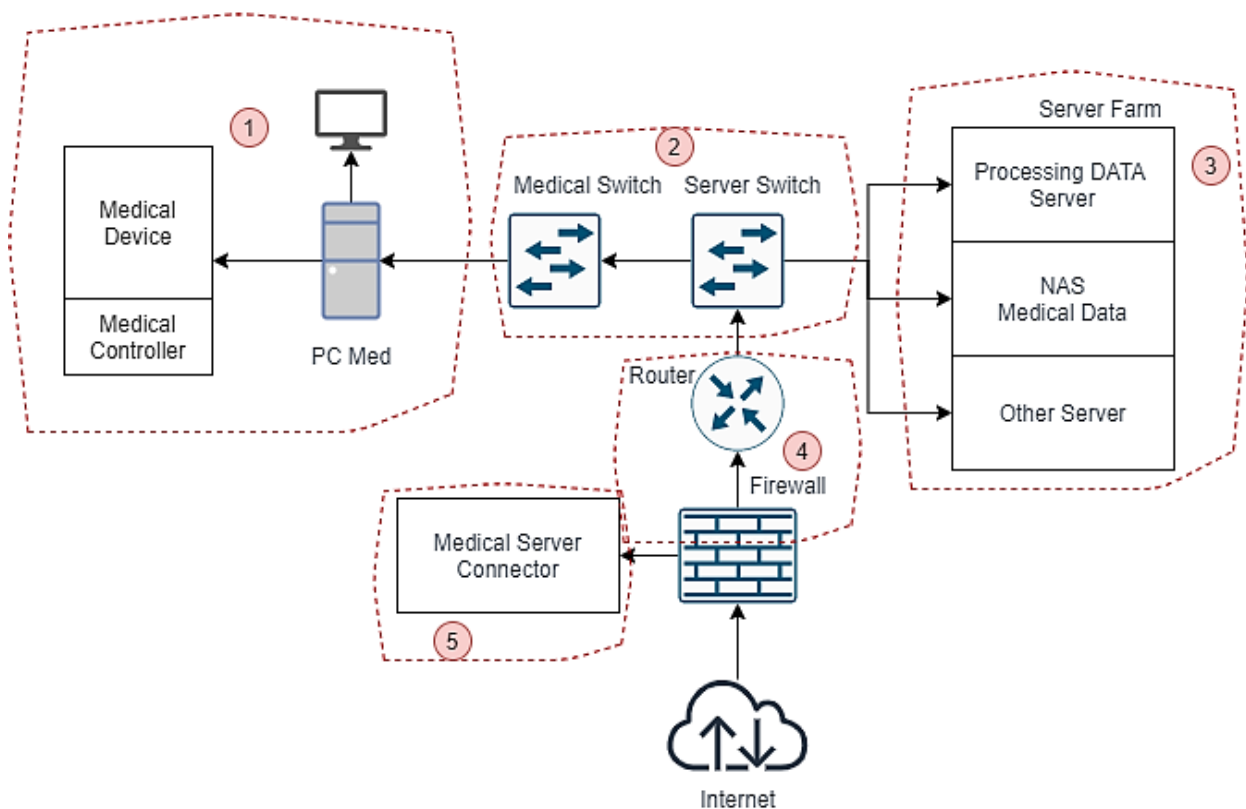


Рисунок 6.2 — Схема взаимодействия объектов медицинской инфраструктуры организации здравоохранения

Инфраструктура состоит из:

1. Зоны медицинских приборов и оборудования;
2. Зоны сетевого коммутационного оборудования;
3. Зоны серверов, обслуживающих медицинское оборудование;
4. Зоны маршрутизации и межсетевого экранирования;
5. Зоны серверов медицинских сервисов, требующих обмена данных с внешними сервисами.

Рассмотрим каждую из функциональных зон подробнее.

Зона медицинских приборов и оборудования. Эта зона является одной из наиболее критических. Тут происходит сбор медицинских данных пациентов, обработка и дальнейшая передача информации в единые системы обработки медицинских данных (ЕМИАС и т. д.). Аппаратное и программное обеспечение этой зоны подвержены различным рискам сбоев в результате внешнего воздействия на данную систему.

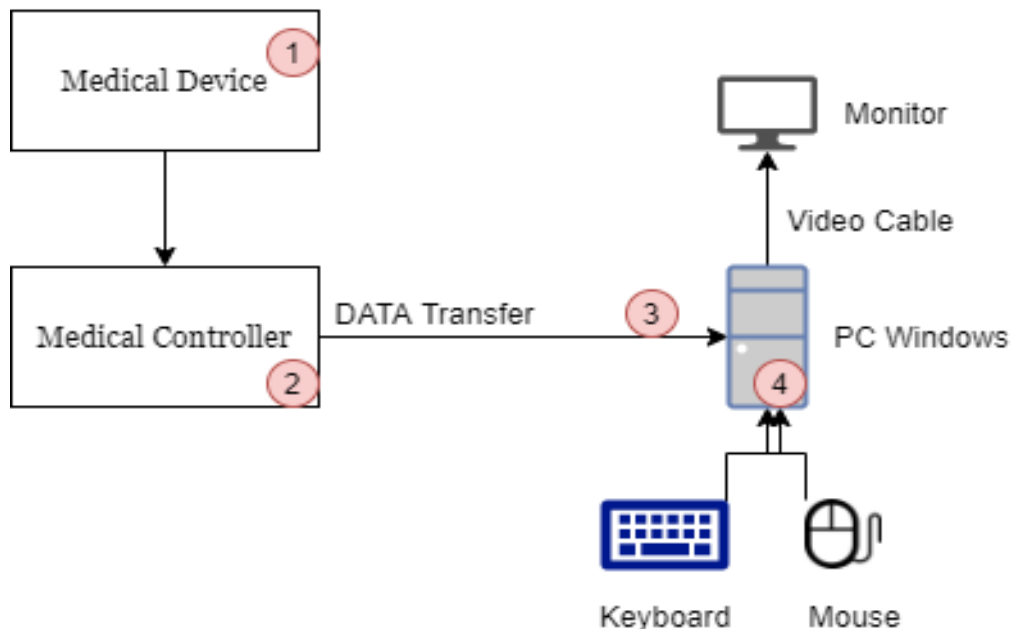


Рисунок 6.3 — Схема взаимодействия медицинского оборудования с АРМ

В состав системы входят:

1. Медицинское оборудование;
2. Различные сопутствующие устройства для взаимодействия с серверным оборудованием организации;
3. Автоматизированное рабочее место, оборудованное необходимой периферией и оборудованием;
4. Дополнительное оборудование автоматизированного рабочего места (опционально).

Медицинское оборудование в основном представлено следующими устройствами: аппараты КТ, МРТ, УЗИ, рентгеновское оборудование, инсулиновые помпы и всевозможные датчики, контролирующие и обеспечивающие процессы жизнедеятельности пациентов. Всё оборудование имеет в своем составе медицинские датчики и управляющие элементы.

В свою очередь аппаратное обеспечение управляется своим специализированным программным обеспечением (firmware), которое зачастую имеет ошибки и уязвимости. Такое программное обеспечение, как правило, обновляется на заводе-изготовителе или во время гарантийного обслуживания. Ниже рассмотрим подробно уязвимости, которым подвержены рассматриваемые системы.

Зона сетевого коммутационного оборудования. Функциональная особенность данной зоны заключается в передаче медицинских данных между медицинским оборудованием, рабочим местом врача и сервером программно-аппаратного комплекса медицинского оборудования. На рис. 6.4 представлена схема соединения медицинского и коммутационного оборудования медицинского учреждения.

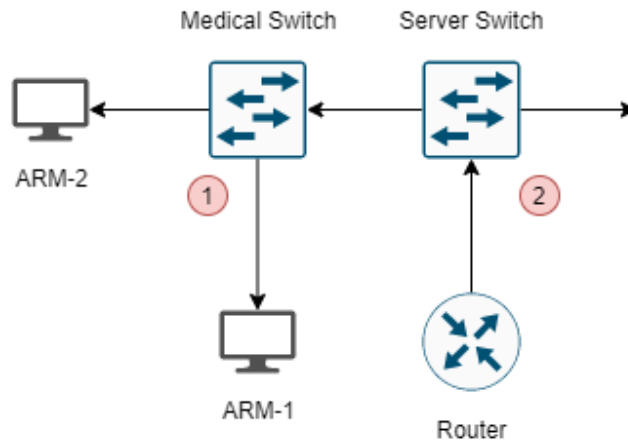


Рисунок 6.4 — Схема коммутационного оборудования

В состав системы входят:

1. Коммутационное оборудование;
2. Маршрутизаторы;
 - кабельные линии;
 - сетевая часть медицинского оборудования и рабочих мест.

Обычно в качестве среды передачи медицинских данных используется компьютерная сеть Ethernet с применением специализированных протоколов передачи данных.

Зона серверного оборудования, необходимого для работы медицинского оборудования (рис. 6.5). Серверное оборудование необходимо для обработки и хранения различных типов медицинских данных. Для цифровой обработки «сырых» данных с медицинского оборудования применяются специализированные программно-аппаратные комплексы, в которые входит в том числе и серверное оборудование.

В состав системы входят:

1. Серверные коммутаторы;
2. Серверы обработки данных;
3. Серверы хранения данных;
4. Серверы для обеспечения работы других сервисов.

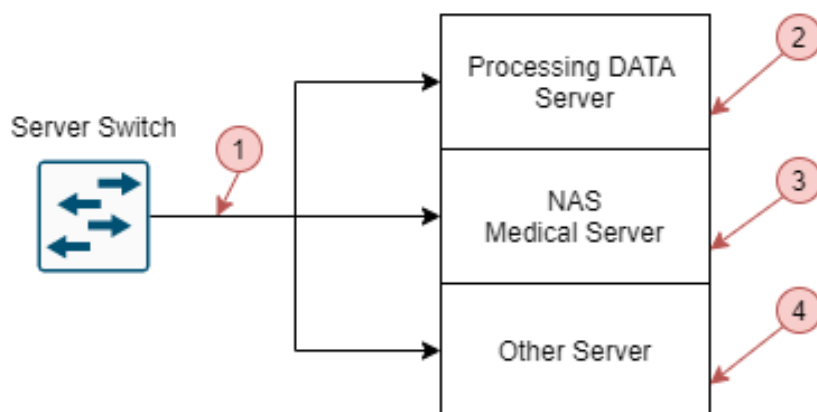


Рисунок 6.5 — Схема взаимодействия медицинского оборудования с серверами

Зона сетевого оборудования, которое отвечает за маршрутизацию и межсетевое экранирование трафика организации (рис. 6.6).

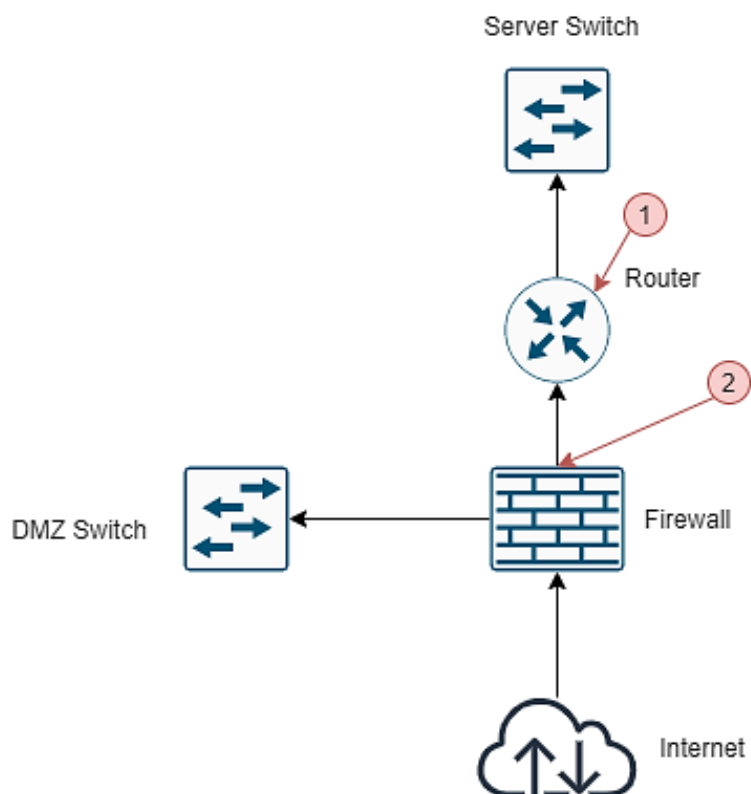


Рисунок 6.6 — Схема подключения сетевого оборудования, выполняющего маршрутизацию и межсетевое экранирование трафика

Развитие информационных технологий привело к тому, что выход в интернет является обязательным условием любого бизнес-процесса. А за последние несколько лет это привело к тому, что некоторое медицинское оборудование потребовало наличия постоянного соединения с глобальной сетью. В одном случае — для обслуживания и проверки лицензий оборудования, в другом — для передачи определенных данных на серверы других медицинских организаций. Прямое подключение медицинского оборудования к глобальной сети потенциально опасно. Для обеспечения безопасности применяются межсетевые экраны (Firewall).

В состав системы входят:

1. Внутренние маршрутизаторы медицинской организации;
2. Межсетевые экраны;
3. Внешние маршрутизаторы.

Зона работы внешних сервисов — DMZ (демилитаризованная зона). Для обеспечения непрерывной передачи данных между организациями используются специальные серверы, которые могут обмениваться медицинскими данными. Помимо них, для публикации открытых данных, веб-порталов и других открытых ресурсов используются веб-серверы. Распределение возможной высокой нагрузки на ресурсы осуществляется благодаря прокси-серверам. Принципиальная схема DMZ представлена на рис. 6.7.

В состав системы входят:

1. Коммутационное оборудование DMZ;
2. Сервера, обеспечивающие прием и передачу медицинских данных;
3. Веб-порталы и ВС организации;
4. Прокси-серверы.

Наличие демилитаризованной зоны необходимо для предотвращения возможных атак на внутреннюю инфраструктуру организации при возможном нарушении периметра.

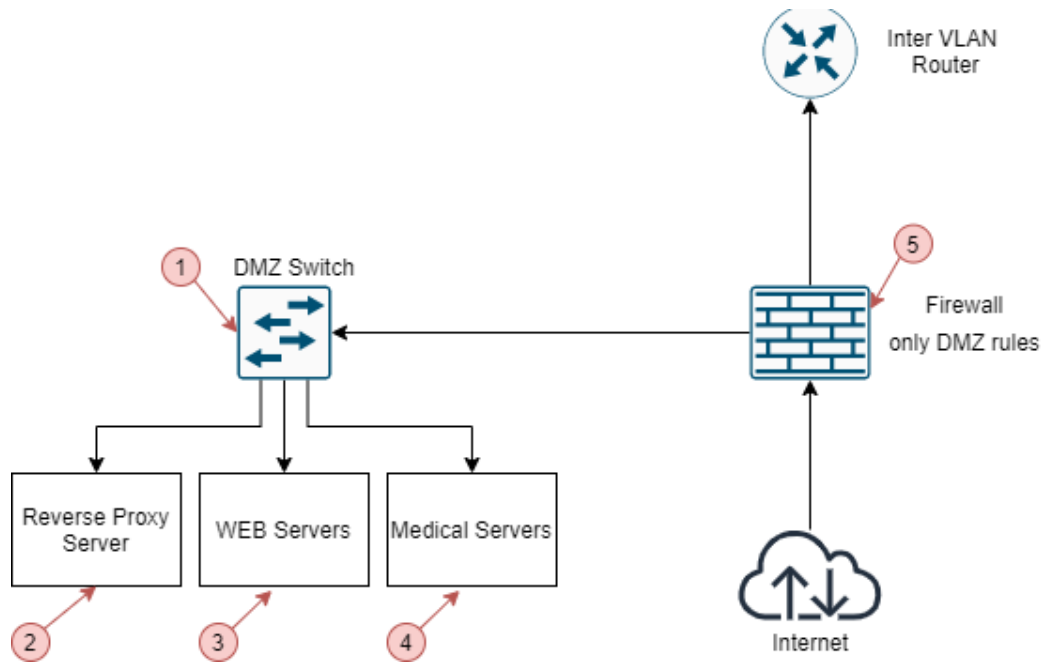


Рисунок 6.7 — Схема взаимодействия медицинского оборудования с АРМ

6.1.2. Наиболее вероятные угрозы для медицинских учреждений

Остановимся подробнее на применяемых механизмах несанкционированного проникновения в медицинское учреждение.

Разобьем на три группы основные объекты, которые, прежде всего, будут интересовать злоумышленников.

1. *Клинические информационные системы* [14, 201, 214] состоят из большого количества модулей, включающих решения как от различных поставщиков, так и всевозможные решения с открытым исходным кодом, которые взаимодействуют и обмениваются файлами друг с другом, поэтому уязвимость одного из компонентов может повлиять на другие. Другая проблема — это повышение функциональной совместимости. Актуальна глобальная задача по созданию единой государственной информационной системы в сфере здравоохранения, которая подразумевает использование данных различными системами, не только внутри организации, но и при взаимодействии с внешними учреждениями. В таком случае к уязвимости

одного из компонентов добавляется проблема обеспечения безопасного обмена данными посредством внешней сети.

2. *Медицинское оборудование* можно сравнить по функциональности и времени эксплуатации с автоматизированными системами управления технологическими процессами со всеми присущими проблемами обеспечения безопасности. Медицинское оборудование является достаточно дорогим, поэтому в медицинских учреждениях планируют использовать эти устройства в течение многих лет. Из-за этого возникают сложности при получении технической поддержки от производителей, которые, как правило, пытаются разработать новое оборудование, а заниматься поддержкой морального устаревшего считают нецелесообразным. По этой причине уязвимости появляются, а поскольку устранением практически никто не занимается, то их могут использовать злоумышленники при организации эффективных кибератак.

Следующая, не менее важная, проблема заключается в том, что медицинское оборудование обычно является достаточно сложным в управлении и настройке. Как правило, врачи и специалисты информационного отдела (если такой отдел существует в медучреждении) не проходят обучение на новом оборудовании. Обычно в медицинском учреждении оставляют стандартную настройку оборудования, поэтому предотвращение использования паролей по умолчанию и обеспечение того, чтобы неизвестные функции не активировались, является еще одной проблемой. На устройствах могут быть реализованы оперативные процедуры (например, запросы на дату/время, передача технических и сервисных данных производителю, запросы на техническое обслуживание, автоматические обновления), которые могут инициировать оповещения безопасности в системе предотвращения вторжений в информационную систему учреждения (необходимо учитывать, что их применение не получило достаточной степени распространения). Эта взаимосвязанность открывает злоумышленникам множе-

ство возможностей получить доступ к инфраструктуре медицинского учреждения. Также важно учесть, что новейшие устройства обычно имеют функции удаленного управления и даже возможность подключения к беспроводной сети. Это позволяет поставщикам снизить затраты на обслуживание и выполнять другие операции, что обычно очень удобно для медицинского учреждения. Но эти уязвимости, если их игнорировать или ими пренебречь, могут привести к появлению уязвимостей в организации, поскольку они часто возникают без ведома медицинского учреждения.

Также серьезной проблемой медицинского оборудования, требующего внимания, является сертификация в различных ведомствах — процедура очень долгая и дорогая. К примеру, производитель производит инфузионные насосы, которые, согласно официальной документации, работают на 23 порту под операционной системой Windows XP. Процедура сертификации была пройдена в 2003 г. На сегодняшний день поддержка операционной системы Windows XP прекратилась, но производитель не заинтересован в том, чтобы пройти новую сертификацию с более надежной операционной системой, а значит мы получаем уязвимые устройства с большим количеством Common Vulnerabilities and Exposures (CVE, база данных общеизвестных уязвимостей информационной безопасности).

3. *Сети*. Одна из проблем — это использование специфических медицинских протоколов. Хотя протоколы были разработаны с учетом вариантов использования, но при этом не были приняты во внимание возможные угрозы информационной безопасности. Персональные данные пациентов не меняются, а значит утечка данных может быть угрозой в течение всей жизни пациента. Повышение безопасности протоколов, используемых для обмена данными пациента, имеет решающее значение.

Следующая и не менее серьезная проблема — это небезопасное конфигурирование сети для обмена информацией через интернет, подключе-

ние различных сервисов, открывающих незащищённые сетевые интерфейсы.

Используя информационно-поисковую систему для мониторинга «интернета вещей» (Internet of Things) Shodan, можно очень найти большое количество медицинских учреждений по всему миру (рис. 6.8), в инфраструктуре которых размещены публично доступные системы, обрабатывающие медицинские данные (рис. 6.9).

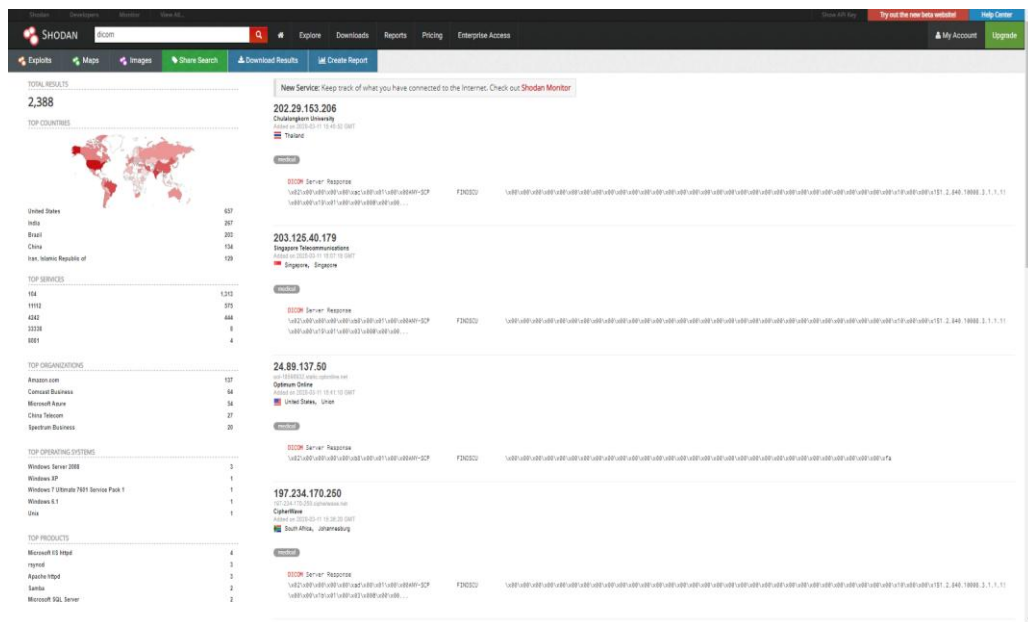


Рисунок 6.8 — Использование поисковой системы Shodan

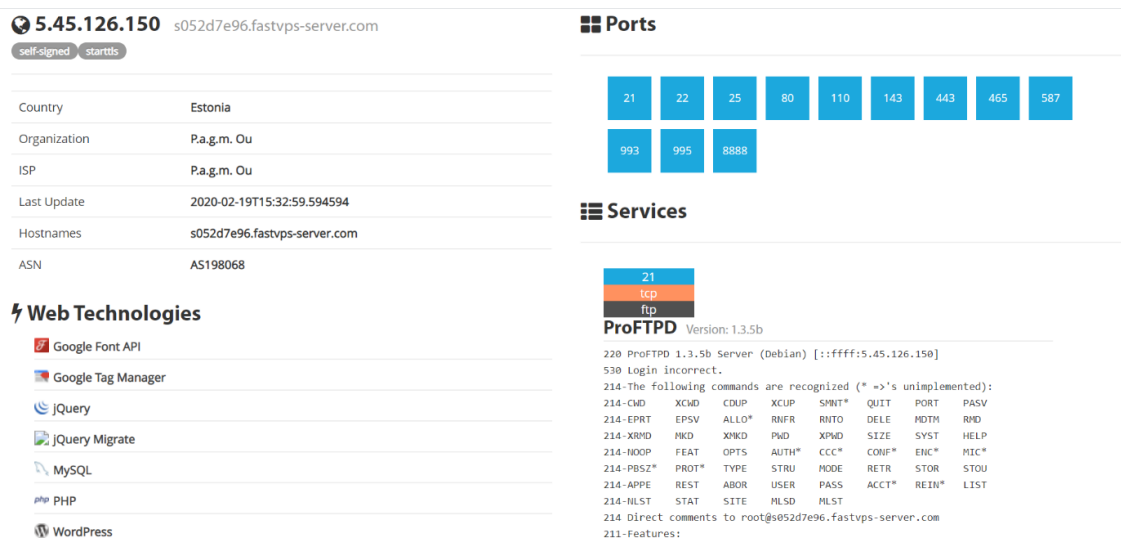


Рисунок 6.9 — Просмотр портов доступных из внешней сети

Медицинские учреждения сами публикуют конфиденциальную информацию в общем доступе, так что для её чтения не нужно специальных навыков и взлома, достаточно воспользоваться поисковой системой. Например, можно найти незащищённый паролем интерфейс для просмотра снимков УЗИ (рис. 6.10).



Рисунок 6.10 — Просмотр снимка УЗИ через публично доступный интерфейс в сети клиники

На рис. 6.9 видно, что имеется огромное количество открытых сетевых портов, которые можно атаковать. Например, можно найти интерфейсы администрирования Linux-систем (порты 22, 5800, 5900), управляющие интерфейсы ОС Windows (порты 137, 138, 139, 445), а также веб-интерфейсы приложений для учета пациентов, обработки клинических изображений и т. д. Таким образом, видно, что у злоумышленника есть реальная возможность проникнуть в подсеть с медицинскими учреждениями. При этом в некоторых пакетах медицинского ПО уже есть публично известные уязвимости с соответствующими идентификаторами CVE, которые также можно эксплуатировать для взлома медицинской сети.

Что касается CVE, то в каталоге, в 2021 г. появились новые уязвимости в медицинском оборудовании и программном обеспечении. Например, [15]:

- CVE-2020-6961 — поставка на устройствах общего SSH-ключа, позволяющего подключиться к любому устройству и выполнить код на нём. Данный ключ также используется в процессе доставки обновлений.
- CVE-2020-6962 — общие для всех устройств предопределенные учётные данные для доступа на запись и чтение к файловой системе по протоколу SMB;
- CVE-2020-6963 — возможность применения приложений MultiMouse и Kavoom KM для удалённого управления устройством (эмуляция клавиатуры, мыши и буфера обмена) без проведения аутентификации;
- CVE-2020-6964 — предопределенные для всех устройств параметры подключения по протоколу VNC;
- CVE-2020-6965 — предустановка уязвимой версии Webmin, позволяющей удаленно получить доступ с правами root;
- CVE-2020-6966 — применяемый на устройствах менеджер установки обновлений допускает подмену обновления (обновления заверяются известным SSH-ключом).

Причем, как указано в источнике, пяти уязвимостям присвоен максимальный уровень опасности (CVSSv3, 10 из 10). Это означает, что перечисленные уязвимости позволяют получить полный контроль за устройствами, что позволяет внести изменения на уровне операционной системы, отключения сигнала тревоги или подмены данных о состоянии пациента. На момент написания работы эти уязвимости не закрыты.

6.2. Анализ уязвимости инфраструктуры медицинских цифровых систем

Общие принципы работы сетей многократно описаны в литературе, но защита медицинских протоколов и оборудования, имеющая свою специфику, мало изучены. Особенно это касается программного обеспечения, работающего с распространенным протоколом DICOM (Digital Imaging and Communications in Medicine) [147], и аппаратов медицинского назначения [131].

DICOM применяется почти во всех рентгенологических, кардиологических изображениях и радиотерапевтических устройствах (рентген, КТ, МРТ, УЗИ и прочие), а также все чаще в устройствах других областей медицины, таких как офтальмология и стоматология. Имея сотни тысяч используемых устройств медицинской визуализации, DICOM является одним из наиболее широко распространенных стандартов обмена сообщениями в области здравоохранения в мире. В настоящее время для оказания медицинской помощи используются буквально миллиарды изображений DICOM.

Такое широкое применение DICOM послужило признанием его Международной организацией по стандартизации стандартом ISO 12052 [232]. Широкое применение также привлекает все большее количество исследователей для анализа уязвимости.

Рассмотрим использование тактик MITRA [233] на вычислительную инфраструктуру медицинской организации. В зависимости от типа атаки, злоумышленнику не обязательно проходить все фазы. К примеру, он может ограничиться получением первоначального доступа, закреплением в атакуемой системе и сбором данных.

Рассмотрим первый вектор атаки. Доставка в атакуемую среду зловредного кода и обеспечение возможности его запуска является целью злоумышленника на этапе получения первоначального доступа. Способы доставки в зависимости от местоположения и типа оборудования могут очень сильно различаться. Однако на примере использования поискового сервиса Shodan убедились, что для этого не обязательно проникать во внутренний периметр организации, достаточно получение первоначального доступа (Initial Access) через открытые порты.

В качестве второго вектора рассмотрим следующую реализацию. Initial Access проводится посредством фишинговой рассылки, получения доступа к компьютеру сотрудника, а затем происходит либо горизонтальное продвижение (Lateral Movement), либо используется тот же компьютер если он имеет доступ к нужному сегменту сети.

Во многих медицинских учреждениях инфраструктура PACS реализована на основе проекта с открытым исходным кодом под названием — dcm4chee [139]. Проект также сопровождается подробной документацией по установке и эксплуатации, чем объясняется его популярность. Открытость и популярность этого и подобных проектов ожидаемо вызывают у злоумышленников и исследователей безопасности желание проверить его устойчивость к взлому.

Помимо шифрования и проблем протокола, нужно учитывать и свойства серверного ПО, обрабатывающего поступающие сообщения. Если отсутствуют механизмы авторизации, то любой атакующий может просматривать снимки любых пациентов по протоколу DICOM [214].

В частности, в рамках исследования было выявлено, что таким свойством обладает пакет ПО dcm4che (представляет собой набор ПО и утилит для работы с DICOM), в который входит DICOM-сервер, программы для извлечения и загрузки DICOM-файлов, клиент, а также веб-приложение для просмотра результатов. В веб-приложении реализован механизм авто-

ризации, для просмотра снимков необходимо ввести логин и пароль, однако атакующий может подключиться к серверу по протоколу DICOM и извлечь чужие снимки при помощи DICOM-сервиса Query/Retrieve.

В целях оценки защищенности распространенных реализаций DICOM была смоделирована инфраструктура медицинского учреждения при помощи пакета dcm4che, в который входит DICOM-сервер, веб-интерфейс для просмотра изображений и различные вспомогательные утилиты.

В экспериментальной инфраструктуре был развернут DICOM-сервер, работающий на порте TCP 11112, веб-интерфейс на порте 80, защищенный механизмом авторизации. На DICOM-сервер был загружен тестовый файл DICOM, взятый из онлайн-коллекции [160, 234].

В рамках исследования были изучены возможности пакета dcm4che, доступные утилиты и механизмы безопасности. Подразумевается, что врачи в больнице должны пользоваться веб-сервером, введя логин и пароль от своей учётной записи. При этом сами DICOM-устройства загружают изображения через интерфейс DICOM-сервера (порт 11112).

Как выяснилось, на этом интерфейсе доступны все DICOM-сервисы, включая Query, без какой-либо авторизации.

Для взаимодействия с DICOM-сервером воспользуемся входящей в пакет утилитой findscu [139]. Строка запуска утилиты выглядит следующим образом:

```
usage: findscu [options] -c <aet>@<host>:<port> [dcmfile_in...]
```

Таким образом, подключение определяется тремя параметрами: aet, host, port. Параметр AET — это значение Application Entity Title, в котором принято записывать уникальный идентификатор DICOM-устройства, состоящий из букв в верхнем регистре и цифр. В документации было обнаружено значение по умолчанию для AET: строка “DCM4CHEE”.

Ключ “-c” в вызове программы означает отправку запроса C-FIND по протоколу DICOM. При этом также можно передать опцию “-m”, в кото-

рой передаётся фильтр для поиска изображений по различным параметрам, таким как имя пациента, тип снимка, возраст и т. д.

Было выявлено, что в параметры фильтра можно подставлять не только буквальные значения, но и шаблоны: символ “*” означает любую подстроку.

Таким образом, утилита позволяет извлечь из настроенного по умолчанию DICOM-сервера с защищенным веб-интерфейсом на основе проекта dcm4che результаты исследований любых пациентов.

Пример запуска атакующим субъектом следующей команды для извлечения снимка, загруженного правомерно ранее на экспериментальный сервер:

```
$ ./findscu -c DCM4CHEE@10.10.0.17:11112 -m PatientName='*'
00:21:24,416 INFO - Initiate connection from 0.0.0.0/0.0.0.0:0 to
10.10.0.17:11112
00:21:24,437 INFO - Established connection Socket[addr=/10.10.0.17,port=11112,localport=35385]
00:21:24,468 INFO - FINDSCU->DCM4CHEE(1) << A-ASSOCIATE-
RQ
...
00:21:24,631 DEBUG - FINDSCU->DCM4CHEE(1) >> 1:C-FIND-RSP
Dataset:
(0008,0052) CS [STUDY] QueryRetrieveLevel
(0008,0054) AE [DCM4CHEE] RetrieveAETitle
(0008,0056) CS [ONLINE] InstanceAvailability
(0010,0010) PN [SHAMIL^MAGOMEDOV] PatientName
(0088,0130) SH [] StorageMediaFileSetID
(0088,0140) UI [] StorageMediaFileSetUID
```

В результате выполнения скрипта можно получить все данные значения PatientName, обходя при этом авторизацию.

Разработка эксплойта уязвимости для open source PACS сервера dcm4chee. Эксплойт написан на языке программирования Python и использует сторонние библиотеки pynetdicom и pydicom. Первым шагом пытаемся обнаружить DICOM-сервер в инфраструктуре, далее составляем запрос

на получение всех пациентов с указанием необходимых данных. Вторым шагом отправляется запрос без данных, необходимых для аутентификации пользователя, на обнаруженный DICOM сервер, который использует ПО dcm4chee.

Для защиты от данного эксплойта можно использовать правила в IPS/IDS системах, которые будут перехватывать пакеты Query/Retrieve к серверу PACS dcm4chee и проверять хеш-данные авторизации, указанные в пакете с запросом. Далее правило будет пропускать или отклонять данный пакет в зависимости от соответствия хеша данных авторизации, указанных в пакете с хешем хранимыми IPS/IDS системой.

Рассмотрим уязвимости аппаратного обеспечения. Ранние медицинские устройства взаимодействовали только с пациентами. Современные медицинские устройства управляются операционными системами и взаимодействуют с сетевым оборудованием. Передовые технологии в данной сфере направлены на создание точных инструментов, улучшающих качество медицинской помощи, но в то же время это приводит к дополнительным рискам, связанным с информационной безопасностью.

Врачи и пациенты полагаются на различное специализированное аппаратное обеспечение как для безопасного и точного введения жидкости и лекарств, так и для контроля жизнедеятельности различных органов. Однако существуют проблемы, которые могут поставить под угрозу безопасное использование аппаратного обеспечения. Данные проблемы могут привести к чрезмерному или недостаточному вливанию лекарственных препаратов, и впоследствии к неправильному лечению и оценке состояния пациента.

Сфера применения данного подхода заключается в рассмотрении обобщенного жизненного цикла аппаратуры медицинского назначения от его покупки до вывода из эксплуатации. Жизненный цикл состоит из следующих пунктов:

- закупка,
- постановка на учет,
- обучение и инструктирование персонала,
- конфигурирование,
- использование,
- техническое обслуживание,
- деактивация,
- вывод из эксплуатации.

В зависимости от типа аппаратуры каких-либо пунктов может не быть.

В процессе использования аппаратуры доступ к ней получает множество людей. Они используют системы, необходимые для оказания помощи пациентам. Однако в данный процесс могут вклиниваться люди с плохими намерениями или с недостаточной квалификацией. Список лиц, которые могут взаимодействовать с устройством:

- пациент,
- медицинский работник,
- фармацевт,
- инженер поставщика,
- биомедицинский инженер,
- сетевой менеджер рисков (медицинские информационные технологии),
- инженер по информационной безопасности,
- ИТ-инженер сети,
- центральный работник снабжения,
- посетитель пациента,
- хакер.

Сценарий основан на действиях участников и взаимодействии каждого из них с аппаратурой. Сценарий может быть изменен на основе инфор-

мации от команды разработчиков. Базовый сценарий начинается с того, что ИТ-инженер предоставляет беспроводную сеть, далее биомедицинский инженер подключает аппаратуру к сети. Затем медицинский работник настраивает устройство для лечения пациента. Врач выписывает лекарства пациенту, а фармацевт выдает их. После того, как устройство установлено и настроено, медицинский работник применяет его для лечения пациента. Обслуживание обеспечивается инженером ИТ-безопасности и центральными работниками снабжения, которые удостоверяются в исправности аппаратуры. Пациенты могут взаимодействовать с медицинскими работниками, если у работников или у пациента есть вопросы или проблемы. Хакеры могут попытаться атаковать аппаратуру через различные векторы, включая само устройство, сервер данного устройства, беспроводную сеть, клинические и больничные ИТ-системы. После происходит несколько циклов ремонта устройства и в дальнейшем списание и утилизация в случае выхода из строя или истечения срока службы.

Для более наглядного примера рассмотрим один из вариантов атак — аппаратные закладки (Hardware Additions) (рис. 6. 11).

Данный тип атак использует аппаратные возможности оборудования с применением модифицированного программного обеспечения с целью беспрепятственного проникновения вовнутрь критической инфраструктуры.

Создание аппаратных закладок преследует цели предоставления третьей стороне доступа к защищенным данным, а также вызов сбоев в критически важных моментах работы схем, тем самым делая ее ненадежной.

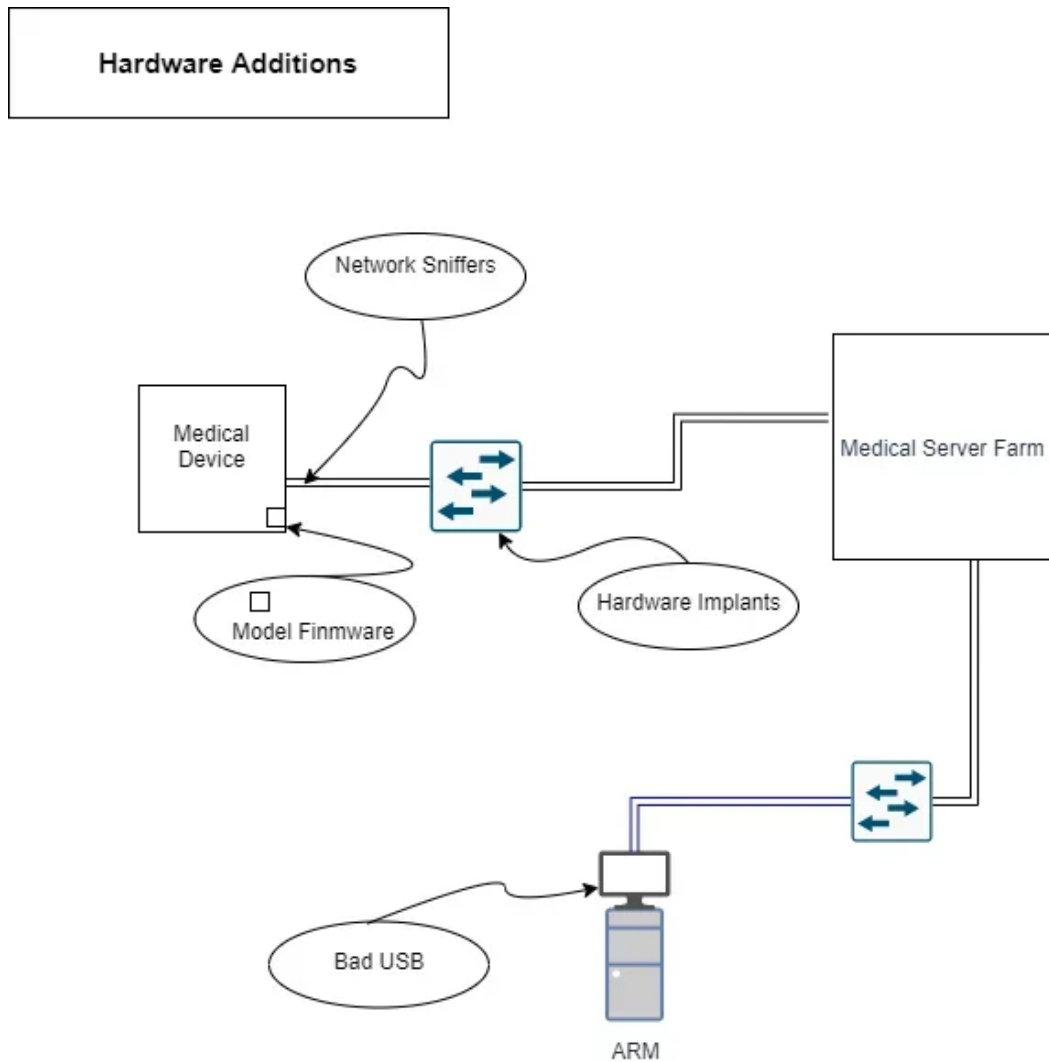


Рисунок 6.11 — Возможные векторы атак с помощью аппаратных закладок

Вне организации (до поставки оборудования в медицинскую организацию) внедряется модифицированное программное обеспечение. Перепрошивается программное обеспечение главного или периферийных модулей медицинского оборудования с внедрением недокументированных возможностей скрытой передачи или искажения информации. Далее при поставке оборудования в медицинскую организацию, оно начинает скрыто передавать конфиденциальную информацию третьим лицам. В том числе данное ПО может иметь дополнительные функции в виде RAT (Remote Access Trojan), которое может позволить подключиться к оборудованию извне.

В Spiegel был опубликован список существующих аппаратных закладок, разработанных в National Security Agency (Агентстве национальной безопасности) США, который включал в себя разработки, связанные с сетевым оборудованием Cisco, Huawei, Juniper [235].

Эффективным методом защиты от такого рода уязвимостей является публикация производителем полного описания механизмов функционирования готового изделия — микроконтроллерного оборудования, операционных систем, а также микропрограмм.

Применение свободного программного обеспечения с открытым исходным кодом подразумевает поставку программ, низкоуровневых драйверов в исходном коде, позволяя специалистам определить существующие закладки и устранить их.

6.3. Экспериментальный стенд для оценки ресурсоэффективности систем контроля доступа

Функционирование описанных компонентов можно обеспечить в среде виртуальных машин, что поможет улучшить отказоустойчивость за счет механизмов миграции ВМ, активируемых при отказе физических серверов, а также уменьшить накладные расходы, связанные с администрированием серверных систем. Рекомендуемое распределение компонентов по виртуальным машинам приведено в табл. 6.1 и 6.2, описывающих серверные роли, выполняемые ВМ. Функционирование всех ВМ предполагается под управлением ОС Linux x64, выбор конкретного дистрибутива определяется рекомендациями разработчиков развертываемого ПО.

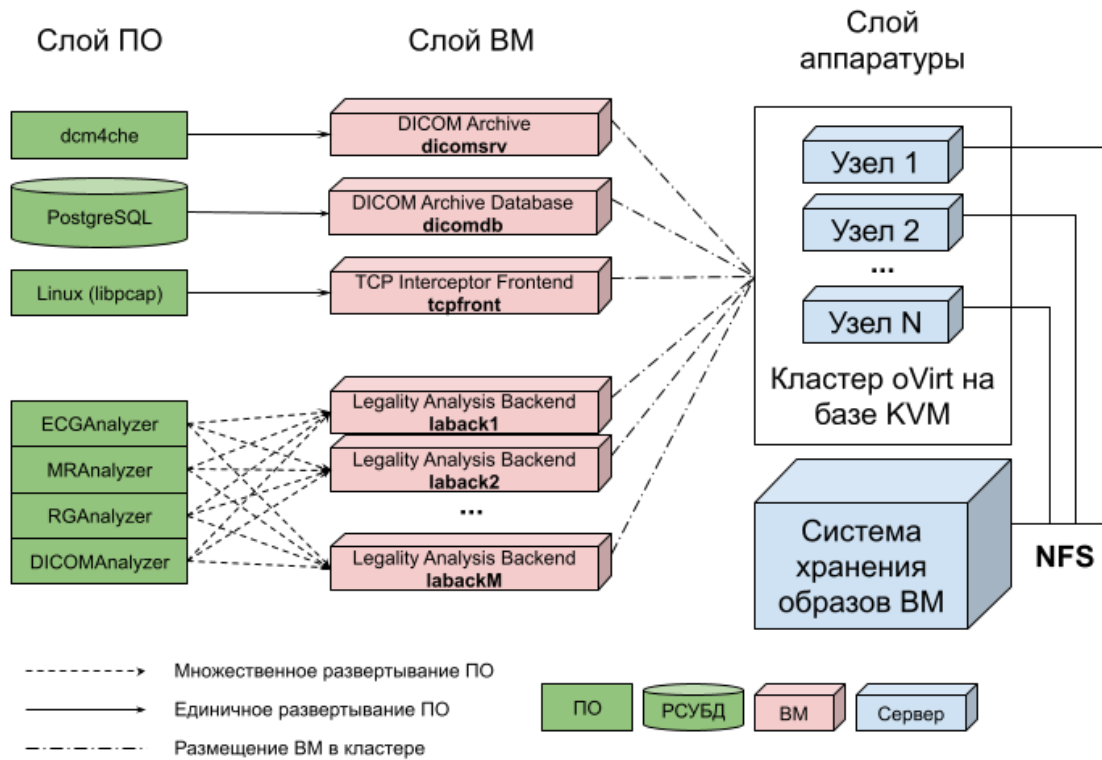
Таблица 6.1 — Серверные роли виртуальных машин
(кластер для проверки корректности содержимого в архиве DICOM)

Имя ВМ	Серверная роль ВМ	Компоненты ПО	Описание ВМ
dicomsrv	DICOM Archive	dcm4che	Архив DICOM, содержащий медицинские данные. Является защищаемым объектом
dicomdb	DICOM Archive Database	PostgreSQL	База данных архива DICOM, необходимая для его функционирования
tcpfront	TCP Interceptor Frontend	Linux (libpcap)	Входящий трафик, предназначенный для PACS, просматривается на TCPInterceptorFrontend и направляется для анализа на узлы LegalityAnalysisBackend с балансировкой по алгоритму round-robin
laback1, ..., labackM	Legality Analysis Backend	DICOMAnalyzer RGAnalyzer MRAnalyzer ECGAnalyzer	Содержит компонент анализа содержимого файлов DICOM (DICOMAnalyzer), а также плагины проверки корректности медицинских данных для каждой модальности (RG, MR, ECG)

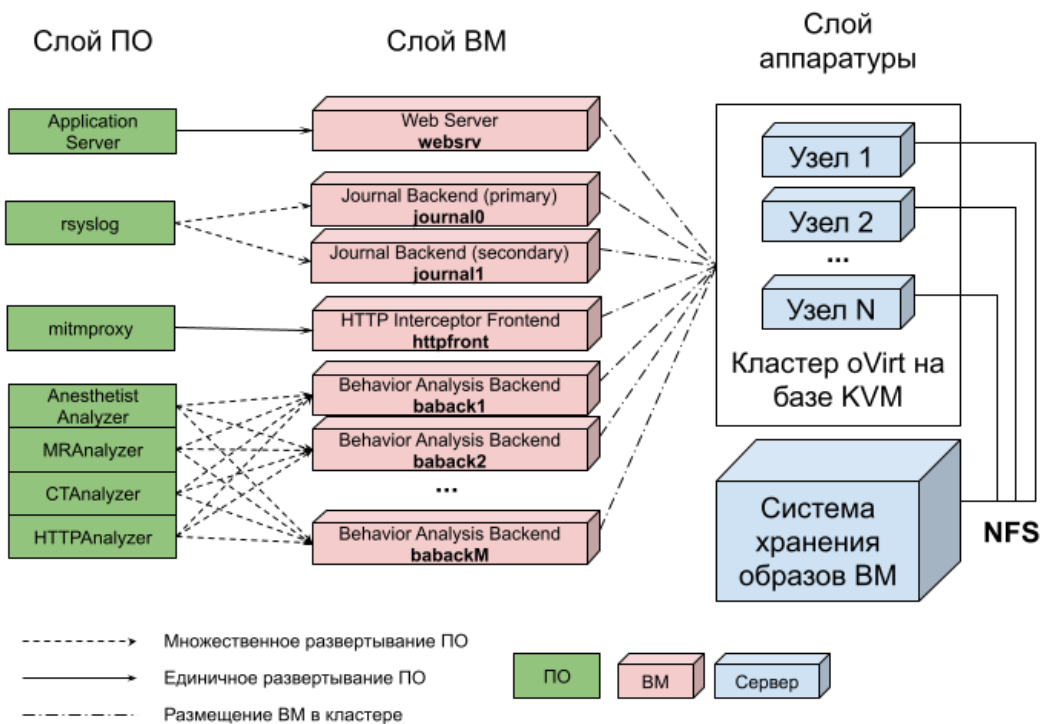
На рис. 6.12 представлена рекомендуемая схема развертывания кластеров проверки целостности архива DICOM (а) и анализа пользовательского поведения (б) с учетом слоя виртуализации. Отказоустойчивость кластеров обеспечивается за счет множественности экземпляров серверных ролей Legality Analysis Backend и Behavior Analysis Backend.

Таблица 6.2 — Серверные роли виртуальных машин (кластер для проверки корректности пользовательского поведения)

Имя VM	Серверная роль VM	Компоненты ПО	Описание VM
websrv	Web Server	ApplicationServer	Сервер приложений МИС. Является защищаемым объектом
journal0	Journal Backend (primary)	rsyslog	Журнал пользовательских действий. Отказоустойчивость обеспечивается наличием первичного и вторичного экземпляров rsyslog [236]. При отказе первичного экземпляра данные направляются на вторичный. При возвращении в строй первичного экземпляра он вновь начинает принимать данные
journal1	Journal Backend (secondary)	rsyslog	
httpfront	HTTP Interceptor Frontend	mitmproxy	Входящий трафик, предназначенный для сервера приложений, просматривается на узле HTTPInterceptorFrontend и направляется для анализа на узлы BehaviorAnalysisBackend с балансировкой по алгоритму round-robin
baback1, ..., babackM	Behavior Analysis Backend	HTTPAnalyzer MRAnalyzer CTAnalyzer AnesthetistAnalyzer	Содержит компонент анализа поведения пользователей (HTTPAnalyzer), а также плагины проверки корректности пользовательского поведения для различных врачебных специализаций (СТ, MR, Anesthetist)



а) рекомендуемая схема развертывания кластера проверки целостности архива DICOM



б) рекомендуемая схема развертывания кластера анализа пользовательского поведения

Рисунок 6.12 — Развертывание виртуальных машин и программного обеспечения

Для размещения предлагаемых серверных ролей использована лезвийная система Supermicro 938-16, содержащая 8 лезвий в едином шасси. Характеристики оборудования приведены в табл. 6.3 и 6.4.

Таблица 6.3 — Характеристики вычислительного оборудования

Компонент лезвия	Характеристики компонента
Процессор	Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz. 10 ядер, 20 потоков.
Оперативная память	DDR3 1600MHz, 16Gb
Сетевой адаптер Ethernet	2 адаптера Intel Corporation I350 Gigabit Network Connection (rev 01)
Сетевой адаптер InfiniBand	Mellanox Technologies MT25408A0-FCC-QI ConnectX, Dual Port 40Gb/s
Дисковые накопители	2 накопителя HDD по 4TB: Seagate Desktop HDD.15 ST4000DM000-1F2168

Таблица 6.4 — Характеристики сетевого оборудования

Компонент сети	Характеристики компонента
Ethernet Switch	D-Link Gigabit Ethernet Switch
InfiniBand Switch	Mellanox InfiniBand QDR Switch

Сети Ethernet и InfiniBand функционируют без конфигурации VLAN. На вычислительных лезвиях функционирует драйвер IP over IB. На каждом лезвии задействован только один порт Ethernet и InfiniBand.

Все лезвия функционируют под управлением операционной системы CentOS 7 x64. Дисковые накопители объединены в программном RAID1. Уровень виртуализации сконфигурирован с помощью qemu-kvm [237]. Описание виртуальных машин, развертываемых на вычислительных лезвиях, приведено в табл. 6.5. Все они функционируют под управлением ОС Centos 7 x64.

Таблица 6.5 — Характеристики виртуальных машин

Имя VM	Характеристики VM
dicomsvr	4 ядра, 15Гб ОЗУ, 2Тб пространства HDD, Gigabit Ethernet
dicomdb	2 ядра, 8Гб ОЗУ, 2Тб пространства HDD, Gigabit Ethernet
tcpfront	4 ядра, 4Гб ОЗУ, 2Тб пространства HDD, Gigabit Ethernet
laback0, laback1, laback2, laback3, laback4	4 ядра, 8Гб ОЗУ, 4Гб пространства HDD, Gigabit Ethernet

Любая из виртуальных машин может быть развернута на любом из лезвий, если оно располагает достаточным количеством ресурсов на момент развертывания. На рис. 6.13 проиллюстрирована возможная схема развертывания на восьми лезвиях компонентов и машин, применяемых в эксперименте.

Экспериментальное исследование системы проводилось под следующей нагрузкой: на вход машины tcpfront подавались запросы на прием фрагмента ЭКГ со случайным интервалом длительностью от 0 до 625 мс (ГСЧ работает согласно равномерному распределению). Общее количество запросов равно 200. Размер фрагмента ЭКГ — 1,25Мб. Общее время работы системы для обслуживания всех принятых запросов составило 61 с. На рис. 6.14 приведены графики потребления ресурсов каждой VM.

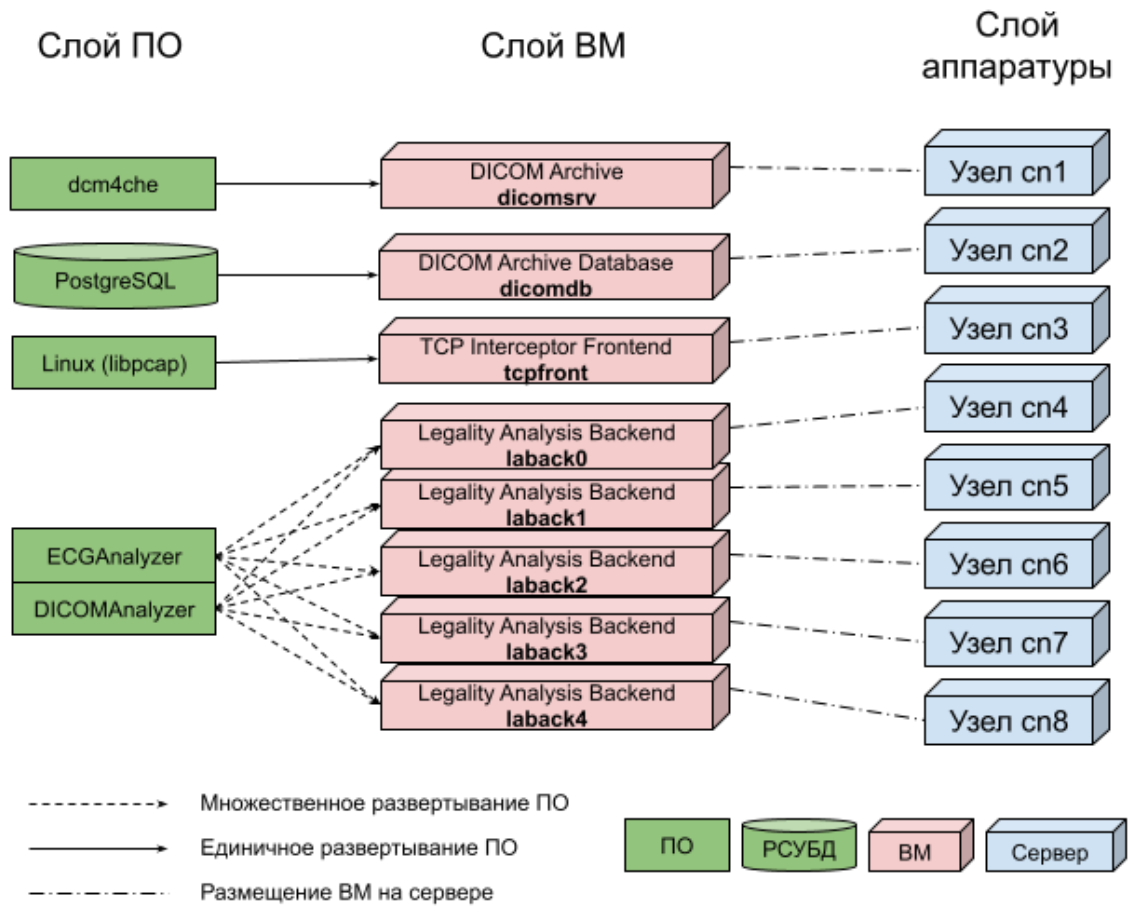
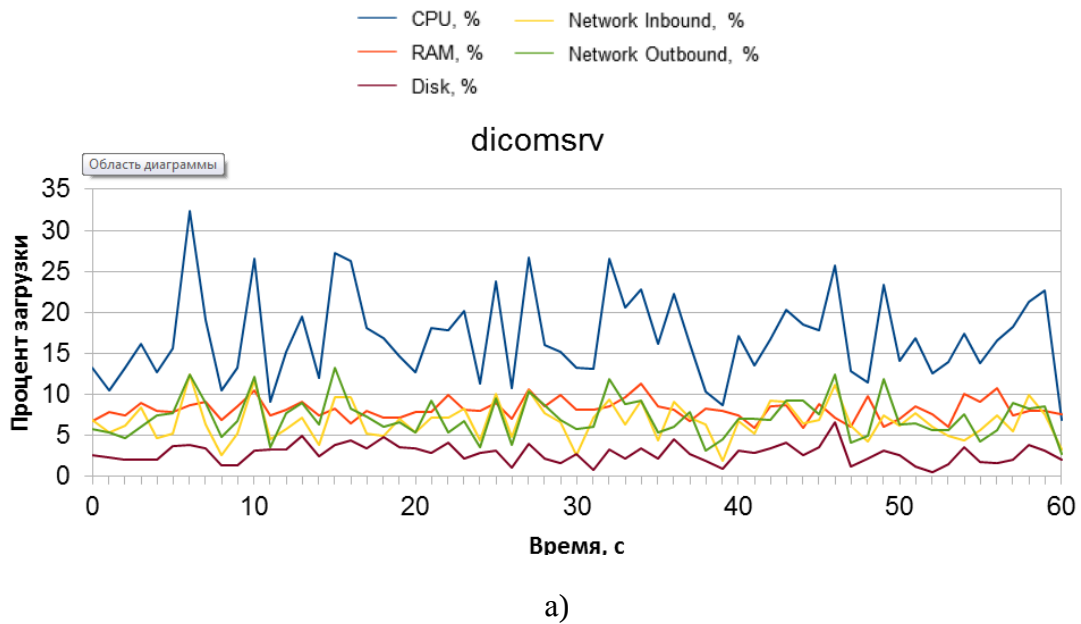
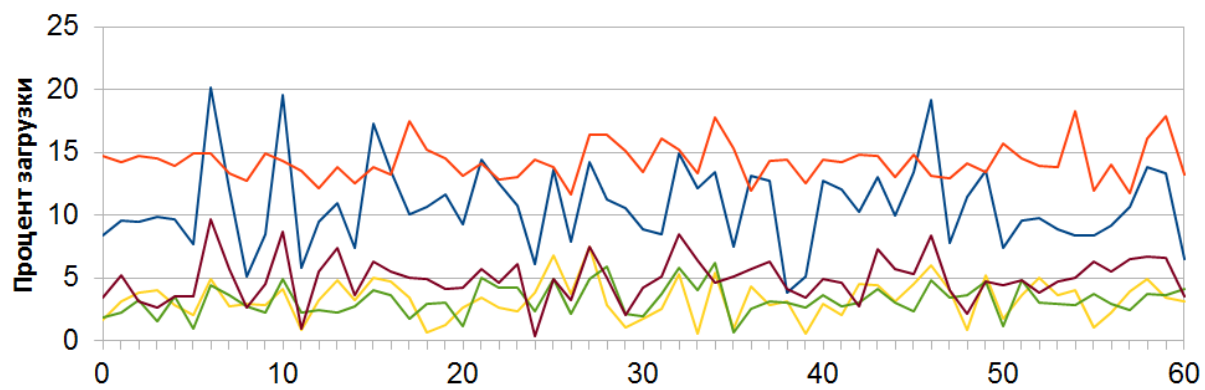


Рисунок 6.13 — Размещение виртуальных машин и ПО

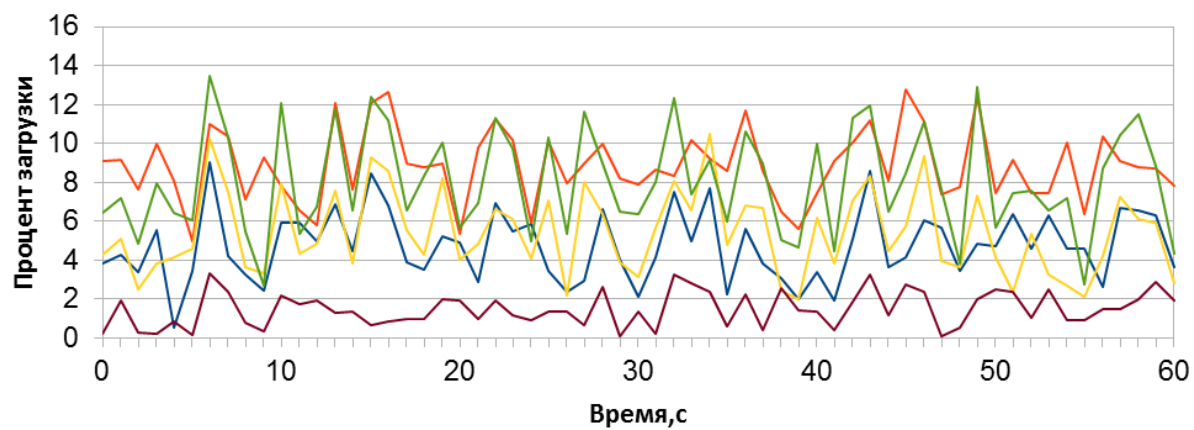


dicomdb



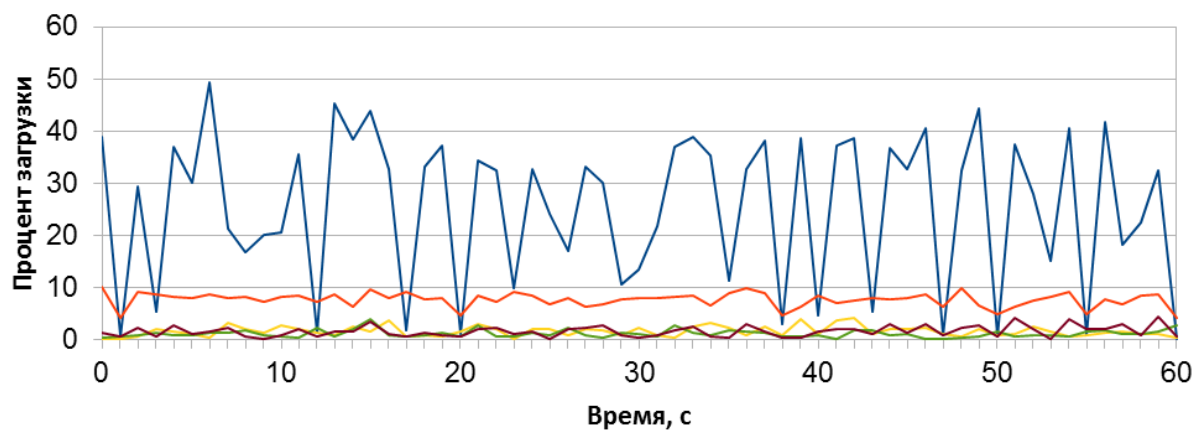
б)

tcpfront



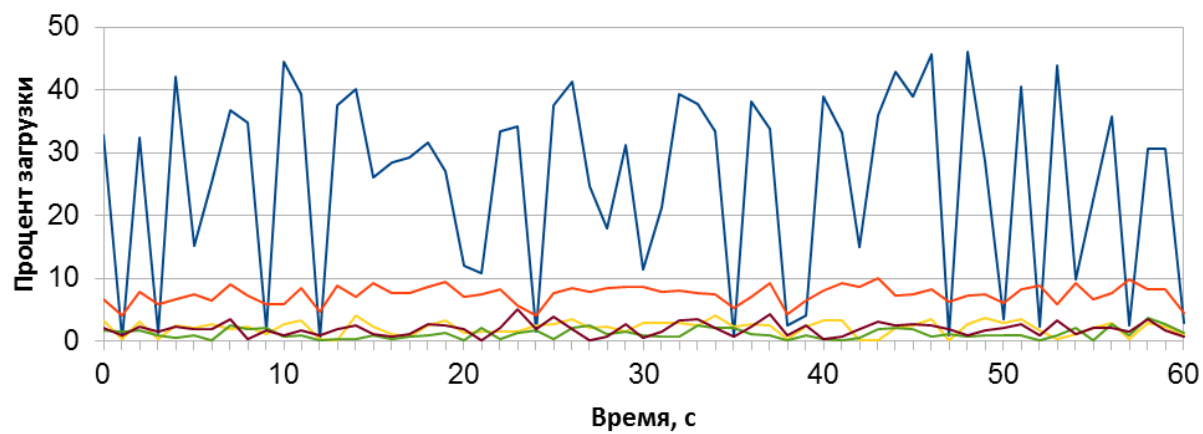
в)

laback0



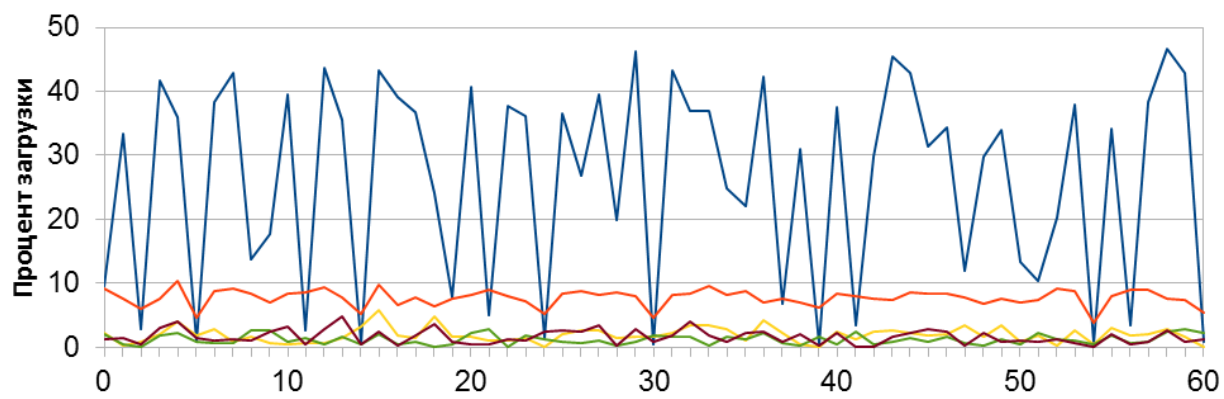
г)

laback1



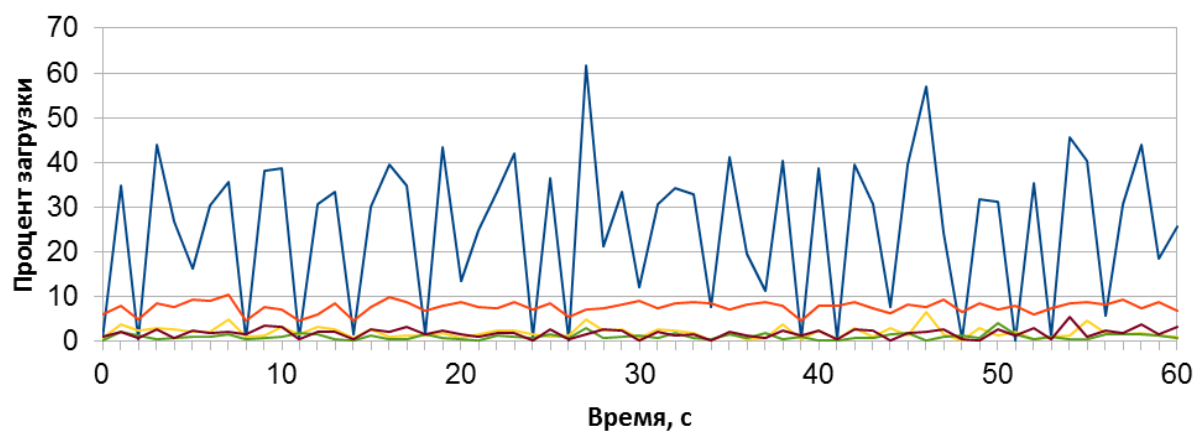
д)

laback2

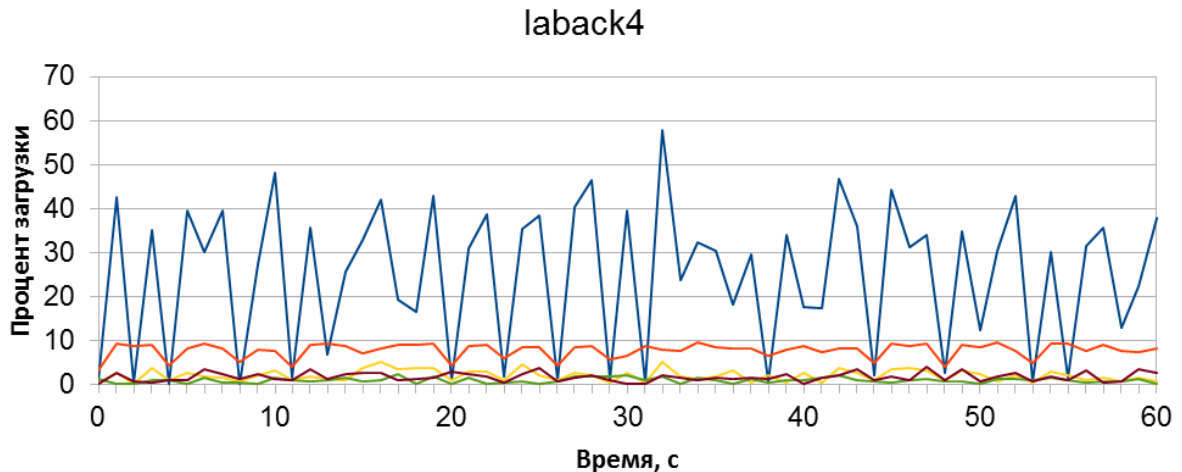


е)

laback3



ж)



3)

Рисунок 6.14 — Потребление ресурсов виртуальными машинами

Тестирование показало почти симметричную нагрузку на входящий и исходящий сетевой каналы машины `dicomsrv`. Это объясняется тем, что на каждую запись в архив DICOM приходится одно чтение записанных данных в аналитическом компоненте DICOM Analyzer. Всплески активности на машине `dicomdb` соответствуют таковым у машины `dicomsrv`, что ожидаемо в условиях эксклюзивного использования БД PostgreSQL компонентом `dcm4che`. Машина `tcpfront` значительно более нагружена по сетевому интерфейсу, чем по остальным ресурсам. Это объясняется тем, что на ней не запускаются аналитические задачи, а только перехватываются сетевые пакеты. Заметим, что нагрузка на ее исходящий канал примерно вдвое превышает нагрузку на входящий: принятый DICOM-трафик направляется как в архив DICOM, так и на аналитические машины Legality Analysys Backend. Производящиеся на них операции анализа корректности периодичности принятых фрагментов ЭКГ не требуют значительных объемов памяти, поэтому основная нагрузка по их выполнению ложится на процессоры. График на рис. 6.15 показывает загрузку процессоров аналитических машин, нагружаемых по алгоритму `round-robin`.

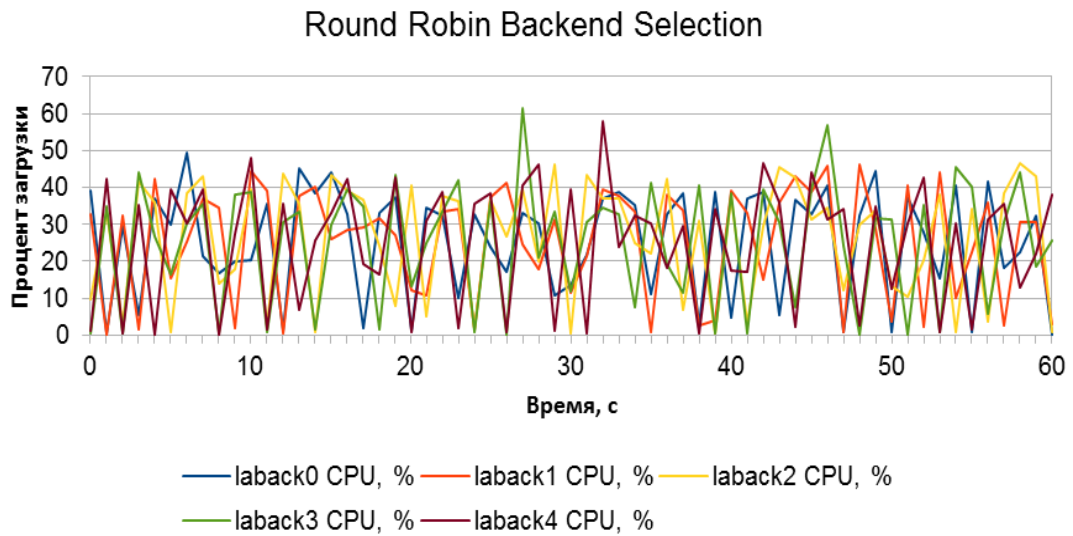


Рисунок 6.15 — Потребление ресурсов процессора аналитическими машинами

В табл. 6.6 приведена средняя загрузка ресурсов на всех восьми виртуальных машинах. Исходя из данных табл. 6.6, можно заключить, что тестовый аналитический кластер может быть оптимизирован путем уменьшения объема оперативной памяти, выдаваемой виртуальным машинам. Нагрузку на процессоры можно оценить как среднюю, запас для обработки всплесков количества запросов остается. Однако при добавлении новых аналитических плагинов, оценку ресурсов требуется повторить.

Загрузка защищаемых компонентов DICOMArchive (dcm4che) и DICOM Archive Database (PostgreSQL) при отсутствии аналитического кластера ожидаемо снижается. Это обусловлено отсутствием операции чтения данных из архива DICOM, проводимой аналитическими компонентами для каждого принятого DICOM-файла (остается только запись в архив DICOM).

Таблица 6.6 — Средняя загрузка ресурсов на виртуальных машинах

ВМ	Средняя загрузка CPU, %	Средняя загрузка RAM, %	Средняя загрузка сети, входящий канал, %	Средняя загрузка сети, исходящий канал, %	Средняя загрузка диска, %
dicomsrv	16,96	8,10	6,68	7,15	2,74
dicomdb	10,75	14,25	3,27	3,23	4,93
tcpfront	4,73	8,86	5,40	8,05	1,48
laback0	25,31	7,65	1,59	1,12	1,60
laback1	25,33	7,41	2,07	1,16	1,88
laback2	26,14	7,76	1,95	1,25	1,64
laback3	24,99	7,59	1,88	0,96	1,72
laback4	24,81	7,74	2,03	0,93	1,68

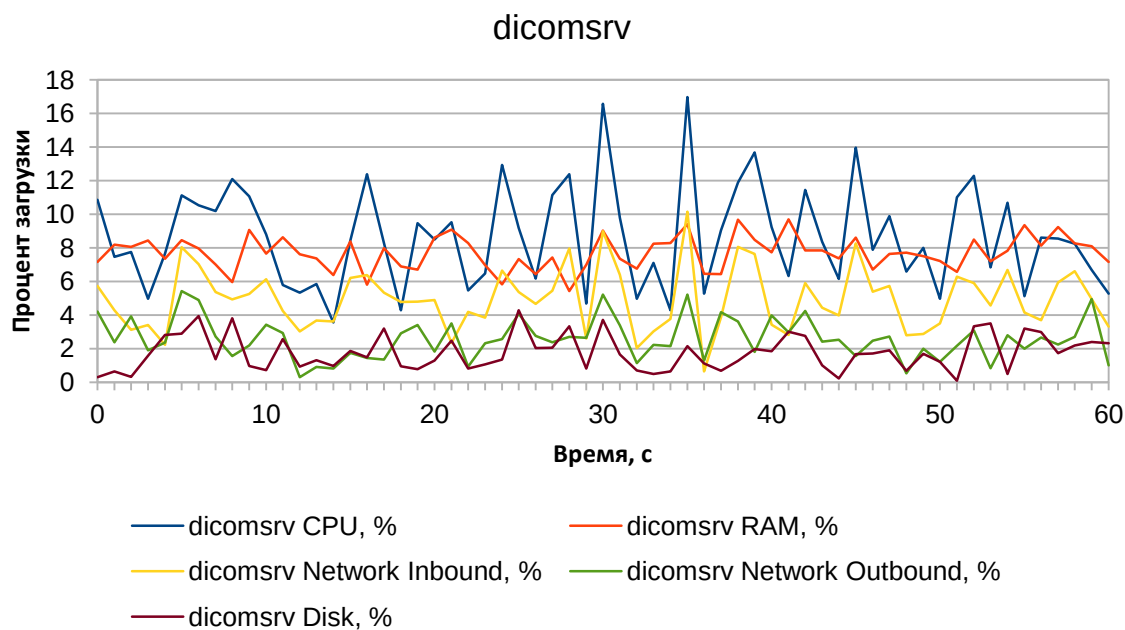
В табл. 6.7 приведена средняя загрузка ресурсов на двух используемых виртуальных машинах dicomsrv и dicomdb.

Таблица 6.7 — Средняя загрузка ресурсов на виртуальных машинах dicomsrv и dicomdb

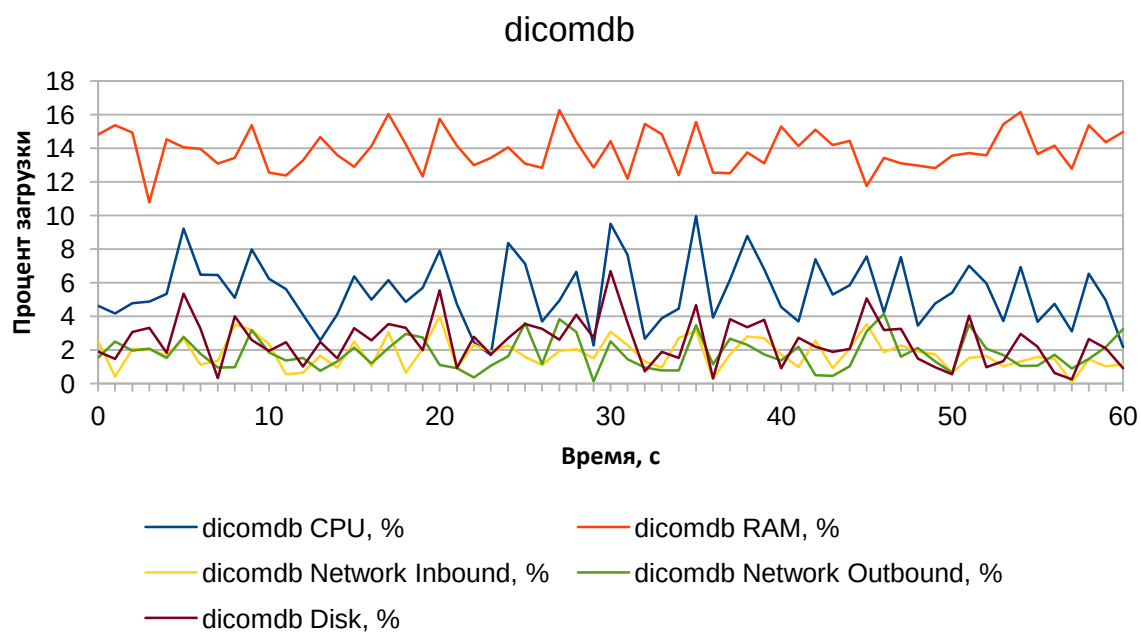
ВМ	Средняя загрузка CPU, %	Средняя загрузка RAM, %	Средняя загрузка сети, входящий канал, %	Средняя загрузка сети, исходящий канал, %	Средняя загрузка диска, %
dicomsrv	8,66	7,70	4,94	2,58	1,75
dicomdb	5,44	13,91	1,79	1,79	2,52

На рисунке 6.16 приведены графики загрузки ресурсов двух ВМ dicomsrv и dicomdb при сохранившемся количестве запросов и интервалами между ними.

В табл. 6.8 приведен коэффициент снижения нагрузки на ресурсы ВМ в условиях отсутствия аналитических компонентов.



а)



б)

Рисунок 6.16 — Потребление ресурсов виртуальными dicomsvr и dicomdb машинами без аналитического кластера

Таблица 6.8 — Коэффициент снижения нагрузки
на ресурсы ВМ dicomsrv и dicomdb

ВМ	Средняя загрузка CPU, раз	Средняя загрузка RAM, раз	Средняя загрузка се- ти, входя- щий канал, раз	Средняя загрузка сети, исходящий канал, раз	Средняя загрузка диска, раз
dicomsrv	1,96	1,05	1,35	2,77	1,56
dicomdb	1,98	1,02	1,83	1,80	1,95

Почти двухкратная разница в загрузке процессоров объясняется двухкратным уменьшением количества запросов в DICOM-архив. Значительно изменилась нагрузка на исходящий канал dicomsrv — остались только служебные данные, передаваемые по протоколу DICOM для обеспечения записи в архив DICOM. Также заметно снижение нагрузки на диск — теперь отсутствует обслуживание операции чтения из архива DICOM.

Разработанный экспериментальный фреймворк и предложенный подход к тестированию применимы для оценки производительности как существующих кластерных конфигураций, так и планируемых к приобретению, поскольку для оценки доступны ресурсы, потребляемые каждым из компонентов в отдельности.

6.4. Рекомендации к построению безопасной цифровой среды медицинского учреждения

Предложенные выше, в гл. 3, новые серверные роли для защиты архива DICOM и сервера приложений медицинской информационной системы функционируют в трех перечисленных зонах:

- зона медицинских приборов и оборудования;
- зона серверов, обслуживающих медицинское оборудование;
- зона серверов медицинских сервисов, требующих обмена данных с внешними сервисами.

Выше описаны различные способы, с помощью которых злоумышленники могут получить доступ к медицинским данным пациентов. Рассмотрим шаги, которые необходимо предпринять всем медицинским учреждениям для повышения безопасности медицинских данных.

Первая и самая необходимая рекомендация — это убрать все узлы, которые участвуют в обработке медицинских данных из публичного доступа. Очевидный факт: медицинская информация должна оставаться исключительно в пределах локальной сети учреждения. Однако на данный момент более тысячи DICOM-устройств находятся в публичном доступе, о чем говорит статистика, полученная с помощью поисковой системы Shodan (рис. 6.9). Как правило, в «открытом доступе» находятся всевозможные PACS-серверы и EMR-системы (системы учета пациентов), которые хранят в себе ценную для злоумышленника информацию. Такие системы необходимо поместить в соответствующие сегменты внутри корпоративного периметра, изолировать от их неавторизованного использования третьими лицами и осуществлять регулярное резервное копирование их содержимого. Практически любую систему обнаружения вторжений, в том числе и с открытым исходным кодом (например, Suricata) [238] можно настроить на обнаружение незашифрованных пакетов, передаваемых по протоколу DICOM в PACS-сети.

Еще один из вариантов к повышению защищенности — это защита передачи данных между сервером и медицинским оборудованием [239]. Необходимо ставить дополнительное оборудование для шифрования трафика медицинского оборудования. Для исключения возможности подключения между медицинским оборудованием и оборудованием для шифрова-

ния вводятся модули проверки и аутентификации оборудования на основе протокола 802.1x и анализа трафика данного оборудования. Для серверов вводится дополнительный периметр защиты с применением межсетевого экрана (для фильтрации и обслуживания только VPN трафика), а также Reverse Proxy и Web Application Firewall. Для подключения к серверам следует использовать защищенный протокол HTTPS для медицинского персонала. В этом случае, медицинская сеть является максимально приближенной к изолированной сети. Схематически это можно изобразить так, как представлено на рис. 6.17.

Вторая рекомендация — обязательное ведение журналов. Журналы являются важной частью стратегии обеспечения безопасности. Предполагается, что рано или поздно любую систему можно будет скомпрометировать, как внешним злоумышленникам, так и внутренним, поэтому журналы являются одним из наиболее полезных инструментов, которые можно использовать для отслеживания того, как злоумышленники получили доступ к системе. Также журналы позволяют организации быстрее вернуться в строй, так как можно понять вектор атаки и понять масштаб бедствия. Обеспечение безопасности журналов является одной из наиболее важных задач, хотя ее отсутствие не ставит под угрозу уже реализованную защиту.

Третья рекомендация: ввиду разнообразия ролей в больнице (врачи, регистратура, ординаторы, медсестры, администрация и т. д.) должны быть введены процедуры и регламенты контроля доступа. А именно, каждая роль должна быть четко описана, и для неё должны быть конкретно перечислены системы и интерфейсы, которыми пользователь с данной ролью может пользоваться, а остальные, не являющиеся необходимыми для работы, должны быть недоступны. Также учетные данные пользователей должны регулярно проверяться на соответствие реальной роли сотрудника (учитывать увольнения, переход в другую организацию или на другую должность и т. д.).

Рисунок 6.17 — Рекомендованная настройка сегмента сети,
содержащего PACS

Четвертая рекомендация: на сегодняшний день концепция «принеси свое собственное устройство» (BYOD) [240] популярна во всех организациях, и медицинские учреждения не являются исключением. Использование личных мобильных устройств для решения повседневных задач, будь это проверка почты, пересылка диагноза, вход в клиническую систему, необходимо запретить, так как защищенность данных на личных мобильных устройствах не контролируется организацией, при этом большинство пользователей достаточно халатно относится как к персональной, так и к корпоративной безопасности.

Пятая рекомендация, которая также является одной из основных для повышения надежности функционирования сети [241], — это своевременное обновление всех программных компонентов медицинского учреждения и удаление не относящихся к функционированию организации программ. Выше показаны примеры, как легко найти актуальные уязвимости и использовать их, поэтому анализ установленного программного обеспечения очень важен.

Шестая рекомендация заключается в применении сканирования на регулярной основе. Для обеспечения безопасного функционирования информационной инфраструктуры ВК вычислительных сервисов здравоохранения необходимо предпринять перечень мер. В [121] были предложены рекомендации к построению безопасной инфраструктуры, а также рекомендованная настройка сегмента сети, содержащего PACS. Однако процесс перенастройки текущей инфраструктуры — процесс долгий, требующий большого количества согласований, а также не мешающий повседневной работе организации. В связи с этим предлагается наладить непрерывный процесс мониторинга инфраструктуры ВК, чтоб своевременно выявлять потенциально несанкционированный доступ к информации.

Ниже предлагаются алгоритм и блок-схема для данного процесса.

Алгоритм сканера подразумевает выполнение следующих шагов:

1. Сканирование портов сетевого периметра.
 - 1.1. Идентификация новых портов (ранее не обнаруженных).
2. Определение сервисов.
 - 2.1. Определение сервисов общего назначения (уже имеющиеся сканеры nmap, nessus, openvas).
 - 2.2. Определение сервисов медицинского назначения (уже имеющиеся сканеры и, возможно, плагины).
3. Поиск старых версий ПО (vulners, openvas, nessus).
4. Поиск открытых медицинских интерфейсов.
 - 4.1. Веб-вьюверов DICOM.
 - 4.2. Веб-интерфейсов EMR.
 - 4.3. Интерфейсов протокола DICOM (например, сервера dcm4chee).
 - 4.3.1. Проверить возможность аутентификации с известным АЕТ (перебрать по словарю).
5. Экспорт результатов в систему мониторинга и оповещения.
 - 5.1. Оповещение о новых открытых портах.
 - 5.2. Оповещение об уязвимостях сервисов (старые версии ПО).
 - 5.3. Оповещение об открытых медицинских интерфейсах.
6. Повторять регулярно, сохраняя предыдущий результат.

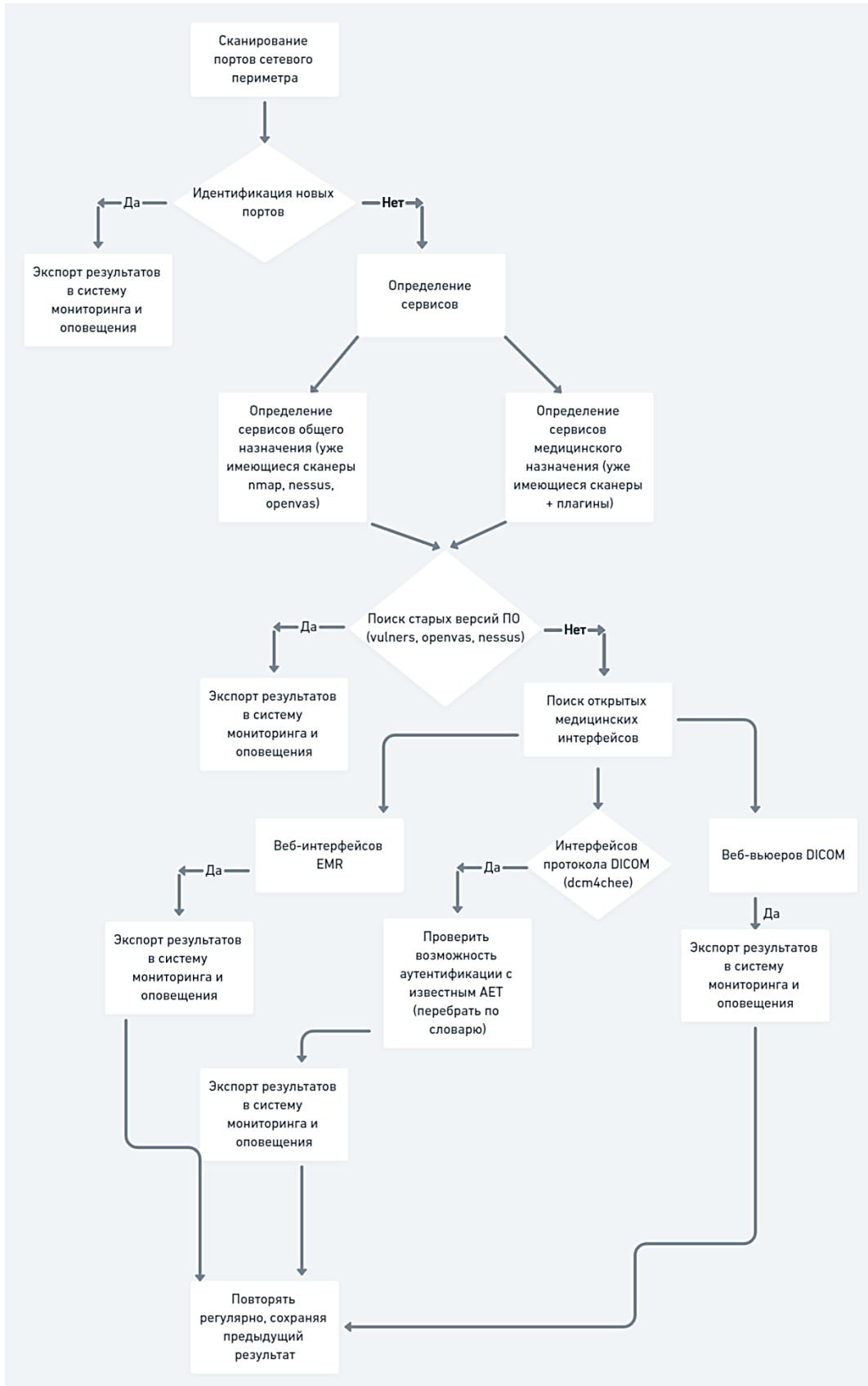


Рисунок 6.18 — Блок схема мониторинга медицинской инфраструктуры

Выводы по главе

Проанализированы кибератаки, которым подвергается медицинская инфраструктура. Выявлены критически важные подсистемы (зоны) в медицинской инфраструктуре: зона медицинских приборов и оборудования; зона сетевого коммутационного оборудования; зона серверов, обслуживающих медицинское оборудование; зона маршрутизации и межсетевого экранирования; зона серверов медицинских сервисов.

В целях оценки защищенности распространенных реализаций DICOM была смоделирована инфраструктура медицинского учреждения при помощи пакета dcm4che, в который входит DICOM-сервер, веб-интерфейс для просмотра изображений и различные вспомогательные утилиты.

Разработан эксплойт уязвимости для open source PACS сервера dcm4chee. Для защиты от подобных эксплойтов предложено использовать правила в IPS/IDS системах, которые будут перехватывать пакеты Query/Retrieve к серверу PACS dcm4chee и проверять хеш-данные авторизации, указанные в пакете с запросом, хранимыми IPS/IDS системой.

Разработаны рекомендации по конфигурированию вычислительной сети медицинского учреждения для повышения защищенности медицинских данных.

Разработанный экспериментальный фреймворк и предложенный подход к тестированию применимы для оценки производительности как существующих кластерных конфигураций, так и планируемых к приобретению, поскольку доступны для оценки ресурсы, потребляемые каждым из компонентов в отдельности.

Глава 7. ПОСТРОЕНИЕ МНОГОУРОВНЕВОЙ АРХИТЕКТУРЫ ВЫЧИСЛИТЕЛЬНЫХ КОМПЛЕКСОВ ДЛЯ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ДОСТУПА К СЕРВИСАМ УЧРЕЖДЕНИЙ ВЫСШЕГО ОБРАЗОВАНИЯ

В главе рассмотрены прикладные аспекты внедрения полученных в работе результатов в ВК, обеспечивающие информационную поддержку образовательных услуг в высшем образовательном учреждении. Разработаны архитектурные решения в соответствии с разработанными методами и моделями.

7.1. Типовая архитектура распределенных вычислительных комплексов для вычислительных сервисов сферы образования

В настоящее время, особенно во время пандемии короновируса COVID-19, высшие образовательные учреждения предоставляют целый комплекс образовательных услуг в дистанционном формате. Кроме того, ВС вуза содержат ресурсы, предназначенные для преподавателей и сотрудников организации. Все это определяет сложную систему ВК со структурно-сложной инфраструктурой. Современные образовательные учреждения предоставляют возможность подключения с различных устройств к вычислительным ресурсам и сервисам организации, нередко используются и беспроводные соединения.

На основе опыта разработки и внедрения [210, 240–244] ВС можно предложить типовую ИТ-инфраструктуру учреждений высшего образования (см. рис. 7.1). Разработаем архитектуру системы КД и проанализируем эффективность и защищенность ВС при ее использовании.

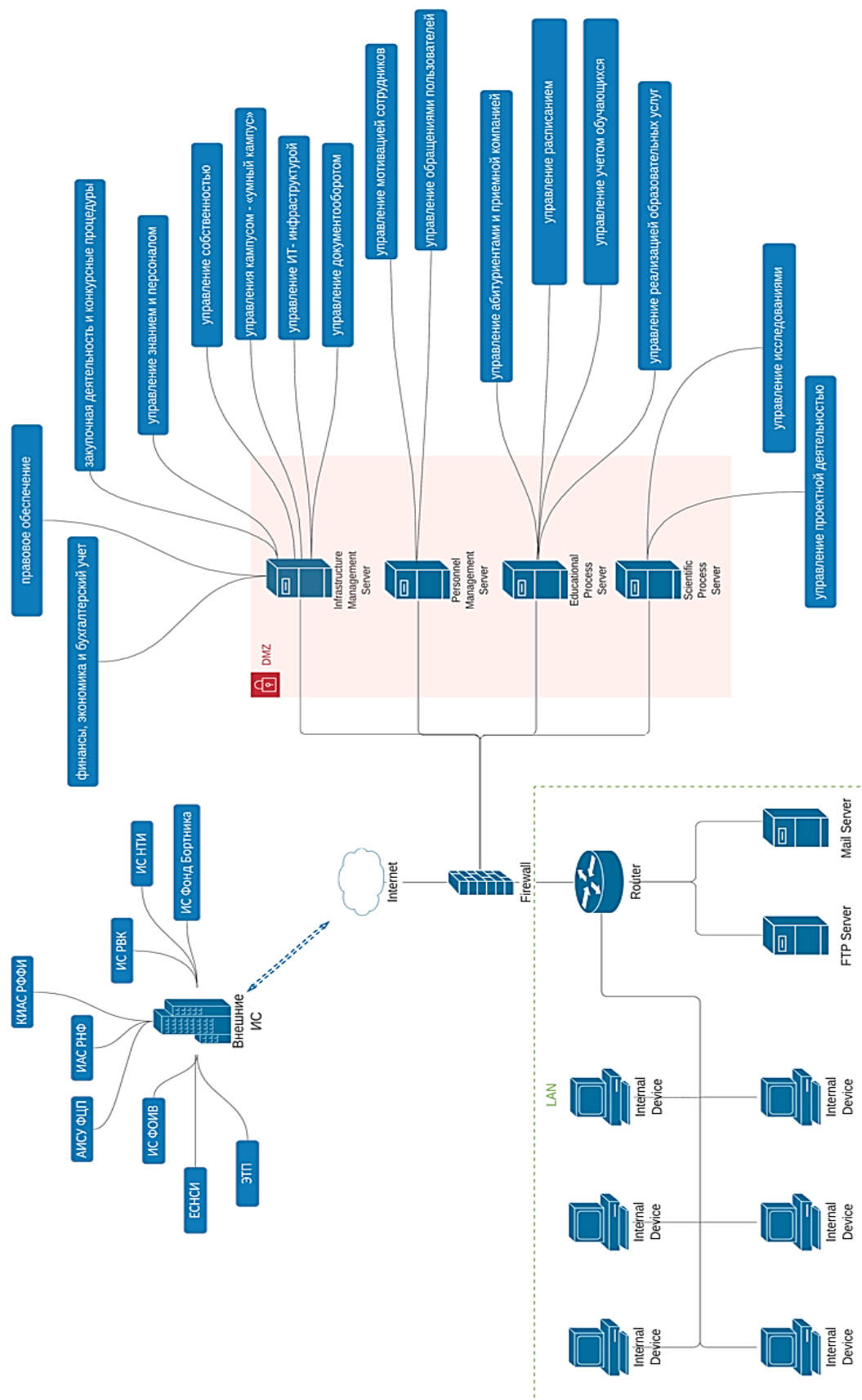


Рисунок 7.1 — ИТ-инфраструктура учреждений высшего образования

Условно ИТ-инфраструктуру ВК образовательного учреждения высшего образования можно разбить на 2 логические части:

- первая — это корпоративная инфраструктура, включающая в себя рабочие места административных единиц, серверы, обслуживающие их, а также сети учебных аудиторий и лабораторий;
- вторая — серверная часть образовательного портала, включающая в себя сервисы авторизации пользователей, серверы хранения контента, серверы обработки запросов пользователей и балансировщики нагрузки.

Образовательный портал, как правило, построен на основе микросервисной архитектуры, использующей контейнеризацию.

Сеть корпоративной инфраструктуры часто является одноранговой, но может быть разделена на подсети с использованием технологии VLAN. В большинстве случаев не происходит разделения сетевого доступа между подсетями. В случае контроля сетевого доступа нередко случается так, что системы были один раз настроены без динамического изменения правил доступа при изменении компонентов сетевой инфраструктуры.

Доступ к сети интернет контролируется на прокси-серверах и межсетевых экранах.

Согласно Федеральному Закону Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», на компьютерах образовательного учреждения запрещен доступ к ресурсам, содержащим информацию, причиняющую вред здоровью и (или) развитию детей.

На рис. 7.2 представлена типовая схема компьютерной сети вуза.

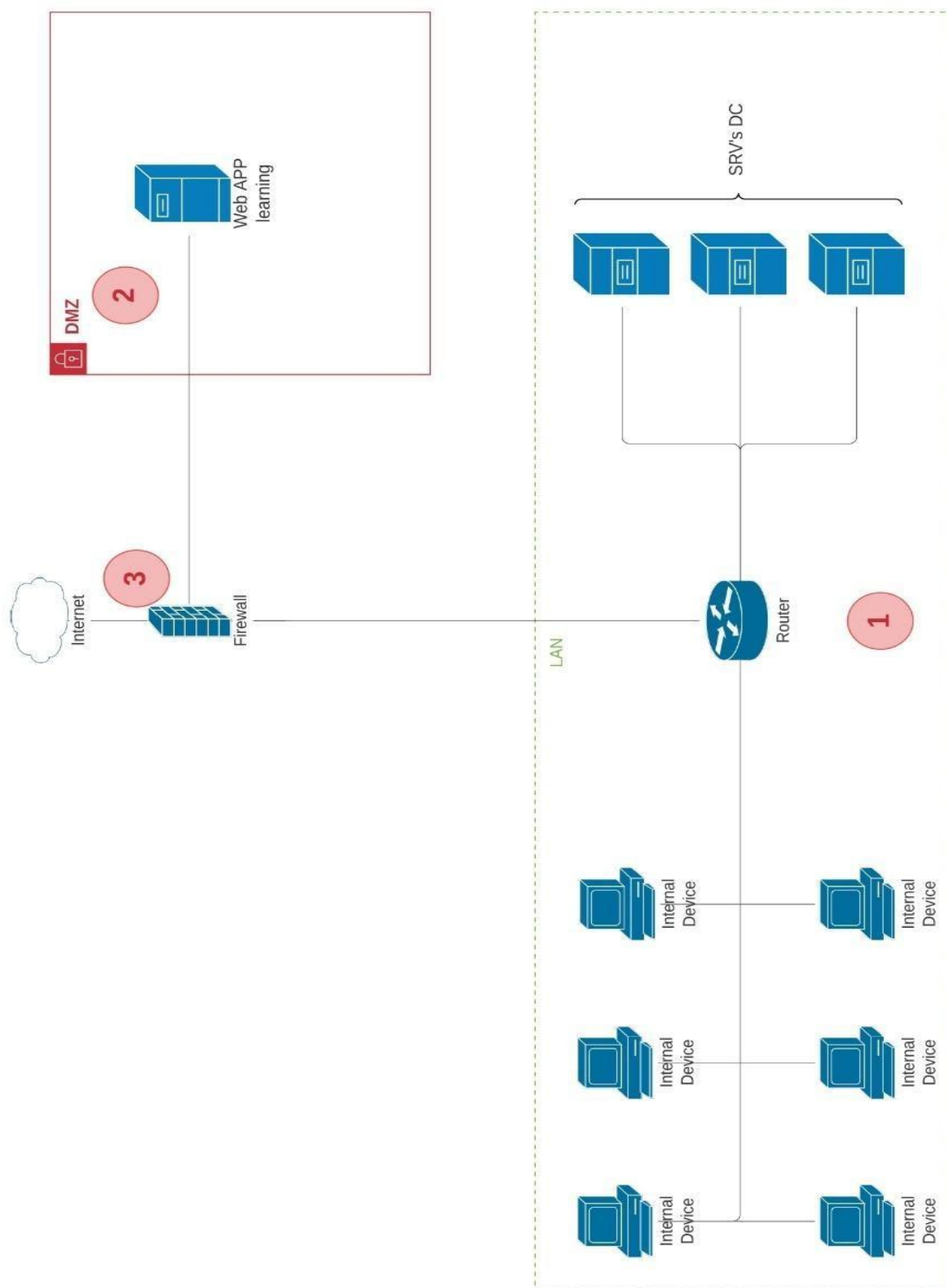


Рисунок 7.2 — Схема взаимодействия объектов ИТ-инфраструктуры образовательного учреждения

ИТ-инфраструктура сети ВК разделена на 3 зоны:

1. LAN (Local Area Network) — корпоративная сеть организации, в которой располагаются пользователи и сервера образовательного учреждения;
2. DMZ (Demilitarized Zone) — сеть, в которой располагаются общедоступные образовательные ресурсы организации и внутренняя зона;
3. Внешняя зона WAN (Wide Area Network) — сеть интернет, выделенная зона для общедоступных ресурсов.

Разделение на зоны не гарантирует полной защиты от несанкционированных действий, так как при проникновении во внутреннюю сеть корпоративного сегмента злоумышленник будет иметь доступ как к компьютерам, так и к серверам организации. Как правило, в подобных инфраструктурах не применяется мониторинг событий информационной безопасности, а также отслеживание сетевых аномалий.

Образовательный портал построен не на основе контейнеризации, а с использованием традиционных систем виртуализации или же на физических серверах. В свою очередь это может вносить дополнительные проблемы при восстановлении инфраструктуры в случае сбоя или взлома с повреждением данных. Образовательный портал имеет несколько компонентов, которые требуют обязательной авторизации пользователей. Ведение журналов авторизаций позволяет отследить попытки неавторизованного доступа пользователей, а также предотвратить попытки входа методом грубой силы (BruteForce). В типовой инфраструктуре образовательного портала отсутствует мониторинг действий пользователей, что может привести к взлому или несанкционированному доступу к ВС портала с последующим их повреждением или сбором конфиденциальных данных.

В настоящее время наиболее частым типом компьютерной атаки на общеобразовательные учреждения Российской Федерации являются АРТ-атаки. Самым распространенным вектором атаки является фишинг.

Злоумышленники проникают во внутреннюю инфраструктуру благодаря макросам, встроенным в файлы.

Вторым вектором АРТ-атаки являются уязвимые сервисы или сетевое оборудование (межсетевые экраны, маршрутизаторы) внешнего периметра организации. Необходимо ежедневно обновлять ПО и следить за выходом новых уязвимостей.

Еще одной проблемой во время пандемии COVID-19 стали случаи DDoS-атак на ВС вуза, особенно в дни зачетных недель. Специалистам ИБ необходимо разворачивать данные сервисы за CloudFlare с целью недопущения данных инцидентов.

Нередки случаи использования зараженных USB-накопителей для использования во внутренней сети. Служба ИБ вуза обязана информировать и обучать своих сотрудников с целью недопущения данных инцидентов информационной безопасности.

7.2. Система анализа поведения пользователей (UBA)

Без непрерывного анализа современных тенденций, а также отслеживания внутренних информационных процессов сложно сформировать ИТ-инфраструктуру вуза, обеспечивающую условия для эффективной работы сотрудников, преподавателей и студентов.

Технология UBA все активней используется как элемент защиты инфраструктуры ВК. Система UBA позволяет обнаружить несанкционированное воздействие на ИТ-инфраструктуру (рис. 7.3).

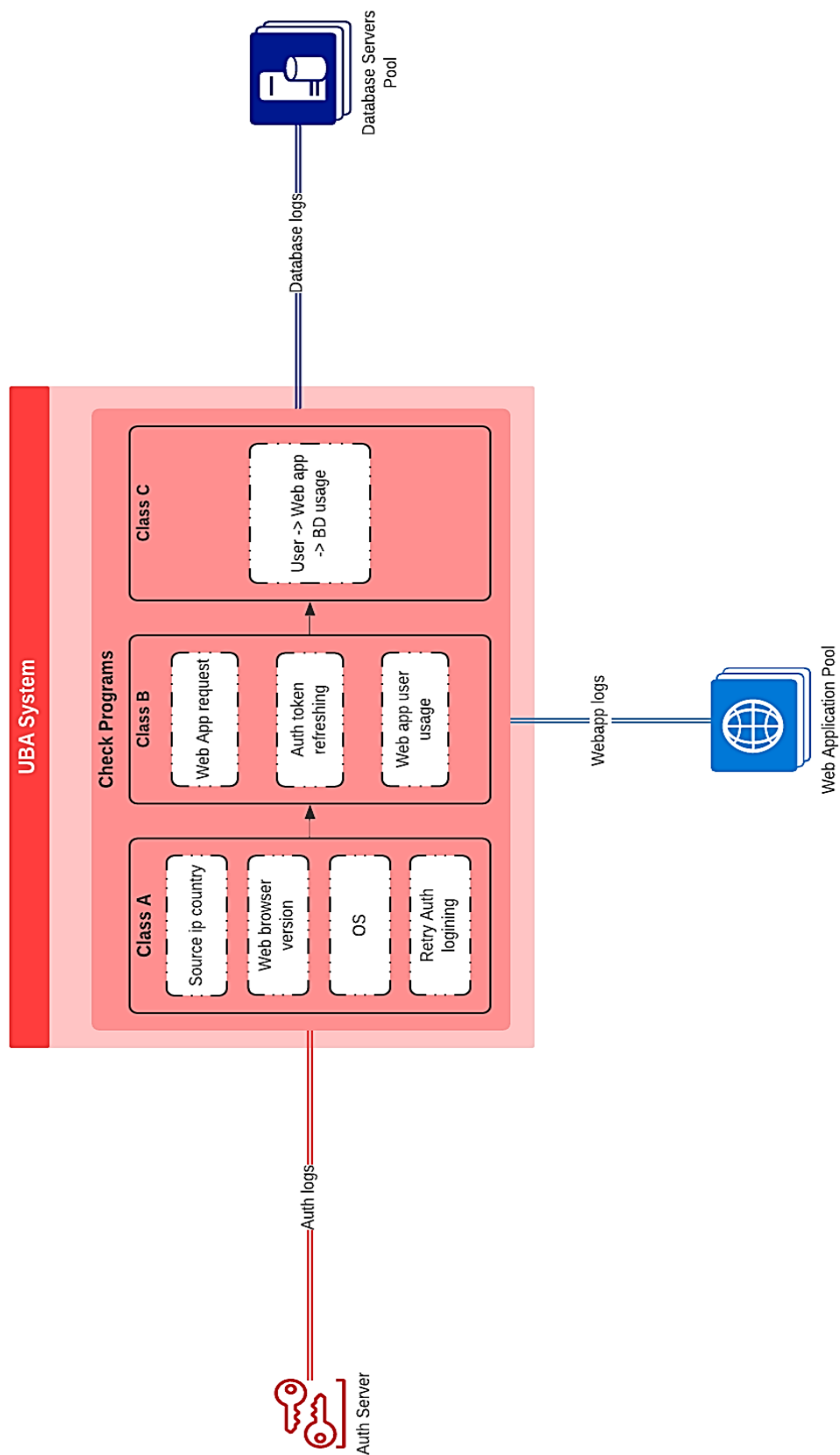


Рисунок 7.3 — UBA System Logic

Задачи, решаемые UBA системы КД к вузовским ВС.

1. Внутренние угрозы. В случае, если пользователь или группа пользователей совершают деструктивные действия — кражу персональных данных или служебной информации, авторизовавшись в системе, UBA может обнаружить утечку данных, злоупотребление привилегиями, совершенное персоналом.

2. Скомпрометированные учетные записи. Если пользователь незлоумышленно установил вредоносное ПО на свою рабочую станцию или его аккаунт был подделан, система UBA способна выявить утекшие учетные записи прежде, чем злоумышленники нанесут реальный ущерб.

3. Атаки методом перебора. Иногда злоумышленники нацеливаются на облачные сервисы университета, а также на сторонние системы с аутентификацией пользователей. С помощью системы UBA можно обнаружить попытки перебора и в дальнейшем заблокировать доступ к атакуемым объектам.

4. Модификация политик доступа и создание суперпользователей. Система UBA выдаст предупреждение при обнаружении повышения привилегий.

5. Замена пользователя в ходе авторизованного сеанса. Например, пользователь ввел пароль, успешно прошел авторизацию, а его сеансом может воспользоваться кто-то другой. Сюда же относится передача логинов/паролей легитимных пользователей другим лицам, например для сдачи онлайн-тестов.

Место системы UBA в архитектуре защищенного вычислительного комплекса системы высшего образования представлено на рис. 7.4.

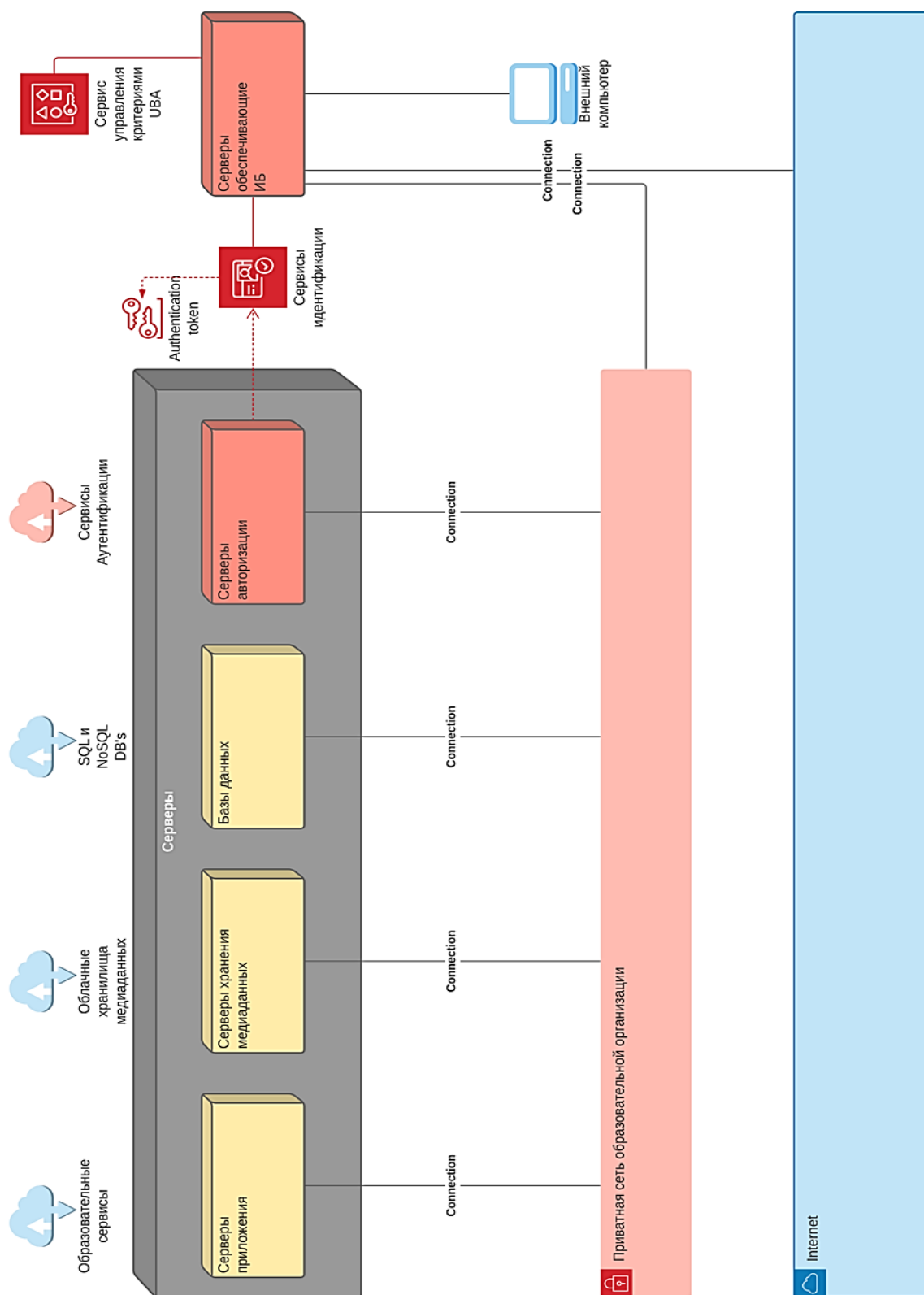


Рисунок 7.4 — Архитектура защищенного вычислительного комплекса с использованием UBA

7.3. Система сетевого анализа трафика на основе поведения пользователей

При доступе к ВС вуза пользователи оставляют множество следов в виде паттернов поведения (используемые устройства и браузеры, IP-адреса, посещаемые страницы, характеристики ввода текста с клавиатуры и движений мыши), что позволяет составить картину поведения каждого пользователя и в случае отклонения от типичного поведения вводить дополнительные проверки.

Такой механизм особенно актуален в формате дистанционного обучения, поскольку занятия и контрольные мероприятия в заочном формате лишены физического уровня защиты, что повышает возможности для списывания, подлога, а также саботажа учебной работы. Проверка «почерка» студентов позволит снизить вероятность таких нарушений.

Предлагаемый сетевой анализатор (кластер) предназначен для перехвата HTTP-трафика и автономного анализа поступающих запросов, отправляемых браузерами студентов при взаимодействии с интерфейсами тестирующей информационной системы. Программные компоненты низкого уровня полагаются на функциональность `mitmproxy` [245] для захвата трафика, предназначенного для веб-сервера тестирующей системы. Все функции Linux для простоты обозначены как компонент `LinuxKernel` на представленных UML-диаграммах.

Диаграмма классов на рис. 7.5 иллюстрирует анатомию компонентов анализа поведения студентов.

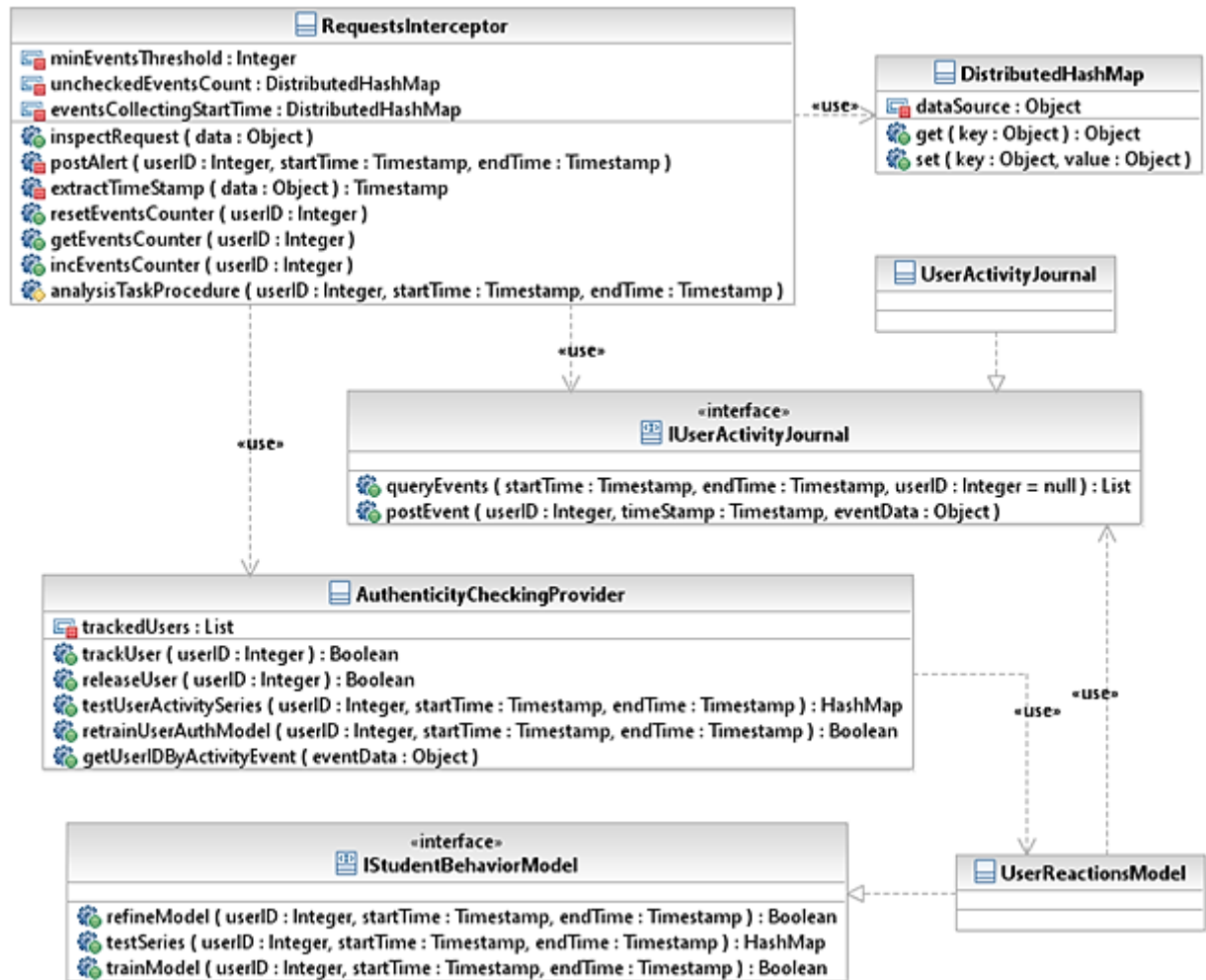


Рисунок 7.5 — Диаграмма классов анализатора поведения студентов

1. Класс `RequestsInterceptor` (табл. 7.1) предназначен для анализа запросов HTTP и запуска проверки содержимого. Это основной класс, взаимодействующий с `mitmproxy`.

2. Класс `DistributedHashMap` предоставляет функциональность распределенного отказоустойчивого ассоциативного массива, разделяемого экземплярами `RequestsInterceptor`, функционирующими в кластерной среде. Информация о счетчиках количества событий (`uncheckedEventsCount`) и отметках начала их сбора (`eventsCollectingStartTime`) должна быть доступна каждому экземпляру `RequestsInterceptor`, и операции обновления должны быть атомарными.

Таблица 7.1 — Класс `RequestsInterceptor`

<code>minEventsThreshold</code>	Минимальный порог количества новых событий, ассоциированных с пользователем, при достижении которого начинается анализ поведения
<code>eventsCollectingStartTime</code>	Ассоциативный массив. Сопоставляет идентификатор пользователя с отметкой времени, когда для него начался сбор новых событий
<code>uncheckedEventsCount</code>	Ассоциативный массив. Сопоставляет идентификатор пользователя с количеством непроверенных событий, собранных с момента начала сбора новых событий (см. <code>eventsCollectingStartTime</code>)
<code>extractTimestamp</code>	Извлекает отметку времени из заголовков HTTP
<code>incEventsCounter</code>	Увеличивает счетчик новых событий активности пользователя в <code>uncheckedEventsCount</code> для пользователя с идентификатором <code>userID</code>
<code>resetEventsCounter</code>	Сбрасывает счетчик новых событий активности пользователя с идентификатором <code>userID</code> на ноль. Устанавливает для него время начала сбора событий на текущее время (см. <code>eventsCollectingStartTime</code>)
<code>getEventsCounter</code>	Возвращает значение счетчика новых событий активности пользователя с идентификатором <code>userID</code>
<code>postAlert</code>	Публикует оповещение для указанного интервала времени активности пользователя с идентификатором <code>userID</code>
<code>analysisTaskProcedure</code>	1. Запускает анализ новых событий для пользователя с идентификатором <code>userID</code>. 2. В случае появления подозрений, публикует оповещения (см. <code>postAlert</code>)
<code>inspectRequest</code>	Если данные являются действительным HTTP-запросом с действием пользователя, определяется идентификатор пользователя из запроса, и для отслеживаемого пользователя выполняется следующие: 1. Извлекается временная метка из запроса. 2. Размещаются данные о событии в журнале активности пользователей. 3. Увеличивается счетчик новых событий для определенного пользователя (см. <code>incEventsCounter</code>). Если он достигает <code>minEventsThreshold</code>, асинхронно запускается процедура анализа <code>analysisTaskProcedure</code>, а затем сбрасывается счетчик событий для определенного пользователя на ноль (см. <code>ResetEventsCounter</code>)

3. Класс `UserActivityJournal` предназначен для управления журналом пользовательской активности и предоставления данных аналитическим компонентам.

4. `IUserActivityJournal` (табл. 7.2) — интерфейс для работы с журналом пользовательской активности.

Таблица 7.2 — Класс `IUserActivityJournal`

<code>queryEvents</code>	Запросить события из журнала за указанный интервал времени для пользователя с указанным идентификатором
<code>postEvent</code>	Записать данные о событии в журнал с указанием отметки времени и идентификатора пользователя

5. Класс `AuthenticityCheckingProvider` (табл. 7.3) предназначен для управления конфигурацией и обеспечения функции проверки соответствия для компонента анализа поведения пользователей (`AccessAnalyzer`).

Таблица 7.3 — Класс `AuthenticityCheckingProvider`

<code>trackedUsers</code>	Список идентификаторов отслеживаемых пользователей
<code>trackUser</code>	Добавить пользователя с идентификатором <code>userID</code> в список отслеживания. Истина возвращается, если соответствующий плагин модели поведения доступен и запись еще не добавлена
<code>releaseUser</code>	Больше не отслеживать пользователя с идентификатором <code>userID</code> . Истина возвращается, если запись существует в списке отслеживания
<code>testUserActivitySeries</code>	Возвращает ассоциативный массив с отметками времени событий в качестве ключей и оценкой их подлинности в виде логических значений

Таблица 7.3 — Окончание

retrainUserAuthModel	Переобучить модель машинного обучения для указанного пользователя с заданным интервалом данных для обучения
getUserIDByActivityEvent	Возвращает идентификатор пользователя по событию его активности

6. `IStudentBehaviorModel` (табл. 7.4) — это общий интерфейс, который должен реализовывать любой плагин проверки поведения активности студента.

Таблица 7.4 — `IStudentBehaviorModel`

trainModel	Обучить модель машинного обучения для пользователя с идентификатором <code>userID</code> с указанным интервалом данных для обучения. Модель сохраняется для использования в методах <code>testSeries</code> и <code>refineModel</code>
testSeries	Возвращает ассоциативный массив с отметками времени событий в качестве ключей и их оценкой в виде логических значений. Истина — достоверно. Ложь — незаконно. Применяется модель машинного обучения, подготовленная ранее с помощью <code>trainModel</code> для пользователя с идентификатором <code>userID</code> , ряды данных определяются активностью этого пользователя
refineModel	Уточнить модель поведения для пользователя с идентификатором <code>userID</code> с помощью данных его активности, заданных временным интервалом

7. `UserReactionsModel` — это плагин проверки поведения студента, реализующий интерфейс `IStudentBehaviorModel`.

Все классы, кроме классов проверки поведения студентов (`UserReactionsModel`), реализованы в компоненте `AccessAnalyzer`. Классы проверки поведения студентов реализованы в отдельных компонентах. Диаграмма компонентов на рис. 7.6 иллюстрирует взаимосвязь компонентов в системе и другого программного обеспечения, с которым она работа-

ет, например, тестирующего сервера, предоставляющего функциональность дистанционного обучения студентов.

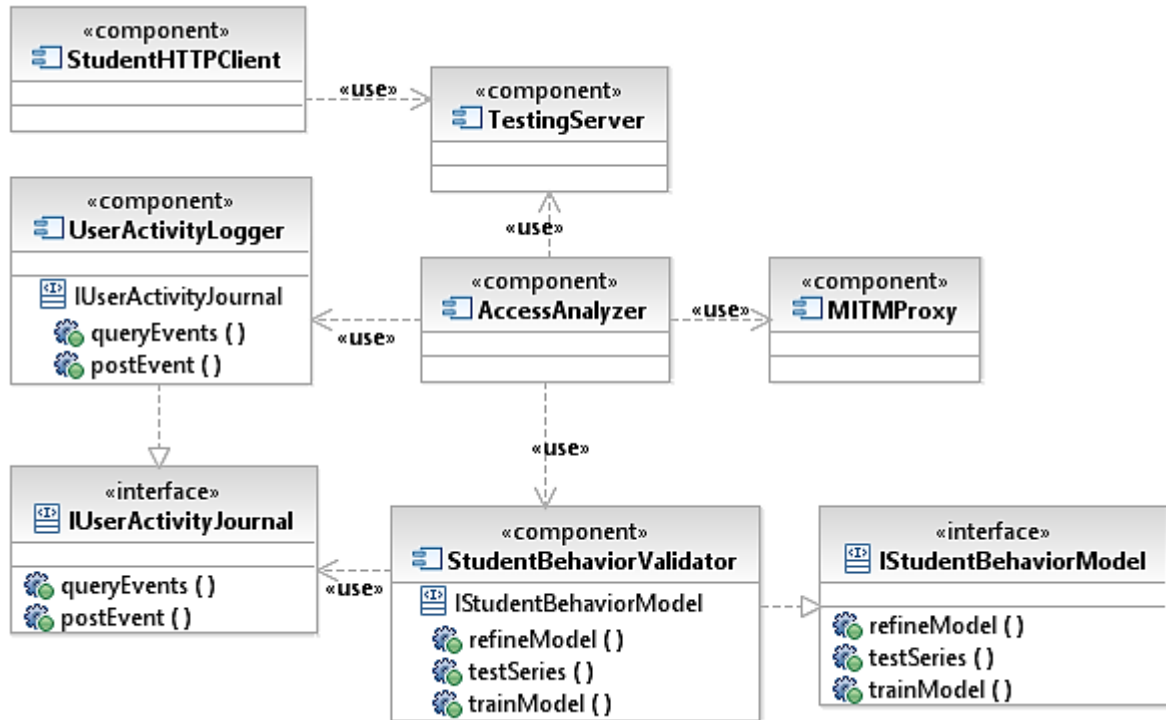


Рисунок 7.6 — Диаграмма компонентов анализатора поведения студентов

Источником событий для последнего являются различные клиентские устройства студентов с веб-браузером.

7.4. Описание тестового стенда с многоуровневым контролем доступа

Для размещения предлагаемых серверных ролей выбрана лезвийная система Supermicro 938-16, содержащая 8 лезвий в едином шасси. Характеристики оборудования приведены в табл. 7.5 и 7.6.

Таблица 7.5 — Характеристики вычислительного оборудования

Компонент лезвия	Характеристики компонента
Процессор	Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz. 10 ядер, 20 потоков.
Оперативная память	DDR3 1600MHz, 16Gb
Сетевой адаптер Ethernet	2 адаптера Intel Corporation I350 Gigabit Network Connection (rev 01)
Сетевой адаптер InfiniBand	Mellanox Technologies MT25408A0-FCC-QI ConnectX, Dual Port 40Gb/s
Дисковые накопители	2 накопителя HDD по 4TB: Seagate Desktop HDD.15 ST4000DM000-1F2168

Таблица 7.6 — Характеристики сетевого оборудования

Компонент сети	Характеристики компонента
Ethernet Switch	D-Link Gigabit Ethernet Switch
InfiniBand Switch	Mellanox InfiniBand QDR Switch

Сети Ethernet и InfiniBand функционируют без конфигурации VLAN. На вычислительных лезвиях функционирует драйвер IP over IB. На каждом лезвии задействован только один порт Ethernet и InfiniBand.

Все лезвия функционируют под управлением операционной системы CentOS 7 x64. Дисковые накопители объединены в программном RAID1. Уровень виртуализации сконфигурирован с помощью qemu-kvm [237]. Описание виртуальных машин, развертываемых на вычислительных лезвиях, приведено в табл. 7.7. Все они функционируют под управлением ОС Centos 7x64.

Таблица 7.7 — Характеристики виртуальных машин

Имя ВМ	Серверная роль ВМ	Компоненты ПО	Характеристики ВМ
websrv	Web Server	Moodle MySQL PHP nginx	10 ядер, 15Гб ОЗУ, 2Тб пространства HDD
journal0	Journal Backend (primary)	rsyslog	4 ядра, 4Гб ОЗУ, 2Тб пространства HDD
journal1	Journal Backend (secondary)	rsyslog	4 ядра, 4Гб ОЗУ, 2Тб пространства HDD
front	HTTP Interceptor Frontend	mitmproxy	8 ядер, 8Гб ОЗУ, 4Гб пространства HDD
back0	Behavior Analysis Backend	redis AccessAnalyzer StudentBehaviorValidator	10 ядер, 15Гб ОЗУ, 2Тб пространства HDD
back1	Behavior Analysis Backend	redis AccessAnalyzer StudentBehaviorValidator	10 ядер, 15Гб ОЗУ, 2Тб пространства HDD
back2	Behavior Analysis Backend	redis AccessAnalyzer StudentBehaviorValidator	10 ядер, 15Гб ОЗУ, 2Тб пространства HDD
back3	Behavior Analysis Backend	redis AccessAnalyzer StudentBehaviorValidator	10 ядер, 15Гб ОЗУ, 2Тб пространства HDD

Любая из виртуальных машин может быть развернута на любом из лезвий, если оно располагает достаточным количеством ресурсов на момент развертывания. На рис. 7.7 проиллюстрирована возможная схема развертывания на восьми лезвиях.

Веб-сервер websrv развернут как необходимый для работы аналитического кластера защищаемый компонент. Отказоустойчивость компонента журнала обеспечивается наличием первичного и вторичного экземпляров rsyslog [236, 246, 247].

Конфигурация такова, что при отказе первичного экземпляра данные направляются на вторичный. При возвращении первичного экземпляра, он вновь начинает принимать данные. Отказоустойчивость кластера Behavior Analysis Backend обеспечивается за счет множественности экземпляров аналитических компонентов AccessAnalyzer и StudentBehaviorValidator, а также распределенного отказоустойчивого хранилища redis, реализующего хранение распределенных структур данных.

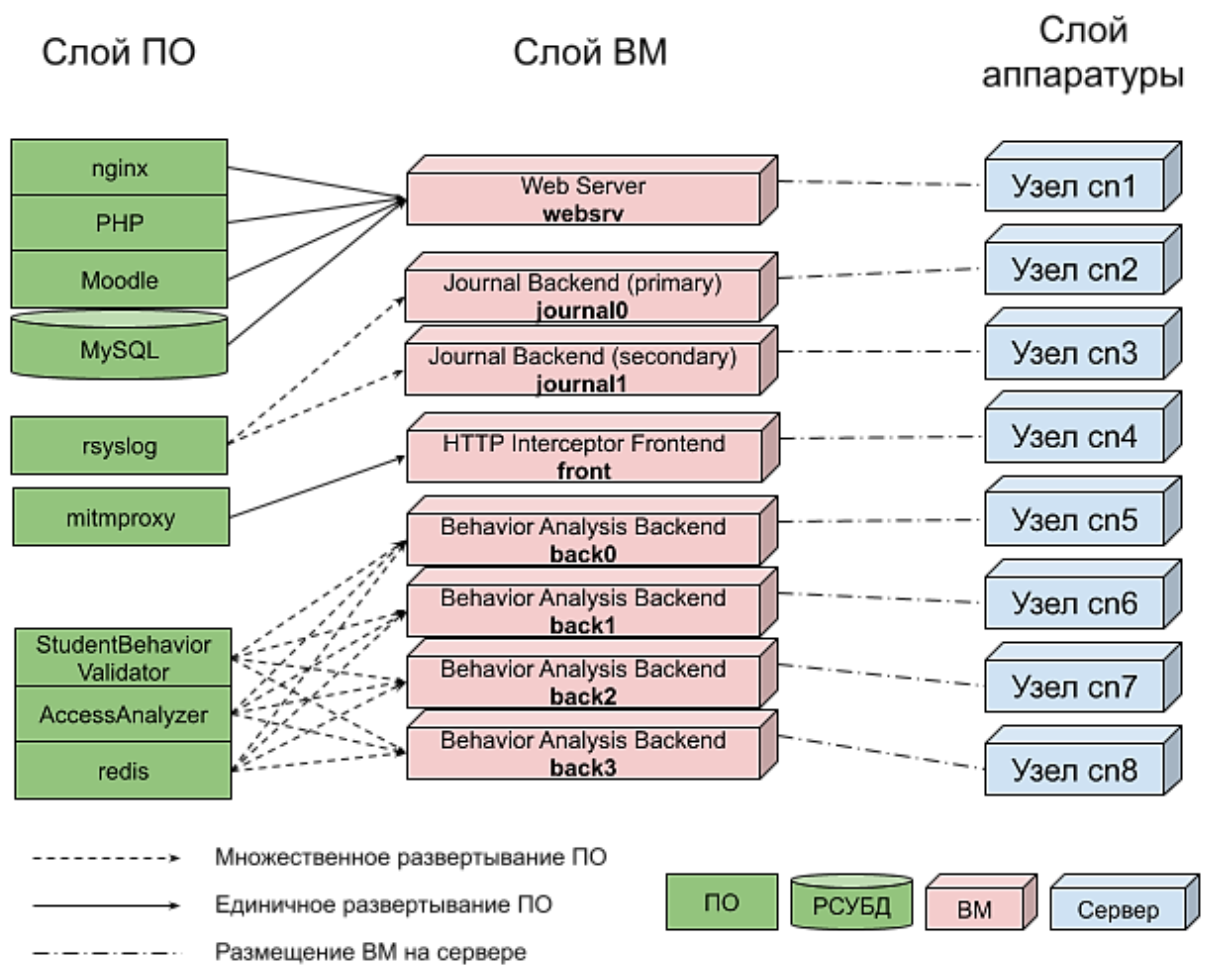


Рисунок 7.7 — Размещение виртуальных машин и программного обеспечения

Экспериментальные исследования системы проводилось под следующей нагрузкой: на вход машины front подавались HTTP-запросы для Moodle со случайным интервалом длительностью от 0 до 100 мс (ГСЧ работает согласно равномерному распределению). Общее количество запросов равно 1200. Используются два типа запросов:

1. «Легковесный», требующий меньшего количества вычислительных ресурсов для обработки, и индуцирующий передачу данных по сети в обоих направлениях до 1 Мбит. Примером такого запроса является выставление оценки за студенческую работу.

2. «Тяжеловесный», требующий большего количества вычислительных ресурсов для обработки, и индуцирующий передачу данных по сети в исходящем направлении до 15 Мбит. Передача данных по сети во входящем направлении нужна только для передачи запроса и не превышает 1 Мбит. Примером такого запроса является открытие журнала оценок для потоков, включающих множество групп студентов.

На 9 «легковесных» запросов приходится 1 «тяжеловесный».

Общее время работы системы для обслуживания всех принятых запросов составило 61 с.

На рис. 7.8 приведены графики потребления ресурсов каждой ВМ.

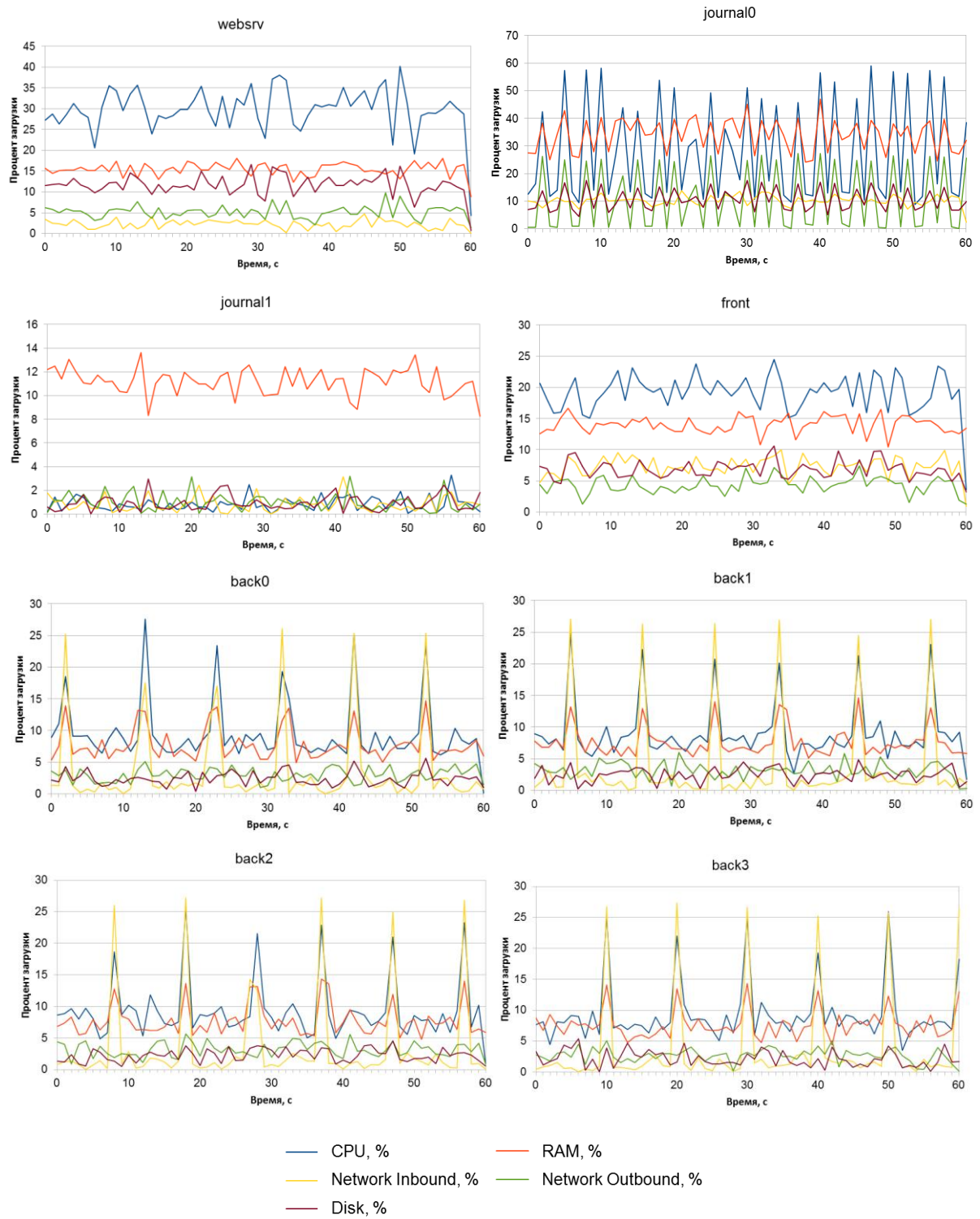


Рисунок 7.8 — Потребление ресурсов виртуальными машинами

Экспериментальное тестирование показало следующее.

Наличие асимметричной нагрузки на сетевой интерфейс машины `websrv` из-за наличия «тяжеловесных» запросов, ответы на которые нагружают исходящий канал.

Машина `front` значительно более нагружена по процессору, чем по остальным ресурсам. Это объясняется тем, что на проксирование трафика HTTP затрачивается в заметном объеме процессорное время сервисом `mitmproxy`, в то время как HTTP запросы и ответы на них не столь велики, чтоб утилизировать сетевой канал даже на 10%.

Заметим, что нагрузка на ее входящий канал включает как запросы, адресованные `websrv`, так и ответы на них, исходящие от `websrv`, что обусловлено выполняемым на машине `front` проксированием HTTP-трафика. Принятый HTTP-запрос направляется также на аналитические машины `Behavior Analysis Backend` (см. диаграмму последовательности на рис. 7.12). На них производятся операции анализа пользовательского поведения (разр. в главе 5), но не при поступлении каждого отдельного запроса, а при накоплении 50 непроанализированных запросов, которые формируют статистику, доступную для анализа. При этом каждый поступающий запрос ведет к записи пользовательской активности в журнале на машине `journal0` (`journal1` пребывает в резерве и не нагружена). Всплески активности на машине `journal0` обусловлены запуском аналитических процедур на машинах `back0`, ..., `back3`, которые производят чтение непроанализированных событий пользовательской активности из журнала. Входящий сетевой канал имеет более равномерную нагрузку, чем исходящий, поскольку обслуживает однородные запросы на запись событий, а не обслуживает массивные, но более редкие, запросы на чтение. Работа аналитических процедур на машинах `back0`, ..., `back3` заметна по пикам нагрузки на процессор, память и входящий сетевой канал. Количество пиков активности журнала соответствует общему количеству пиков активности на аналитических

машинах, поскольку нагрузка на них балансируется по алгоритму round-robin. График на рис. 7.9 показывает загрузку процессоров аналитических машин.

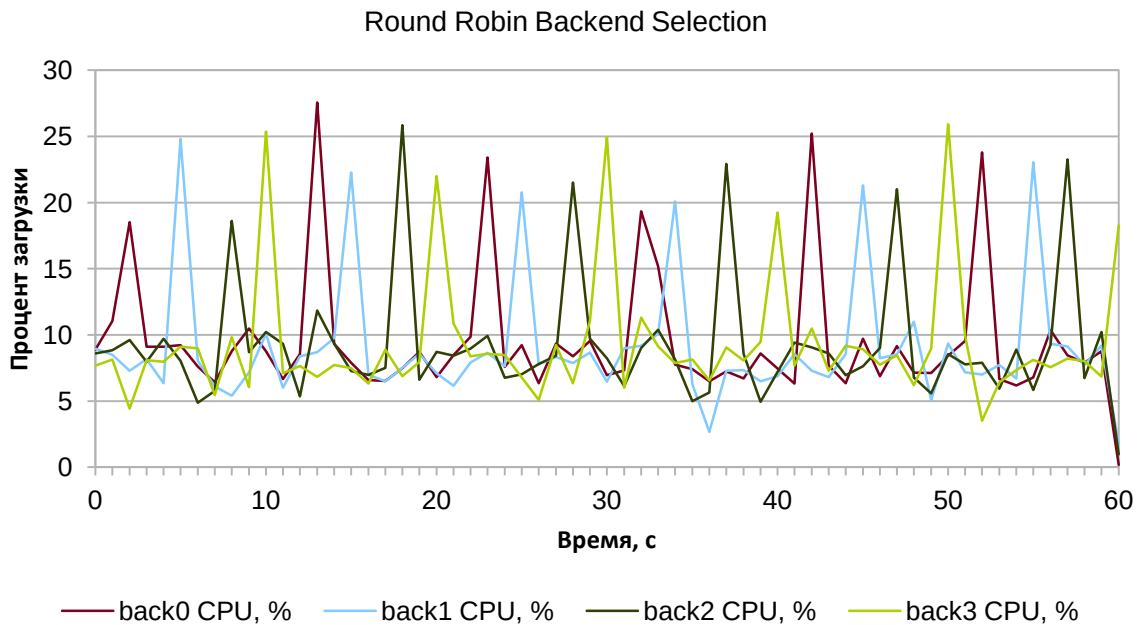


Рисунок 7.9 — Потребление ресурсов процессора аналитическими ВМ

В табл. 7.8 приведена средняя загрузка ресурсов на всех восьми виртуальных машинах.

Таблица 7.8 — Средняя загрузка ресурсов на виртуальных машинах

ВМ	Средняя загрузка CPU, %	Средняя загрузка RAM, %	Средняя загрузка сети, входящий канал, %	Средняя загрузка сети, исходящий канал, %	Средняя загрузка диска, %
websrv	29,83	15,43	2,25	5,18	11,62
journal0	28,03	33,95	10,22	10,56	10,53
journal1	0,86	11,19	0,85	1,00	0,94
front	19,15	14,03	7,30	4,34	6,86
back0	9,50	7,80	3,59	3,03	2,41
back1	9,04	7,58	3,66	3,16	2,46
back2	9,24	7,71	3,50	3,16	2,23
back3	9,34	7,68	3,63	2,69	2,14

Исходя из данных, приведенных в табл. 7.4, можно заключить, что тестовый аналитический кластер может быть оптимизирован путем уменьшения объема оперативной памяти, выдаваемой виртуальным машинам. Нагрузку на процессоры можно оценить как среднюю, запас для обработки всплесков количества запросов остается. Однако при добавлении новых аналитических плагинов в будущем, потребность в ресурсах ВМ требуется оценить заново с использованием экспериментальных имитационных стендов.

На рис. 7.10 проиллюстрировано место сетевого анализатора (кластера Traffic Analyzer) в типичной сетевой инфраструктуре образовательного учреждения.

Новые серверные роли HTTP Interceptor Frontend, Behavior Analysis Backend, Journal Backend вместе с существующим Web Server формируют кластер Servers Cluster, для которого целесообразно выделение отдельного VLAN. Трафик, который ранее направлялся на Web Server, должен быть направлен на HTTP Interceptor Frontend. После прохождения через Behavior Analysis Backend он будет направлен на Web Server автоматически — это его поведение по умолчанию. Последний аспект регулируется отдельной опцией, чтобы дать возможность альтернативного развертывания аналитического кластера: трафик, направляющийся непосредственно на Web Server, может быть продублирован на HTTP Interceptor Frontend с помощью зеркалирования портов на управляемом коммутаторе. В этом случае направление пакетов от Behavior Analysis Backend к Web Server было бы избыточно, а потому должно быть отключено.

Правила маршрутизации трафика, в том числе и между VLAN, должны быть разработаны с учетом специфики расположения рабочих мест сотрудников и не должны быть чрезмерно пермиссивными в целях уменьшения поверхности сетевой атаки.

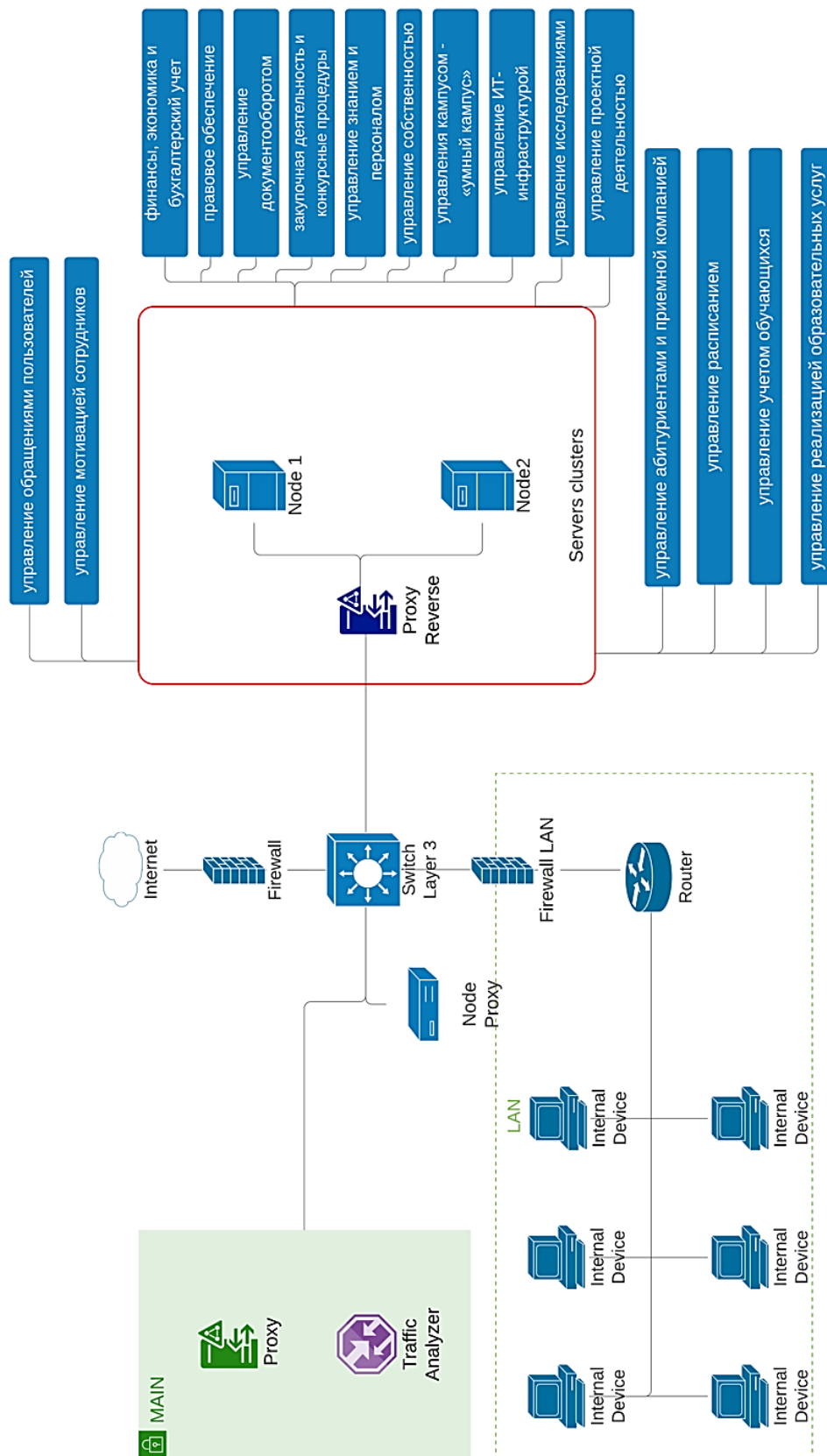


Рисунок 7.10 — Сетевая инфраструктура с анализом трафика

Веб-сервер вместе с предложенными компонентами его защиты формируют централизованную систему, предназначенную для развертывания в рамках локальной вычислительной сети образовательного учреждения. Базы данных, необходимые для функционирования защищаемых компонентов (БД веб-приложений), а также журнал пользовательской активности (JournalBackend) не могут быть вынесены за пределы периметра ЛВС, поскольку требуют соединения с низкими временными задержками. Они содержат все данные, приходящие в образовательное учреждение и генерируемые в нем, и являющиеся предметом интереса настоящей работы. Информационная система образовательного учреждения имеет децентрализованную подсистему аналитического кластера для обеспечения горизонтальной масштабируемости и улучшения отказоустойчивости.

Первичный запуск системных функций требует участия системного администратора. Данные активности пользователей будут подвергаться анализу только в том случае, если для соответствующего пользователя включено отслеживание в системе. При этом ассоциированные модели машинного обучения должны быть инициализированы на обучающей выборке регулярных легальных данных, задаваемой временным интервалом (класс `AuthenticityCheckingProvider`). После этого поведение системы сводится к непрерывному автоматическому анализу входящих потоков больших данных и выдаче предупреждений в случае обнаружения нежелательной активности — опасных пользовательских действий.

`AccessAnalyzer`, `StudentBehaviorValidator` должны быть упакованы как отдельные артефакты (с соответствующими именами, рис. 7.11). Все они должны быть развернуты на узле `BehaviorAnalysisBackend`. Эти узлы должны быть кластеризованы для обеспечения высокой доступности. Входящий трафик, предназначенный для сервера тестирования, просматривается на узле `HTTPInterceptorFrontend` и направляется для анализа на узлы `BehaviorAnalysisBackend` с балансировкой по алгоритму `round-robin`. Функ-

функциональность журнала пользовательской активности может быть предоставлена компонентом rsyslog [236], который развертывается на отдельном узле JournalBackend. Функциональность распределенного ассоциативного массива может быть предоставлена компонентом redis [200], который развертывается на BehaviorAnalysisBackend вместе с AccessAnalyzer. Сервер тестирования, предоставляющий функциональность дистанционного обучения, должен быть развернут на отдельном узле WebServer.

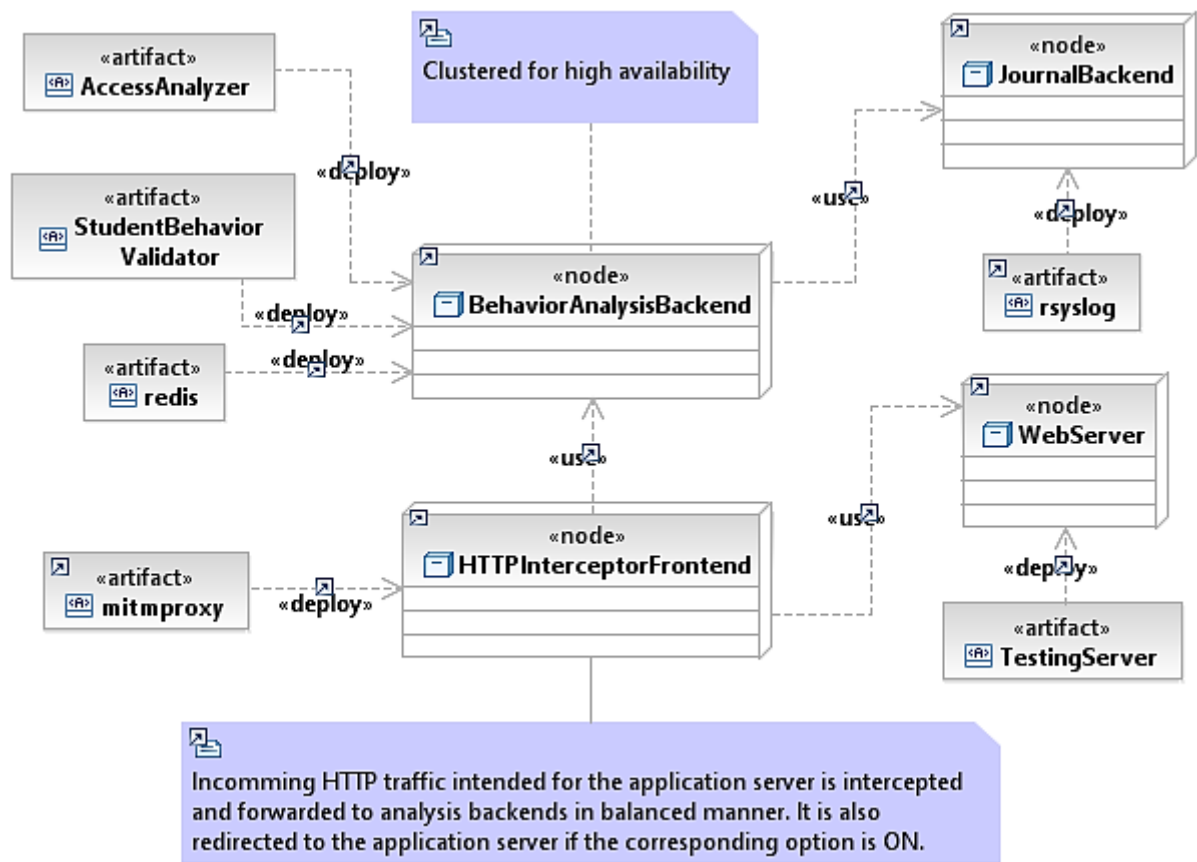


Рисунок 7.11 — Диаграмма развертывания анализатора поведения студентов

Разработана методика учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру вычислительных комплексов образовательных услуг, которую можно представить в виде диаграммы последовательностей (см. рис. 7.12). Диаграмма иллюстрирует процесс

проверки и анализа пакетов HTTP в системе на аналитическом кластере. Предполагается, что модели поведения студентов уже обучены. Могут быть проанализированы только действительные запросы HTTP, несущие данные активности студента.

Когда пакет прибывает в прокси mitmproxу на узле HTTPInterceptorFrontend, он перенаправляется для анализа на один из узлов BehaviorAnalysisBackend, где проверяется компонентом AccessAnalyzer. Если проверяемый пакет является допустимым запросом HTTP, ассоциированным с активностью студента, происходит следующее: выясняется идентификатор пользователя, и в случае, если пользователь отслеживается, то из запроса извлекается значение временной метки события, последнее затем регистрируется в журнале, и инкрементируется счетчик новых входящих событий для определенного пользователя.

Если достигнут минимальный порог количества новых входящих событий, процедура их анализа запускается асинхронно. Ей передается временной интервал сбора событий (начало извлекается из eventsCollectingStartTime, конец — это временная отметка последнего входящего события).

Начинается анализ на предмет подлинности пользовательской активности с помощью UserReactionsModel, сбрасывается счетчик новых входящих событий до нуля, и фиксируется текущее время как новая отметка начала регистрации событий для определенного пользователя. При возникновении подозрений вызывается метод postAlert, который может нести требуемую функциональность оповещения об опасностях и дополнительного журналирования событий.

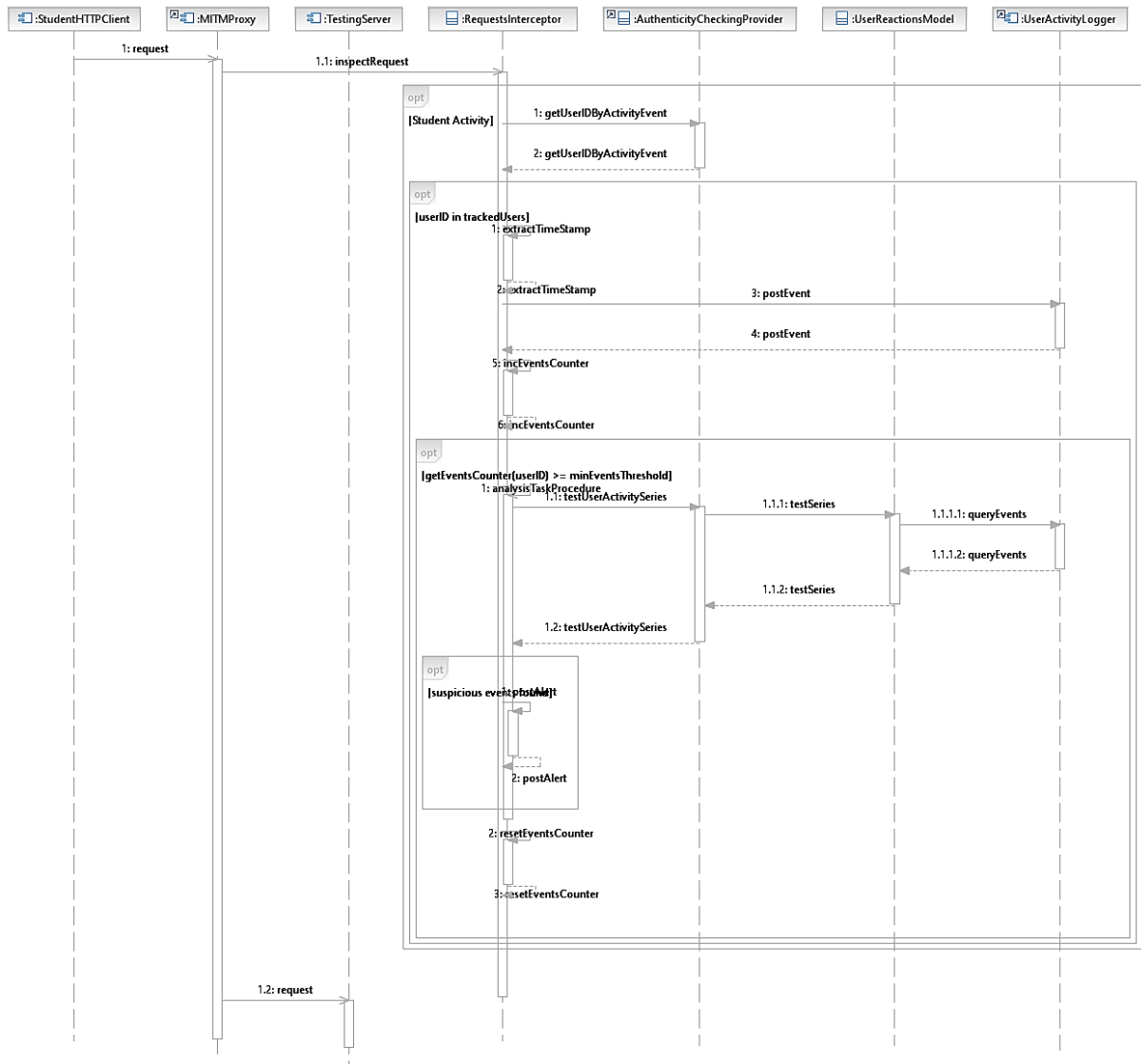


Рисунок 7.12 — Анализ поведения студентов

Таким образом, ВС вуза являются цифровой средой, обеспечивающей взаимодействие студентов и сотрудников университета в учебном процессе. Современная система образования тесно связана с внедрением новейших информационных технологий и формированием научно-образовательной среды.

Совокупность ВС, составляющих цифровую среду вуза, создает коммуникативную среду, базирующуюся на современных решениях в сфере ИТ, автоматизируя решение важнейших задач университета. Комплексная безопасность на уровне информационных ресурсов обеспечивается

сервисами, реализующими единую точку входа (SSO — Single Sign-On) в интегрированную научно-образовательную среду.

На рис. 7.13 представлена рекомендуемая архитектура сервисов образования.

Внедрение SSO, с одной стороны, сокращает некоторые риски (какой-либо из 20 разных паролей потерять проще, чем 1), но при этом создаёт единую точку отказа: DDoS-атака или взлом SSO может привести к неработоспособности или компрометации многих систем.

Развитие существующей ИТ-инфраструктуры вуза осуществляется путем решения ряда задач:

- создание конвергентной телекоммуникационной среды;
- построение центров для управления сетевой инфраструктурой, разработка ВС и ЦП, формирующих ядро ИТ-инфраструктуры;
- развитие электронной библиотеки;
- создание универсально-технических центров дистанционного образования, применяющих технологию UBA для анализа корректности пользовательского поведения.

Разработаны *принципы и информационные модели проектирования архитектуры системы КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза* в условиях защищенной цифровой образовательной среды с использованием инструментов UBA. Использование разработанных методов моделей КД способствует повышению защищенности образовательных ресурсов от несанкционированного доступа, возможности для списывания, подлога, а также саботажа учебной работы. Проверка индивидуальных особенностей студентов позволяет снизить вероятность таких нарушений.

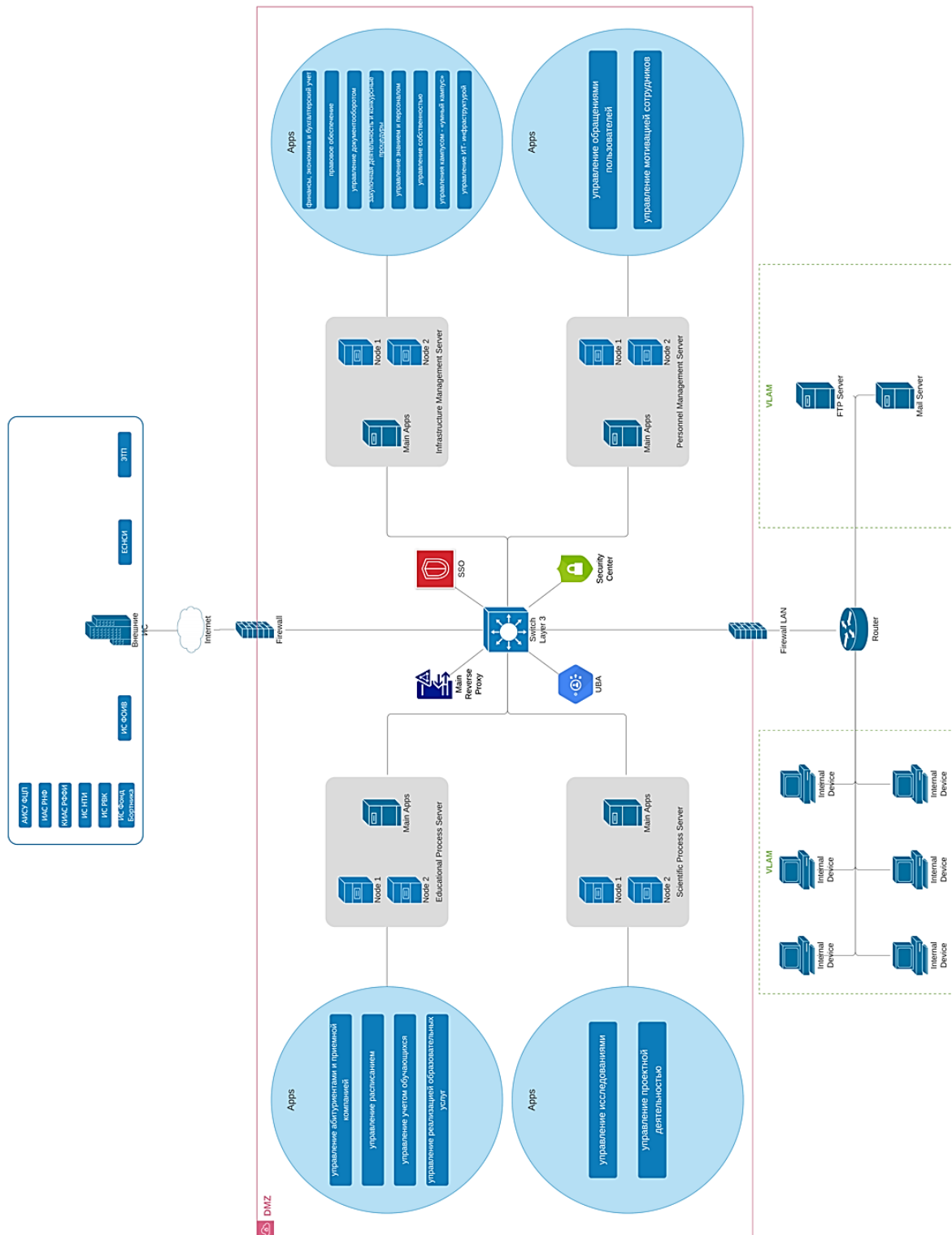


Рисунок 7.13 — Архитектура вычислительных сервисов в вузе

Результаты внедрения в РТУ МИРЭА показывают эффективность предложенных решений.

Выводы по главе

Предложенная архитектура аналитических кластеров предназначена для улучшения функциональности сервисов образования. Она разработана специально, чтобы обеспечить интеграцию проверки поведения пользователей в процессе их взаимодействия с СДО в рамках дистанционного обучения.

Практический эффект разработки и внедрения программного обеспечения заключается в обеспечении подлинности пользователей, объективности оценивания, а также защищенности профессиональной репутации специалистов в частности и учреждения в целом.

Поскольку нет никаких требований к плагинам, за исключением реализации одного общего интерфейса, который должен обеспечивать управление моделью корректности, отсутствуют технические сложности при реализации модельно-ориентированных подходов для проверки данных, что позволяет программистам расширять систему с помощью новых анализаторов, когда появляются новые эффективные методы.

Программная реализация предложенных архитектурных принципов может лечь в основу фреймворка, предназначенного для сбора и анализа данных пользовательского поведения на предмет их подлинности. Наличие подобного инструментария позволит исследователям, работающим в указанном направлении, упростить задачи сбора данных и проведения экспериментов при отладке моделей машинного обучения.

Предложена архитектура системы, готовой к обработке больших данных при автономной проверке корректности пользовательского поведения.

Условие отказоустойчивости — это наличие кластеризованных экземпляров компонентов StudentBehaviorValidator и AccessAnalyzer, развернутых на разных физических машинах с наличием или отсутствием уровня виртуализации или контейнеризации. Аналитические плагины должны развертываться с такой же избыточностью. Перспективным направлением развития аналитических компонентов является использование современных подходов по распаралеливанию программ и инструментов для обработки больших данных [248], а также методов искусственного интеллекта [249].

ЗАКЛЮЧЕНИЕ

Разработаны принципы, методы и модели построения четырехуровневой масштабируемой архитектуры контроля доступа, обеспечивающей реализацию технологий передачи, хранения, управления, мониторинга и анализа действий пользователей и устройств в вычислительных комплексах, предоставляющих веб-сервисы с учетом оценки ресурсной эффективности систем КД и технико-экономических характеристик заданных условий функционирования.

В ходе выполнения исследований получены следующие основные результаты.

1. Проведен обзор подходов к построению архитектур и используемых технологий обеспечения контроля доступа к вычислительным сервисам, позволивший выделить актуальные задачи, перспективные подходы к их решению, определить направление исследований с целью повышения эффективности контроля доступа к ВС.

2. Сформулирована задача построения архитектуры КД как подсистемы, обеспечивающей собственные, отличные от ВС: сбор, передачу, хранение и обработку данных о действиях пользователей. Решение позволяет сформулировать задачи, являющиеся типовыми для обеспечения информационной безопасности; определить состав и требуемые ресурсы для компонентов анализа данных КД.

3. Разработана четырехуровневая масштабируемая архитектура контроля доступа, интегрируемая в вычислительные комплексы, обеспечивающие взаимодействие пользователей с ВС через компьютерные сети. Архитектура позволяет оценивать эффективность, разрабатывать и внедрять разные варианты технологических решений КД: SIEM, UBA.

4. Разработана методика построения облачной инфраструктуры, обеспечивающей решение задач КД. Приведены примеры построения для SIEM и UBA со специализированным протоколом DICOM.

5. Разработан метод анализа затрат вычислительных ресурсов на основе подхода, использующего имитационные виртуальные стенды в условиях заданных технико-экономических характеристик эксплуатации. Метод и соответствующая модель позволяют решать задачу выбора технических реализаций.

6. Предложен метод КД на основе анализа психологических реакций пользователя при взаимодействии с элементами интерфейса с учетом времени ответа на контрольные вопросы. Проведенные экспериментальные исследования на большой выборке позволили подтвердить достоверность измеряемых данных и получить нормированные значения для трех вопросов об уровне образования.

7. Разработаны методики учета прикладных аспектов внедрения многоуровневого контроля доступа в архитектуру специализированных вычислительных комплексов в учреждения здравоохранения и вузы. Предложена архитектура программных средств, реализующих SIEM и UBA решения.

8. Разработаны принципы и информационные модели проектирования архитектуры КД для разграниченного доступа к образовательным вычислительным ресурсам и сервисам вуза с учетом инструментов UBA.

9. Результаты внедрены в учреждения образования и учреждения здравоохранения. Полученные результаты внедрения свидетельствуют об эффективности научных и практических результатов диссертации.

ЛИТЕРАТУРА

1. *Gil-Garcia J. R., Flores-Zúñiga M. Á.* Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors // *Government Information Quarterly*. 2020. Vol. 37. No. 4. P. 101518.
2. *Lewinter K. E., Hudson S. M., Kysh L., Lara M., Betz C. L., Espinoza J.* Reconsidering reviews: the role of scoping reviews in digital medicine and pediatrics // *NPJ Digital Medicine* 2020. Vol. 3. No. 1. P. 1–4.
3. *Li F., Lu H., Hou M., Cui K., Darbandi M.* Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality // *Technology in Society*. 2021. Vol. 64. No. 5. P. 101487.
4. *Emejulu A., McGregor C.* Towards a radical digital citizenship in digital education // *Critical Studies in Education*. 2019. Vol. 60. No. 1. P. 131–147.
5. *Elia G., Margherita A., Passiante G.* Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process // *Technological Forecasting and Social Change*. 2020. Vol. 150. P. 119791.
6. *Силкина Г. Ю., Шевченко С. Ю.* Инновационные процессы в цифровой экономике. Информационно-коммуникационные драйверы: монография. — СПб. : ФГАОУ ВО СПбПУ, 2017. — 262 с.
7. *Зацаринный А. А., Киселев Э. В., Козлов С. В., Колин К. К.* Информационное пространство цифровой экономики России. Концептуальные основы и проблемы формирования. — М. : ООО «НИПКЦ Восход-А», 2018.

8. Rasool A., Shah F. A., Islam J. U. Customer engagement in the digital age: a review and research agenda // *Current Opinion in Psychology*. 2020. Vol. 36. P. 96–100.

9. De Hert P., Papakonstantinou V., Malgieri G., Beslay L., Sanchez I. The right to data portability in the GDPR: Towards user-centric interoperability of digital services // *Computer law & security review*. 2018. Vol. 34. No. 2. P. 193–203.

10. Стырин Е. М., Дмитриева Н. Е., Синятуллина Л. Х. Государственные цифровые платформы: от концепта к реализации // *Вопросы государственного и муниципального управления*. 2019. №. 4. С. 31–60.

11. Магомедов Ш. Г. Архитектура вычислительного комплекса для веб-сервисов и порталов с многоуровневым контролем доступа по общедоступным сетям // *International Journal of Open Information Technologies*. 2021. Vol. 9. № 3. С. 36–43.

12. Nikulchev E., Ilin D., Silaeva A., Kolyasnikov P., Belov V., Runtov A., Pushkin P., Laptev N., Alexeenko A., Magomedov S., Kosenkov A., Zakharov I., Ismatullina V., Malykh S. Digital psychological platform for mass web-surveys // *Data*. 2020. Vol. 5. No. 4. P. 95.

13. Magomedov S., Gusev A., Ilin D., Nikulchev E. Used the time of user reactions to improve security and control access to web services // *Applied Science*. 2021. Vol. 11. No. 5. P. 2561.

14. Cai F., He J., Ali Zardari Z., Han S. Distributed management of permission for access control model // *Journal of Intelligent & Fuzzy Systems*. 2020. Vol. 38. No. 2. P. 1539–1548.

15. Yarmand M. H., Sartipi K., Down D. G. Behavior-based access control for distributed healthcare systems // *Journal of Computer Security*. 2013. Vol. 21. No. 1. P. 1–39.

16. Гузев О. Ю., Чижов И. В. Масштабируемая архитектура комплексов обеспечения сетевой безопасности // *Современные информационные технологии и ИТ-образование*. 2019. Т. 15. № 1. С. 154–163.

17. Elshoush H. T., Osman I. M. Alert correlation in collaborative intelligent intrusion detection systems — a survey // *Applied Soft Computing*. 2011. P. 4349–4365.

18. Magomedov S., Pavelyev S., Ivanova I., Dobrotvorsky A., Khrestina M., Yusubaliev T. Anomaly detection with machine learning and graph databases in fraud management // *International Journal of Advanced Computer Science and Applications*. 2018. Vol. 9. No. 11. P. 33–38.

19. Magomedov S. G., Dobrotvorsky A. S., Khrestina M. P., Pavelyev S. A., Yusubaliev T. R. Application of artificial intelligence technologies for the monitoring of transactions in aml-systems using the example of the developed classification algorithm // *International Journal of Engineering and Technology (UAE)*. 2018. Vol. 7. No. 4.36. P. 76–79.

20. Xi X., Zhang T., Ye W., Wen Z., Zhang S., Du D., Gao Q. An ensemble approach for detecting anomalous user behaviors // *International Journal of Software Engineering and Knowledge Engineering*. 2018. Vol. 28. P. 1637–1656.

21. Lee J., Kim J., Kim I., Han K. Cyber threat detection based on artificial neural networks using event profiles // *IEEE Access*. 2019. Vol. 7. P. 165607–165626.

22. Csaba K., Péter H. B. Analysis of cyberattack patterns by user behavior analytics // *AARMS – Academic and Applied Research in Military Science*. 2018. Vol. 17. No. 3. P. 101–114.

23. Kufel L. Security event monitoring in a distributed systems environment // *IEEE Secur. Priv.* 2013. Vol. 11. Iss. 1. P. 36–43.

24. Дрозд А. Обзор SIEM-систем на мировом и российском рынке. [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market
25. Лаврова Д. С. Методологическое и математическое обеспечение для SIEM-систем в интернете вещей: дисс. ... канд. техн. наук: 05.13.19. — СПб., 2016.
26. Security QRadar SIEM. [Электронный ресурс]. URL: http://www.siem.su/docs/ibm/IBM_Security_QRadar.pdf
27. Sekharan S. S., Kandasamy K. Profiling SIEM tools and correlation engines for security analytics. In *Proceedings of 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 2017, pp. 717–721.
28. Symantec Security Information Manager (SSIM). [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Symantec_Security_Information_Manager
29. El Arass M., Souissi N. Smart SIEM: From big data logs and events to smart data alerts // *Int. J. Innov. Technol. Explor. Eng.* 2019. Vol. 8. Iss. 8. P. 3186–3191.
30. Coppolino L. et al. Enhancing SIEM technology to protect critical infrastructures. In *Proceedings of the International Workshop on Critical Information Infrastructures Security*, 2013, pp. 10–21.
31. Miloslavskaya N., Tolstoy A. IoT Block SIEM for information security incident management in the internet of things ecosystem // *Cluster Computing*. 2020. Vol. 23. P. 1911–1925.

32. Kotenko I. V., Polubelova O. V., Saenko I. B. The ontological approach for SIEM Data repository implementation. In *Proceedings of IEEE Intern. Conf. on Green Computing and Communications*. 2012, pp. 761–766.
33. Al-Duwairi B., Al-Kahla W., AlRefai M.A., Abdelqader Y., Rawash A., Fahmawi R. SIEM-based detection and mitigation of IoT-botnet DDoS attacks // *Int. J. Electr. Comput. Eng.* 2020. Vol. 10. No. 2. P. 2182–2191.
34. Moukafih N., Orhanou G., El Hajji S. Neural network-based voting system with high capacity and low computation for intrusion detection in SIEM/IDS systems // *Security and Communication Networks*. 2020. P. 3512737.
35. Sancho J. C., Caro A., Ávila M., Bravo A. New approach for threat classification and security risk estimations based on security event management // *Future Generation Computer Systems*. 2020. Vol. 113. P. 488–505.
36. Hasan M., Sugla B., Viswanathan R. A conceptual framework for network management event correlation and filtering systems. In *Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Network Management*. 1999, pp. 233–246.
37. Bryant B. D., Saiedian H. A novel kill-chain framework for remote security log analysis with SIEM software // *Computers & security*. 2017. Vol. 67. P. 198–210.
38. Schefer-Wenzl S., Strembeck M. Modelling context-aware RBAC models for mobile business processes // *International Journal of Wireless and Mobile Computing*. 2013. Vol. 6. No. 5. P. 448–462.
39. Corapi D., Ray O., Russo A., Bandara A., Lupu E. Learning rules from user behaviour. In *Proceedings of the IFIP International Conference on Artificial Intelligence Applications and Innovations*. Springer, Boston, MA, 2009, April, pp. 459–468.

40. Walker A., Svacina J., Simmons J., Cerny T. On automated role-based access control assessment in enterprise systems. In *Information Science and Applications*. — Springer, Singapore, 2020, pp. 375–385.

41. Nyame G., Qin Z. Precursors of role-based access control design in KMS: A conceptual framework // *Information*. 2020. Vol. 11. No. 6. P. 334.

42. Trnka M., Cerný T. On security level usage in context-aware role-based access control. In *Proceedings of the SAC, Symposium on Applied Computing*. Pisa, Italy, 4–8 April 2016, pp. 1192–1195.

43. Bertino E., Bonatti P.A., Ferrari E. TRBAC: A temporal role-based access control model // *ACM Transactions on Information and System Security (TISSEC)*. 2001. Vol. 4. No. 3. P. 191–233.

44. Kayes A. S. M., Kalaria R., Sarker I. H., Islam M., et al. A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues // *Sensors*. 2020. Vol. 20. No. 9. P. 2464.

45. Qiu J., Tian Z., Du C., Zuo Q., Su S., Fang B. A survey on access control in the age of internet of things // *IEEE Internet of Things Journal*. 2020. Vol. 7. No. 6. P. 4682–4696.

46. Kayes A. S. M., Rahayu W., Dillon T., Chang E., Han J. Context-aware access control with imprecise context characterization for cloud-based data resources // *Future Generation Computer Systems*. 2019. Vol. 93. No. 7. P. 237–255.

47. Akutota, T. Choudhury S. Big data security challenges: An overview and application of user behavior analytics // *International Research Journal of Engineering and Technology*. 2017. Vol. 4. No. 10. P. 1544–1548.

48. Монахова М. М., Шерунтаев Д. А., Марков И. С., Мазурок Д. В. Модель поведения пользователя корпоративной сети передачи данных // Сборник статей Девятой всероссийской научно-практической конферен-

ции по имитационному моделированию и его применению в науке и промышленности. — Екатеринбург, 2019. С. 603–608.

49. *Bosnjak M., Tuten, T. L., Wittmann W. W.* Unit (non) response in web-based access panel surveys: An extended planned-behavior approach // *Psychology & Marketing*. 2005. Vol. 22. No. 6. P. 489–505.

50. *Lee J., Kim J., Kim I., Han K.* Cyber threat detection based on artificial neural networks using event profiles // *IEEE Access*. 2019. Vol. 7. P. 165607–16562.

51. *Anrijs S., Ponnet K., De Marez L.* Development and psychometric properties of the Digital Difficulties Scale (DDS): An instrument to measure who is disadvantaged to fulfill basic needs by experiencing difficulties in using a smartphone or computer // *PloS One*. 2020. Vol. 15. No. 5. P. e0233891.

52. *Трутнев Д. Р.* Архитектуры информационных систем. Основы проектирования: учебное пособие. — СПб. : НИУ ИТМО, 2012. — 66 с.

53. *Забегалин Е. В.* Концептуальная схема организации процессной автоматизации больших военных организаций // *Системы управления, связи и безопасности*. 2020. № 4. С. 1–43.

54. *Дрожжинов В., Штрик А.* Стандартизация архитектуры государственных ведомств США // *PC Week/RE*. 2005. № 28. С. 27–28.

55. IEEE 1471-2000. IEEE Recommended Practice for Architectural Description for Software-Intensive Systems.

56. IEEE Recommended Practice for Architectural Description, Draft 3.0 of IEEE P1471, May 1998.

57. *Zachman A.* A framework for Information Systems Architecture // *IBM Systems Journal*. 1999. Vol. 38. No. 2. P. 454–470.

58. Данилин А., Слюсаренко А. Архитектура и стратегия. «Инь» и «Янь» информационных технологий предприятия: монография. — М. : Интернет-Университет Информационных технологий, 2005.

59. Зиндер Е. З. Архитектура предприятия в контексте бизнес-реинжиниринга. Ч. 2 // *Intelligent Enterprise*. 2008. № 7. [Электронный ресурс]. URL: <http://www.iemag.ru/analytics/detail.php?ID=18024>

60. Zachman J. A., Sowa J. Extending and formalizing the framework for information systems architecture // *IBM Systems Journal*. 1992. Vol. 31. No. 3. P. 590.

61. ГОСТ 34.320-96 Информационные технологии (ИТ). Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. Введен в действие Постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 22 февраля 2001 г. № 87-ст.

62. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Утвержден и введен в действие Постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 27.12.90 № 3399.

63. The Zachman Framework Evolution. [Электронный ресурс]. URL: <https://www.brcommunity.com/articles.php?id=b811>

64. ISO-15704, Industrial automation systems – Requirements for enterprise-reference architectures and methodologies. URL: <https://www.iso.org/standard/28777.html>

65. COBIT 2019 Framework: Introduction and Methodology. [Электронный ресурс]. URL: <https://community.mis.temple.edu/>

mis5203sec001sp2019/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

66. *Krafzig D., Banke K., Slama D.* Enterprise SOA: Service-Oriented Architecture Best Practices. — Prentice Hall PTR, 2004. — 408 p.

67. OMG Unified Modeling Language (UML) Specification, March 2003 Version 1.5. [Электронный ресурс]. URL: <https://www.omg.org/spec/UML/1.5/PDF>

68. About the Unified Modeling Language Specification Version 2.5.1. [Электронный ресурс]. URL: <https://www.omg.org/spec/UML/About-UML/>

69. FEA Consolidated Reference Model Document, May 2005. [Электронный ресурс]. URL: <http://xml.coverpages.org/OMB-FEA-ConsolidatedRefModel200505.pdf>

70. Federal Enterprise Architecture Framework Version 2. [Электронный ресурс]. URL: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

71. *Linthicum D. S.* Enterprise Application Integration. — Addison-Wesley Professional. 2000.

72. ISO 19439:2006 Enterprise integration — Framework for enterprise modelling. [Электронный ресурс]. URL: <https://www.iso.org/standard/33833.html>

73. ISO 35.100. Open systems interconnection. [Электронный ресурс]. <https://www.iso.org/ics/35.100/x/>

74. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Утвержден и введен в действие Постановлением Государственного комитета СССР по стандартам от 24.03.89 № 661.

75. ГОСТ 34.601-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Утвержден и введен в действие Постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 29.12.90 N 3469.

76. Rational Unified Process Best Practices for Software Development Teams Microsoft Word — TP026B.doc. [Электронный ресурс]. URL: <https://www.ibm.com/ru-ru>

77. The Open Group Architecture Framework TOGAF. [Электронный ресурс]. URL: <https://www.opengroup.org/togaf>

78. Путилов А. В., Харитонов В. В., Гусева А. И. и др. Цифровые платформы управления жизненным циклом комплексных систем: монография. — М. : Научный консультант, 2018.

79. Миронова Л. Цифровая страна: государство как платформа: Россия в новой цифровой реальности. — [Saarbrücken]: Lambert acad. publ. (LAP), cop. 2019. — 190 с.

80. Логинов Е. Л., Шкута А. А. Внедрение цифровых платформ для управления сложными техно-организационными системами топливно-энергетического комплекса России. От цифровой энергетики — к цифровой экономике: монография. — М. : ИПР РАН, 2018.

81. Чен П. П. Ш. Модель «сущность — связь» — шаг к единому представлению данных // Журнал «Системы управления базами данных». 1995. № 3.

82. ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011. Национальный стандарт Российской Федерации. Системная и программная инженерия. Описание архитектуры. Systems and software engineering. Architecture description. Утвержден и введен в действие Приказом Федерального

агентства по техническому регулированию и метрологии от 22 сентября 2016 г. N 1190-ст.

83. Грекул В. И., Денищенко Г. Н., Коровкина Н. Л. Проектирование информационных систем. — М.: Интернет-университет информационных технологий, 2005.

84. Горбачев В. А. Вопросы проектирования информационных технологий при создании электронной информационно-образовательной среды СПбГЛТУ // Сборник статей конференции «Информационные системы и технологии: теория и практика». — СПб., 2018. С. 30–39.

85. Анисифоров А. Б., Дубгорн А. С. Научные принципы развития архитектуры информационных систем и их реализация в управлении организационно-экономическими преобразованиями на предприятии // *Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент»*. 2019. № 4. С. 31–40.

86. Turner M. Microsoft® solutions framework essentials: building successful technology solutions. — Microsoft Press, 2006.

87. Marrone M., Kolbe L. M. ITIL and the creation of benefits: An empirical study on benefits, challenges and processes. In *Proceedings of the 18th European Conference on Information Systems*. 2010, p. 66.

88. Microsoft Operations Framework 4.0. [Электронный ресурс]. URL: [https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc506049\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc506049(v=technet.10))

89. Kruegel C., Valeur F., Vigna G. Intrusion detection and correlation. Challenges and solutions. — Springer, 2004. — 118 p.

90. Ghorbani A. A., Lu W., Tavallae M. Network intrusion detection and prevention. — Springer, 2010. — 224 p.

91. Приказ ФСТЭК от 21.12.2017. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». (<https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossiiot-21-dekabrya-2017-g-n-236>)

92. Приказ ФСТЭК от 25.12.2017. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (<https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossiiot-25-dekabrya-2017-g-n-239>)

93. Магомедов Ш. Г., Кашкин Е. В., Муравьев В. В., Назаренко М. А., Новиков А. С., Горобец А. И., Миськов Д. В. База данных системы управления закупками и проектами для построения контрольных карт Шухарта индивидуальных значений по 30 измерениям с целью определения наличия особых точек за пределами границ статистической управляемости (150 вариантов) // Свидетельство о государственной регистрации базы данных RU 2019620701. 29.04.2019.

94. Ning P., Xu D. Correlation Analysis of Intrusion Alerts. *Intrusion Detection Systems. Ser.: Advances in Information Security*. Springer, 2008. Vol. 38. P. 65–92.

95. Zurutuza U., Uribeetxeberria R. Intrusion Detection Alarm Correlation: A Survey // *In Proceedings of IADAT Intern. Conf. on Telecommunications and Computer Networks*. 2004, pp. 1–3.

96. IEEE 1003.23-1998 — IEEE Guide for Developing User Open System Environment (OSE) Profiles. [Электронный ресурс]. URL: https://standards.ieee.org/standard/1003_23-1998.html

97. Рекомендации по стандартизации. Информационные технологии. Руководство по проектированию профилей среды открытой системы (СОС) организации-пользователя. Приняты и введены в действие Постановлением Госстандарта России от 14 ноября 2002 г. № 415-ст.

98. Магомедов Ш. Г. Формирование состава типовых макроопераций для систем разграничения и контроля доступа // *Информация и безопасность*. 2018. Т. 21. № 1. С. 118–123.

99. Лось В. П., Тышук Е. Д., Магомедов Ш. Г. Место контроля доступа в системах обеспечения информационной безопасности объектов обработки данных // *Информация и безопасность*. 2017. Т. 20. № 3. С. 356–361.

100. Магомедов Ш. Г. Оценка степени влияния сопутствующих факторов на показатели информационной безопасности // *Российский технологический журнал*. 2017. Т. 5. № 2. С. 47–56.

101. Kotenko I. V., Chechulin A. A. A Cyber Attack Modeling and Impact Assessment Framework. In *Proceedings of the 5th Intern. Conf. on Cyber Conflict 2013 (CyCon 2013)*. 2013, pp. 119–142.

102. Sadoddin R., Ghorbani A. Alert correlation survey: framework and techniques. In *Proceedings of the 2006 Intern. Conf. on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (PST'06)*. 2006. Art. no. 37.

103. Hanemann A., Marcu P. Algorithm Design and Application of Service-Oriented Event Correlation. In *Proceedings of the 2008 3rd IEEE/IFIP International Workshop on Business-driven IT Management*. 2008, pp. 61–70.

104. Limmer T., Dressler F. Survey of event correlation techniques for attack detection in early warning systems: tech report. — University of Erlangen, Dept. of Computer Science 7, 2008. — 37 p.

105. *Müller A.* Event correlation engine: master's thesis. — Eidgenössische Technische Hochschule Zürich. 2009.
106. *Fossi M., Egan G., Haley et al.* Symantec internet security threat report trends for 2010. 2011. Volume 16. [Электронный ресурс]. URL: http://book.itep.ru/depository/trends/Symantec_April_2011_threat_report.pdf
107. Risk Fabric. A predictive security analytics platform. [Электронный ресурс]. URL: <https://www.qualys.com/docs/bay-dynamics-qualys-integration-datasheet.pdf>
108. B2B platform for IT buyers, vendors and suppliers. [Электронный ресурс]. URL: <https://roi4cio.com/en/>
109. *Şora I., Popovici D. T.* Automatic extraction of behavioral models from distributed systems and services. In *Proceedings of International Conference on Evaluation of Novel Approaches to Software Engineering*. Springer, Berlin, Heidelberg, 2013. pp. 190–202.
110. *Salitin M. A., Zolait A. H.* The role of user entity behavior analytics to detect network attacks in real time. In *Proceedings of the 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. 2018, pp. 1–5.
111. Positive Technologies. [Электронный ресурс]. URL: <https://www.ptsecurity.com/ru-ru/about/news/top-5-tekhnologicheskikh-trendov-razvitiya-siem-sistem-v-blizhayshie-tri-goda/>
112. *Coppolino L. et al.* Cloud security: Emerging threats and current solutions // *Computers & Electrical Engineering*. 2017. Vol. 59. P. 126–140.
113. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (<http://kremlin.ru/acts/bank/24154>)
114. *Карнов О. Е., Акаткин Ю. М., Коняевский В. А., Шишканов Д. В., Ясиновская Е. Д.* Цифровое здравоохранение в цифровом обществе

стве. Экосистема и кластер: монография. — М. : Издательство «ДПК Пресс», 2017. — 220 с.

115. *Королюк И. П.* Медицинская информатика: учебник. — 2 изд., перераб. и доп. — Самара : ООО «Офорт» : ГБОУ ВПО «СамГМУ», 2012. — 244 с.

116. *Гулиев Я. И., Цветков А. А.* Обеспечение информационной безопасности в медицинских организациях // *Врач и информационные технологии*. 2016. № 6. С. 49–62.

117. Procurement Guidelines for Cybersecurity in Hospitals. [Электронный ресурс]. URL: <https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services>

118. Cybersecurity Ventures. [Электронный ресурс]. URL: <https://about.crunchbase.com/cybersecurity-research-report-2021/>

119. HIMSS Cybersecurity Survey. [Электронный ресурс]. URL: https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf

120. 2020 Cybersecurity Survey. [Электронный ресурс]. URL: https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf

121. *Cao F., Huang H. K., Zhou X. Q.* Medical image security in a HIPAA mandated PACS environment // *Computerized medical imaging and graphics*. 2003. Vol. 27. No. 2–3. P. 185–196.

122. Health IT Security Journal. [Электронный ресурс]. URL: <http://healthitsecurity.org/>

123. *Улумбекова Г. Э. и др.* Финансирование здравоохранения в России (2021–2024 гг.). Факты и предложения // *ОРГЗДРАВ: Новости. Мнения. Обучение. Вестник ВШОУЗ*. 2019. № 4 (18). С. 4–19.

124. Gartner Magic Quadrant for Security Information and Event Management. [Электронный ресурс]. URL: <https://www.gartner.com/en/documents/3981040/magic-quadrant-for-security-information-and-event-manage>
125. Patient Insecurity: Explosion Of The Internet Of Medical Things. [Электронный ресурс]. URL: <https://cybersecurityventures.com/patient-insecurity-explosion-of-the-internet-of-medical-things/>
126. The authorities are investing 28 billion in Russia's cyber security, without daring to triple this amount. [Электронный ресурс]. URL: https://cnews.ru/news/top/2020-01-03_vlasti_vkladyvayut_v_kiberbezopasnost
127. Ransomware Goes Hollywood. [Электронный ресурс]. URL: <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/ransomware-goes-hollywood>
128. WannaCry cyber-attack cost the NHS £92m as 19,000 appointments cancelled. [Электронный ресурс]. URL: <https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/>
129. Health care's huge cybersecurity problem. [Электронный ресурс]. URL: <https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation>
130. Магомедов Ш. Г. Архитектура информационной системы для проверки подлинности медицинских данных в архиве DICOM // *International Journal of Open Information Technologies*. 2020. Т. 8. № 10. С. 84–89.
131. Магомедов Ш. Г. Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения // *Cloud of Science*. 2020. Т. 7. № 3. С. 685–704.

132. Паспорт приоритетного проекта «Совершенствование процессов организации медицинской помощи на основе внедрения информационных технологий» от 25.10.2016. (<http://static.government.ru/media/files/9ES7jBWMiMRqONdJYVLPTyoVKYwgr4Fk.pdf>)

133. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (<https://minzdrav.gov.ru/documents/7025>)

134. Беклемищева Н. Б., Жуков В. Г., Михайлов К. Д. О некоторых вопросах информационной безопасности медицинских устройств // *Актуальные проблемы авиации и космонавтики*. Т. 2. № 13. 2017. С. 191–193.

135. Бурков С. М., Косых Н. Э., Левкова Е. А., Савин С. З., Свиридов Н. М. Об одном методе декомпозиции для защиты персональных данных в медицинских информационных системах // *Врач и информационные технологии*. 2018. № 4. С. 59–66.

136. Рябко С. Д. Защита информационной инфраструктуры медицинского учреждения // *Здравоохранение*. 2012. № 7. С. 34–38.

137. Саттаров А. Б., Милославская Н. Г. Учебно-лабораторный комплекс по изучению атак типа «человек посередине» и способов защиты от них // *Безопасность информационных технологий*. 2018. Т. 25. № 4. С. 63–74.

138. Hewett A. J., et al. Conformance testing of DICOM image objects // *Proceedings of the Medical Imaging 1997: PACS Design and Evaluation: Engineering and Clinical Issues*. Vol. 3035. International Society for Optics and Photonics, 1997.

139. Open Source Clinical Image and Object Management. [Электронный ресурс]. URL: <https://www.dcm4che.org/>

140. Magomedov S., Lebedev A. Protected network architecture for ensuring consistency of 2 medical data through validation of user behavior and DICOM 3 archive integrity // *Applied Science*. 2021. Vol. 11. No. 5. P. 2072.
141. Coatrieux G., Montagner J., Huang H., Roux Ch. Mixed reversible and RONI watermarking for medical image reliability protection. In *Proceedings of the 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2007, pp. 5654–5657.
142. Abd-Eldayem M. M. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine // *Egyptian Informatics Journal*. 2013. Vol. 14. No. 1. P. 1–13.
143. Al-Haj A. Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images // *Journal of digital imaging*. 2015. Vol. 28. No. 2. P. 179–187.
144. Singla S., Singh J. Cloud data security using authentication and encryption technique // *Global Journal of Computer Science and Technology*. 2013. Vol. 13. Iss. 3.
145. Dorgham O., et al. Enhancing the security of exchanging and storing DICOM medical images on the cloud // *International Journal of Cloud Applications and Computing (IJCAC)*. 2018. Vol. 8. No. 1. P. 154–172.
146. Mirsky Y., Mahler T., Shelef I., Elovici Y. CT-GAN: Malicious tampering of 3D medical imagery using deep learning // In *Proceedings of the 28th {USENIX} Security Symposium {USENIX} Security* 19. 2019, pp. 461–478.
147. Digital imaging and communications in medicine (DICOM). [Электронный ресурс]. URL: <https://www.dicomstandard.org/>

148. *Cozzolino D., Thies J., Rössler A., Riess C., Nießner M., Verdoliva L.* Forensictransfer: Weakly-supervised domain adaptation for forgery detection. 2018. arXiv preprint arXiv:1812.02510.
149. IBM Technology Partners. [Электронный ресурс]. URL: <https://www.ibm.com/support/pages/technology-partners>
150. IBM QRadar User Behavior Analytics (UBA) app: User Guide. [Электронный ресурс]. URL: https://www.ibm.com/support/knowledgecenter/SS42VS_SHR/com.ibm.UBAapp.doc/b_Qapps_UBA.pdf
151. About USM Appliance. [Электронный ресурс]. URL: <https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-solution.htm>
152. USM Appliance. Develop New Plugins from Scratch. [Электронный ресурс]. URL: <https://cybersecurity.att.com/documentation/usm-appliance/plugin-management/developing-new-plugins.htm>
153. Configuring High Availability in USM Appliance Enterprise Systems. [Электронный ресурс]. URL: <https://cybersecurity.att.com/documentation/usm-appliance/configuring-ha/deploying-ha-in-usm-enterprise-prods.htm>
154. *Надеждин Е. Н., Цветков А. А.* Синтез программы мониторинга ресурсов вычислительной сети образовательной организации // *Интернет-журнал Науковедение*. 2014. № 5 (24). С. 66.
155. *Гродзенский С. Я., Попов Д. А.* Цикл Шухарта-Деминга и новейшие инструменты управления качеством // *Вестник МГТУ МИРЭА*. 2014. № 3. С. 230–234.
156. *Veeramachaneni K., Arnaldo I., Korrapati V., Bassias C., Li K.* AI²: training a big data machine to defend // *In Proceedings of the 2016 IEEE*

2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 49–54.

157. Magomedov S., Ilin D., Silaeva A., Nikulchev E. Dataset of user reactions when filling out web questionnaires // *Data*. 2020. Vol. 5. No. 4. P. 108.

158. Voit A., Stankus A., Magomedov S., Ivanova I. Big data processing for full-text search and visualization with elasticsearch // *International Journal of Advanced Computer Science and Applications*. 2017. Vol. 8. No. 12. P. 76–83.

159. Yarmand M. H., Sartipi K., Down D. G. Behavior-based access control for distributed healthcare systems // *Journal of Computer Security*. 2013. Vol. 21. No. 1. P. 1–39.

160. Tavallae M., Bagheri E., Lu W., Ghorbani A. A. A detailed analysis of the KDD CUP 99 data set // In *Proceedings of the 2009 IEEE symposium on computational intelligence for security and defense applications*, pp. 1–6.

161. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pp. 108–116.

162. Магомедов Ш.Г., Колясников П.В., Никульчев Е.В. Разработка технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок времени реакций пользователей // *Российский технологический журнал*. 2020. Т. 8. № 6. С. 34–46.

163. Ильин Д. Ю., Колясников П. В., Лантев Н. В., Магомедов Ш. Г., Алексеенко А. С., Никульчев Е. В. Архитектура вычислительного комплекса

цифровой платформы DigitalPsyTools междисциплинарных исследований в системе образования // *Cloud of Science*. 2020. Т. 7. № 4. С. 936–949.

164. Магомедов Ш. Г. Проектирование микропроцессорных устройств, разработанных для систем контроля и управления доступом // *Cloud of Science*. 2019. Т. 6. № 4. С. 752–761.

165. Магомедов Ш. Г., Шамхалов Ф. И. Особенности использования микропроцессорных устройств в системах контроля доступа // *Промышленные АСУ и контроллеры*. 2018. № 3. С. 16–19.

166. Магомедов Ш. Г. Классификация рубежей доступа и связанных с ними факторов влияния в системе контроля доступа // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2018. № 1. С. 62–70.

167. Лось В. П., Росс Г. В., Магомедов Ш. Г. Мультиагентный подход для защиты данных в информационном тумане // *Промышленные АСУ и контроллеры*. 2017. № 6. С. 47–50.

168. Магомедов Ш. Г. Построение системы обмена закрытыми данными в вычислительных сетях на основе использования систем счисления остаточных классов // *Промышленные АСУ и контроллеры*. 2017. № 1. С. 42–46.

169. Магомедов Ш. Г. Построение системы обмена закрытыми данными в вычислительных сетях на основе использования систем счисления остаточных классов // *Промышленные АСУ и контроллеры*. 2017. № 1. С. 42–46.

170. Магомедов Ш. Г., Шуршев В. Ф., Попов Г. А., Дорохов А. Ф., Руденко М. Ф. Построение моделей описания рисков охранных действий по защите внешних периметров организации // *Вестник Астраханского госу-*

дарственного технического университета. Серия: Управление, вычислительная техника и информатика. 2017. № 3. С. 31–39.

171. Медведев Н. В., Гришин Г. А. Модели управления доступом в распределенных информационных системах // *Наука и образование*. 2011. №. 1. С. 1.

172. Миронова В. Г., Шелупанов А. А., Югов Н. Т. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях // *Доклады Томского государственного университета систем управления и радиоэлектроники*. 2011. №. 2-3 (24). С. 206–210.

173. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие. – 2012.

174. Девянин П. Н., Леонова М. А. Приёмы описания модели управления доступом ОСCH Astra Linux Special Edition на формализованном языке метода Event-B для обеспечения её верификации инструментами Rodin и ProB // *Прикладная дискретная математика*. 2021. №. 52. С. 83–96.

175. Шаньгин В. Информационная безопасность. – Litres, 2022

176. Магомедов Ш. Г., Колотилов Ю. В. Системный анализ процесса разграничения доступа при дискреционной политике управления // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2017. № 4. С. 39–44.

177. Стандарт TCSEC [Электронный ресурс] URL: <http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt>

178. ISO/IEC 27001:2013 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — М., 2013
179. Крайнова Ю. Краткий курс: Международные стандарты аудита. — М., 2009.
180. Gusev A., Ilin D., Kolyasnikov P., Nikulchev E. Effective selection of software components based on experimental evaluations of quality of operation // *Engineering Letters*. 2020. Vol. 28. No. 2. P. 420–427.
181. Магомедов Ш. Г. Выбор оптимального варианта совершенствования системы защиты информации // *Промышленные АСУ и контроллеры*. 2017. № 3. С. 47–51.
182. Popov G., Magomedov S. Comparative analysis of various methods treatment expert assessments // *International Journal of Advanced Computer Science and Applications*. 2017. Vol. 8. No. 5. P. 35–39.
183. Магомедов Ш. Г. Математическое моделирование охранных действий на объекте защиты // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2016. № 1. С. 70–80.
184. Благодырев В. А., Хачумов В. М. Информационная защита вычислительных систем управления космическими аппаратами // *Авиакосмическое приборостроение*. 2012. № 8. С. 11–25.
185. Otsokov S.A., Magomedov S.G. Using of redundant signed-digit numeral system for accelerating and improving the accuracy of computer floating-point calculations. // *International Journal of Advanced Computer Science and Applications*. 2020. Vol. 11, No. 9. P. 357–363.

186. *Limmer T., Dressler F.* Survey of event correlation techniques for attack detection in early warning systems: tech report. — University of Erlangen, Dept. of Computer Science 7, 2008. — 37 p.
187. *Дойникова Е. В., Котенко И. В.* Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности // *Информационно-управляющие системы*. 2016. № 5. С. 54–65.
188. *Котенко И. В., Дойникова Е. В.* Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // *Информационно-управляющие системы*. 2015. № 3. С. 60–69.
189. *El Sibai R., Gemayel N., Bou Abdo J., Demerjian J.* A survey on access control mechanisms for cloud computing // *Transactions on Emerging Telecommunications Technologies*. 2020. Vol. 31. No. 2. P. e3720.
190. *Magomedov S. G., Los V. P.* Forming the composition of functions and instructions of microprocessor devices for access control systems // *Automatic Control and Computer Sciences*. 2019. Vol. 53. No. 8. P. 883–888.
191. *Magomedov S.G.* Increasing the efficiency of microprocessors in an access control systems // *International Journal of Engineering and Technology (UAE)*. 2018. V. 7, No. 4.36. P. 80–83.
192. *Magomedov S., Ilin D., Silaeva A., Nikulchev E.* Dataset of User Reactions When Filling Out Web Questionnaires // *Data*. 2020. Vol. 5. No. 4. P. 108.
193. *Voit A., Stankus A., Magomedov S., Ivanova I.* Big data processing for full-text search and visualization with elasticsearch // *International Journal of Advanced Computer Science and Applications*. 2017. Vol. 8. No. 12. P. 76–83.

194. *Исмаилов Ш. М. А., Магомедов Ш. Г.* Алгоритмы и структуры преобразования числовых данных из позиционной системы счисления в систему остаточных классов // *Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление.* 2008. № 5 (65). С. 159–169.
195. *Магомедов Ш. Г., Морозова Т. Ю., Акимов Д. А.* Обеспечение безопасности передачи данных в вычислительных сетях на основе использования систем остаточных классов // *Проблемы информационной безопасности. Компьютерные системы.* 2016. № 3. С. 43–47.
196. *Magomedov S.* Organization of Secured Data Transfer in Computers Using Sign-Value Notation // *ITM Web of Conference.* 2017. Vol. 10. P. 04004.
197. *Magomedov S.G.* The technology of secure dataprocessing in production systems based on the use of special microcontrollers // *International Journal of Engineering and Technology (UAE).* 2018. Vol. 7. No. 4.36. P. 84–87.
198. *Мустафаев А.Г., Магомедов Ш.Г., Савинова А.М., Мустафаев А.Г.* Управление технологическим процессом формирования структур интегральных элементов // *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика.* 2012. № 2. С. 56–61.
199. *Mijumbi R., Serrat J., Gorricho J. L., Latré S., Charalambides M., Lopez D.* Management and orchestration challenges in network functions virtualization // *IEEE Communications Magazine.* 2016. Vol. 54. No. 1. P. 98–105.
200. *Магомедов Ш.Г., Лебедев А.С.* Система автоматического распараллеливания линейных программ для машин с общей и распределенной памятью // *Российский технологический журнал.* 2019. Т. 7, № 5. С. 7–19.

201. Magomedov S. G., Lebedev A. S. Automatic parallelization of affine programs for distributed memory systems // *Communications in Computer and Information Science*. 2021. Vol 1396. P. 91–101.
202. Magomedov S. A system for off-line validation of medical data in DICOM archive // *Journal of Physics: Conference Series*. 2021. Vol. 1727. P. 012011.
203. Dehlinger J., Dixon J. Mobile application software engineering: Challenges and research directions. In *Proceedings of the Workshop on mobile software engineering*. 2011, October. Vol. 2, pp. 29–32.
204. Mikliaev E.M., Antonova I.I., Nikonov V.V., Magomedov S.G. An approach to emergency situation forecasting in the field of road maintenance based on big data analysis // *International Journal of Engineering and Technology (UAE)*. 2018. Vol. 7. No. 4.36. P. 88–91.
205. Yin X. C., Liu Z. G., Ndibanje B., Nkenyereye L., Riazul Islam S. M. An IoT-based anonymous function for security and privacy in healthcare sensor networks // *Sensors*. 2019. Vol. 19. No. 14. P. 3146.
206. Петров А. В., Большаков О. С., Лебедев А. С., Голубева Н. Е. Метод шаблонов приложений для повышения мобильности распределенных систем сбора и ретрансляции информации с биомедицинских датчиков // *Журнал радиоэлектроники*. 2013. Т. 5. С. 7.
207. Лебедев А. С., Большаков О. С., Петров А. В. Проектирование распределенной системы ретрансляции данных с мобильными клиентами на основе кроссплатформенных методов разработки программного обеспечения // *Современные проблемы науки и образования*. 2013. Т. 1. С. 133–133.
208. Mortajez S., Tahmasbi M., Zarei J., Jamshidnezhad A. A novel chaotic encryption scheme based on efficient secret keys and confusion tech-

nique for confidential of DICOM images // *Informatics in Medicine Unlocked*. 2020. Vol. 20. P. 100396.

209. Shini S. G., Thomas T., Chithraranjan K. Cloud based medical image exchange-security challenges // *Procedia Engineering*. 2012. Vol. 38. P. 3454–3461.

210. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М.И., Татарканов А. А. Программный модуль интеллектуального автоматизированного поиска ситуационных событий в видеопотоке / Свидетельство о регистрации программы для ЭВМ 2021664645, 10.09.2021. Заявка № 2021663707 от 25.08.2021.

211. Магомедов Ш.Г., Лебедев А.С., Смирнов П.А. Модуль генерации участков с болезненными признаками на маммографических изображениях / Свидетельство о регистрации программы для ЭВМ RU 2021614527, 25.03.2021.

212. Мустафаев А.Г., Магомедов Ш.Г., Ирзаев Г.Х. Программа для определения сходства семантических сетей / Свидетельство о регистрации программы для ЭВМ RU 2015617768, 22.07.2015. Заявка № 2015614331 от 25.05.2015.

213. Мустафаев А.Г., Магомедов Ш.Г. Система управления версиями / Свидетельство о регистрации программы для ЭВМ RU 2015618491, 11.08.2015. Заявка № 2015615233 от 16.06.2015.

214. Magomedov S. Software for analyzing security for healthcare organizations // *Communications in Computer and Information Science*. 2021. Vol. 1395. P. 181–189.

215. Open Source Clinical Image and Object Management. [Электронный ресурс]. URL: <https://www.dcm4che.org/>

216. *Puntambekar A. A.* Analysis and design of algorithms: Conceptual Approach. — Technical Publications, Pune, 2020
217. *Nikulchev E., Ilin D., Gusev A.* Technology stack selection model for software design of digital platforms // *Mathematics*. 2021. Vol. 9. No. 4. P. 308.
218. *Magomedov S, Ilin D, Nikulchev E.* Resource Analysis of the Log Files Storage Based on Simulation Models in a Virtual Environment. // *Applied Science*. 2021. Vol. 11. No. 11. P. 4718.
219. *Борисов А. В.* Имитационное моделирование распределенной экспертно-информационной системы // *Известия Института инженерной физики*. 2008. Т. 4. № 10. С. 30–33.
220. *Босов А. В., Борисов А. В.* Модели оптимизации функционирования Информационного веб-портала // *Труды Института системного анализа Российской академии наук*. 2009. Т. 45. С. 107–133.
221. *Шелухин О. И., Антонян А. А.* Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями // *Т-Сотт-Телекоммуникации и Транспорт*. 2014. Т. 8. № 6. С. 61–64.
222. *Шелухин О. И., Долгова А. В.* Фрактальные характеристики сетевых атак // Материалы XIII международной отраслевой научно-технической конференции «Технологии информационного общества». — М., 2019. С. 405–409.
223. *Nikulchev E., Pluzhnik E.* Study of chaos in the traffic of computer networks // *International Journal of Advanced Computer Science and Applications*. 2014. Vol. 5. No. 9. P. 60–62.
224. *Karpukhin A., Griciv D., Nikulchev E.* Simulation of chaotic phenomena in infocommunication systems with the TCP protocol // *Journal of The-*

oretical and Applied Information Technology. 2018. Vol. 96. No. 15. P. 5080–5093.

225. Mironov V., Gusarenko A., Yusupova N., Smetanin Y. Json documents processing using situation-oriented databases // *Acta Polytechnica Hungarica*. 2020. Vol. 17. No. 8. P. 29–40.

226. Петрушин В. Н., Рытиков Г. О. Адаптивно-вероятностная модель прогнозирования временных рядов // *Известия вузов. Проблемы полиграфии и издательского дела*. 2013. №. 5. С. 125–140.

227. Никульчев Е. В., Петрушин В. Н., Ульянов М. В. Интервальная оценка средних значений случайной величины в условиях неопределенности функции плотности распределения вероятностей // *Известия вузов. Проблемы полиграфии и издательского дела*. 2013. №. 2. С. 053–059.

228. Mironov V., Gusarenko A., Yusupova N., Smetanin Y. Json documents processing using situation-oriented databases // *Acta Polytechnica Hungarica*. 2020. Vol. 17. No. 8. P. 29–40.

229. Миронов В. В., Гусаренко А. С., Юсупова Н. И. Применение веб-сервисов на основе ситуационно-ориентированной базы данных для мониторинга просмотра учебного видеоконтента // *Моделирование, оптимизация и информационные технологии*. 2019. Т. 7. № 3 (26). С. 27.

230. Kim J., Gabriel U., Gyga P. Testing the effectiveness of the Internet-based instrument PsyToolkit: A comparison between web-based (PsyToolkit) and lab-based (E-Prime 3.0) measurements of response choice and response time in a complex psycholinguistic task // *PloS One*. 2019. Vol. 14. No. 9. P. e0221802.

231. Nikulchev E., Ilin D., Kolyasnikov P., Magomedov S., Alexeenko A., Kosenkov A. N., Sokolov A., Malykh A., Ismatullina V., Malykh S. Isolated sand-

box environment architecture for running cognitive psychological experiments in web platforms // *Future Internet*. 2021. Vol. 13. No. 10. P. 245

232. NEMA P. S. ISO 12052 //Digital imaging and communications in medicine (DICOM) standard, National Electrical Manufacturers Association, Rosslyn, VA, USA (<http://medical.nema.org/>). – 2017.

233. Strom B. E., Applebaum A., Miller D. P., Nickels K. C., Pennington A. G., Thomas, C. B. Mitre att&ck: Design and philosophy /*Technical report*. — 2018.

234. Decraene B., Saad T., Beeram V., Jalil L. Using Entropy Label for Network Slice Identification in MPLS networks. draft-decraene-mpls-slid-encoded-entropy-label-id-01. 2021. [Электронный ресурс]. URL: <https://datatracker.ietf.org/doc/html/draft-decraene-mpls-slid-encoded-entropy-label-id-01>

235. Клянчин А. И. Каталог закладок АНБ (Spiegel). Часть 1. Инфраструктура // *Вопросы кибербезопасности*. 2014. № 2 (3). С. 63–65.

236. RSyslog Documentation. [Электронный ресурс]. https://www.rsyslog.com/doc/master/tutorials/failover_syslog_server.html

237. qemu-kvm — QEMU is a machine emulator and virtualizer. [Электронный ресурс]. URL: https://centos.pkgs.org/7/centos-x86_64/qemu-kvm-1.4.3-175.el7.x86_64.rpm.html

238. Suricata. Open Source IDS / IPS / NSM engine. [Электронный ресурс]. URL: <https://suricata-ids.org/>

239. CyberMDX Research Team Discovers Vulnerability in GE CARESCAPE, ApexPro, and Clinical Information Center Systems. [Электронный ресурс]. URL: <https://www.cybermdx.com/vulnerability-research-disclosures/cic-pro-and-other-ge-devices>

240. Смирнов С.И., Прибылов И.А., Магомедов Ш.Г., Изергин Д.А. Программный комплекс обнаружения вредоносной активности в корпоративной сети / Свидетельство о регистрации программы для ЭВМ 2021614531, 25.03.2021.

241. Otsokov S.A., Magomedov S.G. On the possibility of implementing high-precision calculations in residue numeral system // *International Journal of Advanced Computer Science and Applications*. 2019. Vol. 10, No. 11. С. 9–13.

242. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М.И., Татарканов А. А. Конфигуратор настройки параметров работы сервера / Свидетельство о регистрации программы для ЭВМ 2021664584, 09.09.2021.

243. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М.И., Татарканов А. А. Программный модуль интеллектуального анализа потоковых видеоданных на основе методов машинного обучения / Свидетельство о регистрации программы для ЭВМ 2021664913, 15.09.2021.

244. Сигов А. С., Рагуткин А. В., Александров И. А., Магомедов Ш. Г., Ставровский М. Е., Сидоров М.И., Татарканов А. А. Многофункциональная программная платформа видеоаналитики / Свидетельство о регистрации программы для ЭВМ 2021664454, 07.09.2021.

245. Mitmproxy. [Электронный ресурс]. <https://mitmproxy.org/>

246. Jose J. M., Reeja S. R. Anomaly Detection on System Generated Logs—A Survey Study // *Mobile Computing and Sustainable Informatics*.—Springer, Singapore, 2022. P. 779–793.

247. Weise M., Kovacevic F., Popper N., Rauber A. OSSDIP: Open Source Secure Data Infrastructure and Processes Supporting Data Visiting. // *Data Science Journal*. 2022. Vol. 21. No. 1.

248. *Belov V., Tatarintsev A., Nikulchev E.* Choosing a Data Storage Format in the Apache Hadoop System Based on Experimental Evaluation Using Apache Spark // *Symmetry*. Vol. 13. No. 2, P. 195.

249. Артамонов В. А., Артамонова Е. В. Искусственный интеллект и безопасность: проблемы, заблуждения, реальность и будущее // *Россия: тенденции и перспективы развития*. 2022. №. 17-1. С. 585–594.

ПРИЛОЖЕНИЕ 1 Копии актов о внедрении

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ

**ФЕДЕРАЛЬНОЕ БЮРО
МЕДИКО-СОЦИАЛЬНОЙ
ЭКСПЕРТИЗЫ**

МИНИСТЕРСТВА ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

(ФГБУ ФБ МСЭ Минтруда России)

ул. Ивана Сусанина 3, Москва, 127486

Тел. 8(499) 487-57-11; факс 8 (499) 487-81-81

E-mail: fbmse@fbmse.ru <http://www.fbmse.ru>

ОКПО 55220088, ОГРН1047743057493

ИНН/КПП 7743085670/773401001

АКТ

внедрения результатов диссертационной работы Шамиля Гасангусейновича Магомедова представленной на соискание ученой степени доктора технических наук

Настоящим актом подтверждается, что основные результаты диссертационного исследования, выполненного Магомедовым Шамилем Гасангусейновичем, направленного на решение научно-практической задачи построения многоуровневой масштабируемой архитектуры контроля доступа к сервисам вычислительного комплекса в цифровой среде, методик проектирования инфраструктуры виртуальных ресурсов контроля доступа и методики оценки ресурсных затрат при внедрении технологий контроля доступа, внедрены в ходе выполнения проекта «Проектирование платформы непрерывного медицинского образования», проводимого для повышения квалификации врачей-экспертов медико-социальной экспертизы.

Использование внедренных результатов диссертационного исследования позволило осуществить разработку и проектирование архитектуры серверных мощностей, позволяющих эффективно и безопасно обрабатывать запросы масштабируемой до ста тысяч пользователей одновременно, поэтапное развёртывание информационных систем на базе созданного виртуального ЦОДа. Выбранные информационно-технологические решения обеспечили надежное функционирование созданных образовательных порталов.

Председатель комиссии:

Заместитель руководителя по ИТ ФГБУ ФБ МСЭ Минтруда России

Члены комиссии:

Заведующая отделом методологических основ
по профессиональной подготовке и переподготовке
специалистов в области МСЭ

Начальник отдела Защиты информации Центра ИТО и МЭВ

Руководитель Центра ИТО и МЭВ



[Signature]

С.В. Терсков

[Signature]

И.В. Кузина

[Signature]

И.В. Садыков

[Signature]

О.В. Симаков



ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО КОСМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ «РОСКОСМОС»
 ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
 «НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ТЕХНОМАШ»
 (ФГУП «НПО «Техномаш»)

127018, г.Москва, 3-й проезд Марьиной Рощи, д. 40, а/я 131
 тел.: (495)689 50 66, факс (495) 689 73 45
 e-mail: info@tmnp.ru www.tmnp.ru

ОКПО 07527638, ОГРН 1037739453982, ИНН 7715012448, КПП 771501001

УТВЕРЖДАЮ

Заместитель генерального директора
 по научно-технологическому сопровождению
 работ по созданию изделий РКТ



А.Н. Дементьев

« 24 » 05 2021 г.

АКТ-02/2021

**внедрения результатов диссертационной работы
 Магомедова Шамиля Гасангусейновича представленной
 на соискание ученой степени доктора технических наук**

Комиссия в составе:

председателя комиссии:

- И.о. директора центра обеспечения технологичности изделий РКТ
 Арсеньева К.В.

и членов комиссии:

- начальника отдела исследования технологических проектов создания
 изделий РКТ центра научно-технического сопровождения создания изделий
 РКТ Андреева Г.И.
- главного специалиста центра обеспечения технологичности изделий РКТ
 Дмитриева В.Г.
- специалиста центра обеспечения технологичности изделий РКТ Басака А.А.

составила настоящий акт о том, что в диссертации на соискание ученой степени
 доктора технических наук Магомедова Шамиля Гасангусейновича полученные
 научные результаты:

- методики учета прикладных аспектов внедрения многоуровневого контроля
 доступа в архитектуру специализированных вычислительных комплексов;

- методики анализа затрат вычислительных ресурсов для реализации систем контроля доступа;

- методики проектирования инфраструктуры виртуальных ресурсов контроля доступа

внедрены ФГУП «НПО «Техномаш» при подготовке и выполнении следующих работ:

- СЧ ОКР «Подтверждение требований надежности БАО-СК. Разработка программно-аппаратных средств моделирования показателей надежности на основе оценки интегрального потока нейтронов, экспозиционной дозы гамма-излучений, энергетических спектров заряженных частиц» (Шифр СЧ ОКР «Иртыш-СК-Надежность»);

- СЧ ОКР «Анализ технологической готовности и качества разрабатываемых и изготавливаемых составных частей изделий, разрабатываемых в рамках ОКР «Двина-КВТК»;

- СЧ ОКР «Анализ технологической готовности и качества разрабатываемых и изготавливаемых составных частей изделий, разрабатываемых в рамках ОКР «Амур»;

- НИР (Шифр НИР «Телескоп»);

- ОКР (Шифр ОКР «Орел-РВ»).

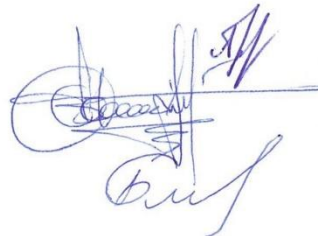
Научные результаты являются достоверными, надежными и могут использоваться предприятиями отрасли при решении научно-практических задач.

Председатель комиссии:



Арсеньев К.В.

Члены комиссии:



Андреев Г.И.

Дмитриев В.Г.

Басак А.А.



Разработка программного
обеспечения: Java, Net
Core, Python, PHP и др.

ООО «Коллектив Интеллидженс
Системс». 123557, Россия, Москва,
Электрический пер. 3/10с1

Юсубалиев Тимур,
89251477526,
ytr@kpr-it.com

Утверждаю
Генеральный директор ООО «КПР»
Юсубалиев Тимур Ринатович
«18» февраля 2022 года

АКТ
внедрения результатов диссертационной работы Ш.Г.Магомедова
в ООО «Качественные программные решения».

Настоящим подтверждается, что результаты диссертационного исследования Магомедова Шамиля Гасангусейновича «Методы и модели построения масштабируемой архитектуры системы контроля доступа к вычислительным сервисам» внедрены в ООО «Качественные программные решения».

Применение методик оценки ресурсных затрат и построения облачной инфраструктуры, созданной Ш.Г. Магомедовым позволило улучшить технико-экономические характеристики разрабатываемых программных решений компанией ООО «Качественные программные решения».

Результаты полученные Ш.Г. Магомедовым, являются достоверными, надежными и могут использоваться организациями которые занимаются разработкой, проектированием вычислительной комплексов а также безопасностью обмена информацией по общедоступным сетям.

Генеральный директор ООО «КПР»



Юсубалиев Т.Р.

Общество с ограниченной
ответственностью «Непрерывные
технологии» (ООО «Непрерывные
технологии»)
г. Москва, ул. Новодмитровская Б.,
д. 23, строение 3, 127015
тел. +7(499) 444-12-46
ИНН 9715347215, ОГРН 1197746340330

27 «января» 2022 г. №17-Ф

АКТ

Об использовании результатов диссертационной работы Ш. Г. Магомедова на тему:
«Методы и модели построения масштабируемой архитектуры системы контроля
доступа к вычислительным сервисам» в ООО «Непрерывные технологии».

Для анализа сетевого трафика, предотвращения утечки конфиденциальной
медицинской информации, отслеживания пользовательского поведения применение
разработанных Магомедовым Ш.Г., архитектурных решений показало:

1. Высокую производительность выборочного анализа сетевого трафика, предназначенного PACS, с помощью разработанного в ООО «Непрерывные технологии» аналитического кластера согласно архитектурным принципам, предложенным в диссертации.
2. Эффективность выявления некачественных медицинских изображений в архиве DICOM с помощью разработанного в ООО «Непрерывные технологии» плагина проверки корректности.
3. Возможность выявить несвоевременно полученные медицинские изображения с помощью модели корректности периодичности.
4. Возможность осуществления классификации пользовательского поведения “на легу” и выявления неэффективной работы медицинских специалистов с помощью разработанного программного обеспечения.

Генеральный директор
ООО «Непрерывные технологии»

О. А. Ганиев





МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

РТУ МИРЭА

просп. Вернадского, д. 78, Москва, 119454
тел.: (499) 215 65 65 доб. 1140, факс: (495) 434 92 87
e-mail: mirea@mirea.ru, <http://www.mirea.ru>

№ _____
на № _____ от _____



Утверждаю

Проректор по инновационному развитию

А.В. Рагуткин

«16» *марта* 2021г.

Акт

внедрения результатов диссертационной работы Шамиля
Гасангусейновича Магомедова представленной на соискание ученой
степени доктора технических наук

Настоящим актом подтверждается, что основные результаты диссертационного исследования, выполненного Магомедовым Шамилем Гасангусейновичем, направленного на решение научно-практической задачи построения многоуровневой масштабируемой архитектуры контроля доступа к сервисам вычислительного комплекса в цифровой среде, методик проектирования инфраструктуры виртуальных ресурсов контроля доступа и учета прикладных аспектов при разработке архитектуры, внедрены в ходе выполнения проекта «Создание цифровой образовательной среды и разработка (доработка) ЭОР для учителей школ за

рубежом», проводимого в рамках Национальной программы «Цифровая экономика Российской Федерации».

Использование внедренных результатов диссертационного исследования позволило осуществить разработку концепции цифровой образовательной среды, а также развёртывание мультязычной цифровой образовательной среды на базе технологий адаптивного электронного обучения. Выбранные информационно-технологические решения обеспечили надежное функционирование во время эксплуатации системы.

Начальник управления
научно-исследовательских разработок



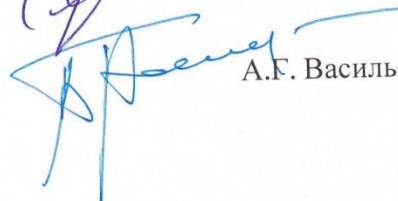
О.Е. Винокуров

Заместитель директора по инновационному
развитию ИРТС, д.т.н., доцент



М.С. Костин

Директор ИРТС, д.ф.-м.н., профессор



А.Г. Васильев

**Общество с ограниченной ответственностью
«Лаборатория Наносемантика»
(ООО «Лаборатория Наносемантика»)**

ИНН 7703761097, КПП 773101001 ОГРН 1127746015517
121357, г. Москва, ул. Вере́йская, д. 29, стр. 134, этаж 7, помещение Н2

15.02.2022 г.

**АКТ
внедрения результатов диссертационной работы Шамиля
Гасангусейновича Магомедова представленной на соискание ученой
степени доктора технических наук**

Настоящим актом подтверждается, что основные результаты диссертационного исследования, выполненного Магомедовым Шамилем Гасангусейновичем, на тему «Методы и модели построения масштабируемой архитектуры системы контроля доступа к вычислительным сервисам» внедрены в ходе выполнения проекта «Маркер» (система сбора и разметки обучающих данных).

Метод анализа психологических реакций пользователя при взаимодействии с элементами интерфейса на основе анализа времени ответа на контрольные вопросы позволил повысить качество собираемых данных при формировании датасетов. Предложенный метод применим в том числе для верификации пользователей при доступе в вычислительные системы.

Полученные результаты Магомедовым Ш.Г., являются надежными и достоверными, которые имеют не только теоретическое, но и прикладное значение.

Генеральный директор
ООО «Лаборатория Наносемантика»





АКТ

внедрения результатов диссертационного исследования Магомедова
Шамяля Гасангусейновича, представленной на соискание ученой степени
доктора технических наук

Комиссия в составе: председателя – научного консультанта 2 отдела, доктора технических наук доцента Коньшева Михаила Юрьевича и членов комиссии: старшего научного сотрудника научно-организационного отдела кандидата физико-математических наук Романца Андрея Владимировича и старшего научного сотрудника научно-организационного отдела кандидата технических наук Смирнова Сергея Владиславовича, составила настоящий акт о внедрении результатов диссертационного исследования Магомедова Шамяля Гасангусейновича, а именно:

1. Методики построения облачной инфраструктуры, обеспечивающей решение задач контроля доступа.
2. Методики ресурсного анализа реализации контроля доступа на основе имитационных исследований.

Использование указанных результатов в НИР «Аверс» позволило провести анализ уязвимостей мобильных операционных систем при решении задач контроля доступа.

Председатель комиссии:
доктор технических наук, доцент
Члены комиссии:
кандидат технических наук
кандидат физико-математических наук

 М.Ю. Коньшев
 С.В. Смирнов
А.В. Романец