МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра Прикладная математика и информатика
(наименование)

02.03.03 Математическое обеспечение и администрирование информационных систем
(код и наименование направления подготовки, специальности)

Мобильные и сетевые технологии
(наименование профиля, специализации)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему Разработка автоматизированной системы управления событиями безопасности

Обучающийся Д.А. Бурдин _____
(Инициалы Фамилия) (личная подпись)

Руководитель канд. пед. наук, доцент, О.М. Гущина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант канд. пед. наук, доцент, А.В. Егорова
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Тема бакалаврской работы: «Разработка автоматизированной системы управления событиями безопасности».

Бакалаврская работа посвящена разработке автоматизированной системы управления событиями безопасности.

В ходе выполнения исследований по бакалаврской работе был проведен анализ системы управления событиями безопасности, проектирование управления событиями безопасности, протестирована автоматизированная система управления событиями безопасности.

Во введении прописывается актуальность темы, написаны цель и задачи.

В первом разделе рассматривается предметная область исследования и проводится анализ аналогов.

Во втором разделе моделируется архитектура системы, приводится математический анализ эффективности защиты и разработана автоматизированная система управления событиями безопасности.

Третий раздел содержит поиск смоделированной атаки и тестирование обнаружения вторжения.

В заключении представлены результаты выполнения выпускной квалификационной работы.

Бакалаврской работа состоит из введения, трёх разделов, заключения и списка использованной литературы.

Бакалаврская работа состоит из 48 страницы, 24 рисунков, 2 таблиц, 30 источников.

Abstract

The title of the bachelor’s thesis is “Development of an automated security event management system”.

The research is devoted to development of an automated security event management system.

When doing a research, the analysis of the security event management system, the design of security event management was carried out, the automated security event management system was tested.

The introduction reveals the relevance of the research and gives a brief description of the work done.

The first section the subject area of the study is considered and the analysis of analogues is carried out.

The second section the system architecture is modeled, a mathematical analysis of the effectiveness of protection is given, and an automated security event management system is developed.

The third section contains the search for a simulated attack and testing of intrusion detection.

In conclusion, the conclusions of the entire work are drawn.

The bachelor’s thesis consists of an introduction, three sections, a conclusion and list of used literature.

The volume of the bachelor's thesis is 48 pages, it also contains 24 figures, 2 tables and a list of 30 references.

Содержание

Введение

Возрастающая сложность и частота кибератак требуют от организаций внедрения эффективных систем управления событиями безопасности. Традиционных ручных подходов к выявлению и устранению инцидентов безопасности уже недостаточно, чтобы справиться с растущим объемом и сложностью угроз безопасности. Чтобы решить эту проблему, автоматизированная система управления событиями безопасности может предоставить организациям мониторинг в реальном времени, точное обнаружение и эффективное реагирование на инциденты безопасности [15].

Эта работа направлена на разработку автоматизированной системы управления событиями безопасности с использованием российских источников. Предлагаемая система будет использовать методы машинного обучения и анализа данных для выявления и приоритизации событий безопасности, уменьшения ложных срабатываний и отрицательных результатов и улучшения общего состояния безопасности организаций. Система будет предназначена для сбора данных из различных источников, включая сетевые журналы, системные журналы и журналы приложений, и обработки их в режиме реального времени для выявления подозрительных действий [13].

Система также будет включать в себя возможности реагирования на инциденты и управления, чтобы обеспечить быстрое сдерживание и разрешение инцидентов безопасности. Предлагаемая система будет протестирована в смоделированной среде, и результаты будут оцениваться на основе эффективности, действенности и точности системы при выявлении и реагировании на инциденты безопасности.

Разработка автоматизированной системы управления событиями безопасности с использованием российских источников имеет большое значение для организаций, работающих на российском рынке. Система может предоставить организациям надежный и эффективный механизм

защиты их критически важных активов и конфиденциальной информации от кибератак. Результаты этого исследования могут также способствовать разработке аналогичных систем в других регионах и улучшить понимание управления событиями безопасности в сообществе кибербезопасности.

Объектом исследования является система управления событиями безопасности.

Предметом исследования является автоматизация системы управления событиями безопасности.

Цель работы: спроектировать и разработать автоматизированную систему управления событиями безопасности.

Задачи:

– Провести обзор литературы по системам управления событиями безопасности и определить их ограничения.

– Определить требования автоматизированной системы управления событиями безопасности.

– Спроектировать и разработать систему с использованием соответствующих технологий.

– Протестировать и оценить систему с использованием различных сценариев.

Бакалаврская работа состоит из введения, трех разделов, заключения, списка используемой литературы и приложения.

Бакалаврская работа включает 48 страниц текста, 24 рисунка, 2 таблицы и 30 источников.

1 Анализ системы управления событиями безопасности

1.1 Постановка задачи исследования

Растущее число кибератак и нарушений безопасности стало серьезной проблемой для организаций всех размеров и секторов. С ростом сложности угроз безопасности и огромным объемом данных, генерируемых системами безопасности, специалистам по безопасности становится все труднее эффективно управлять событиями безопасности и своевременно реагировать на потенциальные угрозы. Это привело к высокому спросу на автоматизированные системы управления событиями безопасности, которые могут помочь организациям повысить уровень безопасности и снизить риски, связанные с кибератаками[26].

Традиционного подхода ручного управления событиями безопасности уже недостаточно для решения растущих проблем безопасности, с которыми сталкиваются организации. Ручные процессы отнимают много времени, подвержены ошибкам и часто не в состоянии идти в ногу со скоростью и изощренностью современных киберугроз. Кроме того, ручное управление событиями не позволяет в режиме реального времени предоставлять аналитические данные и оповещения о потенциальных угрозах, что может привести к задержке реагирования и увеличению рисков.

Автоматизированная система управления событиями безопасности может предоставить организациям возможность отслеживать и анализировать события безопасности в режиме реального времени, быстрее обнаруживать угрозы и более эффективно реагировать на них. Он также может предоставлять группам безопасности контекстную информацию и аналитические данные, что позволяет им принимать обоснованные решения и предпринимать соответствующие действия. Автоматизируя управление событиями безопасности, организации могут повысить уровень безопасности, снизить риск утечки данных и свести к минимуму влияние

инцидентов безопасности [6].

Однако разработка эффективной автоматизированной системы управления событиями безопасности требует значительных исследований и разработок. Он включает в себя интеграцию различных технологий безопасности, таких как системы обнаружения вторжений, брандмауэры и каналы информации об угрозах, а также использование расширенной аналитики и алгоритмов машинного обучения для обнаружения угроз безопасности и реагирования на них. Система также должна быть гибкой, масштабируемой и простой в использовании, а также должна соответствовать соответствующим отраслевым стандартам и нормам.

Таким образом, постановка задачи исследования разработки автоматизированной системы управления событиями безопасности состоит в том, чтобы определить ключевые проблемы и требования, связанные с разработкой эффективной системы, которая может помочь организациям повысить уровень безопасности и снизить риски, связанные с кибератаками. Это будет включать в себя исследование новейших технологий и передового опыта в области безопасности, анализ существующих систем и разработку комплексной основы и методологии для создания автоматизированной системы управления событиями безопасности, которая будет эффективной, действенной и удобной для пользователя. В конечном счете, цель этого исследования – помочь организациям внедрить надежную и эффективную систему управления событиями безопасности, которая поможет защитить их от потенциальных киберугроз.

1.2 Основы безопасности информационных систем

Основы безопасности информационных систем включают в себя широкий круг вопросов, связанных с защитой информации от нежелательного доступа, изменения, уничтожения и других видов угроз. Для обеспечения безопасности информационных систем используются различные

методы и подходы, включая криптографические алгоритмы, контроль доступа, мониторинг событий безопасности и др.

Одним из ключевых аспектов безопасности информационных систем является защита от кибератак. Кибератаки могут привести к утечке конфиденциальной информации, нарушению работоспособности системы, угрозам для деятельности организации и даже к причинению физического вреда [18].

Для защиты информационных систем от кибератак необходимо использовать комплексный подход, который включает в себя меры по обеспечению физической, технической и программной безопасности системы, а также обучение сотрудников правилам безопасности и контроль их действий.

Основы безопасности информационных систем являются фундаментом для разработки автоматизированной системы управления событиями безопасности, которая должна обеспечивать надежную защиту информации и своевременное реагирование на угрозы безопасности.

В рамках данного раздела будут рассмотрены основные принципы и методы обеспечения безопасности информационных систем, а также выделены наиболее значимые угрозы и уязвимости, которые могут возникнуть при использовании информационных технологий.

В качестве основных принципов безопасности информационных систем можно выделить следующие:

- конфиденциальность – защита информации от несанкционированного доступа;
- целостность – защита информации от несанкционированных изменений;
- доступность – обеспечение доступа к информации только тем, кто имеет на это право.

Для обеспечения безопасности информационных систем используются различные методы и подходы, такие как:

– криптографические алгоритмы – методы защиты информации с помощью шифрования и дешифрования данных;
– контроль доступа – методы, позволяющие определить, кто имеет право получить доступ к определенной информации;
– мониторинг событий безопасности – методы, позволяющие отслеживать события, связанные с безопасностью информационной системы.

Основная цель данного раздела – рассмотреть все эти методы и подходы более подробно и показать, как они могут быть применены для обеспечения безопасности информационных систем.

Безопасность информационных систем является важнейшим компонентом успеха любой современной организации [8],[10]. С ростом использования технологий организации сталкиваются с большей потребностью в защите своих информационных активов. Цель этого раздела состоит в том, чтобы предоставить обзор фундаментальных концепций и принципов безопасности информационных систем.

Безопасность информационных систем относится к защите информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения. Сфера безопасности информационных систем включает физические, технические и административные средства контроля, необходимые для защиты информационных активов.

Угрозы безопасности информационных систем можно разделить на три основные категории: человеческие, природные и технические. Человеческие угрозы включают в себя социальную инженерию, внутренние угрозы и киберпреступность. Природные угрозы включают экологические катастрофы, такие как наводнения или землетрясения. К техническим угрозам относятся вредоносные программы, вирусы и хакерские атаки. [20]

Цели безопасности информационных систем включают конфиденциальность, целостность и доступность. Конфиденциальность

относится к защите конфиденциальной информации от несанкционированного доступа или раскрытия. Целостность относится к защите информации от несанкционированной модификации, уничтожения или разрушения. Доступность относится к способности авторизованных пользователей получать доступ к информационным системам и данным, когда это необходимо.

Меры безопасности информационных систем можно разделить на три основные категории: физические, технические и административные. К физическим средствам контроля относятся такие меры, как контроль доступа, контроль окружающей среды и физическая безопасность. К техническим средствам контроля относятся такие меры, как шифрование, брандмауэры и системы обнаружения вторжений. Административный контроль включает политики, процедуры и программы обучения [12].

Существует несколько стандартов и структур безопасности информационных систем, включая ISO 27001, ITIL и NIST. Эти структуры содержат рекомендации и лучшие практики для управления безопасностью информационных систем.

1.3 Системы информационной безопасности

Системы информационной безопасности (СИБ) представляют собой решение, направленное на обеспечение защиты критичной информации организации от разглашения, утечки и несанкционированного доступа. Как и КСЗИ, СИБ объединяет в себе комплекс организационных мероприятий и технических средств защиты информации.

При построении системы информационной безопасности нет необходимости выполнять требования нормативных документов в сфере технической защиты информации, так как основными потребителями системы информационной безопасности являются коммерческие организации, которые не обрабатывают информацию, принадлежащую

государству. Вторым принципиальным отличием является отсутствие контролирующего органа, и, как следствие, спроектированная СИБ не требует проведения государственной экспертизы. Еще одно отличие от комплексной системы защиты информации – свободный выбор технических средств, возможное применение любых аппаратных и программных средств защиты информации.

Информационная безопасность необходима для любой организации, которая работает с секретными или конфиденциальными данными. Системы информационной безопасности предназначены для защиты этих данных от несанкционированного доступа, кражи, модификации или уничтожения. В этом анализе мы рассмотрим некоторые из существующих систем информационной безопасности и оценю их эффективность [3],[4]:

– брандмауэр – это система сетевой безопасности, которая отслеживает и контролирует входящий и исходящий сетевой трафик. Он действует как барьер между внутренней сетью и Интернетом. Брандмауэр отфильтровывает нежелательный трафик и пропускает только разрешенный трафик. Брандмауэры эффективно предотвращают несанкционированный доступ к сети, но не защищают от внутренних угроз;

– антивирусное программное обеспечение. Антивирусное программное обеспечение – это программа, которая обнаруживает, предотвращает и удаляет вредоносное ПО из компьютерной системы. Он сканирует файлы и каталоги на наличие известных вирусов и других вредоносных программ. Антивирусное программное обеспечение эффективно предотвращает атаки вредоносных программ, но требует регулярных обновлений, чтобы не отставать от новых угроз;

– система обнаружения вторжений (IDS): IDS – это система, которая отслеживает сетевой трафик на наличие признаков вредоносной активности. Он обнаруживает и предупреждает системного администратора о любых подозрительных действиях. IDS может помочь предотвратить сетевые атаки, но также может генерировать ложные тревоги;

– системы контроля доступа. Системы контроля доступа используются для управления доступом к ресурсам внутри организации. Оно может быть физическим или логическим. Системы контроля физического доступа используются для ограничения доступа в здания, помещения или центры обработки данных. Логические системы управления доступом используются для ограничения доступа к компьютерным системам, приложениям или данным. Системы контроля доступа эффективно предотвращают несанкционированный доступ к ресурсам;

– шифрование – это процесс преобразования данных в код для предотвращения несанкционированного доступа. Это эффективно для защиты данных от кражи или подделки. Однако могут возникнуть трудности с управлением ключами шифрования и их обслуживанием.

Существуют различные системы информационной безопасности, которые организации могут использовать для защиты от киберугроз. Однако ни одна система не может обеспечить полную защиту. Крайне важно использовать комбинацию систем и регулярно обновлять, и поддерживать их для обеспечения их эффективности. Кроме того, обучение и подготовка сотрудников имеют решающее значение для предотвращения внутренних угроз и обеспечения надлежащего использования сотрудниками систем безопасности [29].

СИБ можно рекомендовать коммерческим организациям, которые заботятся о сохранности своей коммерческой (критичной) информации или собираются принимать меры по обеспечению безопасности своих информационных активов.

Для определения необходимости построения СИБ и направления работ по защите информации, а также для оценки реального состояния информационной безопасности организации необходимо проводить аудит информационной безопасности.

Важным моментом, который касается эксплуатации как КСЗИ, так и СИБ, является тот факт, что недостаточно просто построить и

эксплуатировать эти системы защиты, необходимо постоянно их совершенствовать так же, как совершенствуются способы несанкционированного доступа, методы взлома и хакерские атаки.

1.4 Существующие методы и средства управления событиями безопасности

Существует несколько методов управления событиями безопасности, включая ручной, полуавтоматический и автоматический подходы. Ручной подход основан на вмешательстве человека для обнаружения и расследования событий безопасности. Хотя этот подход предлагает определенный уровень гибкости, он отнимает много времени и подвержен ошибкам. Полуавтоматический подход сочетает вмешательство человека с автоматизированными инструментами для обнаружения и анализа событий безопасности. Этот подход обеспечивает более высокую точность и эффективность, чем ручной подход, но требует квалифицированной рабочей силы. Автоматизированный подход основан на программных инструментах для обнаружения событий безопасности и реагирования на них. Этот подход обеспечивает высокую точность и эффективность при обнаружении событий безопасности и реагировании на них, но требует значительных инвестиций в технологии и инфраструктуру [7].

Существуют различные инструменты для управления событиями безопасности, в том числе системы управления информацией и событиями безопасности (SIEM), системы обнаружения вторжений (IDS) и платформы безопасности, автоматизации и реагирования (SOAR). Системы SIEM обеспечивают мониторинг и анализ событий безопасности в режиме реального времени и широко используются в корпоративных средах. IDS обнаруживают и предупреждают о потенциальных угрозах безопасности, а платформы SOAR автоматизируют процесс реагирования на инциденты. Каждый инструмент имеет свои сильные и слабые стороны, и выбор

подходящего инструмента зависит от потребностей и требований организации.

В таблице 1 описаны существующие методы и средства управления событиями безопасности.

Таблица 1 – Существующие методы и средства управления событиями безопасности

Метод	Описание	Плюсы	Минусы
Руководство	События безопасности идентифицируются и анализируются вручную человеком-аналитиком.	Обеспечивает высочайший уровень контроля и гибкости процесса анализа.	Может занимать много времени и сил и может быть не масштабируемым для больших объемов событий безопасности.
Полуавтоматический	Сочетание ручного и автоматического подходов, при котором события безопасности сначала идентифицируются и фильтруются автоматическими инструментами, а затем анализируются и выполняются аналитиком-человеком.	Предлагает баланс между контролем и эффективностью. Автоматизированные инструменты могут быстро сортировать большие объемы событий безопасности, в то время как аналитики-люди могут сосредоточиться на событиях с высоким приоритетом.	Все еще может занимать много времени и может потребовать значительного опыта для правильной настройки и использования автоматизированных инструментов.
Автоматический	События безопасности идентифицируются и анализируются полностью автоматизированными инструментами без вмешательства человека.	Обеспечивает высочайший уровень эффективности и масштабируемости с возможностью быстрого анализа больших объемов событий безопасности.	Может не обеспечивать такой же уровень контроля и гибкости, как ручной или полуавтоматический подходы. Автоматизированные инструменты также могут давать ложные срабатывания или ложноотрицательные результаты.

Ручной подход обеспечивает гибкость, но подвержен ошибкам и отнимает много времени. Полуавтоматический подход сочетает в себе вмешательство человека с автоматизацией и обеспечивает более высокую точность и эффективность, но требует квалифицированной рабочей силы. Автоматизированный подход обеспечивает высокую точность и эффективность при обнаружении событий безопасности и реагировании на них, но требует значительных инвестиций в технологии и инфраструктуру. Системы SIEM обеспечивают мониторинг и анализ событий безопасности в режиме реального времени, но требуют квалифицированного персонала для управления и обслуживания. IDS обнаруживают и предупреждают о потенциальных угрозах безопасности, но могут генерировать большое количество ложных срабатываний. Платформы SOAR автоматизируют процесс реагирования на инциденты и сокращают время реагирования, но требуют значительных инвестиций и могут быть сложными для интеграции с существующими системами [24].

Управление информацией и событиями безопасности (SIEM):

SIEM – это подход к управлению безопасностью, который включает сбор, анализ и хранение событий безопасности из различных источников. Это помогает организациям выявлять угрозы безопасности и своевременно реагировать на них. Система SIEM объединяет в себе средства управления информационной безопасностью (SIM) и средства управления событиями безопасности (SEM). Технология SIEM позволяет собирать данные журнала событий от различных источников, анализировать их в реальном времени, выявляя аномальные действия, и принимать необходимые меры. Инструменты SIEM собирают данные из таких источников, как брандмауэры, системы обнаружения вторжений (IDS), средства защиты конечных точек и файлы журналов. Инструмент собирает данные, сопоставляет их и представляет группе безопасности для анализа. Система также может генерировать оповещения при обнаружении подозрительной активности. Цель системы SIEM – предоставить централизованное представление о

состоянии безопасности организации и обеспечить быстрое реагирование на инциденты безопасности.

Организация безопасности, автоматизация и реагирование SOAR – это подход к управлению безопасностью, который автоматизирует реагирование на события безопасности. Он включает в себя интеграцию инструментов и технологий безопасности для обеспечения более эффективного и действенного реагирования на инциденты безопасности. Платформы SOAR автоматизируют сбор, анализ и реагирование на события безопасности. Инструмент создает сценарии, определяющие реакцию на события безопасности. Плейбуки можно настроить в соответствии с конкретными потребностями организации. Основное преимущество SOAR заключается в том, что он сокращает время реагирования на инциденты безопасности и позволяет специалистам по безопасности сосредоточиться на более сложных задачах [17].

Аналитика угроз – это подход к управлению безопасностью, включающий сбор, анализ и распространение информации об угрозах безопасности. Цель состоит в том, чтобы предоставить организациям информацию, необходимую им для выявления инцидентов безопасности и реагирования на них. Источники аналитики угроз включают аналитику с открытым исходным кодом, коммерческие каналы и внутренние источники, такие как файлы журналов и сетевой трафик. Информация анализируется для выявления закономерностей и тенденций, которые могут помочь в обнаружении возникающих угроз. Аналитика угроз может использоваться для повышения эффективности других технологий безопасности, таких как SIEM и SOAR.

Реагирование на инциденты – это подход к управлению безопасностью, включающий действия, предпринимаемые для реагирования на инциденты безопасности. Цель состоит в том, чтобы свести к минимуму последствия инцидента, локализовать угрозу и как можно быстрее восстановить нормальную работу. Процесс реагирования на инциденты включает шесть

этапов: подготовка, идентификация, сдерживание, устранение, восстановление и извлеченные уроки. Планы реагирования на инциденты обеспечивают основу для реагирования на инциденты безопасности и должны регулярно обновляться и тестироваться [5].

1.5 Порядок создания комплексной системы защиты информации

Разработка комплексной системы защиты информации осуществляется в соответствии с нормативным документом на техническую систему защиты информации и на основании требований, указанных в техническом задании на техническую систему защиты информации. Кроме того, рекомендуется следовать стандарту при проектировании КСЗИ.

В состав КСЗИ входят мероприятия и средства, которые реализуют способы, методы, механизмы защиты информации от:

- утечки техническими каналами, к которым относятся каналы побочных электромагнитных излучений и наводок, акустоэлектрических и других каналов;
- несанкционированных действий и несанкционированного доступа к информации, которые могут осуществляться путем подключения к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, преодоление мероприятий защиты с целью использования информации или навязывания ошибочной информации, применение закладных устройств или программ, использование компьютерных вирусов и т.п.;
- специального влияния на информацию, которое может осуществляться путем формирования полей и сигналов с целью нарушения целостности информации или разрушения системы защиты.

Несмотря на простоту структуры разработки КСЗИ, большинство организаций придерживается именно этого алгоритма. Однако данный алгоритм – это лишь основа проектирования. Каждый представленный этап отражает множество уровней в ходе проектирования, в зависимости от структуры АС требования, предъявляемых к ее системе защиты. Рассмотрим эти этапы подробнее на рисунке 1.

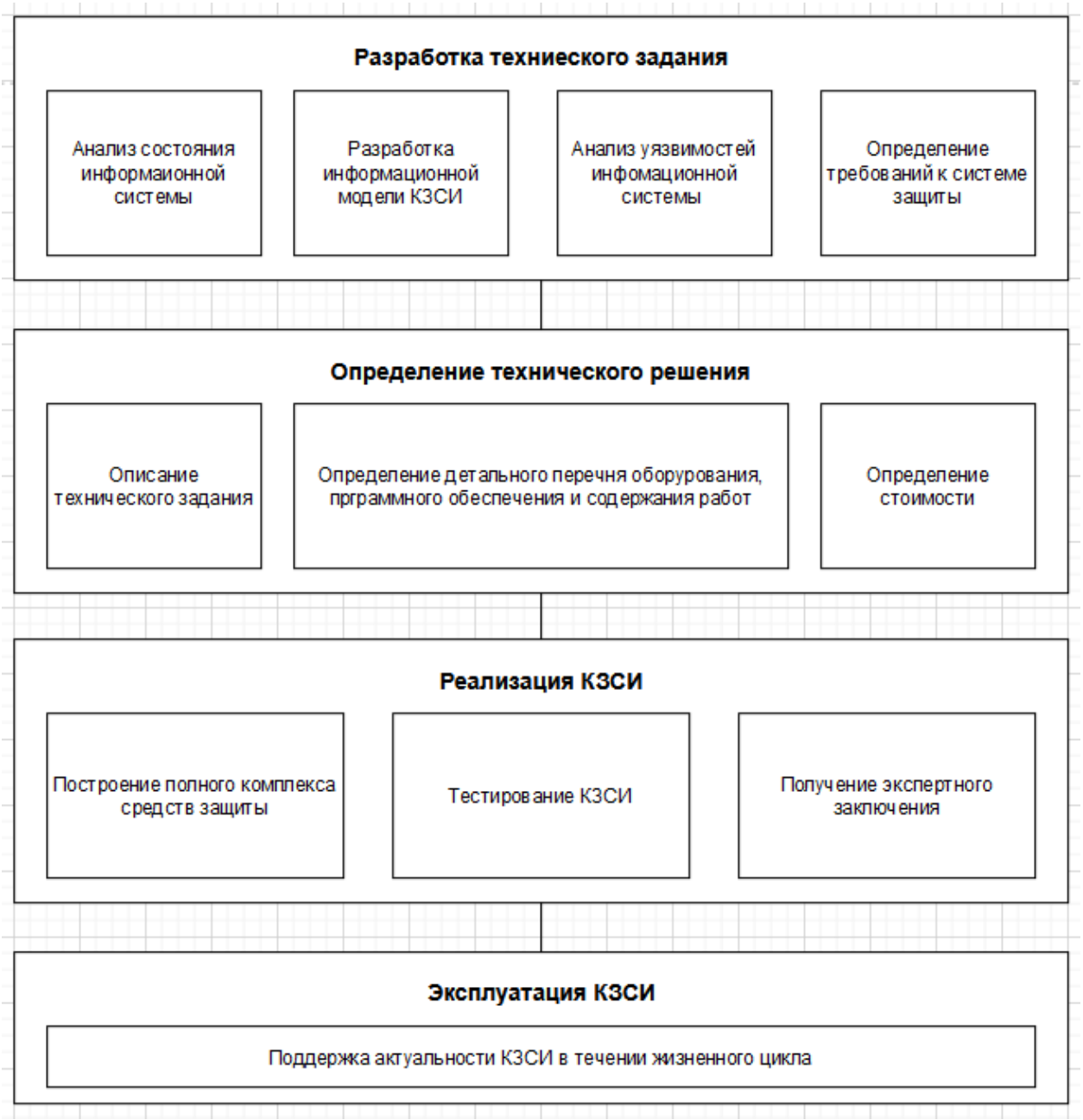

Рисунок 1 – Этапы проектирования комплексной системы защиты информации

1.6 Обзор и сравнение средств управления событиями безопастности

Существует множество средств управления событиями безопасности, но большинство из них имеют определенные недостатки. Рассмотрим некоторые из них [14],[28]:

– Splunk Enterprise Security – мощный инструмент для анализа и управления событиями безопасности, однако его использование требует значительных затрат на обучение и настройку;
– IBM QRadar – также является мощным инструментом, но имеет высокую стоимость и сложность в установке и настройке;
– AlienVault USM – отличается относительно низкой стоимостью и легкостью в использовании, но имеет ограниченный функционал.
– ELK Stack – открытый инструмент сбора и анализа данных, но требует значительных затрат на настройку и поддержку.

В таблице 2 представленно сравнение аналогов. Оценка каждого критерия будет представлена от 1 до 5, где 1 – наименьшая, 5 – наивысшая оценка.

Таблица 2 – Сравнение аналогов

	Splunk Enterprise Security	IBM QRadar	AlienVault USM	ELK Stack
Безопасность	3	4	2	3
Функциональность	5	4	2	4
Стоимость	2	1	5	2
Скорость	4	3	5	3

Таким образом, после проведения сравнительного анализа аналогов, видно, что каждая программа уступает другим программам, поэтому было принято решение делать свою программу для управления событиями

безопасности. Которая могла бы конкурировать и даже превзойти описанные выше аналоги по функциональности, безопастности, скорости и стоимости.

Выводы по разделу 1

В первом разделе ВКР была поставлена задача на исследования, также были описаны основы безопасности информационных систем.

Были рассмотрены существующие методы и средства управления событиями безопасности, где пришли к выводу, что существующие подходы к управлению событиями безопасности предоставляют организациям ряд инструментов и технологий для обнаружения инцидентов безопасности, реагирования на них и восстановления после них. Интегрируя эти подходы, организации могут улучшить свою систему безопасности и уменьшить влияние инцидентов безопасности.

И после проведения сравнительного анализа аналогов, видно, что каждая программа уступает другим программам, поэтому было принято решение делать свою программу для управления событиями безопасности.

2 Проектирование управления событиями безопастности

2.1 Моделирование архитектуры системы

Автоматизированная система управления событиями безопасности (ASEMS) представляет собой сложный программный комплекс, состоящий из нескольких компонентов и модулей. Архитектура системы предназначена для предоставления масштабируемого и гибкого решения для управления событиями безопасности в режиме реального времени. В этом разделе представлен обзор архитектуры ASEMS, включая компоненты, модули и их взаимодействие [16]. На рисунке 2 представлена подсистема управлени и обеспечения защиты информации.

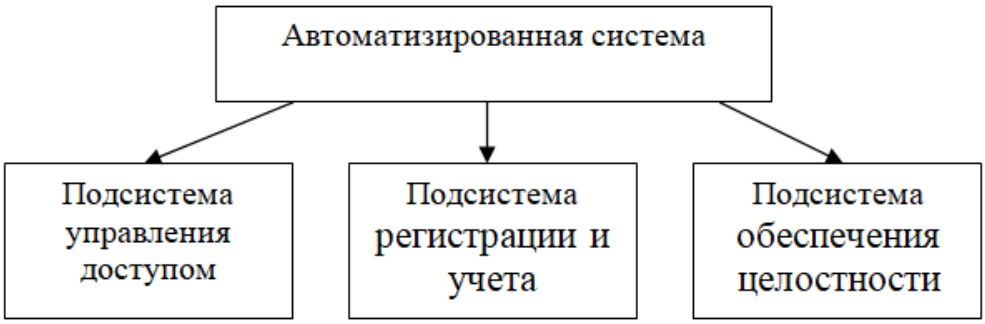

Рисунок 2 – Подсистемы управления и обеспечения защиты информации

Архитектура ASEMS состоит из следующих компонентов:

- источники данных. Это системы и устройства, генерирующие события безопасности, такие как системы обнаружения вторжений, брандмауэры и системы контроля доступа;
- модуль сбора данных. Этот модуль отвечает за сбор событий безопасности из различных источников данных и их сохранение в централизованной базе данных;

- модуль корреляции событий. Этот модуль анализирует собранные события безопасности для выявления шаблонов и взаимосвязей между различными событиями. Он использует различные алгоритмы корреляции для выявления потенциальных угроз безопасности и создания предупреждений;
- модуль управления предупреждениями. Этот модуль отвечает за управление предупреждениями, генерируемыми модулем корреляции событий. Он определяет приоритет предупреждений в зависимости от их серьезности и отправляет уведомления соответствующим сотрудникам службы безопасности;
- модуль отчетности. Этот модуль создает отчеты о событиях безопасности и дает представление о состоянии безопасности организации.; административный модуль. Этот модуль обеспечивает административные функции, такие как управление пользователями, настройка системы и обслуживание.

Модули ASEMS взаимодействуют друг с другом, обеспечивая цельное и интегрированное решение для управления событиями безопасности. Модуль сбора данных собирает события безопасности из различных источников данных и сохраняет их в централизованной базе данных. Модуль корреляции событий анализирует собранные события безопасности для выявления потенциальных угроз безопасности и создает предупреждения. Модуль управления оповещениями приоритизирует оповещения в зависимости от их серьезности и отправляет уведомления соответствующему персоналу службы безопасности. Модуль отчетов создает отчеты о событиях безопасности и предоставляет информацию о состоянии безопасности организации. Административный модуль обеспечивает административные функции, такие как управление пользователями, настройка системы и обслуживание [23].

Для разработки автоматизированной системы управления событиями безопасности требуется надежная система управления качеством и

безопасностью. Архитектура такой системы должна обеспечивать своевременное и эффективное обнаружение, анализ и устранение всех событий безопасности. В этом разделе мы опишем архитектуру системы управления качеством и безопасностью для автоматизированной системы управления событиями безопасности.

Архитектура системы менеджмента качества и безопасности состоит из нескольких компонентов. Эти компоненты включают модуль обнаружения событий безопасности, модуль анализа и разрешения, модуль отчетности и модуль обратной связи.

Модуль обнаружения событий безопасности отвечает за обнаружение событий безопасности в режиме реального времени. Этот модуль предназначен для постоянного мониторинга системы и выявления любых потенциальных угроз безопасности. Модуль должен иметь возможность обнаруживать как известные, так и неизвестные угрозы и отправлять предупреждения модулю анализа и разрешения [11].

Модуль анализа и разрешения отвечает за анализ и устранение событий безопасности. Этот модуль должен иметь возможность анализировать данные о событии и предоставлять решения для разрешения события безопасности. Модуль также должен иметь возможность расставлять приоритеты событий в зависимости от их серьезности и предлагать соответствующие решения.

Модуль отчетов отвечает за формирование отчетов об обнаруженных и устраненных событиях безопасности. В отчетах должен содержаться подробный анализ событий безопасности, включая первопричину, влияние и предпринятые шаги по устранению. Модуль также должен предоставлять показатели производительности системы, такие как количество обнаруженных и устраненных событий и среднее время, затрачиваемое на их устранение.

Модуль обратной связи отвечает за сбор отзывов от пользователей системы. Этот модуль должен предоставить пользователям механизм,

позволяющий сообщать о любых проблемах или вносить предложения по улучшению системы. Модуль также должен иметь механизм мониторинга и реагирования на отзывы, чтобы система постоянно улучшалась.

На рисунке 3 представлена архитектура системы управления качеством и безопасностью для автоматизированной системы управления событиями безопасности.

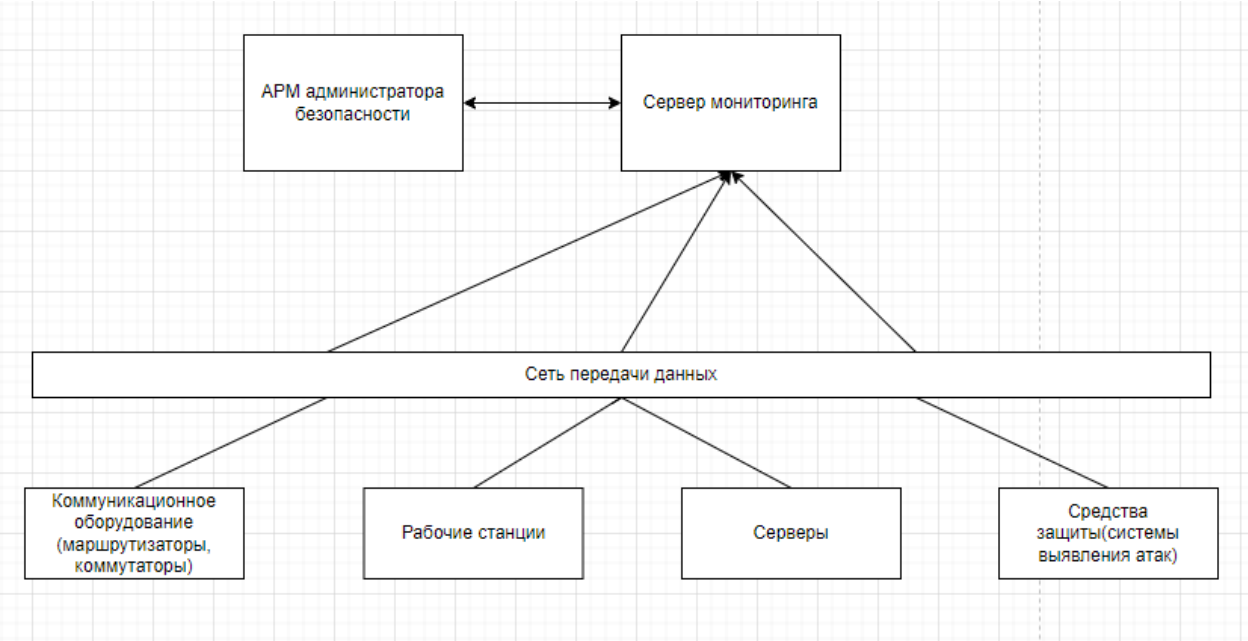

Рисунок 3 – Архитектура системы

Архитектура системы управления качеством и безопасностью для автоматизированной системы управления событиями безопасности имеет решающее значение для обеспечения своевременного и эффективного обнаружения, анализа и устранения всех событий безопасности. Система должна быть спроектирована таким образом, чтобы обнаруживать как известные, так и неизвестные угрозы, приоритизировать события в зависимости от их серьезности, создавать подробные отчеты и собирать отзывы пользователей [30].

2.2 Математический анализ эффективности защитных меропиятий

Система безопасности включает в себя человеческие, материальные и технические ресурсы, которые работают для борьбы с угрозами в определенное время и в определенном пространстве. Пространство угроз определяется объектами, требующими защиты, такими как персонал, активы и конфиденциальная информация.

Основной целью системы безопасности является нейтрализация потенциальных угроз за счет использования передовых технологий и квалифицированного персонала. Каждая угроза представляет собой потенциальный риск, и система безопасности работает так, чтобы минимизировать ущерб и в идеале полностью устранить угрозу, хотя это не всегда возможно. Эффективность системы безопасности необходимо оценивать, измеряя степень ущерба, который она предотвратила [22]. Например, можно измерить относительный ущерб, предотвращенный ею (рисунок 4).

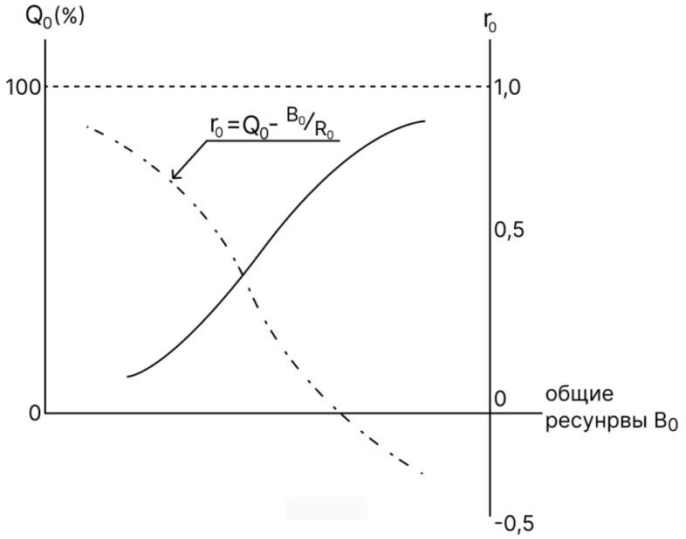

Рисунок 4 – Типичная зависимость эффективности Q_0 и рентабельности r_0 защиты от общих ресурсов

Величина Q_0 – мера общей эффективности защиты. Чем больше Q_0, тем меньший ущерб создадут угрозы. Таким образом, мерой риска является величина $(1 - Q_0)$. Стремление обеспечить высокоэффективную защиту, когда Q_0 близко к 1 (или 100%), вполне естественно, но это потребует значительных расходов на ресурсы. То есть чем выше совокупные ассигнования (B_0) на ресурсы, тем на большую эффективность защиты можно рассчитывать. Возникшая при этом зависимость видна на рис 3. Однако чрезмерные расходы на собственную безопасность не всегда оправданны экономически. Можно столкнуться с ситуацией, когда стоимость защиты (B_0) превысит уровень (R_0) максимального ущерба от реализации угроз. В этом случае возникает опасность угрозы «саморазорения» от защиты. Ее уровень также можно оценить, к примеру, величиной r разности относительного «защищенного» ущерба Q_0 и относительных затрат $\frac{B_0}{Q_0}/$ на ресурсы. Назовем эту величину рентабельностью защиты. Если она положительная (т.е. $B_0 <= P_0 Q_0$), то защита рентабельна. В отличие от эффективности, чем больше затраты (B_0), тем меньше рентабельность. Эта противоположность создает неоднозначную ситуацию в выборе стратегии защиты [1].

Рассмотрим типовую зависимость эффективности защиты (Q_0) и ее рентабельности (r_0) от максимального ущерба R_0. По сути, это является мерой масштабности бизнеса. Нетрудно увидеть, что сделать защиту одновременно и высокоэффективной, и высокорентабельной под силу лишь крупным коммерческим структурам (область G), для которых характерны большие величины максимального ущерба. Достаточно, например, чтобы $B_0 = R_0(l - Q_0)$.Тогда при r→l,Q_0→l. В худшем положении оказываются интересы среднего (область M) и малого (область S) бизнеса, поскольку из-за ограниченности ресурсов выбор стратегии защиты более сложен. Здесь рекомендации просты. Надо обеспечить максимально возможную эффективность при положительном показателе рентабельности защиты. То есть в первую очередь следует противодействовать наиболее вероятным и опасным угрозам. В любом случае

нельзя забывать об экономии ресурсов. Совершенно ясно, что выбор стратегии защиты облегчается, если при меньших затратах удастся обеспечить равную или даже большую эффективность защиты.

Очевидны и источники экономии затрат: использование более экономичных средств и решений универсального характера; рациональное распределение ресурсов и более совершенные формы управления ими; привлечение кооперативных форм обеспечения безопасности и др. Весь этот перечень присущ крупным коммерческим структурам, однако для среднего и малого бизнеса он, к сожалению, существенно сужается. Идеология их системы безопасности должна строиться на рентабельной защите лишь от отдельных видов угроз. В противном случае защита может себя не оправдать. Поэтому надо иметь в виду, что экономии ресурсов в этих условиях будут способствовать кооперативные формы защиты в рамках единой местной или региональной системы безопасности [27].

Выгоду кооперативных форм противодействия угрозам иллюстрирует рисунок 5.

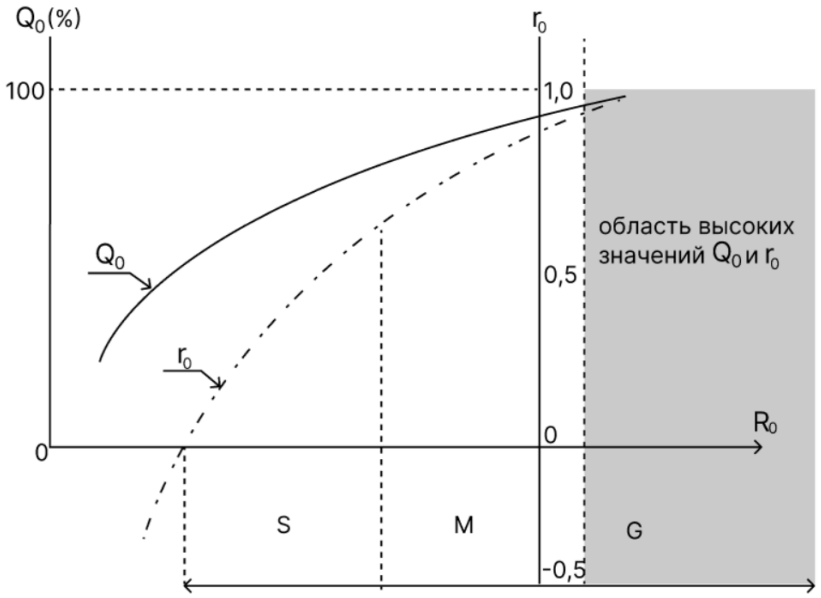

Рисунок 5 – Зависимость эффективности и рентабельности защиты от максимального ущерба R_0

На рисунке 6 представлены характерные зависимости величины риска $R = R_0(1 - Q_0)$ и общих затрат (B_0) на ресурсы от эффективности автономной (I) и кооперативной (II) защиты. Точка пересечения (A_0) зависимостей R(Q) и B(Q) для автономной защиты соответствует примерно области минимальных общих потерь $R_0(1 - Q_0) + B_0$. Экономия ресурсов выразится в том, что исходная зависимость (I) окажется «выше» новой зависимости (II), которая отображает кооперацию в использовании ресурсов. Соответственно новая точка пересечения кривых (A1) окажется правее прежней (A_0). Практически это означает, что при сохранении рентабельности защиты увеличивается ее эффективность. Причем выигрыш тем существенней, чем больше экономия.

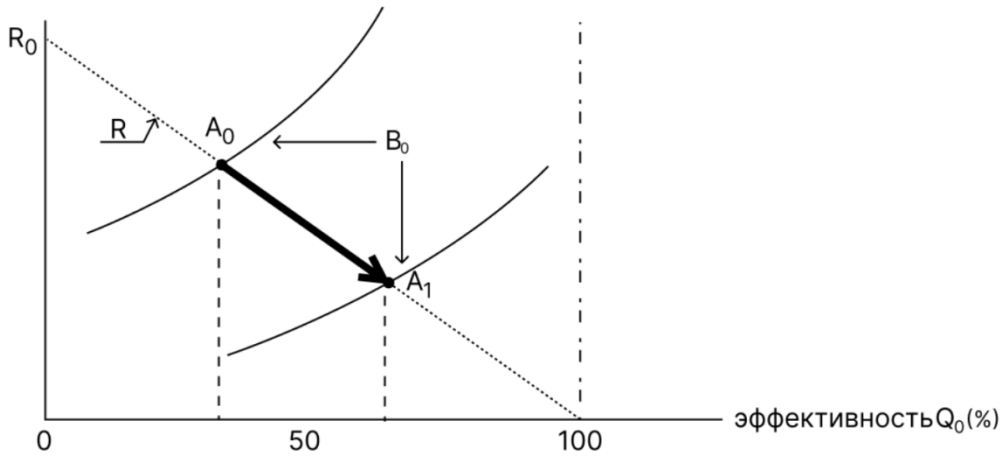

Рисунок 6 – Характерные зависимости риска R и расходов на ресурсы B_0 как функций от эффективности защиты Q_0

На практике в основном кооперируются по двум формам – материально-техническим и кадровым ресурсам, которые и являются составными частями общего. Что касается первой формы, то она характерна для ситуаций, когда пространство угроз не расширяется. Иными словами, объединяются лишь материально-технические средства одного и того же предприятия, но предназначенные для различных целей.

Одним из примеров сложной системы безопасности является защита собственности и информации. Он включает в себя различные инструменты, такие как контроль доступа, системы контрольно-пропускных пунктов и оборудование для пожаротушения [19]. Однако эта форма безопасности практична только для крупного бизнеса. Вторая форма, которая заключается в сотрудничестве с человеческими ресурсами, обычно используется для решения проблем безопасности в конкретном регионе, где зона риска преднамеренно расширена, например, в нескольких коммерческих учреждениях в одном регионе. В таких случаях объединение осуществляется исключительно через группы быстрого реагирования.

Основные выводы и рекомендации очевидны. Одновременное противодействие будет достаточным для высокоэффективной защиты от угрозы, если реакция на нее будет быстрой. Эта задача вполне реальна для объектов большого бизнеса. Кооперативные же формы противодействия в условиях медленной реакции на угрозы не принесут эффекта, если отсутствуют средства задержки и блокирования угроз. Говоря о тактических вопросах системы безопасности бизнеса в части технических каналов связи, прежде всего имеют в виду скорость ее реакции, надежность решений, блокирование развития угроз и их ликвидацию. Особенно важно обеспечить жесткие требования к надежности всех систем защиты, которая зависит от времени их функционирования и периодичности обновления ресурсов. Если это время превышает 5 лет, то требование надежности реализуется несколькими способами, среди которых - резервирование решений, многорубежность защиты, автоматизация первичных решений, централизованное управление ресурсами в кризисных ситуациях и т.п. Прежде чем определиться в вопросах тактики, надо помнить, что она должна соответствовать стратегии и опираться на точный количественный анализ. Для объектов среднего и малого бизнеса такой анализ вполне реален даже без средств автоматизации [25]. Однако необходимо привлечь специалистов и экспертов, которые бы проанализировали обстановку и свойства

защищаемого объекта, разработали модель угроз, изучили рынок существующих средств и методов. Эти данные и помогли бы оценить саму систему и при необходимости модернизировать ее.

2.3 Выбор технологий и инструментов разработки

При разработке автоматизированной системы управления событиями безопасности выбор соответствующих технологий и инструментов имеет решающее значение для создания надежной и эффективной системы. В этом разделе обсуждается выбор технологий и инструментов, которые можно использовать при разработке системы управления качеством и безопасностью для автоматизированной системы управления событиями, связанными с безопасностью.

Технологии и инструменты разработки системы менеджмента качества и безопасности:

– языки программирования. Для разработки автоматизированной системы управления событиями безопасности можно использовать такие языки программирования, как Python, Java, C++ и Ruby [2]. Эти языки имеют мощные библиотеки и фреймворки, которые могут помочь в создании надежной системы;

– системы управления реляционными базами данных (RDBMS). СУРБД, такие как MySQL, PostgreSQL и Oracle, можно использовать для хранения информации о событиях безопасности, инцидентах и журналах. РСУБД позволяет легко управлять данными, извлекать их и манипулировать ими;

– облачные вычисления. Платформы облачных вычислений, такие как AWS и Google Cloud, могут использоваться для размещения автоматизированной системы управления событиями безопасности. Облачные вычисления обеспечивают масштабируемость, гибкость и экономичность;

– инструменты управления информацией и событиями безопасности (SIEM). Инструменты SIEM, такие как Splunk, ELK и IBM QRadar, можно использовать для управления событиями безопасности, централизации данных журналов и выявления угроз безопасности;

– интерфейсы прикладного программирования (API). API-интерфейсы могут быть интегрированы в автоматизированную систему управления событиями безопасности, чтобы обеспечить связь с внешними системами, такими как системы обнаружения вторжений и брандмауэры [21].

Для написания автоматизированной системы управления событиями безопасности будем использовать язык программирования Python и фреймворк Django. Сделаем модель для хранения информации о событиях безопасности (рисунок 7).

```python
from django.db import models

class SecurityEvent(models.Model):
    name = models.CharField(max_length=100)
    description = models.TextField()
    date = models.DateTimeField()
    severity = models.CharField(max_length=20)
    resolved = models.BooleanField(default=False)

    def __str__(self):
        return self.name
```

Рисунок 7 – Модель для хранения информации о событиях безопасности

Затем сделаем представления (views) для отображения информации из этой модели, для вывода списка всех событий безопасности (рисунок 8).

```python
from django.views.generic import ListView
from .models import SecurityEvent

class SecurityEventListView(ListView):
    model = SecurityEvent
    template_name = 'security_event_list.html'
```

Рисунок 8 – Вывод списка всех событий безопастности

Чтобы добавлять новые события безопасности, создадим форму и представление для ее обработки (рисунок 9).

```python
from django.views.generic.edit import CreateView
from django.urls import reverse_lazy
from .models import SecurityEvent

class SecurityEventCreateView(CreateView):
    model = SecurityEvent
    fields = ['name', 'description', 'date', 'severity']
    template_name = 'security_event_form.html'
    success_url = reverse_lazy('security-event-list')
```

Рисунок 9 – Создание формы

Здесь reverse_lazy используется для перенаправления пользователя на страницу со списком всех событий безопасности после добавления нового события.

Также добавляем функциональность для редактирования и удаления событий безопасности, а также защиту от несанкционированного доступа к системе и обработку ошибок.

Для обеспечения безопасного доступа к системе используем встроенную функциональность Django, такую как авторизация и аутентификация пользователей. Для этого используем стандартные представления (views) и шаблоны (templates) Django.

Далее создадим представление для регистрации новых пользователей (рисунок 10).

```
from django.contrib.auth.forms import UserCreationForm
from django.contrib.auth.views import LoginView
from django.urls import reverse_lazy
from django.views.generic.edit import CreateView

class UserRegistrationView(CreateView):
    template_name = 'registration/register.html'
    form_class = UserCreationForm
    success_url = reverse_lazy('login')
```

Рисунок 10 – Регистация пользователей

Здесь UserCreationForm – это встроенная Django-форма для регистрации новых пользователей.

Также сделаем представление для входа в систему, которое представленно ниже, на риунке 11.

```
class UserLoginView(LoginView):
    template_name = 'registration/login.html'

    def get_success_url(self):
        return reverse_lazy('security-event-list')
```

Рисунок 11 – Вход в систему

Здесь LoginView - это встроенное представление Django для входа в систему.

Для обработки ошибок используем функцию handle_exception для обработки исключений. Добавим следующий код в файл views.py, как показано на рисунке 12.

```python
from django.views import View
from django.http import JsonResponse

class ErrorHandlingView(View):
    def dispatch(self, request, *args, **kwargs):
        try:
            return super().dispatch(request, *args, **kwargs)
        except Exception as e:
            return JsonResponse({'error': str(e)})
```

Рисунок 12 – Обработка ошибок

Здесь *dispatch* является методом Django для обработки запросов, а JsonResponse - метод для возврата данных в формате JSON.

При разработке автоматизированной системы управления событиями безопасности также необходимо обеспечить ее безопасность.

Для обеспечения безопасности используем библиотеки для проверки наличия уязвимостей в коде и защиты от атак известных векторов. Используем библиотеку *bandit* для проверки безопасности кода и библиотеку *django-axes* для защиты от атак по протоколу HTTP (рисунок 13).

```python
import bandit
from bandit.core import constants as C

# Задание настроек сканирования безопасности
config = {
    'exclude': [],
}

# Сканирование кода на уязвимости
bandit_results = bandit.run(
    paths=['/path/to/project'],
    config=config,
    profile=C.BASIC_PROFILE
)

# Вывод результатов сканирования
for result in bandit_results['results']:
    print(result)
```

Рисунок 13 – Защита атак по протоколу HTTP

AXES_LOGIN_FAILURE_LIMIT - это количество неудачных попыток входа в систему до временной блокировки, AXES_LOCK_OUT_AT_FAILURE - логическое значение, определяющее, будет ли учетная запись блокироваться или нет, как это сделано на рисунке 14.

```
MIDDLEWARE = [
    # ...
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'axes.middleware.AxesMiddleware',
    # ...
]

AXES_ENABLED = True
AXES_LOGIN_FAILURE_LIMIT = 3
AXES_LOCK_OUT_AT_FAILURE = True
AXES_COOLOFF_TIME = datetime.timedelta(minutes=15)
```

Рисунок 14 – Защита атак по протоколу HTTP

Для логирования информации о событиях безопасности будем использовать встроенный в Django модуль logging. Создаем logger в файле settings.py (рисунок 15).

```
# settings.py
LOGGING = {
    'version': 1,
    'disable_existing_loggers': False,
    'handlers': {
        'file': {
            'class': 'logging.FileHandler',
            'filename': 'Security.log',
        },
    },
    'loggers': {
        'security': {
            'handlers': ['file'],
            'level': 'DEBUG',
        },
    },
}
```

Рисунок 15 –Логирование информации о событиях безопасности

Здесь мы создаем файловый обработчик, который записывает сообщения лога в файл Security.log. Затем мы создаем логгер security и привязываем его к обработчику.

Затем, чтобы записать сообщение в лог, используем логгер, созданный в settings.py, это представлено на рисунке 16.

```python
import logging

logger = logging.getLogger('security')

def handle_security_event(event):
    # обработка события безопасности
    logger.info('Security event occurred: {}'.format(event))
```

Рисунок 16 – Написание сообщение в лог

Создаем логгер security и записываем информацию о событии безопасности с помощью метода info.

Также настраиваем электронную почту или систему уведомлений для получения уведомлений об определенных событиях безопасности.

```python
# settings.py
SECURITY_EMAIL_RECIPIENTS = ['security@example.com']

def handle_security_event(event):
    # обработка события безопасности
    send_mail(
        'Security event occurred',
        'Event: {}'.format(event),
        'security@example.com',
        SECURITY_EMAIL_RECIPIENTS,
        fail_silently=False,
    )
```

Рисунок 17 – Настойка почты для уведомления о событиях безопастности

Приведенный выше код (рисунок 17) использует библиотеки и фреймворк Django для создания автоматизированной системы управления событиями безопасности, и его нужно запускать в контексте Django-приложения. Для запуска кода достаточно запустить Django-приложение.

Выводы по разделу 2

Во втором разделе были рассмотрены методы анализа и сравнения существующих систем, где на основе проведенного анализа были выделены основные требования к разрабатываемой системе управления событиями безопасности, которые были учтены при ее разработке.

Также был проведен математический анализ эффективности защитных меропиятий.

И была описана и разработана автоматизированная система управления событиями безопасности на языке программирования Python и фреймворк Django.

3 Тестирование автоматизированной системы управления событиями безопасности

3.1 Смоделированная атака

После моделирования атаки и действий легитимных пользователей операционной системы, запустим разработанную систему для анализа log-файлов и поиска в них признаков смоделированной атаки.

На рисунке 18 представлен результат обнаруженной атаке APT41.

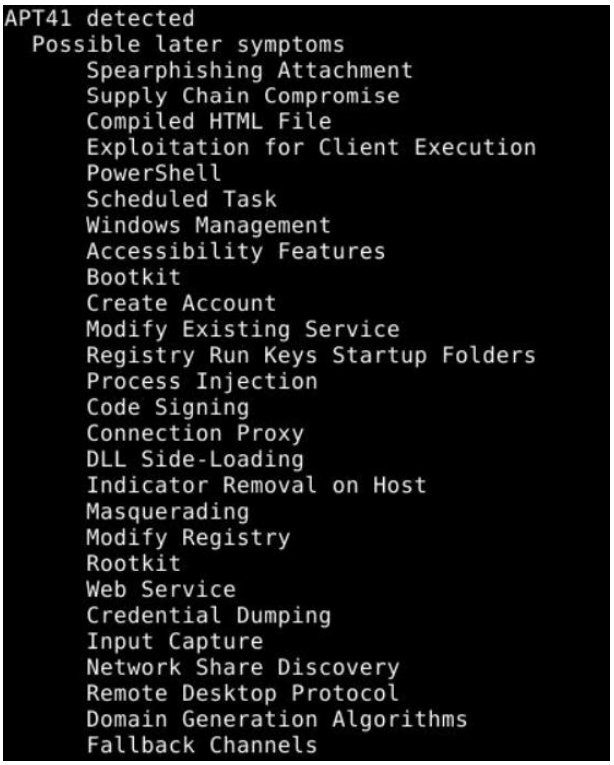

Рисунок 18 – Уведомление об обнаруженной атаке APT41

APT41 — сложная китайская хакерская группа, известная проведением кампаний кибершпионажа и финансовых атак. Группа работает с 2012 года и нацелена на широкий спектр отраслей, включая здравоохранение, телекоммуникации, технологии и игры. APT41 также известен тем, что использует передовые тактики и методы, такие как эксплойты нулевого дня,

специализированные вредоносные программы и атаки на цепочки поставок, для компрометации своих целей. Некоторые известные атаки, приписываемые APT41, включают кражу интеллектуальной собственности у медицинских компаний, компрометацию сетей онлайн-игр для кражи виртуальной валюты и развертывание программ-вымогателей против крупной многонациональной корпорации.

На рисунке 19 представлен результат обнаруженной атаке APT32.

Рисунок 19 – Уведомление об обнаруженной атаке APT32

APT32 известен тем, что использует различные тактики, методы и процедуры (TTP) для проникновения и компрометации своих целей. Некоторые из распространенных методов, используемых APT32, включают атаки целевого фишинга, атаки водопоя и использование пользовательских вредоносных программ и бэкдоров.

Выявление признаков атаки также может помочь вам определить, какой тип атаки происходит, как она осуществляется и какие шаги можно

предпринять для ее предотвращения. Возможность обнаружения признаков атаки является важной частью обеспечения безопасности и целостности ваших систем и сети. На рисунке 20 показано обнаружение атак.

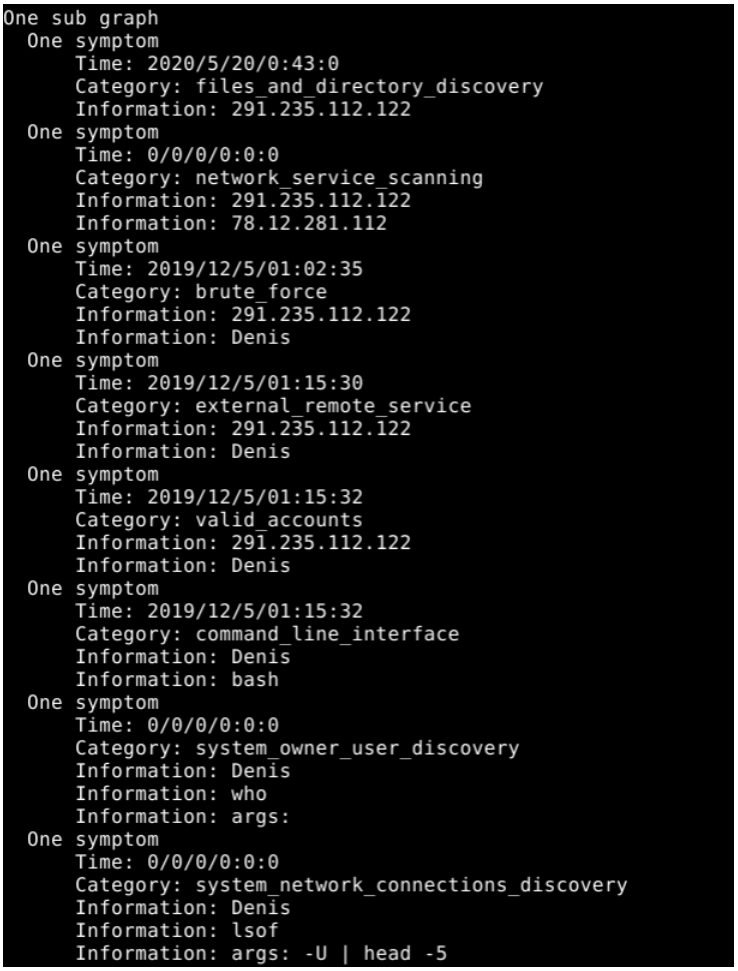

Рисунок 20 – Обнаруженные признаков атаки

На рисунке 21 приведен результат работы обнаруженных признаков атаки.

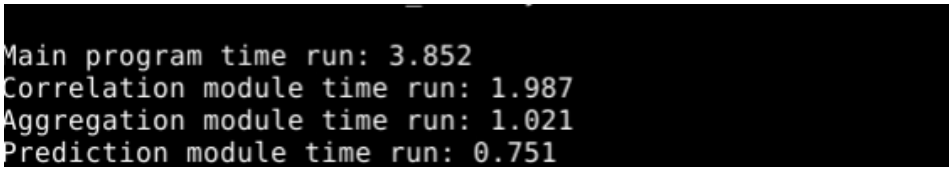

Рисунок 21 – Время работы обнаруженных признаков атаки

На приведенных выше изображениях показано, как система успешно идентифицировала и разработала вектор атаки на основе смоделированных симптомов. Важно отметить, что система мониторинга и управления событиями информационной безопасности предназначена для обнаружения атак на основе определенного количества связанных событий, которое варьируется в зависимости от уровня приоритета, присвоенного каждому событию. Например, если две высокоприоритетные функции обнаруживают взаимосвязь, система создаст уведомление о целевой атаке. Однако если событиям присвоен самый низкий уровень приоритета, уведомление о потенциальном инциденте информационной безопасности будет создано только тогда, когда будет определена связь между набором событий.

3.2 Обнаружения вторжений

Для сравнения, простая система обнаружения вторжений (IDS) будет использоваться для проверки ее способности обнаруживать целевую атаку в сетевом трафике, проходящем через входной узел. В этом моделировании использовалась сетевая IDS/IPS, которая работает на сетевом уровне и может не обнаруживать события информационной безопасности, происходящие на системном уровне [9]. Таким образом, для имитации таких событий будут проводиться различные типы атак:

- External Remote Services (T1133);
- Brute-force;
- Network Service Scanning.

Сканирование портов – это метод, используемый злоумышленниками для выявления открытых портов в целевой системе. Затем открытые порты можно использовать для запуска атаки на систему. Обнаружение сканирования портов – это процесс обнаружения сканирования портов и принятия соответствующих мер для предотвращения атаки.

На рисунке 22 продемонстрирован результат работы системы сканирования портов.

```
06/06/2020-04:41:38.955098  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:254
06/06/2020-04:41:38.956394  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:465
06/06/2020-04:41:38.956480  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:37
06/06/2020-04:41:38.956941  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:481
06/06/2020-04:41:38.957141  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:17
06/06/2020-04:41:38.957343  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:625
06/06/2020-04:41:38.960421  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:512
06/06/2020-04:41:38.962003  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:70
06/06/2020-04:41:38.962273  [**] [1:100985:1] SCAN ports [**] [Classification: Detection of
a Network Scan] [Priority: 3] {TCP} 192.168.1.6:49383 -> 192.168.1.5:1001
```

Рисунок 22 – Детектирование сканирования портов

Атака «полный перебор» – это тип кибератаки, при которой злоумышленник пытается получить несанкционированный доступ к системе, перебирая все возможные комбинации паролей, пока не найдет правильную. Результат обнаружения этой атаки представлен на рисунке 23.

```
06/06/2020-05:25:30.094852  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56702 -> 192.168.1.5:22
06/06/2020-05:25:30.095457  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56710 -> 192.168.1.5:22
06/06/2020-05:25:30.095647  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56710 -> 192.168.1.5:22
06/06/2020-05:25:30.095984  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56712 -> 192.168.1.5:22
06/06/2020-05:25:30.096237  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56712 -> 192.168.1.5:22
06/06/2020-05:25:30.096594  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56714 -> 192.168.1.5:22
06/06/2020-05:25:30.096838  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56710 -> 192.168.1.5:22
06/06/2020-05:25:30.096871  [**] [1:100984:1] SSH brute [**] [Classification: (null)] [Prior
ity: 3] {TCP} 192.168.1.6:56712 -> 192.168.1.5:22
```

Рисунок 23 – Детектирование атаки типа «полный перебор»

Обнаружение авторизации SSH относится к процессу проверки того, авторизован ли пользователь для доступа к удаленному серверу по протоколу SSH (Secure Shell). Обычно это делается для обеспечения безопасности удаленной системы и предотвращения несанкционированного доступа.

Результат проверки показан на рисунке 24.

```
06/06/2020-05:37:56.326576  [**] [1:100983:1] SSH login [**] [Classification: Attempted User
 Privilege Gain] [Priority: 1] {TCP} 192.168.1.6:56722 -> 192.168.1.5:22
06/06/2020-05:37:59.277139  [**] [1:100983:1] SSH login [**] [Classification: Attempted User
 Privilege Gain] [Priority: 1] {TCP} 192.168.1.6:56724 -> 192.168.1.5:22
```

Рисунок 24 – Детектирование авторизации по SSH

На скриншотах выше можно заметить, что IDS успешно обнаружила события ИБ, появившиеся в сетевом трафике, но в отличие от SIEM, IDS не смогла связать их между собой. Для SIEM все эти события равнозначны, и вся работа по поиску взаимосвязей между ними ляжет на плечи администратора информационной безопасности.

Вывод по разделу 3

В последнем разделе ВКР мы запустили и протестировали разработанную систему для анализа log-файлов и поиска в них признаков смоделированной атаки.

Для имитации атаки взяли три типа атак, где пришли к выводу, что IDS успешно обнаружила события ИБ, появившиеся в сетевом трафике, но в отличие от SIEM, IDS не смогла связать их между собой, для SIEM все эти события равнозначны.

Заключение

Бакалаврская работа посвящена разработке автоматизированной системы управления событиями безопасности.

В ходе выполнения ВКР были поставлены задачи на исследования.

Были рассмотрены существующие методы и средства управления событиями безопасности. После проведения сравнительного анализа аналогов, видно, что каждая программа уступает другим программам, поэтому было принято решение делать свою программу для управления событиями безопасности.

Далее были рассмотрены методы анализа и сравнения существующих систем, где на основе проведенного анализа были выделены основные требования к разрабатываемой системе управления событиями безопасности, которые были учтены при ее разработке.

Также был проведен математический анализ эффективности защитных меропиятий.

И была описана и разработана автоматизированная система управления событиями безопасности на языке программирования Python и фреймворк Django.

В последней разделе ВКР, мы запустили и протестировали разработанную систему для анализа log-файлов и поиска в них признаков смоделированной атаки.

Для имитации атаки взяли три типа атак, где пришли к выводу, что IDS успешно обнаружила события ИБ, появившиеся в сетевом трафике, но в отличие от SIEM, IDS не смогла связать их между собой, для SIEM все эти события равнозначны.

Задачи, определённые для достижения цели работы, были выполнены в полном объёме.

Список используемой литературы

1. Агрегация [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Агрегация
2. Алгоритмы справочник / Джодрж Хайнеман, Гэри Поллис, Стэнли Селков.: Orelly, 2017. – 427с
3. APT [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/APT
4. APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник. [Электронный ресурс]. – URL: https://www.ptsecurity.com/ruru/research/analytics/apt-attacks-finance-2019/
5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008.
6. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности от 01.07.2008.
7. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
8. Корреляция информации в SIEM-системах на основе графа связей типов событий / Федорченко А.В., Котенко И.В. // Информационно-управляющие системы – 2018.
9. КОМРАД [Электронный ресурс]. – URL: https://npoechelon.ru/production/65/11174
10. Корреляция SIEM – это просто. Сигнатурные методы [Электронный ресурс]. – URL: https://www.securitylab.ru/analytics/431459.php
11. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 14.02.2008.
12. Методика определения угроз безопасности информации в информационных системах, проект 2015 г.

13. Общие понятия о системах обнаружения и предотвращения вторжений [Электронный ресурс]. – URL: https://habr.com/ru/company/otus/blog/479584/

14. СерчИнформ SIEM [Электронный ресурс]. – URL: https://searchinform.ru/products/siem/

15. Системы мониторинга событий безопасности [Электронный ресурс]. – URL: https://www.anti-malware.ru/security/security-monitoring

16. Что такое APT-атака и как от нее защититься [Электронный ресурс]. – URL: http://www.spy-soft.net/apt-attack/

17. Advanced Persistent Threat(APT). Таргетированные или целевые кибератаки «Развитая устойчивая угроза». [Электронный ресурс]. – URL: http://www.tadviser.ru/a/272878

18. ATT&CK Mapping [Электронный ресурс]. – URL: https://mitreattack.github.io/caret/#/

19. Double Dragon APT41, a dual espionage and cyber crime operation [Электронный ресурс]. – URL: https://content.fireeye.com/apt-41/rpt-apt41

20. FortiSIEM [Электронный ресурс]. – URL: https://www.fortinet.com/ru/products/siem/fortisiem#resources

21. HIDS (Host-based Intrusion Detection System) [Электронный ресурс]. – URL: https://ru.bmstu.wiki/HIDS_(HostBased_Intrusion_Detection_System)

22. Log файлы в Linux по порядку [Электронный ресурс]. – URL: https://habr.com/ru/post/332502/

23. Max Patrol SIEM. Обзор системы управления событиями информационной безопасности [Электронный ресурс]. – URL: https://habr.com/ru/company/tssolution/blog/495280/

24. MaxPatrol SIEM [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/products/mpsiem/

25. McAfee ESM [Электронный ресурс]. – URL: https://www.mcafee.com/enterprise/ru-ru/products/enterprise-ecuritymanager.html

26. MITRE | ATT&CK [Электронный ресурс]. – URL: https://attack.mitre.org/

27. Neomatica [Электронный ресурс]. – URL: https://www.neomatica.com/

28. SIEM: ответы на часто задаваемые вопросы [Электронный ресурс]. – URL: https://habr.com/ru/post/172389/

29. Security Capsule [Электронный ресурс]. – URL: https://www.itb.spb.ru/products/Security_Capsule_SIEM/

30. Suricata как IPS [Электронный ресурс]. – URL: https://habr.com/ru/post/192884/