Департамент образования и науки города Москвы

Государственное бюджетное профессиональное образовательное учреждение города Москвы
«Колледж малого бизнеса № 4»
(ГБПОУ КМБ № 4)

КУРСОВОЙ ПРОЕКТ

по МДК 05.02 Разработка кода информационных систем, МДК 05.03 Тестирование информационных систем

для специальности 09.02.07 Информационные системы и программирование

Базовая подготовка

Тема: Обеспечение безопасности при сопровождении информационных систем

Выполнил(а) студент(ка)

4 курса группы № ИПО-41.21

Бормотов Вадим Дмитриевич
(Фамилия, имя, отчество студента)

Проверил

руководитель курсовой работы

Дрыгваль Валерия Станиславовна

Работа защищена с оценкой

_____

«____» _____2025

Москва, 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире информационные системы играют ключевую роль в деятельности практически любой организации. Они обеспечивают автоматизацию бизнес-процессов, способствуют более эффективному управлению ресурсами и обеспечивают доступ к необходимой информации. Однако с ростом значимости информационных систем возрастает и число угроз, связанных с их безопасностью. В связи с этим обеспечение безопасности при сопровождении информационных систем становится одной из первоочередных задач для любой организации, стремящейся сохранить свою конкурентоспособность, защитить данные и обеспечить непрерывность бизнеса. Актуальность темы обусловлена необходимостью защиты информации от различных угроз, таких как кибератаки, утечки данных, несанкционированный доступ, а также обеспечение соответствия нормативным требованиям и стандартам безопасности.

Целью данной работы является исследование методов и средств обеспечения безопасности при сопровождении информационных систем, а также разработка рекомендаций по повышению их устойчивости к угрозам. В процессе достижения данной цели планируется рассмотреть существующие подходы к обеспечению безопасности, проанализировать основные угрозы и уязвимости, а также изучить возможности использования современных инструментов, таких как платформа Notion, для создания системы документации и управления безопасностью.

Задачи работы включают анализ существующих методов и подходов к обеспечению безопасности информационных систем, изучение нормативно-правовой базы, разработку рекомендаций по повышению уровня безопасности, а также оценку эффективности предложенных мер. Особое внимание будет уделено анализу возможностей Notion как инструмента для управления документацией, а также разработке структуры документации, которая позволит

улучшить процессы сопровождения информационных систем с точки зрения безопасности.

Объектом исследования являются процессы и методы обеспечения безопасности при сопровождении информационных систем, используемые в современных организациях. Эти процессы включают в себя управление доступом, защиту конфиденциальной информации, мониторинг и реагирование на инциденты безопасности, а также использование инструментов для документирования и анализа данных.

Предметом исследования являются методы и средства обеспечения безопасности, а также возможности платформы Notion для создания и управления системой документации в контексте сопровождения информационных систем. Исследование направлено на выявление наиболее эффективных подходов к защите информации и обеспечение соответствия современным требованиям безопасности.

Методы исследования включают анализ существующих научных и практических подходов к обеспечению безопасности, изучение нормативных документов и стандартов, проведение сравнительного анализа инструментов управления документацией, а также разработку и апробацию предложенных решений на практике. Основное внимание будет уделено изучению возможностей Notion для создания системы документации, которая способствует улучшению процессов сопровождения информационных систем.

Практическая значимость данной работы заключается в разработке рекомендаций и решений, которые могут быть применены в реальной практике для повышения уровня безопасности информационных систем. Использование предложенных мер и подходов позволит организациям улучшить защиту данных, повысить эффективность процессов управления безопасностью, а также обеспечить соответствие нормативным требованиям. Внедрение предложенных решений на базе платформы Notion позволит оптимизировать процессы

документирования и управления информацией, что в свою очередь будет способствовать повышению общей устойчивости информационных систем к угрозам безопасности.

1. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

1.1 Основные угрозы и уязвимости информационных систем при их сопровождении

При сопровождении информационных систем организации сталкиваются с широким спектром угроз и уязвимостей, способных привести к утечке данных, сбоям в работе и финансовым потерям. Среди наиболее распространённых угроз можно выделить кибератаки (DDoS, фишинг, вредоносное ПО), внутренние угрозы, ошибки конфигурации и эксплуатационные сбои. Уязвимости могут возникать из-за недостаточной защиты учетных записей, отсутствия обновлений ПО, неправильно настроенных политик безопасности или недостаточного мониторинга событий в системе. Особенно опасны уязвимости «нулевого дня», которые эксплуатируются злоумышленниками до выхода официальных исправлений. Для минимизации рисков необходимо своевременно проводить аудит безопасности, анализировать уязвимости и применять проактивные методы защиты.

Информационная безопасность представляет собой область знаний и практик, направленных на защиту информации от несанкционированного доступа, использования, раскрытия, модификации, уничтожения или нарушения доступности. Основной целью информационной безопасности является обеспечение конфиденциальности, целостности и доступности информации, также известных как триада ЦИА. Конфиденциальность гарантирует, что доступ к информации имеет только тот, кто уполномочен, целостность обеспечивает, что информация остается неизменной и точной, а доступность подразумевает, что данные и ресурсы доступны тогда, когда это необходимо авторизованным пользователям.

Информационная безопасность охватывает широкий спектр понятий, таких как угроза, уязвимость, риск, атака, и контрмера. Угроза — это потенциальное событие или действие, которое может привести к ущербу или

нарушению безопасности информации. Уязвимость представляет собой слабое место в системе, которое может быть использовано угрозой. Риск — это вероятность того, что угроза использует уязвимость для нанесения ущерба. Атака — это намеренное действие, направленное на нарушение безопасности информации. Контрмера — это любое действие или технология, которые используются для предотвращения или смягчения последствий атаки.

Важным аспектом информационной безопасности является управление доступом, которое включает идентификацию, аутентификацию и авторизацию пользователей, а также контроль за их действиями. Безопасное управление доступом минимизирует риски, связанные с несанкционированным использованием информации и систем.

1.2 Методы защиты данных в процессе эксплуатации и обновления информационных систем

Защита данных в процессе сопровождения информационных систем включает в себя комплекс мер, направленных на обеспечение конфиденциальности, целостности и доступности информации. Ключевые методы включают использование шифрования (AES, RSA) для защиты данных при передаче и хранении, резервное копирование для предотвращения потери информации, а также внедрение механизмов контроля доступа (RBAC, ACL) для разграничения прав пользователей. Важную роль играет регулярное обновление программного обеспечения, позволяющее устранять критические уязвимости и снижать вероятность атак. Также активно применяются системы предотвращения утечек данных (DLP), антивирусные решения и средства мониторинга сетевого трафика, позволяющие своевременно обнаруживать и нейтрализовывать угрозы.

При сопровождении информационных систем угрозы безопасности становятся неотъемлемой частью повседневной деятельности. Эти угрозы могут исходить как из внешних, так и из внутренних источников. Внешние угрозы

включают кибератаки, вирусные эпидемии, фишинг и социальную инженерию. К внутренним угрозам можно отнести ошибки сотрудников, умышленные действия инсайдеров или несоблюдение политик безопасности.

Анализ угроз безопасности начинается с выявления потенциальных рисков и их источников. Кибератаки, такие как DDoS (атака распределенного отказа в обслуживании), являются одной из наиболее распространенных форм угроз, которые могут привести к отключению систем и нарушению бизнес-процессов. Вредоносные программы, включая вирусы, черви и трояны, способны инфицировать системы, уничтожать данные или предоставлять злоумышленникам несанкционированный доступ.

Социальная инженерия представляет собой метод манипуляции людьми для получения конфиденциальной информации. Это может включать фишинг, где злоумышленники маскируются под доверенные источники, чтобы обманом получить пароли или другие чувствительные данные. Ошибки и халатность сотрудников также представляют серьезную угрозу, так как могут привести к утечке данных или непреднамеренному нарушению работы систем.

Анализ угроз помогает организациям понять природу и потенциальное влияние этих угроз, что позволяет разработать стратегии для их предотвращения и минимизации ущерба. Это может включать внедрение защитных мер, таких как межсетевые экраны, системы обнаружения вторжений, регулярное обучение сотрудников и тестирование систем на уязвимости.

1.3 Современные подходы к обеспечению информационной безопасности (Zero Trust, Defense in Depth, MFA, SIEM)

Современные концепции кибербезопасности основаны на многоуровневой защите информационных систем и строгом контроле доступа. Подход Zero Trust предполагает, что любая активность в системе потенциально небезопасна, поэтому каждое действие пользователя или приложения должно быть проверено

и аутентифицировано. Defense in Depth (глубокоэшелонированная защита) использует многослойную архитектуру, включающую межсетевые экраны, системы обнаружения атак (IDS/IPS), антивирусы и средства сегментации сети**.** MFA (многофакторная аутентификация) снижает вероятность несанкционированного доступа, требуя подтверждения личности через несколько независимых факторов. SIEM-системы (Security Information and Event Management) позволяют централизованно собирать и анализировать данные о событиях безопасности, помогая выявлять аномалии и быстро реагировать на инциденты. Комплексное использование этих подходов значительно повышает уровень защиты информационных систем.

Современные подходы к обеспечению безопасности информационных систем основываются на интеграции передовых технологий и методологий для создания комплексной системы защиты. Один из таких подходов — это «глубокоэшелонированная защита», которая подразумевает использование нескольких слоев безопасности для создания многопрофильной защиты. Это может включать использование межсетевых экранов, систем обнаружения вторжений, антивирусного программного обеспечения, шифрования данных и управления доступом.

Подход на основе риска стал одной из ключевых методологий в управлении безопасностью. Он включает идентификацию и оценку рисков, связанных с информационными системами, а затем применение мер безопасности, соответствующих уровню риска. Такой подход позволяет организациям сосредоточиться на наиболее значимых угрозах и эффективно использовать ресурсы.

Одна из современных тенденций — это использование машинного обучения и искусственного интеллекта для выявления и предотвращения угроз. Эти технологии способны анализировать большие объемы данных и обнаруживать аномалии, которые могут указывать на потенциальные атаки или

нарушения безопасности. Они позволяют автоматизировать процессы обнаружения угроз и реагирования на них, что значительно повышает эффективность системы безопасности.

Другим важным направлением является использование облачных технологий для обеспечения безопасности. Облачные провайдеры предлагают широкий спектр инструментов для защиты данных, таких как шифрование, управление доступом и мониторинг безопасности. Однако использование облачных сервисов также требует тщательного анализа и управления рисками, связанными с передачей и хранением данных в облачной среде.

Наконец, важной частью современных подходов является постоянное обучение и повышение осведомленности сотрудников. Люди часто являются самым слабым звеном в системе безопасности, поэтому регулярные тренировки и информирование о новых угрозах помогают снизить риск человеческих ошибок и повысить общий уровень безопасности.

1.4 Влияние киберугроз на функционирование информационных систем

Киберугрозы оказывают существенное влияние на работоспособность и безопасность информационных систем, создавая риски для бизнеса и пользователей. Атаки на инфраструктуру могут привести к отказу в обслуживании (DDoS), что делает ресурсы недоступными для пользователей, или к компрометации данных, ставя под угрозу конфиденциальность и репутацию компании. Вредоносные программы, такие как шифровальщики (ransomware), способны зашифровать критически важные файлы, требуя выкуп за их восстановление. Фишинговые атаки, направленные на кражу учетных данных, увеличивают вероятность несанкционированного доступа к системам. Кроме того, современные киберугрозы становятся всё более сложными и автоматизированными, требуя от организаций внедрения передовых механизмов защиты, постоянного мониторинга и оперативного реагирования на инциденты.

Нормативно-правовая база в области информационной безопасности играет ключевую роль в установлении стандартов и требований для защиты информации. В разных странах существуют свои законы и регламенты, направленные на обеспечение безопасности данных, защите персональной информации и соблюдение конфиденциальности.

Одним из основных международных стандартов в области информационной безопасности является ISO/IEC 27001, который устанавливает требования к созданию, внедрению, эксплуатации, мониторингу, поддержанию и совершенствованию системы управления информационной безопасностью (СУИБ). Этот стандарт помогает организациям систематически и последовательно управлять информационной безопасностью.

На уровне Европейского Союза действует Регламент о защите персональных данных (GDPR), который накладывает строгие требования на обработку и защиту персональных данных граждан ЕС. Этот регламент обязывает компании внедрять меры защиты данных и уведомлять о нарушениях безопасности.

В России одним из ключевых нормативных актов является Федеральный закон №152-ФЗ «О персональных данных», который регулирует порядок обработки персональных данных и обязывает организации принимать меры по их защите. Также существует ряд других нормативных документов, таких как Приказ ФСТЭК №17 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Нормативно-правовая база включает также отраслевые стандарты и рекомендации, которые помогают организациям адаптировать общие требования к своим специфическим условиям. Например, банковский сектор следует стандарту PCI DSS для защиты данных о платежных картах.

Таким образом, нормативно-правовая база в области информационной безопасности обеспечивает основу для установления и поддержания высоких стандартов защиты информации, что критически важно для минимизации рисков и обеспечения доверия пользователей и партнеров.

1.5 Обзор нормативных актов и стандартов в области информационной безопасности (ГОСТ, ISO/IEC 27001, NIST, GDPR)

Обеспечение информационной безопасности требует не только внедрения технических мер защиты, но и соблюдения определённых нормативных актов и стандартов, регламентирующих работу с данными, их обработку, хранение и передачу. Эти документы устанавливают требования к защите информации, формируют принципы управления безопасностью и обеспечивают соответствие деятельности организаций современным киберугрозам и регуляторным требованиям. Среди наиболее значимых нормативных актов и стандартов в области информационной безопасности можно выделить ГОСТ, ISO/IEC 27001, NIST и GDPR. Их соблюдение позволяет минимизировать риски утечек данных, атак на информационные системы и правовых последствий, связанных с нарушением требований защиты информации.

ГОСТ представляет собой систему национальных стандартов Российской Федерации, охватывающую различные аспекты защиты информации. В области информационной безопасности применяются несколько ГОСТов, которые регламентируют криптографическую защиту, управление доступом, защиту персональных данных и эксплуатацию защищённых информационных систем. Например, ГОСТ Р 57580-2017 устанавливает требования к обеспечению информационной безопасности финансовых организаций, а ГОСТ Р 50922-96 определяет основные термины и понятия в области защиты информации. Кроме того, существует ГОСТ 34.10-2018, описывающий алгоритмы электронной цифровой подписи, применяемые для обеспечения подлинности передаваемых данных. Соблюдение данных стандартов является обязательным для

государственных структур и рекомендуется для коммерческих организаций, работающих с конфиденциальной информацией.

Одним из наиболее распространённых международных стандартов в области информационной безопасности является ISO/IEC 27001. Этот стандарт разработан Международной организацией по стандартизации (ISO) совместно с Международной электротехнической комиссией (IEC) и представляет собой систему управления информационной безопасностью (СУИБ). Внедрение ISO/IEC 27001 позволяет организациям систематически подходить к защите данных, определяя риски, разрабатывая политики безопасности и проводя постоянный аудит защищённости информационных активов. Сертификация по этому стандарту даёт компаниям конкурентное преимущество на рынке, повышая доверие клиентов и партнёров. Стандарт включает в себя требования к политике безопасности, управлению доступом, мониторингу событий безопасности, управлению инцидентами, резервному копированию и другим аспектам защиты информации. В рамках этого стандарта также предусмотрены механизмы регулярной оценки рисков, что позволяет организациям оперативно реагировать на новые угрозы и изменяющиеся условия работы.

Американский Национальный институт стандартов и технологий (NIST) разрабатывает рекомендации по информационной безопасности, широко применяемые не только в США, но и в других странах. Документы NIST используются в различных отраслях, включая государственные учреждения, коммерческие компании и исследовательские организации. Одним из ключевых документов является NIST Cybersecurity Framework (CSF), который предлагает универсальный подход к управлению рисками в области информационной безопасности. Этот документ включает пять основных функций: идентификация угроз, защита, обнаружение инцидентов, реагирование на угрозы и восстановление после атак. Кроме того, NIST Special Publication 800-53 устанавливает требования к безопасности федеральных информационных

систем и рекомендует меры защиты для различных уровней рисков. Документы NIST активно применяются в банковской сфере, промышленности и других секторах, где необходимо обеспечить высокий уровень защиты данных.

Одним из самых строгих нормативных актов в области информационной безопасности является Общий регламент по защите данных (GDPR), действующий на территории Европейского союза. Этот регламент устанавливает жёсткие требования к обработке и защите персональных данных граждан ЕС, а также налагает серьёзные штрафные санкции за их нарушение. GDPR требует от организаций внедрения механизмов защиты конфиденциальной информации, обеспечения прозрачности обработки данных и получения явного согласия пользователей на сбор и использование их персональной информации. Компании, работающие на международном рынке и обрабатывающие данные граждан ЕС, обязаны соблюдать этот регламент, вне зависимости от их географического расположения. В случае утечки данных или нарушения требований безопасности организации могут быть оштрафованы на сумму до 20 миллионов евро или 4% от их годового оборота. Внедрение GDPR требует от компаний пересмотра своих подходов к безопасности, усиления контроля за обработкой данных и внедрения механизмов шифрования, анонимизации и строгой аутентификации пользователей.

Соблюдение нормативных актов и стандартов в области информационной безопасности становится неотъемлемой частью работы организаций, стремящихся защитить свои информационные активы и избежать юридических последствий, связанных с утечками данных. Внедрение стандартов, таких как ГОСТ, ISO/IEC 27001, NIST и GDPR, позволяет выстроить эффективную систему защиты, минимизировать риски кибератак и обеспечить соответствие требованиям регуляторов. Кроме того, использование международных стандартов способствует повышению уровня доверия клиентов и партнёров, улучшает конкурентные позиции компании и снижает вероятность финансовых

потерь из-за инцидентов безопасности. С каждым годом требования к информационной безопасности становятся всё более строгими, и организациям необходимо постоянно совершенствовать свои методы защиты, адаптируясь к новым вызовам цифровой эпохи.

2. ИССЛЕДОВАТЕЛЬСКИЙ РАЗДЕЛ

2.1 Анализ актуальных киберугроз и их влияние на сопровождение ИС

Современные киберугрозы становятся всё более сложными и динамичными, что создаёт серьёзные риски для сопровождения информационных систем. Основные угрозы включают вредоносное программное обеспечение (вирусы, трояны, шифровальщики), атаки на уязвимости программного обеспечения, DDoS-атаки, утечки данных, фишинговые атаки и эксплуатацию инсайдерских угроз. Наибольшую опасность представляют атаки с использованием уязвимостей «нулевого дня», когда злоумышленники находят слабые места в системах ещё до выхода официальных исправлений. Фишинг остаётся одним из самых распространённых методов компрометации корпоративных учётных записей, что может привести к несанкционированному доступу и утечке конфиденциальных данных. DDoS-атаки способны парализовать работу серверов и сервисов, делая их недоступными для пользователей, что особенно критично для организаций, предоставляющих онлайн-услуги. Для эффективного сопровождения ИС необходимо учитывать актуальные угрозы и адаптировать системы защиты в соответствии с новыми вызовами, обеспечивая постоянный мониторинг и быструю реакцию на инциденты.

Организация безопасного сопровождения информационных систем является комплексной задачей, требующей применения различных методов и подходов для защиты данных и обеспечения устойчивости систем к внешним и внутренним угрозам. В современной практике существует несколько ключевых методов, направленных на создание и поддержание безопасной среды для информационных систем.

Одним из распространенных методов является использование многоуровневой системы защиты, которая предполагает создание нескольких слоев безопасности. Эти слои включают физическую защиту серверов и устройств, сетевую безопасность, защиту приложений и данных, а также меры по обеспечению безопасности на уровне пользователя. Такой подход позволяет минимизировать вероятность проникновения злоумышленников на всех уровнях системы.

Другим важным методом является регулярное обновление программного обеспечения и систем. Обновления устраняют выявленные уязвимости, тем самым снижая риск атак. Это особенно важно в условиях постоянного появления новых угроз и методов взлома. Внедрение систем управления уязвимостями позволяет автоматизировать процесс поиска и устранения слабых мест в системе.

Методы мониторинга и анализа сетевого трафика играют важную роль в обеспечении безопасности. Использование средств анализа логов и мониторинга в реальном времени позволяет своевременно обнаруживать и реагировать на подозрительные действия, предотвращая возможные атаки. Такие инструменты помогают выявить попытки несанкционированного доступа и другие аномалии, которые могут указывать на угрозы.

Обучение сотрудников также является ключевым методом обеспечения безопасности. Люди остаются одним из самых уязвимых звеньев в системе защиты, поэтому регулярное обучение и повышение осведомленности о безопасности помогают снизить риски, связанные с человеческим фактором. Сотрудники должны быть обучены правильному обращению с конфиденциальной информацией, распознаванию фишинговых атак и другим видам угроз.

Таким образом, анализ существующих методов показывает, что для эффективного сопровождения информационных систем необходимо использовать комплексный подход, включающий технические,

организационные и человеческие факторы. Это позволяет создать надежную систему защиты, способную противостоять современным вызовам в области информационной безопасности.

2.2 Определение ключевых требований к системе защиты данных

Создание эффективной системы защиты данных требует соблюдения ряда ключевых требований, направленных на обеспечение конфиденциальности, целостности и доступности информации. Важнейшим аспектом является многоуровневая система безопасности, которая включает в себя механизмы шифрования данных, разграничение прав доступа, мониторинг событий и управление инцидентами. Одним из ключевых требований является применение строгой аутентификации пользователей, включая многофакторную аутентификацию (MFA), что снижает вероятность несанкционированного доступа. Также необходимо реализовать контроль доступа на основе ролей (RBAC) и ограничить привилегии пользователей, чтобы минимизировать риски злоупотребления полномочиями. Важную роль играет резервное копирование данных с возможностью быстрого восстановления информации в случае сбоя или атаки. Кроме того, системы защиты должны соответствовать международным и национальным стандартам безопасности, таким как ISO/IEC 27001 и GDPR, что обеспечивает соблюдение регуляторных требований и повышает доверие со стороны клиентов и партнёров.

Notion представляет собой универсальный инструмент для создания и управления документацией, который может быть эффективно использован в контексте обеспечения безопасности информационных систем. Основным преимуществом Notion является его гибкость и широкие возможности по структурированию данных, что позволяет адаптировать платформу под специфические нужды любой организации.

Один из ключевых аспектов использования Notion для создания системы документации заключается в его способности объединять различные типы

информации в одном месте. Это может быть текстовая документация, таблицы, списки задач, медиафайлы и другие элементы, которые могут быть связаны друг с другом для обеспечения целостной картины. Такая интеграция упрощает процесс управления информацией и делает доступ к ней более удобным для пользователей.

Важным преимуществом Notion является возможность настройки прав доступа для различных пользователей. Это позволяет ограничивать доступ к конфиденциальной информации и обеспечивать, чтобы только уполномоченные лица могли вносить изменения или просматривать определенные разделы документации. Такая функция особенно важна для безопасности, так как помогает контролировать, кто и как взаимодействует с информацией.

Еще одной значимой возможностью Notion является функция ведения истории изменений и управления версиями документов. Это обеспечивает прозрачность в работе с документацией и позволяет отслеживать, кто и когда вносил изменения, а также восстанавливать предыдущие версии в случае необходимости. Это полезно для аудита и анализа изменений, связанных с обеспечением безопасности.

Интерфейс Notion интуитивно понятен и прост в использовании, что снижает порог вхождения для новых пользователей и позволяет быстро освоить основные функции. Это облегчает процесс внедрения системы в организацию и способствует более эффективному использованию платформы для управления документацией по безопасности.

Таким образом, исследование возможностей Notion показывает, что данный инструмент обладает всеми необходимыми функциями для создания эффективной системы документации в контексте обеспечения безопасности информационных систем. Его гибкость, удобство использования и возможности по управлению доступом делают его ценным ресурсом для организаций,

стремящихся улучшить свои процессы документирования и защиты информации.

2.3 Выбор инструментов и технологий для обеспечения безопасности (антивирусные средства, DLP-системы, IDS/IPS, VPN, PKI)

Для защиты информационных систем от различных видов угроз используются специализированные инструменты и технологии, которые позволяют обнаруживать, предотвращать и минимизировать риски атак. Антивирусные средства обеспечивают базовую защиту от вредоносного ПО, но для более комплексного подхода применяются DLP-системы (Data Loss Prevention), предотвращающие утечку конфиденциальной информации за счёт мониторинга и фильтрации данных. IDS/IPS (Intrusion Detection and Prevention Systems) играют важную роль в обнаружении и предотвращении несанкционированных вторжений в сеть, анализируя трафик и выявляя аномалии в поведении пользователей и процессов. Для обеспечения безопасности передаваемых данных активно используются VPN (Virtual Private Network), создающие защищённые каналы связи и минимизирующие риски перехвата информации. PKI (Public Key Infrastructure) применяется для управления цифровыми сертификатами и аутентификации пользователей, что особенно актуально для корпоративных сетей и облачных решений. Комплексное использование данных инструментов позволяет создать многоуровневую систему защиты, обеспечивающую высокую степень безопасности данных при сопровождении ИС.

Разработка требований к системе безопасности при сопровождении информационных систем — это критически важный процесс, который определяет основу для защиты данных и ресурсов организации. Эти требования должны учитывать специфические угрозы и риски, связанные с деятельностью компании, а также соответствовать актуальным стандартам и нормативам в области информационной безопасности.

Одним из первоочередных требований является обеспечение конфиденциальности информации. Это предполагает внедрение мер по защите данных от несанкционированного доступа, что может включать шифрование данных, использование защищенных каналов связи и настройку строгих политик доступа. Конфиденциальность данных особенно важна для информации, связанной с персональными данными клиентов, финансовыми операциями и стратегическими планами компании.

Не менее важным требованием является обеспечение целостности данных, что означает предотвращение несанкционированных изменений или уничтожения информации. Для этого внедряются системы контроля доступа, журналирования операций и регулярного резервного копирования данных. Эти меры помогают обнаружить и предотвратить попытки модификации данных со стороны злоумышленников.

Требование доступности информации заключается в обеспечении постоянного и бесперебойного доступа к данным для авторизованных пользователей. Это включает в себя разработку стратегий резервного копирования и восстановления данных, а также защиту от атак типа отказ в обслуживании (DDoS), которые могут нарушить работу системы. Обеспечение доступности данных критически важно для поддержки бизнес-процессов и минимизации простоев.

Кроме того, система безопасности должна быть адаптируемой и гибкой, чтобы реагировать на новые угрозы и изменяющиеся условия. Это требует регулярного обновления программного обеспечения, внедрения новых технологий защиты и проведения регулярных аудитов безопасности. Разработка требований должна включать процедуры мониторинга и анализа угроз, а также механизмы быстрого реагирования на инциденты.

Таким образом, требования к системе безопасности должны быть комплексными и учитывать все аспекты защиты информации. Это обеспечивает надежную защиту данных и ресурсов организации от возможных угроз и рисков.

2.4 Разработка модели угроз и рисков для сопровождаемой ИС

Разработка модели угроз и рисков является неотъемлемой частью обеспечения безопасности информационной системы, так как позволяет идентифицировать возможные угрозы, оценить их влияние и выработать стратегии защиты. В процессе моделирования угроз анализируются потенциальные векторы атак, такие как социальная инженерия, эксплуатация уязвимостей, атаки на сети и системы хранения данных. Для каждой угрозы определяется уровень риска, который рассчитывается исходя из вероятности её реализации и возможных последствий. Используются такие методы анализа рисков, как метод STRIDE, основанный на классификации угроз по шести категориям (подмена личности, подделка данных, отказ в обслуживании и др.), а также метод OCTAVE, который фокусируется на бизнес-рисках и их влиянии на организацию. На основе полученных данных разрабатываются меры защиты, включая внедрение средств мониторинга, механизмов обнаружения атак и политик управления безопасностью. Эффективная модель угроз и рисков позволяет минимизировать потенциальные угрозы и создать надежную систему сопровождения ИС, устойчивую к современным кибератакам.

Методология оценки эффективности системы безопасности является важным инструментом для проверки и повышения уровня защиты информационных систем. Эффективная оценка позволяет выявить слабые места в системе, определить уровень защищенности данных и разработать меры по улучшению безопасности.

Одним из основных подходов к оценке эффективности является проведение анализа рисков. Этот метод включает в себя идентификацию потенциальных угроз и уязвимостей, оценку вероятности их возникновения и

возможных последствий для системы. На основе этого анализа разрабатываются меры по снижению рисков и усилению защиты.

Тестирование на проникновение, или пентестинг, является еще одним важным элементом методологии оценки. Это процесс имитации атак на систему с целью выявления уязвимостей и оценки ее устойчивости к различным типам угроз. Результаты пентестинга помогают определить, насколько хорошо система способна противостоять реальным атакам и какие меры необходимо принять для улучшения ее безопасности.

Кроме того, оценка эффективности системы безопасности может включать анализ журналов и отчетов о событиях, что позволяет отслеживать подозрительные действия и выявлять закономерности, которые могут указывать на угрозы. Это помогает своевременно реагировать на инциденты и предотвращать их повторное возникновение.

Оценка соответствия требованиям стандартов безопасности, таких как ISO/IEC 27001, также является важной частью методологии. Это помогает убедиться, что система соответствует международным стандартам и лучшим практикам в области безопасности, что способствует повышению доверия со стороны клиентов и партнеров.

Таким образом, методология оценки эффективности системы безопасности должна быть многогранной и включать различные методы и подходы для обеспечения всесторонней проверки и улучшения уровня защиты информационных систем.

2.5 Построение схемы безопасного администрирования информационной системы.

Построение схемы безопасного администрирования информационной системы является важнейшим аспектом обеспечения её устойчивости к кибератакам, защите данных и предотвращению несанкционированного доступа.

Администрирование включает в себя управление пользователями, настройку прав доступа, контроль за изменениями в системе, мониторинг событий безопасности и применение эффективных механизмов аутентификации. Грамотно выстроенная схема администрирования позволяет минимизировать риски, связанные с человеческим фактором, техническими уязвимостями и вредоносными атаками, обеспечивая стабильную работу информационной инфраструктуры.

Первым этапом построения схемы безопасного администрирования является определение ролей и уровней доступа пользователей. В современных информационных системах используется модель управления доступом, основанная на ролях (RBAC), которая позволяет разграничивать полномочия пользователей в зависимости от их обязанностей и необходимости взаимодействия с определёнными ресурсами. Каждый сотрудник должен иметь доступ только к тем данным и сервисам, которые необходимы для выполнения его профессиональных задач. Разграничение прав доступа особенно важно в крупных организациях, где существует множество отделов и подразделений, работающих с различными уровнями конфиденциальности информации.

Другим ключевым элементом безопасного администрирования является централизованное управление учетными записями и аутентификацией. Для этого применяются специализированные системы, такие как Active Directory, LDAP или Kerberos, позволяющие централизованно управлять пользователями, их паролями и уровнями доступа. Одним из важных аспектов является внедрение многофакторной аутентификации (MFA), которая снижает вероятность компрометации учетных записей за счёт дополнительного уровня защиты. Например, для доступа к критически важным системам может потребоваться не только ввод пароля, но и подтверждение через мобильное приложение, одноразовый код или биометрическую аутентификацию.

Безопасное администрирование информационной системы также предполагает тщательный контроль за изменениями в её конфигурации. Для этого используются системы управления изменениями (Change Management), которые фиксируют любые модификации в параметрах работы серверов, программного обеспечения и баз данных. Такой подход позволяет предотвращать случайные ошибки администраторов, а также выявлять возможные попытки саботажа или несанкционированного вмешательства в работу системы. Контроль версий конфигурации и автоматизированные механизмы отката изменений позволяют быстро восстановить работоспособность системы в случае выявления проблем.

Мониторинг событий безопасности является ещё одним важным компонентом схемы безопасного администрирования. Для этого применяются системы централизованного сбора и анализа логов, такие как SIEM (Security Information and Event Management), которые позволяют отслеживать подозрительную активность и оперативно реагировать на инциденты. Логи должны храниться в неизменяемом виде в течение длительного времени, что позволяет проводить ретроспективный анализ атак и выявлять закономерности в поведении злоумышленников. Помимо автоматического анализа, администраторы должны регулярно проводить аудит логов и анализировать отчёты о безопасности, что позволяет выявлять потенциальные угрозы и уязвимости ещё до их эксплуатации.

Для повышения уровня безопасности администрирования необходимо реализовать механизм сегментирования сети и изоляции критически важных сервисов. Администраторские учетные записи должны использоваться исключительно в защищённых сегментах сети, доступ к которым ограничен для обычных пользователей. Это предотвращает возможность компрометации административных привилегий в случае успешной атаки на обычную учетную запись. Кроме того, использование выделенных рабочих станций для

администраторов, которые не имеют доступа к интернету и сторонним ресурсам, позволяет минимизировать риски заражения вредоносным ПО.

Особое внимание должно уделяться управлению обновлениями и патчами программного обеспечения. Устаревшие версии операционных систем, приложений и драйверов могут содержать критические уязвимости, которые активно эксплуатируются злоумышленниками. Для предотвращения подобных угроз необходимо внедрять централизованные системы управления обновлениями, такие как WSUS или SCCM, которые позволяют автоматически развертывать исправления и обновления на всех узлах информационной системы. Администраторы должны регулярно проводить аудит установленных версий ПО и тестировать обновления в изолированной среде перед их массовым развертыванием.

Эффективное администрирование невозможно без строгих политик безопасности, регулирующих работу с конфиденциальными данными, паролями и удалённым доступом. Важным аспектом является применение политики минимизации привилегий, согласно которой каждому пользователю и администратору предоставляются только те права, которые необходимы для выполнения их непосредственных обязанностей. Доступ к критически важным ресурсам должен предоставляться на временной основе, а привилегированные учетные записи должны использоваться только при необходимости и контролироваться системой журналирования событий.

В современном мире администрирование информационных систем всё чаще включает работу с облачными технологиями, что требует дополнительных мер защиты. Использование облачных сервисов (SaaS, PaaS, IaaS) предполагает разграничение доступа между различными пользователями и внедрение специализированных инструментов мониторинга облачной инфраструктуры. Одним из таких инструментов является Cloud Access Security Broker (CASB),

который позволяет контролировать взаимодействие пользователей с облачными ресурсами, предотвращая утечку данных и несанкционированный доступ. Кроме того, рекомендуется использовать аппаратные модули безопасности (HSM) для хранения криптографических ключей и повышения защищенности аутентификации в облачных средах.

Обучение персонала и администраторов играет ключевую роль в обеспечении безопасности информационной системы. Даже самая сложная защита может быть сведена к нулю из-за человеческого фактора, поэтому важно регулярно проводить тренинги и учения по реагированию на инциденты безопасности. Администраторы должны быть осведомлены о современных методах атак, таких как фишинг, социальная инженерия и эксплуатация уязвимостей, а также уметь оперативно реагировать на угрозы. Кроме того, важно внедрять практику ротации паролей и периодически пересматривать политики безопасности, адаптируя их к новым киберугрозам.

Таким образом, построение схемы безопасного администрирования информационной системы требует комплексного подхода, включающего управление доступом, мониторинг событий, контроль изменений, обновление ПО, сегментирование сети и обучение персонала. Только интеграция всех этих компонентов позволяет создать устойчивую систему защиты, способную противостоять современным угрозам и обеспечивать стабильную работу информационной инфраструктуры.

3. ПРАКТИЧЕСКИЙ РАЗДЕЛ

3.1 Разработка и настройка системы защиты для информационной системы

Создание эффективной системы защиты информационной системы включает комплекс мероприятий, направленных на предотвращение утечек данных, защиту от несанкционированного доступа и минимизацию рисков кибератак. Первым шагом является анализ существующих угроз и уязвимостей, позволяющий определить наиболее критические точки защиты. Далее разрабатывается архитектура системы безопасности, включающая механизм аутентификации и авторизации пользователей, защиту каналов передачи данных, настройку межсетевых экранов и систем предотвращения вторжений. Большое внимание уделяется защите хранимых данных, включая шифрование, резервное копирование и контроль доступа. Немаловажным аспектом является регулярное обновление программного обеспечения, позволяющее своевременно устранять обнаруженные уязвимости. Настройка системы защиты требует тщательного тестирования всех её компонентов, чтобы убедиться в их работоспособности и соответствии требованиям безопасности. В результате правильно настроенная система защиты становится основой для безопасного функционирования информационной системы, обеспечивая её устойчивость к внешним и внутренним угрозам.

Разработка структуры документации в Notion — это важный этап создания системы, которая будет использоваться для обеспечения безопасности при сопровождении информационных систем. Основная цель разработки структуры документации заключается в упрощении доступа к информации, систематизации знаний и обеспечении актуальности данных, которые касаются мер безопасности. В Notion создание структуры документации начинается с определения основных категорий и разделов, которые будут использоваться для организации информации. В рамках обеспечения безопасности важно

предусмотреть такие разделы, как политики безопасности, процедуры реагирования на инциденты, инструкции для пользователей и руководства по использованию систем.

Каждый раздел должен быть продуман с точки зрения логической структуры и взаимосвязей между элементами. Например, разделы могут быть организованы по уровням доступа или типам угроз, что позволит пользователям быстро находить необходимую информацию. В Notion можно использовать страницы и подстраницы, что позволяет создать многоуровневую структуру, обеспечивающую гибкость и удобство использования. Кроме того, использование тегов и ссылок между страницами способствует улучшению навигации и позволяет пользователям легко переходить между связанными темами.

Для обеспечения актуальности данных важно внедрить процедуры регулярного обновления информации. В Notion можно настроить напоминания и уведомления о необходимости обновления определенных документов, а также использовать историю изменений для отслеживания и контроля за актуализацией данных. Таким образом, структура документации в Notion должна быть интуитивно понятной, легко обновляемой и адаптированной под специфические потребности организации.

3.2 Реализация механизма контроля доступа (RBAC, ACL, 2FA/MFA)

Контроль доступа играет ключевую роль в обеспечении безопасности информационных систем, так как он определяет, какие пользователи и в каком объёме могут взаимодействовать с ресурсами системы. Одним из наиболее распространённых методов является ролевая модель доступа (RBAC), при которой пользователи получают доступ на основе своей роли в организации. Это позволяет централизованно управлять привилегиями и снижать риски неправомерного использования данных. Другая модель — ACL (Access Control List) — предоставляет более гибкие настройки, позволяя устанавливать

конкретные права доступа к отдельным объектам системы. Дополнительно для повышения уровня защиты применяется двухфакторная или многофакторная аутентификация (2FA/MFA), требующая от пользователей не только ввода пароля, но и подтверждения личности через одноразовый код, биометрические данные или аппаратный ключ. Такой подход значительно снижает вероятность компрометации учётных записей и защищает систему от атак, связанных с подбором паролей или утечками данных. Настройка и регулярная проверка механизмов контроля доступа позволяют обеспечить высокий уровень безопасности и минимизировать потенциальные угрозы.

Реализация системы управления доступом к документации является критически важным элементом в обеспечении безопасности информационных систем. В Notion существует ряд возможностей для настройки доступа, которые позволяют ограничивать и контролировать доступ к различным разделам документации в зависимости от ролей пользователей и их уровня полномочий. При разработке системы управления доступом необходимо учитывать принцип минимизации прав, что подразумевает предоставление пользователям только тех прав, которые необходимы для выполнения их служебных обязанностей.

Настройка доступа в Notion может быть реализована через управление участниками рабочей области и настройку прав доступа для отдельных страниц или разделов. Это позволяет создавать группы пользователей с различными уровнями доступа, начиная от общего доступа для чтения и заканчивая правами на редактирование или удаление контента. Важно продумать и документировать процедуры по созданию и удалению пользователей, а также назначению и изменению их прав доступа.

Кроме того, для повышения уровня безопасности рекомендуется использовать двухфакторную аутентификацию, которая добавляет дополнительный уровень защиты при входе в систему. Регулярный аудит доступа и проверка соответствия прав пользователей их текущим ролям также

являются важными аспектами системы управления доступом. Таким образом, эффективная система управления доступом должна быть гибкой, легко настраиваемой и обеспечивать высокий уровень защиты данных.

3.3 Настройка мониторинга событий безопасности и журналирования

Эффективный мониторинг событий безопасности позволяет оперативно выявлять подозрительную активность и предотвращать атаки на информационные системы. Для этого применяются системы сбора и анализа логов, такие как SIEM (Security Information and Event Management), которые централизуют данные о событиях и анализируют их на предмет аномального поведения. Важно настраивать журналирование всех критически важных действий, включая попытки входа, изменения конфигурации, доступ к конфиденциальным данным и сетевые соединения. Мониторинг также охватывает использование IDS/IPS-систем, которые отслеживают сетевой трафик и выявляют признаки вторжений. Внедрение автоматизированных механизмов оповещения позволяет администраторам мгновенно реагировать на инциденты, предотвращая возможные атаки. Журналы событий должны храниться в надёжном хранилище с ограниченным доступом, что исключает возможность их подмены или удаления злоумышленниками. Настроенный процесс мониторинга обеспечивает непрерывный контроль за состоянием системы и помогает оперативно устранять возникающие угрозы.

Внедрение механизмов защиты конфиденциальной информации — ключевой аспект обеспечения безопасности при сопровождении информационных систем. Конфиденциальность данных предполагает защиту информации от несанкционированного доступа, что особенно важно для данных, содержащих коммерческую тайну, личную информацию сотрудников или клиентов, а также другие чувствительные данные. В рамках работы с Notion защита конфиденциальной информации может быть реализована на нескольких уровнях.

Первым шагом является шифрование данных как при передаче, так и при хранении. Notion использует современные методы шифрования, такие как SSL/TLS для защиты данных в процессе их передачи, а также AES для шифрования данных на серверах. Эти меры обеспечивают базовый уровень защиты от несанкционированного доступа.

Вторым важным элементом является настройка доступа к конфиденциальной информации, как упоминалось ранее. Однако, помимо настройки прав доступа, важно также контролировать действия пользователей с конфиденциальными данными. В Notion можно использовать журналы действий и историю изменений, которые позволяют отслеживать, кто и когда имел доступ к определенной информации, а также какие изменения были внесены.

Наконец, проведение регулярных тренировок и обучения сотрудников по вопросам работы с конфиденциальной информацией является важным аспектом обеспечения ее безопасности. Сотрудники должны быть осведомлены о правилах работы с данными и понимать важность соблюдения процедур безопасности. Таким образом, комплексный подход к защите конфиденциальной информации включает в себя как технические, так и организационные меры.

3.4 Проведение тестирования безопасности (пентест, анализ логов, защита от атак)

Регулярное тестирование безопасности является неотъемлемой частью защиты информационной системы, так как позволяет выявлять потенциальные уязвимости до того, как ими смогут воспользоваться злоумышленники. Один из ключевых методов тестирования — это пентест (penetration testing), который имитирует реальные атаки и оценивает устойчивость системы к возможным угрозам. Специалисты анализируют сеть, серверы, приложения и механизмы аутентификации, проверяя, насколько эффективно они защищены. Помимо пентестов проводится анализ логов, который позволяет выявлять аномалии в действиях пользователей и попытки компрометации системы. Важным аспектом

тестирования является проверка защиты от атак, таких как SQL-инъекции, XSS, атаки методом перебора паролей и DDoS. По результатам тестирования разрабатываются рекомендации по усилению защиты, исправлению уязвимостей и настройке дополнительных мер безопасности. Такой подход позволяет постоянно совершенствовать систему защиты и предотвращать потенциальные инциденты.

Организация резервного копирования и восстановления данных — неотъемлемая часть обеспечения безопасности информационных систем. Резервное копирование данных позволяет минимизировать риски потери информации в случае сбоев, атак или других инцидентов, которые могут привести к утрате данных. В рамках работы с Notion организация резервного копирования может быть реализована с использованием встроенных механизмов и дополнительных инструментов.

Notion автоматически создает резервные копии данных на своих серверах, что обеспечивает базовый уровень защиты от потери данных. Однако для повышения надежности системы рекомендуется внедрить дополнительные меры по созданию резервных копий. Это может включать регулярное экспорта данных из Notion и хранение их на внешних носителях или в других облачных сервисах, что обеспечивает защиту от потери доступа к основной системе.

Процедуры восстановления данных также должны быть четко документированы и протестированы. Важно, чтобы сотрудники знали, как действовать в случае необходимости восстановления информации, и могли быстро и эффективно восстановить доступ к данным. Регулярное тестирование процедур восстановления помогает выявить возможные проблемы и улучшить процессы восстановления.

Таким образом, эффективная организация резервного копирования и восстановления данных обеспечивает высокую надежность и доступность

информации, что критически важно для обеспечения бесперебойной работы информационных систем.

3.5 Разработка инструкций по безопасному сопровождению ИС

Одним из важнейших элементов обеспечения информационной безопасности является разработка подробных инструкций по сопровождению и эксплуатации системы. В них прописываются правила работы с данными, требования к управлению доступом, порядок обновления программного обеспечения и алгоритмы реагирования на инциденты. Инструкции должны охватывать как технические аспекты, так и вопросы информационной гигиены, такие как правила создания паролей, использование корпоративных VPN и безопасное обращение с электронной почтой. Для системных администраторов разрабатываются рекомендации по мониторингу событий, настройке резервного копирования и управлению конфигурацией. Инструкции должны регулярно обновляться с учётом новых угроз и изменений в инфраструктуре системы. Наличие чётких и понятных регламентов снижает вероятность ошибок, повышает осведомлённость сотрудников в вопросах безопасности и обеспечивает более надёжную защиту информационных ресурсов организации.

Тестирование и оценка эффективности разработанной системы являются завершающими этапами в процессе обеспечения безопасности информационных систем. Тестирование позволяет проверить, насколько эффективно работают внедренные меры безопасности, а также выявить и устранить возможные недостатки. В рамках работы с Notion тестирование может быть проведено в нескольких направлениях.

Во-первых, необходимо провести тестирование функциональности системы, чтобы убедиться, что все разделы документации доступны и работают в соответствии с заданными требованиями. Во-вторых, проводится тестирование безопасности, которое включает проверку защиты данных, систем аутентификации и управления доступом. Это может включать проведение тестов

на проникновение, чтобы выявить уязвимости и оценить устойчивость системы к атакам.

Кроме того, необходимо оценить пользовательский опыт и удобство работы с системой. Это позволяет выявить проблемы, связанные с интерфейсом или процессами работы, и внести необходимые улучшения для повышения эффективности использования системы.

Наконец, важным этапом является оценка эффективности системы в долгосрочной перспективе. Это включает мониторинг инцидентов безопасности, анализ их причин и последствий, а также регулярное обновление системы на основе новых угроз и технологий. Таким образом, тестирование и оценка эффективности являются ключевыми элементами в обеспечении надежности и безопасности информационных систем.

3.6 Оценка эффективности примененных методов защиты.

Оценка эффективности применённых методов защиты является неотъемлемой частью процесса обеспечения информационной безопасности. Любая система защиты должна не только соответствовать требованиям безопасности, но и демонстрировать свою эффективность в реальных условиях эксплуатации. Проверка работоспособности механизмов защиты позволяет выявить слабые места, оптимизировать используемые ресурсы и обеспечить высокий уровень защиты данных от потенциальных угроз. Без тщательной оценки невозможно определить, насколько внедрённые меры действительно обеспечивают защиту информационной системы от современных кибератак и насколько быстро они способны реагировать на инциденты.

Первым этапом оценки эффективности защиты является анализ соответствия применённых методов установленным стандартам и нормативным требованиям. Различные отрасли и организации следуют определённым стандартам, таким как ISO/IEC 27001, NIST, ГОСТ или GDPR, которые

устанавливают базовые критерии безопасности. Если система защиты соответствует этим требованиям, это уже является показателем её надёжности, однако одних формальных критериев недостаточно. Необходимо провести практическое тестирование механизмов защиты, чтобы убедиться, что они эффективно справляются с реальными угрозами.

Одним из наиболее распространённых способов проверки эффективности защиты является проведение тестирования на проникновение (пентестов). Этот метод позволяет имитировать действия злоумышленников и выявлять слабые места в защите системы. Пентесты могут проводиться вручную квалифицированными специалистами или автоматически с использованием специализированного программного обеспечения. В ходе тестирования проверяются различные векторы атак, включая эксплуатацию уязвимостей программного обеспечения, социальную инженерию, атаки на пароли и сетевую инфраструктуру. Результаты пентеста позволяют оценить, насколько быстро система способна обнаруживать атаки и предотвращать их последствия.

Ещё одним важным методом оценки является анализ логов и мониторинг событий безопасности. Внедрение SIEM-систем (Security Information and Event Management) позволяет централизованно собирать, анализировать и интерпретировать данные о действиях пользователей, сетевом трафике и изменениях в конфигурации системы. Анализ логов помогает выявить аномальное поведение, попытки несанкционированного доступа и другие подозрительные события. Эффективность системы защиты можно оценить по тому, насколько оперативно она обнаруживает и блокирует подобные инциденты. Если атаки остаются незамеченными или фиксируются с задержкой, это указывает на необходимость оптимизации мониторинговых механизмов.

Для оценки эффективности защиты часто применяется анализ времени реакции на инциденты и быстроты восстановления системы после атак. Время,

которое требуется для обнаружения угрозы, её локализации и устранения последствий, является критически важным показателем. В идеале система защиты должна работать в режиме реального времени, моментально выявляя и блокируя угрозы, но на практике существуют задержки, связанные с обработкой информации, реагированием специалистов и исправлением уязвимостей. Если система защиты не обеспечивает быструю реакцию на инциденты, требуется её доработка, например, за счёт внедрения автоматизированных механизмов реагирования.

Отдельное внимание уделяется оценке надёжности механизмов аутентификации и управления доступом. Использование многофакторной аутентификации (MFA), строгих политик паролей и ролевой модели контроля доступа (RBAC) должно обеспечивать защиту от компрометации учетных записей. Оценка этих механизмов включает в себя анализ случаев успешных и неуспешных попыток входа, проверку эффективности блокировки учётных записей при обнаружении подозрительной активности, а также анализ частоты использования административных привилегий. Если злоумышленникам удаётся получить несанкционированный доступ или сотрудники организации имеют чрезмерные привилегии, это указывает на недостаточную эффективность системы управления доступом.

Эффективность системы резервного копирования и восстановления данных также является важным критерием оценки защиты. Даже если система защиты способна предотвратить большинство атак, необходимо учитывать возможность сбоев или компрометации данных. Оценка включает в себя проверку времени, требуемого для восстановления системы после инцидента, а также тестирование целостности резервных копий. Если процесс восстановления занимает слишком много времени или резервные копии оказываются непригодными, это свидетельствует о недостатках в системе резервного копирования и необходимости её модернизации.

Ещё один аспект оценки – это устойчивость системы к внутренним угрозам. Внутренние пользователи, обладающие доступом к конфиденциальной информации, могут случайно или преднамеренно нарушить политику безопасности. Поэтому важно анализировать действия пользователей, проверять журналы аудита и применять системы предотвращения утечек данных (DLP). Если система не в состоянии контролировать потенциально опасные действия сотрудников, это говорит о низкой эффективности внутренней политики безопасности.

Не менее значимой является оценка экономической эффективности применённых мер защиты. Любая система защиты требует значительных инвестиций, включая затраты на аппаратное и программное обеспечение, обучение сотрудников, аудит и регулярное тестирование. Эффективность защиты можно оценить путём анализа соотношения затрат на безопасность и потенциальных убытков, которые могли бы возникнуть в результате инцидентов. Если система защиты требует слишком больших вложений при минимальном снижении рисков, это может свидетельствовать о неэффективности применяемых мер и необходимости пересмотра стратегии безопасности.

Периодическая оценка эффективности защиты позволяет выявлять уязвимые места и совершенствовать систему безопасности в соответствии с актуальными угрозами. Киберугрозы постоянно эволюционируют, и методы защиты должны адаптироваться к новым вызовам. Регулярные аудиты, тестирование, анализ логов и мониторинг инцидентов помогают поддерживать высокий уровень безопасности и предотвращать потенциальные атаки. Эффективная система защиты – это не статичный набор мер, а динамическая структура, требующая постоянного совершенствования и адаптации к современным реалиям информационной безопасности.

ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования были рассмотрены актуальные аспекты обеспечения безопасности при сопровождении информационных систем, выявлены основные угрозы и уязвимости, а также проанализированы современные подходы и методы защиты информации. Одним из ключевых выводов стало понимание того, что обеспечение безопасности информационных систем требует комплексного подхода, который включает в себя не только технические меры, но и организационные процессы, постоянное обучение персонала, а также регулярное обновление и тестирование систем на наличие уязвимостей.

Основные результаты работы демонстрируют, что интеграция современных инструментов, таких как платформа Notion, в процесс сопровождения информационных систем позволяет значительно повысить эффективность управления документацией и обеспечением безопасности. Notion предоставила возможность создать централизованную систему документации, которая способствует улучшению процессов управления доступом, обеспечивает прозрачность и упрощает контроль над соблюдением политик безопасности. Это особенно важно в условиях динамически меняющейся информационной среды, где своевременное реагирование на угрозы играет решающую роль.

В результате работы были разработаны рекомендации по повышению уровня безопасности при сопровождении информационных систем, а также предложены методы оценки их эффективности. Особое внимание было уделено созданию структуры документации в Notion, что позволило оптимизировать процесс управления информацией и минимизировать риски, связанные с человеческим фактором.

Перспективы развития в области обеспечения безопасности информационных систем связаны с дальнейшей интеграцией искусственного интеллекта и машинного обучения для автоматического выявления и предотвращения угроз. Кроме того, важно продолжать исследования в области облачных технологий и их влияния на безопасность, так как все больше организаций переходят на использование облачных сервисов. Уделяя внимание этим аспектам, можно обеспечить более высокий уровень защиты информации, а также адаптироваться к новым вызовам и требованиям, которые возникают в цифровом мире.

Таким образом, результаты проведенного исследования и разработанные рекомендации могут быть использованы для совершенствования процессов сопровождения информационных систем в различных организациях, что будет способствовать укреплению их безопасности и устойчивости перед лицом современных угроз.

Список литературы

1. Баронов В.В., Калянов Г.Н., Попов Ю.Н., Рыбников А.И., Титовский И.Н. Автоматизация управления предприятием. – М.: ИНФРА-М, 2000.

2. Атре Ш. Структурный подход к организации баз данных. – М.: Финансы и статистика, 2003.

3. Благодатских В.А., Енгибарян М.А., Ковалевская Е.В. Экономика, разработка и использование программного обеспечения ЭВМ. – М.: Финансы и статистика, 1997.

4. Вендров А.М. CASE-технологии. Современные методы и средства проектирования информационных систем. – М.: Финансы и статистика, 1998. – 176 с.

5. Гайкович В., Першин А. Безопасность электронных банковских систем. – М.: Единая Европа, 1994.

6. ГОСТ 19.001-77. Единая система программной документации. Общие положения. – М.: Издательство стандартов, 1994.

7. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. – М.: Воениздат, 1992.

8. Левин В.К. Защита информации в информационно-вычислительных системах и сетях. Программирование, 2004, №5, с. 5-16.

9. Титоренко Г.А. Автоматизированные информационные технологии в экономике. Учебник. – М.: ЮНИТИ, 2001.

10. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2023.

11. Официальная документация Notion по безопасности [Электронный ресурс]. Режим доступа: https://www.notion.so/security

12. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК Пресс, 2024.

13. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2023.

14. Практическое руководство по безопасности облачных систем / Под ред. И.В. Петрова. – СПб.: БХВ-Петербург, 2023.

15. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing [Электронный ресурс]. – 2023.

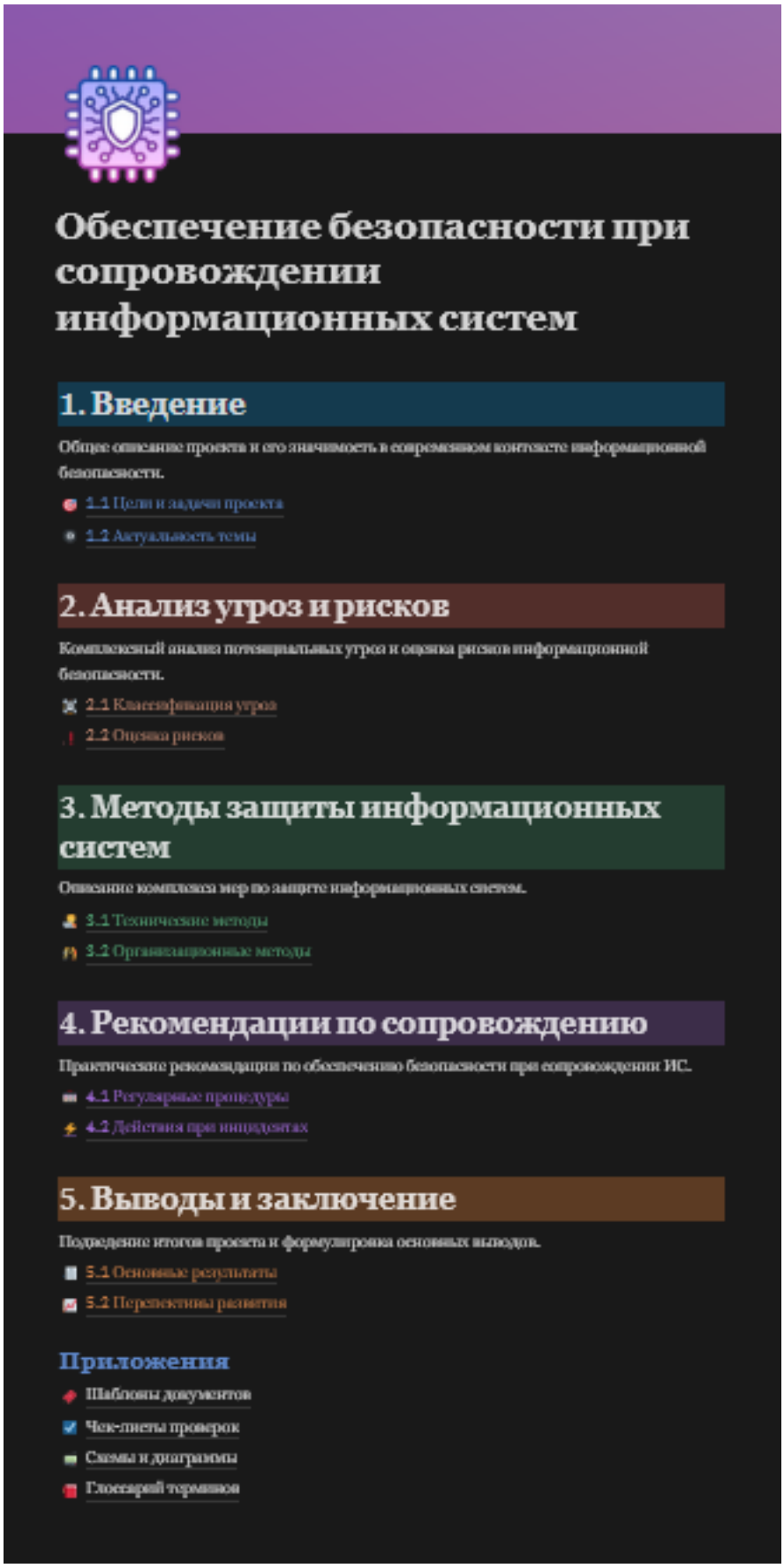
16. Нестеров С.А. Основы информационной безопасности. – СПб.: Лань, 2023.

17. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ.

18. ГОСТ Р ИСО/МЭК 27001-2021 "Информационная технология. Методы и средства обеспечения безопасности."

Приложение

Приложение 1. Главная страница



Приложение 2. Страница 1.2 Актуальность темы

8

1.2 Актуальность темы

Обеспечение безопасности при сопровождении информационных систем становится всё более актуальной задачей в условиях роста количества киберугроз и постоянных изменений в сфере технологий. В этой части руководства рассматриваются современные вызовы информационной безопасности, статистика инцидентов, а также значение вопросов безопасности для бизнеса.

Современные вызовы информационной безопасности

Современные вызовы информационной безопасности можно разделить на несколько ключевых факторов, оказывающих влияние на уровень угроз:

1. **Увеличение числа кибератак:** каждый год количество атак на информационные системы растет. Хакеры используют более сложные методы, такие как фишинг, атаки через уязвимости в ПО, а также злоупотребление правами пользователей.
2. **Сложность систем:** с развитием технологий информационные системы становятся всё более сложными и многослойными. Это затрудняет их защиту и делает их уязвимыми для множества различных типов атак, включая атаки на облачные сервисы, мобильные устройства и IoT.
3. **Риски, связанные с удаленной работой:** с переходом на удаленную работу многие компании столкнулись с необходимостью защищать данные и системы, которые теперь доступны через интернет. Это открывает новые векторы для атак, такие как незащищенные домашние сети сотрудников или использование уязвимых VPN-соединений.
4. **Угрозы внутреннего характера:** все чаще инциденты безопасности происходят не только по вине внешних злоумышленников, но и в результате недобросовестных действий сотрудников или ошибок при конфигурации систем.
5. **Развитие технологий ИИ и машинного обучения:** хотя новые технологии предоставляют множество возможностей для повышения безопасности, они также могут быть использованы злоумышленниками для создания более сложных и непредсказуемых атак.

Статистика инцидентов

Согласно статистике, инциденты в области информационной безопасности становятся всё более частыми и разрушительными для организаций. Некоторые важные данные по статистике инцидентов:

- **Увеличение числа кибератак:** по данным последнего отчета (например, от IBM или Verizon), количество инцидентов, связанных с утечками данных, увеличилось на 15-20% за последний год.
- **Влияние на бизнес:** более 60% компаний признают, что инциденты безопасности негативно сказываются на их финансовых результатах. Стоимость утечек данных, как правило, исчисляется миллионами долларов, включая не только прямые убытки, но и репутационные потери.
- **Типы инцидентов:** в последние годы наблюдается рост числа атак с использованием вредоносных программ, таких как программное обеспечение для шифрования данных (ransomware), а также инцидентов, связанных с фишингом и социальной инженерией.

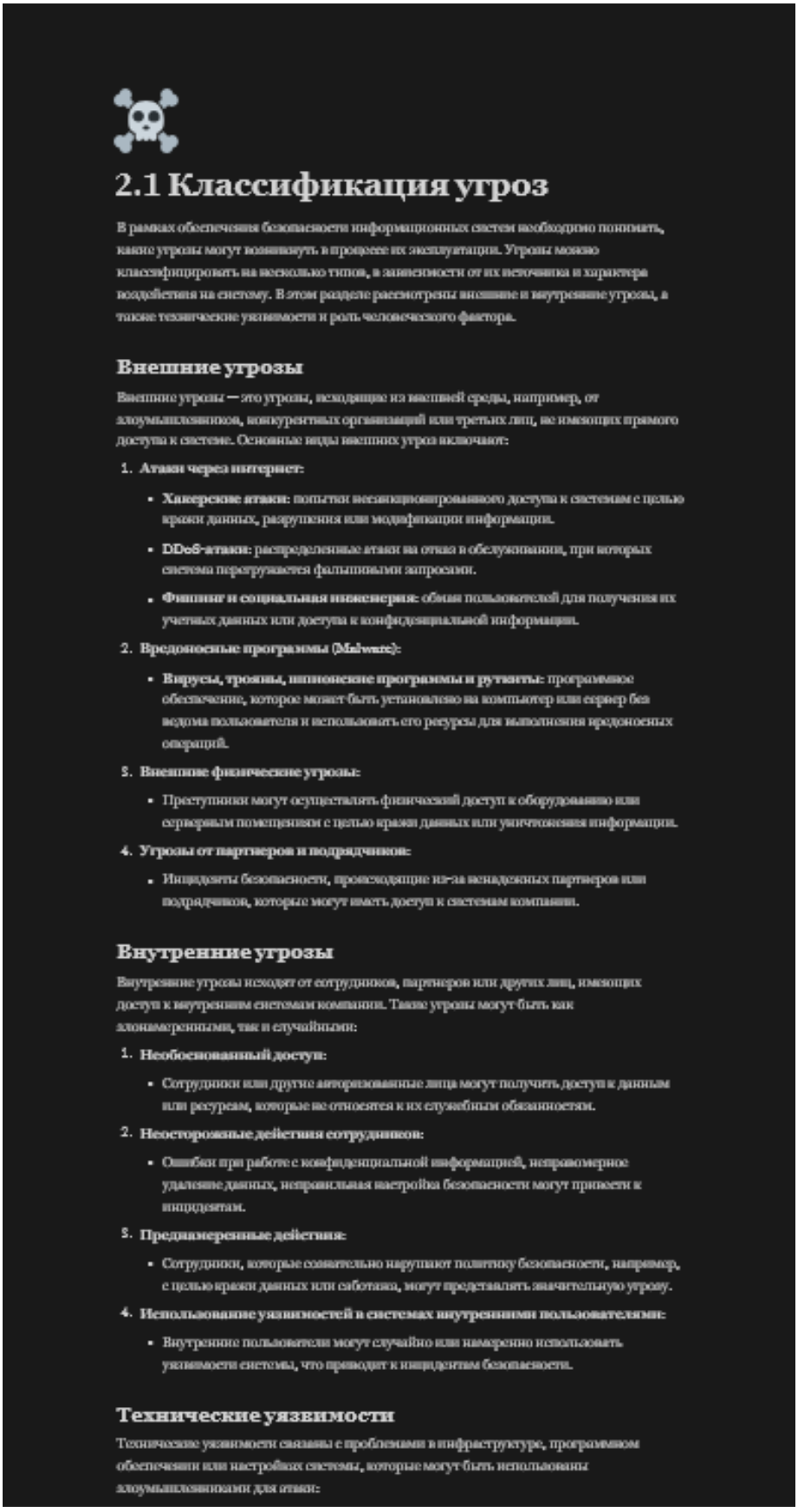
Кроме того, важно отметить, что **40% инцидентов безопасности происходят из-за уязвимостей в программном обеспечении**, которые могли бы быть устранены при правильном управлении патчами и обновлениями.

Значимость для бизнеса

Информационная безопасность имеет прямое влияние на успешность и устойчивость бизнеса. Современные угрозы требуют от компаний внедрения системы безопасности на всех уровнях. Вот несколько причин, почему защита информационных систем важна для бизнеса:

1. **Защита данных клиентов:** утечка данных может привести к потере доверия клиентов, штрафам и юридическим последствиям. В условиях усиления законодательства (например, GDPR) ответственность за утечку данных возлагается

Приложение 3. Страница 2.1 Классификация угроз



2.1 Классификация угроз

В рамках обеспечения безопасности информационных систем необходимо понимать, какие угрозы могут возникнуть в процессе их эксплуатации. Угрозы можно классифицировать на несколько типов, в зависимости от их источника и характера воздействия на систему. В этом разделе рассмотрены внешние и внутренние угрозы, а также технические уязвимости и роль человеческого фактора.

Внешние угрозы

Внешние угрозы — это угрозы, исходящие из внешней среды, например, от злоумышленников, конкурентных организаций или третьих лиц, не имеющих прямого доступа к системе. Основные виды внешних угроз включают:

1. **Атаки через интернет:**
   - **Хакерские атаки:** попытки несанкционированного доступа к системам с целью кражи данных, разрушения или модификации информации.
   - **DDoS-атаки:** распределенные атаки на отказ в обслуживании, при которых система перегружается фальшивыми запросами.
   - **Фишинг и социальная инженерия:** обман пользователей для получения их учетных данных или доступа к конфиденциальной информации.
2. **Вредоносные программы (Malware):**
   - **Вирусы, трояны, шпионские программы и руткиты:** программное обеспечение, которое может быть установлено на компьютер или сервер без ведома пользователя и использовать его ресурсы для выполнения вредоносных операций.
3. **Внешние физические угрозы:**
   - Преступники могут осуществлять физический доступ к оборудованию или серверным помещениям с целью кражи данных или уничтожения информации.
4. **Угрозы от партнеров и подрядчиков:**
   - Инциденты безопасности, происходящие из-за ненадежных партнеров или подрядчиков, которые могут иметь доступ к системам компании.

Внутренние угрозы

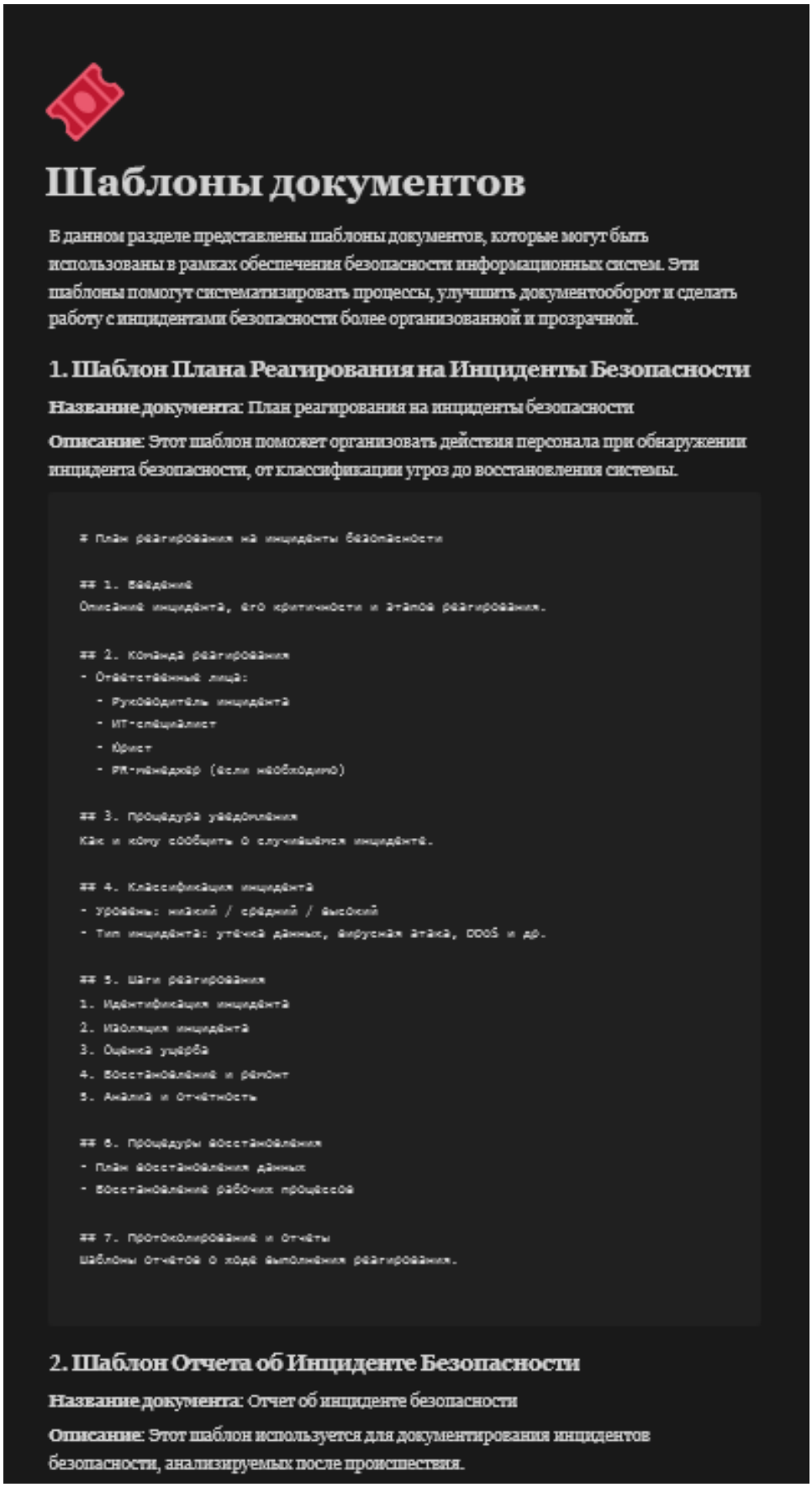
Внутренние угрозы исходят от сотрудников, партнеров или других лиц, имеющих доступ к внутренним системам компании. Такие угрозы могут быть как злонамеренными, так и случайными:

1. **Необоснованный доступ:**
   - Сотрудники или другие авторизованные лица могут получить доступ к данным или ресурсам, которые не относятся к их служебным обязанностям.
2. **Неосторожные действия сотрудников:**
   - Ошибки при работе с конфиденциальной информацией, неправомерное удаление данных, неправильная настройка безопасности могут привести к инцидентам.
3. **Преднамеренные действия:**
   - Сотрудники, которые сознательно нарушают политику безопасности, например, с целью кражи данных или саботажа, могут представлять значительную угрозу.
4. **Использование уязвимостей в системах внутренними пользователями:**
   - Внутренние пользователи могут случайно или намеренно использовать уязвимости системы, что приводит к инцидентам безопасности.

Технические уязвимости

Технические уязвимости связаны с проблемами в инфраструктуре, программном обеспечении или настройках системы, которые могут быть использованы злоумышленниками для атаки:

Приложение 4. Страница Шаблоны документов



Шаблоны документов

В данном разделе представлены шаблоны документов, которые могут быть использованы в рамках обеспечения безопасности информационных систем. Эти шаблоны помогут систематизировать процессы, улучшить документооборот и сделать работу с инцидентами безопасности более организованной и прозрачной.

1. Шаблон Плана Реагирования на Инциденты Безопасности

Название документа: План реагирования на инциденты безопасности

Описание: Этот шаблон поможет организовать действия персонала при обнаружении инцидента безопасности, от классификации угроз до восстановления системы.

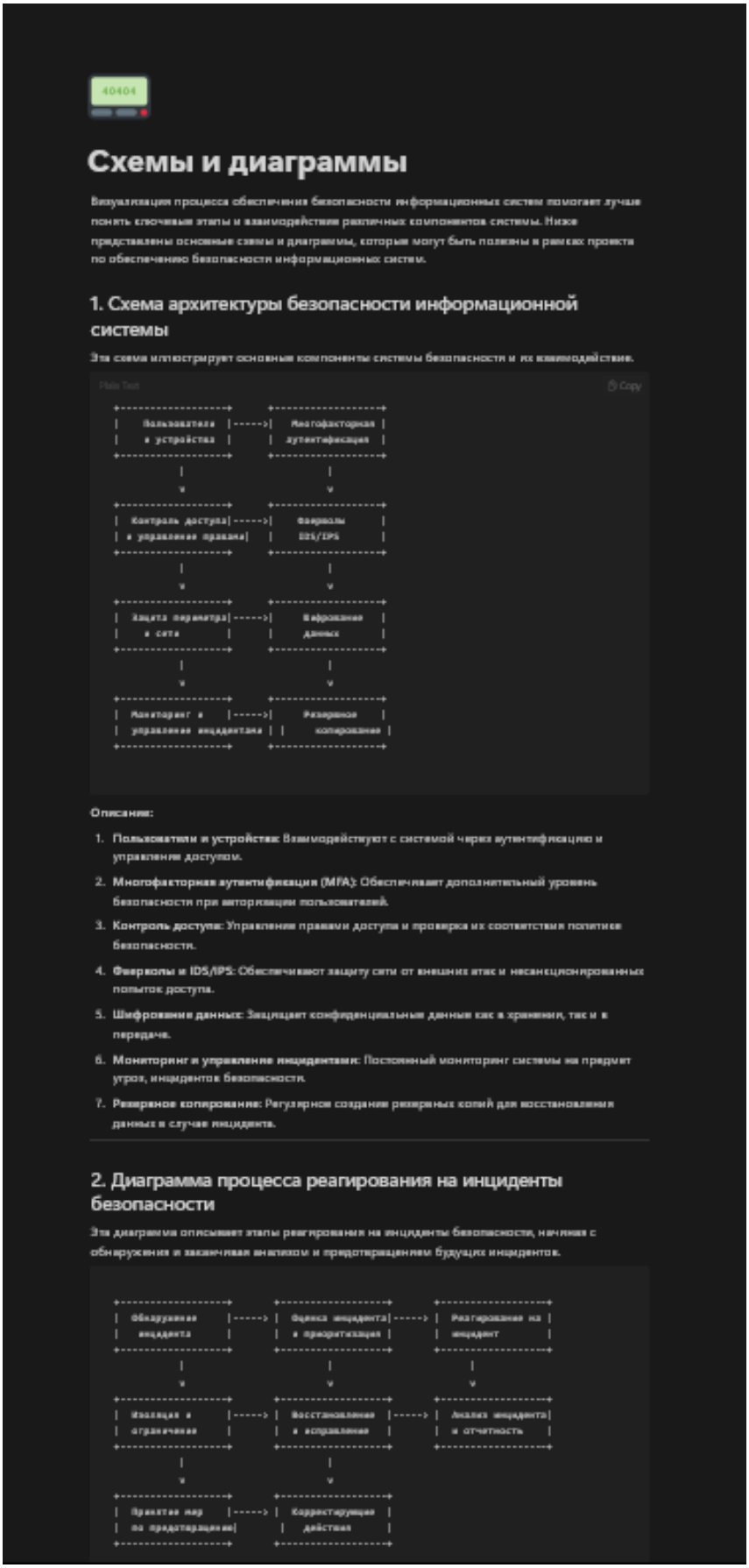
```
# План реагирования на инциденты безопасности

## 1. Введение
Описание инцидента, его критичности и этапов реагирования.

## 2. Команда реагирования
- Ответственные лица:
  - Руководитель инцидента
  - IT-специалист
  - Юрист
  - PR-менеджер (если необходимо)

## 3. Процедура уведомления
Как и кому сообщать о случившемся инциденте.

## 4. Классификация инцидента
- Уровень: низкий / средний / высокий
- Тип инцидента: утечка данных, вирусная атака, DDoS и др.

## 5. Шаги реагирования
1. Идентификация инцидента
2. Изоляция инцидента
3. Оценка ущерба
4. Восстановление и ремонт
5. Анализ и отчетность

## 6. Процедуры восстановления
- План восстановления данных
- Восстановление рабочих процессов

## 7. Протоколирование и отчеты
Шаблоны отчетов о ходе выполнения реагирования.
```

2. Шаблон Отчета об Инциденте Безопасности

Название документа: Отчет об инциденте безопасности

Описание: Этот шаблон используется для документирования инцидентов безопасности, анализируемых после происшествия.

Приложение 5. Страница Схемы и диаграммы



Схемы и диаграммы

Визуализация процесса обеспечения безопасности информационных систем помогает лучше понять ключевые этапы и взаимодействие различных компонентов системы. Ниже представлены основные схемы и диаграммы, которые могут быть полезны в рамках проекта по обеспечению безопасности информационных систем.

1. Схема архитектуры безопасности информационной системы

Эта схема иллюстрирует основные компоненты системы безопасности и их взаимодействие.

```
+-------------------+      +-------------------+
|   Пользователи    |----->|  Многофакторная   |
|   и устройства    |      |  аутентификация   |
+-------------------+      +-------------------+
          |                          |
          v                          v
+-------------------+      +-------------------+
|  Контроль доступа |----->|    Фаерволы       |
|  и управление правами|   |    IDS/IPS        |
+-------------------+      +-------------------+
          |                          |
          v                          v
+-------------------+      +-------------------+
|  Защита периметра |----->|    Шифрование     |
|    и сети         |      |    данных         |
+-------------------+      +-------------------+
          |                          |
          v                          v
+-------------------+      +-------------------+
|  Мониторинг и     |----->|    Резервное      |
|  управление инцидентами | |    копирование  |
+-------------------+      +-------------------+
```

Описание:

1. **Пользователи и устройства:** Взаимодействуют с системой через аутентификацию и управление доступом.
2. **Многофакторная аутентификация (MFA):** Обеспечивает дополнительный уровень безопасности при авторизации пользователей.
3. **Контроль доступа:** Управление правами доступа и проверка их соответствия политике безопасности.
4. **Фаерволы и IDS/IPS:** Обеспечивают защиту сети от внешних атак и несанкционированных попыток доступа.
5. **Шифрование данных:** Защищает конфиденциальные данные как в хранении, так и в передаче.
6. **Мониторинг и управление инцидентами:** Постоянный мониторинг системы на предмет угроз, инцидентов безопасности.
7. **Резервное копирование:** Регулярное создание резервных копий для восстановления данных в случае инцидента.

---

2. Диаграмма процесса реагирования на инциденты безопасности

Эта диаграмма описывает этапы реагирования на инциденты безопасности, начиная с обнаружения и заканчивая анализом и предотвращением будущих инцидентов.

```
+-------------------+      +-------------------+      +-------------------+
|  Обнаружение      |----->|  Оценка инцидента |----->|  Реагирование на  |
|  инцидента        |      |  и приоритизация  |      |  инцидент         |
+-------------------+      +-------------------+      +-------------------+
          |                          |                          |
          v                          v                          v
+-------------------+      +-------------------+      +-------------------+
|  Изоляция и       |----->|  Восстановление   |----->|  Анализ инцидента |
|  ограничение      |      |  и исправление    |      |  и отчетность     |
+-------------------+      +-------------------+      +-------------------+
          |                          |
          v                          v
+-------------------+      +-------------------+
|  Принятие мер     |----->|  Корректирующие   |
|  по предотвращению|      |  действия         |
+-------------------+      +-------------------+
```