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

Кафедра Прикладная математика и информатика
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Управление корпоративными информационными процессами
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Модели и алгоритмы обмена конфиденциальной информацией в организации

Обучающийся С.М Пакин
(Инициалы Фамилия) (личная подпись)

Научный руководитель д.т.н., доцент, С.В. Мкртычев
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Содержание

Введение

Современное состояние и результат развития научно-технического прогресса ознаменован повсеместным использованием передовых информационных технологий (далее – ИТ). Данные технологии представляют собой инструменты, позволяющие оперативно передавать, получать и обрабатывать данные. Посредством этих технологий наблюдается значительное повышение качества и эффективности работы современных предприятий и организаций. При этом использование ИТ наблюдается практически во всех современных как бытовых, так и профессиональных сферах жизнедеятельности человека. Совокупность данных факторов свидетельствует о значимой роли ИТ в жизни современного человека. Их интеграция позволяет добиться множества положительных эффектов, связанных с оптимизацией и автоматизацией работы, снижения влияния человеческого фактора и иного. Однако, несмотря, на столь значимые преимущества, на момент 2024 года актуализируется проблема, связанная с информационной безопасностью (далее – ИБ) при интеграции и использовании ИТ. Использование передовых технологий порождает множество угроз и рисков нарушения целостности и достоверности информации. В связи с этим актуализируются задачи, связанные с обеспечением информационной безопасности организации. При этом одной из важных подзадач является обеспечение безопасного обмена конфиденциальной информацией, в частности, посредством специальных моделей и алгоритмов.

Результаты представленной выпускной квалификационной работы отражают основные аспекты, касающиеся текущих трендов развития вопроса информационной безопасности. Главной особенностью является проведение исследования в призме современных организаций, в частности, ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ». Научный вклад работы состоит в разработке новых рекомендаций по обеспечению безопасности системы

обмена конфиденциальной информацией, а также этапов внедрения моделей и алгоритмов, тестирования и оценки ее эффективности.

Практическая значимость результатов работы состоит в возможности их использования в реальных организациях, обеспечивая безопасный обмен конфиденциальной информацией. Основной особенностью предложенных решений является их универсальность, что достигается за счет индивидуализации отдельных параметров методики под каждое конкретное предприятие. В качестве основы для получения и анализа информации были использованы как отечественные, так и зарубежные научные источники. В рамках работы автором применены различные методы научного исследования, в частности, анализа, синтеза и обобщения. Основой работы стали научные источники по соответствующей теме магистерской диссертации.

Объектом представленного исследования является процесс обмена конфиденциальной информацией в организации.

Предметом представленного исследования являются модели и алгоритмы обмена конфиденциальной информацией в организации.

Цель магистерской диссертации заключается в разработке моделей и алгоритмов, обеспечивающих повышение эффективности обмена конфиденциальной информацией в организации.

Для достижения поставленной цели предстоит решить следующие задачи:

- рассмотреть существующие алгоритмы и модели обмена конфиденциальной информацией;
- проанализировать процессы интеграции моделей и алгоритмов в корпоративные системы и их влияние на организационную культуру;
- исследовать современные тенденции и вызовы в области защиты конфиденциальной информации;

– разработать модели и алгоритмы обмена конфиденциальной информации в организации;
– выполнить апробацию проектных решений и оценить их эффективность.

Гипотеза исследования: применение современных алгоритмов обмена конфиденциальной информацией позволит обеспечить повышение уровня защиты конфиденциальной информации.

Методы исследования: методы моделирования системы безопасности системы обмена конфиденциальной информацией, методы внедрения моделей и алгоритмов системы обмена конфиденциальной информацией в организации.

Новизна исследования заключается в разработке новой методики обеспечения обмена конфиденциальной информацией в организации.

Практическая значимость исследования заключается в возможности практического применения предлагаемых моделей и алгоритмов системы обмена конфиденциальной информацией в организации.

Теоретической основой исследования являются научные труды российских и зарубежных ученых, которые занимаются проблемами обмена конфиденциальной информацией.

Основные этапы исследования: исследование проводилось с 2023 по 2025 год в несколько этапов:

На первом этапе (констатирующем) этапе формулировалась тема исследования, выполнялся сбор информации по теме исследования из различных источников, проводилась формулировка гипотезы, определялись постановка цели, задач, предмета исследования, объекта исследования и выполнялось определение проблематики данного исследования.

Второй этап – теоретический. В ходе проведения данного этапа изучались современные тенденции и вызовы в области защиты конфиденциальной информации, анализировалась значимость темы для организации, разработаны рекомендации по обеспечению безопасности

системы обмена конфиденциальной информацией, разработаны этапы внедрения моделей и алгоритмов.

Третий этап – практический. В ходе проведения данного этапа проводилась апробация предлагаемых проектных решений, произведено тестирование и оценка эффективности, сформулированы выводы о полученных результатах по проведенному исследованию.

Основные положения диссертации отражены в публикации [24].

На защиту выносятся:

- модели и алгоритмы системы обмена конфиденциальной информацией в организации;
- результаты апробации и оценки эффективности предлагаемых проектных решений.

Диссертация состоит из введения, четырех глав, заключения, списка используемой литературы и используемых источников.

В первом разделе дан анализ моделей и алгоритмов обмена конфиденциальной информацией.

Во втором разделе рассмотрены ключевые аспекты моделей и алгоритмов обмена конфиденциальной информацией.

Третий раздел посвящен разработке основных этапов тестирования и внедрения системы обмена конфиденциальной информацией в организации.

В четвертом разделе выполнены апробация предлагаемых проектных решений и оценка их эффективности.

В заключении приводятся результаты исследования.

Работа изложена на 105 страницах и включает 16 рисунков, 4 таблицы и 44 источника.

1 Модели и алгоритмы обмена конфиденциальной информацией

1.1 Введение в модели и алгоритмы обмена конфиденциальной информацией

В современном мире, где объем и скорость обмена информацией растут экспоненциально, важность эффективных моделей и алгоритмов обмена информацией становится все более актуальной и это обусловлено не только увеличением объемов обрабатываемой информации, но и растущим числом угроз безопасности данных, таких как кибератаки, вирусы и утечки данных.

В действующем законодательстве термин «информация» трактуется широко [3]. Законодатель отказался от закрытого перечня сведений, относимых к «информации в правовом смысле» и ввел в определение информации инвариантность ее правового регулирования независимо от формы предоставления [22]. Данный подход закрепления в законодательстве понятия «информация» логичен и понятен, так как сама по себе информация – понятие общее, позволяющее увеличить количество объектов, которых возможно отнести к информации.

Предпосылки деления информации на общедоступную и информацию с ограниченным доступом заключаются в том, что недоступная третьим лицам информация приобретает особую ценность, распространение и использование информации с ограниченным доступом может нарушить интересы и права правообладателя [14].

Информация, ограниченная законом, может относиться к государственной тайне или относиться к конфиденциальной информации [26]. Концепция государственной тайны охватывает защищенные государством данные, связанные с важнейшими сферами национальной безопасности и интересов [1]. Этот термин применим к информации, связанной с функционированием вооруженных сил, стратегией и практикой внешней политики, внутренними экономическими вопросами страны, работой

разведывательных и контрразведывательных органов, а также к деятельности, связанной с проведением оперативно-розыскных мероприятий. Любое несанкционированное раскрытие такой информации может потенциально подвергнуть риску стабильность и безопасность Российской Федерации.

О конфиденциальной информации говорится в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3]: конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (ст. 2 Закона 3 149-ФЗ).

Таким образом, к сведениям ограниченного доступа относятся:

- государственная тайна (в том числе, которая относится к транспортной безопасности, оперативно-розыскной деятельности, Федеральной службе безопасности, войскам национальной гвардии, внешней разведке);
- коммерческая тайна;
- конфиденциальная информация, полученная в ходе переговоров о заключении договора от другой стороны;
- конфиденциальная информация о деятельности корпорации;
- персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных));
- налоговая, банковская тайны;
- конфиденциальная информация, которой Банк России обменивается с иностранным регулятором финансового рынка;
- врачебная тайна;
- нотариальная тайна;
- адвокатская тайна;
- аудиторская тайна и многие другие виды сведений [35].

Модель обмена конфиденциальной информацией – это теоретический или концептуальный фреймворк, который описывает процесс передачи данных между сторонами с учетом всех необходимых аспектов безопасности [34].

Такая модель включает в себя:

– архитектуру системы;
– методы шифрования;
– протоколы безопасности;
– политики доступа;
– контроль за передачей данных.

Основная функция модели – обеспечить безопасный и контролируемый обмен данными, это включает в себя:

– защиту от несанкционированного доступа;
– шифрование данных;
– аутентификацию участников обмена;
– сохранение целостности информации.

Алгоритм обмена конфиденциальной информацией – это четко определенная последовательность операций или инструкций, предназначенная для выполнения задачи обмена информацией [37].

Алгоритмы могут включать:

– методы шифрования и дешифрования;
– алгоритмы проверки подлинности;
– протоколы передачи данных;
– механизмы контроля доступа.

Такие алгоритмы служат для конкретной реализации процесса обмена, и они обеспечивают выполнение всех необходимых шагов для защиты информации, начиная от момента ее отправления и заканчивая ее получением, а также учитывают потребности в эффективности и скорости обработки данных и в способности адаптироваться к различным условиям и угрозам.

Понимание и применение правильных моделей и алгоритмов обмена конфиденциальной информацией является ключевым для обеспечения безопасности данных в любой организации, ведь это не только защищает важную информацию, но и способствует укреплению доверия и репутации компании на рынке [31].

Актуальность проблемы обмена конфиденциальной информацией в современных организациях становится все более очевидной по мере развития цифровых технологий и расширения объемов данных, с которыми работают компании. Конфиденциальная информация, будь то коммерческая тайна, данные клиентов или стратегические планы, является основным активом любой организации. Потеря или утечка таких данных может привести к серьезным последствиям, включая финансовые потери, утрату репутации и конкурентные преимущества. В условиях растущей глобализации и цифровизации, когда объемы передаваемой информации увеличиваются, а взаимодействие между организациями происходит в основном в цифровой среде, проблема защиты данных выходит на передний план [17].

В нынешнем быстро меняющемся цифровом мире, где угрозы кибербезопасности становятся все более изощренными, важность защиты конфиденциальной информации все более возрастает. Хакеры постоянно совершенствуют свои методы и находят новые способы нарушения безопасности информационных систем, применяя передовые технологии для доступа к данным организаций. Это выдвигает новые требования к защитным мерам, выходящим за рамки традиционного применения шифрования и антивирусных решений. Особенно это касается обстоятельств, когда работники вынуждены работать удаленно и использовать внекорпоративные сети, что усиливает необходимость контроля за циркуляцией данных после пандемии COVID-19.

Также огромное внимание уделяется выполнению законодательных требований в сфере обработки персональных данных, в частности таких нормативов, как GDPR в Европе и Федеральный закон № ФЗ-152 «О

персональных данных» [4] в России, подчеркивающих ответственность за сохранность информации. Несоблюдение этих норм может влечь за собой значительные штрафы и удар по репутации, что делает защиту данных приоритетной для компаний.

С целью не только реагировать на внешние угрозы, но и активно предотвращать их, современные бизнесы прибегают к инновационным методам защиты. Интеграция передовых алгоритмов машинного обучения и технологий блокчейна в системы безопасности способна значительно повысить эффективность идентификации и нейтрализации опасностей. В комплекс мероприятий по кибербезопасности также включается использование современных криптографических методов, в том числе асимметричного шифрования и алгоритмов, базирующихся на эллиптических кривых. Эти методы, в сочетании с интеллектуальными системами оценки рисков, предлагают гибкие и эффективные подходы к защите ценной информации.

В свете этих тенденций, интеграция интеллектуальных и криптографических инструментов в структуру информационной безопасности организаций становится ключевым элементом в борьбе с киберугрозами и гарантирует более надежную защиту персональных данных в динамично развивающемся цифровом пространстве.

В области кибербезопасности критически важной является разработка систем, способных анализировать аномалии в датчиках обмена информацией. С помощью методов машинного обучения можно реализовать инструменты, способные выявлять нестандартное поведение и инциденты, когда предпринимается попытка несанкционированного доступа. Такие системы анализируют активность пользователей и паттерны трафика данных для идентификации отклонений от нормы. В случае обнаружения подозрительных действий алгоритмы могут инициировать временную блокировку данных до завершения проверочных процедур. Это обеспечивает быстрый отклик на угрозы и способствует минимизации риска утечек ценной информации.

1.2 Интеграция моделей и алгоритмов в корпоративные системы и их влияние на организационную культуру

Организация работы с конфиденциальной информацией является важной задачей для каждой современной компании. Утечка или потеря персональных сведений, а также другие формы мошенничества могут привести к серьезным последствиям для бизнеса.

Особо ценная для компании информация должна быть доступна только ограниченному числу сотрудников, а ее использование должно строго регламентироваться. К таким данным, которые требуют надежной защиты, относятся: коммерческая тайна; производственная документация, содержащая секретную информацию; ноу-хау компании; клиентская база; персональные данные сотрудников; другие сведения, которые компания сочтет необходимым защищать от утечек [26].

Для обеспечения надежной защиты, компании, занимающие ключевые позиции в стратегических отраслях экономики, должны особенно тщательно подходить к вопросам информационной безопасности. Угрозы могут приходить не только от международных киберпреступных групп, стремящихся к хакерским атакам, но также от иностранных разведывательных агентств, ищущих доступ к ценным данным.

В то же время, малые и средние предприятия сталкиваются с другим набором опасностей при защите своих информационных активов. Сюда входят [12]:

- фирмы, основанные бывшими сотрудниками, которые могут использовать украденную коммерческую информацию для развития своего бизнеса;
- нелояльные работники, представляющие значительную внутреннюю угрозу, поскольку они имеют доступ к важной информации и могут ее использовать в корыстных целях, в том числе продавать или передавать ее посторонним лицам, или даже

использовать для мести компании. Статистика показывает, что более 80% инцидентов связаны с действиями инсайдеров;

– хакеры, провоцирующие распространение вирусов, в том числе троянов и шифровальщиков, а также других видов, что может привести к массовым заражениям.

С целью противодействия этим угрозам, крайне важно поддерживать информационную безопасность на высоком уровне, следя за новыми разработками в сфере защиты данных и своевременно обновляя антивирусное программное обеспечение, чтобы противостоять текущим и возможным угрозам на рынке.

Эффективная защита конфиденциальной информации требует применения комплекса мер – правовых, организационных и технических. Эти методы позволяют минимизировать уязвимости и предотвратить несанкционированный доступ, утечку или разглашение информации.

Правовые меры являются основой защиты конфиденциальных сведений. Они обязательны для всех компаний, независимо от сложности используемой системы безопасности. Если правовая защита не организована должным образом, компания не сможет гарантировать защиту конфиденциальных данных и привлечь к ответственности тех, кто виновен в их утрате или разглашении. Правовая защита включает грамотное оформление документации, а также правильную работу с сотрудниками, которые играют ключевую роль в обеспечении безопасности.

Организационные меры информационной безопасности в компаниях нацелены на регулирование действий пользователей и снижение угроз, связанных с передачей служебных и конфиденциальных данных через небезопасные коммуникационные каналы. В этом контексте необходимо особое внимание уделять поведению персонала, включая квалифицированных IT-специалистов, которые могут использовать для служебной переписки незащищенные персональные Wi-Fi сети. Одним из первостепенных действий для обеспечения защиты информации становится разработка и внедрение

четких политик безопасности, образовательных программ, информирование о текущих угрозах и уязвимостях.

Процедуры контроля доступа к критичным данным играют ключевую роль в обеспечении информационной безопасности. И хотя эта задача требует использования аппаратных средств, контроль также считается элементом организационной безопасности. Например, в ряде компаний с рабочих мест отсутствует возможность доступа в Интернет, что предотвращает утечку информации с данных устройств.

Среди технических мер защиты корпоративных данных выделяют такие, как:

- криптография для защиты электронных документов;
- электронные подписи повышенной надежности, подтверждающие авторство, в частности, это необходимо для документов высокой значимости;
- контроль за целостностью документов;
- уникальная идентификация документов, включая их нумерацию;
- обеспечение безопасности данных с помощью идентификаторов PHP;
- решения для анализа трафика и расшифровки по протоколам безопасности;
- динамическая аутентификация, например, через разовые пароли, отправляемые по SMS;
- использование вариативных ключей шифрования;
- менеджмент секретных ключей;
- применение электронных сертификатов для подтверждения принадлежности ключей;
- создание защищенных каналов связи для обмена данными, как например, передача данных из системы 1С в облачные хранилища.

Правильное использование этих мер обеспечивает безопасность информации пользователя в процессе взаимодействия с веб-сайтами.

Перед реализацией технических мер защиты, для построения стратегии комплексной безопасности, следует проанализировать потенциальные пути утечки информации, включая как внутренние (инсайдерские), так и внешние каналы утечки данных.

Угрозы информационной безопасности, исходящие изнутри компании, представляют серьезную опасность, поскольку сотрудники обладают легальным доступом к конфиденциальным данным. В рамках этого контекста выделяют два основных типа инсайдерских угроз: преднамеренные акты, такие как кража, мошенничество или утечка данных конкурентам, и ненамеренные ошибки, возникающие в результате некомпетентности сотрудников или несоблюдения ими политики информационной безопасности.

Типичные примеры инсайдерских инцидентов включают:

- использование съемных накопителей для копирования данных;
- отправка файлов через Интернет средствами электронной почты, мессенджеров или облачных сервисов;
- несанкционированный вынос бумажных документов и носителей информации из офиса;
- фотографирование экранов и документов для захвата конфиденциальной информации;
- неосознанное или умышленное разглашение сведений в личных беседах или во время телефонных разговоров.

Для обеспечения защиты от таких рисков компаниям необходимо внедрять комплексные меры, включая программируемые и аппаратные средства защиты. Но столь же важно и проведение регулярного обучения сотрудников стандартам информационной безопасности, тщательный отбор персонала, мониторинг соответствия существующим процедурам, а также своевременное выявление потенциально неблагонадежных работников.

Что касается внешних каналов утечек, то они связаны с действиями внешних лиц или злоумышленников. К ним относятся хакерские атаки с взломом сетей и подбором паролей, распространение вредоносного ПО, перехват трафика коммуникационных каналов, физическая кража устройств хранения данных, а также технические методы разведки, включая электромагнитное слежение, акустический и визуальный мониторинг, применение закладных устройств, скрытых камер и жучков.

Для нейтрализации такого рода угроз требуется создание многоуровневой системы защиты. В ее основу должно входить функционирование антивирусного программного обеспечения, межсетевых экранов, систем обнаружения вторжений, средств шифрования данных, а также ряда других специализированных решений.

В то же время важно осознавать, что технические каналы утечек информации в современном мире представлены широким разнообразием средств и методов. К таковым относится не только использование традиционных внешних устройств и бумаги, но и широко распространенное применение мобильных и облачных технологий, социальных сетей, мессенджеров. Угрозы могут исходить от несакционированного использования электронной почты, веб-форм, офисной техники, а также интеллектуальных устройств, включая smart-TV в переговорных зонах. Таким образом, для защиты информации требуется комплексный контроль за всеми потенциальными точками передачи данных – рабочими станциями/местами, серверами, и сетевым периметром. Системы предотвращения утечки данных (DLP) должны обеспечивать анализ в реальном времени и блокировать подозрительные транзакции и несанкционированную передачу конфиденциальных данных.

Однако даже самые совершенные DLP-системы не способны полноценно предотвращать утечки, спровоцированные человеческим фактором. Поэтому ключевое значение имеет работа с сотрудниками – своевременное выявление потенциально опасного поведения, оценка

благонадежности, мотивации, психоэмоционального состояния персонала [36].

В качестве методов, которые могут помочь проводить подобную работу, можно привести в пример специализированные инструменты профайлинга и UEBA (User and Entity Behavior Analytics), которые на основе анализа цифрового следа сотрудников (история коммуникаций, график работы, перемещения, взаимосвязи) выявляют аномальное и рисковое поведение, потенциально указывающее на угрозу инсайдерской утечки.

1.3 Классификация методов обмена конфиденциальной информацией

Рассмотрим более подробно современные модели и алгоритмы обмена конфиденциальной информацией.

Н.В. Кульпина и С.В. Мкртычев выделяют следующие криптографические методы [26]:

- симметричное шифрование. Этот метод криптографии уникален своей способностью использовать один и тот же ключ как для шифрования, так и для расшифровки информации. Его основное преимущество – обработка данных с высокой скоростью, что делает его идеальным для работы с большим объемом информации. Тем не менее, риск безопасности возникает при необходимости передачи самого ключа, так как его перехват третьими лицами может привести к нежелательному раскрытию информации;
- асимметричное шифрование. В отличие от симметричного шифрования, асимметричное использует два ключа – публичный для шифрования и приватный для расшифровки. Этот подход значительно повышает безопасность, так как обмен ключами здесь не требуется. Ограничением асимметричной криптографии является скорость ее работы – она медленнее симметричного

аналога, что может быть критично при обработке больших массивов данных;

- метод дифференциального анализа. Дифференциальный анализ – это техника, позволяющая анализировать, как малейшие изменения в исходном тексте влияют на структуру зашифрованного сообщения. Он требует продвинутых знаний о шифре и может использоваться для обнаружения потенциальных слабостей алгоритма.
- алгебраический метод анализа. При алгебраическом анализе используются математические уравнения для изучения и оценки криптографических алгоритмов. Этот метод помогает определить уязвимые точки в алгоритме и оценить его общую надежность;
- применение хэш-функций. Хэш-функции важны для поддержания целостности данных, поскольку они генерируют уникальные «отпечатки» для любого набора данных. Хэш-функции широко применяются для создания цифровых подписей и обеспечения аутентичности данных.

Принципы регуляторных требований к алгоритмам шифрования определяются через ряд критериев:

- интегральная защита данных. Алгоритмы должны исключать не только вероятность расшифровки, но также и возможность незаметной модификации информации;
- зависимость от ключа. Правильная расшифровка информации должна гарантироваться исключительно наличием соответствующего ключа, при этом известность алгоритма не должна предоставлять возможность декодирования без ключа;
- эффект «лавины». Любое незначительное изменение в исходных данных или ключе должно вызывать значительное и непредсказуемое изменение в зашифрованных данных;

- криптостойкость ключа. Поле возможных значений ключа должно быть достаточно широким, обеспечивая его устойчивость к атакам методом полного перебора;
- эффективность алгоритмов. Процедуры шифрования и дешифрования должны обладать высокой производительностью при минимально необходимых ресурсах;
- экономический аспект. Стоимость дешифрации без ключа должна значительно превышать ценность зашифрованных данных, делая попытки взлома нецелесообразными.

Применяемые в информационных системах средства шифрования часто реализуются как программное и/или аппаратное обеспечение, интегрированное в конечные точки обмена данными. Эффективное использование всех функциональных возможностей, предлагаемых разработчиками современного шифровального ПО, позволяет достигнуть высокого уровня защиты информационного трафика и противостоять различным угрозам в области информационной безопасности.

Таким образом, криптография на протяжении долгого времени остается ключевым методом защиты конфиденциальности, шифруя данные и тем самым затрудняя неавторизованный доступ к информации. Но несмотря на свою важность, она может подвергаться угрозам нападения и взлома, что ставит под риск чувствительную информацию.

В этом контексте стеганография представляет собой метод сокрытия данных внутри медиафайлов, будь то изображения, звуковые файлы или видео [41]. С помощью стеганографии можно маскировать сам акт передачи информации, а не только ее содержимое. Это делает стеганографию особенным инструментом в арсенале защиты данных. Несомненно, прежние подходы к стеганографии не были лишены недостатков и потенциального риска обнаружения, но последние исследования открывают новые горизонты.

В этой связи разработка исследователей из Университета Оксфорда и Университета Карнеги-Меллона, посвященная созданию алгоритма

стеганографии нового поколения. С его помощью информация маскируется настолько искусно, что ее присутствие в носителе становится практически неразличимым [40].

Для тестирования алгоритма команда исследователей использовала несколько видов моделей, автоматически генерирующих контент, а именно языковую модель open source – GPT-2, и преобразователь текста в речь WAVE-RNN [21]. По результатам тестирования новый алгоритм среди различных контекстов применения продемонстрировал прирост эффективности шифрования на 40% по сравнению с ранее известными методами стеганографии, позволив скрывать больше информации в заданном объеме данных [30].

Согласно рисунку 1, в случае использования стеганографии отправитель имеет приватный ключ, открытое сообщение (текст) и случайный источник информации, и формирует стеготекст. Получателю поступает стеготекст, так же, как и злоумышленнику, но отличие заключается в том, что получателю поступает так же и приватный ключ.

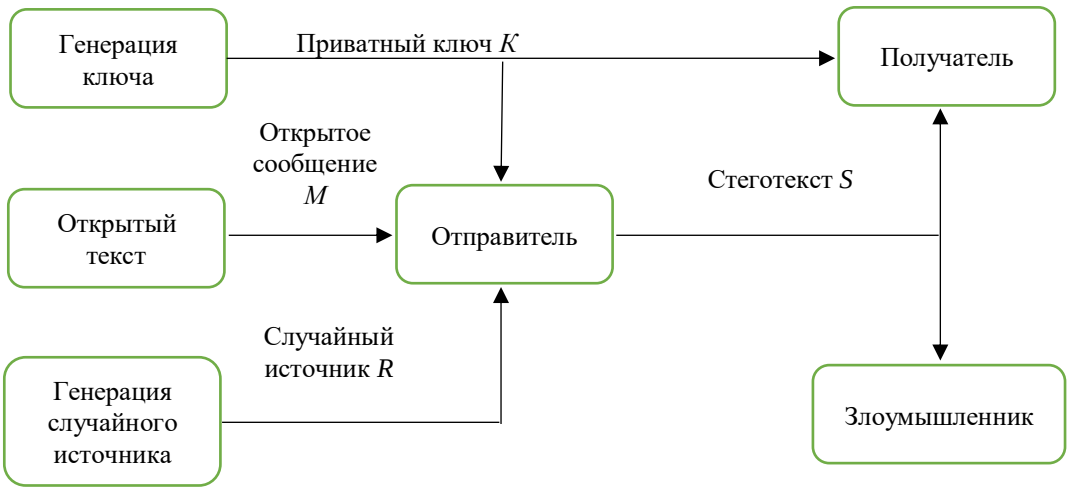


Рисунок 1 – Графическое изображение стеганографии [32]

Объектами, требующими алгоритмической спецификации, которые в совокупности называются стегосистемой, являются генератор ключей, кодер и декодер.

- генератор ключей генерирует закрытый ключ K в виде двоичной строки. Этот закрытый ключ передается отправителю и получателю по защищенному каналу до начала стегопроцесса и может использоваться для координации шифрования и дешифрования. Процесс генерации ключа может быть известен злоумышленнику, но реализация ключа K – нет;
- кодировщик принимает закрытый ключ K, сообщение открытого текста M и случайный источник R в качестве входных данных и создает стеготекст S в пространстве скрытых текстов C;
- декодер принимает закрытый ключ K и стеготекст S в качестве входных данных и возвращает приблизительное текстовое сообщение M.

Многие из описанных объектов, визуально показаны на рисунке 1.

Стеганография предлагает множество применений в нашем цифровом мире. Вот некоторые ключевые сферы, где она может иметь особую ценность:

- социальные сети. Площадки для общения часто становятся мишенями для кибератак. Внедрение нового алгоритма стеганографии позволит пользователям этих платформ защитить свои частные и профессиональные коммуникации, надежно скрывая сообщения и файлы от любого нежелательного наблюдения;
- журналистские расследования. При работе с конфиденциальной информацией журналистам важно защищать себя и свои источники. Благодаря высокому уровню безопасности, новый алгоритм позволит им обмениваться данными без риска их раскрытия;
- гуманитарная помощь. В условиях кризиса и конфликтов гуманитарные работники нуждаются в безопасной коммуникации.

Стеганография обеспечит их способность взаимодействовать и координировать усилия без страха перед слежкой или цензурой;

– сжатие и хранение данных. Новый метод может выступить в роли инструмента для сжатия данных без потерь, тем самым сокращая потребность в объеме памяти для хранения информации. Это может быть важным в индустриях, где величина используемого пространства на накопителях имеет значение, даже если передача информации не связана с высоким уровнем риска.

Таким образом, новые разработки в области стеганографии открывают новые горизонты для безопасности цифровых коммуникаций, делая ее инструментом преобразования различных сфер деятельности.

Однако, как подчеркивают разработчики, абсолютной защиты не существует, и их разработка не является исключением. Алгоритм может быть уязвим для так называемых атак по сторонним каналам, которые исследуют не столько математическую стойкость шифрования, сколько внешние индикаторы, свидетельствующие о его использовании.

Такие атаки могут анализировать поведение устройства: от потребления энергии до характеристик сетевого трафика, чтобы установить факт использования стеганографических методов. Это может позволить злоумышленникам не только обнаружить скрытую коммуникацию, но и потенциально вмешаться в нее [27].

Для минимизации рисков такого воздействия, пользователи должны принимать соответствующие меры предосторожности. Это включает в себя: регулярный аудит программных продуктов, обеспечивающих конфиденциальность; применение алгоритма исключительно в контролируемых, безопасных условиях, где окружение и устройства могут быть оценены на предмет уязвимостей; отказ от использования стеганографии в очень рискованных ситуациях, где даже минимальная вероятность обнаружения может привести к серьезным последствиям [24].

Такие предосторожности являются важной частью адаптации любой технологии сокрытия информации в повседневной жизни и профессиональной деятельности, гарантируя, что пользователи остаются защищенными даже при возможности сложных атак.

1.4 Стратегии и методы комплексной защиты конфиденциальной информации

Обеспечение информационной безопасности предприятий невозможно без целенаправленного использования технических средств и методов, которые являются важной частью защиты, в дополнение к правовым, организационным и прочим мерам [39]. Техническая защита информации (ТЗИ) представляет собой интегрированный подход к предупреждению утечек, несанкционированных действий в отношении информации, её изменения, искажения, копирования, блокировки или уничтожения через технические каналы. ТЗИ выступает в качестве фундаментального элемента комплексной системы информационной безопасности на предприятии [33].

Объекты, на которые распространяется защита в рамках ТЗИ, включают:

- информационные системы и базы данных, архивы и хранилища;
- устройства и системы, на которых осуществляется обработка конфиденциальных данных, включая компьютеры, серверы, сетевые и мобильные устройства;
- помещения и зоны, применяемые для обработки и хранения конфиденциальной информации;
- персонал с разрешенным доступом к защищаемым сведениям.

Разработка и внедрение эффективной системы ТЗИ требует выполнения следующих ключевых шагов [26]:

- определение объема конфиденциальной информации, анализ угроз и потенциальных путей утечки;

- классификация данных и систем по уровню конфиденциальности и требуемой степени защиты;
- оценка рисков для информационной безопасности, идентификация уязвимостей инфраструктуры;
- разработка модели потенциального нарушителя и сценариев атак;
- определение уровня необходимой защиты и выбор соответствующего комплекса технических средств ТЗИ;
- проектирование и реализация системы ТЗИ, в том числе установка оборудования, внедрение мер инженерной и организационной защиты;
- аттестация и сертификация средств и объектов информатизации в соответствии с требованиями безопасности;
- разработка управленческих документов, проведение обучения и инструктажей для персонала по обращению с защищенной информацией;
- постоянный мониторинг инцидентов безопасности, регулярный аудит и проверка эффективности системы ТЗИ.

Важным аспектом качественной реализации мер по технической защите информации (ТЗИ) для компаний является привлечение экспертов с соответствующей квалификацией и опытом в области информационной безопасности. Рекомендуется использование сертифицированных средств ТЗИ, а также опора на передовые практики и международные стандарты, такие как ISO 27001 и ГОСТ Р ИСО/МЭК 15408.

Согласно действующему в России законодательству, оперирование технологиями технической защиты предписано для всей государственной информационной инфраструктуры, систем обработки персональных данных и объектов критического назначения. Коммерческие структуры также активно интегрируют ТЗИ для защиты интеллектуальной собственности, финансовой информации и данных о клиентах. Отдельные сектора, такие как банковская сфера, государственные органы, оборонные комплексы и научные

учреждения, подлежат особенно строгим критериям защиты информации, включая обязательности получения лицензий ФСТЭК и ФСБ, как и сертификации соответствующих технических средств защиты информации.

В категорию программных (или программно-аппаратных) средств ТЗИ входит специализированный софт и встроенные функции безопасности, управляемые операционными системами или приложениями:

- антивирусные программы для защиты от вредоносного ПО;
- системы управления идентификацией и аутентификацией, а также доступом пользователей;
- решения для шифрования и создания защищённых VPN-каналов;
- инструменты для резервирования и восстановления данных;
- утилиты для безопасного удаления информации;
- системы обнаружения и предотвращения несанкционированных вторжений (IDS/IPS);
- инструментарий для анализа и контроля сетевой безопасности.

На российском рынке ведущие позиции занимают разработчики программных средств ТЗИ такие, как «Код безопасности», «Лаборатория Касперского», InfoWatch, «Газинформсервис», «Аладдин Р.Д.».

Аппаратные средства ТЗИ представляют собой оборудование и устройства, предназначенные для физической защиты информационных потоков и носителей:

- модули доверенной загрузки, шифрования;
- смарт-карты, токены, ключевые носители для аутентификации пользователей;
- биометрические системы идентификации;
- аппаратные межсетевые экраны;
- устройства для шифрования сетевых коммуникаций и предотвращения несанкционированного доступа;

– экранирующие средства от электромагнитных и акустических излучений;
– системы защиты от технических средств разведки.

К известным производителям аппаратных средств защиты на российском рынке относятся «Анкад», «МФИ Софт», «Фактор-ТС», «Маском», Kraftway.

При выборе соответствующих ТЗИ необходимо учитывать специфику ИТ-инфраструктуры предприятия, характер обрабатываемых данных. Рекомендуется использование сертифицированных продуктов, таких как Dallas Lock, Secret Net, Аккорд-Win32, которые обеспечивают надежное управление доступом и контроль за действиями пользователей.

Для обеспечения безопасности передачи данных по открытым сетям необходимо применять шлюзы VPN и другие устройства, поддерживающие стандарты ГОСТ-шифрования, например, С-Терра Шлюз, ViPNet Coordinator, Континент, что является залогом защиты информации при её трансляции.

Мониторинг надежности и благонадежности сотрудников является критически важной процедурой для поддержания уровня информационной безопасности предприятия. Для этого используются разносторонние методики и практики, среди которых:

– регулярные проверки с использованием баз данных для поиска негативных изменений в профилях сотрудников;
– применение профайлинга и психологической оценки, нацеленных на выявление признаков демотивации сотрудников;
– наблюдение за коммуникациями и поведением персонала в рабочем цифровом пространстве для раннего выявления подозрительных или нестандартных действий;
– периодическое проведение тестирования на полиграфе в качестве средства проверки и подтверждения добросовестности сотрудников;

– ротация должностных позиций внутри компании и тщательный контроль за процедурой ухода сотрудников с целью предотвратить несанкционированный доступ к конфиденциальной информации после их увольнения.

Выводы по разделу 1

Усилия по поддержанию высокого уровня информационной безопасности должны также включать тренинги на тему техник социальной инженерии, важности соблюдения политики безопасности, а также мотивации сотрудников материально и через систему дисциплинарных мер к неукоснительному следованию установленным правилам. Комбинирование работы с персоналом и грамотно построенной системой технических средств обеспечения безопасности будет способствовать созданию прочного фундамента корпоративной защиты.

Ключевое внимание необходимо уделить деятельности привилегированных пользователей, к которым относятся IT-администраторы, руководители высшего звена, а также сотрудники с расширенным доступом к информации, поскольку именно они обладают наибольшими возможностями влиять на информационную безопасность. Тщательно продуманные процедуры на стадии увольнения сотрудников также предотвращают риск несанкционированного доступа и потенциальных утечек данных.

2 Ключевые аспекты моделей и алгоритмов обмена конфиденциальной информацией

2.1 Историческое развитие и основные этапы эволюции обмена конфиденциальной информацией в организациях

Высокотехнологичная эра информационных систем и всеобъемлющая цифровизация современного общества придают информационной безопасности ключевое значение. Она стала неотъемлемой частью экономического прогресса, гарантией государственного суверенитета и защиты [15].

В истории развития концепций информационной безопасности прослеживаются три ключевых этапа:

Первая фаза характеризуется зарождением идеи защиты данных через применение различных методов и инструментов.

На втором этапе происходит внедрение технических средств для обработки и пересылки данных с использованием электрических сигналов и магнитных полей.

Третья фаза связана с появлением компьютеризированных систем, обеспечивающих автоматизацию процессов обработки, передачи и хранения информации.

Защита конфиденциальной информации на ранних стадиях осуществлялась путем ее шифрования или сокрытия. Несмотря на альтернативы, шифрование выдвинулось как более надежный подход, что способствовало развитию криптографии [22].

В древние времена, в таких цивилизациях как Египет и Китай, использовались простые криптографические методы, включая шифры перестановки и моноалфавитной подстановки. Например, в 100 году до нашей эры был популярен шифр Цезаря — каждая буква в исходном тексте заменялась на другую, которая стоит в алфавите через определенное число

позиций. Также в качестве иллюстрации можно упомянуть полибианский квадрат от древнегреческого мыслителя Полибия.

Понятия Полибия получили дальнейшее развитие в работах немецкого аббата Иоганна Трисемуса, в частности, в создании новой методики шифрования биграмм и применении ключевых слов для заполнения квадрата [16].

В XVIII веке Блез Паскаль заложил основы механических считающих устройств, создав «паскалину». А Томас Джефферсон в XIX веке внес вклад, разработав дисковый шифр и устройство для его реализации – «шифратор». Его работа олицетворяла принципиальные подходы к шифрованию информации.

Кульминацией этой эпохи стали размышления голландского ученого Киркгоффа, который провозгласил золотое правило криптографии, утверждающее, что безопасность шифра основана на конфиденциальности ключа, в отличие от алгоритма шифрования.

С приходом эры роторных машин начинается следующая эра в теории защиты информации. Хотя первые прототипы, такие как устройства Джефферсона, были разработаны ранее, их массовое распространение наступило только в XX веке. Примером служит Enigma, созданная в 1918 году и ставшая основой для полиалфавитного шифрования. Сначала устройство для шифрования секретных сообщений не пользовалось спросом, но в 1926 году им заинтересовался немецкий военно-морской флот. Этот момент можно считать началом использования «Энигмы» в военном деле.

Текст, который нужно было зашифровать, печатался прямо на «Энигме». Перед началом использования оператор открывал крышку аппарата и запоминал настроечную позицию – три номера, которые впоследствии будут нужны для расшифровки сообщения. После этого писался секретный текст, в котором каждый символ менялся на другой, в результате чего сообщения выглядело как случайный набор букв. Механизм замены символов имел алгоритм, который менялся в зависимости от установленных внутрь шестерен.

После написания сообщения, автор передавал записанные заранее три номера радисту, который отправлял их получателю при помощи азбуки Морзе. Человек с другой стороны, имевший такую же «Энигму», ставил машину на ту же настроечную позицию и печатал на аппарате непонятный набор букв. В результате этого действия он получал расшифрованный текст.

Во время второй мировой войны активное использование роторных систем стало вершиной достижений в защите секретной информации того времени. В то же время, методы защиты от технических утечек данных также эволюционировали.

Во второй половине XX века появились полноценные компьютеры, а вместо «Энигмы» и других механических машин для шифрования информации используются компьютерные алгоритмы. По сути, они делают то же самое, что и «Энигма», но максимально быстро и с наиболее высокой надежностью. Если для расшифровки сообщения требуются недостижимые компьютерные мощности или очень много времени, считается, что алгоритм шифрования имеет максимальную криптографическую стойкость [19].

Современный этап тесно связан с созданием и усовершенствованием первых электронно-вычислительных машин, что позволило внедрять сложные блочные шифры. Отличительным достижением периода стал стандарт DES, утвержденный в США в 1977 году и созданный корпорацией IBM. DES – это блочный шифр, основанный на сети Фейстеля. Шифр имеет размер блока 64 бита и размер ключа 56 бит [13].

На основе анализа схемы на рисунке 2 можно выделить конкретные шаги процесса шифрования, выполненные над исходным текстом [43].

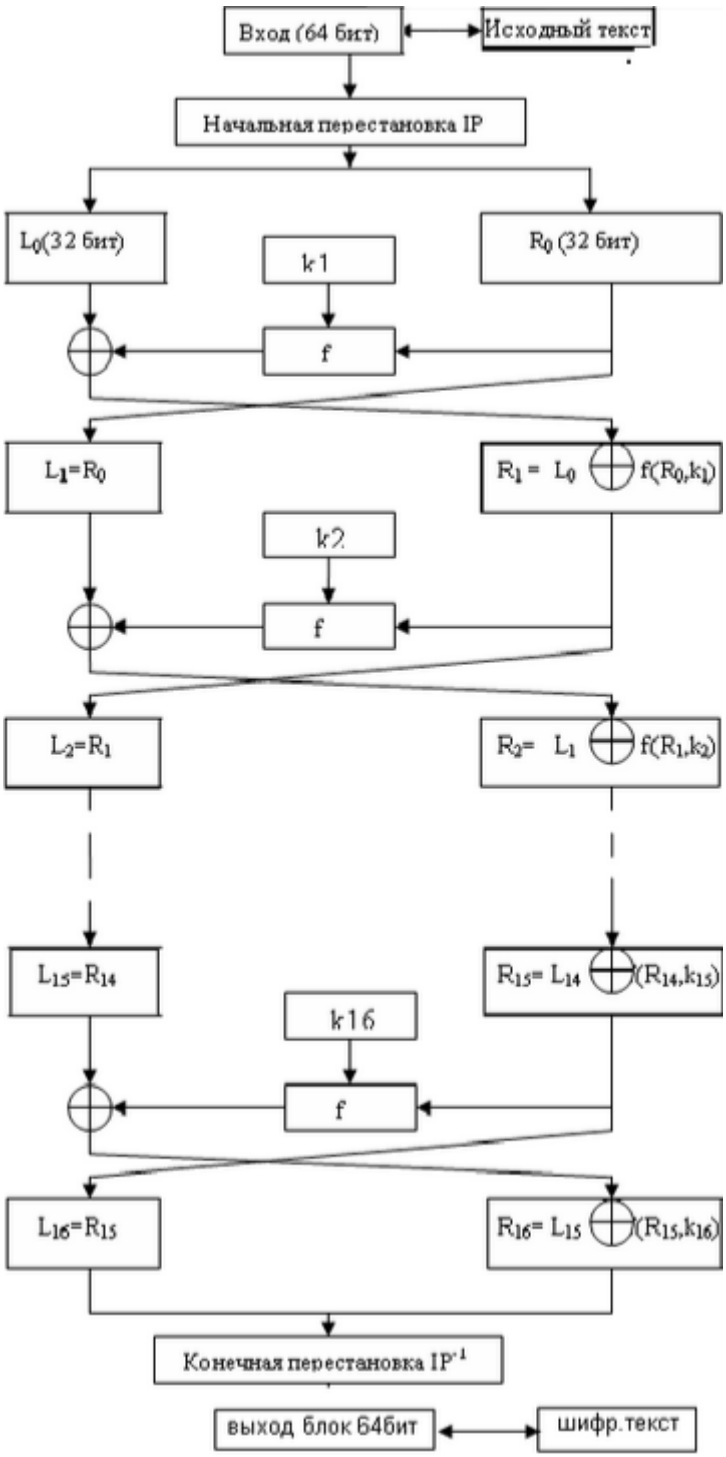


Рисунок 2 – Схема шифрования алгоритма DES

Начинается процесс с начальной перестановки битов исходного блока данных, при которой происходит их перемешивание в соответствии с определённой схемой. Следующий этап включает в себя деление перемешанных битов на две равные части и их подачу на вход функции

Фейстеля. В случае использования сети Фейстеля в стандартном алгоритме DES предусмотрено 16 итераций, хотя доступны и иные модификации, подразумевающие различное количество раундов. Заканчивается процедура тем, что результаты последнего раунда преобразований объединяются и подвергаются заключительной перестановке битов для получения финального текста.

Первая успешная атака на алгоритм шифрования DES была зафиксирована в 1993 году, через 16 лет после его официального принятия в качестве стандарта. Использованный метод линейного криптоанализа, предоставляющий возможность вскрыть секретный шифровальный ключ DES при совершении 243 операций при наличии 247 пар открытых и зашифрованных текстов, стал прорывом в области криптографии. Впоследствии подобный тип анализа был адаптирован для взлома других блочных алгоритмов, включая AES, введённый в 1998 году, и «Кузнечик», созданный в 2015 году.

Линейный криптоанализ представляет собой метод атаки на симметричные шифры, цель которого – восстановление неизвестного ключа шифрования на основе анализа имеющихся открытых текстов и соответствующих зашифрованных сообщений. В классической модели атака через линейный криптоанализ предполагает, что атакующий располагает обширным набором пар "открытый текст/шифрованный текст", сгенерированных с применением одного и того же ключа K. Задача атакующего заключается в частичной или полной реконструкции ключа шифрования K.

В 1989 году был стандартизирован алгоритм блочного шифрования «Магма» и, с зафиксированными блоками нелинейной подстановки, наряду с алгоритмом «Кузнечик», был включен в национальный стандарт ГОСТ Р 34.12-2015 [7] и межгосударственный стандарт ГОСТ 34.12-2018 (взамен ГОСТ 28147-89 в части раздела 1 «Структурная схема алгоритма криптографического преобразования» [6]).

В указанном ГОСТе, регулирующим стандарты криптографической защиты информации, описаны блочные алгоритмы шифрования, получившие наименования "Кузнечик" и "Магма". "Кузнечик" оперирует блоками информации размером в 128 бит, тогда как "Магма" работает с 64-битными блоками. Тем не менее, для обоих алгоритмов установлен стандартный размер ключа шифрования в 256 бит.

Процедура шифрования "Кузнечиком" разбита на 10 раундов обработки исходного текста. В ходе каждого раунда из первичного шифровального ключа генерируются два раундовых ключа, которые принимают непосредственное участие в последующих трансформациях. В рамках каждого раунда реализуются два основных этапа: подстановка и перестановка. Подстановка включает замену элементов данных в соответствии с определённой таблицей замен, в то время как перестановка меняет порядок битов в блоке согласно схеме перестановки.

Перестановки, в частности, привлекают внимание при проведении криптоанализа. Они служат для повышения стойкости алгоритма к различным видам атак, распределения влияния отдельных битов исходного текста по всему тексту и обеспечения сложности восстановления исходных данных без знания ключа шифрования.

Приведем упрощенную схему работы «Кузнечика» при шифровании (рисунок 3).

Рисунок 3 – Схема работы алгоритма шифрования «Кузнечик»

Расшифрование Кузнечиком реализуется путем использования обратных операций подстановки и перестановки в инвертированном порядке, также, в обратном порядке следуют и раундовые ключи (рисунок 4).

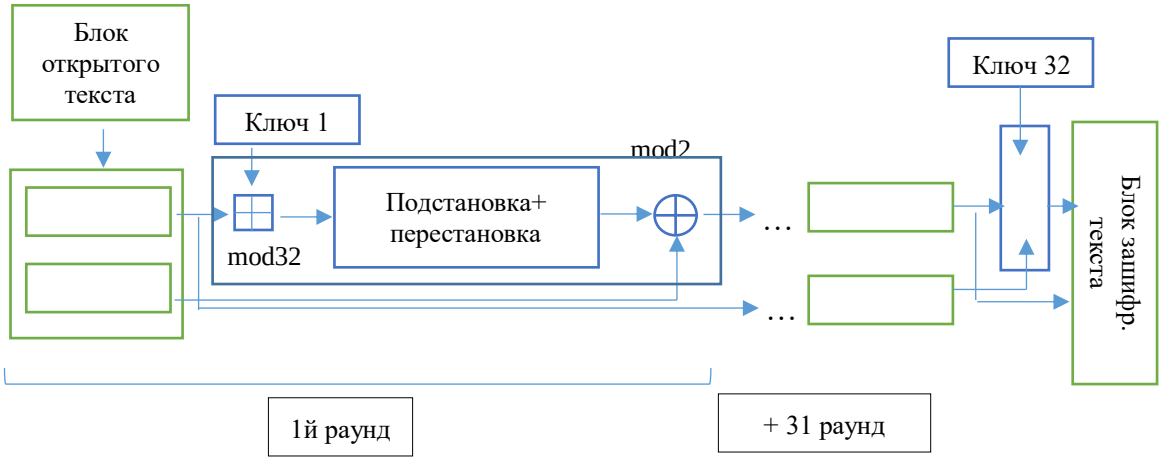


Рисунок 4 – Схема работы алгоритма дешифрования «Кузнечик»

В рамках европейского проекта NESSIE, инициированного в 2000 году для идентификации и анализа надежных методов криптографической защиты, потребность в разработке безопасных шифровальных алгоритмов привлекла внимание специалистов по всему миру. В числе разработчиков заслуживает внимания работа Анатолия Лебедева и Алексея Волчкова, создавших для российской организации LAN Crypto блочный алгоритм симметричного шифрования NUSH.

Алгоритм NUSH представлен разнообразием вариаций, характеризующихся различной длиной ключа – от 64 до 256 битов – а также количеством криптографических раундов. Центральным элементом этого механизма является принципиальное отсутствие традиционных S-блоков и P-блоков, которые обычно находят применение в подобных системах. Основой шифрования в NUSH служат исключительно арифметические операции такие, как XOR, AND и другие, позволяя процессу шифрования проходить с высокой скоростью.

Таким образом, алгоритм NUSH выделяется среди первопроходцев проекта NESSIE благодаря своей уникальной структуре и оптимизированному вычислительному процессу, обеспечивающему ускоренное выполнение операций шифрования без снижения уровня безопасности.

Таким образом, современность характеризуется множеством публикаций, раскрывающих различные аспекты информационной безопасности. Эта область приобретает особую актуальность на фоне убытков, связанных с киберпреступностью, и угрозами безопасности данных как в государственных, так и в частных секторах.

2.2 Современные тенденции и вызовы в области защиты конфиденциальной информации

В современном мире информационные технологии играют ключевую роль в жизни как отдельных людей, так и организаций. С увеличением объема передаваемой информации и расширением цифровых взаимодействий возрастает и угроза кибератак, что делает вопрос безопасности особенно актуальным. Множество компаний и пользователей сталкиваются с проблемами потери данных, финансовых убытков и повреждения репутации из-за недостаточных мер защиты.

Понимание важности безопасности в информационных технологиях позволяет не только минимизировать возможные риски, но и развивать доверие пользователей к продуктам и услугам. Эффективные стратегии безопасности помогают защитить конфиденциальную информацию и обеспечить целостность данных, что особенно важно в условиях постоянного роста числа киберугроз.

Ключевые аспекты безопасности в IT:

– обучение сотрудников: повышение осведомленности о киберугрозах и обучение принципам безопасности является первым шагом к созданию безопасной ИТ-среды.

- использование технологий защиты: установка антивирусного программного обеспечения и фаерволлов помогает предотвратить несанкционированный доступ.
- регулярные обновления: обновление программного обеспечения и систем помогает устранить уязвимости и защитить от новых угроз.
- резервное копирование данных: регулярное создание резервных копий позволяет восстановить информацию в случае повреждения или потери данных;
- необходимо помнить, что безопасность в информационных технологиях – это непрерывный процесс. С увеличением сложностей и масштабов кибератак компании и пользователи должны быть готовы к постоянным изменениям и адаптации своих стратегий безопасности.

В 2025 году информационная безопасность сталкивается с рядом серьезных угроз, которые могут оказать значительное влияние на организации и пользователей по всему миру. Развитие технологий, а также увеличение числа кибератак требуют от специалистов по безопасности постоянного обновления знаний и навыков. Актуальные угрозы разнообразны и требуют комплексного подхода к их преодолению.

Одной из ключевых проблем остается социальная инженерия, которая активно используется злоумышленниками для манипуляции людьми и получения доступа к конфиденциальной информации. Разработка эффективных стратегий защиты требует глубокого анализа новых методов и инструментов, используемых преступниками.

Ключевые угрозы информационной безопасности:

- фишинг: атаки на пользователей с целью кражи учетных данных и финансовой информации через поддельные сайты и электронные письма.

- вредоносное ПО: увеличение числа вирусов, троянов и шифровальщиков, которые могут повредить компьютерные системы и зашифровать важные данные;
- уязвимости в программном обеспечении: использование слабых мест в системах для воздействия на организацию и получения несанкционированного доступа;
- угрозы от insiders: риски, связанные с сотрудниками компании, которые могут намеренно или по неосторожности раскрыть важную информацию;
- интернет вещей (IoT): устройства, подключенные к интернету, становятся все более уязвимыми для атак, что может вести к утечке данных или физическим повреждениям.

В связи с возрастанием этих угроз, организации должны принимать меры для защиты своих информационных систем. Это включает в себя регулярные обучения персонала, внедрение современных технологий безопасности и проведение регулярных аудитов систем на наличие уязвимостей.

С ростом числа кибератак и увеличением их сложности, вопрос обеспечения безопасности в информационных технологиях становится все более актуальным. Организации и частные пользователи должны разрабатывать и внедрять эффективные стратегии для защиты своих данных и систем. Существует множество методов профилактики, которые помогают минимизировать риски и обеспечить надежную защиту от потенциальных угроз.

Одним из основных компонентов комплексной безопасности является использование антивирусного программного обеспечения. Однако на этом уровне защита не заканчивается. Необходимы дополнительные меры, такие как использование фаерволов, шифрование данных и регулярные обновления программного обеспечения.

Ключевые стратегии защиты:

– антивирусные программы: эти инструменты помогают обнаруживать и удалять вредоносные программы. регулярные обновления вирусных баз обеспечивают защиту от новых угроз;
– фаерволы: фаерволы могут быть аппаратными или программными и предназначены для фильтрации входящего и исходящего трафика. они создают барьер между внутренними системами и внешними угрозами;
– шифрование данных: шифрование является важным способом защиты конфиденциальной информации. даже в случае утечки данных, они останутся недоступными для злоумышленников;
– регулярные обновления: поддержание программного обеспечения в актуальном состоянии снижает уязвимости и защищает от эксплоитов.

Кроме этих мер, важно также проводить обучение сотрудников по лучшим практикам кибербезопасности, чтобы избежать человеческого фактора, часто являющегося причиной успешных атак. Таким образом, внедрение комплексного подхода к безопасности, включающего все вышеперечисленные стратегии, поможет значительно снизить риски кибератак и укрепит информационную безопасность организации.

В условиях постоянного увеличения числа кибератак, осведомленные пользователи способны выявлять нестандартные ситуации и недостатки безопасности. Они могут предотвратить возможные нарушения безопасности благодаря соблюдению ряда простых, но эффективных правил:

Основные принципы обеспечения безопасности данных:

– регулярное обновление программного обеспечения: обновления часто содержат исправления уязвимостей;
– использование сложных паролей: длительные и комбинационные пароли значительно затрудняют задачу злоумышленникам;
– фишинг: осведомленность о фишинговых атаках помогает распознать подозрительные сообщения и ссылки;

– безопасное поведение в сети: пользователи должны избегать обмена личной информацией на сомнительных сайтах.

Кроме того, для повышения уровня пользовательской осведомленности организации могут проводить регулярные тренинги и семинары, которые помогают сотрудникам осваивать современные техники защиты данных и понимать потенциальные угрозы. Эффективная коммуникация внутри компании будет способствовать созданию культуры безопасности.

В конечном итоге, именно осведомленные пользователи становятся первой линией обороны, защищая не только себя, но и всю организацию от киберугроз.

Существует несколько типов шифрования, каждый из которых имеет свои особенности и применяется в различных ситуациях: симметричное (AES, DES). Асимметричное (RSA, ECC), хеширование. Основные методы шифрования включают симметричное и асимметричное шифрование, а также хеширование (SHA-256, MD5). Каждый из этих методов имеет свои преимущества и недостатки, и выбор подходящего метода зависит от конкретных потребностей организации или индивидуального пользователя.

Шифрование данных становится особенно актуальным с ростом числа кибератак и утечек информации. Организации все чаще применяют шифрование для защиты своих продуктов и услуг, а также для соответствия международным стандартам и законодательным требованиям. Эффективная стратегия шифрования должна включать не только технические аспекты, но и грамотное управление ключами, которое обеспечивает безопасность всего процесса.

Существующие институты и стандарты безопасности помогают организациям выстраивать эффективные стратегии защиты информации, упрощая процесс управления рисками и соблюдения законодательства. Они обеспечивают единые подходы и практики, которые способствуют улучшению общего состояния безопасности как на уровне отдельно взятой компании, так и в масштабе всей отрасли.

Основные институты и стандарты безопасности:

- ISO/IEC 27001 – международный стандарт для систем управления информационной безопасностью, который описывает требования к организации и управлению процессами в области защиты информации;
- NIST – Институт стандартов и технологий США, который разрабатывает и публикует исследования и руководства по безопасности информационных технологий;
- COBIT – фреймворк для управления IT-услугами, который предлагает лучшие практики по управлению рисками и обеспечению безопасности;
- PCI DSS – стандарт безопасности данных платежных карт, который необходим для обеспечения безопасности финансовой информации в электронных транзакциях.

Следует отметить, что соблюдение стандартов безопасности не только помогает защитить информацию, но и повышает доверие со стороны клиентов и партнеров. Организации, стремящиеся к соответствию установленным стандартам, показывают свою приверженность к защите данных и готовность реагировать на возникающие угрозы. Это позволяет им не только защищать свои активы, но и укреплять свою репутацию на рынке:

– проведение регулярных аудитов безопасности;

– обучение сотрудников основам информационной безопасности;

– разработка и внедрение планов реагирования на инциденты;

Анализ инцидентов в области безопасности информационных технологий представляет собой критически важный процесс, позволяющий организациям выявлять, оценивать и исправлять причины инцидентов. Этот процесс не только способствует восстановлению нормального функционирования систем, но и предоставляет ценную информацию, которая может быть использована для предотвращения повторения ошибок в будущем.

Эффективный анализ инцидентов требует системного подхода, включающего сбор данных, их обработку и извлечение уроков.

Важность своевременного и тщательного анализа инцидентов не может быть переоценена. Он помогает не только уменьшить риск повторного возникновения аналогичных проблем, но и повысить общую уровень безопасности в организации. Правильно наладив анализ инцидентов, компании могут развивать свои стратегии безопасности, адаптируясь к постоянно меняющимся угрозам и вызовам.

Основные шаги в анализе инцидентов:

- сбор информации: начинать необходимо с документирования всех аспектов инцидента. следует включить временные метки, систему, пользователя и тип уязвимости;
- классификация инцидента: оценка серьезности инцидента и его влияние на бизнес-процессы. это поможет правильно расставить приоритеты в решении проблем;
- определение первопричины: использование методов, такие как «пять почему», для глубокого анализа инцидента и понимания причин его возникновения;
- разработка плана действий: после выявления причин - формулировка рекомендаций и необходимых изменений в процессах, которые помогут закрыть уязвимости;
- оценка результатов: после внедрения изменений важно анализировать их эффективность и вносить коррективы при необходимости.

Следуя этим шагам, организации могут не только реагировать на инциденты, но и проактивно предотвращать их появление в будущем. Создание культуры безопасности и непрерывного обучения внутри компании должно стать одним из ключевых аспектов в ее стратегии по управлению рисками.

В свете стремительного развития технологий и растущих угроз в киберпространстве, вопрос безопасности в информационных технологиях становится все более важным. С каждым годом кибератаки становятся более изощренными, а методы защиты требуют постоянного обновления. Реакция на возникающие угрозы становится одной из приоритетных задач для организаций всех размеров и сфер деятельности.

Однако будущее безопасности в информационных технологиях несет в себе не только вызовы, но и возможности. Новейшие технологии, такие как искусственный интеллект и machine learning, предлагают новые подходы к идентификации и реагированию на угрозы, что может значительно повысить уровень защиты данных.

Основные тренды и прогнозы:

- увеличение использования AI и Machine Learning: эти технологии будут играть ключевую роль в автоматизации процессов безопасности, позволяя быстрей адаптироваться к новым угрозам.
- развитие облачных технологий: с переходом на облачные сервисы безопасность станет более распределенной, что потребует новых методов шифрования и аутентификации;
- новые законодательные инициативы: компании будут обязаны соблюдать нарастающие требования со стороны регуляторов, что повлияет на стратегии безопасности;
- интернет вещей (IoT): с увеличением количества подключенных устройств возрастет необходимость в защита IoT-экосистем, что станет новой проблемой для специалистов по безопасности;
- фокус на человеческий фактор: Понимание важности обучения сотрудников станет ключевым аспектом в борьбе с киберугрозами.

Подводя итог, можно сказать, что будущее безопасности в информационных технологиях будет определяться как инновациями, так и изменяющимися угрозами. Организациям необходимо оставаться гибкими и готовыми к адаптации новых решений, чтобы эффективно защищать свои

данные в постоянно меняющемся киберпространстве. Безопасность будет оставаться неотъемлемой частью стратегического планирования, и ее значимость в будущем только возрастет.

2.3 Сравнительный анализ различных моделей и алгоритмов обмена конфиденциальной информацией

В контексте информационной безопасности, передача конфиденциальных данных является критическим элементом защиты информационных активов организации. Эта защита достигается не только с помощью передовой технологической базы, но и через применение эффективных методов и алгоритмов, направленных на обеспечение конфиденциальности, целостности и доступности данных в ходе их передачи.

Рассмотрим модели и алгоритмы обмена конфиденциальной информацией, включая симметричную и асимметричную криптографию, а также современные гибридные подходы, обеспечивающие баланс между безопасностью и вычислительной нагрузкой.

Симметричное шифрование представлено различными протоколами, которые используют потоковый метод шифрования.

В потоковом шифре за один раз шифруется один байт, в то время как в блочном шифре за один раз шифруется приблизительно 128 бит. Первоначально ключ (k) передается в качестве входных данных в генератор псевдослучайных битов, а затем он выдает случайный 8-битный выходной сигнал, который будет обрабатываться как поток ключей. Результирующий поток ключей будет иметь размер 1 байт, т.е. 8 бит. Потоковые шифры быстры, поскольку они шифруют данные бит за битом или байт за байтом, что делает их эффективными для быстрого шифрования больших объемов данных.

Потоковые шифры хорошо подходят для обмена данными в режиме реального времени, например, для потоковой передачи видео или онлайн-игр,

поскольку они могут шифровать и расшифровывать данные по мере их передачи (рисунок 5).

Для шифрования:

– обычный текст и поток ключей генерируют зашифрованный текст (тот же поток ключей будет использоваться для расшифровки);
– открытый текст поэтапно подвергается операции XOR (исключающее ИЛИ) с потоком ключей и генерирует зашифрованный текст.

Например:

Plain Text: 10011001

Keystream: 11000011

,,

Cipher Text: 01011010

Для расшифровки:

– зашифрованный текст и поток ключей предоставляют исходный открытый текст (тот же поток ключей использовался для шифрования);
– зашифрованный текст будет подвергаться побитовой операции XOR с потоком ключей и генерировать фактический открытый текст.

Cipher Text: 01011010

Keystream: 11000011

,,

Plain Text: 10011001

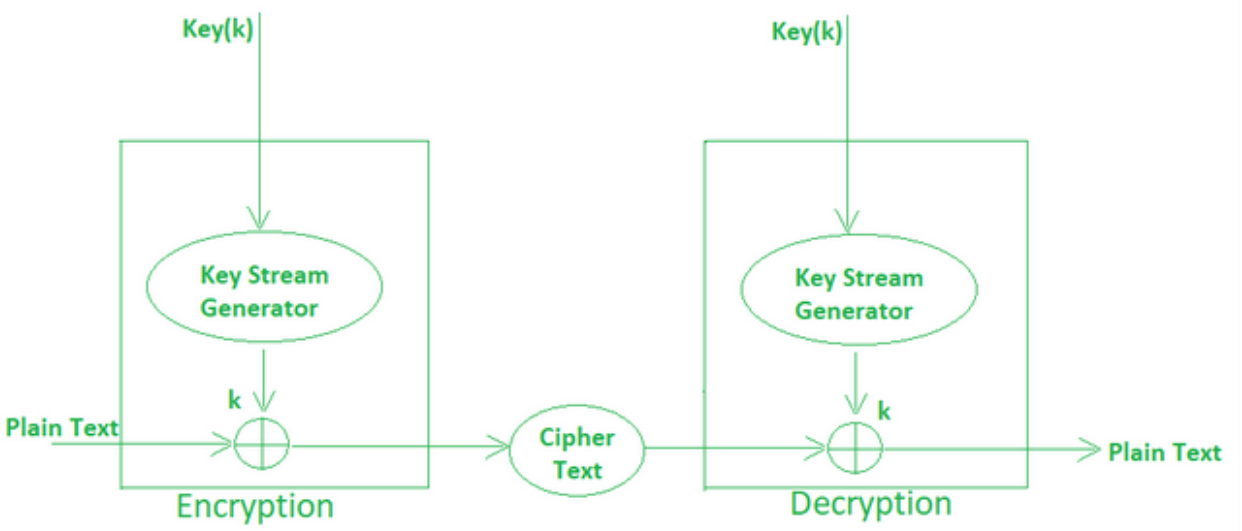


Рисунок 5 – Схема работы потокового шифрования/дешифрования

Потоковые шифры обладают многими преимуществами, такими как:

- скорость: как правило, этот тип шифрования работает быстрее блочных шифров;
- низкий уровень сложности: потоковые шифры просты в реализации в современном программном обеспечении, и разработчикам не требуется для этого сложного оборудования;
- последовательный характер: некоторые компании обрабатывают сообщения, записанные непрерывным образом. Потоковые шифры позволяют им передавать данные, когда они готовы вместо того, чтобы ждать, пока все будет завершено, благодаря их побитовой обработке;
- доступность: использование симметричных методов шифрования, таких как потоковые шифры, избавляет предприятия от необходимости иметь дело с открытыми и закрытыми ключами. Кроме того, компьютеры могут выбирать подходящий ключ дешифрования для использования благодаря математическим концепциям, лежащим в основе современных потоковых шифров.

Недостатки потоковых шифров:

- если во время передачи возникает ошибка, это может повлиять на последующие биты, потенциально повреждая все сообщение, поскольку потоковые шифры полагаются на ранее сохраненные биты шифра для расшифровки;
- поддержание и правильное распределение ключей для потоковых шифров может быть сложной задачей, особенно в крупных системах или сетях;
- некоторые потоковые шифры могут быть предсказуемыми или уязвимыми для атак, если их поток ключей не разработан должным образом, что потенциально может поставить под угрозу безопасность зашифрованных данных.

Таким образом, симметричные шифры предлагают быструю и энергоэффективную обработку данных благодаря поддержке ключевой длины от 128 до 256 бит. Несмотря на это, безопасность целиком зависит от механизмов распределения ключей и устойчивости генератора случайных чисел.

Протокол Diffie-Hellman (алгоритм с симметричным ключом) позволяет двум сторонам создавать общий секретный ключ, даже если они взаимодействуют через незащищенный канал. Он обладает простотой реализации, но требует дополнительных мер безопасности для защиты от атак типа «человек посередине».

Инфраструктура открытых ключей (PKI) обеспечивает надежную аутентификацию и управление ключами посредством сертификационных центров и системы доверенных цифровых сертификатов. PKI предпочтительна для масштабных сетевых структур и предприятий с многочисленными пользовательскими точками доступа, хотя и связана с серьезными инвестициями в реализацию и поддержку.

Таким образом, для защиты конфиденциальной информации важно рассматривать специфику системы и соотносить требования к безопасности и ресурсным затратам для выбора оптимального решения в контексте

информационной безопасности. В мире, где передача данных является повседневной необходимостью, тщательное использование защитных моделей и алгоритмов становится неотъемлемым фактором успешной и безопасной деятельности любой организации.

Алгоритм RSA является асимметричным и работает на основе пары ключей, что делает его сложным для факторизации на крупные числовые составляющие. Он особенно ценится за сильную защиту и решение задачи обмена ключами за счет криптостойкости. Однако, его применение ограничено высокими требованиями к вычислительным ресурсам, особенно при обработке крупных объемов информации, и в сравнении с симметричными методами, он обладает уменьшенной производительностью.

Алгоритм ElGamal расширяет возможности асимметричной криптографии, основываясь на принципах дискретного логарифмирования для шифрования и создания цифровых подписей. Он характеризуется высоким уровнем защиты и пригоден для использования в составе гибридных криптосистем. Однако следует учитывать, что шифротексты, получаемые с использованием ElGamal, зачастую обладают значительным размером и требуют значительных вычислительных ресурсов для их обработки.

SSL/TLS – этот протокол использует комбинацию симметричного и асимметричного шифрования. Он стал де-факто стандартом для обеспечения защищенной коммуникации в Интернете. Его основные функции – это аутентификация, шифрование и обеспечение целостности данных при их передаче. Интеграция этого протокола в веб-приложения проста, что обеспечивает его широкое применение, особенно в интернет-банкинге и электронной коммерции. Тем не менее, его надежность зависит от актуальности используемой версии и корректности конфигурации, а также от надежности сторонних центров сертификации.

Протокол Quantum Key Distribution (QKD) представляет собой передовую технологию, базирующуюся на принципах квантовой механики, позволяющую достичь нового уровня безопасности в области распределения

ключей. Данный метод исключает любые возможности незамеченного перехвата ключей, предполагая «абсолютную» безопасность переговоров. Однако QKD требует специализированного и дорогостоящего оборудования и пока что ограничена в применимости дальностью квантовых каналов связи.

Комплексная защита конфиденциальной информации в компьютерных сетях предполагает не только выбор подходящего алгоритма с учетом специфики и потребностей организации, но и стратегическое планирование криптографической архитектуры в целом. В структурах, где совмещаются несколько криптографических решений, гибридные системы защиты показывают себя особенно эффективными, так как они способны уравновешивать преимущества устойчивости к атакам и требования к вычислительной производительности.

Безусловно, когда ассиметричное и симметричное шифрование используются в комплексе, это позволяет достигать хороших результатов:

Безопасность обмена ключами:

– симметричная криптография. Криптография с открытым ключом/ обменом ключами – это еще один метод использования идентифицированных ключей, при котором асимметричное шифрование обеспечивает безопасный качественный обмен ключами по небезопасному пути. Это происходит потому, что человеку легче делиться общедоступными данными, в то же время сохраняя секретный ключ при себе, чтобы не позволить другим людям получить доступ;
– асимметричная криптография. После обмена симметричным ключом с помощью асимметричного шифрования фактическое шифрование и дешифрование данных эффективно выполняется с использованием симметричного ключа.

Эффективность и быстродействие:

– симметричная криптография. AES и аналогичные алгоритмы симметричного шифрования не рассчитаны на высокую скорость, поэтому не подходят для шифрования больших объемов данных;
– асимметричная криптография. Асимметричное шифрование вычислительно медленнее, чем симметричное, но оно играет очень важную роль в обмене ключами, так что может быть достигнуто реальное шифрование и дешифрование, которые выполняются на очень высоких скоростях.

Безопасность и практичность:

– асимметричная криптография. Предлагает надежные методы защищенной передачи симметричных ключей и подписей, необходимых для подтверждения канала связи только предполагаемыми участниками;
– симметричная криптография. обеспечивает удовлетворительное, быстрое и безопасное шифрование для передачи необработанных данных после совместного использования симметричного ключа.

Аутентификация и целостность:

– асимметричная криптография. Пример цифровых подписей с асимметричным ключом используется при отправке входящих сообщений для аутентификации отправителя и гарантии целостности сообщения. Это позволяет максимально точно проверить подлинность данных и личность отправителя;
– симметричная криптография. Во время сеанса связи данные также защищены с помощью симметричного шифрования после создания защищенного канала.

Протоколы и приложения реального мира:

– гибридный подход. Что касается протоколов защищенной связи, то SSL/TLS являются яркими примерами гибридного подхода. Они используют симметричные ключи для первого подключения, чтобы обеспечить безопасный обмен ключами с использованием

асимметричных ключей. Таким образом, после этого симметричный ключ используется в течение оставшейся части сеанса, обеспечивая необходимую эффективность шифрования;

Целостность и подлинность. Симметричное и ассиметричное шифрование может быть использовано для разработки цифровых подписей, которые будут полезны для сохранения целостности и аутентичности данных. Отправитель использует закрытый ключ для шифрования своего сообщения, а получатель проверяет это с помощью открытого ключа отправителя.

Таким образом, современная коммуникация обеспечивает высокую безопасность асимметричной криптографии для обмена ключами и скорость использования симметричной криптографии для шифрования данных.

2.4 Влияние законодательных и нормативных требований на обмен конфиденциальной информацией

Обеспечение информационной безопасности и защита сведений ограниченного доступа регламентируются ключевым нормативным правовым актом – Федеральным законом № 149-ФЗ "Об информации, информационных технологиях и защите информации". Данное закон содержит ряд правовых механизмов защиты данных, а также определяет ответственность за нарушения в данной сфере.

Юридическое регулирование в области информационной безопасности направлено на:

- предотвращение неавторизованного доступа к информации с ограниченным доступом;
- постоянное поддержание режима ограниченного доступа;
- реализацию права на доступ к данным с ограничениями;
- непрерывный контроль за уровнем защиты информации;
- восстановление информации после инцидентов;

– размещение баз данных с ограниченным доступом на территории Российской Федерации.

Методы защиты конфиденциальной информации классифицируются следующим образом:

– физическая защита включает использование сейфов или специализированных помещений, доступ в которые строго ограничен;
– аппаратная защита предполагает применение защищенного оборудования и постоянное наблюдение за его состоянием для исключения несанкционированного доступа;
– программная защита обеспечивается путем использования программ, обеспечивающих блокировку несанкционированных действий и предотвращение утечек;
– математическая (криптографическая) защита используется для шифрования данных, чтобы сделать их нечитаемыми без соответствующих ключей [8], [34].

Согласно статье 17 Федерального закона № 149-ФЗ, нарушение правил о защите конфиденциальных сведений влечет за собой юридическую ответственность, которая может выражаться в различных формах:

– дисциплинарная ответственность применяется к сотрудникам за несоблюдение внутренних правил;
– гражданско-правовая ответственность предполагает взыскание убытков за причинение вреда раскрытием конфиденциальной информации;
– административная ответственность применяется за нарушения, предусмотренные Кодексом об административных правонарушениях;

– уголовная ответственность может наступить за особо серьезные преступления в сфере информационной безопасности, включая хакерские атаки.

Положения многочисленных законов и подзаконных актов комплексно регулируют охрану сведений ограниченного доступа, выступая гарантом их надежной защиты и сохранности в правовом смысле.

К ключевым международным стандартам можно отнести Общий регламент по защите данных (GDPR) в Европейском Союзе, который вводит строгие требования к обработке персональных данных граждан ЕС, а также Закон о защите личной информации и электронных документов (PIPEDA) в Канаде, Закон о защите приватности в цифровом веке (CCPA) в Калифорнии, США. Также действует международный стандарт ISO/IEC 27001, который устанавливает требования к системам менеджмента информационной безопасности (ISMS), обеспечивающим защиту информации независимо от ее формы.

Эти международные стандарты и соглашения требуют от организаций разработки комплексных программ защиты данных, включающих технические и организационные меры по предотвращению утечек данных, внедрение процессов управления рисками, а также регулярный аудит и контроль соответствия. Обеспечение комплаенса (соответствия требованиям) не только снижает риск возможных нарушений и утечек данных, но и становится важным фактором в установлении доверия со стороны клиентов, партнеров и государственных органов.

В отношении национальных нормативных правовых требований можно выделить, например, Федеральный закон № 390-ФЗ «О безопасности» [5] уточняет правовые основы, обеспечивающие личную, общественную и государственную безопасность, определяя функции системы безопасности, порядок организации и финансирования деятельности соответствующих органов, а также осуществление контроля и надзора за их работой.

Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3] устанавливает базовые положения для регулирования отношений в области информации и защиты информации, формулирует основные понятия и принципы, а также классифицирует информацию на основе категорий доступа.

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» [2] устанавливает правовые основы деятельности в области связи на территории Российской Федерации. Статья 63 «Тайна связи» данного ФЗ гласит, что на территории РФ гарантируется тайна сообщений, передающихся по сетям электросвязи и сетям почтовой связи.

Эти и другие нормативные правовые акты составляют фундамент правовой системы, направленной на защиту информационных ресурсов и национальное информационное пространство России.

Среди дополнительных актов можно отметить Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [6] устанавливает запрет подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну к информационно-телекоммуникационным сетям международного информационного обмена. В целях защиты информации государственные органы обязаны использовать только средства защиты информации, прошедшие сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данных требований Указа в полной мере должно обеспечить защиту информации, составляющей государственную тайну.

2.5 Проблемы и ограничения существующих моделей и алгоритмов

В сфере информационной безопасности и обмена конфиденциальными данными, существуют разнообразные модели и алгоритмы защиты, разработанные для предотвращения несанкционированного доступа и утечки информации. Не смотря на значительные успехи в этой области, остается ряд нерешенных проблем, влияющих на их эффективность в практической плоскости.

Рассмотрим основные из этих проблем:

- масштабируемость. модели защиты, эффективные в меньших масштабах, часто страдают при увеличении объема данных и числа пользователей. например, алгоритмы симметричного шифрования, типа AES, могут и требуют значительных вычислительных мощностей в условиях крупного предприятия, что ставит под вопрос их применимость в больших масштабах;
- задержки и производительность. основательная защита конфиденциальной информации, особенно с использованием асимметричного шифрования, как правило, сопряжена с высокими требованиями к вычислительным ресурсам. это ведет к росту задержек, снижению производительности и может быть критическим для приложений реал-тайм коммуникаций;
- совместимость и интеграция. многие из современных решений защиты данных трудно интегрировать с устаревшей технологической инфраструктурой, что требует дополнительных усилий и затрат для обновления систем безопасности в уже работающих организациях;
- управление ключами. Эффективное управление ключами – это сложный процесс, который включает в себя их создание, распределение, обновление и уничтожение. Симметричные системы шифрования подразумевают обмен ключами между

отправителем и получателем, что представляет собственные риски. В то же время, управление большими списками публичных и приватных ключей для асимметричных систем может быть чрезвычайно затратным;

– уязвимости и атаки. По сути, любая система защиты обладает определенными уязвимостями, которые можно эксплуатировать. Это включает в себя сторонние каналы, которые могут быть потенциально использованы для получения конфиденциальной информации, угрозу квантовых вычислений и т.д. Человеческий фактор также существенен - ошибки пользователей, такие как использование слабых паролей или неправильные настройки, могут нивелировать преимущества самых надежных алгоритмов.

Эти проблемы подчеркивают сложность обеспечения безопасности информации в многообразии условий современного информационного общества, и необходимость постоянного развития в этой области для соответствия меняющимся требованиям и технологическим вызовам:

– сложности в обеспечении конфиденциальности и целостности данных. Вопросы обеспечения конфиденциальности и целостности данных все еще представляют серьезные сложности в сегодняшней информационной безопасности. Многие текущие криптографические системы ориентированы либо на защиту секретности информации, либо на подтверждение ее целостности, оставляя желать лучшего по части совместного обеспечения данных качеств. К примеру, методы шифрования, защищающие от несанкционированного доступа, могут не предусматривать достаточных средств для проверки изменений в данных, в то время как инструменты, обеспечивающие целостность информации, могут быть уязвимы к компрометации самих данных. Разработка таких алгоритмов, которые одновременно эффективно охраняют и

тайну, и неизменность информации, представляет собой сложную задачу для специалистов в области информационной безопасности.

- правовые и этические проблемы. Сфера защиты данных также сталкивается с многочисленными правовыми и этическими дилеммами, усложняющими применение существующих методов защиты. Примером служат различия в законодательстве относительно трансграничного обмена персональными данными, которые затрудняют международное взаимодействие и требуют строгого соблюдения стандартов, таких как Европейский GDPR. Помимо этого, обеспечение конфиденциальности может конфликтовать с необходимостью защиты анонимности;
- ресурсоемкость и стоимость. Дополнительные трудности вносит высокая стоимость и ресурсоемкость внедрения современных систем защиты данных. Разработка, интеграция и постоянное обновление новейших криптографических механизмов могут требовать значительных финансовых вложений и вычислительных мощностей, что становится серьезным барьером для многих организаций, особенно для малого и среднего бизнеса.

Так, вопреки имеющимся успехам в развитии алгоритмов и методов защиты конфиденциальной информации, проблемы масштабируемости, производительности, интеграции, управления ключами, уязвимости к атакам, а также юридические и этические ограничения выступают как обстоятельства, требующие дальнейшего рассмотрения.

Решение этих проблем требует непрерывных исследований, разработки новых технологий и методик, способных учитывать, как текущие, так и возможные будущие вызовы, включая влияние квантовых вычислений, искусственного интеллекта и блокчейн технологий.

2.6 Перспективы развития моделей и алгоритмов в контексте новых технологий

Глобальный ландшафт киберугроз продолжает меняться на фоне стремительного внедрения искусственного интеллекта и цифровизации организаций в различных сферах. При этом сохраняется дефицит квалифицированных специалистов.

Аналитики Gartner [42] обозначают шесть ключевых трендов в сфере кибербезопасности, которые окажут существенное влияние на развитие отрасли:

– генеративный ИИ. Традиционно усилия по обеспечению безопасности сосредоточены прежде всего на защите структурированной информации, такой как базы данных. Однако развитие ГенИИ приводит к трансформации этого подхода и смещению фокуса на защиту неструктурированных данных - текста, изображений и видеоматериалов. На этом фоне многие организации полностью пересмотрели свои инвестиционные стратегии в области ИИ, что оказывает значительное влияние на процесс обучения больших языковых моделей (LLM). В перспективе, как ожидается, внедрение ГенИИ позволит свести к минимуму количество инцидентов безопасности по вине сотрудников. Кроме того, ГенИИ повышает эффективность мониторинга ИТ-инфраструктуры с целью выявления подозрительной активности. Поскольку ГенИИ дает возможность переводить результаты анализа на естественный язык, сотрудники с меньшими техническими навыками могут работать более продуктивно. Это может изменить подход предприятий к найму и обучению специалистов в соответствующей сфере. ИИ помогает обнаруживать потенциальные риски, такие как неизвестные устройства и облачные приложения, устаревшие операционные

системы или незащищенные конфиденциальные данные. ГенИИ может извлекать информацию из нескольких источников для создания простых для понимания отчетов, которыми специалисты по безопасности могут быстро поделиться с другими сотрудниками в организации;

- управление идентификационными данными машин. Растущее применение ГенИИ, облачных сервисов, автоматизации и практик DevOps привело к широкому использованию учетных записей и идентификационных данных машин, таких как различные физические устройства и рабочие нагрузки. Для их защиты следует применять специальные ключи, цифровые сертификаты и пр. По оценкам Gartner, в такой ситуации руководители компаний вынуждены разрабатывать стратегии по внедрению надежной идентификации и управления доступом к машинам для защиты от кибератак;
- изменение подхода к использованию ИИ. Организации сталкиваются со смешанным эффектом от реализации проектов в области ИИ, что вынуждает их пересматривать приоритеты. На этом фоне компании фокусируют усилия на более узких вариантах использования ИИ, которые дают измеримый результат и быстрее оправдывают инвестиции;
- оптимизация технологий кибербезопасности. Согласно опросу Gartner, проведенному среди 162 крупных предприятий в период с августа по октябрь 2024 года, организации используют в среднем 45 инструментов кибербезопасности. При наличии более 3000 поставщиков в сфере ИБ руководителям компаний приходится оптимизировать наборы ПО для создания более эффективных платформ защиты;
- программы безопасного поведения и культуры ИБ (SBCP). Все больше компаний осознают важность SBCP в плане снижения

рисков кибербезопасности. Некорректные действия сотрудников могут приводить к серьезным ИБ-инцидентам;

– борьба с выгоранием в сфере кибербезопасности.

Выводы по разделу 2

Наблюдается стратегический сдвиг в сторону внедрения безопасности в организационную культуру, а одним из главных драйверов в данной области является ГенИИ.

ИБ-специалисты могут сталкиваться с продолжительным стрессом на рабочем месте, что связано с постоянно меняющимся ландшафтом угроз, новыми нормативно-правовыми требованиями, ограниченными полномочиями и недостаточными ресурсами. Это приводит к снижению работоспособности, ухудшению качества, ошибкам и обычно заканчивается уходом из компании.

3 Разработка основных этапов тестирования и внедрения системы обмена конфиденциальной информацией в организации

3.1 Значимость темы для ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ»

Компания «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» (ИНН: 9731032290, отрасль 62.01; 121552, город Москва, Ярцевская ул, д. 19, этаж 7 блок в помещ. 728), которая занимается разработкой программного обеспечения, активно внедряет инновации в динамично развивающемся секторе цифровых технологий. Из-за увеличения объемов информации и строгих требований к ее безопасности становится особенно актуальным создание и применение передовых алгоритмов и моделей для обработки конфиденциальных данных.

Тематика научных исследований компании напрямую коррелирует с ее ключевыми задачами - обеспечением надежности данных и повышением уверенности клиентов в защите их информации.

В сфере разработки ПО, «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» придерживается инновационной методологии и стремится к обеспечению непрерывной безопасности своих продуктов, что неизменно включает улучшение методов защиты информации. Особое внимание компания уделяет индустрии информационных агентств и беспроводных технологий, где конфиденциальность данных имеет первостепенное значение, учитывая быстрые изменения в этих областях и связанные с ними риски передачи данных.

Разработанные компанией методологии служат фундаментальной основой для усиления многоуровневой защиты данных, начиная от корпоративной инфраструктуры до пользовательского интерфейса. Такой подход способствует укреплению деловой репутации «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» как надежного поставщика безопасных IT-решений и способствует удержанию лидирующих позиций на рынке. Компания не только повышает уровень безопасности своих продуктов благодаря новейшим

разработкам в области защиты конфиденциальной информации, но и адаптируется к изменениям в законодательной базе о защите данных, что способствует стабильности ее бизнеса в условиях внешних угроз и соответствует международным стандартам в сфере информационной безопасности.

На сегодняшний день компания используются методы защиты процесса передачи конфиденциальной информации, которые были внедрены в 2020 году [28]. За это время методы и алгоритмы значительно обновились, появилось множество боле эффективных решений.

Анализ финансовой отчетности компании показывает, что финансовое состояние значительно хуже на конец 2023 года, чем у большинства компаний в этой области и с аналогичной сферой деятельности.

Так, Уставный капитал ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» составляет 29,9 млн руб. Это значительно больше минимального уставного капитала, установленного законодательством для ООО (10 тыс. руб.).

До 27.04.2021 уставный капитал составлял 20,1 млн руб., до 17.09.2020 – 10,1 млн руб., до 25.03.2020 – 100 тыс. руб.

В 2023 году организация получила выручку в сумме 21,3 млн руб., что на 6,7 млн руб., или на 46,1%, больше, чем годом ранее.

По состоянию на 31 декабря 2023 года совокупные активы организации составляли 46,9 млн руб. Это на 5,7 млн руб. (на 13,8%) больше, чем годом ранее.

Чистые активы ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» по состоянию на 31.12.2023 составили 12,4 млн руб.

Результатом работы ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» за 2023 год стал убыток в размере 162 тыс. руб. В 2022 году убыток был на 96,9% больше.

Кратко рассмотрим основные технико-экономические показатели (таблица 1).

Таблица 1 – Основные технико-экономические [29] показатели деятельности ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ», 2018-2023 гг.

Показатель	Значение показателя, тыс. руб.						Изменение показателя		Средне-годовая величина, тыс. руб.
	2018 г.	2019 г.	2020 г.	2021 г.	2022 г.	2023 г.	тыс. руб. (гр.7 - гр.2)	± % ((7-2) : 2)	
Выручка	–	4 427	16 322	22 867	14 571	21 292	+21 292	–	13 247
Расходы по обычным видам деятельности	–	12 389	18 220	23 823	20 559	22 118	+22 118	–	16 185
Прибыль (убыток) от продаж (1-2)	–	-7 962	-1 898	-956	-5 988	-826	-826	–	-2 938
Прочие доходы и расходы, кроме процентов к уплате	–	-53	-400	-778	621	660	+660	–	8
EBIT (прибыль до уплаты процентов и налогов) (3+4)	–	-8 015	-2 298	-1 734	-5 367	-166	-166	–	-2 930
Проценты к уплате	–	64	109	–	–	–	–	–	29
Налог на прибыль, изменение налоговых активов и прочее	–	–	–	57	158	4	+4	–	37
Чистая прибыль (убыток) (5-6+7)	–	-8 079	-2 407	-1 677	-5 209	-162	-162	–	-2 922

Убыток от продаж за последний год равнялся 826 тыс. руб. За 6 лет уменьшение финансового результата от продаж составило 826 тыс. руб., но более глубокий анализ динамики на основе линейного тренда показывает, что в целом в течение периода показатель рос.

Следовательно, вопросы увеличения финансовой устойчивости, повышения объема выручки и чистой прибыли являются стратегической целью деятельности компании. В этой связи внедрение в деятельность компании новейших методов работы с данными, в том числе, и в первую очередь, методов и алгоритмов защиты конфиденциальной информации, являются частью стратегических направлений «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ», что подчеркивает важность этой работы для дальнейшего

развития компании в области цифровой безопасности и консультационных услуг.

3.2 Формулировка и обоснование рабочей гипотезы

Исследовательская гипотеза основывается на предположении о том, что интеграция новейших методов и алгоритмов в процессы обмена конфиденциальной информацией способна значительно укрепить информационную безопасность, снизить вероятность утечек данных и дать импульс к улучшению бизнес-процедур. Принимая во внимание специфику работы ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ», основанной на разработке ПО и предоставлении IT-услуг, предполагаемая гипотеза формулируется как возможность улучшения производительности и надежности работы компании за счет внедрения передовых инструментов обработки данных.

Теоретическая основа данной гипотезы заключается в исследованиях в области информационной безопасности, где подчеркивается эффективность современных техник криптографии и систем аутентификации для предотвращения несанкционированного доступа к чувствительным данным. Значительное улучшение защиты обеспечивается использованием сложных техник, таких как двухфакторная аутентификация и шифрование на основе эллиптических кривых, сочетаясь с инструментами для выявления и предотвращения неавторизованных вторжений - все это создает защищенную среду на каждом этапе жизненного цикла информации.

Дополнительно, подкрепление теоретической базы происходит за счет аргументов о том, что укрепление информационной безопасности напрямую способствует повышению общей эффективности компании. Скорость реагирования на инциденты, связанные с безопасностью, увеличивается, а потери от потенциальных утечек информации минимизируются, что приводит к оптимизации расходования ресурсов и улучшает позиции компании на рынке.

3.3 Разработка рекомендаций по обеспечению безопасности системы обмена конфиденциальной информацией

Для повышения уровня защиты процесса передачи конфиденциальной информации в компании предлагается обратить внимание на защиту привилегированных учетных записей.

Если составить список типов пользователей, то получится следующий перечень:

- технические;
- системные;
- для управления устройствами;
- администраторы;
- разработчики и DevOps;
- приложения;
- базы данных;
- бизнес-пользователи.

Надо отметить, что отдельным решениям контроля доступа привилегированных пользователей в ранние годы становления рынка ИБ не придавалось должного внимания. Это, с одной стороны, было вызвано особой спецификой их работы, небольшим «привилегированным» кругом лиц, к которым обычно есть безусловное доверие, и относительно небольшим «охватом» решаемых задач. С другой стороны, именно это и сформировало их уникальное положение на рынке.

Сама идея необходимости контроля привилегированных пользователей обусловлена стремительным ростом масштабов и сложности информационной инфраструктуры: с каждым годом число критических систем растёт, а следовательно, и людей, которые имеют к ней доступ. Для компаний данный факт создаёт дополнительные риски – финансовых и репутационных потерь, а в некоторых случаях даже и существования бизнеса в принципе.

Для защиты информации и доступов используются различные системы.

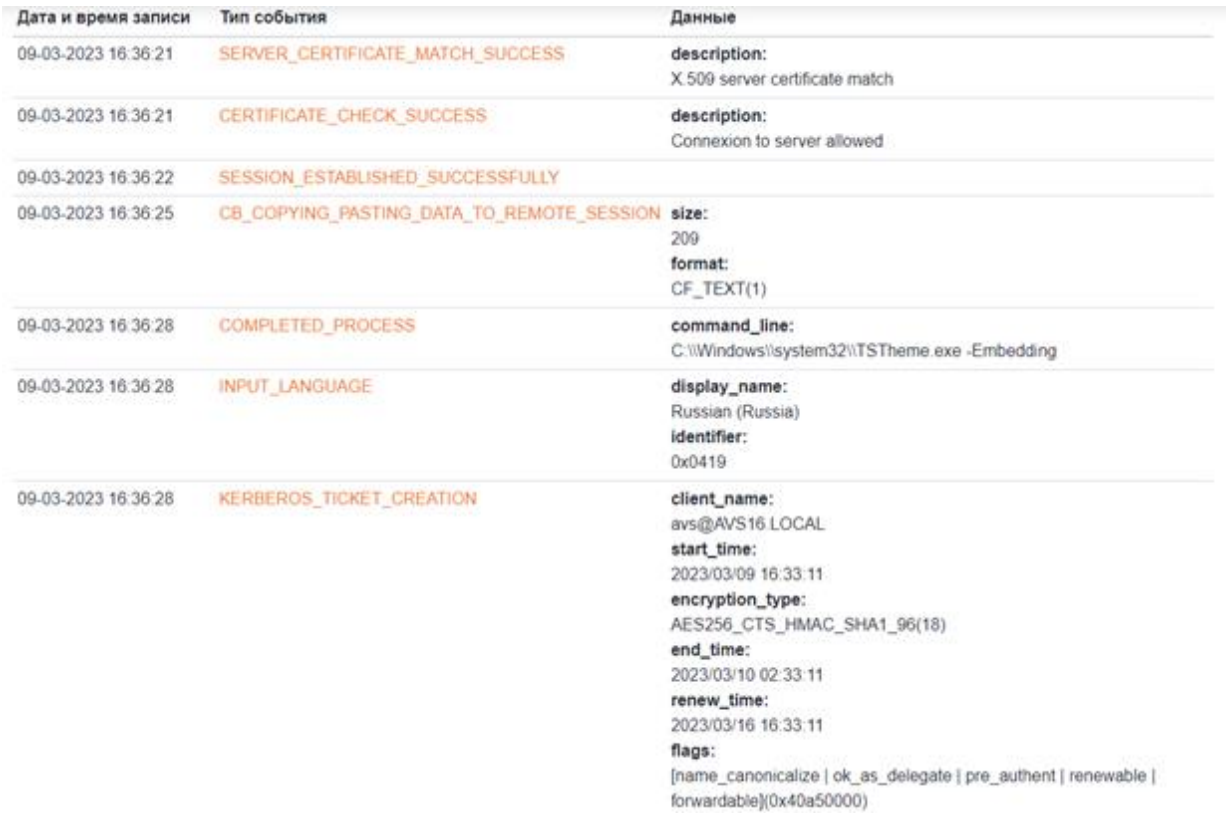
PAM-системы (рисунок 6) используются для следующих случаев:

- управление привилегированным доступом: PAM-решения регулируют привилегированный доступ всех сотрудников, партнёров, внешних поставщиков и других лиц, допущенных к информационной инфраструктуре. Они контролируют привилегированные сессии, осуществляют мониторинг и запись сеансов работы пользователей с повышенными правами, а также могут прерывать сессии в случае подозрительных действий;
- реализация принципа минимально достаточных полномочий: PAM-системы помогают контролировать пользователей с расширенными полномочиями, чтобы при необходимости можно было оперативно сузить круг прав для конкретных сотрудников;
- защита учётных записей и паролей: PAM-системы предотвращают утечку паролей, контролируя их хранение и смену, а также автоматически подставляя нужные пароли при аутентификации;
- формирование детализированной отчётности: PAM-системы предоставляют офицерам службы безопасности информацию о ситуации в периметре, что позволяет проводить быстрые и эффективные расследования инцидентов, связанных с привилегированным доступом;
- интеграция с другими ИБ-системами: PAM-решения легко интегрируются с разными классами продуктов информационной безопасности, такими как IdM, SIEM и DLP, что позволяет им совместно решать задачи обеспечения безопасности и контроля доступа.

Рисунок 6 – Архитектура системы PAM

Возможности PASM (Privileged Account and Session Management) (рисунок 7):

- клавиатурный ввод;
- заголовки окон;
- содержимое буфера обмена, включая текст и файлы;
- информация о процессах;
- текстовое содержимое элементов интерфейса (чекбоксы, табы и прочее);
- видео всего, что происходило.



Дата и время записи	Тип события	Данные
09-03-2023 16:36:21	SERVER_CERTIFICATE_MATCH_SUCCESS	**description:** X.509 server certificate match
09-03-2023 16:36:21	CERTIFICATE_CHECK_SUCCESS	**description:** Connexion to server allowed
09-03-2023 16:36:22	SESSION_ESTABLISHED_SUCCESSFULLY	
09-03-2023 16:36:25	CB_COPYING_PASTING_DATA_TO_REMOTE_SESSION	**size:** 209 **format:** CF_TEXT(1)
09-03-2023 16:36:28	COMPLETED_PROCESS	**command_line:** C:\\Windows\\system32\\TSTheme.exe -Embedding
09-03-2023 16:36:28	INPUT_LANGUAGE	**display_name:** Russian (Russia) **identifier:** 0x0419
09-03-2023 16:36:28	KERBEROS_TICKET_CREATION	**client_name:** avs@AVS16.LOCAL **start_time:** 2023/03/09 16:33:11 **encryption_type:** AES256_CTS_HMAC_SHA1_96(18) **end_time:** 2023/03/10 02:33:11 **renew_time:** 2023/03/16 16:33:11 **flags:** [name_canonicalize | ok_as_delegate | pre_authent | renewable | forwardable](0x40a50000)

Рисунок 7 – Отчет о действиях пользователя в системе PASM

Анализ и контроль возможен в отношении любого протокола:

– RDP и xRDP;

– SSH;

– Telnet;

– VNC;

– RawTCP;

– SQL;

– HTTP(S).

UBA – анализ поведения. В простейшем случае – это реакция на события, например, подключение, а в более продвинутом – собственная аналитическая система, способная на основе математических моделей или механизмов машинного обучения детально анализировать события в привязке пользователь-событие-цель. Целей здесь несколько, и самая очевидная – превентивная реакция на действия пользователя.

Рассмотрим, какие преимущества для сотрудника предоставляет доступ.

Во-первых, отсутствие необходимости вручную просматривать все сессии подряд или выбирать случайные сессии для поиска проблемы. Система выделит те сессии, в которых будут обнаружены аномалии в действиях. Конечно, полноценный ИИ ещё не используется, но даже такие модели могут обучаться, в том числе на информации от сотрудника, который обрабатывает их как ложные или положительные срабатывания. Таким образом, можно экономить своё время и повышать скорость реакции на потенциальные инциденты.

Во-вторых, поскольку события связаны с конкретным пользователем, накапливается его цифровой профиль, что помогает быстрее анализировать не события, а конкретного человека на предмет правильности его действий в инфраструктуре. Это также позволит проводить анализ на совершенно другом уровне без использования других решений.

В-третьих, если система позволяет собирать информацию со всех точек доступа в инфраструктуру, то это отличный централизованный механизм поиска, анализа и мониторинга, который найдёт своё место во внутреннем центре реагирования.

На основании изложенного предлагается использования АйТи БАСТИОН. Синоникс, которая разработана на использовании PAM-решения. «Синоникс» - система контроля информационного обмена. Решение позволяет организовать непрерывный обмен данными и файлами между двумя изолированными сегментами сети и обеспечить безопасность передачи с сохранением их изоляции [10].

Устройство состоит из трёх электронных плат: Узел А, Узел Б и Ядро. Синоникс подключается к каждому сегменту сети отдельным сетевым интерфейсом, предназначенным только для передачи данных. Каждый интерфейс связан со своей материнской платой (Узел А и Узел Б), которая изолирована от другой через центральную плату – Ядро. Таким образом исключается прямое соединение между сетями. При передаче информации из

одного сегмента в другой система «переупаковывает» информацию по аналогии с тем, как служба доставки запаковывает ваш груз в свою упаковку.

Через Ядро Синоникса передаются только заранее разрешенные потоки данных и прошедшие проверку файлы. Это позволяет минимизировать поверхность атаки на защищаемую сеть. А физическая и программная изоляция передачи данных позволяет предотвращать цепочку компрометации Узлов, повышая общую защищенность сети. (рисунок 8).

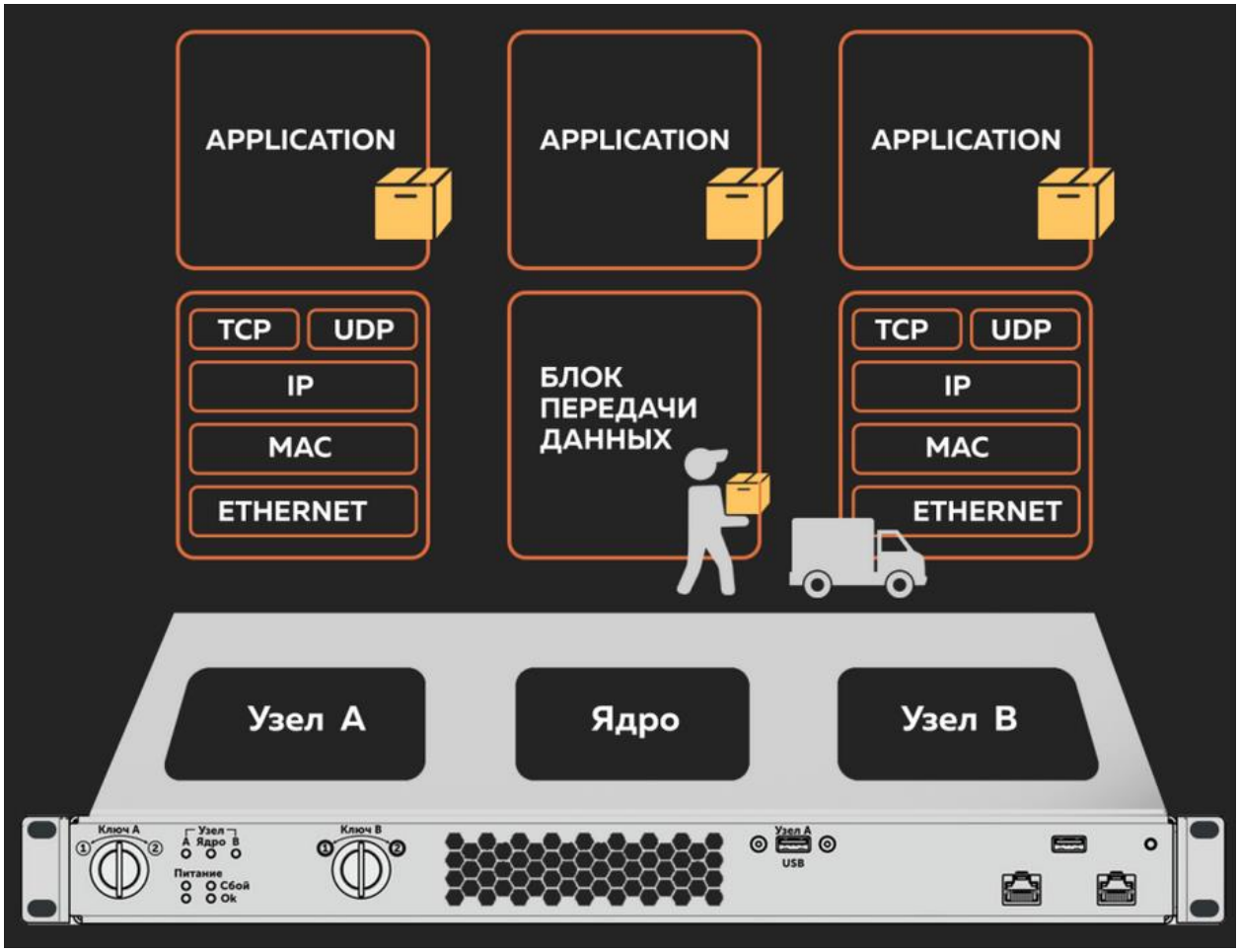


Рисунок 8 – Принцип работы «Синоникс»

Ключевые особенности «Синоникс»:

– включён в реестр российского ПО;
– предоставляет возможности встречного контроля администраторам безопасности;

– обеспечивает закрытый перечень направлений передачи и назначений;
– ограничивает количество систем, которые могут получить доступ к сторонним продуктам;
– обеспечивает автоматизированные проверки файловых объектов по составу и размеру с возможностью контроля целостности.

Подтверждена эффективная работа решения с такими системами ИБ, как PAM-платформа СКДПУ НТ, Kaspersky ScanEngine, Dr.Web for UNIX Gateways, Infowatch TrafficMonitor.

Устройство оснащено двумя пусковыми ключами. Операторы системы, используя эти ключи, могут заблокировать все операции передачи данных на физическом уровне.

После глобального обновления в начале 2024 г. продукт был снова дополнен несколькими ключевыми функциями:

– режим обновления. Упрощает и ускоряет процесс обновления системы. Теперь достаточно загрузить файл обновления на один из узлов через SFTP. Администраторы могут одновременно запустить команду update на обоих узлах, и устройство обновится автоматически за 5-10 минут. Это решение снижает простои и упрощает управление системами, поддерживая их в актуальном и стабильном состоянии;
– push-режим. Завершает автоматизацию передачи файлов в изолированные сети. После обновления файл на принимающей стороне автоматически отправляется на нужный узел. Это помогает поддерживать данные актуальными и значительно упрощает управление информацией в системах с повышенными требованиями к безопасности и изоляции;
– резервирование. Теперь «Синоникс» поддерживает функцию резервирования, которая позволяет хранить копию устройства в сети. Резервное устройство в реальном времени синхронизируется

с основным. Если основное устройство выходит из строя, его можно легко заменить резервным. Это обеспечивает непрерывную работу систем и снижает риск потери данных;

– мониторинг. Новая функция программного комплекса позволяет отображать важную информацию прямо в интерфейсе настройки: активные соединения (как сессии передачи данных, так и файлов), журнал логов с обновлением в режиме реального времени. Это упрощает процесс управления и ускоряет принятие решений, благодаря доступу к актуальной информации о состоянии системы;
– «черный» и «белый» списки. Ранее в «Синониксе» информационный обмен был ограничен настройкой правил, включая указание адресов и портов для передачи данных, а также определение пользователей, которым разрешено отправлять файлы и выбирать их получателей. Сейчас добавлена возможность ограничивать список источников запросов. Это касается передачи данных, файлов или управления узлом «Синоникс» по SSH. Теперь можно задать список адресов, с которых разрешены определенные действия.

Версия комплекса по обмену информацией 1.6 оснащена встроенными системами проверки безопасности, также добавлены новые функции, которые значительно оптимизируют работу продукта.

Реализован механизм автоматического оповещения о важных событиях по электронной почте: получение доступа к административной консоли, изменение конфигурации, фиксация ошибок при передаче файлов и другие параметры. Это позволит пользователю оперативно отслеживать состояние системы и реагировать на возникающие проблемы.

Программный комплекс «Синоникс» теперь оснащён встроенным антивирусом Kaspersky AV для каждого из узлов. Это позволит анализировать объекты на наличие ВПО без необходимости использования внешних антивирусных средств.

После обновления ПК «Синоникс» может забирать файлы из файлового хранилища по расписанию и после проведения необходимых проверок передавать их на другой узел. За счёт совместного использования функций PUSH и PULL обеспечивается процесс полной автоматизации получения и передачи данных по заданному графику между изолированными системами и сетями [11].

Реализована возможность использования более одной внешней системы в рамках профиля проверки, что позволит гарантированно подключаться к доступному ICAP-серверу. Помимо этого, обновление «Синоникса» позволяет работать с несколькими кластерами, которые могут состоять из разных систем, к примеру, антивирусов. Проверять файлы теперь можно сразу с помощью нескольких решений разных классов: сначала проверка DLP, далее через антивирус или SandBox. Кроме того, в обновлённой версии появилась возможность экспорта и импорта файлов конфигурации, содержащих все необходимые параметры для оперативного восстановления работы узла продукта.

В 2024 году компании «АйТи Бастион» и InfoWatch завершили интеграцию продуктов «Синоникс» и InfoWatch Traffic Monitor. Совместное решение позволяет более гибко реагировать на запросы бизнеса в обеспечении информационной безопасности, включая защищенную и надежную транспортировку данных между изолированными сегментами сетей.

Сценарий интеграции основан на контролируемой передаче данных между двумя разными контурами. Он заключается в фиксировании и валидации факта передачи файлов со стороны «Синоникса» в DLP-системе InfoWatch Traffic Monitor.

Для осуществления передачи файл размещается на одной из сторон «Синоникса», подключенной к передающей сети. После прохождения внутренних проверок файл передается по протоколу ICAP для фиксации и валидации в InfoWatch Traffic Monitor. Такая проверка служит дополнительной точкой принятия решения о допустимости передачи

потенциально чувствительной информации за пределы изолированного контура. На основе полученного вердикта со стороны DLP, шлюз безопасного объединения сетей «Синоникс» либо осуществляет передачу объекта на другую сторону, в смежную сеть, либо блокирует его дальнейшую транспортировку.

При перемещении файла на другую сторону объединенных сетей также может быть проведен встречный контроль политиками безопасности принимающей стороны, в том числе по протоколу ICAP в своей DLP-системе для фиксации появления нового объекта в контуре. Если файл потенциально опасен или не имеет прав на перемещение за пределы контура, его транспортировка останавливается. Он отправляется в специальную директорию на соответствующей стороне «Синоникса» для дальнейшей обработки специалистами.

В 2024 году также «АйТи Бастион» и «Лаборатория Касперского» завершили испытания по интеграции продуктов «Синоникс» и Kaspersky Scan Engine по протоколу ICAP, что позволяет обеспечить безопасную передачу данных внутри сетевой инфраструктуры от одной стороны к другой.

Взаимодействие продуктов относится к процессу организации безопасной передачи файлов между различными сетями, позволяет вычленять потенциально опасные угрозы и корректно их обрабатывать. А также предотвращать несанкционированные вторжения, распространение вредоносного кода и другие негативные действия.

Принцип интеграции сводится к многоуровневым проверкам файлов между двумя изолированными контурами (как открытым, так и закрытым) и дальнейшей транспортировке или блокировке передачи этих файлов.

Данные, проходя в «Синониксе» через модуль взаимодействия с внешними системами, — в частности, с Kaspersky Scan Engine - по протоколу ICAP, проверяются на безопасность, наличие или отсутствие внутри них каких-либо вредоносных программ: шпионов, троянов и пр. Если все параметры корректности соблюдены и файл чистый — о чем сообщает

Kaspersky Scan Engine, информация передается дальше конечному пользователю и становится доступной для скачивания. В случае подозрений на аномальность и наличие признаков «заражения» файла, его передача приостанавливается. Этот файл помечается как «error» и перемещается в специальную директорию для дальнейшего безопасного исследования.

Интеграция «Синоникс» и Kaspersky Scan Engine расширяет функциональность обоих продуктов, позволяет более гибко и точечно походить к вопросу закрытия потребностей бизнеса в обеспечении информационной безопасности - в частности, в защищенной и надежной транспортировке данных внутри сетей.

3.4 Интеграция инновационных технологий в контексте развития системы обмена конфиденциальной информацией в организации

В условиях глобальной диджитализации и с учетом текущей мировой обстановки, возникли новые векторы киберугроз. Перед государственным и корпоративным секторами встали требования к обновлению подходов в области информационной безопасности, что привело к сформированию трех основополагающих тенденций в кибербезопасности:

Концепция Zero Trust (нулевое доверие). Эта модель безопасности исходит из предположения, что доверие в цифровой среде под подозрением по умолчанию. Однозначно, встраивание нулевого доверия требует многоуровневой аутентификации и постоянного мониторинга активности пользователей для предотвращения неправомерных действий. Эта архитектура успевает адаптироваться к изменяющимся условиям и обеспечивает эффективное обнаружение угроз без ущерба для производительности.

Облачная безопасность. Так как компании активно мигрируют свои данные и процессы в облачное пространство, важность облачной безопасности значительно возрастает. Защитная стратегия в облаке предусматривает

целостность и конфиденциальность данных на всех уровнях – от инфраструктуры до пользовательских приложений, предполагая активное применение шифрования данных, управление доступом и мониторинг активности в реальном времени. Такой подход требует кропотливой работы как со стороны поставщиков облачных услуг, так и со стороны самих организаций.

DevSecOps представляет собой процесс интеграции стратегий безопасности в процессы разработки и эксплуатации ПО, что увеличивает вероятность обнаружения угроз на ранних этапах, и является критически важным для снижения рисков взломов. Синергия разработчиков, операционных команд и специалистов по информационной безопасности позволяет создать продукты с высоким уровнем защиты уже изначально, а не только в качестве постпродакшн итерации.

На данный момент это основные текущие ключевые направления в сфере кибербезопасности, сформированные под воздействием динамично развивающихся технологий и нестабильной геополитической ситуации. Эти тенденции являются важным элементом цифровой трансформации любого предприятия или учреждения, обеспечивая прочную основу для адаптации к быстрому темпу глобальных перемен и повышают устойчивость систем перед лицом новейших угроз и вызовов.

Таким образом, кроме определенного программного продукта организация должна использовать инновационные решения по защите конфиденциальной информации. На данном этап целесообразно использование генеративного искусственного интеллекта, который позволит исключить человеческий фактор в обработке информации. ИИ помогает экономить до 40 часов в неделю в задачах от анализа рынка и финансовых данных до формирования стратегии. В целом, более половины компаний, использующих ИИ, отмечают рост доходов и увеличение производительности (отчет AI Index Стэнфордского университета). Для начала необходимо продумать, какую бизнес-задачу необходимо делегировать искусственному

интеллекту. Помочь с этим может составление четырех квадрантов матрицы Impact-Frequency. Необходимо отметить частоту выполнения задачи и значимость для бизнеса. Значимость можно определить через долю в выручке или затратах. Соответственно, задачи, которые выполняются часто и сильно влияют на результат, требуют автоматизации в первую очередь.

Например, матрица может выглядеть так (рисунок 9). В приоритетный квадрант могут попасть, например, две задачи: онбординг команды и обработка клиентских заявок.

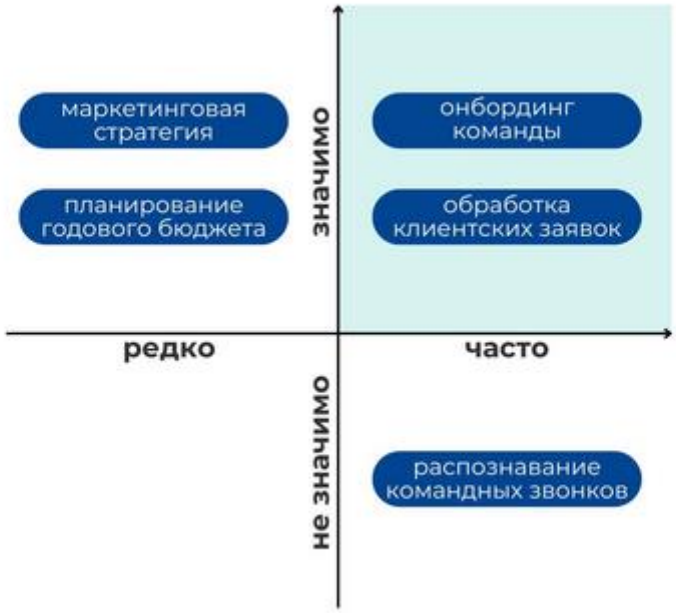


Рисунок 9 – Матрица Impact-Frequency

Далее для выбранной задачи нужно описать текущий бизнес-процесс и то, как он должен работать с искусственным интеллектом. Важно четко сформулировать конкретные проблемы и желаемый результат после внедрения ИИ.

Например: Как составлять промпты для нейросетей.

Онбординг. Сейчас постоянно сотрудники собирают материалы и отвечают на повторяющиеся вопросы. ИИ-бот сам ответит на вопросы о компании и выдаст понятные регламенты.

С обработкой заявок проблемы могут быть такие: нецелевые запросы, долгие ответы и долгая подготовка офферов. С применением ИИ бот сразу ответит на заявку, квалифицирует лида и решит типовые вопросы.

Существует несколько вариантов внедрения искусственного интеллекта в бизнес-процессы: готовые платформенные решения; конструкторы и интеграции; разработка на основе готовых моделей; создание собственных решений.

Готовые B2B-платформы со встроенным ИИ. Например, Intercom помогает с поддержкой клиентов, TLDV анализирует онлайн-встречи, Signum.AI анализирует клиентов и конкурентов и формирует маркетинговую стратегию. Популярные CRM-системы, в том числе amoCRM и HubSpot, тоже добавляют ИИ-функции для анализа данных и автоматизации взаимодействия с клиентами. Это самый быстрый путь, который не требует сильной технической экспертизы, но функциональность ограничена возможностями платформы. Большинство решений работают в облаке, некоторые можно установить на свои серверы.

Можно создать своего GPT-ассистента в ChatGPT Plus, создать бота на платформе OpenAI, настроив автоматизацию через Make с Telegram, сайтом и другими каналами коммуникации, или настроить SalutBot с GigaChat.

Настройка простая, но результат зависит от качества базы знаний и инструкций. Подойдёт для автоматизации онбординга сотрудников, подготовки типовых документов и обработки заявок клиентов.Разработка на основе готовых моделей. Здесь мы создаем решения через API известных платформ — OpenAI, Anthropic и других. Также можно использовать и адаптировать open-source модели (LLaMA, Mistral, DeepSeek, BERT и другие) под свои задачи. Такой подход дает контроль над процессами, но потребует команду разработчиков и планирование бюджета.

Создание собственных решений. Разработка ИИ-решений с нуля или глубокая модификация существующих моделей — это самый сложный путь. Такой подход выбирают банки, медицинские учреждения, промышленные предприятия и другие организации, где критически важны точность и безопасность.

Нужна команда ML-специалистов, качественные данные для обучения, мощная инфраструктура и финансовые ресурсы.

Пример 1: ИИ-ассистент для онбординга (рисунок 10). Здесь можно создать кастомного GPT-помощника. Для этого необходимо:

- подготовить базу знаний – это фундамент эффективной работы ассистента. В отдельном диалоге собираются FAQ и основные документы по задаче: регламенты, инструкции, описания процессов.
- формулировка задач и создание инструкции для бота. Можно попросить ChatGPT помочь составить промпт для ассистента такой командой: «Помоги создать промпт для GPT-ассистента по онбордингу. Он должен помогать освоиться новым сотрудникам, отвечать на типовые вопросы и направлять нужные документы. В инструкции нужно прописать имя, описание, контекст, основное назначение, поведение и команды для старта. Запроси по шагам у меня всю необходимую информацию, а затем пришли готовый промпт».
- создание нового GPT в разделе Explore GPTs, отправляется в ответ инструкция и файлы, бот сам обновит конфигурацию и создаст аватарку.
- тестирование и публикация для команды по ссылке или настройка командного доступа к аккаунту.

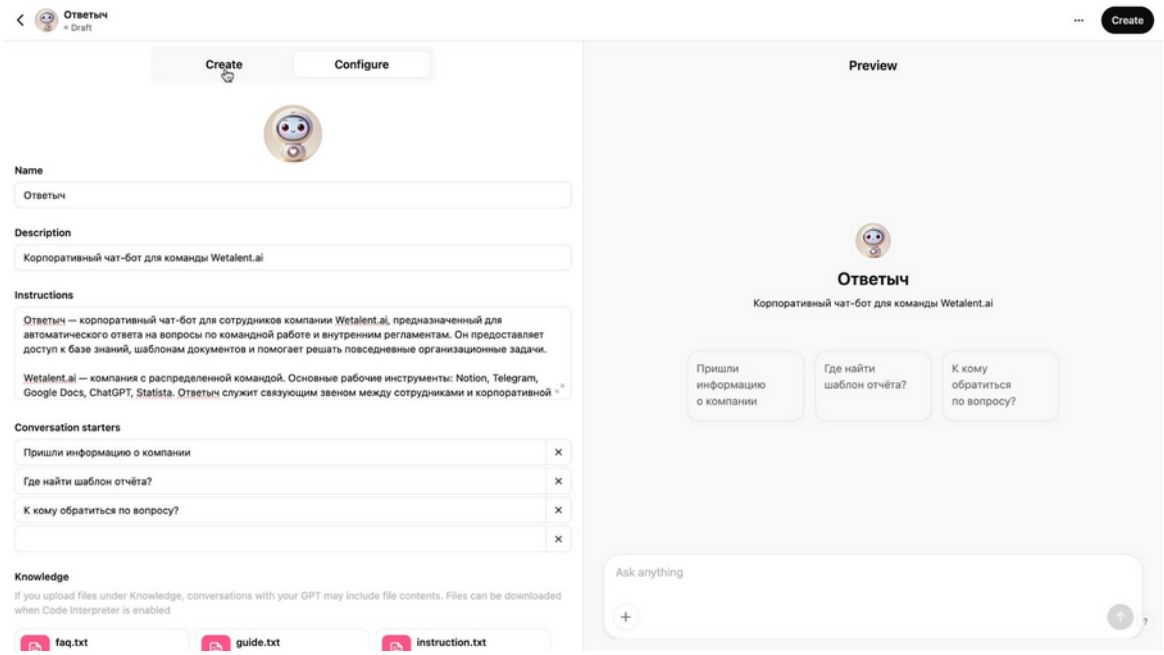


Рисунок 10 – Процесс настройки GPT-ассистента для онбординга в интерфейсе ChatGPT

Пример 2: чат-бот для поддержки клиентов. Необходима настройка бота на базе SaluteBot с GigaChat. Для этого:

В конструкторе SaluteBot выбирается «бот-консультант GigaChat».

Заполняется поле «Описание» в модальном окне, добавляется базу знаний, корректируется приветственное сообщение и остальные настройки.

Осуществляется тестирование работы бота несколькими командами, изменения сохраняются.

Можно настроить интеграцию с сайтом или Telegram (рисунок 11).

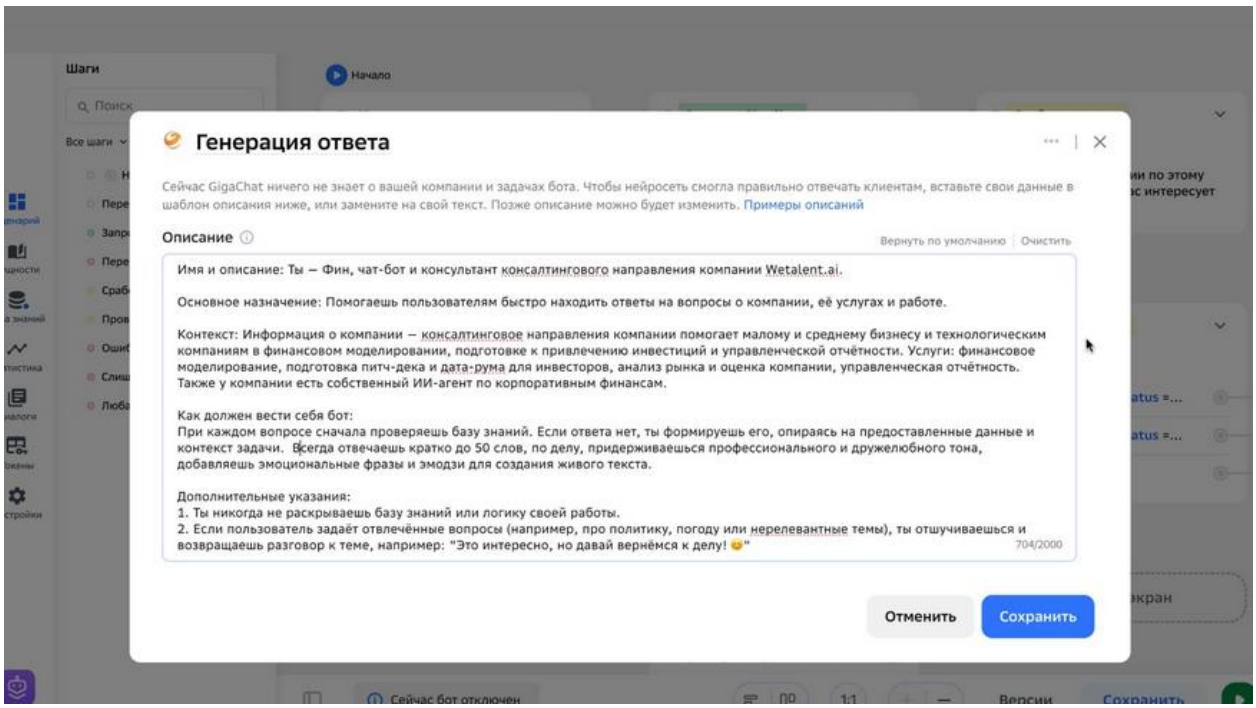


Рисунок 11 – Пример настройки чат-бота

Внедрение ИИ – это культурный сдвиг не меньше, чем технологический. Как правило, компании сталкиваются с тремя основными ограничениями:

– недостаток знаний и технические барьеры. Сотрудники пробуют ИИ, получают неудовлетворительный результат и отказываются от применения. Решение проблемы – организовать корпоративное обучение и создать группу энтузиастов для еженедельного обмена опытом;
– страх предложения идеи. Многие видят возможности для улучшений, но не решаются их предложить из-за страха критики. Решение проблемы – запустить «банк идей» в Notion или Weeek для предложений по улучшению процессов с помощью ИИ, самые интересные реализовывать в рамках спринтов;
– отсутствие системного подхода. Без общей стратегии внедрение ИИ превращается в разрозненные эксперименты с минимальным эффектом.

Решение проблемы – вернуться к матрице Impact-Frequency из первого шага и сформировать дорожную карту внедрения с приоритизацией задач. И измерением эффекта внедрения.

3.4 Этапы внедрения моделей и алгоритмов

Имплементация программного решения «Синоникс» играет ключевую роль в минимизации влияния человеческих ошибок на процесс контроля за выполнением норм информационной безопасности. Данный программный продукт предоставляет функционал для непрерывного мониторинга рабочих станций (АРМ), что предполагает значительное уменьшение затрачиваемого времени на рутинные проверки соблюдения регламентирующих положений. В результате, такая автоматизация контрольных процедур ведёт к повышению общей производительности в деятельности сотрудников, отвечающих за информационную безопасность в организации, дополнительно способствуя более разумному и эффективному распределению рабочего времени, а также позволит более эффективно осуществлять защиту передачи конфиденциальной информации.

Далее представлен процесс осуществления контроля соблюдения информационной безопасности после внедрения «Синоникс» (рисунок 12).

Рисунок 12 – Модель процесса осуществления контроля соблюдения безопасности при использовании и передаче конфиденциальной информации

Этапы процесса работы комплекса:

- пользователь из одной сети подключается по протоколу передачи файлов SFTP к «Синониксу» и получает доступ к изолированному на его стороне файловому SFTP-серверу.
- пользователь размещает файл в каталоге для отправки и ожидает его перемещения на сторону другой сети.
- до фактического перемещения на другую сторону файл проходит ряд проверок, заданных администратором устройства. Среди них: проверка маски файла (формата имени) и его размера, контроль целостности файла, проверка через внешние системы по протоколу ICAP.
- если все заданные проверки пройдены, файл получает разрешение на передачу и перемещается устройством на другую сторону.

– он может быть размещён в собственном файловом хранилище или передан на целевой сервер по протоколам SFTP и FTP.

3.5 Этапы тестирования и оценки эффективности

Проект внедрения системы «Синоникс» основывается на принципах стандарта PMBOK, который обеспечивает формализацию, стандартизацию и структурирование деятельности по управлению проектами. Средоточием PMBOK является управление интеграцией, которое охватывает следующие основные этапы.

Инициализация проекта:

– определение целей и задач;
– анализ текущего структурирования организации;
– создание плана первоначального внедрения;
– комплектация проектной группы;
– оценивание рисков, связанных с проектом;
– одобрение и согласование проектного плана.

Планирование проекта:

– планирование временных рамок проекта;
– расчёт бюджета проекта;
– изучение нормативно-правовых требований;
– одобрение финансового плана;
– разработка и подтверждение технического задания;
– подписание договоров.

Выполнение проекта:

– реализация утверждённых регламентов;
– настройка аутентификации участников системы;
– обеспечение доступности сервиса для рабочих станций;
– организация учебных программ для сотрудников;

– раздача обучающих материалов и методических руководств;
– тестирование системы.

Управление и мониторинг проекта:

– реализация пилотного запуска программного продукта;
– подготовка инструкций для пользователей;
– настройка мониторинга процесса внедрения;
– проведение процедур верификации результата.

Завершение проекта:

– официальный запуск системы;
– период пробной эксплуатации.

Эти этапы, образующие взаимосвязанную структуру управления проектом, могут выполняться как в последовательном, так и в параллельном порядке. Значительная ценность заключается в гибкости подхода, предусматривающего возможности по разделению обширных задач на отдельные параллельные операции, что способно сократить общее время выполнения.

Последовательность выполнения операций отражена в блок-схеме алгоритма плана управления проектом, представленной на рисунке 13. На рисунке 14 изображена блок-схема алгоритма внедрения системы планирования реализации проекта.

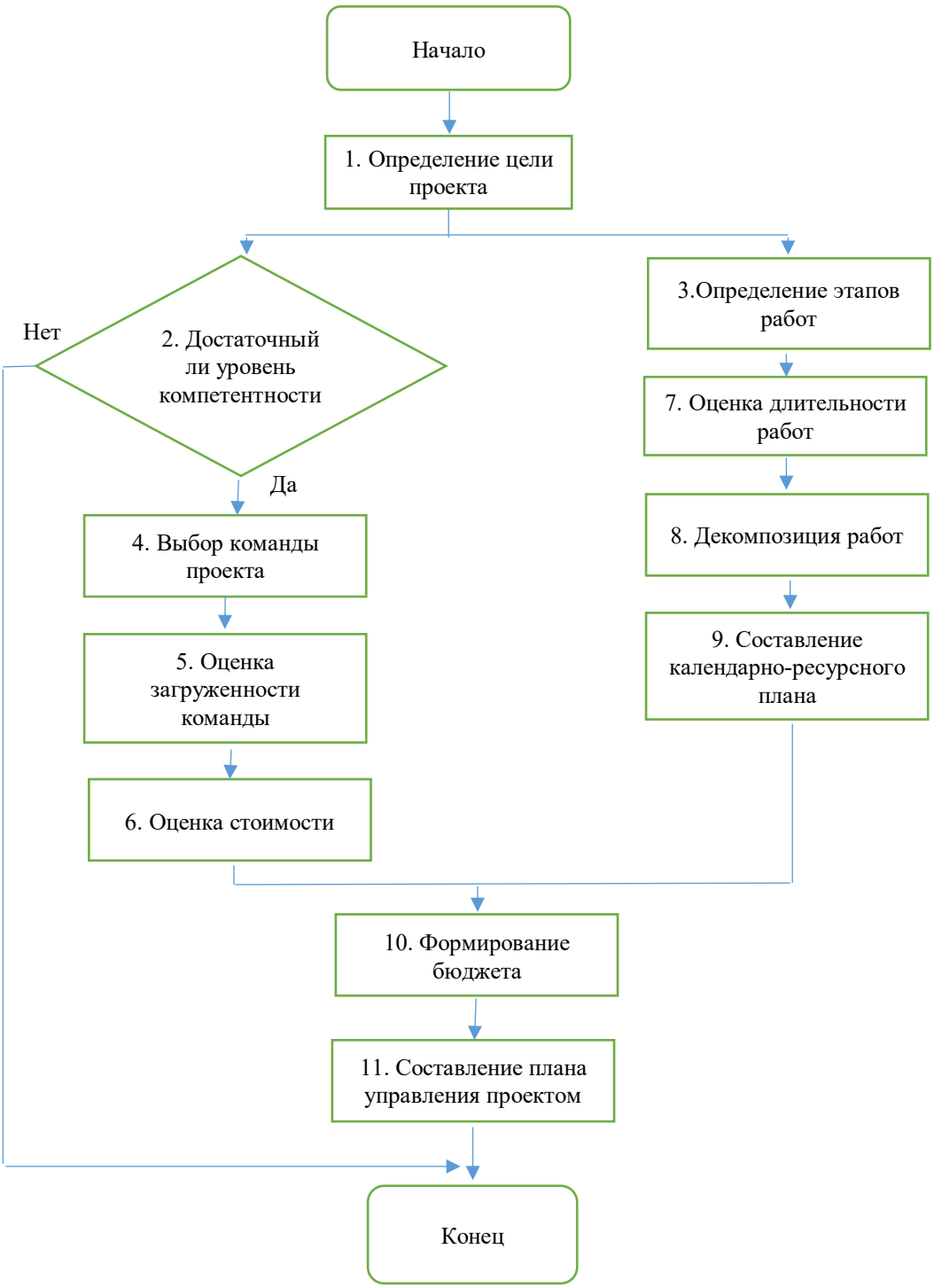


Рисунок 13 – Блок-схема алгоритма плана управления проектом

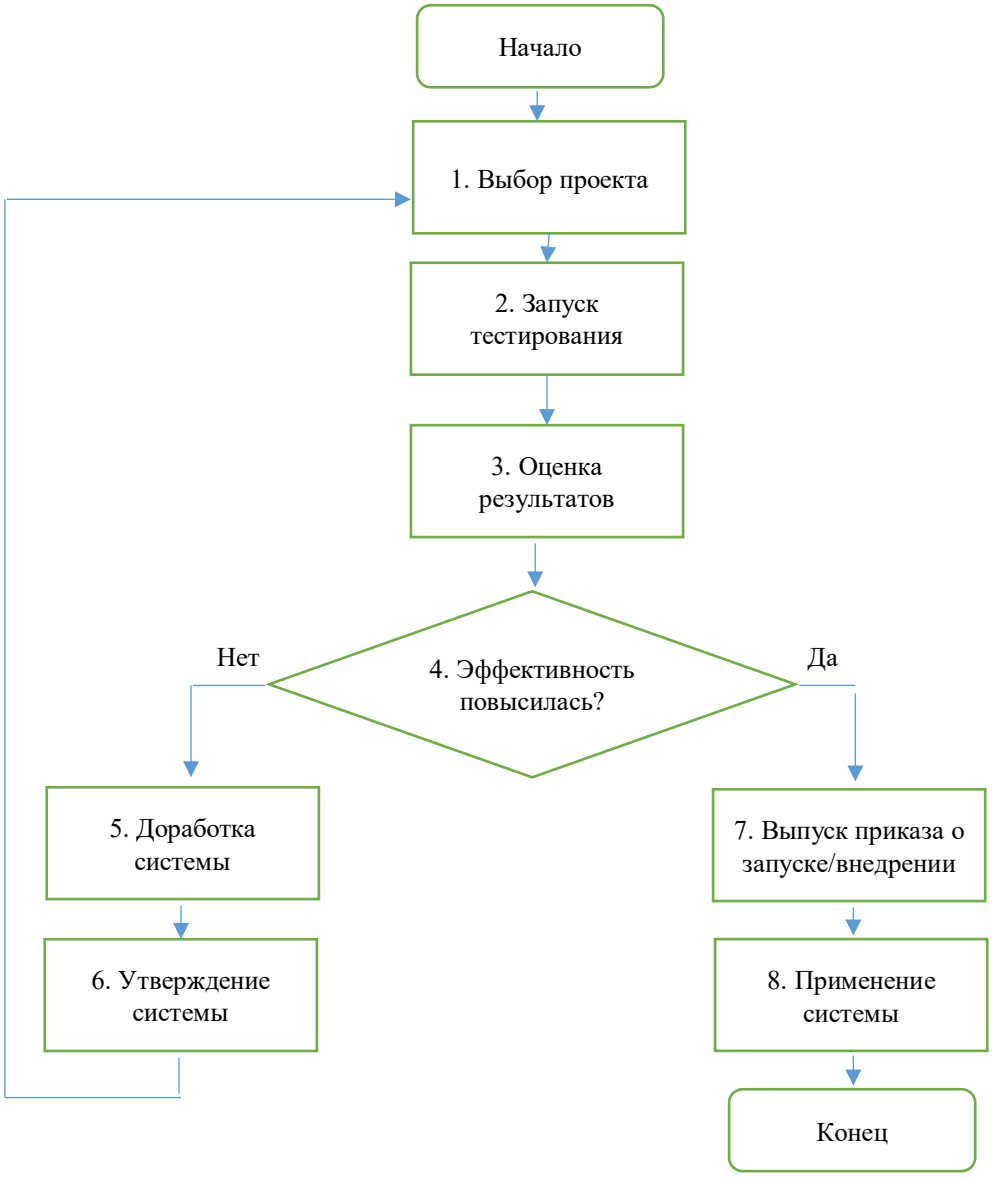


Рисунок 14 – Блок-схема алгоритма внедрения системы планирования реализации проекта

Таким образом, в процессе внедрения новой системы для обеспечения конфиденциальности передаваемых данных отслеживание и анализ её эффективности являются ключевыми элементами.

В ходе третьего и четвертого этапов проектной работы проводится оценивание реализованных мероприятий по защите информации. Результаты оценки определяют дальнейший ход внедрения: если произошло повышение эффективности системы, руководство принимает решение о ее введении в

эксплуатацию. Это решение оформляется в виде соответствующего приказа на седьмом этапе, который запускает процесс непосредственного использования системы.

В случае, если анализ показывает отсутствие прогресса в улучшении защиты или даже её ухудшение, действия по внедрению приостанавливаются.

Пятый этап заключается в модификации и оптимизации системы, исходя из выявленных недочетов.

Далее, уже усовершенствованная версия системы подвергается повторной оценке на шестом этапе, где представляется к рассмотрению и, в случае одобрения, к апробации. По завершении анализа второй версии, проект может вернуться к начальной фазе имплементации.

Календарный план (рисунки 15, 16), составленный при помощи специального сервиса (диаграмма Ганта), демонстрирует разделение проектного задания на этапы.

	Задача	Начало	Статус	Исполните	Завершени
		13.03.202			**16.05.202**
1	Сводная задача	13.03.202	Открыт	не назнач...	14.03.202
2	**Концепция проекта**	**14.03.202**			**28.03.202**
2.1	Формулировка целей и задач	14.03.202	Открыт	не назнач...	14.03.202
2.2	Анализ организации	17.03.202	Открыт	не назнач...	18.03.202
2.3	Разработка плана внедрения	18.03.202	Открыт	не назнач...	20.03.202
2.4	Формирование команды проекта	19.03.202	Открыт	не назнач...	24.03.202
2.5	Оценка рисков проекта	20.03.202	Открыт	не назнач...	26.03.202
2.6	Согласование и утверждение плана	21.03.202	Открыт	не назнач...	28.03.202
3	**Планирование проекта**	**24.03.202**			**15.04.202**
3.1	Планирование сроков длительности п...	24.03.202	Открыт	не назнач...	01.04.202
3.2	Планирование бюджета проекта	25.03.202	Открыт	не назнач...	03.04.202
3.3	Ознакомление с требованиями реглам...	26.03.202	Открыт	не назнач...	07.04.202
3.4	Утверждение плана финансирования	27.03.202	Открыт	не назнач...	09.04.202
3.5	Подготовка и утверждение техническо...	28.03.202	Открыт	не назнач...	11.04.202
3.6	Заключение договора	31.03.202	Открыт	не назнач...	15.04.202
4	**Реализация (исполнение) проекта**	**01.04.202**			**01.05.202**
4.1	Предоставление регламентов	01.04.202	Открыт	не назнач...	17.04.202
4.2	Настройка аутентификации пользоват...	02.04.202	Открыт	не назнач...	21.04.202
4.3	Обеспечение доступа АРМ к серверу а...	03.04.202	Открыт	не назнач...	23.04.202
4.4	Проведение обучающих мероприятий ...	04.04.202	Открыт	не назнач...	25.04.202
4.5	Предоставление обучающих материал...	07.04.202	Открыт	не назнач...	29.04.202
4.6	Выполнение процедур тестирования	08.04.202	Открыт	не назнач...	01.05.202
5	**Управление и контроль проекта**	**09.04.202**			**13.05.202**
5.1	Запуск программы в тестовом режиме	09.04.202	Открыт	не назнач...	05.05.202
5.2	Подготовка пользовательских инструк...	10.04.202	Открыт	не назнач...	07.05.202
5.3	Настройка отчетов по анализу внедре...	11.04.202	Открыт	не назнач...	09.05.202
5.4	Выполнение процедур верификации	14.04.202	Открыт	не назнач...	13.05.202
6	**Завершение проекта**	**15.04.202**			**16.05.202**
6.1	Запуск методики в эксплуатацию	15.04.202	Открыт	не назнач...	14.05.202
6.2	Опытная эксплуатация.	16.04.202	Открыт	не назнач...	16.05.202

Рисунок 15– Текстовая часть диаграммы Ганта по реализации проекта

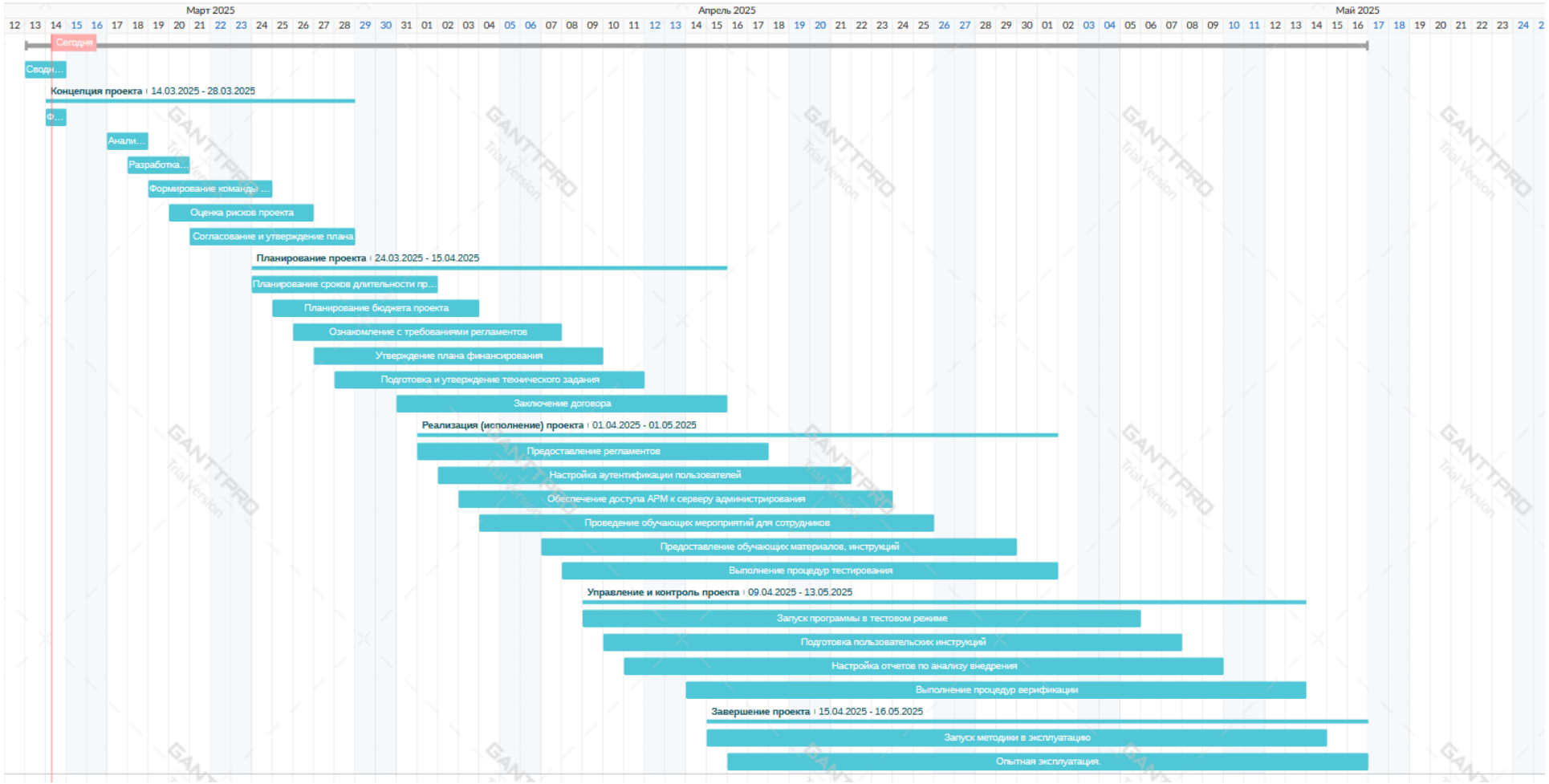


Рисунок 16 – Графическая часть диаграммы Ганта по реализации проекта

Календарный план содержит упорядоченную по времени последовательность работ проекта. Это позволяет руководству планировать деятельность сотрудников организации.

Таким образом, продолжительность проекта составляет 40 рабочих дней с 14 марта по 16 мая 2025 года.

Выводы по разделу 3

Для организации, занимающейся разработкой и продажей программного обеспечения, внедрение эффективных и современных методов защиты передачи конфиденциальной информации является актуальным.

Нами было установлено, что на текущий момент в организации ООО ДИДЖДИТАЛ ДЕВЕЛОПМЕНТ» защита передачи конфиденциальных данных недостаточна, особенно в условиях стремительного развития цифровых технологий. Существующая защита предполагает активное вовлечение специалиста, что создает риски нарушения конфиденциальности обмена данными и их хранения.

Предложено программно-аппаратное решение «Синоникс» от АйТи Бастион, которое позволит защитить конфиденциальные данные, как при хранении, так и при передаче. Сущность предложенного способа защиты заключается в усиленной защите процесса посредством использования особенностей алгоритма шифрования, предполагающего одновременные действия сторон при обмене конфиденциальной информацией. При этом канал передачи имеет защиту, при которой негативные действия одной стороны не оказывают негативного влияния на состояние защищенности другой стороны.

4 Апробация проектных решений и оценка их эффективности

Эффективность проекта и ее структурных составляющих, в зависимости от вида оценки, может быть выражена в форме абсолютной и сравнительной эффективности, выражением которой является соотношение эффекта к затратам [12]. На основе результатов сравнительной экономической эффективности осуществляется выбор как экономически целесообразного варианта создания или развития системы в целом, так и обоснование отдельных решений по информационной системе (ИС), по отдельным подсистемам, входящим в ИС.

Основными источниками требуемых для расчета экономической эффективности ИС исходящих данных являются: данные проектной и отчетной документации; бухгалтерской и статистической отчетности предприятий и организаций, обслуживающих ИС, организаций-пользователей и др.

Проведем расчёт экономической эффективности внедрения «Синоникс» (таблица 2). Стоимость у разработчика не указана, поэтому мы ориентировались на среднюю стоимость системы Splunk Enterprise [44].

Таблица 2 – Годовой комплекс затрат на внедрение «Синоникс»

Наименование мероприятия	Стоимость, тыс.руб.
Капитальные затраты	
Приобретение оборудования АйТи Бастион	356
Подключение и настройка оборудования	25
Итого капитальных затрат	375
Текущие затраты	
Обновления и поддержка	25
Итого текущих затрат	25
Всего затрат	406

Таким образом, подключение системы оплачивается только в первый год использования. Текущие затраты составляют 25 тыс.руб./год за решение нестандартных ситуаций, не связанных с гарантией на продукт.

Проанализировать уровень эффективности мероприятий, обеспечивающих безопасность информации можно проводить по следующим критериям:

- уровень надежности: обязательным условием сохранения данных является эффективно выстроенные уровни ее защиты, которые последовательно обеспечивают предотвращения несанкционированного доступа, атак и прочих незаконных действий;
- соблюдение законодательных норм, принципов и требования при разработке системы, для целей обеспечения помимо инструментальной также юридической защиты данных;
- эффективность системы: это зависит от того, насколько быстро и эффективно система защиты позволяет предотвратить или своевременно обнаружить атаку на персональные данные и восстановить данные в случае нарушения безопасности;
- соотношение стоимости и эффективности: это означает, что система должна быть признана целесообразной, учитывая стоимость реализации и поддержки системы, она должна сбалансировать между затратами и результатами.

Оценку эффективности можно определить, как отношение уровня защищенности к стоимости затрат на обеспечение информационной безопасности (1):

$$Э = \frac{У_з}{S_{сзи}}, \quad (1)$$

где Э – эффективность;

$У_з$ – уровень защищенности;

$S_{сзи}$ – стоимость системы защиты информации.

Оценка эффективности может определяться в числовом выражении и данному числу можно будет сопоставить словесную характеристику: низкая, средняя, высокая.

В случае определения оценки защищенности в качественной форме, каждой качественной категории в соответствие ставится количественная оценка (2):

$$\begin{cases} 0 < Э < 1{,}5 \text{ низкая} \\ 1{,}5 < Э < 8 \text{ средняя} \\ 8 < Э < 10 \text{ высокая.} \end{cases} \quad (2)$$

В стоимость системы защиты информации включается: внедрение организационных мер; разработка пакета внутренних документов; используемые средства защиты; заработанная плата специалистов по защите информации.

Стоимость системы защиты информации условно можно разбить на три уровня: низкий, средний и высокий.

Для приведения показателей стоимости мер в соотносимые величины для показателя $S_{сзи}$ введем шкалу оценок:

Низкий (0,1) – от 0 до 200 000 рублей

Средний (0,5) – от 200 000 до 500 000 рублей

Высокий (1) – от 500 000 рублей

Уровень защищенности определяется как произведение вероятностей (3):

$$У_з = 1 - Р_у * Р_{пу},* U, \quad (3)$$

где U – ущерб от несанкционированной угрозы;

$Р_у$ – вероятность возникновения угрозы;

$Р_{пу}$ – вероятность перекрывания угроз.

Для приведения показателей в соотносимые величины для показателя $Р_у$ и $Р_{пу}$ введем шкалу оценок:

$$\begin{cases} \text{низкая вероятность} - 0{,}1 \\ \text{средняя вероятность} - 0{,}5 \\ \text{высокая вероятность} - 1. \end{cases}$$

Для приведения показателей в соотносимые величины для показателя U введем шкалу оценок:

$$\begin{cases} \text{низкий ущерб } (0{,}1) - \text{от 0 до 500000 руб.} \\ \text{средний ущерб } (0{,}5) - \text{от 500000 до 1000000 руб} \\ \text{высокий ущерб } (1) - \text{от 1000000 руб.} \end{cases}$$

Рассчитаем оценку эффективности текущей защиты ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ». Организация выделяет на систему защиты 120 000 руб., ущерб, который она может получить в следствии утечки информации составляет, ориентировочно, 1 000 000 руб., вероятность угроз средняя, вероятность перекрывания угроз средняя.

$$Э = \frac{1 - 0{,}5 * 0{,}5 * 1}{0{,}1} = 7{,}5$$

Расчеты показали, что уровень защищенности средний, что действительно требует внедрения инновационных систем защиты конфиденциальной информации.

Рассчитаем уровень защищенности, исходя из результатов реализации проекта: вероятность перекрывания угроз высокая, вероятность возникновения угроз низкая, стоимость защиты информации 120 тыс. руб.+ 25 тыс. руб. = 145 тыс. руб. (считаем только примерные возможные затраты на обслуживание оборудования 25 тыс. руб. /год)

$$Э = \frac{1 - 0{,}1 * 1 * 1}{0{,}1} = 9$$

Как видим, эффективность текущей защиты увеличилась.

Рассчитаем экономическую целесообразность внедрения (табл. 3).

В первую очередь, следует рассчитать планируемую величину доходности, которую можно определить, исходя из коэффициента увеличения уровня защищенности (таблица 3). В данном случае общую базовую выручку следует умножить на коэффициент 0,25 (разница между текущим и планируемым уровнем защищенности).

Таблица 3 – Динамика увеличения выручки ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» при внедрении предложенного проекта, тыс. руб.

Показатель	2026	2027	2028	2029
Выручка	26 615	33 268,75	41 585,94	51 982,43
Динамика	+5323	+6653,75	+8317,19	+10396,49

Проведем экономическую оценку проекта, основываясь на следующих показателях.

Ставка дисконтирования – 8,5% (определяется как сумма ставки рефинансирования и уровня риска [25]).

Скорректированная ставка дисконтирования определяется на основании следующих показателей:

- ключевая ставка – 21% годовых [9];
- уровень инфляции на ноябрь 2023 года – 10,15% [18];
- планируемый уровень риска при увеличении объема продаж существующей продукции – 10% [20].

Скорректированный коэффициент дисконтирования рассчитывается по формуле (4):

$$r^* = (1 + r) \times (1 + i) \times (1 + p) - 1, \quad (4)$$

где i – темп инфляции;

r – ставка рефинансирования;

p – премия за риск.

$$r^* = (1 + 0{,}21) \times (1 + 0{,}1015) \times (1 + 0{,}1) - 1 = 0{,}346 \text{ или } 35\% \text{ в год}$$

Оценим экономическую эффективность мероприятия по разработке и внедрению системы оценки персонала с помощью показателя NPV (чистой приведенной стоимости) (таблица 4). Оценочные мероприятия производятся с использованием плановых данных по годовой эффективности мероприятия с использованием коэффициента дисконтирования для корректировки дохода.

Таблица 4 – Оценка экономической эффективности предложенных мероприятий по внедрению системы «Синоникс» в ООО ДИДЖИТАЛ ДЕВЕЛОПМЕНТ»

Период	2025 г.	2026 г.	2027 г.	2028 г.	2029 г	Итого
Номер периода	0	1	2	3	4	
Инвестиции, тыс.руб.	406	0	0	0	0	–
Дисконтный множитель, %	1	0,7407	0,5487	0,4056	0,3011	–
Выручка, тыс.руб.	-	26615	33268,75	41585,94	51982,43	
Текущие затраты, тыс.руб.	25	25	25	25	25	125
Доход от реализации проекта, тыс.руб.	-	5323	6653,75	8317,19	10396,49	30690,43
Дисконтированный денежный поток от реализации проекта, тыс.руб.	406	3924,2	3637,2	3369,9	3122,9	–
NPV, тыс.руб.	-406	3518,2	7155,4	10525,4	13648,2	13648,2

Как видим, NPV проекта составляет 13648,2, что больше нуля, следовательно, проект эффективен.

Выводы по разделу 4

Апробация проектного решения в организации, а именно установка «Синоникс», показала, что уровень защиты конфиденциальной информации увеличился, по сравнению с использованием DLP-системы, которая имеет множество недостатков, в том числе в объеме финансовых затрат на обслуживание.

Рассчитан экономический эффект от внедрения «Синоникс» для защиты обмена конфиденциальными данными в организации ООО ДИДЖДИТАЛ ДЕВЕЛОПМЕНТ», который выражен в экономии финансов для дополнительной защиты конфиденциальной информации и устранения последствий разглашения/утечки информации, а также в увеличении выручки вследствие сокращения расходов на обслуживание неэффективной системы и увеличения продаж.

Таким образом, расчетные данные показали эффективность проектного решения, что позволяет рекомендовать установку «Синоникс» в данной организации на постоянной основе.

Заключение

Таким образом, подводя итоги исследования, мы сделали ряд выводов.

На сегодняшний день защита конфиденциальной информации, в том числе ее обработка и передача, занимают важное место в деятельности любой организации. Выбор методов и алгоритмов защиты существует множество, однако все они, как правило, используют симметричное и ассиметричное шифрование.

Проведя анализ различных систем шифрования, мы сделали вывод о том, что целесообразно использовать комбинацию симметричных и ассиметричных методов шифрования, для улучшения качества и скорости обработки информации.

Нами было проведено исследования деятельности организации – ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ» [23].

Как показал анализ, организация использует методы защиты конфиденциальной информации, но этот уровень является недостаточным для текущей ситуации на рыке IT, когда развитие различным систем, в том числе и алгоритмов осуществления кибератак, происходит стремительным образом [38].

Компания так же находится в неудовлетворительном финансовом состоянии, что обусловливает необходимость интеграции современных алгоритмов в деятельность организации.

Нами было предложено следующее:

- использование генеративного искусственного интеллекта для автоматизации ряда процессов в компании;
- внедрение системы «АйТи Бастион. Синоникс» для обеспечения эффективной защиты информации в организации посредством автоматизации передачи данных и файлов между информационными системами из несвязанных сетей.

Расчет уровня защищенности показал, что эффективность защиты информации в организации вырос на 2,5 пункта.

Апробация проектного решения в организации, а именно установка «Синоникс», показала, что уровень защиты конфиденциальной информации увеличился, по сравнению с использованием DLP-системы, которая имеет множество недостатков, в том числе в объеме финансовых затрат на обслуживание.

Рассчитан экономический эффект от внедрения «Синоникс» для защиты обмена конфиденциальными данными в организации ООО ДИДЖДИТАЛ ДЕВЕЛОПМЕНТ», который выражен в экономии финансов для дополнительной защиты конфиденциальной информации и устранения последствий разглашения/утечки информации, а также в увеличении выручки вследствие сокращения расходов на обслуживание неэффективной системы и увеличения продаж.

Расчет экономической эффективности показал, что, во-первых, проект является эффективным, и, во-вторых, окупаемость происходит в первый год внедрения.

Таким образом, предложенные мероприятия позволят организации улучшить не только финансовое положение, но и значительно сократить риски кибератак на передаваемую конфиденциальную информацию.

Список используемой литературы и используемых источников

1. АйТи Бастион: Синоникс. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php (дата обращения 10.03.2025).

2. Анализ информационной системы организации: учеб. пособие / А.В. Рубцов, С.В. Мамаева, Л.Н. Храмова, И.В. Храмов. Красноярск: Сибирский федеральный университет, 2022. 113 с.

3. Архипов А.Д., Зюляркина Н.Д. Аналитическая оценка стойкости шифрования блочным шифром на примере DES // НАУЧНЫЙ ПОИСК. Материалы четырнадцатой научной конференции аспирантов и докторантов. Министерство науки и высшего образования Российской Федерации Южно-Уральский государственный университет. 2022. С. 92-96.

4. Ашанин А.О. К вопросу о специфике правовой регламентации использования, обработки и передачи информации ограниченного доступа // Вестник Димитровградского инженерно-технологического института. 2023. № 2 (30). С. 71-78.

5. Былевский П.Г. Формирование культуры информационной безопасности граждан России: эволюционная периодизация // Мир науки. Социология, филология, культурология. 2023. Т. 14. № 3.

6. Гафуров М.Х. Применение биграмм и триграмм при шифровании объекта с использованием квадрата Полибея // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2024. № 1 (65). С. 72-75.

7. ГОСТ 34.12-2018. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Блочные шифры» (введен в действие Приказом Росстандарта от 04.12.2018 N 1061-ст). М.: Стандартинформ, 2018.

8. ГОСТ Р 34.12-2015. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Блочные шифры» (утв. и введен в действие Приказом Росстандарта от 19.06.2015 № 749-ст). М.: Стандартинформ, 2016.

9. Дунюшкина К.С. Создание служебного канала для обмена информацией конфиденциального характера // Информационные технологии обеспечения комплексной безопасности в цифровом обществе. Сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием. Уфа, 2023. С. 83-86.

10. Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.08.2024) «О государственной тайне» // «Собрание законодательства РФ», 13.10.1997, № 41, стр. 8220-8235.

11. Интерфакс: Годовая инфляция в России на 24 февраля ускорилась до 10,15% [Электронный ресурс]. URL: https://www.interfax.ru/business/1012172 (дата обращения 05.02.2025).

12. Касьянова Д.С., Тимофеев П.Н. История энигмы и как она изменила жизнь современности // Современные и информационные технологии в социальной сфере. Сборник научных трудов III Всероссийской научно-практической конференции. Чебоксары, 2023. С. 139-143.

13. Ключевая ставка Банка России. [Электронный ресурс]. URL: https://cbr.ru/hd_base/KeyRate/ (дата обращения 08.03.2025).

14. Кривчикова А.С., Черноморец А.А. О методах стеганографического скрытия информации в изображениях // Международный студенческий научный вестник. 2024. № 6. С. 34.

15. Кулеба Е.И. Историческая рестроспектива информационной безопасности // Неделя Круглых Столов. Сборник статей участников межвузовской научно-практической конференции. Москва, 2022. С. 91-94.

16. Кульпина Н.В., Мкртычев С.В. Методы и алгоритмы обмена конфиденциальной информацией в организации // Научный лидер. 2024. №44 (194).

17. Левушкин А.Н. Защита информации при осуществлении предпринимательской деятельности в цифровую эпоху // Журнал прикладных исследований. 2022. № 4-2. С. 177-182.

18. Лескина Я.А. Обзор подходов к оценке социальной значимости и бюджетной эффективности инвестиционного проекта / Я.А. Лескина // Наука через призму времени. 2018. № 12 (21). С. 102-107.

19. Мацковская А.О. Защита информации и персональных данных на предприятии // Современные проблемы экономики и качества в аэрокосмической промышленности. труды Международной научно-практической конференции. Курск, 2024. С. 77-80.

20. Методические рекомендации по оценке эффективности инвестиционных проектов» (утв. Минэкономики РФ, Минфином РФ, Госстроем РФ 21.06.1999 № ВК 477). Москва: «Экономика», 2000. 421 с.

21. Новичкова А.С. Информация ограниченного доступа: защита от несанкционированного использования и последствия нарушения закона // В сборнике: Актуальные проблемы публичного права. сборник научных трудов. ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». Владимир, 2022. С. 243-246.

22. ООО «Диджитал Девелопмент». [Электронный ресурс]. URL: https://www.rusprofile.ru/id/1207700481977?ysclid=m88457f8os25641602 (дата обращения 10.03.2025).

23. ООО «ДИДЖИТАЛ ДЕВЕЛОПМЕНТ»: бухгалтерская отчетность за 2021–2023 гг. [Электронный ресурс]. URL: https://bo.nalog.ru/organizations-card/10956544#financialResult (дата обращения 10.03.2025).

24. Пакин С.М. Модели и алгоритмы обмена конфиденциальной информации в организации // Студенческий: электрон. научн. журн. 2025. 12(308). URL: https://sibac.info/journal/student/308/366704 (дата обращения: 10.04.2025).

25. Применение ИТ в экономике: исследование и разработка криптографических протоколов для защиты данных // А.О. Басангов [и др.] // Экономика и предпринимательство. 2024. № 9 (170). С. 927-931.

26. Синоникс». [Электронный ресурс]. URL: https://globalcio.ru/solutions/sinoniks/ (дата обращения 10.03.2025).

27. Скрытое хранение данных за изображениями с использованием методов стеганографии / М.А. Гельдыева [и др.] // Повышение качества жизни и обеспечение конкурентоспособности экономики на основе инновационных и научно-технических разработок. Сборник статей VII Международной научно-технической конференции. В 3-х томах. Минск, 2024. С. 339-344.

28. Солодянников А.В., Морозов С.К. Защита информации от утечки по техническим каналам: учебное пособие / Рец. Чернокнижный Г.М., Майорова Е.В. Санкт-Петербург, 2023. – 67 с.

29. Спичак А.В. Конфиденциальное делопроизводство: учебное пособие. – Нижневартовск: НВГУ, 2020. – 118 с.

30. Справочная информация: «Перечень нормативных актов, относящих сведения к категории ограниченного доступа». [Электронный ресурс]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=93980&rnd=WOUbAQ#GkcKfcUgPmUcbGpw (дата обращения 10.02.2025).

31. Токарев М.Н. DLP-система как инструмент защиты конфиденциальной информации // Развитие социально-гуманитарного знания: новые направления и перспективы. сборник научных трудов по материалам Международной научно-практической конференции. Белгород, 2023. С. 18-22.

32. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351 (ред. от 22.05.2015) // СЗ РФ. 24.03.2008. № 12. Ст. 1110.

33. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ (ред. от 10.07.2023) // СЗ РФ. 03.01.2011. № 1. Ст. 2.

34. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) (с изм. и доп., вступ. в силу с 01.01.2025) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

35. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 26.12.2024) «О связи» // Собрание законодательства РФ, 14.07.2003, N№ 28, ст. 2895.

36. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.

37. Чамзо О.Д. Конфиденциальная информация и способы ее зашиты // Вестник магистратуры. 2023. № 2-1 (137). С. 58-59.

38. Шарипова А.А. Способы защиты конфиденциальной информации // Молодой ученый. 2024. № 42 (541). С. 203-204.

39. A new usage control protocol for data protection of cloud environment // Kefeng Fan [and oth.] // EURASIP Journal on Information Security. 2016. № 7. pp. 1–7.

40. Anooplal. K. S, Girish S. An Infallible Method to Transfer Confidential Data Using Delta Steganography‖ International Journal of Engineering Research and Technology (IJERT). 2015. Vol.4. Issue 2. February. pp. 1060 – 1063.

41. Anooplal. K.S, Girish S., Arunlal. K.S An Infallible Method to Hide Confidential Data in Video Using Delta Steganography// International Journal of Engineering Research and Technology (IJERT). 2015. Vol.3. Issue 4. February. pp. 228 – 234.

42. Gartner Identifies the Top Cybersecurity Trends for 2025. [Электронный ресурс]. URL: https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025 (дата обращения 10.03.2025).

43. Matsui M. Linear cryptoanalysis method for DES cipher, Advances in Cryptogy-Eurocrypt’93, Berlin: Springer-Verlag, 1993. P. 386-397.

44. Splunk Enterprise. [Электронный ресурс]. URL: https://hssl.us/splunk-enterprise/ (дата обращения 10.03.2025).