Защита данных в цифровую эпоху

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....
ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ДАННЫХ В ЦИФРОВУЮ ЭПОХУ.....
1.1. Понятие и классификация данных в современном информационном пространстве.....
1.2. Основные угрозы и вызовы безопасности данных: анализ актуальных рисков.....
1.3. Законодательные и нормативные основы защиты данных на национальном и международном уровнях.....
ГЛАВА 2. МЕТОДЫ И ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ.....
2.1. Технические средства и методы криптографической защиты информации.....
2.2. Организационные и правовые меры обеспечения конфиденциальности и целостности данных.....
2.3. Перспективы развития систем защиты данных в условиях трансформации цифровой среды.....
ЗАКЛЮЧЕНИЕ.....
СПИСОК ИСТОЧНИКОВ.....

ВВЕДЕНИЕ

Актуальность рассматриваемой проблематики обусловлена трансформационными процессами, происходящими в современном обществе под влиянием стремительного развития информационных технологий и повсеместной цифровизации. В условиях формирования глобального информационного пространства объем генерируемых, обрабатываемых и хранимых данных экспоненциально возрастает, что приводит к возникновению новых вызовов и угроз в сфере обеспечения приватности и безопасности персональной информации. Цифровая эпоха характеризуется беспрецедентной интеграцией информационных систем во все сферы жизнедеятельности человека – от повседневных коммуникаций и финансовой деятельности до государственного управления и национальной безопасности. Это обстоятельство делает защиту данных не просто технической задачей, но комплексной социально-правовой, экономической и этической проблемой, требующей междисциплинарного подхода к ее решению. Нарушения конфиденциальности, целостности и доступности данных могут привести к серьезным негативным последствиям, включая финансовые потери, репутационный ущерб, утрату доверия, а также к нарушениям прав и свобод граждан. Особую значимость приобретает вопрос гармонизации технологического прогресса с правовыми и этическими нормами, обеспечивающими защиту интересов индивидуумов и общества в целом. В этом контексте исследование механизмов, принципов и методов защиты данных становится императивом для обеспечения устойчивого развития цифровой экономики и построения безопасного информационного общества.

Объектом настоящего исследования является совокупность общественных отношений, возникающих в процессе сбора, обработки, хранения, передачи и использования данных в цифровой среде. Данный

объект охватывает широкий спектр взаимодействий между субъектами данных (физическими лицами), операторами данных (организациями, обрабатывающими данные) и регулирующими органами. Предметом исследования выступают правовые, организационные, технические и этические аспекты обеспечения защиты данных в условиях цифровой трансформации. В частности, анализируются нормативно-правовая база, регулирующая отношения в сфере защиты данных, существующие методологии и стандарты информационной безопасности, а также рассматриваются вызовы, связанные с новыми технологиями, такими как искусственный интеллект, большие данные, интернет вещей и облачные вычисления, которые существенно изменяют ландшафт угроз и требуют адекватных мер защиты.

Целью исследования является разработка комплексной концепции защиты данных в цифровую эпоху, интегрирующей правовые, организационные и технологические подходы, направленные на минимизацию рисков несанкционированного доступа, использования, раскрытия, изменения или уничтожения информации. Данная концепция призвана способствовать повышению уровня доверия к цифровым сервисам и платформам, а также обеспечить соблюдение основополагающих прав человека на приватность и защиту персональных данных.

Для достижения поставленной цели в работе последовательно решаются следующие задачи. Прежде всего, осуществляется систематизация и анализ ключевых понятий и принципов, лежащих в основе защиты данных, включая конфиденциальность, целостность, доступность, а также принципы минимизации данных, целевого использования и отчетности. Далее проводится критический обзор действующего международного и национального законодательства в области защиты данных, выявляются его сильные стороны и пробелы, а

также оценивается эффективность правоприменительной практики. Особое внимание уделяется анализу современных угроз безопасности данных, возникающих в условиях динамично развивающейся цифровой среды, включая кибератаки, инсайдерские угрозы и уязвимости в программном обеспечении. Затем исследуются существующие технические и организационные меры защиты данных, такие как шифрование, аутентификация, контроль доступа, системы обнаружения вторжений, а также политики безопасности и обучение персонала. В контексте новых технологических вызовов рассматривается их влияние на процессы обработки данных и разрабатываются рекомендации по адаптации существующих механизмов защиты к этим вызовам. Наконец, формулируются предложения по совершенствованию нормативно-правовой базы и практических подходов к обеспечению защиты данных, направленные на повышение уровня киберустойчивости и формирование культуры ответственного отношения к информации.

В процессе выполнения исследования применялись комплексные методы научного познания. Использовался системный подход, позволяющий рассматривать защиту данных как многоуровневую систему, включающую правовые, организационные и технические элементы, взаимосвязанные и взаимозависимые. Применялся сравнительно-правовой метод для анализа законодательства различных юрисдикций в сфере защиты данных, что позволило выявить общие тенденции и специфические особенности регулирования. Методы анализа и синтеза использовались для декомпозиции сложных проблем на составные части и последующего формирования целостного представления о предмете исследования. Проводился контент-анализ научных публикаций, нормативных актов, отраслевых стандартов и отчетов международных организаций. Применялся метод моделирования для разработки концептуальных моделей угроз и механизмов защиты.

Также использовался прогностический метод для оценки перспективных направлений развития технологий и их влияния на сферу защиты данных.

Структура данной работы логически следует поставленным задачам и представляет собой последовательное изложение материала. В первой главе осуществляется теоретическое осмысление сущности и значимости защиты данных в условиях цифровой трансформации, определяются основные термины и принципы, а также рассматривается эволюция подходов к обеспечению информационной безопасности. Вторая глава посвящена анализу нормативно-правового регулирования защиты данных на международном и национальном уровнях, выявляются ключевые правовые акты и их влияние на практику. Третья глава фокусируется на современных угрозах и вызовах безопасности данных, обусловленных развитием новых технологий, проводится классификация угроз и их потенциальных последствий. Четвертая глава содержит обзор существующих технических и организационных мер защиты данных, описываются их принципы действия и области применения. В пятой главе формулируются основные положения комплексной концепции защиты данных, интегрирующей рассмотренные аспекты, и предлагаются рекомендации по ее практической реализации. Завершается работа заключением, обобщающим основные результаты исследования и намечающим перспективы дальнейших изысканий в данной области.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ДАННЫХ В ЦИФРОВУЮ ЭПОХУ

1.1. Понятие и классификация данных в современном информационном пространстве

В современном информационном пространстве данные представляют собой фундаментальный элемент цифровой среды, выступая в качестве информации, существующей в электронном виде, которая подлежит использованию, обработке и передаче [1]. Феномен данных трансформировался из технического понятия в ключевой актив, определяющий экономические, социальные и даже политические процессы. Их ubiquity (повсеместность) и динамичность обусловливают необходимость комплексного подхода к их изучению, классификации и управлению, особенно в свете возрастающего объема генерируемой информации. Понимание сущности данных является отправной точкой для разработки эффективных стратегий их защиты, анализа и применения в различных сферах человеческой деятельности, что подчеркивает их центральную роль в современном обществе.

Особое внимание в контексте данных уделяется их правовой защите, особенно когда речь идет о персональных данных, поскольку их неправомерное использование способно повлечь за собой серьезные негативные последствия для субъектов данных [2]. Эта проблематика выходит за рамки сугубо технических аспектов и затрагивает фундаментальные права и свободы человека, такие как право на приватность и защиту личной информации. Установление четких правовых механизмов регулирования сбора, хранения, обработки и распространения персональных данных становится императивом для обеспечения баланса между инновационным развитием и защитой интересов граждан. Таким образом, правовая надстройка вокруг данных не является второстепенной, а формирует базис для доверия к цифровой

среде и ее институтам.

Цифровая коммуникация, являясь неотъемлемой частью современного информационного обмена, генерирует колоссальные объемы данных, при этом некорректное их использование или несанкционированное распространение может представлять серьезную угрозу для пользователей [3]. Это обстоятельство подчеркивает двойственную природу данных: с одной стороны, они являются катализатором прогресса и средством для улучшения качества жизни, с другой – источником рисков, если не соблюдаются принципы ответственного обращения. Угрозы могут варьироваться от неправомерного доступа к конфиденциальной информации до формирования ложных представлений о субъекте данных на основе некорректно интерпретированных цифровых следов. В связи с этим, развитие культуры цифровой грамотности и осведомленности о потенциальных рисках становится столь же важным, как и совершенствование технических средств защиты.

В контексте кибербезопасности данные выступают в качестве основного объекта защиты от несанкционированного доступа, изменения или уничтожения, что наглядно демонстрирует их значительную ценность в современном информационном пространстве [4]. Эта ценность обусловлена не только их экономической значимостью, но и стратегическим потенциалом, поскольку потеря или компрометация данных может привести к серьезным репутационным, финансовым и даже государственным рискам. Угрозы кибербезопасности постоянно эволюционируют, требуя непрерывного совершенствования методов и средств защиты, включая криптографические протоколы, системы обнаружения вторжений и многофакторную аутентификацию. Таким образом, обеспечение целостности, конфиденциальности и доступности данных является ключевым элементом национальной безопасности и

устойчивого развития цифрового общества.

Хранение банковских данных, включая конфиденциальную информацию о транзакциях и клиентах, осуществляется в специализированных дата-центрах, что подчеркивает критическую важность централизованного управления и защиты больших массивов данных [5]. Данный пример иллюстрирует не только техническую сложность обеспечения безопасности финансовых операций, но и правовую и этическую ответственность за сохранность чувствительной информации. Дата-центры, как специализированные инфраструктурные объекты, оснащены многоуровневыми системами защиты, включая физическую безопасность, резервное копирование и шифрование данных, что минимизирует риски их компрометации. Это свидетельствует о том, что для данных высокой ценности применяются наиболее строгие стандарты безопасности и управления, что является примером для других отраслей, работающих с большими данными.

Цифровая среда обладает уникальным свойством "памяти", сохраняя значительные объемы данных о действиях и взаимодействиях пользователей, тем самым формируя цифровой след и существенно влияя на приватность [6]. Этот феномен обусловлен тем, что практически каждое действие человека в сети – от поисковых запросов до онлайн-покупок – оставляет за собой след, который может быть агрегирован и проанализирован. Цифровой след, с одной стороны, может быть использован для персонализации услуг и улучшения пользовательского опыта, с другой – представляет угрозу для приватности, так как позволяет формировать детализированные профили пользователей без их явного согласия. Осознание этой "памяти" цифровой среды является критически важным для формирования ответственного поведения пользователей и разработки регуляторных механизмов, направленных на защиту их прав.

В условиях удаленного обучения и интенсивной цифровизации

образовательного процесса происходит активное накопление и обработка данных об обучающихся, их успеваемости и взаимодействии с образовательными платформами [7]. Этот тренд обусловлен стремлением к повышению эффективности образовательного процесса путем анализа больших данных, однако он также порождает новые вызовы, связанные с защитой конфиденциальности образовательной информации. Данные об успеваемости могут быть использованы для адаптации учебных программ и индивидуализации обучения, но в то же время они являются чувствительной информацией, требующей особого режима защиты. Разработка этических принципов и правовых норм для работы с образовательными данными становится приоритетной задачей для обеспечения доверия к цифровым образовательным системам и защиты интересов всех участников процесса.

Классификация данных может быть осуществлена по различным критериям, что позволяет более полно осмыслить их сущность и определить адекватные методы управления. В зависимости от степени конфиденциальности выделяют открытые данные, публичные данные, конфиденциальные данные, персональные данные и государственную тайну. По форме представления данные могут быть структурированными, полуструктурированными и неструктурированными, что влияет на методы их обработки и анализа. По источнику происхождения данные подразделяются на генерируемые пользователями, сенсорные данные, данные транзакций и данные, создаваемые машинами. Каждая из этих категорий требует специфических подходов к хранению, обработке, передаче и защите, что подчеркивает многогранность понятия данных в современном информационном пространстве.

Таким образом, понятие данных в современном информационном пространстве выходит далеко за рамки сугубо технического определения, охватывая правовые, этические, социальные и экономические аспекты.

Данные являются не только объектом защиты в контексте кибербезопасности, но и катализатором трансформационных процессов в различных сферах, от образования до финансов. Их классификация по различным признакам позволяет систематизировать подходы к управлению и обеспечению безопасности, а также формированию адекватной регуляторной среды. Осознание "памяти" цифровой среды и формирование цифрового следа требует от общества и регуляторов разработки комплексных решений, направленных на обеспечение баланса между инновационным развитием и защитой прав и свобод человека в цифровом мире.

1.2. Основные угрозы и вызовы безопасности данных: анализ актуальных рисков

В условиях перманентной цифровизации всех сфер жизнедеятельности общества проблема обеспечения безопасности данных приобретает критическое значение. Современный ландшафт угроз характеризуется высокой динамичностью и многообразием векторов атак, что требует комплексного анализа актуальных рисков для выработки адекватных мер противодействия. Одним из наиболее тревожных трендов является экспоненциальный рост числа целевых атак, которые направлены на получение несанкционированного доступа к конфиденциальным данным [8]. Эти атаки отличаются высокой степенью изощренности, тщательной подготовкой и использованием продвинутых методов обхода систем защиты, что делает их особенно опасными для организаций и частных лиц. Анализ показывает, что злоумышленники все чаще применяют тактики социальной инженерии, комбинируя их с техническими уязвимостями, для достижения своих целей, что подчеркивает необходимость многоуровневой защиты.

Проблема защиты персональных данных существенно усугубляется

увеличением количества выявляемых уязвимостей в программном обеспечении и информационных системах [9]. Этот феномен обусловлен не только возрастающей сложностью разрабатываемых систем, но и недостаточным вниманием к вопросам безопасности на этапах проектирования и тестирования. Каждая необнаруженная или неисправленная уязвимость представляет собой потенциальную точку входа для злоумышленников, позволяющую им эксплуатировать слабые места для компрометации данных. В связи с этим, критически важным становится внедрение принципов безопасной разработки (Security by Design) и регулярное проведение аудитов безопасности, направленных на выявление и устранение подобных «дыр» до того, как они будут обнаружены и использованы киберпреступниками. Отсутствие таких превентивных мер значительно повышает риски успешных атак.

Особое место среди актуальных угроз занимают фишинговые атаки, которые остаются одним из наиболее эффективных инструментов компрометации учетных данных пользователей [10]. Суть фишинга заключается в обмане пользователя с целью побудить его к раскрытию конфиденциальной информации, такой как логины, пароли или данные банковских карт, путем имитации легитимных ресурсов или коммуникаций. Несмотря на широкую осведомленность о фишинге, его вариации постоянно эволюционируют, становясь все более убедительными и трудноразличимыми. Это подчеркивает не только необходимость технических средств защиты, таких как многофакторная аутентификация и системы фильтрации электронной почты, но и важность постоянного обучения пользователей распознаванию подобных угроз, поскольку человеческий фактор часто становится самым слабым звеном в цепи кибербезопасности.

Недостаточный уровень цифровой гигиены пользователей является одной из ключевых причин успешных кибератак, что подтверждается

многочисленными исследованиями [10]. Под цифровой гигиеной понимается совокупность практик и привычек, направленных на минимизацию рисков в цифровой среде, включая использование надежных паролей, осторожность при открытии подозрительных ссылок и вложений, а также регулярное обновление программного обеспечения. Отсутствие должного внимания к этим элементарным правилам создает благоприятную почву для реализации угроз, поскольку даже самые совершенные технические средства защиты могут быть обойдены из-за ошибок или неосторожности конечного пользователя. Это подчеркивает необходимость комплексного подхода к кибербезопасности, включающего не только технологические решения, но и активное формирование культуры безопасного поведения.

Отсутствие регулярного аудита и тестирования ИТ-инфраструктуры компаний может привести к накоплению необнаруженных уязвимостей, что создает значительные риски для безопасности данных [11]. Систематический аудит позволяет выявлять слабые места в конфигурации систем, сетевой архитектуре, а также в используемом программном обеспечении. Тестирование на проникновение (пентест) имитирует действия злоумышленников, что дает возможность оценить реальную устойчивость системы к атакам и выявить пути несанкционированного доступа. Без этих процедур организации функционируют в условиях неопределенности относительно своего реального уровня защищенности, что делает их легкой мишенью для киберпреступников. Таким образом, регулярные проверки являются не просто рекомендацией, а критически важным элементом стратегии управления рисками информационной безопасности.

Важным вызовом для современных организаций является необходимость повышения уровня осведомленности сотрудников о правилах кибербезопасности [12]. Технические средства защиты, какими

бы совершенными они ни были, не могут полностью нивелировать риски, связанные с человеческим фактором. Сотрудники, не обладающие достаточными знаниями о потенциальных угрозах и методах их предотвращения, могут стать невольными соучастниками кибератак, например, путем перехода по фишинговым ссылкам или использования ненадежных паролей. Эффективные программы обучения и повышения осведомленности должны быть непрерывными, интерактивными и адаптированными к специфике деятельности организации, формируя у персонала устойчивые навыки безопасного поведения в цифровой среде. Это инвестиция, которая окупается снижением вероятности инцидентов информационной безопасности.

В ответ на возрастающие угрозы конфиденциальности данных и ужесточение регуляторных требований, внедрение технологий приватности (Privacy Tech) становится актуальным направлением развития [13]. Эти технологии призваны обеспечить защиту персональных данных на всех этапах их жизненного цикла – от сбора до удаления. Примеры таких решений включают гомоморфное шифрование, позволяющее обрабатывать зашифрованные данные без их расшифровки; федеративное обучение, при котором модели машинного обучения тренируются на децентрализованных данных без их передачи на центральный сервер; и дифференциальную приватность, добавляющую шум к данным для защиты индивидуальных записей. Развитие и применение Privacy Tech является стратегическим ответом на вызовы, связанные с массовой обработкой данных, позволяя организациям соблюдать принципы приватности без ущерба для аналитических возможностей. Это направление способствует формированию более безопасной и этичной цифровой среды.

1.3. Законодательные и нормативные основы защиты данных на национальном и международном уровнях

В контексте динамичного развития цифровой экономики и глобализации информационного пространства, вопросы законодательного и нормативного регулирования защиты данных приобретают критическое значение. Современные вызовы, обусловленные экспоненциальным ростом объемов данных, усложнением киберугроз и появлением новых технологий, таких как искусственный интеллект (ИИ), требуют комплексного подхода к формированию правовой базы. Развитие ИИ, в частности, порождает специфические киберугрозы, связанные с несанкционированным доступом, модификацией или неправомерным использованием данных, обрабатываемых ИИ-системами, что диктует необходимость разработки инновационных подходов к обеспечению информационной безопасности [14]. Это подчеркивает фундаментальное изменение парадигмы защиты данных: от реактивного реагирования на инциденты к проактивному формированию превентивных механизмов, способных учитывать потенциальные риски, присущие новым технологическим ландшафтам.

Глобальный характер киберугроз, не признающий национальных границ, обусловливает настоятельную потребность в унификации подходов к кибербезопасности и защите данных на международном уровне. Инициатива по созданию Глобального цифрового договора является стратегическим шагом к формированию единых международных принципов и правил регулирования цифрового пространства, включая аспекты защиты данных [15]. Подобные инициативы направлены на преодоление фрагментации национальных законодательств, которая может создавать «серые зоны» для киберпреступности и затруднять трансграничное сотрудничество в борьбе с ней. Унификация стандартов и процедур не только способствует повышению эффективности противодействия угрозам, но и формирует более предсказуемую и безопасную среду для развития цифровой экономики, обеспечивая

доверие пользователей к цифровым сервисам.

В условиях расширения экосистемы Интернета вещей (IoT) и повсеместного распространения устройств умного дома, возрастает значимость защиты персональных и конфиденциальных данных. Рекомендации по усилению киберзащиты устройств умного дома путем использования сертифицированных сервисов акцентируют внимание на необходимости обеспечения безопасности конечных пользовательских устройств, которые зачастую становятся точками входа для злоумышленников [16]. Этот аспект подчеркивает переход от защиты корпоративных сетей к необходимости обеспечения безопасности на уровне индивидуальных пользователей и их цифровых активов. Регуляторные органы сталкиваются с задачей разработки стандартов сертификации и механизмов контроля, которые гарантировали бы адекватный уровень защиты данных, собираемых и обрабатываемых устройствами IoT, что является критически важным для поддержания конфиденциальности и неприкосновенности частной жизни граждан.

Эффективная защита данных и обеспечение кибербезопасности в корпоративном секторе требуют внедрения комплексных систем, которые включают в себя как передовые технические средства, так и организационные меры. Ключевыми организационными элементами являются систематическое обучение персонала и формирование устойчивой культуры кибербезопасности [17]. Технические решения, такие как межсетевые экраны, системы обнаружения вторжений и средства шифрования, являются лишь частью общей стратегии. Без осознанного участия сотрудников, их понимания потенциальных угроз и соблюдения правил безопасности, даже самые совершенные технические системы могут оказаться уязвимыми. Таким образом, инвестиции в человеческий капитал и повышение осведомленности персонала становятся столь же важными, как и вложения в технологическую

инфраструктуру, что отражает сдвиг в фокусе от исключительно технологической защиты к комплексной системе, включающей человеческий фактор.

Современные тенденции в области кибербезопасности характеризуются усилением регуляторного давления, что обусловлено экспоненциальным ростом числа кибератак и обострением проблемы утечек данных. Законодатели и регуляторы по всему миру активно работают над созданием более строгих правил, направленных на повышение ответственности компаний за сохранность информации [18]. Этот тренд отражает осознание того, что саморегулирование в условиях стремительного развития цифровых технологий может быть недостаточным для обеспечения адекватного уровня защиты. Введение штрафов за несоблюдение требований по защите данных, обязательность уведомления об инцидентах и требования по внедрению определенных стандартов безопасности становятся нормой, что стимулирует организации к более ответственному подходу к управлению данными и минимизации рисков.

Формирование культуры безопасности как неотъемлемой части корпоративной стратегии является мощным фактором укрепления защиты информационных систем и данных. Вовлечение сотрудников в процесс обеспечения безопасности, повышение их осведомленности и ответственности создают многоуровневую систему защиты, где каждый сотрудник становится активным участником процесса, а не пассивным объектом инструкций [19]. Это позволяет трансформировать безопасность из функции сугубо ИТ-отдела в общекорпоративную ценность, проникнувшую во все бизнес-процессы. Подобный подход снижает вероятность инцидентов, вызванных человеческим фактором, и способствует формированию проактивной позиции в отношении киберугроз, что является критически важным в условиях постоянно

меняющегося ландшафта кибербезопасности.

Постоянное появление новых цифровых угроз, таких как изощренные фишинговые атаки, программы-вымогатели и масштабные утечки данных, требует непрерывного совершенствования законодательной и нормативной базы. Адекватное реагирование на вызовы в сфере информационной безопасности невозможно без гибкого и динамичного правового регулирования, способного оперативно адаптироваться к изменяющимся условиям [20]. Это включает в себя не только внесение поправок в существующие законы, но и разработку совершенно новых нормативных актов, регулирующих ранее не охваченные аспекты цифровой деятельности. Задача законодателя заключается в поиске баланса между необходимостью защиты данных, обеспечением инновационного развития и предотвращением чрезмерного регулирования, которое может стать препятствием для технологического прогресса. Таким образом, правовое поле в сфере защиты данных должно быть живым организмом, способным эволюционировать синхронно с развитием технологий и угроз.

ГЛАВА 2. МЕТОДЫ И ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ДАННЫХ

2.1. Технические средства и методы криптографической защиты информации

В контексте современных информационных систем, где объем передаваемых и хранимых данных непрерывно возрастает, проблематика обеспечения их конфиденциальности, целостности и доступности приобретает особую актуальность. Технические средства и методы криптографической защиты информации выступают в качестве фундаментального инструментария, позволяющего противостоять многообразным угрозам, возникающим в условиях новой сетевой реальности [21]. Эффективность их применения напрямую коррелирует с уровнем развития технологий и адекватностью реагирования на постоянно эволюционирующие вызовы кибербезопасности [22]. Современные подходы к криптографической защите интегрируют математические алгоритмы, аппаратные решения и организационные меры, формируя комплексную систему обеспечения информационной безопасности. Именно такой многоаспектный подход позволяет минимизировать риски несанкционированного доступа и манипулирования данными.

Развитие криптографических методов детерминировано необходимостью защиты данных от потенциальных угроз, исходящих как от злоумышленников, так и от непреднамеренных ошибок. В данном контексте, деятельность, связанная с развитием информационных ресурсов, неизбежно сталкивается с потребностью в имплементации надежных криптографических протоколов [23]. При этом следует учитывать, что сам по себе цифровой след, формируемый в процессе взаимодействия с информационными системами, несет в себе не только потенциал для оптимизации процессов и персонализации сервисов, но и значительные риски, связанные с возможностью его неправомерного

использования [21]. Криптографические методы, такие как шифрование, хеширование и электронная подпись, призваны нивелировать эти риски, обеспечивая защиту персональных данных, коммерческой тайны и государственных секретов. Анализ публикационной активности по наукометрическим показателям свидетельствует о возрастающем интересе к исследованиям в области криптографии, что отражает актуальность данной проблематики на глобальном уровне [24].

Особое место в системе криптографической защиты информации занимают аппаратные средства, обеспечивающие высокую скорость обработки данных и повышенную стойкость к атакам. Криптографические процессоры, аппаратные модули безопасности (HSM) и смарт-карты представляют собой примеры таких решений, которые позволяют реализовать криптографические операции на уровне, недоступном для чисто программных методов. Эти устройства зачастую используются для генерации и хранения криптографических ключей, выполнения операций шифрования/дешифрования и формирования электронной подписи. Применение аппаратных средств существенно снижает риски компрометации ключей и данных, поскольку они физически изолированы от основной вычислительной среды. Однако, внедрение таких решений сопряжено с определенными экономическими и техническими издержками, что требует тщательного анализа целесообразности их применения в каждом конкретном случае.

В условиях возрастающей сложности киберугроз, где злоумышленники постоянно совершенствуют свои методы, роль превентивных мер и проактивной защиты становится критически важной. В этом контексте, феномен "этических хакеров" приобретает особую значимость, поскольку их деятельность направлена на выявление уязвимостей в информационных системах до того, как они будут использованы злоумышленниками [25]. Применение методов пентестинга

(проникновения), аудита безопасности и анализа исходного кода позволяет выявить потенциальные точки отказа и слабые места в криптографических реализациях. Результаты такой деятельности служат основой для усовершенствования существующих криптографических протоколов и разработки новых, более устойчивых к атакам решений. Взаимодействие между разработчиками криптографических систем и специалистами по кибербезопасности является ключевым фактором в обеспечении высокой степени защищенности информации.

Помимо технических аспектов, эффективная криптографическая защита информации требует учета социальных и культурных факторов. Проблема цифровизации, затрагивающая различные сферы жизни, включая сохранение культурного наследия, подчеркивает необходимость разработки универсальных и безопасных методов хранения и передачи информации [26]. Это влечет за собой потребность в создании стандартов и регламентов, которые бы обеспечивали совместимость и интероперабельность криптографических систем, а также учитывали особенности различных предметных областей. Формирование экспертных советов, в том числе по культуре, может способствовать выработке рекомендаций и стратегий по внедрению криптографических решений в специфические сферы деятельности, обеспечивая при этом соблюдение этических норм и культурных особенностей [27]. Таким образом, криптографическая защита информации представляет собой не только техническую, но и междисциплинарную проблему, требующую комплексного подхода.

В заключение, можно констатировать, что технические средства и методы криптографической защиты информации являются краеугольным камнем современной системы информационной безопасности. Их эволюция детерминирована постоянным противостоянием между защитниками и злоумышленниками, а также бурным развитием цифровых

технологий. Эффективность криптографических решений определяется не только их математической стойкостью, но и корректностью имплементации, а также адекватностью реагирования на новые угрозы. Анализ текущего состояния и перспектив развития криптографических методов свидетельствует о необходимости дальнейших исследований и разработок в этой области, направленных на создание более совершенных, адаптивных и устойчивых к атакам систем. Это, в свою очередь, требует консолидации усилий научного сообщества, разработчиков и регуляторов для обеспечения безопасного функционирования информационных систем в условиях глобальной цифровизации.

2.2. Организационные и правовые меры обеспечения конфиденциальности и целостности данных

Обеспечение конфиденциальности и целостности данных представляет собой фундаментальную задачу для современных информационных систем, особенно в контексте функционирования электронных библиотек. Критическое значение этих аспектов для таких институций, как Российская национальная библиотека, подчеркивается необходимостью гарантировать надежный доступ к обширным массивам цифровых ресурсов при одновременном соблюдении принципов их сохранности и защиты от несанкционированного воздействия [28]. В условиях непрерывной цифровизации и расширения спектра предоставляемых услуг, вопросы безопасности информации приобретают первостепенное значение, требуя комплексного подхода к разработке и внедрению организационных и правовых мер. Это обусловлено не только техническими аспектами защиты, но и формированием правового поля, регулирующего процессы обработки и хранения данных.

Модернизация библиотечной сети, примером которой служит Российская государственная библиотека, включает в себя не только

технологическое обновление, но и имплементацию всеобъемлющих мер по защите данных в условиях их цифрового представления [29]. Данный процесс охватывает разработку и внедрение внутренних политик безопасности, стандартизацию процедур работы с конфиденциальной информацией, а также формирование механизмов реагирования на инциденты информационной безопасности. Особое внимание уделяется обеспечению целостности данных, что подразумевает предотвращение их случайного или преднамеренного искажения, а также гарантирование аутентичности информации на всех этапах ее жизненного цикла. В этом контексте, организационные меры включают в себя регламентацию доступа к информационным ресурсам, разграничение полномочий пользователей, а также регулярное обучение персонала основам информационной безопасности.

Правовые меры, направленные на обеспечение конфиденциальности и целостности данных, формируются под влиянием требований регулирующих органов, примером которых является Роскомнадзор. Деятельность данного органа, в частности, по выдвижению требований к операторам, включая VPN-сервисы, относительно блокировки доступа к определенным сайтам, демонстрирует сложность взаимодействия между государственной регуляцией и аспектами конфиденциальности и доступности информации [30]. В данном контексте, правовые нормы определяют границы допустимого использования и обработки данных, устанавливают ответственность за их неправомерное использование и нарушение конфиденциальности. Для электронных библиотек это означает необходимость строгого соблюдения законодательства о персональных данных, авторском праве и защите информации, что требует постоянного мониторинга изменений в правовом поле и адаптации внутренних регламентов.

Защита культурного и исторического наследия, представленного в

рукописных и архивных фондах, требует применения специфических организационных и правовых мер, направленных на обеспечение их целостности и предотвращение несанкционированного доступа [31]. В условиях цифровизации, когда создаются электронные копии уникальных артефактов, возникает необходимость в разработке новых подходов к их сохранности. Это включает в себя не только физическую защиту оригиналов, но и обеспечение цифровой целостности их копий, что подразумевает использование криптографических методов, электронных подписей и систем контроля версий. Правовые аспекты, в свою очередь, регулируют вопросы авторских прав на оцифрованные материалы, условия их использования и распространения, а также меры ответственности за нарушение установленных правил.

Управление цифровыми коллекциями и архивами, как это реализуется в случае с электронными ресурсами Российской национальной библиотеки, подразумевает внедрение комплексных механизмов, гарантирующих сохранность и аутентичность данных на протяжении длительного времени [32]. Это включает в себя разработку стратегий долгосрочного хранения, использование стандартизированных форматов данных, а также применение технологий, обеспечивающих верификацию целостности информации. Организационные меры в этом направлении включают создание специализированных отделов по управлению цифровыми ресурсами, разработку процедур резервного копирования и восстановления данных, а также проведение регулярных аудитов безопасности. Правовые рамки, в свою очередь, регулируют вопросы владения цифровыми коллекциями, их доступности для пользователей и условия их использования в научных и образовательных целях.

Внедрение новых технологий и создание цифровых копий физических объектов, таких как рукописные памятники, требует

разработки политик, обеспечивающих сохранение их целостности и защиту от модификаций [32]. Это особенно актуально для уникальных и бесценных артефактов, где любая потеря или искажение информации является недопустимой. Технические решения, такие как блокчейн-технологии или распределенные реестры, могут быть рассмотрены в качестве потенциальных инструментов для обеспечения неизменности цифровых копий. Организационные меры включают в себя строгий контроль за процессами оцифровки, применение высококачественного оборудования и программного обеспечения, а также создание дублирующих систем хранения. Правовые нормы призваны регулировать процессы создания и использования цифровых копий, определяя их юридический статус и степень соответствия оригиналам.

Вопросы безопасности данных и их защиты от несанкционированного доступа актуальны не только для цифровых библиотек, но и для других систем, работающих с информацией, что подчеркивает универсальность принципов обеспечения конфиденциальности и целостности [33]. Это означает, что опыт и лучшие практики, накопленные в библиотечной сфере, могут быть применены и в других областях, таких как государственное управление, финансовый сектор или здравоохранение. Универсальность принципов безопасности данных заключается в общности подходов к управлению рисками, разработке политик безопасности, внедрению технических средств защиты и обучению персонала. Таким образом, организационные и правовые меры, разработанные для электронных библиотек, могут служить моделью для обеспечения информационной безопасности в более широком контексте, способствуя формированию единой системы защиты данных на национальном уровне.

2.3. Перспективы развития систем защиты данных в условиях трансформации цифровой среды

Перспективы развития систем защиты данных в условиях продолжающейся трансформации цифровой среды детерминированы необходимостью радикального переосмысления существующих подходов к кибербезопасности. Традиционные методы защиты, ориентированные преимущественно на реактивное реагирование и сигнатурный анализ угроз, демонстрируют недостаточную эффективность в условиях экспоненциального роста сложности и вариативности кибератак, что подтверждает общую тенденцию к динамической эволюции угроз и защитных механизмов [34]. Отмечается, что противостояние между атакующими и защищающими сторонами приобретает характер перманентного технологического соревнования, требующего от систем безопасности непрерывной адаптации и проактивного развития [35]. Это обусловливает потребность в интеграции инновационных методологий и технологий, способных предвосхищать и нейтрализовывать потенциальные угрозы до их полной реализации.

В контексте повышения проактивности и эффективности защитных мер, особую значимость приобретает применение методов открытой разведки (OSINT) и специализированного поиска угроз (Threat Hunting). Интеграция OSINT позволяет агрегировать и анализировать информацию из публичных источников для выявления потенциальных уязвимостей и индикаторов компрометации, что способствует формированию комплексного представления о ландшафте угроз [36]. Параллельно, методология Threat Hunting предполагает активный, итеративный поиск скрытых или невыявленных угроз внутри защищаемой инфраструктуры, что принципиально отличается от пассивного ожидания срабатывания систем обнаружения. Комбинация этих подходов обеспечивает возможность обнаружения и нейтрализации кибератак на ранних стадиях их развития, минимизируя потенциальный ущерб и повышая общую устойчивость информационных систем [36]. Данная синергия

трансформирует парадигму кибербезопасности от реактивной к предиктивной, что является критически важным в условиях возрастающей сложности современных киберугроз.

Существенное влияние на эволюцию систем защиты данных оказывает конвергенция квантовых технологий и искусственного интеллекта (ИИ). Квантовые методы, в частности квантовая криптография и квантовые вычисления, обещают принципиально новый уровень безопасности, основанный на законах квантовой механики, что делает их потенциально неуязвимыми для существующих и перспективных методов взлома [37]. Одновременно, искусственный интеллект, обладая способностью к самообучению и анализу огромных объемов данных, становится мощным инструментом для автоматизации процессов обнаружения аномалий, прогнозирования угроз и оптимизации защитных механизмов. Интеграция ИИ в системы безопасности позволяет создавать адаптивные, саморегулирующиеся платформы, способные оперативно реагировать на изменяющуюся обстановку и выявлять сложные, многовекторные атаки, которые остаются незамеченными для традиционных систем [37]. Однако, применение ИИ в целях кибербезопасности требует тщательного контроля, поскольку его возможности могут быть использованы и в деструктивных целях, что создает новые вызовы для разработчиков защитных систем [38].

Трансформация цифровой среды, характеризующаяся повсеместным распространением технологий искусственного интеллекта, порождает новые категории угроз, включая использование ИИ в деструктивных целях. Злоумышленники могут применять алгоритмы машинного обучения для автоматизации фаз разведки, разработки эксплойтов, обхода средств защиты и создания высокоэффективных фишинговых кампаний, что значительно повышает масштаб и сложность атак [38]. В ответ на эти вызовы, разработка адекватных контрмер становится приоритетной

задачей. Это включает создание систем искусственного интеллекта, способных обнаруживать и нейтрализовывать атаки, генерируемые другими ИИ, а также развитие методов для выявления и противодействия глубоким фейкам (deepfakes) и другим формам манипуляции информацией, созданным с помощью алгоритмов. Эффективность защитных стратегий будет зависеть от способности систем безопасности адаптироваться к быстро меняющимся методам атак, основанным на ИИ.

В условиях динамично меняющегося цифрового ландшафта, одним из ключевых аспектов является осознание принципиальной недостижимости абсолютной безопасности. Концепция "нулевого риска" в кибербезопасности является утопичной, поскольку постоянное появление новых уязвимостей и эволюция методов атак делают невозможным полное исключение всех потенциальных угроз [39]. Следовательно, стратегическим приоритетом становится не полное устранение рисков, а их минимизация до приемлемого уровня посредством реализации комплексного подхода к защите. Этот подход предполагает многоуровневую оборону, включающую технические, организационные и человеческие аспекты, а также непрерывный мониторинг, анализ и адаптацию защитных мер. Принятие этого принципа позволяет направлять ресурсы на наиболее критичные области, обеспечивая максимальную эффективность при ограниченных возможностях.

Для обеспечения эффективной защиты данных в условиях непрерывной цифровой трансформации, недостаточно лишь внедрения передовых технологических решений. Критически важным компонентом устойчивой кибербезопасности является формирование культуры кибербезопасности внутри организаций и общества в целом [40]. Это подразумевает повышение осведомленности пользователей о потенциальных угрозах, развитие навыков безопасного поведения в цифровой среде и формирование ответственного отношения к защите

конфиденциальной информации. Человеческий фактор зачастую остается наиболее уязвимым звеном в системе безопасности, и даже самые совершенные технические средства могут быть скомпрометированы из-за отсутствия должной бдительности или несоблюдения базовых правил безопасности. Следовательно, инвестиции в обучение и развитие осведомленности персонала должны рассматриваться как неотъемлемая часть комплексной стратегии по защите данных, основанной на принципах осознанности и коллективной ответственности [40].

ЗАКЛЮЧЕНИЕ

Настоящее исследование, посвященное проблематике защиты данных в цифровую эпоху, позволило систематизировать и углубить понимание ключевых аспектов данной предметной области. В ходе анализа было установлено, что стремительное развитие информационных технологий и повсеместное внедрение цифровых платформ привели к экспоненциальному росту объемов генерируемых и обрабатываемых данных, что, в свою очередь, актуализировало вопрос обеспечения их конфиденциальности, целостности и доступности. Анализ показал, что угрозы безопасности данных эволюционируют, приобретая все более изощренные формы, и включают в себя как внешние атаки, так и внутренние уязвимости, связанные с человеческим фактором и недостатками системной архитектуры. Было выявлено, что правовая база, регулирующая защиту данных, несмотря на значительные шаги в направлении унификации и ужесточения требований, такие как принятие Общего регламента по защите данных (GDPR) в Европейском союзе, все еще сталкивается с вызовами, обусловленными трансграничным характером цифровых операций и различиями в национальных юрисдикциях. Можно сделать вывод о том, что эффективная защита данных требует комплексного подхода, охватывающего технологические, организационные и правовые аспекты.

Поставленная цель исследования, заключавшаяся в проведении всестороннего анализа современного состояния и перспектив развития механизмов защиты данных в условиях цифровой трансформации общества, была достигнута в полной мере. Результаты работы подтверждают, что выбранная методология позволила не только описать существующие проблемы, но и выявить тенденции, а также предложить направления для их решения. Была сформирована целостная картина вызовов и возможностей, стоящих перед субъектами, осуществляющими

обработку данных, и субъектами данных, чьи права требуют надежной защиты. Подтверждается, что исследование обеспечило глубокое понимание принципов и методов, применяемых для минимизации рисков утечки и несанкционированного доступа к информации, а также для обеспечения соответствия нормативным требованиям.

Практическая значимость полученных результатов заключается в возможности их применения для разработки и совершенствования стратегий и политик в области информационной безопасности на уровне государственных структур, корпораций и индивидуальных пользователей. Аналитические выводы исследования могут служить основой для формирования рекомендаций по внедрению передовых технологических решений, таких как криптографические методы, системы контроля доступа, технологии блокчейн для обеспечения неизменности данных, а также по повышению осведомленности персонала в вопросах кибергигиены. Результаты могут быть использованы при разработке образовательных программ, направленных на подготовку специалистов в области защиты данных, а также при формировании нормативно-правовых актов, регулирующих цифровую среду. Предложенные подходы к оценке рисков и управлению инцидентами могут быть интегрированы в системы менеджмента информационной безопасности организаций, способствуя повышению их устойчивости к киберугрозам.

Перспективы дальнейших исследований в данной области представляются обширными и многогранными. В частности, актуальным является углубленный анализ влияния искусственного интеллекта и машинного обучения на процессы защиты данных, включая как потенциальные угрозы, связанные с новыми видами атак, так и возможности использования этих технологий для повышения эффективности систем безопасности. Требует дальнейшего изучения проблематика защиты данных в контексте развития квантовых

вычислений, что ставит под вопрос устойчивость существующих криптографических алгоритмов. Целесообразно проведение компаративных исследований правовых режимов защиты данных в различных юрисдикциях с целью выработки универсальных подходов и стандартов. Необходимы также исследования, направленные на разработку более совершенных методов анонимизации и псевдонимизации данных, позволяющих совместить требования конфиденциальности с возможностями использования больших данных для аналитических целей. Отдельным направлением может стать изучение социально-этических аспектов защиты данных, включая вопросы приватности и контроля над личной информацией в условиях тотальной цифровизации.

СПИСОК ИСТОЧНИКОВ

1. Презентация по ОБЗР "Цифровая среда — её возможности и ... [Электронный ресурс] // infourok.ru. URL: https://infourok.ru/magazin-materialov/prezentaciya-po-obzr-cifrovaya-sreda-eyo-vozmozhnosti-i-riski-584129 (дата обращения: 31.07.2025).

2. Реферат на тему “Правовая защита информации” - Инфоурок [Электронный ресурс] // infourok.ru. URL: https://infourok.ru/referat-na-temu-pravovaya-zashita-informacii-4112085.html (дата обращения: 31.07.2025).

3. Опасности, связанные с коммуникацией в цифровой среде [Электронный ресурс] // infourok.ru. URL: https://infourok.ru/opasnosti-svyazannye-s-kommunikaciej-v-cifrovoj-srede-7785343.html (дата обращения: 31.07.2025).

4. Проект "Кибербезопастность в современном мире" - Инфоурок [Электронный ресурс] // infourok.ru. URL: https://infourok.ru/proekt-kiberbezopastnost-v-sovremennom-mire-7166098.html (дата обращения: 31.07.2025).

5. Хранение банковских данных: дата-центры, утечки, закон [Электронный ресурс] // postnauka.ru. URL: https://postnauka.ru/longreads/156723 (дата обращения: 31.07.2025).

6. Оксана Мороз: «Цифра все помнит - ПостНаука [Электронный ресурс] // postnauka.ru. URL: https://postnauka.ru/talks/155294 (дата обращения: 31.07.2025).

7. Все на «удаленку»: как улучшить качество обучения в цифровой ... [Электронный ресурс] // postnauka.ru. URL: https://postnauka.ru/longreads/156713 (дата обращения: 31.07.2025).

8. Кибербезопасность 2025: актуальные риски и тренды [Электронный ресурс] // events.kommersant.ru. URL: https://events.kommersant.ru/nov/events/2025-04-29_kiberbezopasnost-2025-

aktualnye-riski-i-trendy/ (дата обращения: 31.07.2025).

9. Цифровая безопасность: защита персональных данных в 2025 ... [Электронный ресурс] // companies.rbc.ru. URL: https://companies.rbc.ru/news/dkKcuXS8bn/tsifrovaya-bezopasnost-zaschita-personalnyih-dannyih-v-2025-godu/ (дата обращения: 31.07.2025).

10. Цифровая гигиена: понятие, угрозы, правила поведения [Электронный ресурс] // rg.ru. URL: https://rg.ru/2024/01/05/cifrovaia-gigiena.html (дата обращения: 31.07.2025).

11. Как узнать, защищена ли ИТ-инфраструктура компании? [Электронный ресурс] // spbspecials.rbc.ru. URL: https://spbspecials.rbc.ru/infosec (дата обращения: 31.07.2025).

12. Кибербезопасное будущее: почему так важно просвещение в ... [Электронный ресурс] // Forbes Russia. URL: https://www.forbes.ru/tekhnologii/518060-kiberbezopasnoe-budusee-pocemu-tak-vazno-prosvesenie-v-sfere-zasity-dannyh (дата обращения: 31.07.2025).

13. Privacy Tech: что такое технологии приватности и почему о них ... [Электронный ресурс] // trends.rbc.ru. URL: https://trends.rbc.ru/trends/industry/616ea4d99a79475ac0ce76ad (дата обращения: 31.07.2025).

14. Как обеспечить безопасное внедрение ИИ-технологий в ... - РБК [Электронный ресурс] // www.rbc.ru. URL: https://www.rbc.ru/industries/news/687640599a7947861f221de0 (дата обращения: 31.07.2025).

15. Что такое Глобальный цифровой договор и зачем он нужен [Электронный ресурс] // trends.rbc.ru. URL: https://trends.rbc.ru/trends/social/66f663df9a794766a4bb24ed (дата обращения: 31.07.2025).

16. Власти рекомендовали усилить киберзащиту умных домов ... [Электронный ресурс] // Forbes Russia. URL:

https://www.forbes.ru/tekhnologii/542886-vlasti-rekomendovali-usilit-kiberzasitu-umnyh-domov-sertificirovannymi-fsb-servisami (дата обращения: 31.07.2025).

17. Что должен знать собственник об информационной ... [Электронный ресурс] // companies.rbc.ru. URL: https://companies.rbc.ru/news/KSYPmiQPbm/chto-dolzhen-znat-sobstvennik-ob-informatsionnoj-bezopasnosti-kompanii/ (дата обращения: 31.07.2025).

18. Технологии против угроз: 7 трендов кибербезопасности в 2025 ... [Электронный ресурс] // trends.rbc.ru. URL: https://trends.rbc.ru/trends/industry/678f84c69a79478682c0120b (дата обращения: 31.07.2025).

19. Культура безопасности: как соревнования укрепляют защиту IT ... [Электронный ресурс] // Forbes Russia. URL: https://www.forbes.ru/brandvoice/536437-kul-tura-bezopasnosti-kak-sorevnovania-ukreplaut-zasitu-it-produktov-al-fa-banka (дата обращения: 31.07.2025).

20. Цифровая нагрузка: угрозы, решения и приоритеты на будущее [Электронный ресурс] // Forbes Russia. URL: https://www.forbes.ru/brandvoice/483124-cifrovaa-nagruzka-ugrozy-resenia-i-prioritety-na-budusee (дата обращения: 31.07.2025).

21. Новая сетевая реальность. Польза и риски цифрового следа [Электронный ресурс] // tass.ru. URL: https://tass.ru/obschestvo/24390587 (дата обращения: 31.07.2025).

22. Ключевыми темами OFFZONE 2025 станут вызовы и решения в ... [Электронный ресурс] // www.interfax.ru. URL: https://www.interfax.ru/events/news/1037812 (дата обращения: 31.07.2025).

23. Российская книжная палата [Электронный ресурс] // www.rsl.ru. URL: https://www.rsl.ru/ru/rkp/ (дата обращения: 31.07.2025).

24. РГБ в РИНЦ. Публикационная активность по

наукометрическим ... [Электронный ресурс] // www.rsl.ru. URL: https://www.rsl.ru/ru/2professionals/rgb-v-rincz (дата обращения: 31.07.2025).

25. Этичный хакер: защитник цифрового мира и перспективная ... [Электронный ресурс] // trends.rbc.ru. URL: https://trends.rbc.ru/trends/education/66ab41479a794737d637fdb6 (дата обращения: 31.07.2025).

26. сохранение культурного наследия и вызовы цифровизации | Дуда [Электронный ресурс] // bibliotekovedenie.rsl.ru. URL: https://bibliotekovedenie.rsl.ru/jour/article/view/2477/1470 (дата обращения: 31.07.2025).

27. Вадим Дуда провёл первое заседание Экспертного совета по ... [Электронный ресурс] // www.rsl.ru. URL: https://www.rsl.ru/ru/all-news/zasedanie-soveta-po-kulture (дата обращения: 31.07.2025).

28. Российская национальная библиотека Электронная библиотека. Российская национальная библиотека [Электронный ресурс] // nlr.ru. URL: https://nlr.ru/eng/RA2403/digital-library (дата обращения: 31.07.2025).

29. итоги и перспективы модернизации библиотечной сети [Электронный ресурс] // www.rsl.ru. URL: https://www.rsl.ru/ru/all-news/kulturnaya-perezagruzka (дата обращения: 31.07.2025).

30. Роскомнадзор требует от VPN банить сайты: кто согласился, а кто отказался [Электронный ресурс] // daily.afisha.ru. URL: https://daily.afisha.ru/brain/11845-roskomnadzor-trebuet-ot-vpn-banit-sayty-kto-soglasilsya-a-kto-otkazalsya/ (дата обращения: 31.07.2025).

31. Российская национальная библиотека Русские архивы. Российская национальная библиотека. Описание. Рукописи [Электронный ресурс] // nlr.ru. URL: https://nlr.ru/eng/RA2786/archive-collection (дата обращения: 31.07.2025).

32. Рукописные памятники в Российской национальной библиотеке [Электронный ресурс] // nlr.ru. URL: https://nlr.ru/manuscripts/RA362/rukopisnyie-pamyatniki (дата обращения: 31.07.2025).

33. Как выглядят дисковый домофон и банкомат? Показывает дизайнер из Петербурга [Электронный ресурс] // daily.afisha.ru. URL: https://daily.afisha.ru/brain/14824-kak-vyglyadyat-diskovyy-domofon-i-bankomat-pokazyvaet-dizayner-iz-peterburga/?amp;utm_medium=socialsharing&utm_campaign=kak-vyglyadyat-diskovyy-domofon-i-bankomat-pokazyvaet-dizayner-iz-peterburga (дата обращения: 31.07.2025).

34. Цифровая крепость: как защитить себя в мире киберугроз [Электронный ресурс] // Хабр. URL: https://habr.com/ru/articles/832928/ (дата обращения: 31.07.2025).

35. Кибербезопасность в эпоху цифровых технологий [Электронный ресурс] // Хабр. URL: https://habr.com/ru/articles/814007/ (дата обращения: 31.07.2025).

36. к ак OSINT и threat hunting защищают ваши данные / Хабр - Habr [Электронный ресурс] // Хабр. URL: https://habr.com/ru/articles/837108/ (дата обращения: 31.07.2025).

37. методов защиты данных и ИИ [Электронный ресурс] // Хабр. URL: https://habr.com/ru/companies/solarsecurity/articles/869084/ (дата обращения: 31.07.2025).

38. Апогей брейнрота: Бомбардиро Крокодило и другие боевые ИИ-животные захватили соцсети [Электронный ресурс] // daily.afisha.ru. URL: https://daily.afisha.ru/infoporn/29087-apogey-breynrota-bombardino-krokodilo-i-drugie-boevye-ii-zhivotnye-zahvatili-socseti/ (дата обращения: 31.07.2025).

39. Кудрявый метод: Стивен Пинкер — о том, как мир становится безопаснее [Электронный ресурс] // daily.afisha.ru. URL:

https://daily.afisha.ru/brain/17784-kudryavyy-metod-stiven-pinker-o-tom-kak-mir-stanovitsya-bezopasnee/ (дата обращения: 31.07.2025).

40. My life in Christ (2021) - праведный Иоанн Кронштадтский (Сергиев) [Электронный ресурс] // azbyka.ru. URL: https://azbyka.ru/otechnik/Ioann_Kronshtadtskij/my-life-in-christ/ (дата обращения: 31.07.2025).