УДК 334.02
DOI 10.22213/2618-9763-2025-2-82-89

К. А. Ямшанов, магистрант
И. Н. Тестова, кандидат технических наук, доцент
Ижевский государственный технический университет имени М. Т. Калашникова, Ижевск, Россия

СИСТЕМА УПРАВЛЕНИЯ ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ В СОЦИАЛЬНЫХ УЧРЕЖДЕНИЯХ

В исследовании представлена разработка концепции Единой системы управления персональными данными для социальных учреждений, ориентированной на обеспечение защиты персональных данных клиентов. Основное внимание уделено анализу современных киберугроз, таких как фишинговые атаки, вредоносное программное обеспечение и распределенные атаки типа «отказ в обслуживании», а также выявлению организационных уязвимостей, способствующих их реализации. Предложена архитектура централизованной системы, интегрируемой с существующими информационными платформами. Система реализует безопасный обмен данными с применением современных криптографических методов и строгих механизмов контроля доступа. Особое внимание уделено вопросам аутентификации операторов системы, для чего предусмотрены многофакторные механизмы проверки подлинности, в частности использование одноразовых паролей и уникальных токенов для электронной подписи. Отмечено, что разработанная система предоставляет пользователям комплекс инструментов для управления персональными данными, среди которых просмотр журналов доступа, настройка параметров обработки, возможность удаления или корректировки информации. Доступ к функционалу осуществляется через специализированные интерфейсы, включая мобильные приложения и веб-порталы. Для противодействия сетевым атакам предложен комплекс защитных мер, основанных на применении распределенных сетей доставки контента и алгоритмов машинного обучения для анализа сетевого трафика. Проведена комплексная оценка рисков, связанных с внедрением системы, учитывающая технические ограничения, кадровые вопросы и требования к надежности функционирования. Разработаны методические рекомендации по поэтапному внедрению системы, направленные на минимизацию организационной нагрузки. В завершении подчеркивается, что исследование позволяет существенно повысить уровень защиты персональных данных, обеспечить соответствие законодательным требованиям и укрепить доверие пользователей к социальным учреждениям.

Ключевые слова: защита данных; кибератаки; социальные учреждения; персональные данные; информационная безопасность; управление рисками.

Введение

В современном обществе социальные учреждения играют ключевую роль в обеспечении благополучия граждан, предоставляя разнообразные услуги в области здравоохранения, образования, социальной защиты. В процессе своей деятельности учреждения оперируют огромными объемами персональных данных клиентов, что делает их привлекательными целями для киберпреступников. Утечка или компрометация такой информации может привести к серьезным последствиям как для отдельных лиц, так и для общества в целом, включая финансовые потери, усиление телефонного мошенничества, ущерб репутации, штрафы в связи с нарушением законодательства в области защиты данных.

Актуальность создания организационной системы, включающей структуру управления, способы сотрудничества между подразделениями и информационные технологии, для обеспечения безопасности информации клиентов в социальных организациях определяется рядом причин:

1) Рост числа кибератак. В последние годы наблюдается увеличение количества и сложности информационных атак на различные организации, включая социальные учреждения. Злоумышленники используют разнообразные методы и инструменты для получения несанкционированного доступа к конфиденциальной информации, что требует от социальных учреждений постоянного совершенствования своих защитных мер[1].

2) Требования законодательства. В большинстве стран, включая Россию, действуют строгие законодательные нормы, регулирующие обработку и защиту персональных данных. Социальные учреждения обязаны соблюдать эти требования, чтобы избежать штрафов и других юридических последствий. Разработка и вне-

[1] Путин заявил о росте числа кибератак на отечественную цифровую инфраструктуру // Российская газета. 2025. URL: https://rg.ru/2025/02/27/putin-zaiavil-o-roste-chisla-kiberatak-na-otechestvennuiu-cifrovuiu-infrastrukturu.html (дата обращения: 01.03.2025).

дрение организационной системы защиты данных позволяет учреждениям соответствовать законодательным стандартам и обеспечивать надлежащий уровень конфиденциальности информации[1].

3) Доверие клиентов. Эффективная система защиты данных способствует повышению доверия клиентов к социальным учреждениям. В условиях, когда утечки данных становятся все более распространенными, клиенты ценят и выбирают те организации, которые могут гарантировать сохранность их личной информации. Это способствует укреплению репутации учреждения и его конкурентоспособности на рынке [1].

4) Сложность управления данными. Социальные учреждения обрабатывают большие объемы информации, которые поступают из различных источников и хранятся в разных системах. Управление такими данными и обеспечение их защиты представляет собой сложную задачу, требующую разработки комплексной организационной системы, которая бы учитывала все аспекты обработки и хранения информации [2].

Таким образом, разработка системы, направленной на защиту персональных данных клиентов в социальных учреждениях, является актуальной и важной задачей, которая требует особого внимания.

Цель исследования – разработать организационную систему защиты персональных данных клиентов в социальных учреждениях, опираясь на теоретические методы, нормативно-законодательную базу и практический опыт в области информационной безопасности.

Анализ видов кибератак и организационных факторов риска

Рассмотрим наиболее популярные виды кибератак на информационную систему социальных учреждений. Согласно источнику от *Kaspersky*, среди наиболее популярных видов кибератак на различные учреждения, включая социальные, можно выделить следующие [3]:

1) Фишинговые атаки: злоумышленники рассылают поддельные электронные письма или сообщения, которые выглядят как уведомления от надежных источников. Цель – убедить получателя раскрыть конфиденциальную информацию, такую как пароли или данные банковских карт.

2) Атаки с использованием вредоносного программного обеспечения: загрузка вирусов, троянов, шпионских программ и других вредоносных приложений, которые могут украсть данные, повредить системы или предоставить злоумышленникам удаленный доступ к компьютеру. Злоумышленники активно используют известные уязвимости в программном обеспечении и эксплойты – уязвимости программного обеспечения, позволяющие обходить меры защиты информационных систем или воздействовать на них, например, остановкой работы системы.

3) *DDoS*-атаки (*Distributed Denial of Service* – распределенная атака типа *отказ в обслуживании*): целью таких атак является перегрузка серверов и сетей, что делает услуги, сайты, приложения недоступными для пользователей.

Эти виды атак представляют серьезную угрозу для социальных учреждений, поскольку они могут привести к утечке конфиденциальных данных, нарушению работы сервисов и финансовым потерям.

Для формирования организационной структуры, позволяющей защититься от данных типов кибератак, необходимо определить факторы, позволяющие кибератаке случиться, и повлиять на учреждения, а также рассмотрим основные способы защиты, анализ которых позволит достичь цели исследования.

1. *Фишинговые атаки*. В современных учреждениях есть ряд серьезных организационных проблем, которые могут привести к успешному осуществлению атаки. Согласно исследованиям, средняя успешность обнаружения фишинговых схем составляет всего 65 %, что указывает на существенные пробелы в системах информационной безопасности организаций [4]. К ключевым организационным факторам риска относятся недостаточная эффективность программ обучения персонала, задержки в реагировании на инциденты безопасности и отсутствие четких протоколов действий при обнаружении подозрительной активности.

Человеческий фактор играет значительную роль в реализации рисков фишинговых атак. Личностные характеристики сотрудников, такие как экстраверсия, доверчивость и импульсивность при работе с веб-ресурсами, существенно влияют на уязвимость организации. Системные недочеты, включая слабую техническую защиту от фишинговых ссылок и недостаточный контроль за всплывающими окнами браузера, в сочетании с управленческими проблемами, такими как неэффективное распределение ответст-

[1] Основные нормативные правовые акты в области персональных данных // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). 2022. URL: https://54.rkn.gov.ru/directions/protection/p32048/p32050/ (дата обращения: 03.03.2025).

венности за кибербезопасность, создают благоприятную среду для успешного проведения атаки.

2. *Атаки с использованием вредоносного программного обеспечения* (*ПО*). Организационные недочеты и факторы, способствующие успешным атакам с использованием вредоносного программного обеспечения, включают недостаточную подготовку персонала, слабую подготовку процессов кибербезопасности и отсутствие эффективных механизмов реагирования на инциденты. Согласно исследованиям, проведенным компанией *Group-IB*, в 74 % российских банков в 2018 г. отсутствовала должная подготовка к хакерским атакам. У одной третьей финансовых учреждений были выявлены заражения вредоносными программами, а у половины – следы ранее совершенных атак. Серьезные недостатки наблюдались в управлении сетевыми ресурсами: у 64 % организаций на согласование действий по киберинцидентам между подразделениями уходило более четырех часов, что значительно превышает нормативное время в один час. Это свидетельствует о низкой оперативности и несогласованности в действиях внутренних подразделений, что делает организации более уязвимыми для атак.

Кроме того, недостаточная осведомленность сотрудников в вопросах информационной безопасности и их халатность являются ключевыми факторами, способствующими успешному внедрению вредоносного ПО. Исследования *Positive Technologies* показали, что в 75 % банков сотрудники переходили по ссылкам в фишинговых письмах, а в 25 % случаев вводили свои учетные данные в ложные формы аутентификации. Более того, в 25 % организаций сотрудники запускали вредоносные вложения на своих компьютерах. Эти данные подчеркивают, что даже при наличии технических средств защиты человеческий фактор остается одной из главных уязвимостей, позволяющей злоумышленникам успешно внедрять вредоносное ПО и нарушать функционирование организации [5].

3. *DDoS-атаки* (распределенные атаки типа *отказ в обслуживании*) представляют собой одну из наиболее опасных киберугроз, способных парализовать работу учреждения. Успешность таких атак часто обусловлена техническими и организационными недостатками.

Во-первых, недостаточная пропускная способность сети и отсутствие резервных каналов связи делают организации уязвимыми к перегрузке трафика. Даже небольшая атака может привести к отказу сервисов, если инфраструктура не рассчитана на высокие нагрузки.

Во-вторых, слабая защита, включая отсутствие межсетевых экранов, систем обнаружения вторжений (*IDS*/*IPS*) и технологий распределения нагрузки (например, *CDN*), повышает риск успешной атаки.

Организационные недочеты также играют ключевую роль. Отсутствие регулярного мониторинга сетевой активности, своевременного обновления программного обеспечения и подготовки персонала в области кибербезопасности увеличивает возможность реализации уязвимостей. Неумение распознавать признаки атаки и задержки в реагировании усугубляют ситуацию. Кроме того, если не разработаны стратегии действий в случае возникновения проблем, это может привести к длительному простою и росту экономических потерь [6].

Основными факторами, влияющим на информационные технологии учреждения, являются человеческий фактор, отсутствие аудита используемых программно-аппаратных средств, игнорирование фундаментальных принципов защиты информации. Данные проблемы характерны для организаций, в которых отсутствует выделенный *IT*-отдел. Особенно это касается социальных учреждений, для которых найти ресурсы практически невозможно, а используемые программно-аппаратные средства декларированы свыше.

Согласно законодательству Российской Федерации, а именно Федеральному закону № 152-ФЗ «О персональных данных», ст. 19, организации, обрабатывающие персональные данные, обязаны обеспечивать их защиту от неправомерного доступа, утечек и иных нарушений[1]. Для этого требуется внедрение организационных и технических мер, таких как разработка регламентов, обучение сотрудников, использование шифрования и регулярный аудит систем. Уровень защиты должен соответствовать возможным угрозам, что предполагает оценку рисков и выбор адекватных мер предостережения. В случае утечки данных оператор обязан уведомить Роскомнадзор и, при необходимости, субъекта данных, а также устранить последствия инцидента.

Тем не менее, рост числа утечек и недобросовестное отношение организаций к обработке данных клиентов подчеркивают необходимость изменения управления данными. Это требует ужесточения контроля, расширения правовых норм и внедрения четких стандартов взаимодействия с информацией, включая регулярный

[1] Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ // КонсультантПлюс : справ.-правовая система. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 01.03.2025).

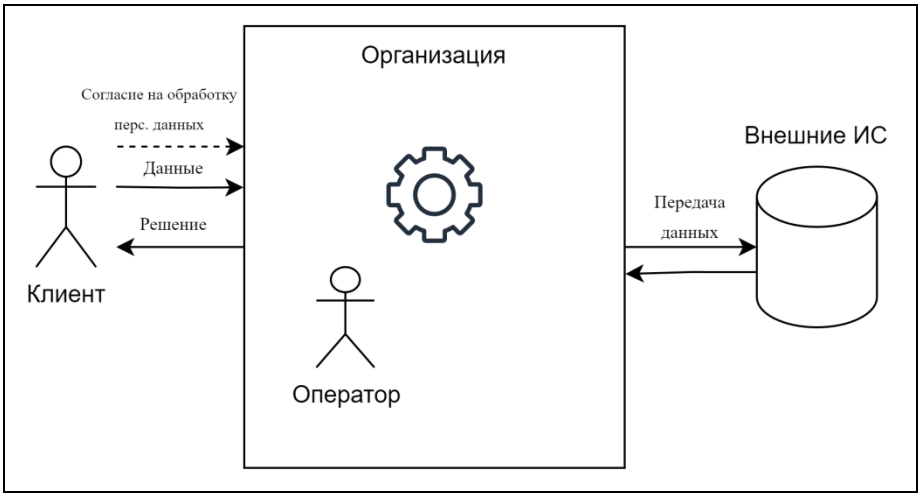
мониторинг, повышение прозрачности процессов и усиление ответственности за нарушения. Такие меры помогут минимизировать риски, повысить доверие граждан и обеспечить надежную защиту персональных данных в цифровую эпоху.

Описание Единой системы управления персональными данными

Решением проблемы может стать создание Единой системы управления персональными данными (далее ЕСУПД), подчиняющейся министерству цифрового развития, связи и массовых коммуникаций. В задачи данной системы входит создание нормативной базы и программно-аппаратных средств в области обеспечения безопасности персональных данных.

Разработка системы в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» сталкивается с рядом ограничений. Прежде всего, необходимо учитывать требования по обеспечению конфиденциальности, целостности и доступности информации, что предполагает использование современных криптографических методов и средств контроля доступа. Кроме того, закон обязывает организации проводить регулярную оценку уровня защищенности персональных данных, что накладывает дополнительные требования к ресурсам и компетенциям специалистов, ответственных за информационную безопасность. Важно учитывать необходимость минимизации объема собираемых персональных данных и сроков их хранения, что может потребовать пересмотра бизнес-процессов и практик работы с информацией в социальных учреждениях[1].

Рассмотрим процессы использования информационных систем в организациях. Социальные учреждения используют различные информационные системы (ИС), работающие с персональными данным, например Единая государственная информационная система социального обеспечения (ЕГИССО) или Медицинские информационные системы (МИС). В соответствии с законодательством, перед тем как начать обработку персональных данных, организации должны получить согласие клиента. Только после этого они имеют право передавать и обрабатывать информацию в соответствующих ИС. В процессе передачи и хранения данных должны использоваться защищенные каналы связи и современные алгоритмы шифрования данных. В случае запрета клиента на использование данных или при истечении срока хранения данные должны уничтожаться в соответствии с установленными процедурами. Иллюстрация процессов указана на рис. 1.



Источник: выполнен авторами.

Рис. 1. Схема процесса передачи персональных данных в организации

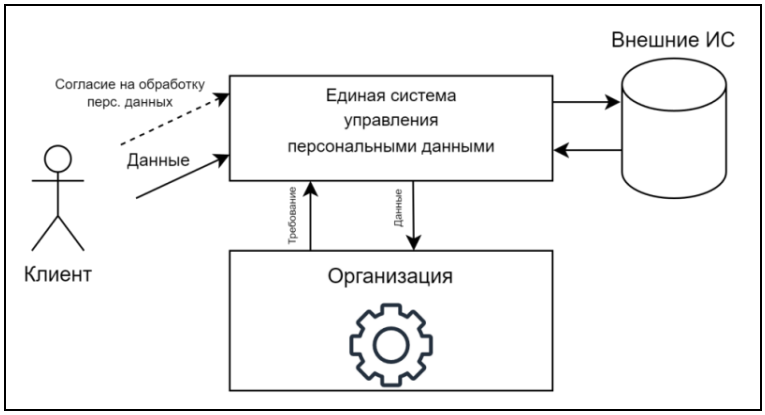
Fig. 1. The scheme of the personal data transfer process in the organization

Наиболее уязвимыми местами являются: незнание клиента последствий передачи персональных данных, человеческий фактор оператора, включая саботаж, недостаточная защищенность каналов передачи данных, халатное отношение организации к работе с персональными данными, например, избыточность данных.

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // КонсультантПлюс : справ.-правовая система. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 01.03.2025).

Рассмотрим функции ЕСУПД. Система позволяет получать, добавлять, удалять, изменять персональные данные клиентов. Она не хранит данные, а взаимодействует с другими системами, которые специализированы под хранение определенных типов данных, например биометрических. Получение данных должно сопровождаться согласием клиента, необходимостью организации в данных, записью в журнал момента взаимодействия с данными, их надежное шифрование в процессе передачи. Внедрение в реальные процессы использования системы должно накладывать ограничения на текущую обработку данных клиентов. Если сейчас организации хранят персональные данные в собственных ИС, то с переходом на единую систему организация должна отказаться от этого и не сохранять информацию после завершения обработки. Нарушение этого правила, повлекшее утечку персональных данных клиентов, должно наказываться. Учитывая сложность или невозможность доработки, предлагается разработать сертификат использования единой системы, который служит гарантом безопасности персональных данных клиентов. Система должна предоставлять клиентам простые способы получения журнала использования их данных. Ими могут служить интернет-сервисы, включая мобильные приложения или сайты, услуга, предоставляемая через многофункциональный центр. Клиент имеет право ограничить использование своих персональных данных, полностью удалить их или внести изменения. В случае невозможности получить доступ к необходимым данными, организация может отказать или приостановить обслуживание. Чтобы ускорить процесс предоставления данных, организация может получить от клиента право передачи персональных данных в единую систему. После получения персональных данных в одном экземпляре они не подлежат сохранению. После завершения передачи этот экземпляр должен быть уничтожен. Согласие клиента на передачу персональных данных равносильно прямому предоставлению данных клиентом в единую систему через различные каналы взаимодействия, такие как интернет-сервисы, мобильные приложения, сайты, а также многофункциональные центры. После передачи данных, выдачи разрешения на доступ к данным организацией, формирования ее требований к данным она может продолжить представление услуги клиенту. Процесс работы с данными с использованием единой системы и прямую передачу данных от клиента в систему проиллюстрирован на рис. 2, с участием посредника – на рис. 3.

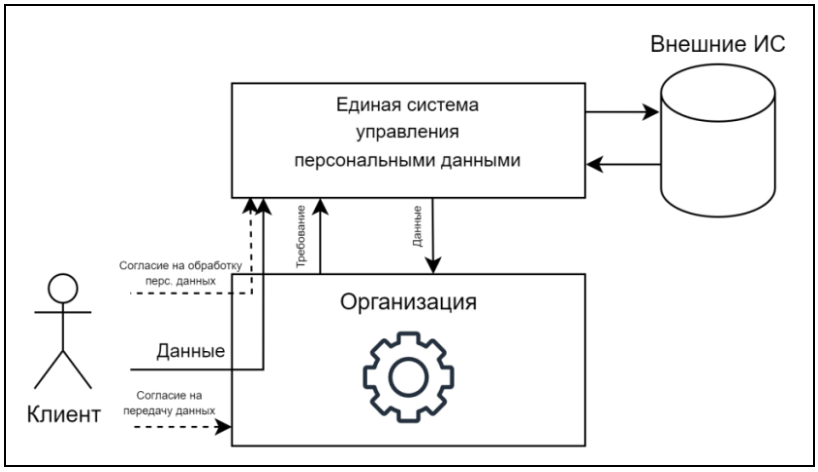
В контексте разработки системы противодействия кибератакам в социальных учреждениях ключевым аспектом является минимизация ущерба от *DDoS*-атак. Для этого необходимо внедрение комплексных мер: использование брандмауэров, сетей доставки контента (*CDN – Content Delivery Network*), регулирование трафика и укрепление сетевой инфраструктуры. Современные инструменты, такие как *Cloudflare* и *Akamai*, позволяют эффективно выявлять и блокировать вредоносный трафик. Интеграция методов машинного обучения и анализа поведения пользователей обеспечивает своевременное обнаружение атак, что снижает риски утечки персональных данных и повышает их безопасность [7].



Источник: выполнен авторами.

Рис. 2. Схема процесса передачи данных через ЕСУПД при прямом участии клиента

Fig. 2. The scheme of the data transfer process through a single personal data management system with the direct participation of the client



Источник: выполнен авторами.

Рис. 3. Схема процесса передачи данных через ЕСУПД при участии посредника

Fig. 3. The scheme of the data transfer process through a single personal data management system with the participation of an intermediary

Внедрение отдельной географически распределенной информационной системы позволит не только распределить риск между различными узлами, но и сократить расходы организаций на обслуживание частных информационных систем. Кроме того, такая система обеспечит делегирование ответственности за защиту персональных данных и информационной инфраструктуры, а также реализацию механизмов защиты от *DDoS*-атак. Это, в свою очередь, минимизирует ущерб от простоя организации в случае реализации атаки, обеспечивая непрерывность работы и сохранность критически важных данных.

Для предотвращения несанкционированного доступа к системе рекомендуется рассмотреть возможность внедрения многофакторной проверки подлинности, помимо использования сложного пароля [8]. Многофакторная аутентификация, такая как двухфакторная аутентификация с использованием одноразовых паролей, значительно повышает уровень безопасности [9]. Эти методы требуют от пользователя предоставления не только пароля, но и дополнительного фактора, например, кода из приложения или физического устройства, что усложняет задачу злоумышленникам, пытающимся получить доступ через фишинговые атаки. Оценивая важность единой системы, рекомендуется внедрение взаимной аутентификация с использованием устройств класса *SSCD* (*Secure signature creation device* – устройства безопасного формирования подписи), которые предотвращают атаки типа *человек посередине* и фишинг. Эти устройства обеспечивают криптографическую защиту и исключают возможность перехвата персональных данных, даже если злоумышленник узнал пароль.

Развитие единой системы должно сопровождаться оценкой рисков. Как отмечают некоторые авторы, государственные системы являются привлекательными объектами для кибератак, например за 2021 г. 29 % атак были направлены на госучреждения и социальные учреждения [10]. Таким образом важно реалистично оценивать риски перехода на ЕСУПД.

Реализация системы может сопровождаться следующими рисками: организационные проблемы, непреодолимые или сложнопреодолимые технические ограничения, недостаточная квалификация сотрудников [11]. Кроме того, выход из строя системы может заблокировать работу зависимых учреждений, что приведет к финансовым и репутационным потерям. При разработке системы необходимо учитывать технологические уязвимости в используемом программно-аппаратном обеспечении, риски при использовании зарубежных технологий, кадровые ограничения, стандарты информационной безопасности, правовые и регуляторные требования [12].

Интеграция с системой может требовать значительных ресурсов организаций: временных, человеческих, технологических. Поэтому важно разработать прозрачные процессы интеграции отдельных программно-аппаратных блоков и инструменты помощи, например консультации.

Выводы

Защита персональных данных клиентов имеет важное значение в процессах работы организации. Утечки данных негативно влияют на

клиентов, на их финансовое, моральное и физическое благополучие. В данной статье предложена Единая система управления персональными данными для социальных учреждений, направленная на решение этой актуальной проблемы.

Цель исследования – разработка организационной системы защиты персональных данных – достигнута за счет создания централизованной архитектуры, интегрируемой с существующими информационными платформами. Система включает современные криптографические методы, многофакторную аутентификацию, строгий контроль доступа и инструменты управления данными, что позволяет эффективно противостоять киберугрозам, таким как фишинг, вредоносное ПО и *DDoS*-атаки.

Внедрение ЕСУПД не только повысит уровень защиты данных и обеспечит соответствие законодательным требованиям, но и укрепит доверие клиентов к социальным учреждениям. Однако для успешной реализации системы необходимо учитывать выявленные риски, включая технические ограничения, кадровые вопросы и организационные сложности. Таким образом, предложенное решение представляет собой важный шаг в совершенствовании информационной безопасности и требует дальнейшей проработки механизмов внедрения.

Библиографические ссылки

1. Формирование методики оценки показателя цифрового доверия (digital trust) как индикатор качества информационных ресурсов государственного управления / И. П. Гладилина, В. В. Колесник, Ю. Н. Прохоров [и др.] // Экономика: вчера, сегодня, завтра. 2022. Т. 12, № 8А. С. 368–378. DOI: 10.34670/AR.2022.32.97.048. EDN: NSTNQA

2. *Гуров О. Н., Конькова (Кураева) Т. А., Новиков Р. Ю.* Использование больших данных в социальной науке – перспективы и ограничения // Искусственные общества. 2021. Т. 16. № 2. Порядков. номер 5. DOI: 10.18254/S207751800015213-3. EDN: AZWEIC

3. Предотвращение кибератак // Kaspersky. URL: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-prevent-cyberattacks (дата обращения: 26.02.2025).

4. *Нежельский А. Ю.* Разработка системы защиты персональных данных в организации // Актуальные исследования. 2024. № 23-1 (205). С. 35–38. EDN: XBCCXE

5. *Семеко Г. В.* Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. № 1. С. 77–96. DOI: 10.31249/snsn/2020.01.06. EDN: ANGCNJ

6. *Марцеленко С. А.* Оценка экономических последствий кибератак на региональные инфраструктуры // Актуальные проблемы современной экономики. 2024. № 8. С. 297–302. EDN: SHRIDZ

7. *Сулейменова Р. Д., Патутин В. В., Антонов И. В.* DDoS-атаки и способы защиты по их предотвращению // Наукосфера. 2023. № 5-2. С. 312–316. EDN: SOEPTH

8. *Близно Л. В., Евенко И. А., Мирная А. Н.* Система информационной безопасности на современном предприятии : монография. Ставрополь : Губерния, 2021. 102 с. ISBN: 978-5-6044710-8-1. EDN: IJPGQI

9. *Бочнев Н. А., Харисов А. Р.* Надежные методы аутентификации в государственных и корпоративных системах: принципы, технологии и перспективы // Вестник науки. 2024. № 12 (81). С. 642–649. EDN: MRBKBW

10. *Иванова Е. К., Иванова М. Р.* Риски кибератак и утраты персональных данных // Страховое право. 2021. № 4 (93). С. 70–74. EDN: VBQASO

11. *Островских Ж. В., Хохлова О. М., Рожкова А. К.* Информационная безопасность в системе национальной безопасности современной России в период пандемии COVID-19 // Сибирский юридический вестник. 2022. № 2 (97). С. 111–112. DOI: 10.26516/2071-8136.2022.2.105. EDN: TOXTAZ

12. *Масова О. А.* Риски и угрозы цифровой экономики // Инновации. Наука. Образование. 2022. № 61. С. 49–55. EDN: RFPHSY

Reference

1. Gladilina I.P., Kolesnik V.V., Prokhorov Yu.N., Talan M.V., Fokina A.N. [Formation of a methodology for assessing the digital trust indicator as an indicator of the quality of public administration information resources]. *Economics: yesterday, today, tomorrow*, 2022, vol. 12, no. 8A, pp. 368-378. (in Russ.). DOI: 10.34670/AR.2022.32.97.048. EDN: NSTNQA

2. Gurov O.N., Konkova T.A., Novikov R.Yu. [The use of big data in social science – prospects and limitations]. *Artificial societies*, 2021, vol. 16, no. 2. Serial number 5. (in Russ.). DOI: 10.18254/S207751800015213-3. EDN: AZWEIC

3. *Predotvrashchenie kiberatak* [Preventing cyber attacks]. *Kaspersky*. (in Russ.). Available at: https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-prevent-cyberattacks (accessed 26.02.2025).

4. Nezhel'skij A.Ju. [Development of a personal data protection system in an organization]. *Aktual'nye issledovanija*, 2024, no. 23-1 (205), pp. 35-38. (in Russ.). EDN: XBCCXE

5. Semeko G.V. [Information security in the financial sector: cybercrime and counteraction strategy]. *Social innovation and social sciences*, 2020, no. 1, pp. 77-96. (in Russ.). DOI: 10.31249/snsn/2020.01.06. EDN: ANGCNJ

6. Martselenko S.A. [Assessment of the economic impact of cyber attacks on regional infrastructures]. *Current problems of the modern economy*, 2024, no. 8, pp. 297-302. (in Russ.). EDN: SHRIDZ.

7. Suleimenova R.D., Patutin V.V., Antonov I.V. [DDoS attacks and protection measures to prevent them]. *The science Sphere*, 2023, no. 5-2, pp. 312-316. (in Russ.). EDN: SOEPTH

8. Blizno L.V., Evenko I.A., Mirnaya A.N. *Sistema informatsionnoi bezopasnosti na sovremennom predpriyatii : monografija* [Information security system in a modern enterprise, monograph]. Stavropol, Publ. house of Gubernia LLC, 2021, 102 p. (in Russ.). EDN: SOEPTH

9. Bochnev N.A., Kharisov A.R. [Reliable authentication methods in government and corporate systems: principles, technologies, and prospects]. *Bulletin of Science*, 2024, no. 12 (81), pp. 642-649. (in Russ.). EDN: MRBKBW

10. Ivanova E.K., Ivanova M.R. [Risks of cyber attacks and loss of personal data]. *Insurance law*, 2021, no. 4 (93), pp. 70-74. (in Russ.). EDN: VBQASO

11. Ostrovskikh Zh.V., Khokhlova O.M., Rozhkova A.K. [Information security in the national security system of modern Russia during the COVID-19 pandemic]. *Siberian Law Bulletin*, 2022, no. 2 (97), pp. 111-112. (in Russ.). DOI: 10.26516/2071-8136.2022.2.105. EDN: TOXTAZ

12. Masova O.A. [Risks and threats of the digital economy]. *Innovation. Science. Education*, 2022, no. 61, pp. 49-55. (in Russ.). EDN: RFPHSY

K. A. Yamshanov, Master's Degree Student
I. N. Testova, PhD in Engineering, Associate Professor
Kalashnikov Izhevsk State Technical University, Izhevsk, Russia

MANAGEMENT SYSTEM FOR THE PROTECTION OF PERSONAL DATA OF CLIENTS IN SOCIAL INSTITUTIONS

The study presents the development of the concept of a Unified Personal Data Management System for social institutions, focused on ensuring the protection of personal data of clients. The main focus is on analyzing modern cyber threats such as phishing attacks, malware, and distributed denial-of-service attacks, as well as identifying organizational vulnerabilities that contribute to their implementation. The architecture of a centralized system integrated with existing information platforms is proposed. The system implements secure data exchange using modern cryptographic methods and strict access control mechanisms. Special attention is paid to the issues of authentication of system operators, for which multifactor authentication mechanisms are provided, in particular, the use of one-time passwords and unique tokens for electronic signatures. The developed system provides users with a set of tools for managing personal data, including viewing access logs, configuring processing parameters, and the ability to delete or correct information. The functionality is accessed through specialized interfaces, including mobile applications and web portals. To counter network attacks, a set of protective measures based on the use of distributed content delivery networks and machine learning algorithms for analyzing network traffic is proposed. The work carried out a comprehensive assessment of the risks associated with the implementation of the system, taking into account technical limitations, personnel issues and requirements for operational reliability. Methodological recommendations have been developed for the phased implementation of the system, aimed at minimizing the organizational burden. The results of the study make it possible to significantly increase the level of personal data protection, ensure compliance with legal requirements and strengthen users' trust in social institutions.

Keywords: data protection; cyber-attacks; social institutions; personal data; information security; risk management.

Получена: 26.03.2025
ГРНТИ 82.15.09

Образец цитирования

Ямшанов К. А., Тестова И. Н. Система управления защитой персональных данных клиентов в социальных учреждениях // Социально-экономическое управление: теория и практика. 2025. Т. 21, № 2. С. 82–89. DOI: 10.22213/2618-9763-2025-2-82-89

For Citation

Yamshanov K.A., Testova I.N. [Management system for the protection of personal data of clients in social institutions]. *Social'no-ekonomiceskoe upravlenie: teoria i praktika*, 2025, vol. 21, no. 2, pp. 82-89 (in Russ.). DOI: 10.22213/2618-9763-2025-2-82-89