Право и политика
Правильная ссылка на статью:
Новиков П.А. Совершенствования механизма защиты специальной категории персональных данных // Право и политика. 2025. № 2. С.65-77. DOI: 10.7256/2454-0706.2025.2.73265 EDN: DITQXW URL: https://nbpublish.com/library_read_article.php?id=73265

Совершенствования механизма защиты специальной категории персональных данных

Новиков Петр Александрович

ORCID: 0009-0009-5133-811X

аспирант; ЧОУ ВО "Санкт-Петербургский университет технологий управления и экономики"

190020, Россия, г. Санкт-Петербург, Лермонтовский пр-т, д.44, Лит.А

petnovikov.81@mail.ru

Статья из рубрики "Человек и государство"

DOI:

10.7256/2454-0706.2025.2.73265

EDN:

DITQXW

Дата направления статьи в редакцию:

06-02-2025

Дата публикации:

04-03-2025

Аннотация: С постоянным ростом цифровизации и использовании всевозможных электронных платформ, любые данные оставляют за собой следы информации, которые касаются как общедоступных, так и специальных категорий данных. В статье рассматриваются проблемы защиты специальных категорий персональных данных в условиях цифровизации и растущих угроз безопасности информации. Анализируется нормативно-правовая база Российской Федерации, а также международные стандарты, такие как Общий регламент по защите данных, с целью выявления недостатков в защите данных высокой чувствительности, включающих сведения о здоровье, биометрии, политических и религиозных убеждениях. Предложен комплексный подход к совершенствованию механизма защиты этих данных, включающий технические и организационные меры, усиление правового регулирования, внедрение технологий

шифрования, анонимизации, биометрической аутентификации и системы оценки рисков. Описаны пути повышения роли Роскомнадзора в обеспечении безопасности данных, в том числе через расширение его полномочий и ужесточение ответственности за нарушения. Методы исследования направлены на целостное и интегративное понимание проблемы, поэтому в ходе исследования был проведен анализ нормативно-правовых актов и существующих механизмов защиты специальных категорий данных, исследование технологических аспектов, используемых для обеспечения безопасности, а также оценка потенциальных угроз и слабых мест в процессе их обработки. Научная новизна заключается в разработке и внедрении инновационных подходов и технологий, которые обеспечивают более высокий уровень безопасности и конфиденциальности специфической информации, относящейся к личной жизни граждан. В условиях стремительного развития цифровых технологий и увеличения объемов обрабатываемых данных, защита персональных данных становится критически важной задачей для предотвращения неправомерного доступа, использования и распространения информации. Одним из ключевых аспектов научной новизны является адаптация существующих правовых норм к современным технологическим вызовам, что включает в себя разработку новых методов идентификации и аутентификации пользователей. Выводы исследования направлены на разработку рекомендаций для улучшения защиты конфиденциальной информации, способствующих адаптации национального законодательства к международным требованиям и эффективному противодействию угрозам безопасности в сфере персональных данных.

Ключевые слова:

персональные данные, специальная категория данных, шифрование данных, биометрическая аутентификация, правовое регулирование, анонимизация данных, конфиденциальная информация, информационная безопасность, кибербезопасность, технологии защиты данных

Специальные категории персональных данных в Российской Федерации включают сведения, которые требуют повышенной защиты ввиду их чувствительности и возможного риска для прав и свобод граждан при неправомерном использовании [1]. В соответствии с Федеральным законом «О персональных данных» (ФЗ - №152), к таким данным относятся информация о расовой и национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, а также личные данные, связанные с интимной жизнью граждан [2]. Поскольку обработка этих данных сопряжена с высокими требованиями безопасности, их сбор, хранение и обработка допускаются только при соблюдении специальных условий, таких как наличие письменного согласия субъекта данных или правовые основания, установленные законодательством.

Актуальность совершенствования механизмов защиты этих данных обусловлена быстрым развитием технологий, ростом объёма обрабатываемых данных и необходимостью приведения национальных стандартов в соответствие с международными требованиями, такими как Общий регламент по защите данных (GDPR)[3]. Эти факторы создают новые вызовы для правового регулирования, технической защиты и организационных мер, что требует комплексного подхода к обеспечению безопасности [4].

Цель настоящей статьи — анализ существующих правовых, технических и

организационных методов защиты специальных категорий персональных данных и разработка рекомендаций по их совершенствованию. Основные направления включают:

1. Усиление правового регулирования: обновление законодательства, расширение полномочий надзорных органов и введение дополнительных мер ответственности для улучшения контроля и защиты [5].

2. Применение современных технологий: внедрение шифрования, анонимизации, псевдонимизации, а также биометрической аутентификации для ограничения несанкционированного доступа [6].

3. Организационные меры и обучение персонала: разработка стандартов работы с данными, регулярное обучение сотрудников, работающих с чувствительной информацией [7].

4. Повышение осведомленности субъектов данных: информирование граждан о правах и механизмах защиты персональных данных, что повышает уровень правовой и информационной безопасности [8].

5. Развитие информационных систем и анализ рисков: регулярная оценка уязвимостей, моделирование инцидентов кибербезопасности и внедрение протоколов реагирования на угрозы [9].

Ужесточение ответственности за нарушения в обработке и хранении данных специальной категории представляет собой одно из ключевых направлений для повышения уровня защищенности персональных данных в Российской Федерации. Специальные категории персональных данных включают в себя особо чувствительную информацию, такую как расовая и этническая принадлежность, политические взгляды, религиозные убеждения, состояние здоровья и аспекты интимной жизни. В целях минимизации рисков несанкционированного доступа и утечек информации необходимо внедрить более строгие меры как административной, так и уголовной ответственности, что повысит уровень соблюдения нормативных требований и будет способствовать усилению правовой защиты.

В рамках административной ответственности целесообразно дифференцировать наказания в зависимости от характера и степени нарушения. К примеру, компании, допустившие утечку данных, могут быть подвергнуты крупным штрафам, рассчитываемым на основе их годового оборота, что будет стимулировать бизнес к внедрению более строгих стандартов безопасности. Кроме того, предлагается ввести фиксированные штрафы за несоблюдение обязательных процедур обработки данных, таких как регулярные аудиты, защита каналов передачи, шифрование и контроль доступа. Подобные меры позволят обеспечить постоянный мониторинг и контроль за состоянием защищенности информационных систем, что особенно важно для предотвращения повторных инцидентов.

Серьезные нарушения, такие как систематическое пренебрежение требованиями законодательства, могут стать основанием для введения временных или постоянных ограничений на обработку персональных данных. Например, Роскомнадзор может применять меры временного приостановления деятельности компаний, неоднократно допустивших утечки данных, до тех пор, пока организация не устранит выявленные недостатки. Также предусматривается возможность проведения обязательного аудита со стороны надзорного органа, что позволит систематизировать и контролировать

внедрение необходимых мер защиты.

Помимо административных мер, важно усилить уголовную ответственность за неправомерные действия с персональными данными. Введение новых составов преступлений, связанных с несанкционированным доступом к специальным категориям данных, позволит правоохранительным органам эффективно бороться с попытками неправомерного использования личной информации. Так, умышленные нарушения, такие как продажа данных третьим лицам, могут караться лишением свободы, а серьезная халатность, приведшая к утечке информации, — принудительными работами или штрафами для должностных лиц. Для лиц, неоднократно нарушающих закон, возможно введение запрета на занятие должностей, связанных с обработкой данных, на срок до 10 лет, что существенно ограничит их доступ к информации.

Для юридических лиц, допустивших крупные утечки данных, могут быть предусмотрены дополнительные меры ответственности, такие как конфискация имущества в пользу государства или компенсационного фонда, направленного на поддержку пострадавших от утечки данных. В случаях систематических и многократных нарушений возможно принудительное прекращение деятельности компании через судебное решение, что позволит предотвратить дальнейшие нарушения прав субъектов данных и усилить превентивный эффект законодательства [10].

Одновременно с ужесточением мер ответственности необходимо расширить полномочия надзорных органов, таких как Роскомнадзор, в области контроля за соблюдением требований по защите данных. В частности, это включает в себя возможность проведения внеплановых проверок у организаций, которые были ранее замечены в нарушениях. Для повышения уровня контроля также предлагается ужесточить требования к хранению документации, связанной с обработкой данных, сроком не менее пяти лет. Это позволит более эффективно осуществлять проверки на соответствие требованиям законодательства и отслеживать историю обработки данных, что будет способствовать повышению прозрачности процессов.

Особое внимание необходимо уделить правам самих субъектов данных. Введение компенсаций для пострадавших от утечек данных за счет специального фонда, формируемого из административных штрафов, повысит уровень социальной ответственности и поможет пострадавшим гражданам компенсировать моральный ущерб. Кроме того, расширение прав субъектов данных на исковые требования, включая возможность подачи коллективных исков в случаях массовых утечек, усилит их правовую защиту и станет дополнительным стимулом для компаний соблюдать требования информационной безопасности.

Таким образом, предлагаемые меры по усилению ответственности за нарушения в сфере защиты специальных категорий персональных данных представляют собой комплексный подход, включающий административные и уголовные санкции, расширение прав субъектов данных и усиление надзорных функций государственных органов. Реализация этих мер позволит значительно снизить риски неправомерного обращения с персональными данными, повысит уровень защиты прав граждан и создаст более устойчивую и надежную систему обеспечения информационной безопасности [11].

Для повышения защиты специальных категорий персональных данных в России необходимо значительно расширить полномочия Роскомнадзора в сфере контроля и аудита. Специальные категории данных включают чувствительную информацию, такую как сведения о здоровье, политические и религиозные убеждения, которые требуют

повышенной степени защиты. Роскомнадзор, являясь основным органом, ответственным за соблюдение норм в этой области, должен получить дополнительные возможности для обеспечения безопасности этих данных.

Во-первых, расширение полномочий Роскомнадзора по проведению проверок и аудитов станет важным шагом к усилению контроля над соблюдением требований. Введение регулярных плановых проверок для всех организаций, работающих со специальными категориями данных, позволит создать систематизированный подход к контролю. Основными критериями для плановых проверок могут быть размер компании, объем обрабатываемых данных и уровень потенциального риска. Одновременно Роскомнадзор должен получить право на проведение внеплановых проверок при получении жалоб от субъектов данных или информации от других госорганов о возможных нарушениях, что обеспечит гибкость и оперативность реагирования на угрозы.

Во-вторых, важным направлением усиления деятельности Роскомнадзора является модернизация инструментов и технологий для проведения проверок. Современные аналитические системы и технологии искусственного интеллекта могут применяться для автоматического мониторинга деятельности организаций, что позволит эффективно выявлять отклонения в обработке данных и минимизировать необходимость выездных проверок. Создание автоматизированных систем мониторинга также может включать обработку жалоб субъектов данных и анализ отчетности компаний. Интеграция с базами данных других государственных органов, таких как МВД, ФНС и ФСБ, позволит Роскомнадзору оперативно координировать действия с целью быстрого и полного выявления и пресечения нарушений.

Также для успешного выполнения функций Роскомнадзору требуется повышение финансирования и кадровой обеспеченности. Значительные инвестиции в техническую базу — закупка серверного оборудования, лицензий на аналитические программы и средств автоматизированного контроля — помогут создать условия для эффективного контроля [12]. Также важно выделить финансирование на образовательные программы в области кибербезопасности, что обеспечит высокий уровень квалификации сотрудников, работающих с современными угрозами. Расширение штата Роскомнадзора, особенно в регионах, позволит обеспечить более плотное покрытие территорий и оперативное реагирование на инциденты. Регулярное обучение специалистов новым методам аудита, анализа систем безопасности и выявления уязвимостей будет способствовать повышению качества контроля и предотвращению утечек.

Помимо усиления контроля и повышения квалификации сотрудников, крайне важно повысить уровень прозрачности деятельности Роскомнадзора. Публикация ежеквартальных и ежегодных отчетов о результатах проверок и выявленных нарушениях позволит гражданам и организациям оценить уровень соблюдения норм безопасности различными компаниями. Информация об инцидентах, связанных с утечкой данных, и предпринятых мерах также будет способствовать повышению доверия со стороны общества.

Кроме того, Роскомнадзор должен информировать субъектов данных о любых инцидентах, связанных с утечкой их персональной информации, а также о возможных рисках и мерах защиты. Введение обязательного уведомления субъектов данных об инцидентах позволит им своевременно предпринимать меры для защиты своих прав. Создание горячей линии и онлайн-сервиса для жалоб также позволит гражданам оперативно сообщать о возможных нарушениях, что усилит обратную связь и сделает Роскомнадзор более доступным для граждан [13].

Приведение российского законодательства о защите персональных данных в соответствие с международными стандартами требует комплексного подхода, направленного на обеспечение более высокой защиты данных и упрощение условий для международного сотрудничества. Переход к новым стандартам позволяет учитывать современные вызовы и специфику цифровой среды, особенно при работе со специальными категориями персональных данных.

Одной из ключевых мер актуализации законодательства является уточнение условий обработки данных специальной категории. Необходимо законодательно закрепить цели, при которых возможна обработка таких данных, например, в случае защиты жизненно важных интересов субъекта или для соблюдения правовых требований. Обязательное получение явного согласия субъектов для обработки данных также должно быть частью этой нормы. Согласие должно оформляться в ясной и доступной форме, что позволит гражданам чётко понимать цели и типы обрабатываемых данных.

Закрепление и расширение прав субъектов данных также является приоритетом. В частности, важно закрепить право субъекта на доступ к информации о своих данных и условиях их обработки. Кроме того, прозрачность и доступность информации должны стать обязательными для операторов данных, что включает обеспечение понятного изложения целей и сроков обработки, а также прав субъектов. Ещё один важный элемент — это право на отказ от автоматизированных решений и профилирования, особенно если такие процессы могут серьёзно повлиять на интересы субъекта.

Не менее значимой частью реформы являются изменения в подходах к обработке данных. Здесь актуальным является внедрение обязательных процедур защиты данных, таких как оценка воздействия на защиту данных (DPIA) для операций с высоким уровнем риска. Назначение ответственного за защиту данных (DPO) также становится необходимым, особенно в крупных организациях, работающих с персональными данными. Это поможет централизовать и усилить контроль за соблюдением требований в области защиты информации [14].

Критическим аспектом является внедрение мер по реагированию на утечки данных. Компании должны быть обязаны уведомлять как надзорные органы, так и субъекта данных о фактах утечек, особенно если они могут угрожать правам и безопасности личности. Уведомление должно производиться незамедлительно, но не позднее 72 часов после инцидента. Также необходимо предусмотреть разработку протоколов реагирования на утечки, включая планы по восстановлению работы и минимизации возможного ущерба.

Повышение правовой культуры и осведомленности субъектов данных о своих правах должно стать важным элементом политики в области защиты данных. Создание образовательных ресурсов и проведение разъяснительных кампаний, инициированных Роскомнадзором, может повысить осведомлённость населения о правилах обработки данных [15]. Дополнительное внимание также должно быть уделено поддержке малых и средних предприятий, которым можно предоставить консультации и обучающие программы, чтобы облегчить им соблюдение требований законодательства.

Внедрение современных технологий защиты данных является важнейшим компонентом в обеспечении безопасности информации, особенно для данных специальной категории. Одной из основных технологий защиты является обязательное шифрование, которое выполняет функцию защиты данных как при их передаче, так и при хранении,

минимизируя риски их несанкционированного доступа.

При передаче данных по сети шифрование end-to-end обеспечивает высокий уровень безопасности, так как данные шифруются на стороне отправителя и расшифровываются только на стороне получателя. Это делает их недоступными даже в случае перехвата. Широкое использование протокола TLS, в частности для защищённых HTTPS-соединений, создаёт надёжный канал для передачи данных, гарантируя их безопасность на всех уровнях взаимодействия между клиентом и сервером. Дополнительно, VPN-технологии обеспечивают защиту данных в открытых сетях, а шифрование коммуникаций между приложениями и базами данных защищает взаимодействие на внутренних уровнях системы [16].

Шифрование данных при хранении выполняет функции защиты как на уровне всего носителя, так и на уровне отдельных файлов. Полное шифрование дисков предотвращает доступ к данным при физическом компрометации носителя, например, при утрате или краже устройства. На уровне файлов шифрование защищает структурированные и неструктурированные данные от как внешних, так и внутренних угроз. В случае использования облачных хранилищ стороннее шифрование и клиентское управление ключами обеспечивают дополнительный уровень безопасности, позволяя компаниям сохранять контроль над доступом к данным и их защите, даже если сам провайдер облачного сервиса сталкивается с утечкой.

Эффективное управление ключами, в свою очередь, играет критическую роль в безопасности шифрования. Системы управления ключами (KMS) позволяют централизованно контролировать процесс генерации, хранения и уничтожения ключей, что обеспечивает их безопасность и прозрачность. Разделение ролей и обязанностей при управлении ключами ограничивает доступ к ним и снижает вероятность несанкционированного использования. Регулярная ротация ключей также является важной практикой, которая позволяет своевременно минимизировать риски, связанные с компрометацией ключей, и поддерживает высокий уровень безопасности системы. Сохранение истории всех операций с ключами позволяет не только контролировать их использование, но и проводить анализ в случае выявления инцидентов безопасности, что способствует общей прозрачности и управляемости процесса.

Современные подходы к защите персональных данных всё чаще включают использование технологий анонимизации и псевдонимизации, которые становятся важными инструментами обеспечения конфиденциальности. Эти методы дают возможность обезличить данные, при этом сохраняя их ценность для аналитики и других целей, требующих обработки больших объёмов информации [17]. Благодаря анонимизации и псевдонимизации снижаются риски, связанные с несанкционированным доступом, а организации получают возможность работать с данными, не нарушая законодательных требований и обеспечивая защиту личной информации.

Анонимизация данных представляет собой процесс, при котором удаляется возможность идентификации субъекта, что делает такие данные полностью обезличенными. После анонимизации данные теряют свой персональный характер, а их обработка становится более безопасной и в некоторых случаях выводится из-под действия законов о защите данных, таких как GDPR. Среди методов анонимизации можно выделить удаление идентификаторов, агрегацию данных, обфускацию, случайное размывание и канонимизацию. Например, в здравоохранении анонимизация позволяет проводить статистические исследования, не раскрывая личности пациентов, что делает её востребованной для научных целей. Основное преимущество анонимизации — высокая

степень защиты данных, даже в случае утечки. Однако анонимизация необратима, что исключает возможность восстановления исходной информации [18].

В отличие от анонимизации, псевдонимизация позволяет заменить идентификаторы данных специальными метками или кодами, сохраняя возможность восстановления исходной информации при наличии ключа. Применяя токены, кодирование данных или хеширование с секретным ключом, организации могут управлять данными, не нарушая конфиденциальности. Псевдонимизация позволяет использовать данные в аналитических целях, сохраняя доступ к личной информации только при необходимости. Это особенно важно в медицинских и аналитических системах, где доступ к исходным данным может понадобиться для повторного анализа или оказания услуг. Например, в маркетинговых исследованиях псевдонимизация позволяет собирать информацию о клиентах для анализа их поведения и предпочтений, при этом минимизируя риски раскрытия личности.

Каждая из технологий имеет свои преимущества и ограничения. Анонимизация обеспечивает более высокий уровень защиты, поскольку полностью исключает возможность идентификации, что делает её идеальной для обработки больших массивов данных, где идентификация субъекта не требуется. Псевдонимизация, в свою очередь, предоставляет гибкость использования данных, что полезно в ситуациях, когда требуется возможность восстановления идентифицирующих данных. Однако псевдонимизация требует надёжного управления ключами и строгого контроля за доступом к дополнительной информации, поскольку утечка ключей может привести к компрометации данных.

Применение анонимизации и псевдонимизации в информационных системах особенно актуально для таких сфер, как здравоохранение, аналитика и управление большими данными. В здравоохранении анонимизация позволяет безопасно использовать данные пациентов для исследования, а псевдонимизация позволяет обмениваться данными между медицинскими учреждениями без раскрытия личности пациентов. В аналитических системах компании могут безопасно анализировать пользовательские данные, используя анонимизацию или псевдонимизацию, что обеспечивает защиту конфиденциальности и позволяет использовать данные для улучшения качества услуг. В области больших данных анонимизация и псевдонимизация помогают обрабатывать массивы информации с учётом требований к защите конфиденциальности, а также позволяют безопасно использовать облачные технологии, исключая прямой доступ к персональным данным пользователей.

Биометрическая аутентификация стала одним из наиболее эффективных методов обеспечения безопасности доступа к данным и системам их обработки. Эта технология опирается на уникальные физиологические и поведенческие характеристики пользователя, такие как отпечатки пальцев, черты лица или голос, которые трудно подделать или передать. Благодаря этому биометрия надёжно защищает информацию от несанкционированного доступа.

Принципы биометрической аутентификации включают использование как физиологических, так и поведенческих данных. Среди физиологических методов популярны сканирование отпечатков пальцев, распознавание лица, радужной оболочки глаза и голосовых характеристик. Эти методы позволяют идентифицировать пользователя с высокой точностью и надёжностью. Поведенческие параметры, такие как анализ подписи или паттерны ввода текста, также используются для повышения уровня безопасности, однако в меньшей степени, чем физиологические показатели [19].

Главные преимущества биометрической аутентификации связаны с высоким уровнем безопасности и удобством использования. Биометрические данные сложно подделать или украсть, что выгодно отличает их от традиционных паролей или PIN-кодов. К тому же биометрические данные всегда «под рукой» — пользователю не нужно запоминать длинные пароли или использовать дополнительные устройства для подтверждения личности. Это сокращает время на аутентификацию и снижает вероятность социальных атак, таких как фишинг или манипуляции с помощью социальной инженерии.

Применение биометрической аутентификации на практике становится всё более распространённым. В корпоративной среде биометрия защищает доступ к конфиденциальным данным и рабочим устройствам, гарантируя, что только авторизованные сотрудники имеют доступ к информации. В финансовом секторе биометрия обеспечивает безопасность транзакций и доступ к банковским приложениям, снижая риски мошенничества. В медицинских учреждениях она ограничивает доступ к медицинским записям и контролирует рабочее время сотрудников. Государственные учреждения используют биометрию для допуска в зоны с высокой степенью безопасности и в электронных удостоверениях личности, что упрощает идентификацию граждан и повышает общую безопасность.

Развитие информационных систем и анализ рисков — это важные составляющие для повышения уровня безопасности персональных данных в условиях постоянно меняющихся киберугроз. Эффективная защита требует не только создания надёжных систем, но и их регулярного совершенствования, которое предполагает внедрение многоуровневых мер, позволяющих минимизировать риски и оперативно реагировать на возникающие угрозы.

Первым этапом в обеспечении безопасности информационных систем является регулярная оценка рисков и уязвимостей. Идентификация критически важных данных и активов позволяет выделить наиболее уязвимые и ценные компоненты системы, такие как данные специальной категории или финансовая информация. Анализ потенциальных угроз включает как внутренние риски (ошибки персонала, неправильные настройки систем), так и внешние, такие как кибератаки или природные катастрофы. Оценка вероятности инцидентов и их последствий помогает создать план приоритетных мер защиты, а использование международных стандартов, таких как ISO/IEC 27005 и NIST SP 800-30, упрощает процесс анализа и управления рисками.

Для выявления и устранения уязвимостей систем также важно тестирование на основе методов кибербезопасности. Пентесты (penetration testing) позволяют выявить слабые места, имитируя реальные атаки. Этот метод помогает оценить, насколько система устойчива к угрозам, и улучшить защиту за счёт выявления и исправления уязвимостей. Помимо пентестов, можно использовать моделирование инцидентов, симуляции реальных атак и тесты на проникновение, чтобы проверить готовность системы и сотрудников к потенциальным угрозам. Результаты тестирования помогают оценить текущий уровень защиты и скорректировать план безопасности, обновляя его в соответствии с выявленными уязвимостями и новыми киберугрозами [20].

Важным элементом является внедрение протоколов реагирования на инциденты, которые обеспечивают оперативное восстановление после кибератак и минимизацию ущерба. Разработка подробного плана действий в случае инцидента включает распределение ролей и задач между сотрудниками, а также установление систем мониторинга для быстрого обнаружения проблем. Классификация инцидентов по уровню критичности позволяет использовать соответствующие сценарии реагирования и направить усилия на

наиболее серьёзные угрозы. Устранение последствий включает изоляцию заражённых систем, восстановление данных и уведомление всех заинтересованных сторон, включая Роскомнадзор, если инцидент связан с утечкой персональных данных.

Интеграция с внешними партнёрами и государственными системами также является важным элементом стратегии безопасности. Сотрудничество с консультантами и использование специализированного ПО позволяют обеспечить систематический мониторинг и аудит, а взаимодействие с правоохранительными органами и Роскомнадзором помогает в координации действий в случае масштабных инцидентов. Также важно проводить регулярные тренировки и обучение персонала для повышения осведомлённости о киберугрозах и процедурах безопасности.

Защита специальных категорий персональных данных в Российской Федерации требует строгого соблюдения законодательства и применения комплексных мер, учитывая их повышенную чувствительность и возможные негативные последствия при несанкционированном доступе. К таким данным относятся сведения о расовой и этнической принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, биометрические и генетические данные.

Организационные меры, направленные на повышение защиты данных, включают разработку стандартов и регламентов, обязательное обучение сотрудников и регулярные аудиты на соответствие требованиям законодательства. Эти меры помогают своевременно выявлять уязвимости и обеспечивают надлежащий уровень защиты при удалённой работе и иных потенциально уязвимых сценариях.

Технические меры предполагают использование современных технологий, таких как обязательное шифрование данных, а также анонимизация и псевдонимизация, что позволяет минимизировать риски идентификации в случае утечки. Регулярное тестирование, моделирование кибератак и пентесты повышают устойчивость информационных систем к внешним угрозам, а протоколы реагирования на инциденты обеспечивают оперативное устранение последствий при возникновении проблем безопасности.

Расширение полномочий Роскомнадзора усиливает контроль за соблюдением законодательства и способствует более эффективному регулированию процессов обработки данных. Ужесточение административной и уголовной ответственности за нарушения повышает мотивацию организаций соблюдать стандарты безопасности, снижая риски утечек и нарушений конфиденциальности.

Приведение российского законодательства в соответствие с международными стандартами, такими как GDPR, позволит интегрировать передовые практики и повысить уровень защищённости данных. Закрепление прав субъектов данных, прозрачность обработки и обязательство операторов информировать о действиях с данными укрепляют доверие к системе защиты персональных данных и делают её более предсказуемой и надёжной.

Таким образом, комплексный подход, основанный на сочетании организационных, технических и правовых мер, а также на международном сотрудничестве, создаёт прочную основу для защиты специальных категорий персональных данных. Постоянное совершенствование систем защиты, адаптация к новым вызовам и открытость в вопросах обработки данных способствуют созданию надёжной и устойчивой системы, которая соответствует современным требованиям и обеспечивает высокую степень безопасности.

Библиография

1. Алексеев И. В. Защита персональных данных в информационных системах: правовые и технические аспекты. Москва: Юрайт, 2019. 240 с.
2. Васильева Л. В., Иванов К. С. Современные технологии защиты информации в условиях цифровизации // Информационная безопасность. 2020. Т. 22, № 4. С. 35-42.
3. Гаврилова Т. С. Актуальные проблемы правового регулирования обработки персональных данных в России // Вестник права и юстиции. 2021. № 3. С. 47-53.
4. Европейский регламент по защите данных (GDPR) [Электронный ресурс]. URL: https://gdpr-info.eu. (дата обращения: 06.02.2025)
5. Методические рекомендации по защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] https://rkn.gov.ru/methods-security. (дата обращения: 06.02.2025)
6. Оценка влияния на защиту данных: руководство по проведению DPIA в соответствии с GDPR. Европейская комиссия [Электронный ресурс] URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-directive/dpia-guidelines_en. (дата обращения: 06.02.2025)
7. Комлев Е. С., Сорокина М. В. Применение биометрической аутентификации для защиты персональных данных // Кибербезопасность и защита данных. 2022. Т. 14. № 1. С. 23-30.
8. Николаев В. Н. Управление информационными рисками в корпоративной среде // Защита информации и управление данными. 2021. Т. 10. № 2. С. 59-66.
9. Авдикова В. А. Алгоритм разработки подсистемы защиты персональных данных специальной категории в медицинском учреждении // Современные проблемы радиоэлектроники и телекоммуникаций. 2023. № 6. С. 229-234.
10. Бондаренко И. В. Правовой анализ проблем защиты персональных данных лиц, осужденных к лишению свободы участников СВО в условиях современной цифровизации общества // Аграрное и земельное право. – 2023. № 11(227). С. 195-197. DOI: 10.47643/1815-1329_2023_11_195
11. Шуманская С. А. Правовое регулирование защиты персональных данных и повышение его эффективности // Юриспруденция и современная правовая система: актуальные вопросы, достижения и инновации : Сборник статей IV Международной научно-практической конференции, Пенза, 25 января 2025 года. Пенза: МЦНС «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2025. С. 50-55.
12. Реброва Н. М. Понятие персональных данных и способы их защиты по законодательству Российской Федерации // Российское государство и право: история и современность : сборник статей преподавателей и студентов направления подготовки «Юриспруденция», Новочеркасск, 30 ноября 2020 года / Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова. Новочеркасск: Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, 2020. С. 34-45.
13. Окишев Б. А. Проблема отнесения сведений об инвалидности к специальным категориям персональных данных // Цифровые технологии и право : Сборник научных трудов II Международной научно-практической конференции: в 6 томах, Казань, 22 сентября 2023 года. Казань: Издательство «Познание», 2023. С. 235-239.
14. Новикова Ю. А. Специальные категории персональных данных работников // Кадровик. 2022. № 8. С. 8-14.
15. Крылова М. С. Особенности правовой охраны специальных категорий персональных данных в сфере электронной связи в Европейском Союзе / // Евразийский юридический журнал. 2019. № 2(129). С. 82-84.
16. Кирьянова Л. В. Правовой статус субъектов в институте «охрана персональных данных» // Юридическая наука. 2023. № 4. С. 265-267.

17. Рузанова В. Д. Персональные данные как гражданско-правовая категория // Правовое государство: теория и практика. 2022. № 3(69). С. 77-83. DOI: 10.33184/pravgos-2022.3.10
18. Гайфуллина Д. М. Отдельные правовые аспекты биоэквайринга // Научный Альманах ассоциации France-Kazakhstan. 2024. № 5. С. 25-37.
19. Методы обеспечения безопасности персональных данных в медицинских информационных системах с использованием мобильных технологий / В. П. Гулов, В. А. Хвостов, А. В. Скрыпников [и др.] // Системный анализ и управление в биомедицинских системах. 2020. Т. 19. № 4. С. 132-140. DOI: 10.36622/VSTU.2020.19.4.017.
20. Иванова М. А. Защита персональных данных работника: нормативное регулирование и проблемы обеспечения // Юридический мир. 2023. № 6. С. 17-21. DOI: 10.18572/1811-1475-2023-6-17-21

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

На рецензирование представлена статья «Совершенствования механизма защиты специальной категории персональных данных» для опубликования в журнале «Право и политика». Представленная статья была проверена на соответствие политике журнала об опубликовании научных оригинальных исследований, а также паспорту научной специальности.
Актуальность исследования не вызывает сомнений, поскольку уровень защищенности персональных данных в России вызывает опасения. Особой защите должны подлежать сведения, поименованные в ст. 10 ФЗ «О персональных данных», в силу их неопределенного толкования и отсутствия в России специализированного Регламента защиты персональных данных, аналогичного тому, что действует с 2018 года в странах Евросоюза - GDPR(General Data Protection Regulation). К сожалению, федеральный закон № 152 не содержит полного механизма, обеспечивающего неприкосновенность, защиту от утечки и достаточные меры ответственности виновных лиц в отношении таких сведений как расовая и этническая принадлежность, политические взгляды, религиозные убеждения, состояние здоровья и аспекты интимной жизни. В связи с этим автором совершенно обоснован выбор предмета исследования: правовые, технические и организационные методы защиты специальных категорий персональных данных и разработка рекомендаций по их совершенствованию. Обозначенная цель была достигнута автором путем исследования внутреннего и международного законодательства, регламентов и технических протоколов к ним; достижений современной науки и зарубежных практик защиты данных в различных отраслях жизнедеятельности человека и организаций. Это позволило автору на основе применения общих и специальных методов научного познания достичь решения следующих задач: поиск путей усиления правового регулирования; выявление современных технологий шифрования, анонимизации, псевдонимизации, а также биометрической аутентификации для ограничения несанкционированного доступа; определение организационных мер, в том числе в области обучения персонала компаний; выявление средств осведомленности субъектов данных; систематизация и анализ рисков путем моделирования инцидентов кибербезопасности и внедрения протоколов реагирования на угрозы.
Решение указанных задач позволило автору сформулировать следующие выводы и внести предложения, заслуживающие внимания. Сформулирован перечень

специализированных персональных данных, в который включены помимо указанных в действующем законодательстве, - биометрические и генетические данные. Предложено расширить полномочия Роскомнадзора, предусмотреть систему быстрого удаленного обмена данными по защищенным каналам связи между указанным ведомством, правоохранительными органами и компаниями о фактах утечки данных, принятых мерах и введенных по протоколам организационных и технических мер современной и своевременной защиты. Предложено усилить юридическую ответственность компаний и виновных в утечке данных лиц, в том числе путем введения специального состава уголовной ответственности. С последним предложением рецензент не совсем согласен ввиду минимальной раскрываемости уже существующих уголовно-наказуемых деяний. А потому дополнительная криминализация может повлечь дополнительный к уже существующей в уголовной практике так называемых «мертводействующих» составов. Однако личное убеждение рецензента ни сколь не умаляет значимости в этой части научных изысканий автора статьи. Работа содержит другие интересные прикладные решения, отражающие научную новизну проведенного исследования.

Текст статьи структурирован, логически последователен, изложен научным языком и соответствует требованиям, предъявляемым журналом «Право и политика» к научным публикациям.

Библиографический перечень достаточно обширный и включает в себя 20 источников, датированных с 2019 г. по настоящее время. В числе источников использованы 17 научных трудов, что обеспечило автору глубину и всесторонность исследования.

В целом статья будет интересна ученым, правоприменителю, обучающимся вузов и может быть рекомендована к опубликованию.