Научная статья
УДК 343.4

Уголовно-правовые проблемы охраны персональных данных в системе социальных услуг

Алексей Александрович Ходусов, кандидат юридических наук, доцент

Международный юридический институт
Москва (127427, ул. Кашёнкин луг, д. 4), Российская Федерация
yustas-73@mail.ru
https://orcid.org/0000-0001-6968-0989

Аннотация:
Введение. *Исследуемая тема обладает несомненной научной и практической значимостью, обусловленной возрастающей интенсивностью угроз информационной безопасности в контексте стремительно развивающихся технологий и повсеместного внедрения цифровых решений в социальную сферу. Особое внимание уделяется вопросам обеспечения уголовно-правовой охраны персональных данных, поскольку именно эта категория преступлений приобрела устойчивый тренд в своей динамике, став актуальной проблемой современной криминологии и юридической науки. Возникающие угрозы ставят перед законодателями новые исследовательские задачи, направленные на выработку эффективных инструментов противодействия правонарушениям, затрагивающим основы конституционных прав граждан на личную тайну и безопасность.*
Методы. *Методология исследования включает широкий спектр подходов, позволяющих осуществить глубокий теоретико-прикладной анализ объекта исследования. Среди используемых методов выделяются историческое правоописание, компаративистика нормативных актов разных стран, функционально-доктринальный подход, качественный контент-анализ судебной практики и документов правоохранительных органов, а также системно-аналитический метод.*
Результаты. *Итоговым результатом проведенного научного изыскания стало формулирование ряда значимых выводов относительно недостатков текущего состояния нормативно-правовой базы, касающейся вопросов уголовно-правовой охраны персональных данных в системах оказания социальных услуг. Выявлены существенные юридические лакуны, препятствующие эффективной борьбе с цифровыми нарушениями, заключающиеся в отсутствии ясности квалификации отдельных видов преступлений, неопределенности границ полномочий компетентных органов власти, отсутствия единых критериев оценки тяжести последствий действий преступников. Отдельно подчеркнута необходимость разработки и введения специфического юридического инструментария, направленного на профилактику и предупреждение киберпреступлений.*

Ключевые слова:
уголовно-правовая охрана, защита персональных данных, социальные услуги, комплексный подход, материальные нормы, незаконный сбор, цифровая специфика преступлений

Для цитирования:
Ходусов А. А. Уголовно-правовые проблемы охраны персональных данных в системе социальных услуг // Вестник Санкт-Петербургского университета МВД России. 2026. № 1 (109). С. 202–211.

Статья поступила в редакцию 08.12.2025; одобрена после рецензирования 02.03.2026; принята к публикации 20.03.2026.

Original article

Criminal law issues of personal data protection in the social services system

Alexey A. Khodusov, Cand. Sci. (Jurid.), Docent

The International Law Institute
4, Kashyonkin lug str., Moscow, 127427, Russian Federation
yustas-73@mail.ru
https://orcid.org/0000-0001-6968-0989

© Ходусов А. А., 2026

ISSN 2949-1150 (online)
2071-8284 (print)

Abstract:
Introduction. *The research topic has undoubted scientific and practical significance due to the increasing intensity of information security threats in the context of rapidly developing technologies and the widespread implementation of digital solutions in the social sphere. Special attention is paid to the issues of ensuring the criminal law protection of personal data, as this category of crimes has acquired a steady trend in its dynamics, becoming an urgent problem in modern criminology and legal science. The emerging threats pose new research challenges for lawmakers, aimed at developing effective tools to counteract offences that affect the foundations of citizens' constitutional rights to personal privacy and security.*
Methods. *The research methodology includes a wide range of approaches that allow for a deep theoretical and applied analysis of the research object. Among the methods used, we can name historical legal description, comparative analysis of regulations in different countries, a functional-doctrinal approach, qualitative content analysis of judicial practice and documents from law enforcement agencies and a system-analytical method.*
Results. *The result of the study lies in the formulation of several significant conclusions regarding the shortcomings of the current state of the legal framework related to the criminal protection of personal data in social service systems. The article identifies significant legal gaps that hinder the effective fight against digital violations, such as the lack of clarity in the classification of certain types of crimes, the uncertainty of the competent authority boundaries and the absence of unified criteria for assessing the severity of the consequences of criminal actions. The article also emphasises the need for the development and implementation of specific legal tools aimed at preventing and combating cybercrimes.*

Keywords:
criminal law protection, personal data protection, social services, comprehensive approach, material norms, illegal collection, digital characteristics of crimes

For citation:
Khodusov A. A. Criminal law issues of personal data protection in the social services system // Vestnik of Saint Petersburg University of the MIA of Russia. 2026. № 1 (109). P. 202–211.

**The article was submitted December 8, 2025;
pproved after reviewing March 2, 2026;
accepted for publication March 20, 2026.**

Введение

Эффективность правового обеспечения защиты персональных данных в системе социальных услуг становится одной из важнейших современных научно-практических задач, стоящих перед отечественным правотворчеством и наукой уголовного права. Как отмечается в ряде исследований, существующая система защиты нуждается не только в дальнейших организационных преобразованиях, но и в глубоком развитии всех элементов уголовно-правового механизма, охватывающего как материальные, так и процессуально-исполнительные аспекты правоотношений в сфере информационной безопасности.

Современный этап характеризуется значительным ростом киберугроз и усложнением способов хищения, фальсификации и неправомерного использования персональных данных граждан, осуществляющих взаимодействие с органами социальной поддержки. Несмотря на наличие определенных положений в действующем Уголовном кодексе Российской Федерации[1] (далее – УК РФ) (ст. 137 – нарушение неприкосновенности частной жизни, ст. 272 – неправомерный доступ к охраняемой законом компьютерной информации и др.), практика показывает их существенную ограниченность и фрагментарность. Отсутствие систематизированного и исчерпывающего перечня противоправных деяний, сопряженных с незаконным оборотом персональных данных, отсутствие дифференцированной ответственности для субъектов разного статуса (например, должностные лица учреждений соцзащиты и частные субъекты), низкий уровень определенности квалификационных признаков и недостаточно проработанные механизмы пресечения создают значительные трудности для правоохранительной практики.

Кроме того, процессы цифровизации социальной сферы порождают ряд новых рисков и вызовов, обусловленных особенностями современных информационных технологий и ускоренным развитием рынка электронных услуг. Именно поэтому остро ощущается потребность в формировании нового направления уголовно-правовых исследований, которое бы сосредоточилось на разработке четких и последовательных мер реагирования на возникающие риски. Важно отметить, что, несмотря на имеющиеся отдельные инициативы по изменению и дополнению статей УК РФ, пока отсутствует единый концептуальный подход к построению целостной модели уголовно-правовой защиты, способной эффективно противостоять современным видам злоупотреблений в области персональных данных [1].

Таким образом, предметом настоящего исследования выступает современное состояние уголовно-правовой охраны персональных данных в системе социальных услуг, а целью – выработка предложений по ее дальнейшему развитию и совершенствованию. Данный научный труд призван восполнить существующий дефицит в литературе по проблемам уголовной репрессии за посягательство на информационные права граждан и сформировать концептуальные основания для обновления уголовно-правового законодательства Российской Федерации.

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 17.11.2025) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 1996. № 25. Ст. 2954.

Методы

В качестве методов исследования использованы частнонаучные методы. Методология исследования включает широкий спектр подходов, позволяющих осуществить глубокий теоретико-прикладной анализ объекта исследования. Среди используемых методов выделяются историческое правоописание, компаративистика нормативных актов разных стран, функционально-доктринальный подход, качественный контент-анализ судебной практики и документов правоохранительных органов. Данный метод включает систематический разбор и интерпретацию судебных решений, постановлений, протоколов и иных документов правоохранительных структур. Целью является выявление ключевых тенденций, практических подходов, интерпретационных моделей и проблемных аспектов применения права. Такой анализ помогает понять реальные механизмы реализации законодательства и выявить возможные пробелы или противоречия в практике его применения. Системно-аналитический метод. Этот подход предполагает интеграцию полученных данных из различных источников и методов для формирования целостной картины исследуемого объекта. Он включает структурный анализ, моделирование, выделение взаимосвязей и закономерностей между элементами правовой системы. Использование системно-аналитического метода способствует выявлению причинно-следственных связей и структурных особенностей правовых институтов, что важно для разработки рекомендаций и практических решений.

Обсуждение

Состав преступления, объектом которого выступают персональные данные, представляет собой органичную совокупность объективных и субъективных признаков, квалифицирующих общественно опасное деяние, сопряженное с неправомерным получением, использованием, распространением или уничтожением сведений о физическом лице. Примечательно, что в современном социальном контексте подобные преступные посягательства приобретают исключительную социальную значимость, поскольку они потенциально способны затрагивать особо уязвимые группы граждан и, следовательно, имплицитно нарушать их конституционное право на социальное обеспечение и защиту.

В частности, уголовно-правовое регулирование в Российской Федерации имплементируется посредством ключевых норм, включающих, например, положения о неправомерном доступе к компьютерной информации (ст. 272 УК РФ), которые детерминируют действия по получению информации без надлежащего согласия субъекта или правообладателя; нормы о нарушении неприкосновенности частной жизни, незаконном сборе и распространении персональных данных (ст. 137, 138 УК РФ), предусматривающие ответственность за разглашение личной или семейной тайны; а также составы, регламентирующие создание и использование вредоносных программ (ст. 273 УК РФ), которые квалифицируют незаконное вмешательство в информационные системы, потенциально влекущее утечку данных. Тем не менее, несмотря на установление уголовной ответственности, указанные составы обладают рядом существенных дефектов, ограничивающих эффективность системы правовой защиты. Анализ действующего законодательства позволяет выявить следующие ключевые недостатки. Во-первых, наблюдается нежелательная каузальная неопределенность формулировок: термины «неправомерный доступ» и «нарушение порядка обработки» не обеспечивают достаточной конкретизации противоправных действий и игнорируют специфику социальной сферы, при этом отсутствует четкая дифференциация умышленных и неосторожных форм вины. Также можно отметить недостаточную дифференциацию по объектам и последствиям: УК РФ не учитывает повышенную уязвимость субъектов социальной сферы (таких как несовершеннолетние, престарелые или лица с ограниченными возможностями и др. категории), а также не содержит отдельного регулирования для квалификации массовых утечек или применения персональных данных в целях мошенничества в социальных учреждениях.

Как отмечают исследователи, наблюдается слабость квалификации должностных и коллективных деяний: отсутствуют четкие нормы, регламентирующие ответственность за организационные и управленческие упущения, ставшие причиной утечки данных, что затрудняет квалификацию преступлений, совершенных группой лиц или по неосторожности (халатности). Также следует констатировать низкую превентивную функцию действующих санкций, которые не создают достаточного стимулирующего фактора для соблюдения правил обработки данных и не обеспечивают требуемого профилактического эффекта [2].

ISSN 2949-1150 (online)
2071-8284 (print)

Представляется критически важным развитие превентивной функции УК РФ путем инкорпорации норм, которые стимулируют соблюдение регламентов обработки данных и внутренних правил безопасности, допуская, например, возможность смягчения наказания при добровольном предотвращении или устранении последствий утечки. Дополнительно требуется уточнение понятий ущерба и общественной опасности посредством четкого определения критериев «существенного вреда» и «угрозы общественной безопасности», а также дефинирование юридического момента окончания преступления для целей квалификации.

Следовательно, назрела объективная необходимость в имплементации комплекса мер, направленных на модернизацию действующего уголовного законодательства Российской Федерации с целью повышения эффективности защиты персональных данных граждан.

Также отметим, что комплексное совершенствование УК РФ, направленное на конкретизацию составов, усиление ответственности должностных лиц, введение квалифицирующих признаков и развитие превентивных механизмов, позволит существенно повысить эффективность уголовно-правовой защиты и минимизировать риски нарушения конституционных прав граждан [3].

Как известно, уголовные дела, инициируемые по фактам несанкционированного доступа к персональным данным в системе социальных услуг, обладают рядом специфических характеристик, которые преимущественно обусловлены критической значимостью обрабатываемой информации, уникальными методиками ее обработки, а также особенностями субъектов преступного посягательства. В частности, эффективность правоприменительной практики в рамках уголовного преследования напрямую коррелирует с корректностью квалификации инкриминируемого деяния, надлежащей имплементацией процедур сбора доказательств и активным использованием передовых научно-технических средств.

Результаты

Приоритетное значение приобретает детальная конкретизация объективных признаков составов преступлений, что предполагает разработку и инкорпорацию отдельных правовых норм, дифференцирующих деяния в зависимости от формы вины – умышленного или неосторожного неправомерного доступа к персональным данным. Кроме того, актуальным представляется четкое разграничение уголовно наказуемых деяний, характеризующихся признаком «существенного ущерба», от малозначительных нарушений, которые должны подлежать административной ответственности. Помимо этого, необходимо создание квалифицированных составов преступлений, отражающих специфику и повышенную общественную опасность нарушений, совершенных в системе социальных услуг.

Принципиальным аспектом является усиление ответственности субъектов, обладающих особым правовым статусом. В частности, это касается должностных лиц, в отношении которых требуется введение специальных норм, предусматривающих ответственность за преступления, совершенные с использованием служебного положения. Более того, целесообразно установление уголовной ответственности за организационные нарушения, которые имплицитно создали предпосылки и условия для масштабной утечки данных [4].

Параллельно необходимо развитие специализированных санкций уголовно-правового воздействия. К таковым, в частности, следует отнести конфискацию технических средств, использованных при совершении преступления, блокировку незаконно полученной и распространяемой информации, а также введение отягчающих обстоятельств, когда нарушение прав касается особо уязвимых категорий граждан.

Следует учитывать, что важнейшим компонентом выступает интеграция уголовно-правовых норм с превентивными механизмами. Данный подход предполагает институциональное сотрудничество с социальными учреждениями и разработку мотивационных стимулов для соблюдения мер безопасности, включая возможность применения смягчающих обстоятельств при добровольном предотвращении или минимизации последствий утечки данных.

Таким образом, можно объективно констатировать, что существующие составы преступлений в сфере персональных данных требуют значительной доработки для адекватного реагирования на современные криминогенные угрозы. Ключевые векторы совершенствования УК РФ, заключающиеся в конкретизации составов, усилении ответственности должностных лиц, внедрении квалифицированных составов и специализированных санкций, а также в интеграции уголовно-правовой ответственности с превентивными механизмами, позволят существенно повысить эффективность уголовно-правовой защиты и минимизировать риски нарушений прав граждан.

В контексте обеспечения уголовно-правовой защиты персональных данных в системе социальных услуг критически значимым представляется проведение углубленного анализа объективных и субъективных признаков составов преступных деяний, поскольку именно на их основе происходит формирование критериев уголовно-правовой квалификации и детерминация меры государственного принуждения в виде уголовного наказания [5].

В частности, объективные признаки отражают внешнюю сторону противоправного посягательства и их структура включает несколько ключевых элементов. Во-первых, объективная сторона охватывает общественно опасные действия субъекта, которые могут выражаться в несанкционированном доступе к персональным данным (далее – ПД), незаконном сборе, обработке или неправомерном распространении информации без надлежащего согласия ее субъекта, а также в создании, внедрении или использовании специализированных технических средств, предназначенных для неправомерного получения данных.

Особое внимание уделяется объекту посягательства, которым в рассматриваемом контексте преимущественно выступают ПД граждан, находящихся под социальным обеспечением. К ним, безусловно, относятся сведения об особо уязвимых категориях, таких как несовершеннолетние, лица с ограниченными возможностями здоровья (инвалидностью) и пожилые граждане, а также информационные системы социальных учреждений, обеспечивающие обработку этих данных.

Кроме того, элементом объективной стороны являются общественно опасные последствия деяния, которые проявляются в нарушении конституционного права на неприкосновенность частной жизни и конфиденциальность, создании непосредственной угрозы социальной защищенности указанных категорий лиц и, следует отметить, в потенциальном причинении материального и морального ущерба гражданам [6].

Однако проведенный анализ действующего Уголовного кодекса Российской Федерации обнаруживает ряд существенных пробелов в части регламентации объективной стороны составов, связанных с ПД. В частности, отмечается отсутствие законодательно закрепленной дифференциации по объектам посягательства именно в системе социальных услуг, что объективно препятствует должному учету специфики защиты данных уязвимых групп. Помимо этого, наблюдается отсутствие четкой градации последствий по степени их общественной опасности, а также не предусмотрен учет массовости и системности неправомерной утечки данных в качестве квалифицирующего признака, что существенно снижает эффективность уголовной репрессии.

В целях совершенствования уголовного законодательства представляется целесообразным ввести квалифицированные составы для преступлений, непосредственно затрагивающих социально уязвимые категории граждан, императивно определить критерии существенного ущерба и угрозы социальной безопасности, а также включить признаки массовости и системности как отягчающее обстоятельство.

Вместе с тем анализ субъективной стороны действующих составов УК РФ выявляет недостаточное разграничение умышленных и неосторожных действий, особенно с учетом специфических и потенциально тяжких последствий для социальной сферы. Также наблюдается слабое закрепление ответственности за мотивы, сопряженные с организационными и должностными нарушениями, что создает значительные трудности при квалификации коллективных и должностных преступных деяний [7].

В контексте оптимизации уголовного законодательства рекомендуется ввести отдельные квалифицированные составы для умышленных и неосторожных нарушений в данной сфере, закрепить специальные нормы ответственности за мотивы, способствующие массовым утечкам, и, наконец, уточнить ответственность за коллективные и должностные деяния в системе социальных услуг.

Следует подчеркнуть, что объективные и субъективные признаки преступлений, связанных с неправомерным оборотом ПД в системе социальных услуг, детерминируют уголовно-правовую квалификацию и определение меры наказания. В связи с этим действующее уголовное законодательство объективно требует существенной доработки, включающей конкретизацию объектов и последствий преступлений, четкое разграничение умышленных и неосторожных действий, а также усиление ответственности должностных и коллективных субъектов. Совершенствование УК РФ в указанных направлениях не только обеспечит более точную и справедливую квалификацию, но и существенно повысит превентивную и регулятивную эффективность уголовно-правовой защиты ПД в системе социальных услуг.

Серьезные методологические сложности возникают при установлении непосредственного субъекта преступления, например, в ситуациях использования коллективных или общих

ISSN 2949-1150 (online)
2071-8284 (print)

учетных записей. Более того, наличие признаков служебной халатности и ненадлежащего исполнения обязанностей значительно затрудняет точное определение субъективной стороны преступления (формы вины, включая умысел) должностного лица.

Анализ действующего уголовного законодательства позволяет констатировать существование объективных недостатков. Во-первых, наблюдается существенная неопределенность требований, предъявляемых к доказательствам: уголовный и уголовно-процессуальный кодексы не содержат достаточно четкой нормативной регламентации допустимых видов доказательств для категории дел, связанных с неправомерным использованием персональных данных, что объективно осложняет квалификацию конкретных действий в цифровой среде как «неправомерного доступа» [8].

Также отмечается ограниченная практика квалификации, судебная практика по данной категории дел остается слаборазвитой, вследствие чего отсутствует единообразие в подходах к оценке масштабов утечки, степени общественной опасности и роли должностных лиц в инциденте.

Дополнительно следует отметить низкую превентивную функцию доказательств: в подавляющем большинстве случаев доказательства лишь констатируют факт уже совершенного преступления, но не служат механизмом его предупреждения. Кроме того, обнаруживается дефицит нормативных положений, стимулирующих самоорганизацию и строгое соблюдение мер информационной безопасности в социальных учреждениях.

Представляется целесообразным внесение комплекса предложений по совершенствованию уголовного законодательства. Прежде всего необходимо уточнить требования к доказательствам путем имплементации специальных норм, регламентирующих использование цифровых следов, логов и технических данных, а также детализировать допустимые методы проведения экспертизы и фиксации факта утечки данных.

Критически важным является четкое разграничение умысла и неосторожности через закрепление критериев установления формы вины для должностных лиц и сотрудников социальных служб. Также необходимо предусмотреть квалификацию коллективных действий и организационных нарушений. В связи с этим рекомендуется развивать превентивную функцию доказательств посредством стимулирования документирования и аудита процессов обработки персональных данных и введения норм, учитывающих добросовестное соблюдение мер безопасности как смягчающее обстоятельство при расследовании. Столь же необходимо внедрение типовых методик оценки ущерба в целях создания единых подходов к определению масштаба утечки и ее последствий для социальной сферы, обязательно принимая во внимание категории пострадавших субъектов (дети, пожилые люди, лица с инвалидностью) при квалификации причиненного вреда [9].

Принципиальное значение имеет введение нормы об ответственности за организационную халатность, устанавливающей уголовную ответственность руководителей социальных учреждений за непринятие обязательных мер безопасности. Одновременно необходимо закрепление уголовно-правовых дефиниций цифровых действий (таких как «цифровой след», «несанкционированный доступ», «цифровое хищение», «утечка»), что позволит снизить неопределенность при квалификации. Дополнительно целесообразно развитие инструментов уголовно-правовой превенции, включая возможность освобождения от ответственности при добровольном предотвращении последствий и уточнение санкций (повышение штрафов при массовых утечках, введение дополнительных наказаний, например, запрета на деятельность) [10].

Эффективность уголовно-правовой охраны персональных данных неразрывно связана с развитием институционального и организационного механизма. Сегодня институциональная система характеризуется фрагментарностью государственного контроля (функции надзора сосредоточены у Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) с ограниченными административными полномочиями), отсутствием специализированного органа в системе социальных услуг и недостаточной координацией между социальными службами, МВД России, Следственным комитетом Российской Федерации и регуляторами. Более того, следует признать организационную неготовность социальных учреждений к предотвращению преступлений, выражающуюся в низком уровне цифровой защищенности и квалификации сотрудников.

Говоря об уголовно-правовых недостатках институционального механизма, следует выделить отсутствие правовых обязанностей организаций по содействию расследованию, а именно, норм, обязывающих должностных лиц своевременно информировать о фактах утечки.

Особую проблему представляет слабая ответственность за ненадлежащее хранение доказательств, поскольку отсутствие отдельного состава за умышленное уничтожение или сокрытие

цифровых следов в организациях облегчает уклонение от ответственности. Также неурегулированность статуса Роскомнадзора в уголовном процессе фактически исключает его из механизма расследования, что снижает качество экспертиз и эффективность выявления преступлений.

Для устранения указанных проблем предлагается: закрепить в УК РФ обязанность организаций социальной сферы сообщать о фактах утечки, ввести уголовную ответственность за сокрытие или уничтожение цифровых следов, расширить процессуальный статус Роскомнадзора до уровня экспертного органа, создать специализированные подразделения по расследованию преступлений в сфере данных (аналог киберполиции) и разработать единый межведомственный протокол реагирования на утечки. Кроме того, целесообразно введение уголовно-правовых стимулов повышения безопасности данных, например, смягчение наказания при наличии сертифицированных систем защиты [11].

В целях нивелирования обозначенных проблем и повышения эффективности уголовно-правовой защиты представляется целесообразным осуществить комплекс мер, направленных на совершенствование законодательства. В первую очередь критически важной представляется концептуальная конкретизация и дифференциация составов преступлений путем имплементации отдельных норм, регулирующих умышленное и неосторожное обращение с персональными данными, а также разграничение деяний по степени их общественной опасности и тяжести последствий, принимая во внимание социальную уязвимость пострадавших субъектов. Далее, необходимо уточнение квалификации действий должностных лиц посредством введения специальных норм, регулирующих ответственность за организационные и управленческие нарушения, и в дополнение закрепление повышенной ответственности за системные нарушения, способствующие массовой утечке. Кроме того, следует ввести квалифицирующие признаки, обладающие спецификой социальной сферы, включая особую ответственность за нарушение прав детей, инвалидов и пожилых граждан, а также учитывать массовость утечки данных как отягчающее обстоятельство [12].

Следует заключить, что специфика процесса доказывания преступлений, связанных с неправомерным доступом к персональным данным в системе социальных услуг, требует безотлагательного совершенствования уголовного и уголовно-процессуального законодательства. Ключевые направления реформирования включают уточнение видов допустимых доказательств, дифференциацию формы вины (умысла и неосторожности), развитие превентивных норм и имплементацию типовых методик оценки ущерба. Реализация данных мер позволит обеспечить более высокую точность квалификации, повысить эффективность расследования и гарантировать адекватную защиту конституционных прав граждан [13].

Действующее уголовно-правовое регулирование обнаруживает ряд существенных дефектов. Во-первых, принципиальным недостатком является отсутствие специализированных составов преступлений, ориентированных на социальную сферу, поскольку УК РФ не предусматривает повышенной уголовной защиты данных особо уязвимых категорий граждан, включая, например, несовершеннолетних, лиц с инвалидностью, престарелых или пациентов социальных и медицинских учреждений. Отсутствие специальных квалифицирующих признаков, очевидно, снижает превентивный потенциал норм.

Также наблюдается недостаточная дифференциация ответственности, поскольку нормы УК РФ зачастую не позволяют адекватно разграничить степень общественной опасности между незначительными утечками и крупными, системными нарушениями, а также фактически приравнивают массовое коммерческое распространение данных к единичным преступным эпизодам [14].

Критически важным является отсутствие отдельной ответственности за организационные нарушения: в ситуациях, когда утечка данных обусловлена системным отсутствием надлежащей безопасности, конкретные исполнители могут быть не установлены, что свидетельствует о низкой эффективности охвата управленческой халатности.

При этом следует отметить неопределенность понятийного аппарата, поскольку термины «доступ», «обработка», «хищение информации» не имеют прямых уголовно-правовых дефиниций, а пробелы в терминологии объективно тормозят формирование единообразной следственной и судебной практики [15].

Учитывая вышесказанное, предлагается реализовать комплекс мер по совершенствованию УК РФ. Прежде всего необходимо создание специализированной главы или расширение ст. 272–274^1 УК РФ путем разработки комплексного блока норм, классифицирующих преступления в зависимости от объема утечки, причиненного вреда и категории пострадавших. Крайне важно введение квалифицирующих признаков для социальной сферы, предполагающее установление повышенной ответственности за незаконный доступ к данным уязвимых групп (детей,

ISSN 2949-1150 (online)
2071-8284 (print)

инвалидов, пенсионеров, пациентов) и добавление ответственности за утечку, повлекшую дискриминацию или социальный вред. Более того, требуется усиление ответственности за массовые утечки и их коммерческое использование через введение отдельного состава за продажу или обмен украденных данных, а равно за создание незаконных онлайн-баз.

Заключение

Можно констатировать, что эффективная уголовно-правовая защита персональных данных в системе социальных услуг невозможна без гармоничного развития как материальных норм УК РФ, так и организационно-институционального обеспечения. Предложенный комплексный подход, объединяющий конкретизацию составов, усиление ответственности должностных лиц, введение специализированных санкций и повышение межведомственной координации, позволит обеспечить персонализированную защиту граждан, устранить пробелы, связанные с цифровой спецификой преступлений, и повысить превентивный эффект уголовного законодательства.

Априори следует отметить, что превенция деликтов, ассоциированных с нелегитимным оборотом персональных данных в рамках социального сектора, выступает в качестве фундаментального и имманентного элемента эффективного механизма уголовно-правовой защиты. Следовательно, результативность реализации государственной уголовно-правовой доктрины императивно детерминируется уровнем сформированности правовой культуры субъектов социальной сферы, наличием действенного превентивного инструментария и созданием нормативно-правовых механизмов предупреждения криминальных проявлений.

В частности, ключевое значение в минимизации противоправных посягательств объективно принадлежит правовой культуре. Критически значимым является формирование правосознания уполномоченных должностных лиц. Действительно, персонал социальных учреждений, как правило, обладает доступом к обширным массивам конфиденциальной информации, включая сведения о статусе здоровья, социальном и семейном положении, а также наличии льготных прав граждан.

Однако низкий уровень осознания юридических последствий, в частности, уголовной ответственности, за несанкционированные инциденты утечки персональных данных перманентно способствует эскалации криминализации в данной предметной области. Кроме того, правовая культура самих граждан также является существенным фактором редукции виктимности: поскольку граждане зачастую передают свои данные социальным институтам без должного осмысления потенциальных рисков, а отсутствие навыков верификации источников, адекватного понимания своих прав и способов защиты неизбежно повышает вероятность злоупотреблений. Кроме того, систематически наблюдается дефицит специализированных образовательных инициатив, т. к. до настоящего времени не имплементированы обязательные программы повышения квалификации, сфокусированные на проблематике уголовно-правовой ответственности за неправомерные действия с данными, в то время как социальные учреждения, как правило, ограничиваются исключительно формализованными инструктажами.

Тем не менее детальный анализ действующей системы уголовно-правовой профилактики позволяет выявить ряд существенных институциональных и нормативных лакун. Во-первых, констатируется отсутствие прямого закрепления профилактических прерогатив и обязанностей в УК РФ: в уголовном законодательстве не установлены конкретные императивы для должностных лиц по активному предотвращению угроз утечки данных, вследствие чего профилактическая деятельность носит преимущественно административно-организационный характер и лишена того стимулирующего эффекта, который имманентно присущ уголовно-правовым нормам.

Обращает на себя внимание нечеткая регламентация превентивных мер в рамках уголовного процесса, т. к. УПК РФ не содержит специальных процедур, ориентированных на выявление конкретных предпосылок преступлений в сфере персональных данных, а превентивная деятельность следственных органов ограничивается исключительно общими положениями.

Следует также отметить отсутствие специализированного криминологического обеспечения, что проявляется в недостатке эмпирического анализа факторов виктимности граждан и сотрудников социальных учреждений, а также в неразработанности специализированных криминологических карт рисков утечек данных. При этом наблюдается слабая интеграция концепции цифровой гигиены в систему предупреждения преступлений: поскольку преступные деяния часто становятся возможными в результате служебной небрежности сотрудников (например, вследствие использования тривиальных паролей или отсутствия принципа сегментации

доступа), УК РФ пока не учитывает уровень внедрения защищенных информационных систем в качестве фактора, определяющего степень ответственности.

Представляется научно обоснованным рассматривать профилактику криминальных деяний, сопряженных с неправомерным обращением персональных данных, в качестве ключевого императива современной уголовно-правовой политики. В целях максимизации эффективности превентивного воздействия целесообразно осуществить комплекс мероприятий, направленных на институциональное и нормативное совершенствование в отношении рассмотренных противоправных деяний. Прежде всего требуется легислативное закрепление специальных превентивных норм в Уголовном кодексе Российской Федерации.

Особую значимость приобретает установление стимулирующих положений. Например, следует предусмотреть возможность смягчения уголовного наказания при условии наличия документально подтвержденных мер обеспечения безопасности данных (таких как прохождение сертификации, регулярный аудит или специализированная подготовка персонала), причем эти обстоятельства могут быть учтены как факторы, косвенно свидетельствующие об отсутствии прямого умысла. Безусловным требованием является разработка уголовно-правового механизма предупреждения рецидивной преступности в рассматриваемой сфере. Это включает как лишение права замещать определенные должности, непосредственно сопряженные с обработкой персональных данных, так и установление специального контроля за профессиональной деятельностью лиц, ранее привлекавшихся к ответственности за аналогичные деликты.

Критически важным элементом профилактики выступает введение обязательных программ правового обучения как для работников социальной сферы (с акцентом на уголовно-правовые запреты и служебные обязанности), так и для широкой общественности (посредством разработки информационно-аналитических материалов о потенциальных рисках при передаче данных). Также необходимо нормативное закрепление положений о цифровой гигиене в качестве неотъемлемого компонента профилактической системы. С этой целью предлагается признать нарушение базовых требований цифровой безопасности фактором уголовно-правовой значимости и, возможно, инкорпорировать квалифицирующий признак, предусматривающий повышенную ответственность за совершение преступления вследствие грубого нарушения регламентов информационной безопасности.

Можно резюмировать, что совершенствование правовой культуры, усиление должностных обязанностей, инкорпорирование превентивных норм в УК РФ и создание специализированных программ профилактики, безусловно, позволят существенно редуцировать как количественные показатели преступности, связанной с незаконным обращением персональных данных, так и уровень непосредственной угрозы для граждан в системе социальных услуг.

Список источников

1. *Акинина Н. Ю., Анисимов В. Ф., Кочупалов Р. В.* Криминализация незаконного оборота персональных данных // Вестник Сургутского государственного университета. 2024. Т. 12, №. 3. С. 84–91. https://doi.org/10.35266/2949-3455-2024-3-8

2. *Алиев И. И.* Функции юридической ответственности // Вестник Науки и Творчества : [электронное издание]. 2023. № 3. С. 34–41.

3. *Бронников Д. А.* Передача и распространение массивов персональных данных. Общественная опасность и перспективы криминализации подобных деяний / Молодые ученые России : сборник статей VI Всероссийской научно-практической конференции. Пенза : Наука и Просвещение, 2021. С. 165–167.

4. *Халиулина Э. Т., Журавлева А. С.* Преступления, совершаемые с использованием персональных данных: характеристика состояния // Военное право. 2021. № 2 (66). С. 289–294.

5. *Бредихин А. Л.* К теории юридической ответственности // Философия права. 2021. № 3 (98). С. 52–55.

6. *Минина А. А., Атаян Г. Ю., Богатырева А. Т.* Отдельные особенности правового режима и защиты персональных данных // Право и государство: теория и практика. 2023. № 8 (224). С. 164–167. https://doi.org/10.47643/1815-1337_2023_8_164

7. *Минзов А. С., Невский А. Ю., Баронов О. Р.* Безопасность персональных данных: новый взгляд на старую проблему // Вопросы кибербезопасности. 2022. № 4 (50). С. 2–12. https://doi.org/10.21681/2311-3456-2022-4-2-12

8. *Арланов М. А., Дурдымурадов Д. В.* Защита персональных данных в условиях цифровой экономики // Всемирный ученый. 2024. Т. 1, вып. 20. С. 405–410.

9. *Терещенко И. А.* Биометрические персональные данные: проблемы и перспективы определения понятия // Закон и право. 2024. № 2. С. 186–192. https://doi.org/10.24412/2073-3313-2024-2-186-192

10. *Кузнецова С. С., Мочалов А. Н., Саликов М. С.* Биометрическая идентификация в интернете: тенденции правового регулирования в России и за рубежом // Вестник Томского государственного университета. 2022. № 476. С. 257–267. https://doi.org/10.17223/15617793/476/28

11. *Степаненко Д. А., Рудых А. А.* Технико-криминалистическое обеспечение противодействия преступлениям против информационной безопасности объектов здравоохранения // Академический юридический журнал. 2021. Т. 22, № 1 (83). С. 41–48. https://doi.org/10.17150/1819-0928.2021.22(1).41-48

ISSN 2949-1150 (online)
2071-8284 (print)

12. *Родивилина В. А., Коломинов В. В.* Криминалистическая характеристика отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2022. Т. 21, № 1. С. 110–120. https://doi.org/10.55001/2587-9820.2022.85.75.010

13. *Климанов А. М., Пешков Д. В.* Некоторые вопросы квалификации преступления, предусмотренного ст. 137 УК РФ // Теория и практика общественного развития. 2015. № 9. С. 98–102.

14. *Хохлова Е. В.* К вопросу о защите изображения человека как персональных данных (на основе судебной практики по ст. 137 УК РФ) // Вестник Воронежского института МВД России. 2023. № 1. С. 301–305.

15. *Овсянников П. Ю.* Административная ответственность за несоблюдение требований законодательства Российской Федерации в области персональных данных, а также государственной и иной охраняемой законом тайны // Административное право и процесс. 2022. № 8. С. 24–26. https://doi.org/10.18572/2071-1166-2022-8-24-26

References

1. *Akinina N. Yu., Anisimov V. F., Kochupalov R. V.* Kriminalizaciya nezakonnogo oborota personal'nyh dannyh // Vestnik Surgutskogo gosudarstvennogo universiteta. 2024. T. 12, №. 3. S. 84–91. https://doi.org/10.35266/2949-3455-2024-3-8

2. *Aliev I. I.* Funkcii yuridicheskoj otvetstvennosti // Vestnik Nauki i Tvorchestva : [elektronnoe izdanie]. 2023. № 3. S. 34–41.

3. *Bronnikov D. A.* Peredacha i rasprostranenie massivov personal'nyh dannyh. Obshchestvennaya opasnost' i perspektivy kriminalizacii podobnyh deyanij / Molodye uchenye Rossii : sbornik statej VI Vserossijskoj nauchno-prakticheskoj konferencii. Penza : Nauka i Prosveshchenie, 2021. S. 165–167.

4. *Haliulina E. T., Zhuravleva A. S.* Prestupleniya, sovershaemye s ispol'zovaniem personal'nyh dannyh: harakteristika sostoyaniya // Voennoe pravo. 2021. № 2 (66). S. 289–294.

5. *Bredihin A. L.* K teorii yuridicheskoj otvetstvennosti // Filosofiya prava. 2021. № 3 (98). S. 52–55.

6. *Minina A. A., Atayan G. Yu., Bogatyreva A. T.* Otdel'nye osobennosti pravovogo rezhima i zashchity personal'nyh dannyh // Pravo i gosudarstvo: teoriya i praktika. 2023. № 8 (224). S. 164–167. https://doi.org/10.47643/1815-1337_2023_8_164

7. *Minzov A. S., Nevskij A. Yu., Baronov O. R.* Bezopasnost' personal'nyh dannyh: novyj vzglyad na staruyu problemu // Voprosy kiberbezopasnosti. 2022. № 4 (50). S. 2–12. https://doi.org/10.21681/2311-3456-2022-4-2-12

8. *Arlanov M. A., Durdymuradov D. V.* Zashchita personal'nyh dannyh v usloviyah cifrovoj ekonomiki // Vsemirnyj uchenyj. 2024. T. 1, vyp. 20. S. 405–410.

9. *Tereshchenko I. A.* Biometricheskie personal'nye dannye: problemy i perspektivy opredeleniya ponyatiya // Zakon i pravo. 2024. № 2. S. 186–192. https://doi.org/10.24412/2073-3313-2024-2-186-192

10. *Kuznecova S. S., Mochalov A. N., Salikov M. S.* Biometricheskaya identifikaciya v internete: tendencii pravovogo regulirovaniya v Rossii i za rubezhom // Vestnik Tomskogo gosudarstvennogo universiteta. 2022. № 476. S. 257–267. https://doi.org/10.17223/15617793/476/28

11. *Stepanenko D. A., Rudyh A. A.* Tekhniko-kriminalisticheskoe obespechenie protivodejstviya prestupleniyam protiv informacionnoj bezopasnosti ob"ektov zdravoohraneniya // Akademicheskij yuridicheskij zhurnal. 2021. T. 22, № 1 (83). S. 41–48. https://doi.org/10.17150/1819-0928.2021.22(1).41-48

12. *Rodivilina V. A., Kolominov V. V.* Kriminalisticheskaya harakteristika otdel'nyh vidov prestuplenij, sovershennyh s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij // Kriminalistika: vchera, segodnya, zavtra. 2022. T. 21, № 1. C. 110–120. https://doi.org/10.55001/2587-9820.2022.85.75.010

13. *Klimanov A. M., Peshkov D. V.* Nekotorye voprosy kvalifikacii prestupleniya, predusmotrennogo st. 137 UK RF // Teoriya i praktika obshchestvennogo razvitiya. 2015. № 9. S. 98–102.

14. *Hohlova E. V.* K voprosu o zashchite izobrazheniya cheloveka kak personal'nyh dannyh (na osnove sudebnoj praktiki po st. 137 UK RF) // Vestnik Voronezhskogo instituta MVD Rossii. 2023. № 1. S. 301–305.

15. *Ovsyannikov P. Yu.* Administrativnaya otvetstvennost' za nesoblyudenie trebovanij zakonodatel'stva Rossijskoj Federacii v oblasti personal'nyh dannyh, a takzhe gosudarstvennoj i inoj ohranyaemoj zakonom tajny // Administrativnoe pravo i process. 2022. № 8. S. 24–26. https://doi.org/10.18572/2071-1166-2022-8-24-26