

Скворцов Никита Юрьевич
Смоленский государственный университет
г. Смоленск, Россия
Научный руководитель:
Уварова Валерия Вячеславовна
Смоленский государственный университет
г. Смоленск, Россия

УДК 343.13

ХАЛАТНОСТЬ В СФЕРЕ ЦИФРОВЫХ ГОСУДАРСТВЕННЫХ УСЛУГ: БЕЗДЕЙСТВИЕ ПРИ УТЕЧКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

***Аннотация:** в статье анализируются уголовно-правовые аспекты халатности должностных лиц государственных органов при утечках персональных данных в сфере цифровых государственных услуг. Исследуются вопросы применения ст. 293 УК РФ к бездействию должностных лиц ИТ-подразделений, проблемы установления причинной связи между ненадлежащим исполнением обязанностей и наступившими последствиями, а также вопросы разграничения халатности со смежными составами преступлений (ст. 272, 272.1, 285 УК РФ).*

***Ключевые слова:** халатность, персональные данные, цифровые государственные услуги, должностное лицо, утечка данных, информационная безопасность.*

Цифровая трансформация государственного управления, выразившаяся в развитии системы «Госуслуги», межведомственного электронного взаимодействия (СМЭВ), единой биометрической системы и иных цифровых платформ, неразрывно связана с накоплением государством огромных массивов персональных данных (ПДн) граждан. По оценкам, совокупный объем скомпрометированных записей ПДн в России в 2025 году достиг 1 343 млн, при этом ущерб от одной только утечки через приложения на основе NFCGate в 2025 году превысил 1,5 млрд руб.. Государственные органы, аккумулирующие наиболее чувствительную информацию о гражданах, становятся главной мишенью для кибератак и одновременно — источником угрозы ввиду ненадлежащего исполнения должностными лицами обязанностей по ее защите. Особую остроту проблеме придает то, что, согласно данным компании «Еса Про», в 2025 году 73% всех утечек данных в России пришлось именно на

госсектор. При этом, несмотря на заявления Минцифры о 13-кратном сокращении успешных атак в результате принятых мер, сохраняются значительные разрывы в статистике и, что более важно, сохраняется низкая эффективность привлечения виновных должностных лиц к уголовной ответственности по ст. 293 УК РФ.

Цель настоящего исследования — выявить теоретические и практические проблемы применения ст. 293 УК РФ к бездействию должностных лиц государственных органов в сфере защиты ПДн при оказании цифровых услуг и предложить пути их решения.

Объем и характер утечек персональных данных в государственном секторе: статистика и правовой контекст

Статистические данные за 2024–2025 гг. демонстрируют неоднозначную картину. С одной стороны, официальная статистика фиксирует снижение количества утечек: в 2025 году зафиксировано 118 утечек, что на 13% меньше, чем в 2024 году (135 утечек). Совокупный объем утекших строк сократился на 93% до 52 млн. Однако эти данные расходятся с оценками независимых компаний: по данным F6, объем утекших строк вырос на 68% до 767 млн при снижении числа инцидентов до 225. Такое расхождение объясняется различными методиками подсчета и, возможно, неполным раскрытием информации со стороны государственных органов — в 2024 году 59% структур, выявивших утечки, вообще не разглашали информацию о них.

В уголовно-правовом смысле важна не столько статистика, сколько сам факт того, что значительная часть утечек происходит по вине должностных лиц, ненадлежащим образом исполняющих свои обязанности по защите информации. Речь идет о ситуациях, когда доступ злоумышленников к информационным системам становится возможным из-за отсутствия необходимых организационно-распорядительных мер со стороны ответственных должностных лиц — непроведения аттестации объектов информатизации, отсутствия системы обнаружения вторжений (IDS/IPS), непроведения своевременного обновления

программного обеспечения, неконтролируемого предоставления избыточных прав доступа или игнорирования требований приказа ФСТЭК России № 21.

Уголовно-правовая характеристика халатности применительно к сфере цифровых государственных услуг

Объективная сторона халатности (ст. 293 УК РФ) выражается в бездействии — неисполнении или ненадлежащем исполнении должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе. В сфере цифровых госуслуг это может проявляться в: непроведении обязательных организационно-технических мероприятий по защите ПДн, отсутствии контроля за соблюдением требований информационной безопасности подчиненными сотрудниками, игнорировании предписаний уполномоченных органов об устранении нарушений, ненадлежащем администрировании информационных систем.

При этом обязательным условием наступления уголовной ответственности является причинение крупного ущерба (свыше 2,25 млн руб. в соответствии с примечанием к ст. 293 УК РФ) либо существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства. Пленум Верховного Суда РФ неоднократно подчеркивал, что существенность нарушения подлежит обязательной и тщательной оценке в каждом конкретном случае. Применительно к утечкам ПДн существенное нарушение прав граждан может выражаться в массовом характере утечки, компрометации биометрических данных, использовании утекших данных для совершения мошеннических действий в отношении потерпевших и т.д.

Субъективная сторона халатности характеризуется неосторожной формой вины в виде легкомыслия или небрежности. Должностное лицо должно осознавать возможность наступления общественно опасных последствий, но без достаточных к тому оснований самонадеянно рассчитывать на их предотвращение либо не предвидеть возможности наступления таких последствий, хотя при необходимой внимательности и предусмотрительности

должно и могло их предвидеть. На практике установление субъективной стороны является одной из наиболее сложных проблем: обвинение должно доказать, что должностное лицо не просто формально не исполнило обязанность, но сделало это вследствие именно недобросовестного или небрежного отношения к службе, а не в силу объективных причин (например, недостаточного финансирования).

Субъект халатности в сфере цифровых государственных услуг: проблемы теории и практики

Субъект халатности — специальный, должностное лицо, выполняющее функции представителя власти либо организационно-распорядительные или административно-хозяйственные функции в государственных органах, органах местного самоуправления, государственных и муниципальных учреждениях, а также в Вооруженных Силах РФ, других войсках и воинских формированиях РФ (примечание 1 к ст. 285 УК РФ). В ИТ-подразделениях государственных органов должностными лицами признаются руководители соответствующих структурных подразделений (начальники управлений информатизации, отделов информационной безопасности, ИТ-директора и т.п.), а также иные лица, наделенные в установленном порядке организационно-распорядительными функциями в отношении подчиненных или полномочиями по принятию решений о выделении ресурсов на информационную безопасность.

Однако сложность возникает в отношении специалистов, технически обеспечивающих функционирование систем защиты ПДн, но формально не обладающих властными полномочиями (системных администраторов, инженеров, программистов). Ряд авторов, в частности М.А. Тыняная, справедливо отмечают, что правовой статус указанных лиц в контексте ст. 293 УК РФ требует уточнения, поскольку содержащиеся в примечании 1 к ст. 285 УК РФ положения порождают сложности в правоприменительной деятельности.

Более того, согласно разъяснениям, за исключением случаев, когда субъектом может стать государственный служащий, не являющийся должностным лицом, такие специалисты часто остаются за рамками уголовной

ответственности по ст. 293 УК РФ, что создает «правовой вакуум» в сфере ответственности за технические ошибки и бездействие.

Проблемы разграничения халатности со смежными составами преступлений.

При квалификации деяний, связанных с утечками ПДн из государственных информационных систем, возникает конкуренция ст. 293 УК РФ со ст. 272 (неправомерный доступ к компьютерной информации), 272.1 (незаконное использование, передача, сбор и хранение компьютерной информации, содержащей ПДн), 285 (злоупотребление должностными полномочиями) и 286 (превышение должностных полномочий) УК РФ.

Как отмечает М.И. Рамонова, ключевым критерием отграничения халатности от злоупотребления полномочиями является психическое отношение должностного лица к своим обязанностям и последствиям. При халатности должностное лицо уклоняется от исполнения обязанностей не преднамеренно, а по забывчивости, невнимательности или в силу отсутствия должной подготовки. При злоупотреблении же присутствует умысел на использование служебного положения в корыстных или иных личных целях. Это разграничение имеет принципиальное значение для правильной квалификации, поскольку санкции по ст. 285 и 286 УК РФ существенно выше, чем по ч. 1 ст. 293 УК РФ.

Анализ судебной практики показывает, что привлечение к уголовной ответственности за утечки ПДн по ст. 293 УК РФ встречается крайне редко. Значительно чаще квалификация идет по ст. 272, 272.1 или 285–286 УК РФ. В 2025 году МВД России зарегистрировало 923 преступления, связанных с незаконным использованием, сбором и передачей ПДн (ст. 272.1 УК РФ), однако конкретные данные о количестве приговоров по ст. 293 УК РФ в открытых источниках практически отсутствуют. При этом, как справедливо отметил председатель Комитета Госдумы по информационной политике Александр Хинштейн, значительная часть эпизодов вполне подпадает под ст. 293 УК РФ, особенно в отношении сотрудников госучреждений.

Рассмотренные судебные дела (например, в Брянской области, где экс-сотрудница полиции передавала знакомому данные из баз МВД, нарушив конституционные права не менее 575 граждан; в Ульяновской области, где сотрудница Социального фонда передавала коммерческой организации ПДн, что позволило последней получить из бюджета свыше 6 млн руб.) квалифицировались по ст. 272 и 286 УК РФ, а не по ст. 293, что свидетельствует о предпочтении обвинения квалифицировать умышленные активные действия, а не неосторожное бездействие. Показательно также дело бывшего начальника полиции в Астрахани, осужденной за утечку личной информации граждан по ст. 286 и 272 УК РФ к реальному лишению свободы.

При этом Верховный Суд РФ неоднократно указывал на необходимость тщательного доказывания существенности вреда по делам о халатности, и отсутствие таких доказательств является основанием для отмены приговора. Показательным является и оправдание ВС РФ следователя, осужденной за халатность первой инстанцией, что демонстрирует высокий стандарт доказывания по данной категории дел.

Наиболее сложной проблемой при квалификации деяний по ст. 293 УК РФ в сфере цифровых госуслуг является установление причинной связи между бездействием должностного лица и наступившими последствиями (утечкой ПДн). Необходимо доказать, что у должностного лица имелась реальная возможность надлежащим образом исполнить свои обязанности (например, своевременно провести аттестацию, установить обновления, ограничить доступ); именно неисполнение (ненадлежащее исполнение) конкретной обязанности создало реальную возможность для утечки; утечка произошла именно в результате этого бездействия, а не вследствие иных причин (например, целенаправленного взлома с использованием ранее неизвестной уязвимости нулевого дня, которую должностное лицо не могло предотвратить).

Наличие «внешнего» виновного — непосредственного исполнителя неправомерного доступа (хакера или инсайдера) — существенно осложняет доказывание причинной связи. Однако, как справедливо отмечается в доктрине,

халатность должностного лица может выступать необходимым условием для совершения преступления иным лицом. В таких случаях следует применять теорию «необходимого сопричинения», согласно которой бездействие должностного лица, создавшее реальную возможность для наступления общественно опасных последствий, рассматривается как юридически значимая причина этих последствий наряду с действиями непосредственного исполнителя.

В настоящее время административная ответственность за нарушение законодательства о ПДн предусмотрена ст. 13.11 КоАП РФ, причем размеры штрафов для должностных лиц варьируются от 50 000 до 300 000 руб. в зависимости от тяжести нарушения. С 30 мая 2025 года вступил в силу закон о повышении оборотных штрафов за утечку ПДн: повторная утечка 10 000 идентификаторов или данных не менее 1 000 субъектов грозит оборотным штрафом до 3% годовой выручки — не менее 20 млн и не более 500 млн руб..

В уголовно-правовой плоскости в декабре 2024 года введена ст. 272.1 УК РФ, устанавливающая ответственность за незаконное использование, передачу, сбор и хранение компьютерной информации, содержащей ПДн, а равно за создание и обеспечение функционирования информационных ресурсов для их незаконного хранения и/или распространения. Санкция по ч. 5 ст. 272.1 УК РФ (тяжкие последствия или совершение организованной группой) предусматривает лишение свободы на срок до десяти лет со штрафом до 3 млн руб..

Несмотря на это, проблема привлечения к ответственности именно должностных лиц за бездействие в сфере защиты ПДн (халатность) остается нерешенной. Представляется целесообразным: расширить толкование субъекта халатности в постановлении Пленума Верховного Суда РФ, включив в него должностных лиц, ответственных за организацию информационной безопасности в государственных органах, включая руководителей ИТ-подразделений, а также уточнив, что системные администраторы и иные технические специалисты, наделенные правом принятия решений о внесении изменений в конфигурацию средств защиты информации, также могут нести ответственность по ст. 293 УК РФ при наличии соответствующих признаков.

Ввести квалифицированный состав халатности (ч. 3 ст. 293 УК РФ) — халатность, повлекшую утечку ПДн в крупном размере (более 100 000 записей) либо повлекшую компрометацию биометрических персональных данных, с более строгой санкцией (реальное лишение свободы). Это позволит дифференцировать ответственность в зависимости от степени общественной опасности последствий. Установить презумпцию наличия причинной связи между выявленными нарушениями требований законодательства о ПДн (вступившими в силу предписаниями Роскомнадзора или ФСТЭК России, не исполненными в установленный срок) и наступившей утечкой, с правом должностного лица опровергать эту презумпцию. Это позволит преодолеть основные сложности доказывания. Разработать и утвердить постановление Пленума Верховного Суда РФ, специально посвященное вопросам квалификации халатности в сфере цифровых государственных услуг и информационной безопасности, с подробными разъяснениями понятий «существенное нарушение прав граждан», «крупный ущерб», «причинная связь» применительно к утечкам ПДн.

Проведенное исследование позволяет сделать вывод о том, что, несмотря на высокую общественную опасность утечек персональных данных из государственных информационных систем (73% от всех утечек в 2025 году), механизм привлечения должностных лиц к уголовной ответственности по ст. 293 УК РФ за халатность в этой сфере работает крайне неэффективно. Основные проблемы носят как теоретический (неопределенность субъектного состава, сложность установления причинной связи), так и правоприменительный (неразработанность критериев существенности вреда применительно к ПДн, конкуренция со ст. 272, 272.1, 285–286 УК РФ) характер.

Решение указанных проблем требует комплексного подхода, включающего как разъяснения Пленума Верховного Суда РФ, так и, возможно, точечные изменения уголовного законодательства. В условиях продолжающихся кибератак и нарастающего объема цифровых государственных услуг бездействие государства в части обеспечения уголовно-правовой защиты ПДн

граждан может привести к подрыву доверия к цифровым государственным сервисам и причинению значительного ущерба как отдельным гражданам, так и государству в целом. Как справедливо отметил Александр Хинштейн, «хищения персональных данных должны являться предметом уголовного наказания», и ст. 293 УК РФ является одним из действенных, но пока недооцененных инструментов для достижения этой цели.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024). Ст. 272, 272.1, 285, 286, 293.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 26.02.2026). Ст. 13.11.
3. Постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий».
4. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 29.12.2025) «О персональных данных».
5. Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».
6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Тыняная, М.А. Уголовно-правовая характеристика халатности : дис. ... канд. юрид. наук. Томск, 2017.
8. Рамонова, М.И. Проблемы ограничения халатности от иных составов преступлений // Современная наука: актуальные проблемы теории и практики. 2023. № 2.
9. Царев, Е.В. Уголовное законодательство об ответственности за халатность : монография. Н. Новгород : Нижегородская правовая академия, 2014. 156 с.
10. Хинштейн, А.Е. Виновников утечек можно строго наказывать уже сейчас // ComNews. 2022. 21 июля. URL: <https://www.comnews.ru/content/221294/2022-07-21/2022-w29/vinovnikov-utechek-mozhno-strogo-nakazyvat-uzhe-seychas> (дата обращения: 16.04.2026).
11. Государственные организации стали главной мишенью хакеров в 2025 году // Коммерсантъ. 2025. 22 декабря. URL: <https://www.kommersant.ru/doc/8313440> (дата обращения: 16.04.2026).
12. Лисаев, О. Тщательность оценки «существенности» в конкретных обстоятельствах // Адвокатская газета. 2021. № 16 (345).

13. Борисов, А.В. Отграничение халатности от умышленных должностных преступлений // Современное право. 2017. № 9.

Student
Skvortsov N.Y.
Smolensk State University
Scientific supervisor
Uvarova V.V.
Candidate of Law Sciences
Smolensk State University
Smolensk, Russia

NEGLIGENCE IN THE FIELD OF DIGITAL PUBLIC SERVICES: INACTION IN THE EVENT OF A PERSONAL DATA LEAK

Abstract: The article analyzes the criminal law aspects of negligence by government officials in the event of a personal data leak in the field of digital public services. The article examines the application of Article 293 of the Criminal Code of the Russian Federation to the inaction of officials of IT departments, the problems of establishing a causal relationship between improper performance of duties and the resulting consequences, as well as the issues of distinguishing negligence from related crimes (Articles 272, 272.1, and 285 of the Criminal Code of the Russian Federation).

Keywords: negligence, personal data, digital public services, official, data leakage, information security.