УДК 343:349:004
DOI 10.34755/IROK.2026.77.49.052

Кадомский Андрей Игоревич
УМВД России по Тамбовской области

Правовой анализ регулирования информационно-коммуникационной сферы в Российской Федерации

Аннотация. Настоящее исследование посвящено комплексному анализу правового регулирования информационно-коммуникационной сферы в Российской Федерации, отражающего процессы интенсивной цифровизации общества. В статье рассматривается действующая нормативная правовая база, включающая как нормативные правовые акты федерального законодательства, так и ведомственные приказы и распоряжения. На основе результатов анализа статистических данных ФКУ «ГИАЦ МВД России» особое внимание уделяется росту преступлений, связанных с неправомерным доступом к информации (ст. 272 УК РФ), и увеличению удельного веса преступлений, совершенных с использованием методов социальной инженерии. Полученные результаты направлены на формирование списка предложений по совершенствованию российского законодательства в сфере использования информационно-коммуникационных технологий и укреплению международного взаимодействия для предупреждения преступлений, совершаемых с использованием информационных технологий и обеспечения национальной безопасности Российской Федерации.

Ключевые слова: правовое регулирование, информационно-коммуникационная сфера, информационно-коммуникационные технологии, киберпреступность, персональные данные, информационная безопасность.

Kadomskiy Andrey Igorevich
Ministry of Internal Affairs of the Russian Federation in the Tambov Region

Legal Analysis of the Regulation of the Information and Communication Sphere in the Russian Federation

Annotation. This research concentrates on a comprehensive analysis of the legal regulation of the information and communication sphere in the Russian Federation, which reflects the processes of digitalization in society. The article examines the current legal framework, including the provisions of the Constitution of the Russian Federation and relevant federal legislation. Special attention is given to the protection of personal data and the prevention of crimes committed using information and communication technologies, particularly the unauthorized access to computer information. The analysis of statistical data from the Main Information and Analytical Center of the Ministry of Internal Affairs of the Russian Federation has revealed key trends and existing legal gaps in current legislation. The research aims to generate proposals for improving Russian legislation and systematizing existing legal norms, as well as promoting international cooperation to ensure information security and sustainable development of the information and communication sphere.

Keywords: legal regulation, information and communication sphere, information and communication technologies, cybercrime, personal data, and information security.

Интенсивное развитие информационно-коммуникационных технологий в настоящее время приводит к все большей их интеграции в повседневную жизнь. «Процессы цифровизации затрагивают практически все сферы жизнедеятельности общества, создавая новые экономические и социальные возможности. Вместе с тем возрастают и риски,

связанные с угрозой утраты конфиденциальной информации, ростом числа кибератак и увеличением количества случаев совершения преступлений в информационно-коммуникационной сфере» [7, с. 1095]. В таких условиях перед государством возникает задача разработки эффективных мер, обеспечивающих правовую защиту юридических и физических лиц, а также государственных органов, а правовое регулирование информационно-коммуникационной сферы становится одним из важных элементов стратегии развития страны. Именно поэтому крайне важным становится четкое определение сфер регулирования, позволяющих эффективно решать возникающие проблемы.

Так, согласно положениям Распоряжения Правительства Российской Федерации от 30.12.2024 № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий», информационно-коммуникационная сфера – это совокупность информационно-телекоммуникационных сетей, включая сеть «Интернет», технологической инфраструктуры, обеспечивающей их функционирование, и различных форм человеческой активности, осуществляемой посредством их использования, и «практически каждое третье преступление совершено в информационно-коммуникационной сфере либо с использованием информационно-коммуникационных технологий», где под сферой понимается комплекс действий, включающий создание, обработку, хранение, передачу и использование электронных документов, данных и информации посредством компьютерных сетей, телекоммуникаций и программного обеспечения.

Основой правового регулирования информационно-коммуникационной сферы являются положения Конституции Российской Федерации, гарантирующей свободу слова, право на получение и распространение информации, тайну переписки и неприкосновенность частной жизни [1]. Эти базовые принципы определяют границы вмешательства государства в личную жизнь граждан и формируют общую концепцию построения правового порядка в данном секторе.

Однако вместе с этим возникают ситуации, требующие дополнительного правового регулирования. Так, широко используемый термин «цифровой профиль физического лица» порождает серьезные этические и юридические вопросы относительно степени допустимой открытости персональной информации и способов ее использования различными организациями и государственными учреждениями [10]. А в настоящее время Президент Российской Федерации Владимир Владимирович Путин поручил «Министерству внутренних дел Российской Федерации до 30 июня 2026 г. обеспечить создание государственного информационного ресурса «Цифровой профиль иностранного гражданина», содержащего сведения об иностранных гражданах и лицах без гражданства, въезжающих в Российскую Федерацию, выезжающих из Российской Федерации, пребывающих (проживающих) в Российской Федерации, в целях формирования полной, достоверной и актуальной информации для оценки миграционной ситуации в Российской Федерации, выработки и реализации мер, направленных на регулирование миграционных процессов на территории Российской Федерации» [2].

Так, основной документ, который определяет зону регулирования и взаимодействия с компонентами информационно-коммуникационной сферы в Российской Федерации – Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Также, на процесс нормативного правового регулирования влияют ведомственные нормативные правовые акты и специализированные федеральные программы, такие как «Стратегия развития информационного общества в Российской Федерации на период до 2030 года», утвержденная Президентом Российской Федерации Владимиром Владимировичем Путиным, которые устанавливают цели и приоритеты государственной политики в области цифровизации, одновременно очерчивая зоны риска и возможные пути решения проблемных вопросов [3].

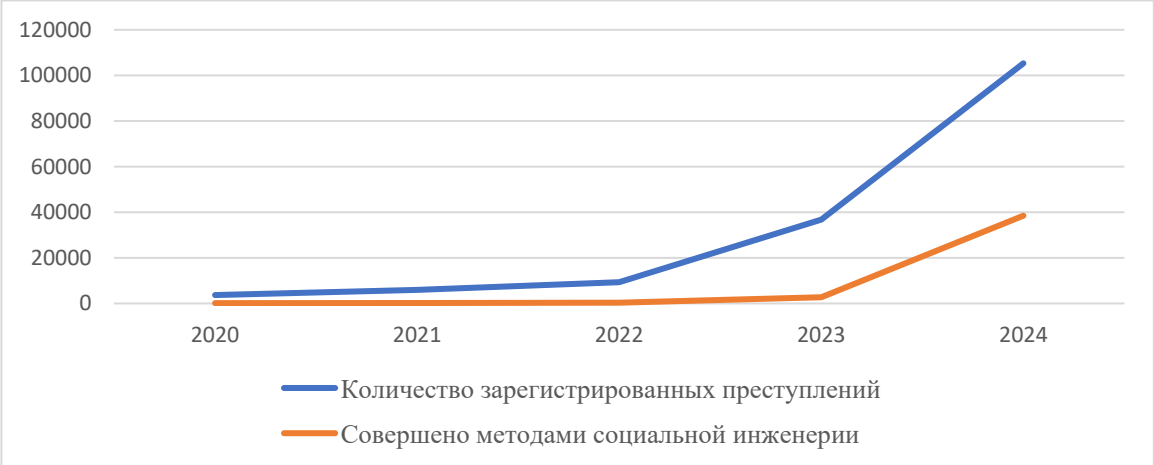
Практическое применение существующих правовых норм сталкивается с рядом трудностей, обусловленных спецификой самой природы информационных технологий. Так, одним из главных недостатков действующей системы регулирования является недостаточный уровень эффективности инструментов контроля за соблюдением норм законодательства. Эта ситуация усугубляется отсутствием единообразных подходов к определению критериев качества предоставления услуг в электронном виде, что создает неопределенность в интерпретации действующих норм законодательства и затрудняет межведомственное взаимодействие между регионами.

Еще одной проблемой является несовершенство методов идентификации пользователей, приводящей к внесению ложных сведений в информационные ресурсы. Использование поддельных или взломанных аккаунтов затрудняет установление лиц, осуществляющих противоправные действия. Для решения этой проблемы все большую популярность набирает внедрение биометрических систем аутентификации.

Так, например, согласно статистическим данным ФКУ «ГИАЦ МВД России», количество выявленных преступлений, связанных с неправомерным доступом к компьютерной информации, ответственность за которые установлена ст. 272 УК РФ, сохраняет стабильно высокие показатели и тенденцию к увеличению (табл. 1) (рис. 1)[1].

Таблица 1 – Статистические сведения ФКУ «ГИАЦ» МВД России о состоянии преступности в сфере неправомерного доступа к компьютерной информации в России за период 2020-2024 гг.

Отчетный период	**2020**	**2021**	**2022**	**2023**	**2024**
Зарегистрировано преступлений	3688	5965	9308	36788	105311
Из них лица установлены ОВД	466	1001	1058	1200	2167
Приостановлено по п.п. 1-4 ч. 1 ст. 208 УПК РФ	2713	4445	6879	26024	95888
Преступлений при помощи социальной инженерии	139	179	341	2707	38485



1 На момент подготовки статьи ФКУ «ГИАЦ МВД России» не предоставлены статистические данные за 2025 год в открытом доступе, по этой причине сравнительный анализ проводился по доступным статистическим данным предыдущих лет.

Рисунок 1 – Количественная характеристика преступлений, ответственность за которые установлена по ст. 272 УК РФ, совершенных с использованием информационно-коммуникационных технологий за период 2022-2024 гг.

При этом удельный вес таких преступлений, совершенных с использованием методов социальной инженерии по итогам 2024 года получил сильный рост и составил 36,54% (7,36% – в 2023) (рис. 2)[2].

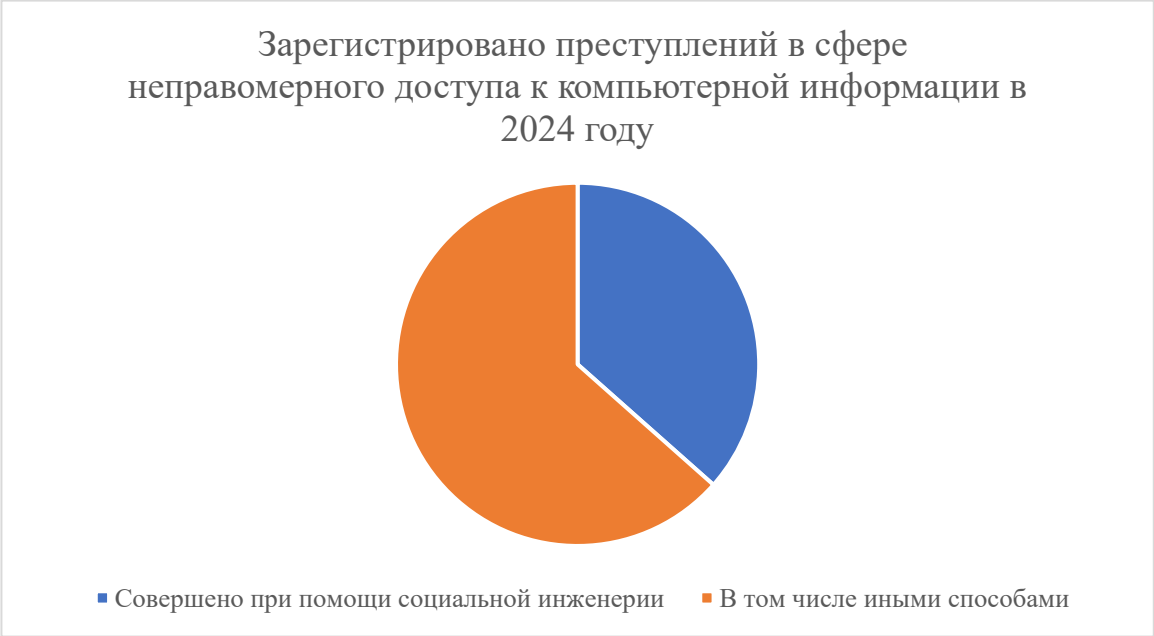


Рисунок 2 – Удельный вес количества всех зарегистрированных преступлений в сфере неправомерного доступа к компьютерной информации, совершенных методами социальной инженерии, среди всех зарегистрированных преступлений по ст. 272 УК РФ с использованием информационно-коммуникационных технологий в 2024 г.

И хотя за 2 месяца 2026 года количество раскрытых преступлений в данной категории увеличилось на 126,5% по сравнению с аналогичным периодом прошлого года, раскрываемость в данной категории составляет только 20,8% (табл. 2).

Таблица 2 – Статистические сведения ФКУ «ГИАЦ» МВД России о состоянии преступности в сфере неправомерного доступа к компьютерной информации в России за январь-февраль 2026 года

	ЗАРЕГИСТРИРОВАНО (в отчетном периоде)	в том числе	Из числа находившихся в производстве					выявлено лиц, совершивших преступлен
			АСКРЫТО	в том числе			раскрываемость в %	ЕРАСКРЫТО
		выявленных сотрудниками		следственными органами	органами внутренн	угловные дела, которые направлены в суд с		

2 Форма № 280, кн. 1 «Сводный отчет по России о результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации». ГИАЦ МВД России. Сведения за 2020-2024 гг.

								Следственного комитета Российской Федерации	их дел	обвинительным заключением, обвинительным актом, обвинительным постановлением						ия (по наиболее тяжкому)	
	сего	,-%	следственных органов Следственного комитета Российской Федерации	органов внутренних дел	органов Федеральной службы безопасности	сего	,-%			сего	,-%	д. вес от раскрытых в %		сего	,-%	сего	,-%
преступления в сфере компьютерной информации глава 28 УК РФ	133	50,7	4	941	52	464	86,5	39	195	421	95,4	7,1	6,4	073	72,1	96	04,2
том числе неправомерный доступ к компьютерн	321	56,8	2	249	0	035	26,5	73	59	009	36,3	7,5	0,8	942	72,9	7	,8

ой информации ст. 272 УК РФ																	

Учитывая, что удельный вес преступлений, совершаемых с целью неправомерного доступа к компьютерной информации составляет 86,76% от всех преступлений, отнесенных к совершаемым в сфере компьютерной информации (глава 28 УК РФ), «без надлежащего уровня защиты информационных систем и обучения сотрудников соблюдению мер по предупреждению неправомерного доступа к сведениям, содержащимся в государственных базах данных, невозможно их стабильное функционирование» [1] (рис. 3).

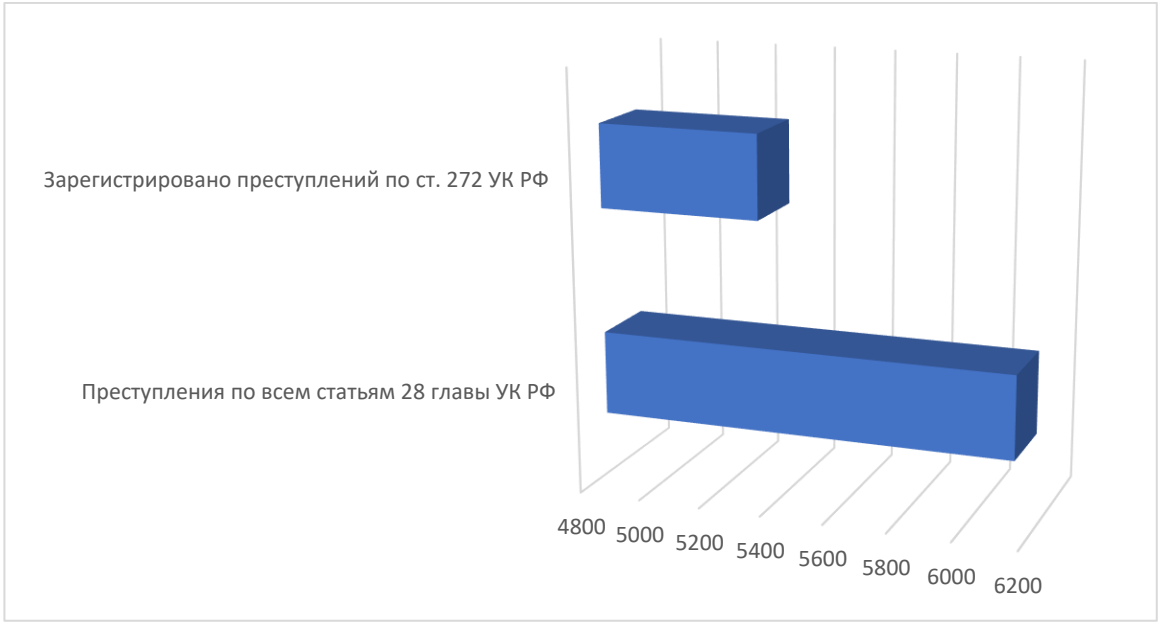


Рисунок 3 – Удельный вес количества всех зарегистрированных преступлений в сфере неправомерного доступа к компьютерной информации, среди всех зарегистрированных преступлений по ст. 272 УК РФ с использованием информационно-коммуникационных технологий за январь-февраль 2026 г.

Необходимо отметить, что развитие информационно-коммуникационных технологий носит глобальный характер, что ставит перед российским законодательством задачи согласования национальных норм с международными стандартами, касающихся защиты персональных данных и противодействию киберпреступности. Одним из примеров успешной интеграции законодательства и мер предупреждения является принятие Конвенции Совета Европы о защите физических лиц при обработке персональных данных (Конвенция № 108), которая с принятием протокола № 223 была подписана Российской Федерацией в 2018 году [5].

Для этого необходимо продолжать работу по составлению и согласованию двусторонних соглашений с иностранными государствами по вопросам взаимного признания доказательств и оказании помощи в расследовании преступлений, совершенных с использование информационно-коммуникационных технологий. Такие соглашения способствуют укреплению доверия между странами и повышению общей безопасности в информационно-коммуникационной сфере.

В соответствии с распоряжением Президента Российской Федерации Генеральной прокуратуре Российской Федерации было поручено подписать от имени Российской Федерации Конвенцию, нацеленную на укрепление международного сотрудничества в

борьбе с киберпреступностью [4]. Проект Конвенции был разработан более 5 лет назад Генеральной прокуратурой России при координирующей роли МИД России. В декабре 2024 года Генассамблея ООН большинством голосов приняла этот документ. 25 октября 2025 года в столице Вьетнама Ханое указанный исторический документ в области международного права был подписан Генеральным прокурором Российской Федерации Александром Гуцаном.

Исходя из проведенного анализа, можно сформулировать следующие практические рекомендации по совершенствованию системы правового регулирования информационно-коммуникационной сферы:

1. Создание единой концепции регулирования информационно-коммуникационной сферы, систематизирующей действующие нормы законодательства и исключающей противоречия в положениях различных нормативных правовых актов.
2. Совершенствование процедуры надзора за исполнением существующего законодательства в данной сфере путем введения обязательного аудита деятельности государственных органов и привлечения независимых экспертов к оценке результатов их деятельности.
3. Формирование действенных механизмов предотвращения несанкционированного доступа к информационным системам и критической инфраструктуре государства, таких как системы автоматического выявления угроз и предупреждения кибератак [8, с. 482].
4. Организация регулярного общественного обсуждения проектов нормативных правовых актов, касающихся регулирования информационно-коммуникационной сферы, привлечение широкого круга заинтересованных сторон, включая представителей бизнеса, научных кругов и гражданского общества.
5. Проведение масштабных кампаний по повышению грамотности населения в области безопасной работы в сети, разъяснению особенностей предоставления услуг, предоставляемых в электронном виде.
6. Профессиональная подготовка сотрудников, обладающих необходимыми компетенциями в области информационно-коммуникационных технологий и способности квалифицированно применять соответствующие знания на практике.

Реализация вышеуказанных мер позволит существенно снизить уровень правовых рисков, устранить существующие недостатки в межведомственном межгосударственном взаимодействии и обеспечить устойчивое развитие информационно-коммуникационной сферы в Российской Федерации [6, с. 94].

Таким образом, исследование показало, что современное понятие информационно-коммуникационной сферы представляет собой сложный объект правового регулирования, сочетающий как положительные эффекты цифровизации общества, так и негативные факторы, угрожающие правам и интересам физических и юридических лиц. Поэтому необходима целенаправленная работа по совершенствованию законодательства и выработке оптимальных моделей реагирования на возникающие вызовы. Только таким образом возможно обеспечить гармоничное развитие государства в сфере информационного права и поддержание высокого уровня информационной безопасности.

Эффективное правовое регулирование предполагает тесное сотрудничество всех заинтересованных сторон: федеральных органов власти, муниципальных образований, бизнеса, научного сообщества и гражданского общества. Лишь при таком подходе можно достичь поставленных целей и сформировать надежную основу для устойчивого развития общества в условиях современных геополитических вызовов.

Как заявил Президент России Владимир Владимирович Путин 24 февраля 2026 года на заседании коллегии ФСБ России: «необходимо развивать и совершенствовать государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» [9].

Список источников

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 25.04.2026).
2. Указ Президента Российской Федерации от 09.07.2025 № 467 «О государственном информационном ресурсе «Цифровой профиль иностранного гражданина» // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_509510/ (дата обращения: 25.04.2026).
3. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 25.04.2026).
4. Распоряжение Президента Российской Федерации от 23.10.2025 № 409-рп «О подписании Конвенции Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям».
5. Конвенция Совета Европы от 28.01.1981 № 108 «О защите физических лиц при автоматизированной обработке персональных данных» // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 25.04.2026).
6. Иванцов С. В. Информационно-телекоммуникационные технологии – современная реальность преступности / С. В. Иванцов, Т. В. Молчанова // Вестник Санкт-Петербургского университета МВД России. – 2020. – № 4(88). – С. 89-96.
7. Кадомский А. И. Предупреждение подделки документов с применением электронной подписи / А. И. Кадомский // Цифровая трансформация: тенденции и перспективы : Сборник трудов IV Международной научно-практической конференции, Москва, 18 декабря 2025 года. – Москва: Общество с ограниченной ответственностью «Издательство «Мир науки», 2025. – С. 1094-1101.
8. Роль информационных технологий в профилактике и раскрытии преступлений / Е. В. Бурцева, И. П. Рак, А. В. Селезнев, А. В. Терехов // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2008. – № 2(58). – С. 479-482.
9. Заседание коллегии ФСБ России // Официальный сайт Президента Российской Федерации. URL: http://kremlin.ru/events/president/news/79216 (дата обращения: 25.04.2026).
10. Что такое Цифровой профиль физического лица // Единая система контекстных справок. URL: https://info.gosuslugi.ru/articles/Что_такое_Цифровой_профиль_физического_лица/ (дата обращения: 25.04.2026).
11. Kemp S., Buil-Gil D., Moneva A., Miró-Llinares F., Díaz-Castaño N. Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19 // Journal of Contemporary Criminal Justice. – 2021. – Vol. 37, No. 4. – P. 480–501.

Сведения об авторе

Кадомский Андрей Игоревич, специалист УМВД России по Тамбовской области, г. Тамбов, Россия.

Information about the author

Kadomskiy Andrey Igorevich, Specialist of the Ministry of Internal Affairs of Russia in the Tambov Region, Tambov, Russia.