

Ссылка для цитирования этой статьи:

Шерстяных А.С. Национальные цифровые сервисы vs киберпреступность: новые законы и технологии // Human Progress. 2025. Том 11, Вып. 7. С. 31. URL: http://progress-human.com/images/2025/Tom11_7/Sherstyanykh.pdf DOI 10.46320/2073-4506-2025-7a-36.

НАЦИОНАЛЬНЫЕ ЦИФРОВЫЕ СЕРВИСЫ VS КИБЕРПРЕСТУПНОСТЬ: НОВЫЕ ЗАКОНЫ И ТЕХНОЛОГИИ



Шерстяных Александра Сергеевна

доцент кафедры информационно-правовых дисциплин и
специальной техники,
Сибирский юридический институт МВД России,
г. Красноярск, Российская Федерация

Аннотация. В России защита информации регулируется комплексом нормативно-правовых актов, включая Федеральный закон «О безопасности», «О персональных данных», «О коммерческой тайне» и положения Уголовного кодекса РФ. Несмотря на развитую законодательную базу, вопросы эффективного противодействия утечкам остаются актуальными. Кибератаки, человеческий фактор и преднамеренные действия злоумышленников требуют не только правовых, но и технических, организационных мер защиты. В данной статье рассматриваются основные новеллы правового регулирования информационной безопасности в России, направленные на противодействие киберпреступности, защиту персональных данных и повышение безопасности финансовых операций. Подчеркивается важность комплексного подхода, сочетающего законодательные меры, технологические инновации и повышение цифровой грамотности населения. Статья будет полезна специалистам в области информационной безопасности, юристам, а также всем, кто интересуется вопросами защиты данных и цифровой трансформации государственных сервисов.

Ключевые слова: информационная безопасность, кибермошенничество, защита персональных данных, многофункциональный сервис обмена информацией

Введение

В современном цифровом мире информация стала одним из ключевых активов государства, бизнеса и граждан. Однако рост её ценности сопровождается увеличением рисков утечек, которые могут привести к значительным финансовым, репутационным и даже геополитическим последствиям.

Утечки информации могут иметь разнообразные причины и механизмы реализации. Среди них – технические сбои, ошибки пользователей, уязвимости в системах безопасности, а также целенаправленные атаки злоумышленников. Последствия таких инцидентов могут быть крайне серьёзными, включая ущерб репутации компаний, правовые последствия для организаций и отдельных лиц, а также нарушение прав граждан на конфиденциальность персональных данных.

В 2024–2025 годах кибермошенничество остается одной из ключевых угроз цифровой безопасности в России. С развитием технологий злоумышленники совершенствуют методы обмана, что приводит к росту числа пострадавших среди граждан и бизнеса. В ответ на эти вызовы правительство России активно развивает законодательную базу и усиливает меры по защите данных. Новые инициативы включают ужесточение наказаний за мошенничество в IT-сфере, расширение полномочий регуляторов, а также внедрение технологических решений для предотвращения атак. Кроме того, особое внимание уделяется просветительской работе с населением, чтобы снизить эффективность атак с использованием социальной инженерии.

Законодательные инициативы в области обеспечения защиты персональных данных в РФ в 2025 году

С первого июня вступил в силу Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

В настоящее время государство, операторы связи, банковские и кредитные организации стараются бороться с кибермошенниками самостоятельно. Новый закон позволит объединить эти усилия в рамках новой государственной информационной системы. Нововведения будут вступать в действие поэтапно, в течение двух лет.

С 1 июня 2025 года вступили в силу следующие новые правила:

1. В целях предупреждения утечек учетных данных при авторизации в информационных системах, интегрированных с Единой системой идентификации и аутентификации (ЕСИА), отправка кода подтверждения будет осуществляться исключительно

при условии отсутствия активного телефонного вызова у абонента (подпункт «в» пункта 5 статьи 9).

2. Для повышения эффективности борьбы с мошенниками, которые выдают себя за сотрудников банков, силовых структур, государственных органов и других организаций, общаясь с потенциальными жертвами через мессенджеры, введён запрет на использование иностранных мессенджеров в работе. Этот запрет распространяется на государственные органы власти, местного самоуправления и подведомственные им организации, а также на Центральный банк РФ, финансовые организации (кредитные и некредитные), операторов связи, а также владельцев платформ для онлайн-общения.

В настоящее время вступил в силу федеральный закон от 24 июня 2025 г. N 156-ФЗ «О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации». Сервис призван обеспечить безопасный обмен сведениями между «...инфраструктурой, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме» [1], с учетом требований согласия субъекта данных. Важным компонентом является поддержка механизмов усиленной квалифицированной и неквалифицированной электронной подписи, функционирующих в рамках единой защищенной инфраструктуры, с соблюдением установленных правительством стандартов верификации.

Области применения многофункционального сервиса обмена информацией (МСОИ) охватывают различные административные процедуры, такие как возрастная и льготная верификация, позволяя подтверждать возраст и права на социальные льготы без необходимости предоставления физических документов. В образовательной сфере сервис обеспечивает цифровое подтверждение факта обучения в образовательных организациях. В гостиничном и транспортном секторе МСОИ используется для идентификации личности при оказании услуг размещения. Дополнительно сервис поддерживает использование машиночитаемых QR-кодов для оперативного доступа к информации через Единый портал госуслуг, а также применяется в иных санкционированных правительством случаях, требующих подтверждения личности или документов в цифровой среде. Таким образом, МСОИ выступает ключевым элементом цифровой трансформации административных процессов, обеспечивая безопасный и эффективный обмен данными в рамках национальной инфраструктуры электронного правительства.

Правительством РФ [2] создание МСОИ поручено обществу с ограниченной ответственностью «Коммуникационная платформа», являющемуся дочерним предприятием холдинга VK. МСОИ будет реализован на основе цифровой платформе МАХ. В настоящее время на платформе МАХ уже доступно [3]:

- быстрый и удобный мессенджер для обмена файлами до 4 ГБ;
- групповые чаты, качественные аудио- и видеозвонки без ограничений по времени и количеству участников, а также при нестабильном интернете;
- защищенные денежные переводы в чате с собеседником;
- цифровой ассистент на базе искусственного интеллекта GigaChat 2.0, позволяющий решать рабочие и бытовые задач.

В ближайшее время появится возможность подключаться к Госуслугам прямо из мессенджера, что сделает использование государственных сервисов более удобным. Также будет внедрён цифровой ID, позволяющий подтверждать личность без бумажных документов в повседневных ситуациях.

Ещё одним нововведением станет Госключ — инструмент для подписания документов электронной подписью и безопасного обмена проверенными данными между гражданами, государством и бизнесом. Кроме того, платформа пополнится образовательными сервисами, созданными для удобного взаимодействия учителей, учеников и их родителей в защищённом контуре национальной платформы.

С 1 сентября 2025 года вступают в силу следующие изменения:

1. Оператор связи обязан (подпункт «б» пункта 5 статьи 9) передавать на экран телефона информацию об абоненте (если он является индивидуальным предпринимателем или юридическим лицом). В настоящее время у многих операторов связи эта услуга уже есть (подключается платно или по запросу абонента), но с 1 сентября операторы будут обязаны эту информацию предоставлять.

2. У пользователей сетей связи появилась возможность отказаться от массовых обзвонков (пункт 3 статьи 9). Сделать они это могут, оправив в адрес оператора связи соответствующий отказ. Исключение составляют обзвоны по инициативе государственных органов власти (подведомственные им организации), а также иные организации, перечень которых будет определяться Правительством РФ.

3. С целью упорядочения оформления сим-карт физические лица могут установить самозапрет на заключение договоров об оказании услуг сотовой связи (подпункты «а» и «б» пункта 4 статьи 9). Сделать это можно двумя способами: онлайн (с помощью портала госуслуг) или оффлайн (посетив многофункциональный центр). При этом у физических лиц остается

возможность передачи сим-карт лицам, которые в соответствии с Семейным кодексом, являются членами семьи или близкими родственниками. При этом законодатель ужесточает наказание за передачу сим-карт посторонним лицам. 17 июля Госдума РФ во втором чтении приняла поправки о введении штрафов за передачу другим лицам абонентского телефонного номера [4]. Штрафы для граждан составят от 30 000 до 50 000 рублей, для юрлиц – до 200 000 рублей.

4. При выдаче наличных через банкоматы кредитные организации обязаны проводить проверку на наличие признаков выдачи наличных денежных средств без добровольного согласия клиента (пункт 2 статьи 2). Перечень таких признаков поручено разработать Банку России и разместить на своем сайте. Скорее всего Банк России порекомендует ориентироваться на следующее:

- сумма снимаемых денежных средств отличается от обычных сумм, обналичиваемых клиентом;
- снятие денежных средств носит нетипичный характер (например, деньги снимаются в ночное время или через банкомат, расположенный в другом городе);

5. Физические лица могут (по соглашению с банком) назначить уполномоченное лицо для подтверждения выбранных денежных операций (подпункты «г» – «о» пункта 4 статьи 2). Банк обязан приостановить выполнение таких операций на срок до 12 часов (более короткий срок может установлен в соглашении) до получения подтверждения от уполномоченного лица. Нововведение призвано защитить накопления людей, склонных к внушению, от посягательств кибермошенников. Если в отношении человека имеются сведения о причастности его к экстремистской деятельности или терроризму, то он не может быть назначен уполномоченным лицом.

Создание новой государственной информационной системы (ГИС) по борьбе с кибермошенничеством планируется завершить к 1 марта 2026 года (статья 1). В информационной системе будет аккумулирована информация о лицах, нарушивших законодательство посредством использования сетей общего пользования, а также их идентификационные номера абонентов. Положение о ГИС, перечень хранимой и обрабатываемой информации, а также порядок обращения и взаимодействия пользователей с системой будет утверждено Правительством РФ (при условии согласования с федеральной службой безопасности РФ). На сегодняшний день предполагается, что пользователи ГИС станут Генеральная прокуратура, Следственный комитет, финансовые и кредитные организации, а также федеральные органы исполнительной власти. Правительству РФ также

поручено разработать специальный перечень организаций, которым будет открыт доступ к новой государственной информационной системе.

Также с 1 марта 2026 года вводится обязательная аутентификация при оформлении потребительского займа в микрофинансовых организациях (статья 7). В пункте 2 статьи 7 говорится о недопущении упрощенной системы идентификации личности при заключении договора займа в микрофинансовых организациях. Нововведение призвано исключить случаи оформления займов с помощью скомпрометированных паспортных данных граждан.

Заключение

Современные вызовы цифровой безопасности требуют комплексного подхода, который объединяет законодательные инициативы, технологические решения и повышение цифровой грамотности населения. Нормативные акты, введенные в 2025 году, отражают стремление российских властей усилить защиту данных, противодействовать кибермошенничеству и сформировать безопасную цифровую среду. Параллельно развиваются национальные цифровые сервисы, такие как МСОИ и платформа МАХ, обеспечивающие безопасный обмен данными. Особое внимание уделяется защите уязвимых групп, например, через введение механизма подтверждения операций с участием уполномоченных лиц.

Однако успех этих мер во многом зависит от их практического воплощения, способности бизнеса адаптироваться к изменениям и готовности граждан принимать новые правила. Для обеспечения устойчивой кибербезопасности в России важно продолжать развивать цифровую инфраструктуру и совершенствовать правовое регулирование в этой сфере.

Список литературы

1. О создании многофункционального сервиса обмена информацией и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 24.06.2025 № 156-ФЗ // СПС КонсультантПлюс.
2. Об организации, обеспечивающей создание и функционирование многофункционального сервиса обмена информацией : Распоряжение Правительства РФ от 12.07.2025 N 1880-р // СПС КонсультантПлюс.
3. Национальным мессенджером станет цифровая платформа МАХ: сайт Минцифры. URL: <https://digital.gov.ru/news/nacziionalnym-messendzherom-stanet-czifrovaya-platforma-max> (дата обращения: 27.07.2025).

4. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях и Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» : Законопроект № 755710-8 // СПС КонсультантПлюс.

NATIONAL DIGITAL SERVICES VS CYBERCRIME: NEW LAWS AND TECHNOLOGIES

Sherstyanykh Alexandra Sergeevna

Candidate of Technical Sciences, Assistant Professor,
Associate of the Department of Information and Legal Disciplines and Special Technique
of the Siberian law Institute of the Ministry of internal Affairs of Russia
Krasnoyarsk, Russian Federation

Annotation. In Russia, information protection is governed by a set of legal regulations, including the Federal Laws "On Security," "On Personal Data," "On Commercial Secrets," and provisions of the Criminal Code of the Russian Federation. Despite a well-developed legal framework, challenges in effectively preventing data breaches remain pressing. Cyberattacks, human error, and malicious insider actions necessitate not only legal but also technical and organizational safeguards. This article explores recent developments in Russia's legal framework for information security, focusing on countering cybercrime, enhancing personal data protection, and securing financial transactions. The importance of an integrated approach combining legislative measures, technological innovations and improving the digital literacy of the population is emphasized. The article will be useful for information security specialists, lawyers, as well as anyone interested in data protection and digital transformation of public services.

Keywords: information security, cyber fraud, personal data protection, multifunctional information exchange service.

References

1. On the creation of a multifunctional information exchange service and on amendments to certain legislative acts of the Russian Federation: Federal Law No. 156-FZ dated June 24, 2025 // SPS ConsultantPlus.
2. On the organization that ensures the creation and operation of a multifunctional information exchange service: Order of the Government of the Russian Federation No. 1880-r dated July 12, 2025 // SPS ConsultantPlus.
3. The national messenger will be the digital platform MAX: website of the Ministry of Digital Development. URL: <https://digital.gov.ru/news/naczionalnym-messendzherom-stanet-czifrovaya-platforma-max> (accessed on 27.07.2025).
4. On Amendments to the Code of Administrative Offenses of the Russian Federation and the Federal Law "On Amendments to the Code of Administrative Offenses of the Russian Federation": Draft Law No. 755710-8 // SPS ConsultantPlus.