# ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ И КРЕДИТНЫХ ОРГАНИЗАЦИЙ

*Иванов Н.Ю.*[1]

***Ключевые слова:*** *правовое регулирование, государственные информационные системы, кредитные организации, информационная безопасность, критическая информационная инфраструктура, защита персональных данных, доступ пользователей, экспериментальный правовой режим, частно-государственное партнерство.*

***Аннотация***

***Цель работы.*** *Состоит в разработке предложений по совершенствованию организационно-правового обеспечения информационной безопасности при взаимодействии государственных ГИС и кредитных организаций на основе научного анализа тенденций развития нормативно-правовой базы.*

***Метод исследования.*** *Методологическую основу исследования составляет комплекс общенаучных и специальных юридических методов. С помощью анализа и синтеза удалось выявить основные тенденции правового регулирования информационной безопасности при взаимодействии ГИС и кредитных организаций. Логический метод послужил инструментом при формулировании выводов и рекомендаций.*

***Результаты исследования.*** *Для дальнейшего совершенствования данного режима предлагается обеспечить унификацию требований к информационной безопасности различных регуляторов (ФСБ, ФСТЭК, Банк России, Роскомнадзор) путем разработки межведомственных и комплексных стандартов и издания совместных нормативных правовых актов, специально предназначенных для правового регулирования деятельности ГИС при взаимодействии с кредитными организациями, а также стимулировать развитие частно-государственного партнерства в области обмена информацией о кибератаках, законодательно закрепив для его участников правовые гарантии конфиденциальности передаваемых данных, упростив порядок подключения частных владельцев объектов критической инфраструктуры к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак.*

*Доказана необходимость модернизации правового регулирования экспериментальных правовых режимов на финансовом рынке, в том числе в области информационной безопасности путем внесения изменений в Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации».*

*Установлено, что для усиления информационной безопасности при взаимодействии ГИС и кредитных организаций может потребоваться внести изменения в 28 главу Уголовного кодекса Российской Федерации в части ужесточения уголовной ответственности за неосторожные преступления в сфере компьютерной информации, а также предусмотреть дополнительную административную и дисциплинарную ответственность.*

**DOI: 10.24412/1994-1404-2026-3-00-29**

[1] ***Иванов Николай Юрьевич****, аспирант кафедры фундаментальной юриспруденции и международного права Российского университета адвокатуры и нотариата имени Г.Б. Мирзоева, г. Москва, Российская Федерация.*

*E-mail: nj_ivanov@mail.ru*

## Введение

В соответствии с национальными целями развития Российской Федерации, определенными Президентом Российской Федерации[2], перед Правительством Российской Федерации поставлена амбициозная задача: к 2030 году обеспечить «цифровую зрелость» в сфере государственного и муниципального управления, а также в ключевых отраслях экономики и социальной сферы. Для оценки прогресса в решении этой задачи правительство включило в систему индикаторов преимущественно показатели, отражающие долю пользователей различных ГИС[3]. Актуальной проблемой государственного управления остается организация взаимодействия ГИС и кредитных организаций при соблюдении требований информационной безопасности.

В Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[4] Федеральным законом от 07.04.2025 № 58-ФЗ[5] внесены существенные изменения по совершенствованию правового режима информационной безопасности ГИС прежде всего в банковской деятельности, которые потребовали от регуляторов значительно обновить их нормативную базу в указанной сфере (Банк России, ФСБ, ФСТЭК, Роскомнадзор).

В настоящее время государственные информационные системы (ГИС) активно используются кредитными организациями в целях поиска клиентов, идентификации, проверки, экспертизы клиентов и их бизнеса, мониторинга финансового состояния клиентов, осуществления мероприятий в целях сбора просроченной задолженности, а также во множестве других операций и действий, как предусмотренных законодательством в качестве обязательных, так и выполняемых банками по собственному усмотрению.

1 августа 2026 года на портале «Госуслуги» стартовал эксперимент по получению гражданами социальных льгот через их банковскую карту, сообщил Председатель Правительства Российской Федерации М.В. Мишустин на оперативном совещании со своими заместителями[6]. В сфере предоставления гражданам различных льгот начинается взаимодействие портала государственных услуг с платежной системой «МИР».

За период в 10—15 лет кредитные организации существенно расширили доступ к необходимой информации — появилась возможность оперативно запрашивать и получать нужные данные из ГИС. Параллельно происходило совершенствование законодательной базы, направленное на повышение прозрачности и открытости данных. Однако внедрение новых правовых норм выявило ряд серьезных проблем: утечки персональных данных и их последующее использование злоумышленниками; злоупотребление режимом коммерческой тайны в целях недобросовестной конкуренции; отмывание денег и финансирование терроризма (ОД/ФТ) как угрозы национальной безопасности; иные формы неправомерного использования информации.

В ответ на эти вызовы государство приняло комплекс мер: были разработаны новые правовые нормы, а действующие положения существенно ужесточены. В результате публичный доступ к ряду категорий информации оказался ограничен. В настоящее время на фоне контрсанкционной политики наблюдаются беспрецедентные шаги государства по ужесточению законодательства в области доступности информации, все новые и новые сведения и правоотношения подпадают под понятие информации ограниченного доступа.

Таким образом, доступность и открытость сведений ГИС, используемых кредитными организациями, с одной стороны, должны сочетаться с необходимостью защиты ГИС в кредитно-финансовой сфере, как объектов критической инфраструктуры. Обозначенные проблемы предопределяют одновременно сложность и важность указанных правоотношений для развития экономики, вследствие чего представляет научный интерес изучение проблематики перспективных направлений правового регулирования обеспечения информационной безопасности при взаимодействии ГИС и кредитных организаций.

## Сложный многоуровневый институт

Эффективное взаимодействие ГИС и кредитных организаций невозможно без создания надежной системы защиты информации. Обеспечение информационной безопасности этих систем является не просто технической задачей, но сложной правовой проблемой. Их правовой режим находится на стыке информационного, административного и финансового права, что порождает специфическую систему регулирования, характеризующуюся высокой степенью императивности, комплексностью и наличием перекрестных требований различных регуляторов.

Правовое регулирование взаимодействия ГИС и кредитных организаций при соблюдении требований информационной безопасности Российской Федерации представляет собой сложный многоуровневый институт. Федеральный закон от 27.07.2006 № 152-ФЗ

---

[2] Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» // Собрание законодательства РФ. 13.05.2024, № 20, ст. 2584.

[3] Постановление Правительства РФ от 28.01.2025 № 58 «Об утверждении методик расчета показателей для оценки эффективности деятельности высших должностных лиц субъектов Российской Федерации и деятельности исполнительных органов субъектов Российской Федерации» // Собрание законодательства РФ. 17.02.2025, № 7, ст. 605.

[4] Собрание законодательства РФ. 31.07.2017. № 31. (Часть I). Ст. 4736.

[5] Собрание законодательства РФ. 14.04.2025, № 15, ст. 1784.

[6] Правительство утвердило параметры эксперимента по использованию платежных карт «Мир» для предоставления отдельных мер соцзащиты // Портал Правительства России. URL: http://government.ru/docs/59432 (дата обращения: 15.08.2026).

«О персональных данных»[7] устанавливает императивные требования к конфиденциальности обработки персональных данных, определяя организационные и технические меры, обязательные для реализации операторами, к категории которых в полной мере относятся кредитные организации.

При этом пользователь ГИС, действуя от имени и в интересах оператора персональных данных, становится конечным исполнителем данных требований, и его действия по вводу, просмотру, модификации или передаче персональных данных в рамках взаимодействия с ГИС получают правовую оценку в контексте соблюдения установленных законом процедур.

Не менее значимую роль играет Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[8], который возлагает на кредитные организации обязанность по защите информации, связанной с финансовыми операциями клиентов, составляющей предмет банковской тайны. Доступ к таким сведениям через ГИС, например, при взаимодействии с Росфинмониторингом, обусловливает повышенную ответственность пользователя, поскольку утечка или искажение данной информации могут парализовать работу по противодействию противоправным финансовым потокам.

Особый правовой режим устанавливается Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[9], который относит банковскую и иную финансовую инфраструктуру к объектам критической информационной инфраструктуры.

Правовой статус банковской тайны, как краеугольного камня доверия в финансовой системе, закреплен в статье 26 Федерального закона «О банках и банковской деятельности»[10], где раскрывается ее содержание и круг субъектов, обязанных обеспечивать ее конфиденциальность. Пользователь, получая доступ к информации, составляющей банковскую тайну, через ГИС, принимает на себя бремя соблюдения данного режима, и его противоправные действия по разглашению таких сведений подпадают под действие не только административного, но и уголовного законодательства.

Уголовный кодекс Российской Федерации в статье 183 предусматривает санкцию за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. При этом уголовная ответственность может наступить, не только когда мотивом нарушения послужили корыстные цели или в результате хищения документов, но и в результате сбора информации, например, для предоставления в суд, когда такие действия нарушают правовой режим охраняемой законом тайны[11], а также требования локальных нормативных актов организации, должностных инструкций[12].

## Нарушение административного законодательства Российской Федерации в области защиты персональных данных

Законодатель не скрывает свои намерения по усилению мер административного воздействия в рассматриваемой области. Кодекс Российской Федерации об административных правонарушениях[13] содержит отдельный состав, непосредственно касающийся сферы персональных данных — статья 13.11, которая устанавливает административную ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Санкции по данной статье регулярно ужесточаются, а практика их применения расширяется, что свидетельствует о повышенном внимании законодателя и контролирующих органов к данному вопросу.

Примером может служить Федеральный закон от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[14], который дополнил статью 13.11 КоАП РФ новыми составами административных правонарушений, предусматривающими установление административной ответственности за утечки баз данных, содержащие персональные данные.

Как отмечалось в пояснительной записке к законопроекту, такие меры административного наказания станут существенным стимулом для инвестиций операторов персональных данных в информационную безопасность и окажут превентивное воздействие на операторов, не соблюдающих требования законодательства о персональных данных[15]. Для пользователя информационной системы это означает, что даже техническая ошибка, приведшая к неправомерному распространению персональных данных, может стать основанием для привлечения к административной ответственности с наложением существенного штрафа.

---

[7] Собрание законодательства РФ. 31.07.2006, № 31 (1 ч.), ст. 3451.

[8] Собрание законодательства РФ. 13.08.2001, № 33 (часть I), ст. 3418.

[9] Собрание законодательства РФ. 31.07.2017, № 31 (часть I), ст. 4736.

[10] Собрание законодательства РФ. 05.02.1996, № 6, ст. 492.

[11] Кассационное определение Четвертого кассационного суда общей юрисдикции от 11.11.2020 № 77-2402/2020 (УИД 23RS0031-01-2019-012379-77) // СПС «КонсультантПлюс».

[12] Определение Восьмого кассационного суда общей юрисдикции от 05.10.2021 по делу № 77-4019/2021 (УИД 42RS0009-01-2020-004129-23) // СПС «КонсультантПлюс».

[13] Собрание законодательства РФ. 07.01.2002, № 1 (ч. 1), ст. 1.

[14] Собрание законодательства РФ. 02.12.2024, № 49 (часть IV), ст. 7411.

[15] Пояснительная записка к проекту Федерального Закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество»). URL: https://sozd.duma.gov.ru (дата обращения: 21.10.2025).

### Нормативное регулирование Банка России

Наряду с федеральным законодательством, существенную регуляторную нагрузку несут нормативные акты Банка России, которые, обладая силой подзаконных актов, фактически выполняют роль прямых руководящих указаний для кредитных организаций. В частности, Положение Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»[16] детализирует технические и организационные стандарты безопасности.

Стандарт Банка России СТО БР ИББС-1.0-2014[17], принятые на его основе методические рекомендации Банка России[18] и иные стандарты[19], хотя и носящие рекомендательный характер, де-факто являются эталоном при построении систем защиты информации в банках. Внутренние (локальные) нормативные акты кредитной организации — Политика информационной безопасности, регламенты доступа в ГИС, должностные инструкции — завершают эту многоуровневую конструкцию. Их юридическое значение заключается в том, что они конкретизируют общие законодательные предписания применительно к специфике конкретного банка и рабочих мест. Ознакомление пользователя с этими документами под подпись является юридически значимым действием, преобразующим общие обязанности, вытекающие из закона, в конкретные трудовые функции. В случае возникновения инцидента именно соответствие или несоответствие действий пользователя положениям внутренних инструкций будет служить первоначальным доказательством при установлении его вины.

### Структура правового регулирования информационной безопасности при взаимодействии ГИС и кредитных организаций

Правовое регулирование информационной безопасности при взаимодействии ГИС и кредитных организаций представляет собой сложную, иерархически организованную систему, которую можно структурировать на четыре основных уровня.

1) Конституционный уровень. Основополагающие принципы, такие как право на тайну частной жизни, личную и семейную тайну (ст. 23 Конституции РФ), право на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 24 Конституции РФ), формируют фундамент для всего последующего регулирования.

2) Уровень федерального законодательства. Данный уровень включает в себя кодифицированные акты и федеральные законы, устанавливающие общие рамки:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: определяет базовые понятия, общие принципы обеспечения информационной безопасности;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: устанавливает обязательные требования к обработке персональных данных, которые в большом объеме обрабатываются в ГИС и информационных системах кредитных организаций;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: ключевой акт, поскольку большинство ГИС и информационных систем кредитных организаций отнесены к объектам КИИ. Закон вводит особый режим безопасности, включая обязательную категорирование объектов, их аттестацию и установление особых правил эксплуатации;
- Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»: наделяет Банк России нормотворческими полномочиями по установлению правил осуществления банковских операций, стандартов защиты информации;
- Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»: регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием и защитой, что актуально для некоторых сегментов ГИС финансового блока.

3) Уровень подзаконных нормативных правовых актов. На этом уровне конкретизируются требования законов. Ключевую роль здесь играют акты Банка России (Указания, Положения, Стандарты), ФСБ России, ФСТЭК России, устанавливающие:

- требования к системе защиты информации (СЗИ);
- порядок проведения оценки соответствия и аттестации;
- методики оценки ущерба и категорирования объектов КИИ;

---

[16] «Вестник Банка России», № 76, 21.12.2023.

[17] «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014» // «Вестник Банка России», № 48-49, 30.05.2014.

[18] Например, «Методические рекомендации Банка России по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка» (утв. Банком России 22.01.2025 № 2-МР) // «Вестник Банка России», № 7, 31.01.2025.

[19] Например, «Стандарт Банка России „Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect. Требования“ СТО БР ФАПИ.СЕК-1.6-2024» (принят и введен в действие приказом Банка России от 07.10.2024 № ОД-1615). URL: https://cbr.ru (дата обращения: 23.10.2025).

– технические стандарты и рекомендации по защите (например, серия руководящих документов ФСТЭК[20]).

4) Уровень международных стандартов и лучших практик. Несмотря на национальную специфику, при построении систем защиты активно применяются международные стандарты (ISO/IEC 27001, серия COBIT, PCI DSS), которые адаптируются к требованиям российского законодательства.

## Особенности правового режима информационных систем Банка России

Банк России выступает в этих правоотношениях и как мегарегулятор финансового рынка, устанавливающий обязательные для всех кредитных организаций требования, и как оператор собственных критически важных информационных систем. Эта двойственность определяет особенности правового режима его информационных систем.

Во-первых, информационные системы Банка России обрабатывают информацию, отнесенную к категории конфиденциальной, а в некоторых случаях — и к государственной тайне (например, сведения о золотовалютных резервах, планах по денежной эмиссии). Это влечет необходимость соблюдения не только требований ФЗ-187, но и строгого режима Закона «О государственной тайне», включая лицензирование деятельности по защите сведений и особый порядок допуска сотрудников.

Во-вторых, Банк России обладает нормотворческой автономией в установлении требований к безопасности своих систем. Он издает внутренние нормативные акты (например, Стандарт Банка России СТО БР ИББС-1.0), которые де-факто являются обязательными для исполнения его подразделениями и устанавливают эталон для всей банковской системы.

В-третьих, на Банк России возложены функции национального координатора по защите прав потребителей финансовых услуг и обеспечению стабильности финансового рынка. Сбой в работе его информационных систем (например, системы БЭСП) может привести к системному риску для всей национальной экономики, что предъявляет экстраординарные требования к отказоустойчивости, бесперебойности и доступности этих систем.

## Проблемы правового регулирования информационной безопасности ГИС при взаимодействии с кредитными организациями

Несмотря на развитую нормативную базу, в научной и экспертной среде все чаще обращается внимание на ряд системных проблем в правовом регулировании информационной безопасности ГИС при взаимодействии с кредитными организациями:

Во-первых, это дублирование и пересечение требований. О необходимости ликвидации устаревших положений, пробелов и дублирования норм в законодательстве, которые приводят не только к появлению противоречащих друг другу нормативных правил в области информационной безопасности, но и к пересечению контрольных функций органов власти в своих работах пишут такие крупные ученые, как профессор В.А. Вайпан [1], С.М. Зырянов [2].

Оператор ГИС, являющейся объектом КИИ и обрабатывающей персональные данные, вынужден одновременно выполнять зачастую разнонаправленные требования ФСБ, ФСТЭК, Роскомнадзора и Банка России. Это приводит к значительному росту финансовой и административной нагрузки. В то же время некоторые ученые считают возможным утверждать о наметившейся тенденции по унификации требований информационной безопасности [3].

Второй проблемой можно выделить проблему атрибуции киберинцидентов. Действующее законодательство не в полной мере регулирует процедуру официального установления виновных лиц в случае кибератаки на ГИС, что затрудняет привлечение их к ответственности и применение мер международного правового характера. С учетом повсеместного применения информационных технологий и повышением доступности их использования также повышаются возможности противоправного и злонамеренного их использования, в результате чего проблема атрибуции подобных атак становится наиболее актуальной. В этой связи А.Ж. Мартиросян считает необходимым принцип атрибуции кибератак возвести в специальный принцип новой отрасли права — международного информационного права [4].

В-третьих, жесткие технические требования зачастую не подкреплены адекватными нормами, стимулирующими повышение киберграмотности и личной ответственности сотрудников, имеющих доступ к ГИС. Профессор Е.Н. Клещина считает нехватку квалифицированных кадров в области информационной безопасности одной из проблем предупреждения преступлений, совершаемых работниками банков посредством информационных технологий [5].

Некоторые ученые полагают недостаточной только лишь уголовную ответственность за нарушение требований о безопасности критической информационной инфраструктуры Российской Федерации. Так, в частности, Д.Д. Савенкова в своей диссертации доказывает необходимость введения также административной

[20] Например, приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований по защите информации, не содержащей сведения, составляющие государственную тайну, содержащейся в государственных информационных системах» // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru, дата обращения: 24.09.2025.

и дисциплинарной ответственности субъектов критической информационной инфраструктуры за нарушение порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [6].

Правительство и Банк России уделяют повышенное внимание внедрению правовых актов, посвященных повышению финансовой и инвестиционной грамотности, финансовой киберграмотности, формировании основ финансовой культуры и рационального поведения.

Была принята Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 г.[21], разработаны и одобрены Советом директоров Банка России «Основные направления развития финансового рынка Российской Федерации на 2024 год и период 2025 и 2026 годов»[22]. Однако профессор Н.А. Поветкина [7] отмечает в этих документах разнонаправленный, несистемный способ формирования и закрепления правового категориального аппарата.

Четвертой проблемой является быстрое устаревание нормативной базы. Скорость развития новых цифровых явлений, в том числе киберугроз опережает скорость законотворческого процесса [8, 9]. Как отмечает А.К. Дубень [10], «современная национальная система правового обеспечения информационной безопасности в Российской Федерации, включая правовое регулирование, пока не в полной мере соответствует вызовам и рискам современности, в целом развивается недостаточно системно, без учета особенностей деятельностного характера средств и методов защиты информации, включая и экспериментальные правовые режимы в сфере цифровых инноваций». Технические требования, закрепленные в подзаконных актах, могут устаревать к моменту их вступления в силу, что снижает их эффективность. Некоторые ученые отмечают также необходимость своевременного определения в нормативных актах государственных регуляторов вводимых новых терминов для их применения в решении практических задач при использовании современных информационных технологий в обстановке усложнения угроз информационной безопасности [11].

## Выводы и предложения по правовому регулированию информационной безопасности ГИС при взаимодействии с кредитными организациями

Правовое регулирование информационной безопасности ГИС при взаимодействии с кредитными организациями представляет собой динамично развивающуюся, сложносоставную область. Ее ключевой особенностью является формирование специализированного правового режима, основанного на принципах максимальной защищенности, бесперебойности и подчинения строгому государственному контролю.

Для дальнейшего совершенствования данного режима представляется целесообразным следующее.

1) Обеспечить унификацию требований к информационной безопасности различных регуляторов (ФСБ, ФСТЭК, Банк России, Роскомнадзора). Сложность анализа «разнородных нормативных требований» и необходимость их интеграции в единую систему управления рисками информационной безопасности отмечается учеными экономистами, которые предлагают для систематизации законодательных норм внедрить матрицу риск-ориентированной интерпретации нормативных требований [12]. С правовой точки зрения, представляется, что для решения этих задач усилия должны быть направлены на разработку межведомственных и комплексных стандартов и издания совместных нормативных правовых актов, специально предназначенных для правового регулирования деятельности ГИС при взаимодействии с кредитными организациями. Необходимо отметить, что возможность издания нормативных правовых актов совместно несколькими федеральными органами исполнительной власти, а также Банком России совместно с федеральными органами исполнительной власти предусмотрена пунктом 3 «Правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации»[23], и пунктом 14.1 Положения Банка России от 22.09.2017 № 602-П «О Правилах подготовки нормативных актов Банка России»[24], однако, представляется, что в отсутствие законодательного требования об обязательности издания совместных нормативных правовых актов при межотраслевом регулировании такое опциональное правило не будет востребовано органами исполнительной власти, так как сопряжено с необходимостью межведомственного взаимодействия, создания рабочих групп, применения согласительных процедур, переговоров и прочих действий, которые сопряжены с риском трудно прогнозируемых результатов и нарушения плановых сроков внедрения нового регулирования.

2) Стимулировать развитие частно-государственного партнерства в области обмена информацией о кибератаках, закрепив для его участников правовые гарантии конфиденциальности передаваемых данных, упростив порядок подключения частных владельцев объектов критической инфраструктуры к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак,

[21] Распоряжение Правительства РФ от 24 октября 2023 г. № 2958-р «Об утверждении Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года» // Собрание законодательства РФ. 2023. № 45. Ст. 8091.

[22] «Вестник Банка России», № 5, 23.01.2024.

[23] Утверждены Постановлением Правительства Российской Федерации от 13.08.1997 № 1009 // Собрание законодательства РФ. 18.08.1997, № 33, ст. 3895.

[24] «Вестник Банка России», № 84, 29.09.2017.

создаваемой в целях предотвращения и устранения последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации (ГосСОПКА).

Следует отметить, что механизм взаимодействия кредитных организаций с регулирующими органами при выявлении компьютерных инцидентов, инцидентов защиты информации подробно урегулирован. При выявлении инцидентов кредитная организация в соответствии с пунктом 1 части 2 статьи 9 Федерального закона № 187-ФЗ направляет в Банк России с использованием технической инфраструктуры Банка России уведомление, содержащее сведения о выявленном инциденте, по форме и в порядке, установленным СТО БР БФБО-1.5-2023[25], а также в Национальный координационный центр по компьютерным инцидентам (далее — НКЦКИ) по форме и в порядке, установленным приказом ФСБ России № 282[26].

При этом в том случае, если кредитной организацией ранее было принято решение направлять информацию об инцидентах в НКЦКИ посредством Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России, дополнительное информирование НКЦКИ о данных событиях не требуется. Однако с учетом постоянно увеличивающегося количества субъектов рассматриваемых правоотношений и роста разнообразия оказываемых ими услуг звучат призывы расширить область применения режима взаимодействия кредитных организаций контролирующими органами.

3) Модернизировать правовое регулирование экспериментальных правовых режимов на финансовом рынке, в том числе в области информационной безопасности путем внесения изменений в Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации»[27] (далее — Закон об ЭПР). На портале Банка России размещена информация о поступлении всего двух инициативных предложений об установлении экспериментального правового режима по направлению «финансовый рынок». Одно из них было отклонено, второе рассматривается с мая 2026 года[28]. Банк России все еще только планирует внести изменение в законодательство с тем, чтобы появилась возможность изменять или исключать действие отдельных положений федеральных законов, что необходимо в целях создания правовых условий для пилотирования цифровых финансовых инноваций [13]. Однако, помимо этого, уже также очевидна необходимость дебюрократизации порядка и сокращения установленных Законом об ЭПР сроков рассмотрения инициатив по установлению ЭПР, в том числе в сфере информационной безопасности.

Реализация этих мер будет способствовать повышению устойчивости к современным угрозам информационной безопасности не только ГИС при взаимодействии с кредитными организациями, но и всей национальной финансовой системы.

4) Для укрепления информационной безопасности при взаимодействии ГИС и кредитных организаций необходимо внести изменения в главу 28 Уголовного кодекса Российской Федерации в части ужесточения уголовной ответственности за неосторожные преступления в сфере компьютерной информации, повлекшие значительный ущерб, а также предусмотреть административную и дисциплинарную ответственность, в том числе за нарушение порядка представления информации в систему ГосСОПКА. Безусловно решению современных вызовов информационной безопасности и уязвимостей ГИС могут способствовать такие предлагаемые учеными меры, как принятие новой Доктрины информационной безопасности [14], однако, по нашему мнению, более действенным будет кодификация многочисленных, зачастую разнополярных правовых актов, регулирующих информационные правоотношения и превращение Федерального Закона «Об информации…» № 149-ФЗ с его 70 изменениями и дополнениями в Информационный Кодекс с учетом значительного числа законодательных актов информационного права при взаимном проникновении правовых норм «финтеха» с включением отдельной главы, посвященной ответственности субъектов информационно-правовых отношений.

---

[25] «Стандарт Банка России «Безопасность финансовых (банковских) операций. Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности. О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности». Принят и введен в действие приказом Банка России от 08.02.2023 № ОД-215. URL: https://cbr.ru (дата обращения: 16.10.2025).

[26] Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». URL: http://pravo.gov.ru (дата обращения: 16.10.2025).

[27] Собрание законодательства РФ. 03.08.2020, № 31 (часть I), ст. 5017.

[28] Сведения о ходе рассмотрения поступивших инициативных предложений об установлении ЭПР. Портал Банка России. URL: https://cbr.ru/vfs/fintech/information_258-fz.xlsx (дата обращения: 18.08.2026).

**Литература**

1. Вайпан В.А. Источники цифрового права // Вестник арбитражной практики. 2024. № 1. С. 3—29.
2. Государство, общество и личность: пути преодоления вызовов и угроз в информационной сфере : монография / Н.С. Волкова, А.А. Ефремов, С.М. Зырянов и др.; отв. ред. Л.К. Терещенко. М. : Инфотропик Медиа, 2024. 352 с.
3. Финансовое право в условиях развития цифровой экономики : монография / К.Т. Анисина, Б.Г. Бадмаев, И.В. Бит-Шабо и др.; под ред. И.А. Цинделиани. М. : Проспект, 2019. 320 с.
4. Мартиросян А.Ж. Международно-правовое регулирование обеспечения безопасности в сфере использования информационно-коммуникационных технологий : дис. ... канд. юр. наук. М., 2024. С. 12.
5. Клещина Е.Н. Проблемы предупреждения преступлений, совершаемых посредством информационных технологий работниками банков // Вестник университета им. О.Е. Кутафина (МГЮА). 2025. № 5. С. 187.
6. Савенкова Д.Д. Институт юридической ответственности в системе правового обеспечения информационной безопасности в Российской Федерации : автореф. дис. ... канд. юрид. наук. М., 2019.
7. Поветкина Н.А. Финансово-правовая культура // Финансовое право. 2024. № 12. С. 2—5.
8. Бут Н.Д., Фомичев А.В. Особенности надзора за исполнением законов в кредитно-банковской сфере в условиях цифровой экономики // Право и цифровая экономика. 2024. № 1. С. 5—15.
9. Гулемин А.Н. Цифровые экосистемы в современном праве: анализ национальных и международных подходов // Электронное приложение к «Российскому юридическому журналу». 2024. № 5. С. 27—36.
10. Дубень А.К. Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации : дис. ... канд. юрид. наук: 5.1.2. М., 2023. 245 с. С. 175.
11. Метельков А.Н. Трансформация объекта защиты в условиях современных угроз безопасности информации // Правовая информатика. 2026. № 1. С. 44—51; с. 45.
12. Козырь Н.С., Бэк В.С. Риск-ориентированная интерпретация требований российского законодательства в сфере кибербезопасности // Правовая информатика. 2026. № 2. С. 52—61; с. 58, 59.
13. Ершова И.В., Тарасенко О.А. Изъятия норм федерального законодательства при установлении экспериментального правового режима // Хозяйство и право. 2025. № 7. С. 25—35.
14. Дубень А.К. Правовое обеспечение информационной безопасности Российской Федерации: нормативно-правовые основы и современные вызовы // Правовая информатика. 2026. № 1. С. 284—288; с. 287.

***SECTION:***
*REGULATORY INFORMATICS*

# ORGANIZATIONAL AND LEGAL SUPPORT FOR INFORMATION SECURITY IN THE INTERACTION BETWEEN STATE INFORMATION SYSTEMS AND CREDIT ORGANIZATIONS

***Ivanov N.Yu.*[29]**

***Keywords:*** *legal regulation, state information systems, credit organizations, information security, critical information infrastructure, personal data protection, user access, experimental legal regime, public-private partnership.*

***Abstract***

***Purpose of work.*** *To develop proposals for improving the organizational and legal framework for information security in the interaction between state information systems and credit organizations, based on a scientific analysis of trends in the development of the regulatory framework.*

***Research method.*** *The methodological basis of the study comprises a set of general scientific and special legal methods. Analysis and synthesis were used to identify the main trends in the legal regulation of information security in the interaction between state information systems and credit organizations. The logical method was applied in formulating conclusions and recommendations.*

[29] ***Nikolai Yu. Ivanov***, *Ph.D. student at the Department of Fundamental Jurisprudence and International Law of the Russian University of Advocacy and Notary Services named after G.B. Mirzoev, Moscow, Russian Federation.*
*E-mail: nj_ivanov@mail.ru*

***Results of the study.*** *To further improve this framework, it is proposed to unify information security requirements established by various regulators — the Federal Security Service, the Federal Service for Technical and Export Control, the Bank of Russia, and Roskomnadzor — by developing interagency and comprehensive standards and adopting joint regulatory legal acts specifically designed to regulate the activities of state information systems interacting with credit organizations.*

*The study also proposes promoting public-private partnerships in the field of information exchange concerning cyberattacks by establishing legal guarantees of confidentiality for the data transmitted by participants and simplifying the procedure for connecting private owners of critical infrastructure facilities to the state system for detecting, preventing, and eliminating the consequences of computer attacks.*

*The study demonstrates the need to modernize the legal regulation of experimental legal regimes in the financial market, including information security, by amending Federal Law No. 258-FZ of July 31, 2020 "On Experimental Legal Regimes in the Sphere of Digital and Technological Innovations in the Russian Federation".*

*It was established that strengthening information security in the interaction between state information systems and credit organizations may require amendments to Chapter 28 of the Criminal Code of the Russian Federation to increase criminal liability for negligent computer-related offenses, as well as to introduce additional administrative and disciplinary liability.*

**References**

1. Vaipan V.A. Istochniki tsifrovogo prava // Vestnik arbitrazhnoi praktiki. 2024. No. 1. S. 3—29.
2. Gosudarstvo, obshchestvo i lichnost': puti preodoleniia vyzovov i ugroz v informatsionnoi sfere : monografiia / N.S. Volkova, A.A. Efremov, S.M. Zyrianov i dr.; otv. red. L.K. Tereshchenko. M. : Infotropik Media, 2024. 352 s.
3. Finansovoe pravo v usloviiakh razvitiia tsifrovoi ekonomiki : monografiia / K.T. Anisina, B.G. Badmaev, I.V. Bit-Shabo i dr.; pod red. I.A. Tsindeliani. M. : Prospekt, 2019. 320 s.
4. Martirosian A.Zh. Mezhdunarodno-pravovoe regulirovanie obespecheniia bezopasnosti v sfere ispol'zovaniia informatsionno-kommunikatsionnykh tekhnologii : dis. ... kand. iur. nauk. M., 2024. S. 12.
5. Kleshchina E.N. Problemy preduprezhdeniia prestuplenii, sovershaemykh posredstvom informatsionnykh tekhnologii rabotnikami bankov // Vestnik universiteta im. O.E. Kutafina (MGIuA). 2025. No. 5. S. 187.
6. Savenkova D.D. Institut iuridicheskoi otvetstvennosti v sisteme pravovogo obespecheniia informatsionnoi bezopasnosti v Rossiiskoi Federatsii : avtoref. dis. ... kand. iurid. nauk. M., 2019.
7. Povetkina N.A. Finansovo-pravovaia kul'tura // Finansovoe pravo. 2024. No. 12. S. 2—5.
8. But N.D., Fomichev A.V. Osobennosti nadzora za ispolneniem zakonov v kreditno-bankovskoi sfere v usloviiakh tsifrovoi ekonomiki // Pravo i tsifrovaia ekonomika. 2024. No. 1. S. 5—15.
9. Gulemin A.N. Tsifrovye ekosistemy v sovremennom prave: analiz natsional'nykh i mezhdunarodnykh podkhodov // Elektronnoe prilozhenie k "Rossiiskomu iuridicheskomu zhurnalu". 2024. No. 5. S. 27—36.
10. Duben' A.K. Pravovoe obespechenie informatsionnoi bezopasnosti v sisteme informatsionnogo prava v Rossiiskoi Federatsii : dis. ... kand. iurid. nauk: 5.1.2. M., 2023. 245 s. S. 175.
11. Metel'kov A.N. Transformatsiia ob"ekta zashchity v usloviiakh sovremennykh ugroz bezopasnosti informatsii // Pravovaia informatika. 2026. No. 1. S. 44—51; s. 45.
12. Kozyr' N.S., Bek V.S. Risk-orientirovannaia interpretatsiia trebovanii rossiiskogo zakonodatel'stva v sfere kiberbezopasnosti // Pravovaia informatika. 2026. No. 2. S. 52—61; s. 58, 59.
13. Ershova I.V., Tarasenko O.A. Iz"iatiia norm federal'nogo zakonodatel'stva pri ustanovlenii eksperimental'nogo pravovogo rezhima // Khoziaistvo i pravo. 2025. No. 7. S. 25—35.
14. Duben' A.K. Pravovoe obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii: normativno-pravovye osnovy i sovremennye vyzovy // Pravovaia informatika. 2026. No. 1. S. 284—288; s. 287.