ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ КАК ОПОРНАЯ ИНФРАСТРУКТУРА НАЦИОНАЛЬНОЙ ПЛАТЁЖНОЙ СИСТЕМЫ: ПРАВОВОЙ РЕЖИМ НЕДОСТУПНОСТИ

Лобанов Н.А.[1]

Ключевые слова: *противодействие мошенничеству, перевод денежных средств без добровольного согласия, оператор по переводу денежных средств, оператор связи, сертификат безопасности, удостоверяющий центр, обязанности оператора, сроки исполнения обязанностей, ответственность, непрерывность функционирования, публичное обсуждение проектов актов.*

Аннотация

Цель: *определить, какими нормами установлены последствия недоступности государственных информационных систем для участников национальной платёжной системы, обязанных с 2027 года использовать такие системы, и предложить модель полноты соответствующего правового режима.*

Метод исследования: *формально-юридический анализ Федерального закона от 26 июня 2026 г. № 210-ФЗ и изменённых им законов, а также проектов подзаконных актов, размещённых на федеральном портале проектов нормативных правовых актов в июле и августе 2026 г. Сравнительно-правовым методом рассмотрены подходы к ответственности поставщиков доверенных услуг, а также к распределению рисков третьих сторон в финансовом секторе. В исследовании использованы материалы публичного обсуждения четырёх проектов актов; их анализ позволил оценить полноту правового регулирования по авторской модели правового режима, элементы которой проверяются в тексте закона, в первых редакциях проектов и в позициях разработчиков.*

Результаты: *выделены три государственные информационные системы, обращение к которым становится условием исполнения обязанностей операторами по переводу денежных средств и операторами связи: система противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, единая система учёта платёжных карт и государственная информационная система национального удостоверяющего центра. Показано, что закон в каждом случае устанавливает обязанность участника и последствия её неисполнения, но не устанавливает ни требований к доступности системы, ни порядка действий участника при её недоступности, ни влияния недоступности на течение сроков и наступление ответственности. Предложена модель правового режима опорной государственной информационной системы из восьми элементов и показатель его полноты; рассчитаны значения показателя для трёх систем на уровне закона и проектов подзаконных актов. Установлено, что элементы режима недоступности появляются только на подзаконном уровне и только по итогам публичного обсуждения: по проекту правил возмещения оператором связи разработчик отметил учтённым предложение автора о приостановлении сроков на период недоступности системы. Сформулированы предложения о закреплении режима недоступности на уровне закона.*

DOI: 10.24412/1994-1404-2026-3-00-31

Введение и постановка задачи

Федеральный закон от 26 июня 2026 г. № 210-ФЗ[2] (далее — Закон № 210-ФЗ) завершил формирование правовой конструкции, в которой исполнение обязанностей участниками национальной платёжной системы поставлено в зависимость от государственных информационных систем. С 1 марта 2027 г. оператор по переводу денежных средств при проверке признаков перевода без добровольного согласия

[2] Федеральный закон от 26 июня 2026 г. № 210-ФЗ "О внесении изменений в Федеральный закон "О связи" и отдельные законодательные акты Российской Федерации" // Собрание законодательства Российской Федерации. 2026. № 26. Ст. 3464.

[1] ***Лобанов Николай Александрович****, независимый эксперт по информационной безопасности и защите критической информационной инфраструктуры, магистрант Института права и национальной безопасности РАНХиГС при Президенте Российской Федерации, г. Москва, Российская Федерация. ORCID: 0009-0006-8187-4528.*

E-mail: nlobanov-25@ranepa.ru

клиента обязан использовать сведения, полученные посредством государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий (часть 3.1 статьи 8 Федерального закона «О национальной платёжной системе»[3] в редакции Закона № 210-ФЗ). С 1 сентября 2027 г. тот же оператор до предоставления клиенту платёжной карты обязан запросить сведения в единой системе учёта платёжных карт и обязан отказать в предоставлении карты, если её выдача нарушит установленное количественное ограничение (части 2.3 и 2.4 статьи 9 того же закона). Органы и организации, указанные в части 2.3 статьи 13 Федерального закона «Об информации, информационных технологиях и о защите информации»[4], обязаны осуществлять электронное взаимодействие с применением сертификатов безопасности национального удостоверяющего центра, а Правительство Российской Федерации вправе установить случаи обязательного использования таких сертификатов в банковской сфере (части 12 и 13 статьи 14.1 Федерального закона «Об электронной подписи»[5] в редакции Закона № 210-ФЗ).

Общая черта этих норм в том, что обязанность участника исполнима только при работоспособности системы, которая ему не принадлежит и им не управляется. При этом последствия неисполнения обязанности закон устанавливает прямо: оператор по переводу денежных средств, исполнивший распоряжение клиента после получения посредством системы сведений об абонентском номере, возмещает клиенту сумму перевода (часть 3.13-1 статьи 8 Федерального закона "О национальной платёжной системе"), оператор связи возмещает сумму перевода при несоблюдении требований о направлении сведений в систему и о приостановлении оказания услуг по полученной из неё информации (часть 11 статьи 1 Федерального закона от 1 апреля 2025 г. № 41-ФЗ[6] в редакции Закона № 210-ФЗ).

В настоящей работе такие системы обозначаются как опорные государственные информационные системы национальной платёжной системы. Термин выбран по функциональному признаку: система является опорной для участника, если обращение к ней составляет условие исполнения его публичной обязанности, а отказ системы не освобождает участника от последствий неисполнения. Это определение отличает рассматриваемые системы от информационных систем, используемых участниками по собственному усмотрению, и от систем, в которых участник выступает лишь поставщиком сведений.

Постановка задачи. Требуется установить, какими нормами определены последствия недоступности опорной государственной информационной системы для обусловленной ею обязанности участника: течение сроков, наступление ответственности, порядок действий участника в период недоступности, а также доказательственная база для подтверждения факта недоступности. Для этого необходимо: 1) выделить круг опорных систем по тексту Закона № 210-ФЗ; 2) сформировать перечень элементов правового режима, без которых обязанность, обусловленная системой, не может считаться исполнимой; 3) проверить наличие этих элементов в законе и в проектах подзаконных актов; 4) оценить, восполняются ли пробелы закона на подзаконном уровне и какую роль в этом играет публичное обсуждение проектов. Эмпирическую основу составили материалы публичного обсуждения четырёх проектов актов, в котором автор участвовал лично.

Степень разработанности темы. Правовая модель информационной системы и статус её оператора исследованы в работах А.Н. Метелькова, который показал, что законодательная конструкция понятия "информационная система" не включает субъекта права как элемент [1] и что термин "оператор" в законодательстве и стандартах многозначен, а требования регуляторов должны строго соответствовать субъектам, наделённым обязанностью их исполнять [2]. Развитие государственных информационных систем как платформ и экосистем государственных услуг рассмотрено Н.А. Троян [3], этапы правовой информатизации и задачи цифрового суверенитета исследованы Т.А. Поляковой и Н.А. Троян [4]. А.К. Дубень обосновывает необходимость единого правового режима защиты государственных информационных систем, систем персональных данных и объектов критической информационной инфраструктуры [5]; Д.А. Ловцов и А.С. Бурый рассматривают киберустойчивость как целевой фактор обеспечения кибербезопасности критически важных объектов [6]. Правовые основы противодействия мошенничеству на финансовом рынке систематизированы М.В. Хадеевой и Е.К. Овчинниковым, которые выделяют институциональные, организационные и функциональные основы национальной антифрод-системы и приводят архитектуру её финансового сегмента [7]; эволюция законодательства о противодействии кибермошенничеству вплоть до создания единого информационного пространства безопасности описана В.А. Гаужаевой и Е.В. Прокофьевой [8]. Распределение ответственности между банком и клиентом при дистанционном обслуживании исследовано П.С. Шуваловым и Н.В. Огановой [9]. Ответственность лиц, оказывающих доверенные услуги, как фактор доверия к цифровому

---

[3] Федеральный закон от 27 июня 2011 г. № 161-ФЗ "О национальной платежной системе" // Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872.

[4] Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

[5] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" // Собрание законодательства Российской Федерации. 2011. № 15. Ст. 2036.

[6] Федеральный закон от 1 апреля 2025 г. № 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" // Собрание законодательства Российской Федерации. 2025. № 14. Ст. 1574.

взаимодействию рассмотрена Н.И. Соловяненко [10]. Зарубежные исследования затрагивают смежные вопросы: состояние механизмов отзыва сертификатов в веб-инфраструктуре открытых ключей [11], последствия нормативного включения сертификатов, выпущенных по правилам публичного регулирования, в программы для доступа к сайтам [12], распределение ответственности за риски третьих сторон между банками, регуляторами и поставщиками технологий по регламенту Европейского союза об операционной устойчивости [13, 14], системный риск концентрации облачных услуг [15] и устойчивость инфраструктуры доменных имён, обслуживающей государственные сервисы [16].

Вместе с тем в известной автору литературе не рассматривался вопрос о правовых последствиях недоступности государственной информационной системы для обязанностей частных лиц, обусловленных обращением к ней. Настоящая работа восполняет этот пробел на материале Закона № 210-ФЗ.

Научная новизна состоит в предложенной модели правового режима опорной государственной информационной системы, в расчёте показателя полноты режима для трёх систем и в эмпирическом установлении того, на каком уровне регулирования и в результате какой процедуры элементы режима недоступности появляются в тексте актов.

РЕШЕНИЕ ЗАДАЧИ

Круг опорных систем по Закону № 210-ФЗ

Анализ Закона № 210-ФЗ позволяет выделить три государственные информационные системы, обращение к которым обусловливает обязанности участников национальной платёжной системы.

Первая система создана Федеральным законом от 1 апреля 2025 г. № 41-ФЗ. Закон № 210-ФЗ расширяет обязанности её пользователей: они обязаны принимать меры, направленные на предотвращение и пресечение противоправных действий, и передавать в систему сведения о выявленных признаках таких действий (часть 6 статьи 1 Федерального закона № 41-ФЗ). Для оператора связи установлены обязанности выявлять по критериям, утверждаемым Правительством Российской Федерации, абонентские номера, используемые для противоправных вызовов и сообщений, направлять сведения о них в систему и приостанавливать оказание услуг по номерам, сведения о которых получены посредством системы (часть 10 той же статьи). Для оператора по переводу денежных средств установлены обязанность использовать сведения системы при проверке признаков перевода без добровольного согласия (часть 3.1 статьи 8 Федерального закона "О национальной платёжной системе"), учёт таких сведений при выявлении операций с признаками перевода без добровольного согласия (пункт 6 части 3.5 той же статьи), а также обязанность направить оператору связи через систему обращение клиента о возмещении (часть 3.13-5 той же статьи, часть 13 статьи 1 Федерального закона № 41-ФЗ). Обязанность возмещения при неисполнении этих требований возложена на оператора по переводу денежных средств (части 3.13-1, 3.13-2 статьи 8) и на оператора связи (части 11 и 14 статьи 1 Федерального закона № 41-ФЗ). Порядок взаимодействия операторов при возмещении устанавливается Правительством Российской Федерации по согласованию с Банком России (часть 13 статьи 1 Федерального закона № 41-ФЗ); соответствующий проект постановления размещён на федеральном портале проектов нормативных правовых актов под идентификатором 02/07/07-26/00169315[7] (далее — проект правил возмещения), проект критериев абонентских номеров под идентификатором 02/07/07-26/00169312[8].

Вторая система, единая система учёта платёжных карт, введена статьёй 9.2 Федерального закона "О национальной платёжной системе" в редакции Закона № 210-ФЗ. Её оператором является оператор национальной системы платёжных карт, пользователями являются Банк России и операторы по переводу денежных средств (части 2 и 4 статьи 9.2). Оператор системы обязан обеспечивать её функционирование, защиту содержащейся в ней информации и предоставление операторам по переводу денежных средств сведений о количестве карт, предоставленных клиенту (часть 6 той же статьи). Оператор по переводу денежных средств обязан направлять в систему сведения о предоставленных картах (часть 7), обязан запросить сведения до предоставления карты и обязан отказать в предоставлении карты при превышении ограничения в двадцать карт (части 2.2 и 2.4 статьи 9). Порядок формирования и ведения системы и правила предоставления сведений устанавливаются нормативными актами Банка России (части 3 и 8 статьи 9.2); этот уровень регулирования в настоящей статье не анализируется.

Третья система, государственная информационная система национального удостоверяющего центра, введена статьёй 13.1 Федерального закона "Об электронной подписи" в редакции Закона № 210-ФЗ. Национальный удостоверяющий центр является федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

---

[7] Проект постановления Правительства Российской Федерации "Об утверждении правил взаимодействия оператора по переводу денежных средств и оператора связи при возмещении суммы перевода денежных средств, осуществленного без добровольного согласия физического лица" (ID 02/07/07-26/00169315) // Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/projects/169315 (дата обращения: 03.09.2026).

[8] Проект постановления Правительства Российской Федерации "Об утверждении критериев абонентских номеров, которые используются в целях совершения телефонных вызовов и (или) направления коротких текстовых сообщений, имеющих признаки совершения противоправных действий, и абонентских номеров, на которые совершаются телефонные вызовы и (или) направляются короткие текстовые сообщения, имеющие признаки совершения противоправных действий" (ID 02/07/07-26/00169312) // Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/projects/169312 (дата обращения: 03.09.2026).

он создаёт сертификаты безопасности, прекращает их действие, подтверждает владение ключом идентификации, ведёт реестр сертификатов безопасности и обеспечивает доступ к нему любым лицам (часть 1 статьи 13.1). Создание, выдача и прекращение действия сертификатов осуществляются с использованием государственной информационной системы национального удостоверяющего центра, оператор которой определяется Правительством Российской Федерации (части 5 и 7 той же статьи). Сертификат безопасности удостоверяет присвоение ключа аутентификации информационной системе или сайту и используется для обеспечения устойчивого и защищённого взаимодействия с ними (часть 1 статьи 14.1). Обязательность применения сертификатов установлена для органов и организаций по части 2.3 статьи 13 Федерального закона "Об информации, информационных технологиях и о защите информации" (часть 12 статьи 14.1), а для банковской сферы может быть установлена Правительством Российской Федерации по согласованию с Банком России (часть 13 той же статьи). Случаи прекращения действия сертификата помимо трёх законных устанавливаются Правительством Российской Федерации (пункт 4 части 7 статьи 14.1); соответствующий проект размещён под идентификатором 02/07/08-26/00170134[9]. Требования к сертификатам и к порядку их создания, выдачи, использования и прекращения действия устанавливаются уполномоченным органом (подпункт "а" пункта 9 части 4 статьи 8 Федерального закона "Об электронной подписи"); проект приказа размещён под идентификатором 02/08/08-26/00170667[10].

Три системы различаются по субъекту оператора (федеральный орган исполнительной власти, оператор национальной системы платёжных карт, орган или организация, определяемые Правительством Российской Федерации), по кругу пользователей и по характеру обязанности участника. Общим для них является то, что обязанность участника не может быть исполнена без работоспособной системы: оператор по переводу денежных средств не может использовать сведения, которые система не передала, не может запросить систему учёта карт, если она не отвечает, и не может организовать защищённое взаимодействие с применением сертификата, если реестр сертификатов недоступен для проверки его статуса.

[9] Проект постановления Правительства Российской Федерации "О случаях, при которых сертификат безопасности национального удостоверяющего центра прекращает свое действие" (ID 02/07/08-26/00170134, размещён 10.08.2026) // Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/projects/170134 (дата обращения: 03.09.2026).

[10] Проект приказа Минцифры России "Об утверждении требований к сертификатам безопасности национального удостоверяющего центра, порядку создания, выдачи, использования и прекращения действия таких сертификатов" (ID 02/08/08-26/00170667, размещён 28.08.2026) // Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/projects/170667 (дата обращения: 03.09.2026).

Модель правового режима опорной государственной информационной системы

Для проверки полноты регулирования предлагается описывать правовой режим опорной государственной информационной системы как множество из восьми элементов R = {r1, ..., r8}, каждый из которых отвечает на один вопрос, возникающий у обязанного лица при отказе системы.

r1. Определённость оператора системы и его обязанности обеспечивать её функционирование.

r2. Обусловленность обязанности участника обращением к системе: норма прямо связывает исполнение обязанности с получением сведений из системы или с передачей сведений в неё.

r3. Последствия неисполнения обусловленной обязанности для участника: возмещение, отказ в совершении операции, иная ответственность.

r4. Требования к доступности системы: показатель доступности, предельное время восстановления, порядок плановых работ.

r5. Порядок действий участника при недоступности системы: допустимый альтернативный способ исполнения обязанности либо прямое указание на её приостановление.

r6. Влияние недоступности на течение сроков и наступление ответственности: приостановление сроков, исчисляемых от событий в системе, и освобождение участника от последствий неисполнения за период недоступности.

r7. Фиксация периодов недоступности оператором системы и уведомление участников: доказательственная база, на которую участник может сослаться.

r8. Возможность участника проверить состояние сведений системы на заданный момент: выписка, реестр, журнал, доступный участнику.

Элементы r1, r2, r3 описывают, как система встроена в обязанность участника; элементы r4, r5, r6, r7, r8 описывают режим её недоступности. Для каждой системы и каждого уровня регулирования элемент оценивается как присутствующий (1), присутствующий частично (0,5) или отсутствующий (0). Показатель полноты режима K определяется как отношение суммы оценок к числу элементов; отдельно рассчитывается показатель полноты режима недоступности Kн по элементам r4 — r8. Модель не претендует на измерение качества нормы; она фиксирует, на какие из восьми вопросов текст акта даёт ответ.

Уровни регулирования: L1, федеральный закон в редакции Закона № 210-ФЗ; L2, проект подзаконного акта в первой опубликованной редакции; L3, позиция разработчика по итогам публичного обсуждения, зафиксированная в сводке предложений или в ответе на странице обсуждения. Уровень L3 отражает письменное намерение разработчика; доработанные редакции рассмотренных проектов на момент подготовки статьи не опубликованы, поэтому текстом акта этот уровень не подтверждён.

Применение модели

Система противодействия правонарушениям. На уровне закона элемент r1 присутствует частично: пользователи системы и их обязанности определены, обязанность оператора системы обеспечивать её функционирование и его ответственность перед пользователями в анализируемых нормах не конкретизированы. Элементы r2 и r3 присутствуют полностью: обязанность использовать сведения системы и возмещение при её неисполнении установлены прямо. Элементы r4 — r8 в законе отсутствуют. Проект правил возмещения в первой редакции связывает каждый срок процедуры с событием в системе: датой получения документа считается дата формирования системой уведомления о его доставке (пункт 3 правил), оператор связи клиента определяется оператором системы в срок не более трёх рабочих дней (пункт 8), обращение доставляется системой (пункт 9), сведения о возмещении вносятся в систему (пункт 30), контрольная сверка проводится оператором системы по её неизменяемым журналам (пункты 31 и 32). Проект предусматривает выписки из системы по состоянию на заданный момент времени и неизменяемые журналы (пункт 3 постановления, пункт 7 правил), что даёт элемент r8 и частично элемент r7. Элементы r4, r5 и r6 в первой редакции отсутствуют: текст не отвечает на вопрос, что происходит со сроками, если система не формирует уведомление о доставке.

Автором в ходе публичного обсуждения проекта правил возмещения было направлено предложение о дополнении правил положением, по которому при недоступности системы течение всех сроков, установленных правилами, приостанавливается, периоды недоступности фиксируются в неизменяемых журналах и учитываются при контрольной сверке, а также предложения об увеличении интервала сверки и о сроке перенаправления обращения надлежащему оператору связи. Согласно сводке предложений, сформированной разработчиком 29 июля 2026 г., позиция автора отмечена как частично учтённая: первое и третье предложения отмечены учтёнными, интервал сверки увеличен с четырёх до шести часов вместо предложенных двадцати четырёх с мотивировкой синхронизации с признаками перевода без добровольного согласия, установленными Банком России. Таким образом, на уровне L3 элемент r6 присутствует, а элемент r7 усиливается за счёт фиксации периодов недоступности. Из двух других участников обсуждения позиция одной кредитной организации отмечена как не учтённая, позиция другой как частично учтённая. По проекту критериев абонентских номеров предложения автора, направленные на защиту от внесения в систему номеров добросовестных абонентов и на закрепление порядка исключения сведений, отмечены частично учтёнными, но по существу не приняты: разработчик сообщил, что возможность исключения номера будет реализована технически на едином портале государственных услуг. Для режима недоступности этот результат значения не имеет, но он показывает, что элемент r8 в части исправления сведений системы разработчик относит к организационному, а не к нормативному уровню.

Единая система учёта платёжных карт. На уровне закона элемент r1 присутствует полностью: оператор назван, обязанность обеспечивать функционирование системы установлена (пункт 1 части 6 статьи 9.2). Элемент r2 присутствует: запрос в систему до предоставления карты обязателен. Элемент r3 присутствует частично: закон устанавливает обязанность отказать в предоставлении карты, но не устанавливает специальных последствий выдачи карты без запроса. Элемент r8 присутствует частично: оператор системы обязан предоставлять сведения, однако форма подтверждения состояния сведений на момент запроса законом не определена. Элементы r4 — r7 отсутствуют. Поскольку подзаконное регулирование отнесено к нормативным актам Банка России, уровни L2 и L3 для этой системы в настоящей работе не оцениваются.

Государственная информационная система национального удостоверяющего центра. На уровне закона элемент r1 присутствует полностью: национальный удостоверяющий центр является федеральным органом, его функции и обязанности перечислены, установлена его ответственность (части 1, 2 и 9 статьи 13.1). Элемент r2 присутствует: обязательность применения сертификатов установлена для определённого круга органов и организаций и может быть распространена на банковскую сферу. Элемент r3 присутствует частично: последствия неприменения сертификата для обязанного лица в рассматриваемых нормах не конкретизированы. Элемент r8 присутствует полностью: реестр сертификатов безопасности с датами и основаниями прекращения действия доступен любым лицам (пункты 4 и 5 части 1 статьи 13.1). Элемент r7 присутствует частично: срок внесения сведений о прекращении действия в реестр установлен только для прекращения по заявлению и по соглашению (часть 8 статьи 14.1) и не установлен для случаев, определяемых Правительством Российской Федерации. Элементы r4, r5 и r6 отсутствуют.

Проект постановления о случаях прекращения действия сертификата в первой редакции содержит четыре случая, текстуально воспроизводящие основания прекращения действия и аннулирования сертификата ключа проверки электронной подписи из частей 6 и 6.1 статьи 14 Федерального закона "Об электронной подписи": решение суда о недостоверности сведений, прекращение деятельности центра без перехода функций, отсутствие у владельца ключа идентификации, наличие ключа аутентификации в ранее созданном сертификате. Для случаев, описанных безличной конструкцией "если установлено", проект не определяет ни субъекта установления, ни момента прекращения действия. Проект приказа о требованиях к сертификатам в части порядка их создания, выдачи, использования и прекращения действия ограничивается перечнем разделов порядка, который затем утверждает сам

национальный удостоверяющий центр; требований к периодичности издания списков прекративших действие сертификатов, к доступности сервисов проверки статуса и к действиям при недоступности системы центра проект не содержит. Иными словами, на уровне L2 для этой системы элементы r4 — r6 отсутствуют, а элемент r7 остаётся частичным. Предложения автора по обоим проектам, направленные 2 сентября 2026 г. и включающие момент прекращения действия сертификата со дня записи в реестре, срок такой записи, уведомление владельца и порядок действий при недоступности инфраструктуры центра, на момент подготовки статьи результатами рассмотрения не подтверждены: публичное обсуждение первого проекта завершено 7 сентября 2026 г., второго продолжается до 25 сентября 2026 г.

Результаты применения модели сведены в таблицу (табл. 1).

Обозначения: СПП, система противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий; ЕСУПК, единая система учёта платёжных карт; ГИС НУЦ, государственная информационная система национального удостоверяющего центра; L1, L2, L3, уровни регулирования по разделу о модели правового режима. Источник: составлено автором по текстам Закона № 210-ФЗ и изменённых им законов, первых редакций проектов 02/07/07-26/00169315, 02/07/08-26/00170134 и 02/08/08-26/00170667, сводки предложений по проекту 02/07/07-26/00169315 от 29 июля 2026 г.

Интерпретация

Из значений (табл. 1) следуют три наблюдения.

Первое. На уровне закона показатель полноты режима недоступности не превышает 0,3 ни для одной из трёх систем; для системы противодействия правонарушениям он равен нулю. Закон подробно описывает, что участник обязан сделать с использованием системы и что произойдёт, если он этого не сделает, но не описывает, что происходит с обязанностью, если система недоступна. Такая асимметрия объяснима генезисом норм: они писались как нормы об обязанностях частных лиц, а система рассматривалась как средство исполнения, надёжность которого презюмируется. В терминах модели А.Н. Метелькова, где информационная система в законодательной конструкции лишена субъекта [1], а требования регулятора должны адресоваться субъекту, обязанному их исполнять [2], можно сказать, что режим недоступности не имеет адресата: обязанность обеспечивать функционирование системы либо вовсе не выражена (система противодействия правонарушениям), либо выражена без показателей и без последствий для участников (единая система учёта платёжных карт, система национального удостоверяющего центра).

Второе. Элементы режима недоступности появляются на подзаконном уровне, причём в наиболее полном виде только по итогам публичного обсуждения. Проект правил возмещения в первой редакции дал элементы r7 и r8, потому что сама процедура сверки требует неизменяемых журналов и выписок; элемент r6 появился в позиции разработчика после предложения участника обсуждения. Для системы национального удостоверяющего центра проекты подзаконных актов элементов r4 — r6 не добавили; порядок, в котором такие элементы могли бы появиться, отнесён к документу самого центра, не проходящему публичное обсуждение. Это согласуется с выводом Н.И. Соловяненко о том, что отсутствие ясности в распределении ответственности является одним из главных факторов, препятствующих доверию к электронным услугам [10]: для сертификата, применение которого обязательно, неопределённость момента прекращения его действия и порядка действий при недоступности реестра прямо влияет на исполнимость обязанности пользователя.

Таблица 1

Полнота правового режима опорных государственных информационных систем национальной платёжной системы по уровням регулирования

Элемент режима	СПП, L1	СПП, L2	СПП, L3	ЕСУПК, L1	ГИС НУЦ, L1	ГИС НУЦ, L2
r1 оператор и его обязанность обеспечивать функционирование	0,5	0,5	0,5	1	1	1
r2 обусловленность обязанности участника	1	1	1	1	1	1
r3 последствия неисполнения для участника	1	1	1	0,5	0,5	0,5
r4 требования к доступности	0	0	0	0	0	0
r5 порядок действий при недоступности	0	0	0	0	0	0
r6 влияние недоступности на сроки и ответственность	0	0	1	0	0	0
r7 фиксация недоступности и уведомление	0	0,5	1	0	0,5	0,5
r8 проверка состояния сведений	0	1	1	0,5	1	1
K, полнота режима	0,31	0,50	0,69	0,38	0,50	0,50
Kн, полнота режима недоступности	0,00	0,30	0,60	0,10	0,30	0,30

Третье. Между тремя системами обнаруживается различие в исходной полноте, объясняемое не значимостью системы, а способом её появления в законе. Единая система учёта платёжных карт и система национального удостоверяющего центра введены статьями, посвящёнными самим системам, поэтому оператор и его обязанности названы (r1 равен единице). Система противодействия правонарушениям введена отдельным законом, а Закон № 210-ФЗ добавляет к нему обязанности пользователей; поэтому в анализируемых нормах обязанность оператора системы перед пользователями остаётся невыраженной. При этом именно для этой системы последствия неисполнения обязанности участника наиболее тяжёлые: возмещение суммы перевода.

Сравнительно-правовой контекст

Зарубежный опыт показывает, что вопрос о последствиях отказа опорной инфраструктуры для обязанных лиц решается в двух плоскостях. В отношении инфраструктуры открытых ключей Д. Бербекару и А. Лиой показывают, что механизмы отзыва сертификатов реализованы неполно и по-разному в разных программах, отчего статус сертификата остаётся неопределённым для проверяющей стороны [11]. Дискуссия о квалифицированных сертификатах аутентификации сайтов по регламенту Европейского союза показала, что предписание включать определённые сертификаты в программы для доступа к сайтам сталкивается с техническими правилами самих разработчиков программ [12]. Для Российской Федерации эти выводы означают, что обязанность применять сертификаты безопасности национального удостоверяющего центра (часть 12 статьи 14.1) и обязанность обеспечивать их предварительную установку в средствах доступа к сайтам (части 10 и 11 той же статьи) требуют, чтобы статус сертификата был проверяем в любой момент, то есть требуют элементов r4, r7 и r8 на нормативном уровне.

В отношении рисков третьих сторон в финансовом секторе регламент Европейского союза об операционной цифровой устойчивости распределяет ответственность за надзор над поставщиками информационно-коммуникационных услуг между финансовыми организациями, регуляторами и самими поставщиками, и в литературе обсуждается, насколько это распределение сбалансировано [13, 14]. Российская конструкция иная: поставщиком опорной услуги выступает государство или уполномоченная им организация, и требования к поставщику устанавливаются не договором с участником, а публично-правовыми нормами. Тем важнее, чтобы эти нормы содержали те элементы, которые в договорной модели обеспечиваются соглашением об уровне обслуживания: показатели доступности, порядок уведомления и последствия простоя. Работы о системном риске концентрации облачных услуг [15] и об устойчивости инфраструктуры доменных имён государственных сервисов [16] подтверждают, что отказ единого для многих участников узла имеет последствия для всех одновременно; для опорной государственной информационной системы это означает, что режим её недоступности должен быть единым для всех участников и установлен заранее.

Предложения

С учётом изложенного предлагается следующее.

1. Закрепить на уровне федерального закона общее правило о последствиях недоступности государственной информационной системы для обязанностей, исполнение которых обусловлено обращением к ней: течение сроков, исчисляемых от событий в системе, приостанавливается на период её недоступности; участник не несёт последствий неисполнения обязанности, если неисполнение вызвано недоступностью системы, подтверждённой её оператором. Такое правило может быть включено в Федеральный закон "Об информации, информационных технологиях и о защите информации" применительно ко всем государственным информационным системам либо в каждый из рассмотренных законов отдельно. Первый вариант предпочтительнее: он отвечает предложению о едином правовом режиме защиты таких систем [5] и исключает расхождения между ними.

2. Установить обязанность оператора опорной государственной информационной системы фиксировать периоды недоступности в неизменяемых журналах, информировать пользователей о плановых и нештатных периодах недоступности и выдавать по обращению пользователя подтверждение периода недоступности. Для системы противодействия правонарушениям такой подход уже отражён в позиции разработчика проекта правил возмещения; его следует перенести с уровня правил взаимодействия операторов на уровень акта о самой системе.

3. Для государственной информационной системы национального удостоверяющего центра определить в постановлении о случаях прекращения действия сертификатов момент прекращения действия для случаев, установленных Правительством Российской Федерации, со дня внесения сведений в реестр, срок такого внесения и обязанность уведомления владельца, а в требованиях к порядку создания, выдачи, использования и прекращения действия сертификатов установить периодичность издания списков прекративших действие сертификатов, требования к доступности сервисов проверки статуса и порядок действий при недоступности инфраструктуры центра. Без этого обязанность по части 12 статьи 14.1 остаётся обусловленной системой, режим недоступности которой не определён.

4. Для единой системы учёта платёжных карт предусмотреть в нормативных актах Банка России форму подтверждения состояния сведений системы на момент запроса и порядок действий оператора по переводу денежных средств при отсутствии ответа системы

в установленный срок. Поскольку закон обязывает отказать в предоставлении карты при превышении ограничения, отсутствие ответа системы в его нынешней редакции означает невозможность предоставить карту любому клиенту, что несоразмерно цели нормы.

5. При подготовке подзаконных актов к Закону № 210-ФЗ использовать предложенную модель как перечень контрольных вопросов: акт, вводящий обязанность, обусловленную системой, должен содержать ответы по элементам r4 — r8 либо отсылку к акту, где они содержатся.

Результаты и выводы

1. Закон № 210-ФЗ ставит исполнение обязанностей операторами по переводу денежных средств и операторами связи в зависимость от трёх государственных информационных систем: системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, единой системы учёта платёжных карт и государственной информационной системы национального удостоверяющего центра. Для каждой из них закон устанавливает обязанность участника и последствия её неисполнения, но не устанавливает режим недоступности системы.

2. Предложенная модель правового режима опорной государственной информационной системы из восьми элементов позволяет измерять полноту регулирования. На уровне закона показатель полноты режима недоступности составляет от 0 до 0,3 для трёх систем; на уровне проектов подзаконных актов он повышается до 0,3; на уровне позиции разработчика по итогам публичного обсуждения проекта правил возмещения достигает 0,6.

3. Элементы режима недоступности отсутствуют в законе и в первой редакции подзаконного акта и появляются только в результате публичного обсуждения, причём лишь там, где процедура обсуждения предусматривает письменную позицию разработчика. Это делает полноту режима зависимой от участия адресатов регулирования в обсуждении, то есть от фактора, который сам по себе нормативно не гарантирован.

4. Устранение выявленного пробела возможно введением общего правила о последствиях недоступности государственной информационной системы для обусловленных ею обязанностей на уровне федерального закона и конкретизацией элементов r4 — r8 в актах о каждой системе.

Практическое подтверждение и достоверность результатов. Значения показателя рассчитаны по опубликованным текстам актов и проектов и могут быть воспроизведены по указанным в сносках идентификаторам. Результативность предложения о приостановлении сроков подтверждена сводкой предложений разработчика, сформированной 29 июля 2026 г. Ограничение работы состоит в том, что уровень L3 отражает намерение разработчика, а не текст акта; после опубликования доработанных редакций проектов значения показателя подлежат пересчёту.

Литература

1. Метельков А.Н. Понятие информационной системы: технические и нормативно-правовые аспекты // Правовая информатика. 2025. № 2. С. 112—118.
2. Метельков А.Н. Оператор: многозначность в подходах и функциях в обеспечении информационной безопасности // Правовая информатика. 2026. № 1. С. 43—51. DOI: 10.24412/1994-1404-2026-1-00-04.
3. Троян Н.А. Правовое регулирование цифровых платформ и экосистемы государственных услуг: вектор развития экономики данных в цифровую эпоху // Правовая информатика. 2026. № 1. С. 145—152. DOI: 10.24412/1994-1404-2026-1-00-15.
4. Полякова Т.А., Троян Н.А. Трансформация государственного управления в Российской Федерации: от кибернетики, информатики к цифровизации // Правовая информатика. 2025. № 4. С. 215—226.
5. Дубень А.К. Правовое обеспечение информационной безопасности Российской Федерации: нормативно-правовые основы и современные вызовы // Правовая информатика. 2026. № 1. С. 284—288. DOI: 10.24412/1994-1404-2026-1-00-31.
6. Ловцов Д.А., Бурый А.С. Кибербезопасность: основные тенденции в обеспечении // Правовая информатика. 2024. № 2. С. 23—34.
7. Хадеева М.В., Овчинников Е.К. Правовые основы функционирования антифрод-системы на финансовом рынке // Вестник Университета им. О.Е. Кутафина (МГЮА). 2025. № 8 (132). С. 164—172. DOI: 10.17803/2311-5998.2025.132.8.164-172.
8. Гаужаева В.А., Прокофьева Е.В. Отдельные аспекты эволюции противодействия кибермошенничеству // Право и управление. 2026. № 4. С. 470—474.
9. Шувалов П.С., Оганова Н.В. Развитие правового механизма дистанционного банковского обслуживания в условиях цифровизации // Юридическая наука. 2023. № 4. С. 187—191.
10. Соловяненко Н.И. Юридические функции и ответственность лиц, оказывающих доверенные услуги в цифровой бизнес-среде // Право и практика. 2021. № 4. С. 138—144. DOI: 10.24412/2411-2275-2021-4-138-144.

11. Berbecaru D.G., Lioy A. An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem // IEEE Access. 2023. Vol. 11. P. 79156—79175. DOI: 10.1109/ACCESS.2023.3299357.
12. Entschew E., Hall K., Bailey C., Nguyen K. A New eIDAS Beginning for QWACs // Datenschutz und Datensicherheit — DuD. 2022. Vol. 46. No. 4. P. 217—224. DOI: 10.1007/s11623-022-1591-x.
13. Wittlin J., Ossowska A., Sawicka K. Is DORA an opportunity for more balanced distribution of third-party risk management assurance responsibilities between banks, regulators and technology providers? // Information & Communications Technology Law. 2025. Vol. 35. No. 1. P. 109—116. DOI: 10.1080/13600834.2025.2514385.
14. Pierides M., Mulligan J. Key themes of resiliency, outsourcing and third-party risk management regimes // Journal of Securities Operations & Custody. 2025. Vol. 17. No. 2. P. 102. DOI: 10.69554/AUIQ5402.
15. Harmon R.L., Vytelingum P., Babaie-Harmon J. Cloud concentration risk: A framework agent-based model for systemic risk analysis // Journal of Financial Compliance. 2021. Vol. 4. No. 3. P. 232. DOI: 10.69554/SGUT4817.
16. Septiadi A., Lyu M., Habibi Gharakheili H., Sivaraman V. Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2026. Vol. 10. No. 2. P. 1—30. DOI: 10.1145/3805629.

SECTION
REGULATORY INFORMATICS

STATE INFORMATION SYSTEMS AS THE SUPPORTING INFRASTRUCTURE OF THE NATIONAL PAYMENT SYSTEM: THE LEGAL REGIME OF UNAVAILABILITY

Lobanov N.A.[11]

Keywords: *fraud prevention, funds transfer without the client's voluntary consent, money transfer operator, telecommunications operator, security certificate, certification authority, operator duties, time limits for performance of duties, liability, continuity of operation, public consultation on draft regulations.*

Abstract

Purpose: *to establish which provisions govern the consequences of unavailability of state information systems for participants required, from 2027, to use such systems, and to propose a model of the completeness of that legal regime.*

Research method: *formal legal analysis of Federal Law No. 210-FZ of 26 June 2026, the laws it amends and the related draft regulations of July and August 2026. The comparative method covers trust service liability and the allocation of third-party risk in the financial sector. The study draws on materials of the public consultation on four drafts; their analysis makes it possible to assess the completeness of the regulation against an author's model applied to the statute, the drafts and developers' recorded positions.*

Results: *three state information systems are identified whose use is a condition for the duties of money transfer and telecommunications operators: the system for countering offences committed with the use of information and communication technologies, the unified payment card register and the state information system of the national certification authority. For each the law imposes a duty and prescribes the consequences of non-performance, but sets no availability requirements, no procedure during downtime and no rule on how downtime affects time limits and liability. An eight-element model of the regime and a completeness index are proposed and calculated. Elements of the unavailability regime emerge only at the secondary level and only through public consultation: the developer of the draft compensation rules marked the proposal to suspend time limits during unavailability as accepted. Enshrining the regime in federal law is proposed.*

[11] ***Nikolay A. Lobanov****, independent expert in information security and critical information infrastructure protection; master's student at the Institute of Law and National Security, Russian Presidential Academy of National Economy and Public Administration, Moscow, Russian Federation. ORCID: 0009-0006-8187-4528.*
E-mail: nlobanov-25@ranepa.ru

References

1. Metel'kov A.N. Poniatie informatsionnoi sistemy: tekhnicheskie i normativno-pravovye aspekty // Pravovaia informatika. 2025. No. 2. S. 112—118.
2. Metel'kov A.N. Operator: mnogoznachnost' v podkhodakh i funktsiiakh v obespechenii informatsionnoi bezopasnosti // Pravovaia informatika. 2026. No. 1. S. 43—51. DOI: 10.24412/1994-1404-2026-1-00-04.
3. Troian N.A. Pravovoe regulirovanie tsifrovykh platform i ekosistemy gosudarstvennykh uslug: vektor razvitiia ekonomiki dannykh v tsifrovuiu epokhu // Pravovaia informatika. 2026. No. 1. S. 145—152. DOI: 10.24412/1994-1404-2026-1-00-15.
4. Poliakova T.A., Troian N.A. Transformatsiia gosudarstvennogo upravleniia v Rossiiskoi Federatsii: ot kibernetiki, informatiki k tsifrovizatsii // Pravovaia informatika. 2025. No. 4. S. 215—226.
5. Duben' A.K. Pravovoe obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii: normativno-pravovye osnovy i sovremennye vyzovy // Pravovaia informatika. 2026. No. 1. S. 284—288. DOI: 10.24412/1994-1404-2026-1-00-31.
6. Lovtsov D.A., Buryi A.S. Kiberbezopasnost': osnovnye tendentsii v obespechenii // Pravovaia informatika. 2024. No. 2. S. 23—34.
7. Khadeeva M.V., Ovchinnikov E.K. Pravovye osnovy funktsionirovaniia antifrod-sistemy na finansovom rynke // Vestnik Universiteta im. O.E. Kutafina (MGIuA). 2025. No. 8 (132). S. 164—172. DOI: 10.17803/2311-5998.2025.132.8.164-172.
8. Gauzhaeva V.A., Prokof'eva E.V. Otdel'nye aspekty evoliutsii protivodeistviia kibermoshennichestvu // Pravo i upravlenie. 2026. No. 4. S. 470—474.
9. Shuvalov P.S., Oganova N.V. Razvitie pravovogo mekhanizma distantsionnogo bankovskogo obsluzhivaniia v usloviiakh tsifrovizatsii // Iuridicheskaia nauka. 2023. No. 4. S. 187—191.
10. Solovianenko N.I. Iuridicheskie funktsii i otvetstvennost' lits, okazyvaiushchikh doverennye uslugi v tsifrovoi biznes-srede // Pravo i praktika. 2021. No. 4. S. 138—144. DOI: 10.24412/2411-2275-2021-4-138-144.
11. Berbecaru D.G., Lioy A. An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem // IEEE Access. 2023. Vol. 11. P. 79156—79175. DOI: 10.1109/ACCESS.2023.3299357.
12. Entschew E., Hall K., Bailey C., Nguyen K. A New eIDAS Beginning for QWACs // Datenschutz und Datensicherheit — DuD. 2022. Vol. 46. No. 4. P. 217—224. DOI: 10.1007/s11623-022-1591-x.
13. Wittlin J., Ossowska A., Sawicka K. Is DORA an opportunity for more balanced distribution of third-party risk management assurance responsibilities between banks, regulators and technology providers? // Information & Communications Technology Law. 2025. Vol. 35. No. 1. P. 109—116. DOI: 10.1080/13600834.2025.2514385.
14. Pierides M., Mulligan J. Key themes of resiliency, outsourcing and third-party risk management regimes // Journal of Securities Operations & Custody. 2025. Vol. 17. No. 2. P. 102. DOI: 10.69554/AUIQ5402.
15. Harmon R.L., Vytelingum P., Babaie-Harmon J. Cloud concentration risk: A framework agent-based model for systemic risk analysis // Journal of Financial Compliance. 2021. Vol. 4. No. 3. P. 232. DOI: 10.69554/SGUT4817.
16. Septiadi A., Lyu M., Habibi Gharakheili H., Sivaraman V. Assessing Resilience in Authoritative DNS Infrastructure Supporting Government Services // Proceedings of the ACM on Measurement and Analysis of Computing Systems. 2026. Vol. 10. No. 2. P. 1—30. DOI: 10.1145/3805629.