ПРАВОВЫЕ МЕХАНИЗМЫ СНИЖЕНИЯ РИСКОВ НЕКАЧЕСТВЕННОЙ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Олифиренко А.А.[1]

Ключевые слова: *информационная безопасность, публичная функция, целостность информации, юридически значимое решение, происхождение данных, версионность, межведомственный обмен, компьютерный инцидент, достоверность сведений, восстановление прав.*

Аннотация

Цель работы. *Цель работы состоит в определении правовых механизмов снижения рисков распространения некачественной информации в государственных информационных системах и устранения последствий ее использования при осуществлении публичных функций.*

Метод исследования. *Формально-юридический метод применен для толкования требований к качеству информации, ее защите и исправлению. Системно-структурный анализ использован для восстановления связи между исходной версией записи, ее преобразованиями и юридически значимыми результатами. Функциональный подход позволил соотнести оценку качества информации с назначением информационного ресурса и содержанием публичной функции.*

Результаты исследования. *Установлено, что некачественное состояние информации определяется нарушением требования, существенного для конкретной публичной функции; нарушение защищаемого состояния информации или функционирования ГИС образует самостоятельное основание для применения мер информационной безопасности. Предложен порядок реагирования, охватывающий переданные сведения, производные результаты и решения, фактически связанные со спорной версией. Компетентный субъект выбирает актуализацию, повторную оценку, временное ограничение использования либо пересмотр решения в установленной процедуре. Техническое восстановление версии записи не удостоверяет ее содержательную пригодность, поэтому возврат в обработку требует проверки по источнику и назначению ресурса. При признаках компьютерного инцидента порядок дополняется регистрацией событий, техническим расследованием и восстановлением защищенного состояния информации и ГИС. Применимость подхода подтверждена позициями Конституционного Суда Российской Федерации по исправлению ошибок публичного органа и исправлению реестровых записей.*

DOI: 10.24412/1994-1404-2026-3-302-311

Введение и постановка задачи

В государственной информационной системе (далее — ГИС) одна запись может последовательно воспроизводиться, сопоставляться с другими сведениями и преобразовываться в результаты, используемые при подготовке административных решений. *Для целей настоящей статьи информационный ресурс рассматривается как организованная совокупность информации в ГИС, предназначенная для использования при осуществлении одной или нескольких публичных функций. В составе такого ресурса выделяются информационные объекты — функционально обособленные единицы информации, имеющие самостоятельное назначение и способные повлиять на юридически значимый результат. Информационным объектом может выступать реестровая запись, электронный документ, сообщение межведомственного обмена или иной результат фиксации и обработки сведений, имеющий самостоятельное значение для осуществления публичной функции. Запись в настоящем исследовании рассматривается как один из видов информационного объекта и обозначает зафиксированную в ГИС совокупность сведений, используемую как*

[1] ***Олифиренко Артем Алексеевич****, ведущий специалист по защите систем искусственного интеллекта, ответственный за безопасность ИИ-систем, руководитель суб-команды мониторинга информационной безопасности ООО «Экосистема недвижимости „Метр квадратный“», Москва, Россия; аспирант кафедры информационного права и цифровых технологий ФГБОУ ВО «Саратовская государственная юридическая академия», Саратов, Россия. ORCID 0000-0002-2186-281X.*

E-mail: artemolifirenko@yandex.ru

единицу хранения и обработки, а версия записи — состояние этой совокупности сведений в определенный момент времени. Разграничение имеет правовое значение, поскольку решение оценивается по той версии записи, которой орган располагал в момент совершения соответствующего действия. Исправление исходного значения изменяет дальнейшую обработку, но не устраняет последствия прежнего использования записи. Для их выявления требуется восстановить последовательность операций с конкретной версией.

Качество информации представляет собой интегральную характеристику степени ее пригодности для совершения действий и принятия решений, отвечающих целям, задачам и интересам субъекта. Для целей статьи конкретная публичная функция понимается как предусмотренное законодательством направление деятельности или полномочие публичного органа, при осуществлении которого информация используется для совершения юридически значимого действия или принятия решения. В ГИС информация признается некачественной, если несоответствие требованию, существенному для такой функции, снижает пригодность сведений для ее выполнения.

Проблема качества информации входит в предмет обеспечения информационной безопасности, если расхождение обусловлено воздействием на защищаемые свойства информации либо нарушением функционирования информационной системы. Под защищаемым состоянием далее понимается состояние информации и ГИС, при котором сохраняются свойства информации и условия функционирования системы, подлежащие защите в соответствии с требованиями информационной безопасности. Приказом ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» утверждены требования, предусматривающие предотвращение несанкционированного доступа и специальных воздействий, направленных в том числе на уничтожение и искажение информации[2]. Методический документ ФСТЭК России «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденный 12 апреля 2026 г., предусматривает регистрацию и последующий анализ событий безопасности[3]. *Содержательная ошибка, содержащаяся в исходных сведениях либо возникшая при применении некорректной методики, может сделать информацию некачественной без нарушения ее защищаемого состояния. Этим обусловлено разграничение предмета технической и содержательной проверок.*

Цель исследования — определить правовые механизмы снижения рисков распространения некачественной информации в ГИС и устранения последствий ее использования при осуществлении публичных функций.

Научно-теоретические подходы к исследованию

В настоящем исследовании юридическая значимость качества записи определяется той функцией, которую она выполняет в механизме правоприменения. Р.В. Амелин указывает, что «неотъемлемой частью механизма правового регулирования является система фиксации и удостоверения юридических фактов» [1, с. 445]. Тем самым официальная фиксация сведений приобретает самостоятельное правовое значение, поскольку сформированная в установленном порядке запись используется для удостоверения обстоятельств, с которыми связываются юридические последствия. С.Е. Чаннов конкретизирует эту связь применительно к публичным информационным системам (так в работе он называет ГИСы), отмечая, что «указанные реестры служат для фиксации определенных юридических фактов, как правило, непосредственно порождающих, изменяющих либо прекращающих обязанности различных субъектов. В этом и заключается их юридическое значение» [2, с. 421]. Значение информационной системы как элемента правового механизма получает дальнейшее развитие в совместной монографии Р.В. Амелина и С.Е. Чаннова, где отмечается, что «публичная информационная система де факто может выступать в качестве формы (источника) права, если закон устанавливает обязательность использования такой системы» [3, с. 10]. Из приведенных положений следует, что *правовое значение записи определяется одновременно ее официальным происхождением, установленной процедурой формирования и ролью в осуществлении публичной функции. Совокупность этих признаков создает основание юридического доверия к записи и позволяет использовать ее в соответствующей правоприменительной процедуре. Юридическая достоверность в данном контексте характеризует возможность руководствоваться официальной записью в установленной процедуре, тогда как фактическая истинность характеризует соответствие содержащихся в ней сведений реальному положению дел.* Такое разграничение позволяет далее оценивать качество информации с учетом как правового статуса записи, так и содержательной пригодности сведений для конкретной публичной функции [4].

Требования к достоверности и своевременности обращения информации закреплены на уровне общих принципов информационного законодательства и конкретизируются применительно

[2] Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». Зарегистрирован в Минюсте России 16 июня 2025 г. № 82619 // СПС «КонсультантПлюс». П. 1.

[3] Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах : методический документ. Утвержден ФСТЭК России 12 апреля 2026 г. // СПС «КонсультантПлюс».

к публичной сфере. Пункт 6 ст. 3 Федерального закона № 149-ФЗ относит к принципам правового регулирования «достоверность информации и своевременность ее предоставления»[4]. Тем самым достоверность закрепляется как общий нормативный стандарт обращения информации. Федеральный закон № 8-ФЗ дополняет его применительно к публичной сфере, закрепляя принцип достоверности информации о деятельности публичных органов и право пользователя получать достоверную информацию[5]. Эти положения связывают общий стандарт достоверности с правом адресата полагаться на официальные сведения и проверять их содержание. *Нормативное требование достоверности охватывает процедурное основание доверия к официальной записи и возможность проверки ее фактического содержания.*

Составляющая качества информации обозначает оцениваемый аспект ее пригодности, метрика — способ измерения такой составляющей, требование — целевое ожидание к значению метрики, порог — граничное значение, отделяющее допустимое состояние информации от недопустимого. Выбор этих элементов определяется назначением сведений. Ф. Серра, В. Перальта, А. Маротта и П. Марсель, обобщая исследования контекстного управления качеством данных, исходят из положения о том, что «DQ must be considered in the context of the task carried out by the data users» («качество данных должно рассматриваться в контексте задачи, выполняемой пользователями данных»; перевод автора) [5, p. 2]. Эта позиция придает выполняемой задаче значение критерия отбора показателей качества данных. Применительно к ГИС такой задачей выступает конкретная публичная функция, поэтому существенным является отклонение от требования, влияющего на ее выполнение.

Разграничение содержательной и технической проверки имеет самостоятельное основание в моделях качества данных. В обзоре Б.М.В. Бернардо, Х.С. Мамеде, Ж.М.П. Баррозу и В.М.П.Д. Сантоса точность характеризуется как степень, в которой значения данных «correctly represent the actual value of a given concept» («правильно представляют фактическое значение соответствующего понятия»; перевод автора), тогда как восстанавливаемость понимается как способность «recover and preserve data and quality in the event of failure, data loss, or corruption» («восстановить и сохранить данные и их качество при сбое, утрате или повреждении»; перевод автора) [6, p. 20]. Сопоставление этих определений показывает различие предметов проверки. Точность требует сопоставления содержания с фактическим состоянием объекта, а восстанавливаемость характеризует способность системы вернуть информационный объект после технического нарушения. Поэтому техническое восстановление версии и проверка ее содержательной пригодности образуют самостоятельные этапы.

А.И. Костогрызов и А.А. Нистратов рассматривают качество функционирования информационной системы как системную характеристику и связывают общую цель ее функционирования с надежностью и своевременностью предоставления информации, полнотой, достоверностью и безопасностью используемой информации; для подсистемы информационной безопасности отдельно выделяется целостность защищаемой информации [7, с. 15]. Такое разграничение показывает различие трех объектов оценки: качества функционирования ГИС, качества используемой в ней информации и целостности защищаемой информации. В настоящем исследовании центральным объектом выступает качество информации, а качество функционирования ГИС и целостность информации учитываются в той мере, в какой их нарушение влияет на пригодность сведений для конкретной публичной функции.

Правовая оценка должна связывать исходную запись и ее версии с межсистемной передачей, результатами обработки и юридически значимыми решениями.

Решение поставленной задачи: правовые механизмы выявления и устранения последствий некачественной информации в ГИС

Критерии признания информации в ГИС некачественной и границы ее проверки

Информация в ГИС признается некачественной при несоответствии требованию, существенному для конкретной публичной функции. Законодательное определение информационной системы как совокупности, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, предполагает ее оценку как на содержательном, так и на технологическом уровне[6].

Если расхождение затрагивает защищаемые свойства информации либо нарушает функционирование ГИС, его последствия входят в предмет обеспечения информационной безопасности. Статья 16 Федерального закона № 149-ФЗ связывает защиту информации с предотвращением неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения сведений[7]. *Проверка устанавливает причину и стадию возникновения расхождения, возможное воздействие на систему и влияние спорной версии на выполнение публичной функции.* Оператор ГИС обеспечивает защиту инфор-

[4] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ч. I. Ст. 3448. П. 6 ст. 3.

[5] Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства Российской Федерации. 2009. № 7. Ст. 776. П. 2 ст. 4, п. 1 ст. 8.

[6] Федеральный закон № 149-ФЗ, ст. 2.

[7] Федеральный закон № 149-ФЗ, ст. 16.

мации «на всех стадиях (этапах) обработки и хранения информации», а также в течение жизненного цикла системы[8].

Границы проверки определяются содержанием и назначением информации, что согласуется с подпунктами «г», «д» пункта 2(1) постановления Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации», предусматривающими определение состава размещаемых сведений, функций системы, ее архитектуры и критериев достижения целей создания[9]. *Профиль качества информации представляет собой документированный набор применимых составляющих качества информации и их целевых значений (метрик, требований и порогов), используемый для оценки пригодности информации в конкретной публично-правовой процедуре.* Он определяет применимые требования и допустимые пределы их значений; источник подтверждения, компетенция субъектов и порядок проверки устанавливаются нормативными и организационными правилами соответствующей процедуры [6; 8; 9].

Р. Миллер, С.Х.М. Чан, Х. Уилан и Ж. Грегорио, сопоставив регулирование и стандартизированные рамки качества данных, установили, что «accuracy, completeness, consistency, and timeliness are equally and well represented across all frameworks» («точность, полнота, согласованность и своевременность одинаково широко представлены во всех рассмотренных рамках»; перевод автора) [8, p. 1]. Результат сопоставления показывает устойчивость этих характеристик независимо от специфики конкретной рамки. Поэтому точность, полнота, согласованность и своевременность образуют ядро профиля качества информации, которое дополняется требованиями, обусловленными назначением конкретного ресурса.

Целостность версии информационного объекта как защищаемое состояние и составляющая качества информации

Целостность версии информационного объекта в правовом контексте характеризует сохранность объема, структуры и связей конкретной версии информационного объекта, непротиворечивость и отсутствие несанкционированных искажений. Она рассматривается двояко: как защищаемое состояние конкретной версии информационного объекта и как специальная составляющая качества информации, когда пригодность зависит от сохранения состава, структуры и связей конкретной версии. Федеральный закон № 149-ФЗ и приказ ФСТЭК России № 117 связывают защиту целостности информации с предотвращением неправомерного уничтожения и модифицирования, а также с восстановлением сведений[10].

Технический контроль целостности версии информационного объекта устанавливает сохранность либо изменение защищаемого состояния версии. *Оценка целостности информации как составляющей качества информации определяет, повлияло ли изменение состава, структуры или связей на пригодность информации для публичной функции; истинность, достоверность, полнота и актуальность проверяются как самостоятельные содержательные составляющие.* При обнаружении воздействия восстанавливаются обстоятельства изменения и подтвержденная версия, после чего оценивается ее пригодность.

Распространение ошибочной версии записи по стадиям обработки и возникновение правового риска

Правовой риск возникает, если использование спорной версии способно повлиять на осуществление публичного полномочия или правовое положение адресата, в частности повлечь необоснованное ограничение, возложение обязанности или отказ в предоставлении положенного блага. Проверка устанавливает причину и стадию расхождения, а также фактическое влияние спорной версии на результат[11]. Пункт 29 приказа ФСТЭК России № 117 требует устанавливать события, которые могут нарушить цели защиты, определять объекты возможного воздействия и учитывать угрозы, реализация которых может привести к негативным последствиям[12].

Связь между состоянием сведений и результатом осуществления публичного полномочия учитывается в Методическом документе ФСТЭК России, в котором отмечается «критическая зависимость реализуемых полномочий (функций)» от устойчивости информационных систем и защищенности содержащейся в них информации[13]. *При оценке события учитывается состояние системы и публичная функция, выполнение которой связано с затронутыми сведениями.*

Корректность программно заданной операции подтверждает соблюдение алгоритма, а не качество использованных сведений. Проверке подлежат результаты, на формирование которых фактически повлияла спорная версия; пока они сохраняют юридическое значение, исправления исходной записи недостаточно.

---

[8] Приказ ФСТЭК России № 117, п. 9.

[9] Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства Российской Федерации. 2015. № 28. Ст. 4241. П. 2(1), пп. «г», «д».

[10] Федеральный закон № 149-ФЗ, ст. 16; приказ ФСТЭК России № 117, прил., п. 2, п. 30.

[11] Приказ ФСТЭК России № 117; Методический документ ФСТЭК России.

[12] Приказ ФСТЭК России № 117, п. 29.

[13] Методический документ ФСТЭК России, п. 2.1.

Проверка качества сведений до их включения в ГИС и фиксация происхождения версии

Предупредительная проверка начинается с определения назначения сведений и требований, существенных для выполнения публичной функции. *Профиль качества информации закрепляет применимые составляющие и их целевые значения (метрики, требования и пороги), тогда как допустимый источник, способ подтверждения записи и компетенция субъекта определяются нормативными и организационными правилами процедуры*[14].

В широком правовом значении информация охватывает содержание, форму представления и порядок обращения; данные характеризуют формальную сторону материально зафиксированной информации. Для разграничения данные понимаются как записи, показатели или значения, пригодные для хранения, передачи и автоматизированной обработки. *Качество данных — интегральная характеристика их пригодности для автоматизированной обработки и формирования осмысленной информации; качество информации — интегральная характеристика пригодности для действий и решений, отвечающих целям, задачам и интересам субъекта.* Такое разграничение отделяет оценку формы данных от оценки юридически значимого содержания.

Требования к качеству государственных данных закреплены приказом Минцифры России от 16 июня 2025 г. № 533 «Об утверждении Порядка управления качеством государственных данных с использованием федеральной государственной информационной системы "Единая информационная платформа национальной системы управления данными"». Пункт 2 определяет полноту через «степень заполненности представляемых государственных данных на уровне записей и полей», достоверность — через соответствие «формату и ограничениям», точность — посредством сопоставления со значениями регистров, справочников и классификаторов, а консистентность — как «непротиворечивость и связанность государственных данных»[15]. Пункт 3 связывает оценку этих характеристик с контролем данных на витринах и при передаче через систему межведомственного электронного взаимодействия, относя выявленные отклонения к инцидентам качества государственных данных[16]. *Используемая в приказе «достоверность» означает соответствие формату и ограничениям и относится к формальной проверке государственных данных; она не тождественна истинности или содержательной достоверности информации, подтверждаемой надежными и верифицируемыми источниками.* Фактическое основание, происхождение и порядок формирования записи устанавливаются отдельно.

Метаданные — это сведения, описывающие данные и операции с ними. В. Кумар, Чандраппа и Н.С. Харинараяна по результатам обзора 55 исследований установили, что «completeness, accuracy, consistency, accessibility, conformance, provenance, and timeliness are commonly used dimensions in metadata quality assessment» («при оценке качества метаданных обычно используются полнота, точность, согласованность, доступность, соответствие требованиям, происхождение и своевременность»; перевод автора) [10, p. 661]. Включение происхождения в этот ряд придает происхождению статус самостоятельной характеристики метаданных и позволяет связывать конкретную версию записи с последующими объектами обработки. *По метаданным определяется момент появления расхождения и устанавливаются объекты, в которых использовалась спорная версия.*

Необходимость сохранять эту связь во времени получает дополнительное обоснование в работе Л. Эрлингер и В. Вёсса. Рассматривая задачи автоматизированного мониторинга качества данных, авторы указывают: «The continuous measurement, storage, and usage of the collected metadata should be possible» («для результатов профилирования данных и измерений качества данных должна быть предусмотрена возможность непрерывного измерения, хранения и использования собранных метаданных»; перевод автора) [9, p. 11]. Непрерывное измерение и хранение метаданных создают временную связь между состояниями записи и позволяют восстановить путь спорной версии. *Результат контроля связывается с конкретной версией и сохраняется вместе со сведениями о проведенной проверке, фиксирующими момент появления расхождения и пределы его дальнейшего распространения.*

Временное ограничение использования спорной версии записи до завершения проверки

Спорная версия сохраняется в истории изменений для установления обстоятельств ее появления и последующего использования. Одновременно она исключается из операций, при которых может возникнуть правовой риск.

Если запись влияет на возникновение права, назначение выплаты, установление статуса или возложение обязанности, соответствующая операция приостанавливается до завершения проверки либо проводится на основе подтвержденного источника. Порядок ограничения использования спорной записи должен закрепляться во внутренних регламентах с разграничением компетенции подразделений.

---

[14] Приказ Минцифры России от 16 июня 2025 г. № 533 «Об утверждении Порядка управления качеством государственных данных с использованием федеральной государственной информационной системы "Единая информационная платформа национальной системы управления данными"». Зарегистрирован в Минюсте России 3 декабря 2025 г. № 84423 // СПС «КонсультантПлюс»; Федеральный закон № 149-ФЗ; Федеральный закон № 152-ФЗ; Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» // Собрание законодательства Российской Федерации. 2007. № 49. Ст. 6043; Федеральный закон № 8-ФЗ.

[15] Приказ Минцифры России № 533, п. 2.

[16] Приказ Минцифры России № 533, п. 3.

Мера РСБ.2 Методического документа ФСТЭК России предусматривает «своевременное выявление признаков компьютерных атак и инцидентов безопасности», а при их обнаружении требует проведения мероприятий по реагированию[17]. При углубленной проверке сведения из разных журналов сопоставляются с результатами анализа уязвимостей и обнаружения вторжений, после чего устанавливается связь расхождения с действиями пользователя либо изменениями в работе системы[18]. Для ГИС на платформе «ГосТех» дополнительная организационная основа предусмотрена п. 22 Положения о платформе, по нему оператор «обеспечивает централизованную реализацию мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак, а также реагированию на компьютерные инциденты»[19]. *Эти положения применимы, когда некачественное состояние информации связано с компьютерной атакой, техническим воздействием или нарушением функционирования компонентов платформы.*

Установление пригодности версии записи и восстановление информационного объекта

Техническая проверка устанавливает способ воздействия и восстанавливает последовательность операций, после чего сведения сопоставляются с источником и документами, положенными в основу записи[20]. Возможность подтверждения зависит от сохранности сведений о событиях безопасности. Мера РСБ.1 предусматривает «определение событий безопасности и данных о них, подлежащих регистрации», мера РСБ.3 требует обеспечить «формирование надежных меток времени и (или) синхронизацию системного времени», а мера РСБ.4 направлена на «обеспечение хранения и защиты данных о событиях безопасности от несанкционированного доступа»[21]. По совокупности этих сведений устанавливаются момент изменения, использованная учетная запись и последовательность межсистемной передачи конкретной версии.

Для восстановления цепочки зависимости используется происхождение данных. Под происхождением данных в настоящей статье понимаются сведения об источнике конкретной версии и последовательности ее преобразований. Б. Главич указывает, что «The provenance of a data item provides a record of how the data item was derived from other data items by a set of transformations» («происхождение элемента данных содержит запись о том, каким образом этот элемент был получен из других элементов данных посредством совокупности преобразований»; перевод автора) [11, p. 211]. Это определение задает критерий фактической зависимости, при котором производный объект включается в область проверки при подтвержденной цепочке преобразований от спорной версии. В той же работе показано, что при диагностике ошибки происхождения данных позволяет выделить входные данные и преобразования, фактически участвовавшие в формировании результата [11, p. 214—215]. *По истории операций устанавливаются момент появления расхождения, последующее использование спорной версии, а также документы, расчеты и решения, в которых она получила отражение.*

Восстановление предыдущей версии решает техническую часть задачи. Такая версия могла быть ошибочной, утратить актуальность или быть сформирована по неверной методике. *Поэтому перед возвратом в обработку версия повторно оценивается по первичным источникам, назначению ресурса и применимому профилю качества информации.*

Предлагаемая последовательность соответствует пункту 22 приказа Минцифры России № 533, согласно которому при выявлении несоответствия требованиям к качеству государственных данных или фактическим данным обладатель вносит изменения «в государственные данные, содержащиеся в источнике государственных данных»[22]. Автоматический инцидент закрывается после «успешного выполнения механизма контроля качества государственных данных»[23]. *Возвращение записи в обработку требует подтверждения ее пригодности, а не только технического восстановления прежнего значения.*

Исправление сведений в зависимых ресурсах и прекращение использования ошибочной версии при межсистемном обмене

После исправления сведений и подтверждения их пригодности запись возвращается в обработку, однако прежняя версия могла сохраниться у получателей либо повлиять на производные объекты. Область исправления устанавливается по истории использования версии, времени операций и направлениям передачи. Для этого сведения технической документации о программных интерфейсах, алгоритмах, электронных моделях процессов, архитектуре и базе данных системы[24] сопоставляются с журналами операций. Область

[17] Методический документ ФСТЭК России, мера РСБ.2.

[18] Методический документ ФСТЭК России, усиление меры РСБ.2.

[19] Постановление Правительства Российской Федерации от 16 декабря 2022 г. № 2338 «Об утверждении Положения о единой цифровой платформе Российской Федерации “ГосТех”, о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6 изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // Собрание законодательства Российской Федерации. 2022. № 52. Ст. 9610. П. 22.

[20] Приказ ФСТЭК России № 117; Методический документ ФСТЭК России.

[21] Методический документ ФСТЭК России, меры РСБ.1, РСБ.3, РСБ.4.

[22] Приказ Минцифры России № 533, п. 22.

[23] Приказ Минцифры России № 533, п. 23.

[24] Постановление Правительства РФ № 676, п. 5(1).

исправления образуют зависимые объекты, на содержание которых повлияла ошибочная версия.

Когда распространение спорной версии связано с неправомерным действием или реализацией угрозы, выявление затронутых ресурсов и восстановление информации входят в процессы защиты, предусмотренные статьей 16 Федерального закона № 149-ФЗ и пунктом 30 приказа ФСТЭК России № 117[25]. Исправление сведений в исходной записи и актуализация зависимых результатов относятся к управлению качеством информации. Получателю передается подтвержденная версия вместе со сведениями о периоде использования прежнего значения, после чего принимающая сторона актуализирует зависимый объект либо временно исключает его из обработки до завершения собственной проверки. До подтверждения исправления прежняя версия исключается получателем из новых операций. Завершение межсистемного обновления подтверждается получателем после прекращения использования прежней версии.

Обновлению зависимых ресурсов предшествует установление причины расхождения и исключение условий его повторного появления. Пункт 66 приказа ФСТЭК России № 117 связывает контроль уровня защищенности с «оценкой возможностей нарушения безопасности информации и (или) нарушения функционирования информационных систем внешними и внутренними нарушителями»[26]. Если расхождение вызвано компьютерным инцидентом, контроль проводится вне установленного периодического графика: пункт 67 предусматривает его осуществление «не реже одного раза в три года или после компьютерного инцидента»[27]. *Реагирование завершается после устранения причины изменения, обновления зависимых сведений и подтверждения того, что спорная версия больше не воспроизводится в информационных системах.*

Проверка юридически значимых решений после исправления записи и восстановление правового положения адресата

С.Е. Чаннов связывает функционирование публичной информационной системы непосредственно с осуществлением публичного управления, указывая, что «реальное осуществление действий в сфере публичного управления оказывается в зависимости […] от функционала используемой публичной информационной системы» [2, с. 420]. Эта зависимость означает, что свойства и сбои информационной системы способны влиять на результат реализации публичного полномочия. Также, по мнению С.Е. Чаннова, «любые сбои и ошибки в публичной информационной системе становятся фактами, имеющими юридическое значение» [2, с. 419]. *Для целей настоящего исследования это означает необходимость проверки уже возникших юридических последствий после исправления записи. Исправление записи не устраняет автоматически правовые последствия ее прежнего использования. В связи с этим необходимо установить, при принятии каких решений использовалась прежняя версия записи и какое влияние она оказала на правовое положение адресата.*

Если причиной некачественного состояния стало нарушение целостности информации либо функционирования ГИС и информация была использована при принятии юридически значимого решения, устранение технических последствий предшествует проверке правовых последствий использования спорной версии. Требования ФСТЭК России связывают защиту информации с предупреждением негативных последствий нарушения ее защищаемых свойств и реализации угроз безопасности[28]. В предлагаемом механизме восстановление подтвержденного состояния информации сопровождается проверкой решения, проводимой принявшим его органом в пределах своей компетенции и с соблюдением установленной законом процедуры.

Принципиальное значение имеет ситуация, при которой ошибка допущена самим публичным органом и длительное время определяла правовое положение гражданина. В Постановлении Конституционного Суда Российской Федерации от 14 января 2016 г. № 1-П Суд указал, что исправление ошибки, допущенной пенсионным органом, относится к праву и обязанности государства, однако механизм ее исправления должен обеспечивать баланс публичных и частных интересов, учитывать отсутствие нарушений со стороны гражданина и исключать его чрезмерное обременение. При распределении неблагоприятных последствий должны учитываться особенности жизненной ситуации, продолжительность периода, в течение которого гражданин полагался на официально признанный государством статус, и другие значимые обстоятельства[29]. Для целей настоящего исследования эта позиция означает, что исправление ошибочной официальной записи или результата ее обработки требует оценки последствий, возникших у добросовестного адресата вследствие доверия к действиям государственного органа.

Иная ситуация возникает, когда ошибочная запись в ЕГРН уже стала основанием возникновения и государственной регистрации права. В Постановлении Конституционного Суда Российской Федерации от 28 января 2025 г. № 3-П указано, что требование

[25] Федеральный закон № 149-ФЗ, ст. 16; приказ ФСТЭК России № 117, п. 30.

[26] Приказ ФСТЭК России № 117, п. 66.

[27] Приказ ФСТЭК России № 117, п. 67.

[28] Приказ ФСТЭК России № 117, п. 10.

[29] Постановление Конституционного Суда Российской Федерации от 14 января 2016 г. № 1-П «По делу о проверке конституционности части первой статьи 13 Закона Российской Федерации "О пенсионном обеспечении лиц, проходивших военную службу, службу в органах внутренних дел, Государственной противопожарной службе, органах по контролю за оборотом наркотических средств и психотропных веществ, учреждениях и органах уголовно-исполнительной системы, и их семей" в связи с жалобой гражданина С.В. Иванова» // Собрание законодательства Российской Федерации. 2016. № 4. Ст. 551. П. 5 мотивировочной части.

о признании зарегистрированного права отсутствующим направлено на обеспечение «достоверности, непротиворечивости содержащихся в ЕГРН публичных сведений о существовании, принадлежности и правовом режиме объектов недвижимости». Вместе с тем ошибки, вызванные несогласованностью действий государственных органов при ведении реестров, «не могут быть поставлены в вину» гражданам, которые рассчитывали на законность действий публичной власти[30]. *Исправление реестровой записи должно учитывать судьбу возникшего на ее основе права и необходимость защиты добросовестного доверия лица к действиям государства.*

Рассмотренные позиции показывают, что проверке подлежит юридически значимый результат, на формирование которого фактически повлияла некачественная информация. Пределы проверки определяются характером изменений правового положения адресата и полномочиями органа, принявшего соответствующий акт. *Негативные последствия организационных и межведомственных ошибок не должны автоматически возлагаться на добросовестное лицо, доверившееся официальным сведениям.* Вопрос о пересмотре акта, восстановлении права и компенсации разрешается в порядке, установленном для соответствующего вида правоотношений [2, с. 419—428; 11][31].

Выводы о правовых механизмах снижения рисков некачественной информации в ГИС

Результаты подтверждают функциональную природу качества информации: применимые требования определяются назначением ресурса, публичной функцией и возможными правовыми последствиями.

Некачественной информацией в ГИС следует признавать сведения, несоответствие которых существенному для конкретной публичной функции требованию снижает их пригодность и создает риск искажения юридически значимого результата. Расхождение может возникнуть в исходных сведениях, при фиксации, преобразовании либо воздействии на информационный объект. Причина и стадия определяют предмет проверки и распределение обязанностей по восстановлению версии и оценке связанных результатов.

Исправление исходной записи открывает проверку связанных результатов, которая в зависимости от их характера выражается в актуализации сведений, повторной оценке, ограничении использования либо пересмотре публично-властного решения в установленном порядке.

Выбор последствия учитывает правовое положение адресата, фактическую зависимость решения от ошибочной версии и защиту добросовестного доверия к официальной информации. *Организационные и межведомственные риски распределяются между публичными субъектами с учетом их компетенции и контроля над соответствующим участком информационного процесса и не должны перекладываться на добросовестного адресата.*

При признаках угрозы или нарушения функционирования ГИС процедура дополняется регистрацией события безопасности, техническим расследованием и восстановлением защищенного состояния информации и ГИС. Содержательная оценка устанавливает пригодность сведений и последствия их использования. *Разграничение этих направлений связывает управление качеством информации с информационной безопасностью, не смешивая их предмет.*

Исследование выполнено за счет гранта Российского научного фонда № 26-18-00420, https://rscf.ru/project/26-18-00420/, финансирование осуществляется через организацию ФГБОУ ВО «Саратовская государственная юридическая академия».

[30] Постановление Конституционного Суда Российской Федерации от 28 января 2025 г. № 3-П «По делу о проверке конституционности статей 12, 209 и 304 Гражданского кодекса Российской Федерации и части 5 статьи 1 Федерального закона “О государственной регистрации недвижимости” в связи с жалобами граждан Н.И. Гришиной, Н.З. Гулордавы и других» // Собрание законодательства Российской Федерации. 2025. № 6. Ст. 538.

[31] Постановления КС РФ № 1-П и № 3-П.

Литература

1. Амелин Р.В. Информационные системы как правовой инструмент воздействия на общественные отношения: анализ российской и мировой практики // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2021. Т. 21, вып. 4. С. 445—452. DOI: 10.18500/1994-2540-2021-21-4-445-452.
2. Чаннов С.Е. Использование цифровых технологий в сфере публичного управления // Известия Саратовского университета. Новая серия. Серия «Экономика. Управление. Право». 2021. Т. 21. Вып. 4. С. 419—428. DOI: 10.18500/1994-2540-2021-21-4-419-428.
3. Амелин Р.В., Чаннов С.Е. Тенденции и перспективы использования государственных информационных систем в государственном управлении: правовые аспекты : монография. М. : ИНФРА-М, 2023. 171 с. ISBN 978-5-16-112170-2.
4. Амелин Р.В., Чаннов С.Е. Эволюция правовых методов под воздействием цифровых технологий // Вестник Поволжского института управления. 2021. Т. 21. № 5. С. 4—12.
5. Serra F., Peralta V., Marotta A., Marcel P. Use of Context in Data Quality Management: A Systematic Literature Review // Journal of Data and Information Quality. 2024. Vol. 16. No. 3. Art. 19. P. 1—41. DOI: 10.1145/3672082.
6. Bernardo B.M.V., São Mamede H., Barroso J.M.P., Santos V.M.P.D. Data Governance & Quality Management: Innovation and Breakthroughs Across Different Fields // Journal of Innovation & Knowledge. 2024. Vol. 9. No. 4. Art. 100598. DOI: 10.1016/j.jik.2024.100598.
7. Костогрызов А.И., Нистратов А.А. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 1. Общий подход // Правовая информатика. 2024. № 3. С. 13—31. DOI: 10.24682/1994-1404-2024-3-13-31.
8. Miller R., Chan S.H.M., Whelan H., Gregório J. A Comparison of Data Quality Frameworks: A Review // Big Data and Cognitive Computing. 2025. Vol. 9. No. 4. Art. 93. DOI: 10.3390/bdcc9040093.
9. Ehrlinger L., Wöß W. A Survey of Data Quality Measurement and Monitoring Tools // Frontiers in Big Data. 2022. Vol. 5. Art. 850611. DOI: 10.3389/fdata.2022.850611.
10. Kumar V., Chandrappa, Harinarayana N.S. Exploring Dimensions of Metadata Quality Assessment: A Scoping Review // Journal of Librarianship and Information Science. 2025. Vol. 57. No. 3. P. 661—673. DOI: 10.1177/09610006241239080.
11. Glavic B. Data Provenance: Origins, Applications, Algorithms, and Models // Foundations and Trends in Databases. 2021. Vol. 9. No. 3—4. P. 209—441. DOI: 10.1561/1900000068.

SECTION:
REGULATORY INFORMATICS

LEGAL MECHANISMS FOR REDUCING RISKS OF LOW-QUALITY INFORMATION IN GOVERNMENT INFORMATION SYSTEMS

***Olifirenko A.A.*[32]**

Keywords: *information security, public function, information integrity, legally significant decision, data provenance, version management, inter-agency exchange, computer incident, data accuracy, restoration of rights.*

Abstract

Purpose of work. *The purpose of the study is to determine legal mechanisms for reducing the risks associated with the dissemination of low-quality information in government information systems and for addressing the consequences of its use in the exercise of public functions.*

Research method. *The formal legal method is used to interpret requirements governing information quality, protection, and correction. System-structural analysis is applied to reconstruct dependencies between an original record, subsequent*

[32] ***Artem A. Olifirenko****, Lead Specialist in Artificial Intelligence Systems Security, responsible for AI systems security, Head of the Information Security Monitoring Sub-Team, LLC "Real Estate Ecosystem 'Metr Kvadratny'", Moscow, Russia; Ph.D. student, Department of Information Law and Digital Technologies, Saratov State Law Academy, Saratov, Russia. ORCID: 0000-0002-2186-281X.*
E-mail: artemolifirenko@yandex.ru

transformations, and legally significant outputs. A functional approach relates quality assessment to the intended use of an information resource and the public function performed with its support.

Results of the study. *The study shows that low-quality information is identified by breach of a requirement material to a particular public function, while interference with the protected state of information independently triggers information-security measures. The proposed response procedure covers transmitted data, derived outputs, and public-authority decisions actually linked to the disputed record version. The competent authority selects the applicable measure according to the dependency and governing procedure: updating the data, reassessing the output, temporarily restricting its use, or reviewing the decision. Restoring a technically verified record version does not establish its substantive fitness; return to processing therefore requires review against the source and intended use. Where a computer incident is suspected, the procedure is supplemented by security-event logging, technical investigation, and restoration of the protected state of information and the GIS. The approach is supported by Constitutional Court cases concerning correction of errors by public authorities and registry corrections.*

References

1. Amelin R.V. Informatsionnye sistemy kak pravovoi instrument vozdeistviia na obshchestvennye otnosheniia: analiz rossiiskoi i mirovoi praktiki // Izvestiia Saratovskogo universiteta. Novaia seriia. Seriia: Ekonomika. Upravlenie. Pravo. 2021. T. 21, vyp. 4. S. 445—452. DOI: 10.18500/1994-2540-2021-21-4-445-452.
2. Channov S.E. Ispol'zovanie tsifrovykh tekhnologii v sfere publichnogo upravleniia // Izvestiia Saratovskogo universiteta. Novaia seriia. Seriia "Ekonomika. Upravlenie. Pravo". 2021. T. 21. Vyp. 4. S. 419—428. DOI: 10.18500/1994-2540-2021-21-4-419-428.
3. Amelin R.V., Channov S.E. Tendentsii i perspektivy ispol'zovaniia gosudarstvennykh informatsionnykh sistem v gosudarstvennom upravlenii: pravovye aspekty : monografiia. M. : INFRA-M, 2023. 171 s. ISBN 978-5-16-112170-2.
4. Amelin R.V., Channov S.E. Evoliutsiia pravovykh metodov pod vozdeistviem tsifrovykh tekhnologii // Vestnik Povolzhskogo instituta upravleniia. 2021. T. 21. No. 5. S. 4—12.
5. Serra F., Peralta V., Marotta A., Marcel P. Use of Context in Data Quality Management: A Systematic Literature Review // Journal of Data and Information Quality. 2024. Vol. 16. No. 3. Art. 19. P. 1—41. DOI: 10.1145/3672082.
6. Bernardo B.M.V., São Mamede H., Barroso J.M.P., Santos V.M.P.D. Data Governance & Quality Management: Innovation and Breakthroughs Across Different Fields // Journal of Innovation & Knowledge. 2024. Vol. 9. No. 4. Art. 100598. DOI: 10.1016/j.jik.2024.100598.
7. Kostogryzov A.I., Nistratov A.A. Metodicheskie polozheniia po veroiatnostnomu prognozirovaniiu kachestva funktsionirovaniia informatsionnykh sistem. Chast' 1. Obshchii podkhod // Pravovaia informatika. 2024. No. 3. S. 13—31. DOI: 10.24682/1994-1404-2024-3-13-31.
8. Miller R., Chan S.H.M., Whelan H., Gregório J. A Comparison of Data Quality Frameworks: A Review // Big Data and Cognitive Computing. 2025. Vol. 9. No. 4. Art. 93. DOI: 10.3390/bdcc9040093.
9. Ehrlinger L., Wöß W. A Survey of Data Quality Measurement and Monitoring Tools // Frontiers in Big Data. 2022. Vol. 5. Art. 850611. DOI: 10.3389/fdata.2022.850611.
10. Kumar V., Chandrappa, Harinarayana N.S. Exploring Dimensions of Metadata Quality Assessment: A Scoping Review // Journal of Librarianship and Information Science. 2025. Vol. 57. No. 3. P. 661—673. DOI: 10.1177/09610006241239080.
11. Glavic B. Data Provenance: Origins, Applications, Algorithms, and Models // Foundations and Trends in Databases. 2021. Vol. 9. No. 3—4. P. 209—441. DOI: 10.1561/1900000068.