

**ВСЕРОССИЙСКИЙ КОНКУРС МОЛОДЕЖИ ОБРАЗОВАТЕЛЬНЫХ И
НАУЧНЫХ ОРГАНИЗАЦИЙ НА ЛУЧШУЮ РАБОТУ
«МОЯ ЗАКОНОТВОРЧЕСКАЯ ИНИЦИАТИВА»**

Направление: «Социальная политика»

Тема: «Государственная политика в жилищной сфере в условиях внедрения систем «умного дома» и «Безопасный город»

**Соискатель: Ростовцева Полина Сергеевна
студентка 3 курса**

**Федерального государственного казенного образовательного учреждения
высшего образования «Университет прокуратуры Российской Федерации»
(УП РФ)**

**Научный руководитель: Абдреев Тимур Ирекович
Доцент кафедры гражданско-правовых дисциплин
Университета прокуратуры
Российской Федерации
советник юстиции
кандидат юридических наук, доцент**

**Место выполнения работы: г. Москва, Федеральное государственное казенное
образовательное учреждение
высшего образования «Университет прокуратуры Российской Федерации»
(УП РФ)**

Аннотация

Научная работа посвящена разработке законодательской инициативы, направленной на обеспечение защиты частной жизни и безопасности граждан, охраны персональных данных, а также совершенствование правового регулирования оборота данных в системах «умного дома».

Рассмотрены ключевые проблемы действующей системы регулирования, включая неопределенность круга операторов персональных данных, экстерриториальность их хранения, техническую невозможность полного удаления сведений из распределенных хранилищ, а также коллизию между частно-правовыми механизмами защиты приватности и публичными интересами обеспечения общественной безопасности в рамках программы «Безопасный город». Отдельное внимание уделено правовому положению специальных субъектов персональных данных (военнослужащих, работников правоохранительных органов), для которых реализация права на удаление информации вступает в противоречие с требованиями режима секретности. Методологическую основу исследования составили анализ нормативно-правовой базы в сфере персональных данных и информационных технологий, изучение материалов правоприменительной практики, а также доктринальных подходов к определению правовой природы «цифровой тени» и производных аналитических сведений.

В настоящее время действующее законодательство не содержит специальных норм, регулирующих оборот данных в системах «умного дома», вследствие чего право на удаление информации, закрепленное в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных), становится труднореализуемым. Предложены конкретные законодательные меры, направленные на введение легального определения данных, фиксируемых устройствами «умного дома», установление требований к их локальному хранению, обеспечение гарантированного удаления таких данных у всех лиц, которым они были переданы, а также на принятие федерального закона, определяющего правовые границы функционирования аппаратно-программного комплекса «Безопасный город».

Полученные результаты могут быть использованы законодателями и государственными органами для совершенствования законодательства о персональных данных, формирования сбалансированной государственной политики в сфере цифровизации жилищной сферы и защиты конституционных прав граждан на неприкосновенность частной жизни и жилища.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	4
ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ РЕГУЛИРОВАНИЯ ОБОРОТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ».....	6
1.1. Понятие и правовая природа данных, фиксируемых устройствами «умного дома»	6
1.2. Конституционно-правовые основы охраны частной жизни и жилища в условиях цифровизации жилищной сферы.....	9
1.3. Статистическая характеристика распространения систем «умного дома» в Российской Федерации.....	12
ГЛАВА 2. АНАЛИЗ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ОБОРОТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ»	16
2.1. Общая характеристика нормативно-правовой базы регулирования персональных данных.....	16
2.2. Механизм реализации права на удаление информации: анализ статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»	19
2.3. Актуальные правовые гарантии обработки персональных данных и их применимость к системам «умный дом».....	22
2.4. Пробелы и противоречия действующего правового регулирования оборота данных в системах «умного дома»	25
ГЛАВА 3. ЗАРУБЕЖНЫЙ ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБОРОТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ» И ПЕРСПЕКТИВЫ ЕГО ИМПЛЕМЕНТАЦИИ В РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО	29
3.1. Сравнительно-правовой анализ регулирования оборота данных в системах «умного дома» в зарубежных юрисдикциях.....	29
3.2. Перспективы использования зарубежного опыта обеспечения безопасности данных в системах «умный дом» в российском законодательстве	33
ГЛАВА 4. ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ЧАСТНОЙ ЖИЗНИ И БЕЗОПАСНОСТИ ГРАЖДАН	36
4.1. Введение легального определения данных системы «умного дома» и установление требований к их локальному хранению.....	36
4.2. Обеспечение гарантированного удаления данных у всех лиц, которым они были переданы	39
4.3. Принятие федерального закона, определяющего правовые границы функционирования аппаратно-программного комплекса «Безопасный город», и усиление контроля за неправомерной обработкой данных.....	42
4.4. Социально-экономические, юридические и иные последствия предлагаемых законодательных инициатив.....	45
ЗАКЛЮЧЕНИЕ	48

ВВЕДЕНИЕ

Охрана частной жизни и жилища представляет собой одно из приоритетных направлений государственной политики Российской Федерации, конституционное закрепление которого свидетельствует о признании данной ценности на высшем нормативном уровне. Статьи 23 и 25 Конституции Российской Федерации гарантируют каждому право на неприкосновенность частной жизни и жилища, а часть 3 статьи 55 Основного закона допускает ограничение этих прав исключительно федеральным законом и лишь в той мере, в какой это необходимо для защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц¹.

Вместе с тем цифровая трансформация жилищной сферы, выразившаяся в массовом внедрении устройств, объединяемых понятием «умный дом», порождает качественно новые вызовы для реализации указанных конституционных положений. Под такими системами в настоящей работе понимается комплекс технических средств, размещённых в местах общего пользования многоквартирного дома и подключённых к сети Интернет, которые в автоматизированном режиме осуществляют сбор, накопление и передачу сведений о происходящем на придомовой территории, в подъездах, на парковках и иных общедомовых пространствах. К числу таких устройств относятся камеры видеонаблюдения, датчики движения, системы контроля доступа, домофоны с функцией видеофиксации. Бесперебойное функционирование перечисленных приборов приводит к формированию значительного массива информации, позволяющего с высокой степенью детализации восстановить распорядок дня, привычки, круг общения и маршруты передвижения жильцов и посетителей. При этом если бы доступ к этой информации имели исключительно правоохранительные органы, угроза приватности была бы ограничена. Однако на практике данные могут передаваться управляющим компаниям, частным охранным предприятиям, интеграторам систем «Безопасный город» и иным третьим лицам, что создаёт дополнительные риски несоразмерного вмешательства в частную жизнь.

Актуальность темы исследования определяется нарастающим противоречием между динамичным развитием технологий «умного дома» и отсутствием в российском законодательстве специальных норм, регулирующих оборот данных, собираемых такими устройствами. Согласно части 1 статьи 3 Закона о персональных данных, персональными данными признаётся любая информация, относящаяся к прямо или косвенно определённому либо определяемому физическому лицу². Видеозаписи с камер, голосовые команды, данные геолокации и телеметрические показатели по отдельности могут не позволять идентифицировать конкретное лицо, однако их совокупность формирует устойчивый информационный образ жильца и членов его семьи.

Проблема усугубляется стремительным ростом рынка устройств для «умного дома». При этом применение таких систем нередко осуществляется без ясного понимания гражданином того, какие именно сведения собираются, где они хранятся, кто имеет к ним доступ и может ли он потребовать их удаления. Закон о персональных данных предоставляет субъекту персональных данных право отозвать согласие на обработку и требовать уничтожения информации, однако реализация данного права в отношении данных, полученных с устройств «умного дома», сопряжена

¹ Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru> (дата обращения: 16.09.2026).

² О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

с рядом серьёзных затруднений: неопределённостью круга операторов, экстерриториальностью хранения, технической невозможностью полного удаления сведений из распределённых хранилищ.

Особую остроту проблема приобретает в контексте функционирования аппаратно-программного комплекса «Безопасный город», в рамках которого камеры видеонаблюдения, разных субъектов правоотношений, интегрируются в единую государственную систему, доступ к которой имеют правоохранительные органы³. Конституция Российской Федерации гарантирует неприкосновенность жилища и охрану частной жизни, однако статус указанного комплекса до настоящего времени не урегулирован отдельным федеральным законом, что создаёт угрозу несоразмерного ограничения конституционных прав граждан. Возникает коллизия: собственники помещений в многоквартирном доме, данные которых собираются общедомовыми камерами, расположенными в местах общего пользования, фактически лишены возможности влиять на дальнейшую судьбу этих данных, поскольку их согласие на обработку зачастую презюмируется самим фактом проживания, а собранная информация может передаваться, в лучшем случае управляющим компаниям, частным охранным предприятиям, а по факту и иным третьим лицам, что противоречит принципу свободного и информированного согласия.

Целью настоящего исследования является комплексный анализ действующего правового регулирования в сфере оборота данных, собираемых устройствами «умного дома», и выработка научно-обоснованных предложений по совершенствованию законодательства Российской Федерации, направленных на обеспечение права потребителя на удаление такой информации при сохранении необходимого баланса между частными интересами защиты приватности и публичными интересами обеспечения общественной безопасности.

Для достижения поставленной цели решаются следующие задачи: раскрытие правовой природы данных, фиксируемых устройствами «умного дома», и определение их места в системе объектов гражданских прав; анализ конституционно-правовых основ охраны частной жизни и жилища в условиях цифровизации жилищной сферы; характеристика статистических данных о масштабах распространения систем «умного дома» и объёмах собираемых ими данных; исследование действующего законодательства с выявлением пробелов и противоречий; изучение зарубежного опыта правового регулирования оборота данных в системах «умного дома»; формулирование конкретных законодательных инициатив и оценка социально-экономических последствий их реализации.

Методологическую основу работы составили формально-юридический, сравнительно-правовой, системно-структурный методы научного познания, а также метод анализа статистических данных.

Круг лиц, на которых предлагается распространить выдвигаемые в работе предложения, охватывает граждан Российской Федерации — пользователей устройств «умного дома», операторов данных (производителей устройств, облачные сервисы, управляющие организации), федеральные органы исполнительной власти в сфере связи и информационных технологий, правоохранительные органы, а также отдельных лиц, для которых предлагается установить особый правовой режим обработки данных в связи с наличием допуска к государственной тайне.

³ Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город»: распоряжение Правительства Российской Федерации от 03.12.2014 № 2446-р (ред. от 05.04.2019) // Собрание законодательства РФ. – 2014. – № 50. – Ст. 7225.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ РЕГУЛИРОВАНИЯ ОБОРОТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ»

1.1. Понятие и правовая природа данных, фиксируемых устройствами «умного дома»

Определение правового режима данных, создаваемых устройствами «умного дома», требует прежде всего установления их места в системе объектов правового регулирования.

Закон о персональных данных в части 1 статьи 3 закрепляет легальную дефиницию персональных данных, под которыми понимается любая информация, относящаяся к прямо или косвенно определённом либо определяемому физическому лицу⁴. Применительно к системам «умного дома» к указанной категории сведений следует отнести видеозаписи с камер наблюдения, установленных в местах общего пользования, данные систем контроля доступа и домофонов с функцией видеофиксации, а также данные датчиков движения, фиксирующих перемещение лиц по придомовой территории, в подъездах и на парковках. Каждый из перечисленных элементов в отдельности может не позволять идентифицировать конкретное лицо, однако их совокупность формирует устойчивый информационный образ жильца и членов его семьи, позволяющий с высокой степенью достоверности восстановить распорядок дня, поведенческие привычки, круг общения и иные аспекты частной жизни.

В доктрине информационного права для обозначения совокупности сведений, формируемых об индивиде в процессе функционирования технических устройств без его непосредственного участия, используется категория «цифровая тень». Под цифровой тенью понимается пассивно формируемый информационный образ субъекта, создаваемый в результате автоматизированной обработки данных устройствами, не находящимися под его контролем. Как отмечают Е.В. Виноградова, Т.А. Полякова и А.В. Минбалеев, цифровой профиль как совокупность данных о субъекте требует специального правового регулирования, поскольку существующие механизмы не обеспечивают должной защиты⁵. Принципиальное отличие цифровой тени от цифрового следа состоит в критерии субъекта сбора сведений: если цифровой след формируется в результате осознанных действий самого пользователя, то цифровая тень образуется независимо от его воли, зачастую без его осведомления. Данное разграничение имеет не только теоретическое, но и практическое значение: оно позволяет обосновать необходимость распространения на цифровую тень всего комплекса гарантий, предусмотренных законодательством о персональных данных.

Проблема усугубляется тем обстоятельством, что в правоприменительной практике данные с «умных» устройств *de jure* зачастую не признаются персональными, что создаёт серьёзные пробелы в их защите. Общественный совет при Минстрое России уже обратил внимание на данную проблему, предложив внести соответствующие поправки в законодательство о персональных данных и разработать для застройщиков стандарты, регламентирующие сбор и хранение информации из систем «умного дома»⁶.

Показательным примером, иллюстрирующим риски чрезмерной опоры на данные, получаемые с помощью цифровых технологий, является уголовное дело в отношении, ученого-гидролога Института биологии внутренних вод РАН Цветкова А., расследование которого сопровождалось активным использованием систем видеоаналитики и алгоритмов распознавания.

⁴ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

⁵ Виноградова, Е. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е. В. Виноградова, Т. А. Полякова, А. В. Минбалеев // Правоприменение. – 2021. – Т. 5, № 4. – С. 5–19.

⁶ Там же. – С. 12.

Как показала практика, некритичное отношение к таким данным без их перепроверки может привести к нарушению прав граждан, включая необоснованное подозрение и несоразмерное вмешательство в частную жизнь. Данный случай демонстрирует, что развитие технологий сбора и анализа информации, включая системы «умного дома», порождает качественно новые вызовы для защиты частной жизни граждан, поскольку собранные сведения могут быть использованы вне контроля самого субъекта и без его явного согласия⁷.

Отдельного внимания заслуживает вопрос о множественности субъектов, чьи права затрагиваются обработкой данных в системах «умного дома». При установке таких устройств не всегда осознаётся, какие именно сведения и в каком объёме будут передаваться производителю или иным лицам. Более того, обрабатываемые данные могут относиться не только к собственнику жилого помещения, но и к членам его семьи, гостям, а в условиях многоквартирного дома — к соседям, попадающим в зону действия камер или датчиков. Видеонаблюдение, домофоны и «умный дом» предполагают сбор и хранение персональных данных всех, кто попадает в зону действия соответствующих устройств, при этом изображение человека является персональными, а во многих случаях и биометрическими данными. Это порождает проблему согласования интересов множества субъектов, каждый из которых обладает самостоятельным правом на защиту своих данных.

С точки зрения гражданского законодательства, данные о частной жизни лица охраняются статьёй 152.2 Гражданского кодекса Российской Федерации, устанавливающей запрет на распространение и использование информации о частной жизни гражданина без его согласия⁸. Вместе с тем остаётся дискуссионным вопрос о том, может ли цифровая тень рассматриваться в качестве самостоятельного объекта гражданских прав в смысле статьи 128 Гражданского кодекса Российской Федерации. Представляется, что совокупность сведений о режиме дня, привычках и предпочтениях лица относится к нематериальным благам, посягательство на которые должно влечь применение мер правовой защиты. Как подчёркивают Т.А. Полякова и А.В. Минбалеев, в условиях цифровой трансформации правовое обеспечение информационной безопасности должно включать не только юридические, но и технические механизмы защиты прав субъектов персональных данных⁹. Данное обстоятельство приобретает особое значение в условиях «умного дома», где обработка информации осуществляется автоматически, нередко без явного и информированного согласия субъекта.

Таким образом, данные, собираемые устройствами «умного дома», должны признаваться персональными данными в смысле действующего законодательства, что влечёт распространение на них всех гарантий, предусмотренных Законом о персональных данных¹⁰. Совокупность таких данных формирует цифровую тень субъекта — пассивно создаваемый информационный образ, обработка которого осуществляется вне контроля самого лица. Отсутствие в действующем законодательстве легального определения данных, собираемых устройствами «умного дома», и неопределённость их правового режима создают предпосылки для несоразмерного вмешательства

⁷ Полякова, Т. А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы / Т. А. Полякова, А. В. Минбалеев, Н. А. Троян // Государство и право. – 2023. – № 5. – С. 131–144.

⁸ Гражданский кодекс Российской Федерации (часть первая) : Федеральный закон от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301. – Ст. 152.2.

⁹ Полякова, Т. А. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации / Т. А. Полякова, А. В. Минбалеев, Н. В. Кроткова // Государство и право. – 2020. – № 5. – С. 75–87.

¹⁰ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451 ; Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru> (дата обращения: 18.09.2026).

в сферу частной жизни и препятствуют эффективной реализации права субъекта персональных данных на удаление такой информации.

1.2. Конституционно-правовые основы охраны частной жизни и жилища в условиях цифровизации жилищной сферы

Конституционно-правовую основу регулирования оборота данных в системах «умный дом» формирует прежде всего Конституция Российской Федерации. Статья 23 Основного закона гарантирует каждому право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, ограничение которого допускается только на основании судебного решения¹¹. Статья 24 Конституции РФ устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия¹². Наконец, статья 25 закрепляет неприкосновенность жилища, устанавливая, что никто не вправе проникать в жилище против воли проживающих в нём лиц иначе как в случаях, установленных федеральным законом, или на основании судебного решения¹³.

Приведённые конституционные положения приобретают особую значимость в условиях цифровизации жилищной сферы. Устройства «умного дома», размещённые в жилом помещении, фактически выступают инструментами непрерывного сбора информации о происходящем внутри жилища. Видеозаписи с камер, голосовые команды, телеметрические показатели — все эти сведения в совокупности позволяют восстановить детальную картину частной жизни проживающих в нём лиц. Как справедливо отмечают исследователи, массовый сбор и обработка персональных данных, развитие технологий «больших данных» и алгоритмического профилирования ведут к размыванию границ между публичной и частной сферами, что делает уязвимость частной жизни особенно острой¹⁴. В этом контексте неприкосновенность жилища в информационном смысле означает не только физическую недопустимость проникновения в жилое помещение, но и недопустимость несанкционированного сбора и обработки сведений о происходящем в нём.

Развитие конституционных положений осуществляется на уровне федерального законодательства. Закон о персональных данных был принят в развитие названных конституционных положений в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну¹⁵. Согласно пункту 1 статьи 3 указанного Закона, персональными данными признаётся любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу¹⁶. Существенно, что законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации¹⁷, что подчёркивает конституционную обусловленность всего массива нормативного регулирования в рассматриваемой сфере.

¹¹ Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации. — URL: <http://pravo.gov.ru> (дата обращения: 16.09.2026).

¹² Там же. Ст. 24.

¹³ Там же. Ст. 25.

¹⁴ Курдюк, П. М. Конституционные проблемы неприкосновенности частной жизни в условиях цифровизации / П. М. Курдюк, В. А. Очаковский // Юридическая наука. — 2024. — № 5. — С. 35–42.

¹⁵ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. — 2006. — № 31 (1 ч.). — Ст. 3451.

¹⁶ Там же. П. 1 ст. 3.

¹⁷ Там же. Ст. 2.

Отдельного внимания заслуживает вопрос о пределах ограничения конституционных прав в условиях цифровизации. Часть 3 статьи 55 Конституции Российской Федерации допускает ограничение прав и свобод человека и гражданина исключительно федеральным законом и лишь в той мере, в какой это необходимо для защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства¹⁸. Применительно к системам «умного дома» данное положение приобретает особую актуальность в контексте функционирования аппаратно-программного комплекса «Безопасный город», в рамках которого частные устройства интегрируются в государственные информационные системы¹⁹. В условиях цифровой трансформации конституционные ценности — права и свободы человека — нуждаются не в декларативном подтверждении, а в эффективных механизмах защиты²⁰. Это предполагает необходимость установления чётких правовых границ вмешательства государства в сферу частной жизни, включая определение целей, объёма и сроков хранения данных, получаемых с частных устройств.

В научной литературе справедливо подчёркивается, что эффективность правового воздействия в рассматриваемой сфере определяется степенью согласованности норм различных отраслей права. Применительно к проблематике настоящего исследования согласованность предполагает гармонизацию норм конституционного права, законодательства о персональных данных, гражданского законодательства (в части охраны частной жизни — статья 152.2 Гражданского кодекса Российской Федерации), жилищного законодательства (в части определения правового режима общего имущества многоквартирного дома, к которому могут относиться камеры видеонаблюдения), а также законодательства об оперативно-розыскной деятельности.

Как отмечают П.М. Курдюк и В.А. Очаковский, необходимо развитие и адаптация конституционно-правовых механизмов защиты частной жизни на основе принципов законности, необходимости и соразмерности с учётом международных стандартов в сфере прав человека²¹. Формулируются также предложения по совершенствованию законодательства о персональных данных, направленные на усиление гарантий неприкосновенности частной жизни в цифровой среде и обеспечение баланса между технологическим развитием, публичными интересами и фундаментальными правами и свободами человека²².

Применительно к системам «умного дома» это означает необходимость закрепления на законодательном уровне специальных гарантий, учитывающих специфику автоматизированного сбора данных в жилых помещениях: обязательного локального хранения первичных данных на территории Российской Федерации, обеспечения технической возможности удаления данных по требованию субъекта, а также обязательного уведомления субъекта о передаче данных третьим лицам.

Научные исследования, представленные в материалах международных конгрессов, также подтверждают актуальность рассматриваемой проблематики. В частности, в работе Е.А. Кулаевой,

¹⁸ Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru> (дата обращения: 18.09.2026).

¹⁹ Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» : распоряжение Правительства Российской Федерации от 03.12.2014 № 2446-р (ред. от 05.04.2019) // Собрание законодательства РФ. – 2014. – № 50. – Ст. 7225.

²⁰ Полякова, Т. А. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации / Т. А. Полякова, А. В. Минбалеев, Н. В. Кроткова // Государство и право. – 2020. – № 5. – С. 75–87.

²¹ Курдюк, П. М. Указ. соч. С. 38.

²² Там же. С. 40.

посвящённой защите права на неприкосновенность частной жизни в условиях развития цифровых технологий, анализируется влияние цифровизации на реализацию конституционного права человека на конфиденциальность личной информации²³.

Таким образом, конституционно-правовые основы охраны частной жизни и жилища в условиях цифровизации жилищной сферы включают конституционные гарантии неприкосновенности частной жизни (статья 23), запрет на сбор и распространение информации о частной жизни без согласия лица (статья 24), неприкосновенность жилища (статья 25), а также конституционный принцип соразмерности ограничения прав и свобод (часть 3 статьи 55). Развитие этих положений на уровне федерального законодательства осуществляется через Закон о персональных данных, который, однако, не содержит специальных норм, учитывающих специфику данных, фиксируемых устройствами «умного дома». Существующая нормативная рамка создаёт необходимые конституционные предпосылки для усиления правового воздействия на процессы обработки таких данных, однако нуждается в развитии применительно к специфике цифровизации жилищной сферы.

1.3. Статистическая характеристика распространения систем «умного дома» в Российской Федерации

Формирование эффективной государственной политики в любой сфере предполагает наличие достоверной статистической базы, позволяющей оценить масштаб проблемы и измерить результативность принимаемых мер. Применительно к обороту данных в системах «умный дом» Российская Федерация находится в ситуации критического дефицита официальных статистических данных, что само по себе является серьёзным системным недостатком.

Централизованный учёт устройств «умного дома», объёмов собираемых ими данных, а также инцидентов, связанных с утечками или неправомерной обработкой такой информации, в России отсутствует. Понятие «данные, фиксируемые устройствами "умного дома"» не закреплено в действующем законодательстве в качестве самостоятельной юридической категории, а методики оценки объёмов обработки таких данных в государственных органах не унифицированы.

Для наглядного представления имеющихся данных целесообразно обратиться к табличной форме. В таблице 1 систематизированы основные статистические показатели, характеризующие распространение систем «умного дома» в Российской Федерации и связанные с ними риски по состоянию на 2025–2026 годы.

Таблица 1 — Основные статистические показатели распространения систем «умного дома» в Российской Федерации и связанных с ними рисков

Показатель	Значение	Источник данных
Объём рынка систем «умного дома» (2024 г.)	26 млрд руб.	en.iz.ru
Объём рынка систем «умного дома» (2025 г.)	32 млрд руб.	en.iz.ru
Ежегодный прирост рынка	25–30 %	en.iz.ru
Рост спроса на установку систем «умного дома» (первое полугодие 2026 г.)	более чем в 3 раза к аналогичному периоду 2025 г.	en.iz.ru

²³ Кулаева, Е. А. Цифровизация и право на неприкосновенность частной жизни: правовые вызовы и перспективы защиты в условиях развития технологий / Е. А. Кулаева, Л. В. Юн // Актуальные вопросы экономики, права и социологии : сборник трудов конференции. – Казань, 2025. – С. 154–160.

Доля россиян, владеющих устройствами «умного дома»	5,8 %	rosstat.gov.ru
Доля россиян, владеющих «умной» колонкой	31,4 %	rosstat.gov.ru
Доля россиян, владеющих роботом-пылесосом	22,7 %	rosstat.gov.ru
Доля ретейлеров, отметивших использование технологий «умного дома» жителями	более 70 %	www.retail.ru
Количество утечек персональных данных (2024 г.)	135 фактов	rkn.gov.ru
Количество записей, попавших в открытый доступ (2024 г.)	710 млн записей	rkn.gov.ru
Количество утечек персональных данных (2025 г.)	118 фактов	rkn.gov.ru
Количество записей, попавших в открытый доступ (2025 г.)	более 52 млн записей	rkn.gov.ru
Рост DDoS-атак с использованием IoT-устройств (январь–октябрь 2025 г.)	в 5 раз	ru-bezh.ru
Доля IoT-атак в общем числе инцидентов (2025 г.)	35 % (в 2024 г. — 7 %)	ru-bezh.ru
Количество ежедневных атак на IoT-устройства (2025 г.)	820 тыс.	ufatime.ru
Рост числа атак на IoT-устройства за год	107 %	ufatime.ru

Как следует из приведённых данных, разрыв между темпами распространения систем «умного дома» (ежегодный прирост рынка 25–30 %, трёхкратный рост спроса в первом полугодии 2026 года) и уровнем правовой защищённости собираемых ими данных является критическим²⁴. Данная тенденция создаёт предпосылки для формирования значительных массивов персональных данных, обработка которых осуществляется вне эффективного правового контроля.

Особую тревогу вызывает статистика инцидентов, связанных с безопасностью данных в рассматриваемой сфере. В 2025 году Роскомнадзор зафиксировал 118 фактов компрометации баз персональных данных, в результате которых в открытый доступ попали более 52 млн записей о гражданах²⁵. Хотя по сравнению с предыдущим годом наблюдается снижение абсолютных показателей, сохраняющийся объём утечек остаётся значительным. Показательно, что в 2025 году специалисты «Лаборатории Касперского» обнаружили уязвимость в мобильном приложении для управления умным домом, которая потенциально позволяла злоумышленникам получить доступ к личным данным пользователей, управлять оборудованием в квартирах и жилых комплексах, а также получать доступ к фотографиям с камер²⁶.

Масштаб атак на устройства Интернета вещей достиг уровня, требующего незамедлительного правового реагирования. Согласно данным компании StormWall, за первые десять месяцев 2025 года количество распределённых сетевых атак с использованием умных

²⁴ Смарт-подход: спрос на установку систем умного дома в РФ вырос втрое // Известия. – 2026. – 18 июля. – URL: <https://iz.ru/1865789/2026-07-18/smart-podkhod-spros-na-ustanovku-sistem-umnogo-doma-v-rf-vyros-vtroe> (дата обращения: 19.09.2026).

²⁵ Роскомнадзор зафиксировал снижение числа утечек персональных данных в 2025 году // ComNews. – 2026. – 22 января. – URL: <https://www.comnews.ru/content/238912/2026-01-22/2026-w04/roskomnadzor-zafiksiroval-snizhenie-chisla-utechek-personalnyh-dannyh-v-2025-godu> (дата обращения: 18.09.2026).

²⁶ Эксперты Kaspersky GReAT обнаружили уязвимость в Rubetek Home, мобильном приложении для умного дома и жилых комплексов // Kaspersky. – 2025. – 23 мая. – URL: <https://www.kaspersky.ru/about/press-releases/eksperty-kaspersky-great-obnaruzhili-uyazvimost-v-rubetek-home-mobilnom-prilozhenii-dlya-umnogo-doma-i-zhilyh-kompleksov> (дата обращения: 18.09.2026).

устройств в России выросло в пять раз по сравнению с аналогичным периодом прошлого года, а их доля в общем числе инцидентов достигла 35 % (в 2024 году — 7 %). Рекордное число подключённых устройств в одной из обнаруженных сетей заражённых устройств составило 118 тысяч единиц²⁷. Как отмечает К. Белоусов, проблемные аспекты защиты персональных данных в рамках Интернета вещей связаны с неопределённостью круга операторов и сложностью обеспечения контроля за обработкой информации²⁸. Г.Г. Камалова справедливо указывает, что обеспечение конфиденциальности информации требует комплексного подхода, учитывающего не только правовые, но и технические аспекты защиты данных²⁹.

Следует подчеркнуть, что все приведённые данные носят оценочный характер и не могут рассматриваться как результат репрезентативного исследования. Единый реестр устройств «умного дома» не создан, чёткая методика оценки объёмов собираемых ими данных не утверждена, а большинство инцидентов, связанных с неправомерной обработкой такой информации, остаются незарегистрированными. Отсутствие объективной статистической базы препятствует не только оценке реальных масштабов проблемы, но и планированию ресурсов для обеспечения информационной безопасности, а также измерению эффективности принимаемых законодательных мер. Как подчёркивают Т.Л. Шугунов и А.З. Жуков, в российском законодательстве отсутствуют специальные нормы, регулирующие использование системы «Умный дом», что создаёт правовую неопределённость³⁰.

На основании изложенного можно заключить, что статистическая характеристика распространения систем «умного дома» в Российской Федерации базируется преимущественно на экспертных оценках и разрозненных данных, а создание полноценной системы мониторинга оборота собираемых ими данных остаётся нерешённой задачей, без осуществления которой невозможно выстроить действительно эффективную государственную политику в рассматриваемой сфере.

²⁷ StormWall: в 2025 году число DDoS-атак с умных устройств в РФ выросло в 5 раз // Газета.ру. – 2025. – 27 ноября. – URL: <https://mt.gazeta.ru/tech/news/2025/11/27/21981097.shtml> (дата обращения: 18.09.2026).

²⁸ Белоусов, К. Интернет вещей: проблемные аспекты защиты персональных данных в рамках правоотношений / К. Белоусов // Цифровые технологии в системе правовых отношений : сборник научных трудов. – 2025. – С. 48–53.

²⁹ Камалова, Г. Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. ... д-ра юрид. наук : 12.00.13 / Камалова Гульфия Гафиятовна. – Москва, 2020.

³⁰ Шугунов, Т. Л. Проблема нормативно-правового регулирования использования системы «Умный дом» в Российской Федерации / Т. Л. Шугунов, А. З. Жуков // Информационное право. – 2023. – № 19. – С. 32–35.

ГЛАВА 2. АНАЛИЗ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ОБОРОТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ»

2.1. Общая характеристика нормативно-правовой базы регулирования персональных данных

Правовое регулирование оборота данных, фиксируемых устройствами «умного дома», осуществляется прежде всего Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных)³¹. Принятие данного закона стало следствием осознания законодателем необходимости обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Как отмечается в преамбуле, законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации³².

Закон о персональных данных установил принципиально новую модель регулирования, основанную на принципах законности, целевого характера обработки, минимизации сбора и достоверности данных. Согласно части 1 статьи 3 указанного Закона, персональными данными признаётся любая информация, относящаяся к прямо или косвенно определённом либо определяемому физическому лицу³³. Применительно к системам «умного дома» к таким сведениям следует отнести видеозаписи с камер, голосовые команды, данные геолокации, а также телеметрические показатели. Подобный подход продемонстрировал свою эффективность: для традиционных категорий персональных данных (паспортные данные, сведения о доходах, медицинская информация) создан достаточно развитый механизм защиты.

Вместе с тем модель 2006 года не учитывала стремительного развития цифровых технологий и Интернета вещей. Хотя Закон о персональных данных устанавливает общий режим обработки, он не содержит специальных норм, регулирующих оборот данных, фиксируемых устройствами «умного дома». Именно сегмент IoT-устройств продемонстрировал наиболее динамичный рост: по данным экспертов, объём российского рынка систем «умного дома» в 2025 году достиг 32 млрд рублей, а ежегодный прирост составляет 25–30 %³⁴. Существенную роль в регуляторной архитектуре играют также Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», закрепляющий «право на забвение», и Федеральный закон от 21 июля 2014 года № 242-ФЗ, установивший требование о локализации баз персональных данных на территории Российской Федерации³⁵.

Отдельного внимания заслуживает Федеральный закон от 6 июля 2016 года № 374-ФЗ, известный как «закон Яровой», который существенно расширил полномочия правоохранительных органов по доступу к информации, включая данные, передаваемые через информационные

³¹ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

³² Там же. Преамбула.

³³ Там же. Ч. 1 ст. 3.

³⁴ Смарт-подход: спрос на установку систем умного дома в РФ вырос втрое // Известия. – 2026. – 18 июля. – URL: <https://iz.ru/1865789/2026-07-18/smart-podkhod-spros-na-ustanovku-sistem-umnogo-doma-v-rf-vyros-vtroe> (дата обращения: 19.09.2026).

³⁵ Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448 ; О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации : Федеральный закон от 21.07.2014 № 242-ФЗ // Собрание законодательства РФ. – 2014. – № 30 (ч. I). – Ст. 4217

системы³⁶. Как будет показано далее, применение данного закона к системам «умного дома» порождает качественно новые вызовы для защиты частной жизни.

Для систематизации элементов действующей нормативной базы целесообразно обратиться к табличной форме. В таблице 2 представлена структура основных нормативных правовых актов, регулирующих оборот данных в системах «умного дома» и связанные с ними отношения.

Таблица 2 — Основные нормативные правовые акты Российской Федерации в сфере оборота данных в системах «умный дом»

Нормативный правовой акт	Предмет регулирования	Дата принятия / последней редакции
Конституция Российской Федерации	Право на неприкосновенность частной жизни, жилища, запрет на сбор информации о частной жизни без согласия (ст. 23, 24, 25)	12.12.1993/ред. 01.07.2020
Гражданский кодекс РФ (ст. 152.2)	Запрет на распространение информации о частной жизни гражданина без его согласия	30.11.1994/ред. 08.08.2024
Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	Общее регулирование обработки персональных данных, права субъектов, обязанности операторов	27.07.2006/ред. 24.06.2025
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Право на забвение, регулирование информационных систем	27.07.2006/ред. 23.11.2024
Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»	Локализация баз персональных данных на территории РФ	21.07.2014
Федеральный закон от 06.07.2016 года № 374-ФЗ «О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»	Доступ правоохранительных органов к информации, хранение трафика	06.07.2016
Федеральный закон от 28.02.2025 № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации»	Особенности обработки персональных данных отдельных категорий лиц, подлежащих государственной защите	28.02.2025

³⁶ О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации : Федеральный закон от 06.07.2016 № 374-ФЗ // Собрание законодательства РФ. – 2016. – № 28. – Ст. 4558.

Федеральный закон от 26.07.2026 № 265-ФЗ «О внесении изменений в статью 12 Федерального закона «О персональных данных» и отдельные законодательные акты Российской Федерации»	Порядок признания иностранных государств обеспечивающими адекватную защиту прав субъектов персональных данных	26.07.2026
Распоряжение Правительства РФ от 03.12.2014 № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город"»	Концепция построения и развития АПК «Безопасный город»	03.12.2014/ред. 05.04.2019

Приведённая систематизация позволяет констатировать, что нормативная база в целом сформирована и охватывает основные аспекты регулирования — общие принципы обработки персональных данных, локализацию, доступ правоохранительных органов, а также специальные гарантии для отдельных категорий субъектов. Вместе с тем, как будет подробнее рассмотрено в последующих параграфах, значительная часть норм носит рамочный характер, а ряд принципиальных вопросов (легальное определение данных, фиксируемые устройствами «умного дома», требования к их локальному хранению, механизм гарантированного удаления у всех лиц, которым они были переданы, а также правовой статус АПК «Безопасный город») остаётся вне поля законодательного регулирования. Действующее законодательство не содержит специальных норм, учитывающих специфику автоматизированного сбора данных в жилых помещениях, что создаёт предпосылки для несоразмерного вмешательства в сферу частной жизни и препятствует эффективной реализации права потребителя на удаление такой информации.

2.2. Механизм реализации права на удаление информации: анализ статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

Принятие Закона о персональных данных стало первым в истории российского правового регулирования шагом по созданию институционального механизма защиты прав субъектов персональных данных. Закон закрепил в статье 21 право субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если такие данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки³⁷. Кроме того, оператор обязан прекратить обработку данных и уничтожить их в случае отзыва субъектом согласия, если отсутствуют иные законные основания для обработки³⁸.

По своей юридической конструкции механизм удаления информации представляет собой реализацию субъективного права лица, осуществляемую путём направления оператору соответствующего требования. После получения такого требования у оператора возникает комплекс правовых последствий: обязанность прекратить обработку данных, уничтожить их в срок, не превышающий тридцати дней с даты поступления обращения, а также уведомить субъекта о выполнении требования³⁹. Положительным аспектом закона является установление правила о том, что в случае выявления неправомерной обработки персональных данных оператор обязан

³⁷ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451. – Ст. 21.

³⁸ Там же. Ч. 2 ст. 9.

³⁹ Там же. Ч. 1 ст. 21.

прекратить такую обработку в течение трёх рабочих дней⁴⁰. Данная норма создаёт юридический механизм защиты лица, чьи данные обрабатываются с нарушением законодательства.

Кроме того, Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в статье 10.3 закрепляет так называемое «право на забвение» — право требовать удаления информации из поисковых систем⁴¹. Однако, как будет показано далее, применение данного механизма к данным, фиксируемым устройствами «умного дома», существенно ограничено.

Вместе с тем анализ положений статьи 21 Закона о персональных данных позволяет выявить ряд существенных ограничений, снижающих потенциальную эффективность механизма применительно к системам «умного дома».

Во-первых, механизм удаления информации рассчитан на классическую модель «оператор — субъект», предполагающую наличие единственного оператора, который обладает полной информацией о составе обрабатываемых данных. В условиях «умного дома» эта модель не работает: в цепочке «производитель устройства — облачный сервис — провайдер связи — управляющая компания» каждый из участников может формально считаться оператором в отношении определённой части данных. В результате субъект персональных данных зачастую не имеет возможности определить, кому именно адресовать требование об удалении. Это создаёт прямую угрозу защите частной жизни и безопасности граждан, поскольку собранные сведения остаются вне их контроля, формируя цифровую тень, которая не может быть удалена по воле самого лица.

Во-вторых, закон не предусматривает механизма гарантированного удаления данных у всех лиц, которым они были переданы. Статья 21 обязывает оператора уничтожить данные, однако не устанавливает обязанности обеспечить уничтожение копий, переданных третьим лицам, включая государственные информационные системы. Учитывая, что данные с устройств «умного дома» распределены по облачным серверам, резервным копиям и системным журналам, уничтожение сведений в одном хранилище не означает, что они исчезли во всех остальных⁴².

В-третьих, механизм удаления не распространяется на производные аналитические сведения. Алгоритмы машинного обучения успевают обработать поступившую информацию и сформировать цифровой профиль пользователя. В зарубежной доктрине справедливо отмечается, что удаление первичных данных не равнозначно удалению выводов, сделанных на их основе. Российское законодательство этот аспект не регулирует⁴³.

Признавая безусловную прогрессивность механизма удаления информации как первого специализированного института защиты субъектов персональных данных, необходимо констатировать, что его конструкция нуждается в дальнейшем развитии — прежде всего в направлении расширения круга обязанных лиц, обеспечения гарантированного удаления данных у всех получателей и распространения требования об уничтожении на производные аналитические сведения.

⁴⁰ Там же. Ч. 3 ст. 21.

⁴¹ Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448. – Ст. 10.3.

⁴² Умный дом как инфраструктура данных: кто зарабатывает на цифровых привычках жильцов // Ведомости. – 2026. – 19 февраля. – URL: <https://www.vedomosti.ru/technology/articles/2026/02/19/1054321-umnyi-dom-kak-infrastruktura-dannyh> (дата обращения: 16.09.2026).

⁴³ Wachter, S. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI / S. Wachter, B. Mittelstadt // Columbia Business Law Review. – 2019. – № 2. – P. 494–620.

2.3. Актуальные правовые гарантии обработки персональных данных и их применимость к системам «умный дом»

Правовое регулирование обработки персональных данных в Российской Федерации осуществляется прежде всего Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных), который закрепляет основные принципы и условия обработки, права субъектов и обязанности операторов⁴⁴. Применительно к системам «умного дома» ключевое значение имеют положения статьи 9, устанавливающей требования к согласию на обработку, статьи 18, определяющей обязанности оператора при сборе данных, и статьи 21, регулирующей порядок уничтожения информации⁴⁵.

Согласно части 1 статьи 9 Закона о персональных данных, согласие субъекта должно быть конкретным, предметным, информированным, сознательным и однозначным⁴⁶. Однако в условиях «умного дома» данное требование нередко не соблюдается: согласие на обработку данных презюмируется самим фактом использования устройства, а его условия закрепляются в лицензионном соглашении, которое пользователь принимает при первом включении прибора. Это противоречит принципу свободного и информированного волеизъявления, поскольку субъект зачастую не осознаёт, какие именно сведения и в каком объёме будут передаваться производителю или третьим лицам.

Статья 21 Закона о персональных данных закрепляет право субъекта требовать уничтожения его данных, а также обязывает оператора прекратить обработку и уничтожить сведения в случае отзыва согласия, если отсутствуют иные законные основания⁴⁷. Оператор обязан исполнить данное требование в срок, не превышающий тридцати дней с даты поступления обращения. Однако, как показывает анализ, применение указанной нормы к данным, собираемым устройствами «умного дома», сопряжено с рядом существенных затруднений.

Во-первых, механизм удаления ориентирован на классическую модель «оператор — субъект», предполагающую наличие единственного оператора, обладающего полной информацией о составе обрабатываемых данных. В условиях «умного дома» эта модель не работает: в цепочке «производитель устройства — облачный сервис — провайдер связи — управляющая компания» каждый из участников может формально считаться оператором в отношении определённой части данных. Субъект персональных данных зачастую не имеет возможности определить, кому адресовать требование об удалении, что делает реализацию такого права неэффективной и создаёт прямую угрозу защите частной жизни и безопасности граждан.

Во-вторых, законодательство не устанавливает требований к получению согласия на обработку данных, собираемых устройствами «умного дома». Производитель устройства вправе передавать такие сведения третьим лицам, формируя цифровой профиль пользователя без его явного одобрения. Механизм отзыва согласия, предусмотренный статьёй 9 Закона о персональных данных, в данном случае неприменим, поскольку исходное согласие как таковое не запрашивалось.

В-третьих, Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» закрепляет в статье 10.3 так называемое «право на забвение» — право требовать удаления информации из поисковых систем⁴⁸. Однако

⁴⁴ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. — 2006. — № 31 (1 ч.). — Ст. 3451.

⁴⁵ Там же. Ст. 9, 18, 21.

⁴⁶ Там же. Ч. 1 ст. 9.

⁴⁷ Там же. Ст. 21.

⁴⁸ Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) // Собрание законодательства РФ. — 2006. — № 31 (1 ч.). — Ст. 3448. — Ст. 10.3.

данная норма не распространяется на данные, хранящиеся в информационных системах операторов персональных данных, и не применяется к сведениям, собираемым устройствами «умного дома».

В-четвёртых, законодательство не регулирует обработку производных аналитических сведений, полученных в результате машинного обучения. Удаление первичных данных не равнозначно удалению выводов, сделанных на их основе. Российское законодательство этот аспект не регулирует, что создаёт предпосылки для сохранения цифрового профиля пользователя даже после отзыва согласия.

Таким образом, действующие правовые гарантии обработки персональных данных, закреплённые в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» и Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», не решают задачу обеспечения права субъекта на удаление информации, собираемой устройствами «умного дома». Действующее регулирование ориентировано на классическую модель, предполагающую осознанное волеизъявление субъекта, и не учитывает специфику автоматизированного сбора данных в жилых помещениях. Это создаёт предпосылки для несоразмерного вмешательства в сферу частной жизни и препятствует эффективной реализации права на удаление такой информации.

2.4. Пробелы и противоречия действующего правового регулирования оборота данных в системах «умный дом»

Проведённый анализ действующего законодательства позволяет систематизировать основные пробелы и противоречия, снижающие эффективность правового регулирования оборота данных, фиксируемых устройствами «умного дома». Для наглядности целесообразно представить выявленные проблемы в табличной форме. Таблица 3 обобщает ключевые пробелы правового регулирования с указанием их существа и потенциальных последствий.

Таблица 3 — Пробелы и противоречия действующего правового регулирования оборота данных в системах «умный дом»

Выявленный пробел / противоречие	Сущность проблемы	Потенциальные негативные последствия
Отсутствие легального определения данных системы «умного дома»	Понятие не закреплено ни в одном федеральном законе; отсутствует единая методика отнесения таких данных к персональным	Затруднение правоприменения, невозможность привлечения операторов к ответственности, пробелы в статистическом учёте ⁴⁹
Неопределённость круга операторов в цепочке обработки	В цепочке «производитель — облачный сервис — провайдер — управляющая компания — интегратор» каждый участник может формально считаться оператором	Субъект персональных данных зачастую не имеет возможности определить, кому адресовать требование об удалении, что делает реализацию такого права неэффективной и создаёт прямую угрозу защите частной жизни и безопасности граждан. 50

⁴⁹ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

⁵⁰ ПДн в нашем доме или 152-ФЗ в практике ЖКХ // Хабр. – 2025. – 16 ноября. – URL: <https://habr.com/ru/articles/966946/> (дата обращения: 16.09.2026).

Экстерриториальность хранения данных	Многие устройства передают данные на серверы за пределами РФ; требование о локализации (ч. 5 ст. 18 Закона о персональных данных) исполняется не всегда	Требование удалить информацию может быть проигнорировано оператором вне юрисдикции РФ; механизмы международного сотрудничества не развиты ⁵¹
Техническая невозможность полного удаления	Данные распределены по облачным серверам, резервным копиям, системным журналам; могли быть переданы партнёрам до отзыва согласия	Уничтожение сведений в одном хранилище не означает их исчезновения во всех остальных; право на удаление становится фикцией ⁵²
Отсутствие регулирования производных аналитических сведений	Алгоритмы машинного обучения формируют цифровой профиль пользователя; удаление исходных данных не равнозначно удалению выводов	Цифровой профиль сохраняется даже после отзыва согласия; российское законодательство этот аспект не регулирует ⁵³
Отсутствие механизма гарантированного удаления у третьих лиц	Статья 21 Закона о персональных данных обязывает оператора уничтожить данные, но не устанавливает обязанности обеспечить уничтожение копий, переданных третьим лицам	Данные, переданные в государственные информационные системы, не могут быть удалены по требованию субъекта ⁵⁴
Отсутствие правового статуса АПК «Безопасный город»	Статус комплекса не урегулирован отдельным федеральным законом; действуют региональные акты и технические регламенты	Отсутствие чётких правовых границ вмешательства государства в частную жизнь; угроза несоразмерного ограничения конституционных прав ⁵⁵
Презюмирование согласия на передачу данных в правоохранительные органы	Согласие на передачу данных зачастую подразумевается самим фактом использования устройства	Противоречие принципу свободного и информированного согласия (ст. 9 Закона о персональных данных) ⁵⁶

⁵¹ Там же.

⁵² Умный дом как инфраструктура данных: кто зарабатывает на цифровых привычках жильцов // Ведомости. – 2026. – 19 февраля. – URL: <https://www.vedomosti.ru/technology/articles/2026/02/19/1054321-umnyi-dom-kak-infrastruktura-dannyh> (дата обращения: 16.09.2026).

⁵³ Wachter, S. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI / S. Wachter, B. Mittelstadt // Columbia Business Law Review. – 2019. – № 2. – P. 494–620.

⁵⁴ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451. – Ст. 21.

⁵⁵ Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» : распоряжение Правительства Российской Федерации от 03.12.2014 № 2446-р (ред. от 05.04.2019) // Собрание законодательства РФ. – 2014. – № 50. – Ст. 7225.

⁵⁶ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451. – Ст. 9.

Отсутствие требований к локальному хранению данных «умного дома»	Законодательство не устанавливает обязательности хранения первичных данных на территории РФ именно для устройств, работающих в жилых помещениях	Данные жильцов хранятся на зарубежных серверах; доступ к ним третьих лиц не контролируется ⁵⁷
--	---	--

Как следует из приведённых данных, наиболее существенные пробелы группируются вокруг четырёх направлений: субъектный состав (кто является оператором и кто защищён); инструментарий воздействия (каким образом обеспечить удаление данных); институциональная инфраструктура (куда обращаться за защитой); борьба с неправомерной обработкой (как обеспечить неизбежность применения норм).

Помимо перечисленных пробелов, необходимо обратить внимание на внутреннее противоречие действующей модели регулирования. Государство, с одной стороны, признаёт необходимость защиты частной жизни граждан (о чём свидетельствует принятие законов 2025–2026 годов, усиливших гарантии для специальных субъектов), а с другой — сохраняет условия, благоприятствующие экспансии рынка IoT-устройств без адекватного правового сопровождения.

В мировой практике подобная проблема решается через закрепление принципа защиты данных на этапе проектирования (встраивание механизмов защиты приватности в архитектуру устройств), установление требований к локальному хранению данных и введение обязательной сертификации IoT-устройств на соответствие стандартам информационной безопасности. Российский законодатель до настоящего времени не прибегал к подобным инструментам, что представляется стратегическим упущением.

На основании изложенного можно констатировать, что действующее правовое регулирование, несмотря на определённые позитивные сдвиги 2025–2026 годов, остаётся фрагментарным и не обеспечивает комплексной защиты права потребителя на удаление информации, фиксируемой устройствами «умного дома». Выявленные пробелы требуют законодательного устранения, а предложения по их восполнению будут сформулированы в четвёртой главе настоящей работы.

⁵⁷ Там же. Ч. 5 ст. 18.

ГЛАВА 3. ЗАРУБЕЖНЫЙ ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБОРОТА ДАННЫХ В СИСТЕМАХ «УМНЫЙ ДОМ» И ПЕРСПЕКТИВЫ ЕГО ИМПЛЕМЕНТАЦИИ В РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО

3.1. Сравнительно-правовой анализ регулирования оборота данных в системах «умного дома» в зарубежных юрисдикциях

Исследование зарубежного опыта представляет значительную ценность для выработки рекомендаций по совершенствованию российского законодательства, поскольку ряд государств значительно опережает Россию в формировании комплексных систем защиты данных, собираемых устройствами Интернета вещей. Сравнительно-правовой анализ позволяет выявить наиболее эффективные регуляторные модели и оценить возможности их адаптации к условиям национальной правовой системы.

Европейский союз располагает одной из наиболее развитых систем регулирования обработки персональных данных, центральным элементом которой является Общий регламент по защите данных⁵⁸. Статья 17 Регламента закрепляет право на удаление, согласно которому субъект данных вправе требовать от оператора без неоправданной задержки удаления персональных данных, касающихся его, при наличии предусмотренных оснований⁵⁹. Применительно к системам «умного дома» указанный Регламент создаёт достаточно высокий стандарт защиты, однако его применение сталкивается с теми же проблемами, что и в России: неопределённость круга операторов, распределённое хранение данных, техническая невозможность полного удаления.

Соединённые Штаты Америки не располагают единым федеральным законом о защите персональных данных, аналогичным европейскому. Однако отдельные штаты принимают собственные акты. Показательным примером является закон штата Калифорния о безопасности подключённых устройств, вступивший в силу в 2020 году⁶⁰. Закон обязывает производителей устройств Интернета вещей оснащать их разумными мерами безопасности, включая уникальные пароли по умолчанию⁶¹. Федеральная торговая комиссия выпустила рекомендации по обеспечению безопасности таких устройств, однако они носят необязательный характер⁶². В 2024 году Федеральная комиссия по связи запустила программу добровольной маркировки устройств Интернета вещей, соответствующую определённым стандартам кибербезопасности⁶³. Данная инициатива стимулирует производителей к повышению уровня защиты, но не создаёт механизма удаления данных по требованию пользователя.

Китайская Народная Республика демонстрирует модель приоритета государственной безопасности над индивидуальной приватностью. Закон о защите персональной информации (PIPL), вступивший в силу в 2021 году, формально закрепляет право субъекта на удаление данных, однако его реализация существенно ограничена требованиями государственных органов⁶⁴. Закон о

⁵⁸ Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных (Общий регламент по защите данных) // Официальный журнал Европейского союза. – 2016. – L 119. – С. 1–88.

⁵⁹ Там же. Ст. 17.

⁶⁰ California Senate Bill No. 327. Information Privacy: Connected Devices // California Legislative Information. – 2018. – URL: <https://leginfo.legislature.ca.gov> (дата обращения: 18.09.2026).

⁶¹ Там же. Ст. 1.

⁶² Federal Trade Commission. Internet of Things: Privacy & Security in a Connected World. – 2015. – URL: <https://www.ftc.gov> (дата обращения: 18.09.2026).

⁶³ Federal Communications Commission. Cyber Trust Mark. – 2024. – URL: <https://www.fcc.gov/cybertrustmark> (дата обращения: 18.09.2026).

⁶⁴ Personal Information Protection Law of the People's Republic of China // National People's Congress. – 2021. – URL: <http://www.npc.gov.cn> (дата обращения: 16.09.2026).

кибербезопасности устанавливает обязательную локализацию данных на территории Китая и требует прохождения проверок безопасности для операторов, обрабатывающих значительные объёмы информации. В контексте «умных городов» китайское законодательство допускает широкое использование видеонаблюдения и аналитики больших данных для целей общественной безопасности, что фактически исключает возможность удаления данных по требованию гражданина.

Великобритания после выхода из Европейского союза сохранила высокие стандарты защиты данных, имплементировав GDPR в национальное законодательство через Data Protection Act 2018. В 2021 году британское правительство опубликовало Кодекс практики по безопасности потребительских IoT-устройств (Code of Practice for Consumer IoT Security), содержащий 13 руководящих принципов, включая запрет на универсальные пароли и обязательное информирование пользователей о политике обработки данных⁶⁵. Однако Кодекс носит рекомендательный характер, а обязательные требования к удалению данных в нём отсутствуют.

Казахстан представляет интерес в контексте регулирования оборота данных в системах «умного дома». Закон Республики Казахстан «О персональных данных и их защите» закрепляет право субъекта на отзыв согласия и удаление данных⁶⁶. В рамках реализации концепции «Умный город» (Астана, Алматы) казахстанское законодательство устанавливает требования к локализации данных государственных информационных систем, однако частные устройства «умного дома» остаются вне специального регулирования. Как отмечают Т.А. Полякова и А.В. Минбалеев, достижение «цифровой зрелости» правового регулирования предполагает комплексное развитие всех элементов — не только ограничительных мер, но и инфраструктуры защиты прав субъектов⁶⁷. Данный вывод может быть экстраполирован и на сферу защиты данных: изолированное применение запретительных инструментов без создания механизмов удаления не позволяет достичь устойчивых результатов.

Для систематизации рассмотренных моделей целесообразно представить сравнительные данные в табличной форме. Таблица 4 содержит основные характеристики регуляторных подходов к обороту данных в системах «умного дома» в рассмотренных юрисдикциях.

Таблица 4 — Сравнительная характеристика регуляторных подходов к обороту данных в системах «умный дом» в зарубежных юрисдикциях

Юрисдикция	Модель регулирования	Право на удаление	Локализация данных	Ограничения для специальных субъектов	Ответственность операторов
Европейский союз	публично-правовая (императивная) модель	Закреплено	Допускается ограничение передач в третьи страны	Специальные категории данных (биометрия, здоровье)	Высокие штрафы (до 4% глобального оборота)

⁶⁵ Code of Practice for Consumer IoT Security // UK Department for Digital, Culture, Media & Sport. – 2021. – URL: <https://www.gov.uk> (дата обращения: 16.09.2026).

⁶⁶ О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 года № 94-V // Ведомости Парламента Республики Казахстан. – 2013. – № 9–10. – Ст. 45.

⁶⁷ Полякова, Т. А. Понятие и правовая природа «цифровой зрелости» / Т. А. Полякова, А. В. Минбалеев // Государство и право. – 2021. – № 9. – С. 107–116.

США (Калифорния)	фрагментарная модель регулирования	Не закреплено	Отсутствует	Не предусмотрены	Штрафы за нарушение безопасности устройств
Китай	публично-правовая (императивная) модель	Формально закреплено , фактически ограничено	Обязательная локализация	Государственн ые служащие, объекты КИИ	Административная и уголовная ответственность
Великобритан ия	публично- правовая (императивная) модель	Закреплено	Допускается передача при адекватной защите	Не предусмотрены	Штрафы до 17 млн фунтов
Казахстан	фрагментарная модель регулирования	Закреплено	Для государственн ых систем	Не предусмотрены	Административная ответственность
Россия	публично-правовая (императивная) модель	Закреплено	Обязательная локализация (242-ФЗ)	Для лиц, подлежащих госзащите (23- ФЗ)	Административная ответственность

Приведённое сравнение наглядно показывает, что российская модель существенно уступает зарубежным аналогам по нескольким параметрам: отсутствуют специальные требования к обработке данных в системах «умного дома», регулирование производных аналитических сведений фрагментарно, а механизмы гарантированного удаления данных недостаточно развиты. Опыт Европейского союза и Великобритании свидетельствует о необходимости закрепления на законодательном уровне принципа защиты данных на этапе проектирования. Опыт Китая демонстрирует риски чрезмерного приоритета публичных интересов над частными правами. Опыт Казахстана подтверждает важность сочетания ограничительных мер и развития инфраструктуры.

3.2. Перспективы использования зарубежного опыта обеспечения безопасности данных в системах «умный дом» в российском законодательстве

Помимо национальных регуляторных моделей, значительный интерес для настоящего исследования представляет анализ общих подходов к обеспечению безопасности данных в устройствах Интернета вещей, которые могут быть адаптированы в российских условиях. Как отмечается в научной литературе, развитие технологий «умного дома» в России имеет свою специфику, связанную с особенностями жилищного фонда, уровнем цифровизации и нормативным регулированием⁶⁸. Вместе с тем вопросы защиты персональных данных, собираемых такими устройствами, остаются недостаточно урегулированными.

Одним из перспективных направлений является закрепление на законодательном уровне принципа защиты данных на этапе проектирования устройств. Согласно данному принципу,

⁶⁸ Самодолов, А. П. Особенности развития «умных домов» в России / А. П. Самодолов, О. А. Самодолова, Е. В. Николаенко // Вестник ЮУрГУ. Серия «Строительство и архитектура». – 2020. – Т. 20, № 1. – С. 45–52.

производитель обязан обеспечить техническую возможность удаления персональных данных по требованию субъекта, а также минимизировать объём собираемых сведений. Как подчёркивают Т.А. Полякова и А.В. Минбалеев, в условиях цифровой трансформации правовое обеспечение информационной безопасности должно включать не только юридические, но и технические механизмы защиты прав субъектов персональных данных⁶⁹. Это означает, что требования к безопасности должны предъявляться не только к операторам, но и к производителям устройств.

Вторым направлением является введение обязательной сертификации устройств «умного дома» на соответствие требованиям информационной безопасности. В научных исследованиях отмечается, что отсутствие единых стандартов приводит к тому, что на рынке появляются устройства, не обеспечивающие должного уровня защиты данных⁷⁰. Сертификация позволила бы создать объективную основу для допуска устройств на рынок и повысить ответственность производителей.

Третьим направлением является координация внедрения системы сертификации и контроля. Представляется логичным возложить соответствующие полномочия на Роскомнадзор, который уже обладает инфраструктурой для работы с персональными данными и взаимодействует с операторами по вопросам трансграничной передачи данных⁷¹. Это не потребует создания новых административных структур и позволит использовать накопленный опыт.

Имплементация указанных мер в российское законодательство потребует внесения изменений в Закон о персональных данных⁷². В частности, целесообразно дополнить статью 6 частью, устанавливающей требования к производителям устройств, собирающих данные в жилых помещениях, а также закрепить обязанность обеспечивать техническую возможность удаления таких данных. Параллельно следует разработать национальный стандарт безопасности устройств «умного дома», предусматривающий обязательную сертификацию.

Таким образом, использование зарубежного опыта в части закрепления принципа защиты данных на этапе проектирования и введения обязательной сертификации устройств представляет собой перспективное направление совершенствования российского законодательства. Реализация данных мер позволит усилить защиту права субъекта персональных данных на удаление информации, собираемой устройствами «умного дома», при сохранении баланса между публичными интересами безопасности и частными интересами защиты данных.

⁶⁹ Полякова, Т. А. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации / Т. А. Полякова, А. В. Минбалеев, Н. В. Кроткова // Государство и право. – 2020. – № 5. – С. 75–87.

⁷⁰ Мухаметов, Д. Р. Проблемы и перспективы реализации концепции «Умный город» в России (на примере Москвы) / Д. Р. Мухаметов // Мир новой экономики. – 2019. – Т. 13, № 3. – С. 81–88.

⁷¹ Чубукова, С. Г. Системы субъектов информационного права: направления цифровой трансформации / С. Г. Чубукова // Вестник Московского университета. Серия 26: Государственный аудит. – 2019. – № 3. – С. 17–27.

⁷² О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

ГЛАВА 4. ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ЧАСТНОЙ ЖИЗНИ И БЕЗОПАСНОСТИ ГРАЖДАН

4.1. Введение легального определения данных системы «умного дома» и установление требований к их локальному хранению

Анализ, проведённый во второй и третьей главах настоящей работы, продемонстрировал, что ключевым структурным недостатком действующего правового регулирования является отсутствие легального определения данных, фиксируемых устройствами «умного дома». Преодоление данного ограничения предполагает законодательное закрепление соответствующей дефиниции и установление специальных требований к обработке таких данных, применительно к которым подобное регулирование обусловлено либо повышенной уязвимостью сведений, собираемых в жилых помещениях, либо публичными рисками, сопряжёнными с их неправомерной обработкой.

Первая новация касается введения легального определения. Предлагается дополнить статью 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»⁷³ пунктом 7.1, изложив его в следующей редакции: «7.1) данные, фиксируемые устройствами «умного дома», — любая информация, создаваемая в автоматическом режиме устройствами, установленными в жилом помещении и подключёнными к сети Интернет, в том числе видеозаписи, аудиозаписи, голосовые команды, данные геолокации, телеметрические показатели». Введение указанной дефиниции позволит устранить правовую неопределённость, препятствующую привлечению операторов к ответственности за неправомерную обработку таких данных. Кроме того, закрепление легального определения создаст основу для формирования единообразной правоприменительной практики и статистического учёта, дефицит которого был отмечен в первой главе настоящей работы.

Вторая новация касается установления специальных требований к обработке данных, фиксируемых устройствами «умного дома». В этих целях целесообразно дополнить статью 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»⁷⁴ частью 1.3, изложив её в следующей редакции: «1.3. Обработка данных, фиксируемых устройствами "умного дома", осуществляется с соблюдением следующих требований: обязательное локальное хранение первичных данных на территории Российской Федерации; обеспечение технической возможности удаления данных по требованию субъекта в течение тридцати дней; обязательное уведомление субъекта о передаче данных третьим лицам». Установление требования о локальном хранении первичных данных на территории Российской Федерации представляет собой реализацию принципа, уже закреплённого в части 5 статьи 18 Закона о персональных данных⁷⁵ для баз данных в целом. Однако применительно к устройствам «умного дома» данное требование приобретает особое значение, поскольку речь идёт о данных, собираемых в жилых помещениях, то есть в сфере, непосредственно затрагивающей конституционное право на неприкосновенность жилища. Как показал анализ, проведённый в главе 2, многие популярные устройства передают данные на серверы, находящиеся за пределами Российской Федерации, что делает невозможным эффективный контроль за их удалением.

Требование об обеспечении технической возможности удаления данных по требованию субъекта в течение тридцати дней направлено на реализацию принципа защиты данных на этапе

⁷³ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

⁷⁴ Там же. Ст. 6.

⁷⁵ Там же. Ч. 5 ст. 18.

проектирования. Как отмечает Т.А. Полякова, в условиях цифровой трансформации правовое обеспечение информационной безопасности должно включать не только юридические, но и технические механизмы защиты прав субъектов персональных данных⁷⁶. В отличие от действующей статьи 21 Закона о персональных данных, которая устанавливает обязанность оператора уничтожить данные, предлагаемая норма обязывает производителя обеспечить техническую возможность такого удаления на этапе проектирования устройства. Подобный подход позволяет трансформировать право на удаление из декларативного в реально исполнимое.

Обеспечение прозрачности обработки данных достигается посредством введения обязательного уведомления субъекта персональных данных о передаче данных третьим лицам. Как отмечалось в главе 2, субъект зачастую не знает, кому передаются данные, собираемые его устройством. Введение такой обязанности позволит субъекту принимать осознанные решения о распоряжении своими данными и, при необходимости, инициировать процедуру их удаления.

Совокупная реализация предложенных мер — введение легального определения данных, фиксируемых устройствами «умного дома», и установление специальных требований к их обработке — качественно расширит охват защитного механизма и усилит его превентивную функцию. Законодательно-технически предлагаемые изменения могут быть оформлены путём внесения дополнений в статью 3 и статью 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»⁷⁷.

4.2. Обеспечение гарантированного удаления данных у всех лиц, которым они были переданы

Второй блок предложений связан с необходимостью обеспечения реального, а не формального удаления данных, фиксируемых устройствами «умного дома», а также с дальнейшим совершенствованием механизма реализации права на удаление информации.

Действующая редакция статьи 21 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» обязывает оператора уничтожить данные в случае отзыва субъектом согласия, однако не устанавливает обязанности обеспечить уничтожение копий, переданных третьим лицам⁷⁸. Данное обстоятельство делает право на удаление неэффективным, поскольку данные, попавшие в распределённые хранилища, резервные копии или государственные информационные системы, фактически остаются доступными. Как отмечалось в главе 1, данные с устройств «умного дома» хранятся не в одном месте: они распределены по облачным серверам, резервным копиям и системным журналам, а также могли быть переданы партнёрам оператора ещё до отзыва согласия. Поэтому уничтожение сведений в одном хранилище не означает, что они исчезли во всех остальных.

Предлагается установить законодательное требование о том, что при обращении субъекта персональных данных с требованием об уничтожении данных, фиксируемых устройствами «умного дома», оператор обязан уничтожить такие данные, а также обеспечить уничтожение данных у всех лиц, которым они были переданы, в течение тридцати дней с момента получения требования. В этих целях целесообразно дополнить статью 21 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» частью 3.1, изложив её в следующей редакции: «3.1. При обращении

⁷⁶ Полякова, Т. А. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России / Т. А. Полякова, А. В. Минбалеес, Н. В. Кроткова // Государство и право. – 2024. – № 9. – С. 166–179.

⁷⁷ Там же. Ст. 3, 6.

⁷⁸ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451. – Ст. 21.

субъекта персональных данных с требованием об уничтожении данных, фиксируемых устройствами «умного дома», оператор обязан уничтожить такие данные, а также обеспечить уничтожение данных у всех лиц, которым они были переданы, в течение тридцати дней с момента получения требования»⁷⁹. Введение указанной нормы позволит создать механизм «сквозного» удаления, при котором требование субъекта распространяется на всю цепочку обработки данных, включая партнёров оператора, облачные сервисы и государственные информационные системы.

Второе направление — регулирование производных аналитических сведений. Как показал анализ, проведённый в главе 2, алгоритмы машинного обучения успевают обработать поступившую информацию и сформировать цифровой профиль пользователя. Удаление исходных данных не равнозначно удалению выводов, сделанных на их основе. В зарубежной доктрине по этому поводу справедливо отмечается: удаление исходных данных не равнозначно удалению выводов, которые были сделаны на их основе (концепция “right to reasonable inferences”)⁸⁰. Российское законодательство этот аспект не регулирует: требование об уничтожении персональных данных не распространяется на производные аналитические сведения. Например, если система «умного дома» зафиксировала, что жилец встаёт в 6 утра и уходит в 7, удаление журналов событий не приведёт к исчезновению этого вывода из уже сформированного профиля.

Применительно к производным данным предлагается дополнить статью 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» определением «производные персональные данные», включив в него сведения, полученные в результате автоматизированной обработки первичных данных и позволяющие идентифицировать субъекта. Данное дополнение создаст правовую основу для распространения требования об уничтожении на аналитические выводы, содержащиеся в цифровом профиле пользователя. Техническая реализация представляется возможной на основе обязательного документирования алгоритмов обработки и предоставления субъекту информации о том, какие выводы были сделаны на основе его данных.

Реализация предложенных мер потребует внесения изменений в статью 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (введение определения производных данных) и в статью 21 указанного Закона (введение механизма «сквозного» удаления). Совокупная реализация предложенных мер позволит трансформировать право на удаление из декларативного в реально исполнимое, обеспечив защиту цифрового профиля пользователя даже после отзыва согласия на обработку данных.

4.3. Принятие федерального закона, определяющего правовые границы функционирования аппаратно-программного комплекса «Безопасный город», и усиление контроля за неправомерной обработкой данных

Третий блок предложений охватывает два взаимосвязанных направления: формирование институциональной основы правового регулирования аппаратно-программного комплекса «Безопасный город» и усиление мер противодействия неправомерной обработке данных, фиксируемых устройствами «умного дома».

Как было установлено в первой главе настоящей работы, статус аппаратно-программного комплекса «Безопасный город» до настоящего времени не урегулирован отдельным федеральным законом. Действуют региональные нормативные акты и технические регламенты, которые не всегда согласуются с требованиями Закона о персональных данных о соразмерности и целевом характере

⁷⁹ Там же. Ст. 21.

⁸⁰ Wachter, S. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI / S. Wachter, B. Mittelstadt // Columbia Business Law Review. – 2019. – № 2. – P. 494–620.

обработки⁸¹. Одной из причин сложившейся ситуации является отсутствие единого подхода к определению правового режима данных, получаемых с частных устройств, интегрированных в государственную систему. В настоящее время интеграция частных камер в систему «Безопасный город» реализована в Москве, Санкт-Петербурге и Казани, а в других регионах ведутся работы по подключению камер торговых сетей. При этом, по признанию представителей правоохранительных органов, основное препятствие для такой интеграции — необходимость решения ряда правовых вопросов, связанных в первую очередь с передачей персональных данных граждан.

Предлагается принять федеральный закон «Об аппаратно-программном комплексе "Безопасный город"», устанавливающий: цели, объём и сроки хранения данных, получаемых с частных устройств; порядок доступа правоохранительных органов к данным, включая обязательность судебного решения; право гражданина на отключение своих устройств от государственной системы без ущерба для иных лиц; ответственность за нарушение порядка удаления информации, включая административные штрафы и компенсацию морального вреда по статье 152.2 Гражданского кодекса Российской Федерации⁸². Модель организации такого регулирования может быть основана на аналогии с законодательством о государственных информационных системах: определение оператора системы, установление требований к защите информации, разграничение полномочий между федеральными и региональными органами власти. Принятие указанного закона позволит установить чёткие правовые границы вмешательства государства в сферу частной жизни.

Привлечение федерального законодателя к регулированию статуса АПК «Безопасный город» обосновано не только правовыми, но и организационными соображениями: именно на федеральном уровне возможно обеспечить единообразие правоприменительной практики и установить минимальные гарантии защиты прав граждан, которые не могут быть снижены на региональном уровне. Кроме того, федеральный закон позволит устранить коллизию между правом на удаление данных (статья 21 Закона о персональных данных) и требованиями режима секретности применительно к специальным субъектам.

Вторым направлением является усиление контроля за неправомерной обработкой данных, фиксируемых устройствами «умного дома». Нелегальный сегмент рынка устройств, по ряду оценок, составляет значительную долю, представляет наибольшую опасность, поскольку функционирует вне какого-либо правового регулирования и не подчиняется ни одному из существующих или предлагаемых ограничений. Производители несертифицированных устройств не соблюдают требований к защите данных, не информируют пользователей о рисках, не предоставляют возможности удаления информации.

Предлагается комплекс мер по усилению контроля за неправомерной обработкой данных, включающий: ужесточение административной и уголовной ответственности за неправомерную обработку данных, фиксируемых устройствами «умного дома» (в том числе за передачу данных третьим лицам без согласия субъекта); расширение полномочий Роскомнадзора по оперативной блокировке интернет-ресурсов, распространяющих устройства, не соответствующие требованиям информационной безопасности; установление ответственности платёжных агрегаторов и кредитных организаций за осуществление переводов в адрес производителей, не прошедших обязательную сертификацию; проведение регулярных мониторинговых мероприятий с

⁸¹ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

⁸² Гражданский кодекс Российской Федерации (часть первая) : Федеральный закон от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301. – Ст. 152.2.

использованием автоматизированных систем обнаружения устройств, не соответствующих стандартам безопасности.

Для наглядного сопоставления предлагаемых мер и ожидаемых результатов целесообразно обратиться к табличной форме. Таблица 5 обобщает предлагаемые меры по усилению контроля за неправомерной обработкой данных.

Таблица 5 — Предлагаемые меры по усилению контроля за неправомерной обработкой данных в системах «умный дом»

Предлагаемая мера	Механизм реализации	Ожидаемый эффект
Ужесточение ответственности за неправомерную обработку данных	Внесение изменений в УК РФ и КоАП РФ	Повышение превентивного воздействия, снижение числа инцидентов
Расширение полномочий Роскомнадзора по блокировке	Внесение изменений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации...»	Сокращение времени доступности несертифицированных устройств
Ответственность платёжных посредников	Внесение изменений в Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе»	Ограничение финансовой инфраструктуры недобросовестных производителей
Автоматизированный мониторинг устройств	Разработка подзаконного акта, определяющего порядок мониторинга	Оперативное выявление и блокировка несертифицированных устройств

Приведённая систематизация демонстрирует, что контроль за неправомерной обработкой данных требует одновременного воздействия на несколько звеньев: производителей, техническую инфраструктуру и платёжные каналы. Изолированное воздействие на одно из звеньев не способно обеспечить системный результат.

4.4. Социально-экономические, юридические и иные последствия предлагаемых законодательных инициатив

Оценка последствий реализации выдвинутых в настоящей работе предложений предполагает анализ воздействия предполагаемых мер на различные группы общественных отношений. Для комплексного рассмотрения целесообразно структурировать ожидаемые последствия по нескольким направлениям.

Социальные последствия являются наиболее значимыми и определяют основную ценность предлагаемых инициатив. Введение легального определения данных, фиксируемых устройствами «умного дома», установление требований к их локальному хранению и обеспечение гарантированного удаления у всех лиц, которым они были переданы, в совокупности направлены на повышение уровня защищённости частной жизни граждан и укрепление доверия к цифровым технологиям. Создание механизма «сквозного» удаления данных призвано сократить разрыв между формальным закреплением права на удаление и его реальной исполнимостью⁸³. Принятие

⁸³ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451. – Ст. 21.

федерального закона «Об аппаратно-программном комплексе "Безопасный город"» позволит установить чёткие правовые границы вмешательства государства в сферу частной жизни, что будет способствовать снижению числа конфликтов между гражданами и правоохранительными органами, а также укреплению доверия к государственным программам цифровизации. Снижение числа инцидентов, связанных с неправомерной обработкой данных, в свою очередь, способно привести к уменьшению числа случаев мошенничества с использованием украденной информации, сокращению расходов граждан на восстановление нарушенных прав и укреплению института семьи за счёт снижения числа конфликтов, обусловленных утечками данных.

Экономические последствия носят двойственный характер. С одной стороны, установление требований к локальному хранению данных и обеспечению технической возможности удаления потребует от производителей дополнительных затрат на модернизацию устройств и сертификацию продукции. С другой стороны, экономические потери от неправомерной обработки данных — расходы на ликвидацию последствий утечек, компенсацию морального вреда, восстановление репутации — существенно превышают затраты на внедрение механизмов защиты⁸⁴. Кроме того, повышение доверия потребителей к системам «умного дома» будет способствовать росту рынка, объём которого, по данным экспертов, в 2025 году достиг 32 млрд рублей, а ежегодный прирост составляет 25–30 %⁸⁵. Борьба с несертифицированными устройствами при одновременном укрупнении легального рынка (сокращение числа производителей при сохранении или увеличении требований к безопасности) потенциально способна увеличить долю легального оборота и, следовательно, компенсировать часть выпадающих доходов.

Юридические последствия заключаются в формировании более целостной и внутренне непротиворечивой системы правового регулирования. Устранение выявленных пробелов (отсутствие легального определения данных, неопределённость круга операторов, отсутствие механизма гарантированного удаления) позволит привести законодательство в соответствие с конституционным принципом охраны частной жизни и международными стандартами⁸⁶.

Закрепление принципа защиты данных на этапе проектирования устройств создаст основу для объективного мониторинга оборота данных и формирования достоверной статистической базы, дефицит которой был отмечен в настоящей работе. Регулирование производных аналитических сведений позволит защитить цифровой профиль пользователя даже после отзыва согласия на обработку данных. Применительно к институциональным последствиям следует отметить, что предлагаемые меры предполагают расширение функциональности существующих институтов (Роскомнадзора, операторов данных) без создания принципиально новых административных структур, что минимизирует организационные издержки реформы. Возложение на Роскомнадзор полномочий по координации внедрения системы сертификации IoT-устройств представляется логичным и организационно оправданным, поскольку регулятор уже обладает инфраструктурой для

⁸⁴ Умный дом как инфраструктура данных: кто зарабатывает на цифровых привычках жильцов // Ведомости. – 2026. – 19 февраля. – URL: <https://www.vedomosti.ru/technology/articles/2026/02/19/1054321-umnyi-dom-kak-infrastruktura-dannyh> (дата обращения: 16.09.2026).

⁸⁵ Смарт-подход: спрос на установку систем умного дома в РФ вырос втрое // Известия. – 2026. – 18 июля. – URL: <https://iz.ru/1865789/2026-07-18/smart-podkhod-spros-na-ustanovku-sistem-umnogo-doma-v-rf-vyros-vtroe> (дата обращения: 19.09.2026).

⁸⁶ Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru> (дата обращения: 16.09.2026). – Ст. 23, 24, 25.

работы с персональными данными и взаимодействует с операторами по вопросам трансграничной передачи данных⁸⁷.

Сводная характеристика ожидаемых последствий представлена в таблице 6.

Таблица 6 — Ожидаемые последствия реализации предлагаемых законодательных инициатив

Направление воздействия	Позитивные последствия	Возможные негативные последствия	Способы минимизации негативных последствий
Социальные	Повышение уровня защищённости частной жизни, укрепление доверия граждан к цифровым технологиям, снижение числа инцидентов	Рост нагрузки на операторов при обработке требований об удалении	Поэтапное введение норм с переходными периодами
Экономические	Рост рынка IoT-устройств за счёт повышения доверия потребителей, снижение расходов на ликвидацию утечек	Дополнительные затраты производителей на модернизацию устройств	Государственная поддержка производителей, внедряющих принцип защиты данных на этапе проектирования
Юридические	Формирование целостной нормативной системы, устранение пробелов	Необходимость разработки значительного объёма подзаконных актов	Поэтапное введение норм с переходными периодами
Институциональные	Расширение функциональности существующих институтов без создания новых	Дополнительная нагрузка на Роскомнадзор	Выделение дополнительного финансирования, обучение сотрудников

Приведённый анализ свидетельствует о том, что совокупный позитивный эффект предлагаемых мер существенно превышает возможные негативные последствия, а последние могут быть эффективно минимизированы при условии комплексной и скоординированной реализации всех элементов предлагаемой реформы.

⁸⁷ Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.

ЗАКЛЮЧЕНИЕ

Проведённое исследование позволяет сформулировать ряд обобщающих выводов и рекомендаций.

Данные, фиксируемые устройствами «умного дома» (видеозаписи, голосовые команды, телеметрические показатели), представляют собой совокупность сведений, которая в отличие от разрозненных элементов позволяет с высокой степенью достоверности идентифицировать конкретное физическое лицо, восстановить распорядок его дня, поведенческие привычки, круг общения и иные аспекты частной жизни. В доктрине информационного права для обозначения данного феномена используется категория «цифровая тень» — пассивно формируемый информационный образ субъекта, создаваемый в результате автоматизированной обработки данных устройствами, не находящимися под его контролем. Принципиальное отличие цифровой тени от цифрового следа состоит в критерии субъекта сбора сведений: если цифровой след формируется осознанными действиями самого пользователя, то цифровая тень образуется независимо от его воли, зачастую без его осведомления, что делает уязвимость частной жизни особенно острой.

Статистическая картина распространения систем «умного дома» в Российской Федерации характеризуется критическим разрывом между темпами технологического развития и уровнем правовой защищённости фиксируемых данных. Объём российского рынка систем «умного дома» в 2025 году достиг 32 млрд рублей, ежегодный прирост составляет 25–30 %, а количество пользователей экосистем исчисляется миллионами. При этом централизованный учёт устройств «умного дома», объёмов фиксируемых ими данных и инцидентов, связанных с неправомерной обработкой такой информации, отсутствует. Понятие «данные, фиксируемые устройствами "умного дома"» не закреплено в законодательстве, а методики оценки объёмов обработки таких данных не унифицированы. Разрыв между экспертными оценками масштабов обработки данных и официальной статистикой утечек свидетельствует о системной неспособности государства объективно оценить масштаб проблемы.

Законодательные реформы 2025–2026 годов — Федеральный закон от 28.02.2025 № 23-ФЗ, установивший особенности обработки персональных данных отдельных категорий лиц, подлежащих государственной защите, и Федеральный закон от 24.06.2025 № 156-ФЗ, запретивший включение согласия на обработку персональных данных в другие документы, — представляют собой важный, но недостаточный шаг. Процедурный характер указанных новелл не затрагивает данных, собираемых автоматически, — видеозаписей с камер, голосовых команд, телеметрических показателей. Согласие на обработку такой информации презюмируется самим фактом использования устройства, что противоречит принципу свободного и информированного согласия. Отсутствие законодательных требований к получению согласия на обработку данных, фиксируемых устройствами «умного дома», означает, что производитель вправе передавать такие сведения третьим лицам, формируя цифровой профиль пользователя без его явного одобрения.

Сравнительно-правовой анализ зарубежного опыта (Европейский союз, США, Великобритания, Казахстан, Китай) подтверждает наличие апробированных инструментов, не задействованных в российской правовой системе: принцип «Privacy by Design», обязательная сертификация IoT-устройств на соответствие требованиям информационной безопасности, регулирование производных аналитических сведений, механизм «сквозного» удаления данных у всех лиц, которым они были переданы.

На основании проведённого анализа в работе сформулированы следующие законодательные инициативы, совокупная реализация которых способна качественно усилить правовую защищённость данных в системах «умного дома»:

- введение легального определения данных, фиксируемых устройствами «умного дома», в статью 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- установление требований к локальному хранению первичных данных на территории Российской Федерации, обеспечению технической возможности удаления данных по требованию субъекта в течение тридцати дней и обязательному уведомлению субъекта о передаче данных третьим лицам (дополнение статьи 6);

- обеспечение гарантированного удаления данных у всех лиц, которым они были переданы, в течение тридцати дней с момента получения требования субъекта (дополнение статьи 21);

- регулирование производных аналитических сведений, полученных в результате машинного обучения, посредством введения определения «производные персональные данные»;

- принятие федерального закона «Об аппаратно-программном комплексе "Безопасный город"», устанавливающего цели, объём и сроки хранения данных, порядок доступа правоохранительных органов (включая обязательность судебного решения), право гражданина на отключение своих устройств от государственной системы и ответственность за нарушение порядка удаления информации.

Государство должно последовательно двигаться по пути обеспечения баланса между публичными интересами безопасности и частными интересами защиты приватности, не допуская гипертрофированного усиления контрольных полномочий в ущерб конституционным правам граждан. Опыт Европейского союза и Великобритании свидетельствует о необходимости перехода от рекомендательных стандартов к обязательной сертификации IoT-устройств, обеспечивающей техническую возможность удаления данных на этапе проектирования. Опыт Китая демонстрирует риски приоритета публичного интереса над частным, что должно быть учтено при разработке российского законодательства.

Реализация предложенных мер способна привести к повышению уровня защищённости частной жизни граждан, укреплению доверия к цифровым технологиям, созданию условий для более широкого внедрения систем «умного дома», формированию достоверной статистической базы, необходимой для дальнейшего совершенствования государственной политики в данной сфере, а также к трансформации права на удаление информации из декларативного в реально исполнимое.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru> (дата обращения: 16.09.2026).
2. Гражданский кодекс Российской Федерации (часть первая) : Федеральный закон от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.
3. Жилищный кодекс Российской Федерации : Федеральный закон от 29.12.2004 № 188-ФЗ (ред. от 03.02.2025) // Собрание законодательства РФ. – 2005. – № 1 (ч. 1). – Ст. 14.
4. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 09.09.2026) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
5. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.
6. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.
7. О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации : Федеральный закон от 21.07.2014 № 242-ФЗ // Собрание законодательства РФ. – 2014. – № 30 (ч. I). – Ст. 4217.
8. О внесении изменений в Федеральный закон «О связи» и отдельные законодательные акты Российской Федерации : Федеральный закон от 06.07.2016 № 374-ФЗ // Собрание законодательства РФ. – 2016. – № 28. – Ст. 4558. Есть такой и полное название везде разное
9. О федеральной службе безопасности : Федеральный закон от 03.04.1995 № 40-ФЗ (ред. от 10.07.2023) // Собрание законодательства РФ. – 1995. – № 15. – Ст. 1269
10. Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) // Собрание законодательства РФ. – 1995. – № 33. – Ст. 3349.
11. О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации : Федеральный закон от 28.02.2025 № 23-ФЗ // Собрание законодательства РФ. – 2025. – № 10. – Ст. 1211.
12. О внесении изменений в статью 12 Федерального закона «О персональных данных» и отдельные законодательные акты Российской Федерации : Федеральный закон от 26.07.2026 № 265-ФЗ // Официальный интернет-портал правовой информации. – URL: <http://pravo.gov.ru> (дата обращения: 16.09.2026).
13. Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» : распоряжение Правительства Российской Федерации от 03.12.2014 № 2446-р (ред. от 05.04.2019) // Собрание законодательства РФ. – 2014. – № 50. – Ст. 7225.

Международные правовые акты и законодательство иностранных государств

14. Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных (Общий регламент по защите данных) // Официальный журнал Европейского союза. – 2016. – L 119. – С. 1–88.

15. Директива (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе (NIS2) // Официальный журнал Европейского союза. – 2022. – L 333. – С. 80–152.
16. California Senate Bill No. 327. Information Privacy: Connected Devices // California Legislative Information. – 2018. – URL: <https://leginfo.ca.gov> (дата обращения: 16.09.2026).
17. Personal Information Protection Law of the People's Republic of China // National People's Congress. – 2021. – URL: <http://www.npc.gov.cn> (дата обращения: 16.09.2026).
18. О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 года № 94-V // Ведомости Парламента Республики Казахстан. – 2013. – № 9–10. – Ст. 45.
19. Code of Practice for Consumer IoT Security // UK Department for Digital, Culture, Media & Sport. – 2018. – URL: <https://www.gov.uk> (дата обращения: 16.09.2026).

Научная литература

20. Белоусов, К. Интернет вещей: проблемные аспекты защиты персональных данных в рамках правоотношений / К. Белоусов // Цифровые технологии в системе правовых отношений : сборник научных трудов. – 2025. – С. 48–53.
21. Виноградова, Е. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации / Е. В. Виноградова, Т. А. Полякова, А. В. Минбалеев // Правоприменение. – 2021. – Т. 5, № 4. – С. 5–19.
22. Гапанович, А. В. Цифровые следы и цифровые тени: правовая квалификация / А. В. Гапанович // Юрист. – 2022. – № 6. – С. 2–7.
23. Камалова, Г. Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества : дис. ... д-ра юрид. наук : 12.00.13 / Камалова Гульфия Гафиятовна. – Москва, 2020. – 472 с.
24. Наумов, В. Б. Институт идентификации в информационном праве : дис. ... д-ра юрид. наук : 12.00.13 / Наумов Виктор Борисович. – Москва, 2021. – 450 с.
25. Полякова, Т. А. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации / Т. А. Полякова, А. В. Минбалеев, Н. В. Кроткова // Государство и право. – 2020. – № 5. – С. 75–87.
26. Полякова, Т. А. Понятие и правовая природа «цифровой зрелости» / Т. А. Полякова, А. В. Минбалеев // Государство и право. – 2021. – № 9. – С. 107–116.
27. Полякова, Т. А. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России / Т. А. Полякова, А. В. Минбалеев, Н. В. Кроткова // Государство и право. – 2024. – № 9. – С. 166–179.
28. Рыжков, Д. И. Нормативные подходы к правовому регулированию городов будущего: от умных счетчиков к умным домам / Д. И. Рыжков // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2026. – № 6. – С. 197–205.

29. Самодолов, А. П. Особенности развития «умных домов» в России / А. П. Самодолов, О. А. Самодолова, Е. В. Николаенко // Вестник ЮУрГУ. Серия «Строительство и архитектура». – 2021. – Т. 21, № 2. – С. 45–52.
30. Чубукова, С. Г. Системы субъектов информационного права: направления цифровой трансформации / С. Г. Чубукова // Вестник Московского университета. Серия 26: Государственный аудит. – 2019. – № 3. – С. 17–27.
31. Шугунов, Т. Л. Проблема нормативно-правового регулирования использования системы «Умный дом» в Российской Федерации / Т. Л. Шугунов, А. З. Жуков // Информационное право. – 2023. – № 19. – С. 32–35.
32. Wachter, S. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI / S. Wachter, B. Mittelstadt // Columbia Business Law Review. – 2019. – № 2. – P. 494–620.

IV. Электронные ресурсы и интернет-источники

33. Смарт-подход: спрос на установку систем умного дома в РФ вырос втрое // Известия. – 2026. – 18 июля. – URL: <https://iz.ru/1865789/2026-07-18/smart-podkhod-spros-na-ustanovku-sistem-umnogo-doma-v-rf-vyros-vtroe> (дата обращения: 19.09.2026).
34. Роскомнадзор зафиксировал снижение числа утечек персональных данных в 2025 году // ComNews. – 2026. – 22 января. – URL: <https://www.comnews.ru> (дата обращения: 16.09.2026).
35. StormWall: в 2025 году число DDoS-атак с умных устройств в РФ выросло в 5 раз // Газета.ру. – 2025. – 27 ноября. – URL: <https://mt.gazeta.ru> (дата обращения: 16.09.2026).
36. Уязвимость в Rubetek Home позволяла получить доступ к умному дому // Anti-Malware.ru. – 2025. – 23 мая. – URL: <https://www.anti-malware.ru> (дата обращения: 16.09.2026).
37. Встреча в цифровой гостиной // Юридический факультет МГУ. – 2026. – 24 апреля. – URL: <https://www.law.msu.ru/news> (дата обращения: 16.09.2026).
38. Для «умного дома» разработают стандарт, защищающий персональные данные жильцов // NormaCS. – URL: <https://ru.normacs.info/news/66875> (дата обращения: 16.09.2026).
39. Умный дом: из фантастики — в повседневность // ВЦИОМ. – 2025. – 15 июля. – URL: <https://wciom.ru> (дата обращения: 16.09.2026).
40. FCC Cyber Trust Mark // Federal Communications Commission. – 2024. – URL: <https://www.fcc.gov/cybertrustmark> (дата обращения: 16.09.2026).