

УДК 34**Правовое регулирование систем «умный дом»: аспекты стандартизации и кибербезопасности****Петренкова Софья Борисовна**

Кандидат педагогических наук,
Донской государственный технический университет,
344003, Российская Федерация, Ростов-на-Дону, пл. Гагарина, 1;
e-mail: spetrenkova@donstu.ru

Натарин Дмитрий Дмитриевич

Исследователь,
Донской государственный технический университет,
344003, Российская Федерация, Ростов-на-Дону, пл. Гагарина, 1;
e-mail: dmitrynatarin.jr@gmail.com

Аннотация

В статье рассматриваются комплексные правовые аспекты регулирования систем "умный дом" в России, охватывающие вопросы технической стандартизации, кибербезопасности, защиты персональных данных и гражданско-правовой ответственности. Особое внимание уделено противоречиям между требованиями законодательства о биометрических данных (152-ФЗ, 572-ФЗ) и технологическими возможностями IoT-устройств, а также проблемам интеграции с государственными системами (ГИС ЕБС). Анализируются механизмы обеспечения безопасности, включая формальную верификацию и сертификацию оборудования (ФЗ-384, ГОСТ Р 71200-2023). Определены ключевые направления совершенствования нормативной базы с учетом необходимости баланса между инновационным развитием и защитой прав пользователей.

Для цитирования в научных исследованиях

Петренкова С.Б., Натарин Д.Д. Правовое регулирование систем «умный дом»: аспекты стандартизации и кибербезопасности // Вопросы российского и международного права. 2025. Том 15. № 3А. С. 328-334.

Ключевые слова

Умный дом, правовое регулирование, IoT-устройства, биометрические данные, персональные данные, формальная верификация, сертификация, кибербезопасность, Жилищный кодекс РФ, технические стандарты, Единая биометрическая система, гражданско-правовая ответственность, электромагнитная безопасность.

Введение

Правовые аспекты функционирования систем "умный дом" образуют сложную многоуровневую систему регулирования, охватывающую различные отрасли права и требующую комплексного междисциплинарного подхода. В основе этой системы лежит необходимость балансирования между технологическим развитием и обеспечением безопасности, что обуславливает особый характер правовых отношений между всеми участниками процесса - от разработчиков и поставщиков услуг до конечных пользователей и государственных регуляторов.

Основное содержание

Современные интеллектуальные жилые системы представляют собой сложные киберфизические комплексы, объединяющие разнородные IoT-устройства, программное обеспечение и сетевую инфраструктуру. Их правовой статус в российском законодательстве определяется через совокупность нормативных актов различного уровня. Жилищный кодекс РФ (ст. 161) устанавливает общие требования к безопасности инженерных систем многоквартирных домов, распространяющиеся и на интеллектуальные компоненты. Более конкретные технические требования закреплены в стандартах ГОСТ Р 71200-2023 и ГОСТ Р 71868-2024, которые регламентируют вопросы совместимости оборудования, стандартизации интерфейсов и классификации зданий по уровню оснащенности. Особое значение имеет запрет на "залоченность" оборудования к конкретным производителям, направленный на предотвращение монополизации рынка и обеспечение свободы выбора для потребителей.

Обеспечение надежности работы систем "умный дом" требует применения современных методов контроля качества, среди которых центральное место занимает формальная верификация. Этот математически строгий метод доказательства корректности работы программного обеспечения позволяет выявлять потенциальные уязвимости на этапе разработки, минимизируя риски эксплуатационных сбоев. В контексте интеллектуальных жилых систем формальная верификация применяется для анализа алгоритмов работы IoT-устройств, сетевых протоколов и, что особенно важно, смарт-контрактов, управляющих автоматизацией домашних процессов. Однако применение этих методов сопряжено с существенными юридическими рисками, поскольку даже самый тщательный анализ не гарантирует абсолютной защиты от всех возможных угроз. Российское законодательство предусматривает многоуровневую систему ответственности за недостатки верификации - от административной (ст. 9.13 КоАП РФ) до уголовной (ст. 238 УК РФ), если они повлекли серьезные последствия.

Важным элементом системы обеспечения безопасности является институт обязательной сертификации, регламентируемый ФЗ-384 "Технический регламент о безопасности зданий". Этот нормативный акт устанавливает единые стандарты для критически важных компонентов умного дома, таких как системы контроля доступа, противопожарной сигнализации и аварийного отключения инженерных коммуникаций. Сертификация и формальная верификация выступают как взаимодополняющие механизмы контроля: если первая обеспечивает соответствие установленным нормативным требованиям, то вторая гарантирует корректность алгоритмической реализации. Такой дуализм создает комплексную систему гарантий безопасности, необходимую для устойчивого функционирования технологически сложных

жилых комплексов.

Обработка биометрических данных в системах "умный дом" представляет собой одну из наиболее сложных проблем современного правового регулирования, требующую тщательного баланса между технологическими возможностями и законодательными ограничениями. Российское законодательство, в частности 152-ФЗ "О персональных данных" и 572-ФЗ, устанавливает строгий режим работы с биометрической информацией, предусматривающий обязательное получение явного согласия пользователей и использование исключительно аккредитованных систем хранения, таких как Единая биометрическая система (ЕБС). Существенные штрафные санкции за нарушения, достигающие 20 млн рублей, отражают серьезность подхода государства к защите персональных данных в условиях активной цифровизации жилищного сектора. Однако практическая реализация этих требований сталкивается с существенными трудностями, обусловленными как технической сложностью интеграции распределенных IoT-систем с централизованными государственными платформами, так и необходимостью сохранения пользовательского удобства и доступности технологий.

Обязательное подключение к ГИС ЕБС при использовании биометрических технологий в частных жилых помещениях создает значительные барьеры для развития инновационных решений в сфере домашней автоматизации. Жесткие требования законодательства, запрещающие хранение биометрических данных вне аккредитованных систем, фактически исключают возможность применения локальных облачных хранилищ, встроенных непосредственно в инфраструктуру умного дома. Такой подход, безусловно направленный на усиление защиты персональной информации, одновременно приводит к усложнению архитектуры интеллектуальных жилых систем, требуя разработки сложных механизмов взаимодействия с централизованными государственными платформами. Это влечет за собой существенное увеличение стоимости решений, усложняет процессы их внедрения и эксплуатации, а также создает дополнительные препятствия для развития отечественных технологий в данной области. Возникающая в результате правовая коллизия между необходимостью обеспечения безопасности персональных данных и потребностями технологического прогресса требует поиска сбалансированных решений, которые позволили бы сохранить высокий уровень защиты информации, не препятствуя при этом развитию инновационных технологий умного дома. Особую актуальность приобретает разработка гибких нормативных подходов, учитывающих специфику работы распределенных IoT-систем и позволяющих найти оптимальное соотношение между требованиями безопасности и практическими аспектами внедрения интеллектуальных решений в жилищной сфере.

Гражданско-правовые аспекты эксплуатации умных домов строятся на договорных отношениях между собственниками жилья, управляющими организациями и поставщиками соответствующих услуг. Особенностью этих отношений является асимметрия технической компетентности сторон, что требует специальных механизмов защиты прав потребителей. Управляющие организации несут существенную ответственность за бесперебойную работу систем, причем в случае серьезных сбоев или утечек данных возможна не только административная, но и уголовная ответственность. Ярким примером служит некорректная работа датчиков утечки газа, которая при возникновении аварийной ситуации может квалифицироваться по ст. 238 УК РФ как оказание услуг, не отвечающих требованиям безопасности. В этом контексте особую важность приобретает право пользователей на доступ к информации о сертификации оборудования и результатах его верификации, особенно для

устройств, взаимодействующих с критической инфраструктурой.

Отдельного рассмотрения заслуживает проблема электромагнитной безопасности IoT-устройств. Несмотря на распространенные опасения пользователей, научные исследования подтверждают, что уровень излучения современных Wi-Fi-датчиков не превышает 10% от установленных санитарных норм, а особенности их импульсного режима работы дополнительно снижают потенциальное воздействие на организм человека. Однако существующая нормативная база в данной области остается фрагментарной и не успевает за технологическим развитием, ограничиваясь преимущественно рекомендательными стандартами. Этот правовой вакуум требует скорейшего заполнения через разработку обязательных технических регламентов, учитывающих специфику различных категорий IoT-устройств.

Перспективы развития правового регулирования умных домов связаны с необходимостью решения нескольких ключевых задач. Во-первых, требуется ускоренная разработка единых обязательных стандартов безопасности для всех компонентов интеллектуальных жилых систем. Во-вторых, необходимо создать эффективную систему сертификации, гармонизированную с международными техническими требованиями. В-третьих, особое внимание следует уделить вопросам распределения ответственности между участниками рынка с учетом их реальных возможностей влиять на безопасность системы. Важным направлением является также развитие механизмов страхования рисков, связанных с эксплуатацией умных домов.

Ключевым условием успешной цифровизации жилищного сектора становится разработка специализированных нормативных актов, учитывающих специфику интеллектуальных технологий. При этом важно сохранить баланс между стимулированием инноваций и защитой прав граждан, что требует гибкого подхода к нормотворчеству. Законодателю необходимо предусмотреть механизмы оперативного обновления нормативной базы в соответствии с технологическим прогрессом, что особенно актуально в условиях стремительного развития интернета вещей. Особого внимания заслуживает вопрос гармонизации российских технических стандартов с международными, что важно как для развития экспортного потенциала отечественных решений, так и для обеспечения совместимости импортного оборудования.

Формирование комплексной системы правового регулирования умных домов требует объединения усилий специалистов различных областей - юристов, инженеров, программистов, специалистов по кибербезопасности. Только такой междисциплинарный подход позволит создать устойчивую правовую платформу, обеспечивающую как технологическое развитие, так и надежную защиту интересов всех участников данного процесса. Особую роль в этом процессе должны играть саморегулируемые организации и отраслевые объединения, способные оперативно реагировать на изменения технологического ландшафта и выработать оптимальные подходы к регулированию.

В заключение следует отметить, что правовое регулирование систем "умный дом" находится на стыке нескольких динамично развивающихся областей - жилищного права, законодательства о персональных данных, технического регулирования и кибербезопасности. Его дальнейшее развитие будет определяться способностью законодателя находить баланс между различными, порой противоречивыми интересами, обеспечивая при этом необходимый уровень безопасности и защиты прав граждан. Уже сейчас очевидно, что без решения этих сложных правовых задач невозможно обеспечить устойчивое развитие рынка интеллектуальных жилых систем в России.

Заключение

Правовое регулирование систем "умный дом" в России формирует сложную и многогранную систему, находящуюся на пересечении различных отраслей законодательства. Современные интеллектуальные жилые системы, представляющие собой комплексные киберфизические образования, требуют особого подхода к правовому регулированию, сочетающего технические стандарты, требования безопасности и защиту прав пользователей. Ключевыми элементами этой системы выступают формальная верификация программного обеспечения и обязательная сертификация оборудования, которые вместе создают многоуровневую систему гарантий надежности и безопасности.

Особую сложность представляет регулирование обработки биометрических данных, где жесткие требования законодательства о защите персональных данных вступают в противоречие с технологическими возможностями распределенных IoT-систем. Обязательная интеграция с государственными системами, такая как подключение к Единой биометрической системе, создает существенные барьеры для развития инновационных решений, требуя поиска сбалансированных подходов, которые позволили бы сочетать высокий уровень защиты информации с удобством пользователей и технологической эффективностью.

Гражданско-правовые аспекты эксплуатации умных домов, включая вопросы ответственности за сбои в работе систем и защиту прав потребителей, также требуют особого внимания законодателя. Не менее важным является решение проблем электромагнитной безопасности IoT-устройств и разработка соответствующих технических регламентов.

Перспективы развития правового регулирования в этой сфере связаны с необходимостью решения нескольких ключевых задач: разработки единых стандартов безопасности, создания эффективной системы сертификации, гармонизированной с международными требованиями, четкого распределения ответственности между участниками рынка и развития механизмов страхования рисков. Особую роль в этом процессе должны играть саморегулируемые организации и отраслевые объединения, способные оперативно реагировать на технологические изменения.

Успешная цифровизация жилищного сектора возможна только при условии создания гибкой и сбалансированной нормативной базы, которая, с одной стороны, будет стимулировать технологическое развитие, а с другой - обеспечит надежную защиту прав и интересов всех участников процесса. Это требует тесного взаимодействия государства, бизнеса и научного сообщества, а также учета международного опыта при сохранении национальных особенностей регулирования. Только такой комплексный подход позволит создать устойчивую правовую платформу для развития интеллектуальных жилых систем в России.

Библиография

1. Bing Huang, Hai Dong, Athman Bouguettaya. Conflict Detection in IoT-based Smart Homes. 2021. 17 p. URL: <https://arxiv.org/pdf/2107.13179> (дата обращения: 21.06.2025).
2. Bryar A. Hassan, Shko M. Qader Formal Verification Model for Card-controlled Doors Using PROMELA with SPIN Model Checker: A Proposed Model. 2024. 12 p. URL: <https://www.researchgate.net/publication/382800981> (дата обращения: 21.06.2025).
3. David A., Kim G. Larsen, Axel Legay, Marius Mikučionis, Danny B. Poulsen. Uppaal SMC Tutorial /. – Aalborg : Aalborg University, 2018. 35 p. URL: <https://uppaal.org/texts/uppaal-smc-tutorial.pdf> (дата обращения: 21.06.2025).
4. Grobelna I., Gajewski K., Karatkevich A. A Systematic Review on the Applications of UPPAAL // Sensors. 2025. Vol. 25. № 11. Article 3484. DOI: 10.3390/s25113484.

5. Holzmann G.J. Basic SPIN Manual. 2023. URL: <https://spinroot.com/spin/Man/Manual.html> (дата обращения: 21.06.2025).
6. Huang Q., Zhang L. Using the SPIN Model Checker for Auto-Tuning // J. Math. Sci. 2025.
7. ISO/IEC 25010:2011. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models. Geneva: International Organization for Standardization, 2011. 31 p.
8. Kondratyev V. Automatic Verification of a Lip-Synchronisation Algorithm Using UPPAAL // Formal Methods Pract. 2024.
9. Lamport L. TLA+ Version 2: A Preliminary Guide. 11 Dec. 2018. 134 p. URL: <https://lamport.azurewebsites.net/tla/tla2-guide.pdf> (дата обращения: 21.06.2025).
10. Li Y., Chen X. Verifying ZooKeeper with TLA+ // Proc. ESEC/FSE. 2022.
11. Nielsen S. et al. A Toolchain for Domestic Heat-Pump Control Using UPPAAL Stratego // J. Syst. Arch. 2023.
12. Page M.J. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews // BMJ. 2021. Vol. 372. Article n71. DOI: 10.1136/bmj.n71.

Legal Regulation of Smart Home Systems: Aspects of Standardization and Cybersecurity

Sof'ya B. Petrenkova

PhD in Pedagogical Sciences,
Don State Technical University,
344003, 1, Gagarina Sq., Rostov-on-Don, Russian Federation;
e-mail: spetrenkova@donstu.ru

Dmitrii D. Natarin

Researcher,
Don State Technical University,
344003, 1, Gagarina Sq., Rostov-on-Don, Russian Federation;
e-mail: dmitrynatarin.jr@gmail.com

Abstract

The article examines comprehensive legal aspects of regulating smart home systems in Russia, covering issues of technical standardization, cybersecurity, personal data protection, and civil liability. Particular attention is paid to the contradictions between the requirements of legislation on biometric data (Federal Laws No. 152-FZ and No. 572-FZ) and the technological capabilities of IoT devices, as well as problems of integration with state systems (GIS EBS). The mechanisms for ensuring security, including formal verification and equipment certification (Federal Law No. 384-FZ, GOST R 71200-2023), are analyzed. Key directions for improving the regulatory framework are identified, taking into account the need to balance innovative development and the protection of user rights.

For citation

Petrenkova S.B., Natarin D.D. (2025) Pravovoe regulirovanie sistem «umnyj dom»: aspekty standartizacii i kiberbezopastnosti [Legal Regulation of Smart Home Systems: Aspects of Standardization and Cybersecurity]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (3A), pp. 328-334.

Keywords

Smart home, legal regulation, IoT devices, biometric data, personal data, formal verification, certification, cybersecurity, Housing Code of the Russian Federation, technical standards, Unified Biometric System, civil liability, electromagnetic safety.

References

1. Bing Huang, Hai Dong, Athman Bouguettaya (2021). *Conflict Detection in IoT-based Smart Homes*. 17 p. Available at: <https://arxiv.org/pdf/2107.13179> [Accessed 21.06.2025].
2. Bryar A. Hassan, Shko M. (2024) *Qader Formal Verification Model for Card-controlled Doors Using PROMELA with SPIN Model Checker: A Proposed Model*. 12 p. Available at: <https://www.researchgate.net/publication/382800981> [Accessed 21.06.2025].
3. David A., Kim G. Larsen, Axel Legay, Marius Mikučionis, Danny B. Poulsen (2018) *Uppaal SMC Tutorial*. Aalborg: Aalborg University. 35 p. Available at: <https://uppaal.org/texts/uppaal-smc-tutorial.pdf> [Accessed 21.06.2025].
4. Grobelna I., Gajewski K., Karatkevich A. (2025) A Systematic Review on the Applications of UPPAAL. *Sensors*, 25 (11). Article 3484. DOI: 10.3390/s25113484.
5. Holzmann G.J. (2023) Basic SPIN Manual.. Available at: <https://spinroot.com/spin/Man/Manual.html> [Accessed 21.06.2025].
6. Huang Q., Zhang L. (2025) Using the SPIN Model Checker for Auto-Tuning. *J. Math. Sci.*
7. ISO/IEC 25010:2011. *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models* (2011). Geneva: International Organization for Standardization.
8. Kondratyev V. (2024) Automatic Verification of a Lip-Synchronisation Algorithm Using UPPAAL. *Formal Methods Pract.*
9. Lamport L. (2018) *TLA+ Version 2: A Preliminary Guide*. 11 Dec. Available at: <https://lamport.azurewebsites.net/tla/tla2-guide.pdf> [Accessed 21.06.2025].
10. Li Y., Chen X. (2022) Verifying ZooKeeper with TLA+. *Proc. ESEC/FSE*.
11. Nielsen S. et al. (2023) A Toolchain for Domestic Heat-Pump Control Using UPPAAL Stratego. *J. Syst. Arch.*
12. Page M.J. et al. (2021) The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372. Article n71. DOI: 10.1136/bmj.n71.