DOI 10.37882/2223-2974.2025.06.38

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТА ВЕЩЕЙ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

LEGAL REGULATION OF THE INTERNET OF THINGS: CURRENT STATE AND DEVELOPMENT PROSPECTS

D. Chaikovsky
V. Izotova

Summary. The article is devoted to the analysis of legal challenges related to the development of the Internet of Things (IoT). Key issues are addressed, including the lack of a unified legal definition of IoT, risks to data privacy, cybersecurity vulnerabilities, and issues of responsibility and standardization. Special attention is paid to Russian legislation and international experience in regulating IoT. The authors propose solutions such as the development of specialized laws, enhanced data protection, increased security standards, and international harmonization of standards. The need for an integrated approach to balance technological progress and the protection of user rights is emphasized.

Keywords: Internet of things, IoT, information security of the Internet of things, legal problems of the Internet of things.

Чайковский Дмитрий Станиславович
кандидат физ.-мат. наук, доцент,
Саратовская государственная юридическая академия
chaikovskyds@gmail.com
Изотова Вера Филипповна
кандидат физ.-мат. наук, доцент,
Саратовская государственная юридическая академия
izotova-vf@yandex.ru

Аннотация. Статья посвящена анализу правовых вызовов, связанных с развитием интернета вещей (IoT). Рассматриваются ключевые проблемы, включая отсутствие единого юридического определения IoT, риски для конфиденциальности данных, уязвимости кибербезопасности, вопросы ответственности и стандартизации. Особое внимание уделено российскому законодательству и международному опыту регулирования IoT. Авторы предлагают пути решения, такие как разработка специализированных законов, усиление защиты данных, повышение стандартов безопасности и международная гармонизация норм. Подчеркивается необходимость комплексного подхода для баланса между технологическим прогрессом и защитой прав пользователей.

Ключевые слова: интернет вещей, IoT, информационная безопасность интернета вещей, правовые проблемы интернета вещей.

Современный мир стремительно движется к повсеместной цифровизации, и интернет вещей (Internet of Things, IoT) занимает в этом процессе ключевое место. По прогнозам исследовательской компании Transforma Insights количество IoT-устройств в мире вырастет до 5 миллиардов к 2030 году[1]. Однако столь бурное развитие технологии создает серьезные вызовы для правовой системы, которая не успевает адаптироваться к новым реалиям.

IoT-технологии проникли во все сферы жизни: от умных домов и носимых гаджетов до промышленных систем и городской инфраструктуры. При этом правовое регулирование этой области остается фрагментарным и несистемным, что создает значительные риски для безопасности [11–13], конфиденциальности и устойчивого развития цифровой экономики [6].

Данная работа посвящена анализу ключевых проблем правового регулирования IoT и поиску путей их решения.

[1] Current IoT Forecast Highlights. URL: https://transformainsights.com/research/forecast/highlights (Дата обращения: 21.04.2025).

Основные правовые проблемы IoT

Проблема правового определения и классификации IoT

Одна из основных проблем правового регулирования IoT заключается в отсутствии единого юридического определения интернета вещей. В разных странах и даже в различных нормативных актах одной страны можно встретить противоречивые трактовки этого понятия.

Например, в Европейском союзе IoT определяется как «инфраструктура взаимосвязанных физических объектов»[2], тогда как в американском законодательстве акцент делается на «автономные устройства, способные собирать и передавать данные»[3].

[2] Europe's Internet of Things Policy.URL: https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy (Дата обращения: 21.04.2025).

[3] S.1691 — A bill to provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes. URL: https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?s=1&r=1&q=%7B%22search%22%3A%22To+provide+minimal+cybersecurity+operational+standards+for+Internet-connected+devices+purchased+by+Federal+agencies%2C+and+for+other+purpose%22%7D (Дата обращения: 21.04.2025).

Отсутствие четко закреплённого законодательного определения IoT создает правовую неопределенность. Эта проблема усугубляется отсутствием четкой классификации IoT-устройств. Необходимо различать:

- Потребительские устройства (умные часы, домашние помощники);
- Промышленные системы (IIoT);
- Устройства критической инфраструктуры (например, умные сети энергоснабжения)
- Медицинские IoT-устройства

Каждая из этих категорий требует особого правового подхода, но современное законодательство не делает таких различий.

В Российском законодательстве IoT упоминается:

1. В Указе Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»: «интернет вещей — концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека;» [1].
2. В Распоряжении Правительства РФ от 25.03.2020 N 724-р «Об утверждении Концепции обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования»: «...»интернет вещей» — совокупность сетей межмашинных коммуникаций и систем хранения (обработки) больших данных, в которых за счет подключения датчиков и актуаторов (исполнительных механизмов) к сети реализуется цифровизация различных процессов и объектов (Internet of Things, IoT);...» [2].

В законодательстве РФ имеют связь с регулированием интернета вещей Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) «О персональных данных» [3], Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2025) [4], Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента РФ от 05.12.2016 N 646 [5].

В пункте 3 статьи 5, закона «О персональных данных» говорится о том, что «не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой» [3]. В пункте 2 этой же статьи также подчеркивается, что «обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных» [3]. Следуя этим принципам, очевидно, что необходимо указать, с какой целью обрабатываются данные конкретного человека. Кроме того, данные должны быть уничтожены или обезличены сразу по окончании срока выполнения цели, для которой они были собраны.

Таким образом, производителям устройств Интернета вещей необходимо информировать пользователей о целях обработки их персональных данных и сроках их хранения. Статья 6 этого же закона требует согласия пользователя на обработку его персональных данных, включая те, которые поступают от IoT-устройств. Кроме того, так как частная жизнь человека обладает неприкосновенностью, то сбор, хранение, использование и распространение информации о частной жизни лица без его согласия является нарушением.

Учитывая технические возможности IoT-устройств, сложно сказать какую именно информацию они собирают о человеке. Поэтому, для технологии Интернета вещей данный пункт требует пересмотра.

Доктрина информационной безопасности свидетельствует о растущем осознании государством значимости информационного права в нашей жизни, включая необходимость обеспечения информационной безопасности в сфере Интернета вещей, поскольку число пользователей данной технологии неуклонно растёт.

В настоящее время происходит формирование базы для разработки соответствующих норм. Например, «дорожная карта», в приказе Минкомсвязи России № 637 «Об утверждении Плана (дорожной карты) реализации Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации». Этот документ должен утвердить список федеральных органов исполнительной власти, ответственных за формирование и одобрение моделей угроз со стороны нарушителей для систем Интернета вещей, что уже указывает на осведомленность государственных органов о данной проблеме.

Некоторые пункты этого плана включают: «

- Утверждение моделей угроз и нарушителей для различных систем узкополосных беспроводных сетей связи «Интернета вещей».
- Проведение пилотных проектов по развёртыванию различных систем идентификации устройств «Интернета вещей».
- Международная и национальная стандартизация в области узкополосных беспроводных сетей связи «Интернета вещей».
- Нормативно-правовое обеспечение построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации.

- Радиочастотное обеспечение узкополосных беспроводных сетей связи «Интернета вещей».
- Разработка отраслевых разделов Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации.»[4]

Проблема защиты персональных данных

IoT-устройства собирают колоссальные объемы персональных данных, часто без должного информирования пользователей. Особую озабоченность вызывают:

- Данные о местоположении (геотрекинг)
- Биометрические данные (отпечатки пальцев, распознавание лица)
- Поведенческие данные (привычки, распорядок дня)
- Даже физиологические показатели (пульс, давление)

Современные правовые системы не всегда способны адекватно регулировать эти вопросы. Например, принцип «согласия на обработку данных», закрепленный в GDPR[5], трудно реализовать для IoT, где данные собираются постоянно и автоматически.

Яркий пример проблемы — случай с умными телевизорами Vizio, которые тайно собирали данные о просмотрах пользователей и продавали их рекламодателям. Компания была оштрафована на $2,2 млн, но подобные случаи продолжают происходить регулярно[6].

Вопросы кибербезопасности

IoT-устройства стали слабым звеном в кибербезопасности. Эксперты «Лаборатории Касперского» заявляли, что IoT-устройства часто отличаются слабой защитой, которую легко взломать[7]. По данным исследования Palo Alto Networks[8]:

- 98 % трафика IoT-устройств не шифруется
- 57 % устройств уязвимы к атакам средней или высокой степени тяжести
- 41 % атак происходит через устаревшие протоколы

Особенно тревожны случаи использования IoT-устройств в масштабных DDoS-атаках. Ботнет Mirai в 2016 году, состоявший из камер наблюдения и маршрутизаторов, парализовал работу Twitter, Netflix и других крупных сервисов[9].

Проблема усугубляется тем, что многие производители экономят на безопасности, а пользователи не используют надёжные пароли. В результате формируется огромная уязвимая экосистема.

Проблемы ответственности

С развитием автономных IoT-систем возникает сложный вопрос ответственности за причиненный вред. Рассмотрим несколько сценариев: Беспилотный автомобиль совершил ДТП — кто виноват? Умный медицинский прибор ошибся в диагнозе — кто ответит? Взломанная система «умного дома» стала причиной пожара — чья вина?

Современное законодательство не дает четких ответов на эти вопросы. В разных странах суды принимают противоречивые решения, что создает правовую неопределенность для всех участников рынка.

Проблемы стандартизации и совместимости

Отсутствие единых стандартов [7] — серьезный барьер для развития IoT. Разные производители используют:

- Различные протоколы связи (Zigbee, Z-Wave, Bluetooth, Wi-Fi)
- Несовместимые платформы
- Собственные стандарты безопасности

Это приводит к фрагментации рынка и усложняет регулирование. Потребитель, купивший устройство одной экосистемы, оказывается «заперт» в ней и не может легко перейти на другую платформу.

Пути решения правовых проблем IoT

Разработка комплексного законодательства

Необходимо принятие специализированных законов об IoT, которые:

- Предоставят четкое юридическое определение IoT

[4] Приказ Минкомсвязи России от 31.10.2019 N 637 «Об утверждении Плана (дорожной карты) реализации Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации». URL: https://digital.gov.ru/uploaded/files/plan-dorozhnaya-karta-realizatsii-kontseptsii-postroeniya-i-razvitiya-uzkopolosnyih-besprovodnyih-setej-svyazi-interneta-veschej-na-territorii-rossijskoj-federatsii_995PGX0.pdf (Дата обращения: 25.04.2025).

[5] General Data Protection Regulation. URL: https://gdpr-info.eu/ (Дата обращения: 21.04.2025).

[6] VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent. URL: https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million (Дата обращения: 21.04.2025).

[7] Исследование «Лаборатории Касперского» показало, насколько плохо защищены умные устройства. Рассказываем, как с этим жить. URL:https://www.kaspersky-security.ru/1392.html (Дата обращения: 21.04.2025).

[8] 2020 Unit 42 IoT Threat Report. URL:https://unit42.paloaltonetworks.com/iot-threat-report-2020 (Дата обращения: 21.04.2025).

[9] Крупнейшие кибератаки в истории. URL: https://ddos-guard.ru/blog/krupneishie-kiberataki-v-istorii (Дата обращения: 21.04.2025).

- Установят классификацию устройств
- Определят права и обязанности всех участников

Хорошим примером может служить европейский «Акт о киберустойчивости» (Cyber Resilience Act), который вводит обязательные требования безопасности для IoT-устройств[10].

Усиление защиты данных

Для решения проблем с персональными данными необходимо:

- Разработать специальные правила согласия для IoT
- Ввести обязательное шифрование данных
- Установить четкие сроки хранения данных
- Предусмотреть «право на забвение» для IoT

Особое внимание следует уделить «проектируемой конфиденциальности» (Privacy by Design) — принципу, согласно которому защита данных закладывается в устройство на этапе проектирования.

Повышение стандартов безопасности

Для решения проблем кибербезопасности необходимо:

- Ввести обязательную сертификацию IoT-устройств
- Запретить использование слабых паролей
- Установить обязательные сроки обновления ПО
- Создать систему мониторинга угроз

Пример удачного регулирования — британский закон PSTI (Product Security and Telecommunications Infrastructure)[11], который вводит жесткие требования к безопасности IoT.

Вот некоторые требования этого закона:

- Запрет на использование стандартных паролей. У каждого устройства должен быть уникальный пароль или пользователи должны устанавливать свой собственный пароль при настройке.
- Обновления безопасности. Производители должны предоставлять обновления безопасности в течение разумного периода, чтобы устройства оставались защищёнными от известных уязвимостей.
- Отчетность о уязвимостях. Производители должны сообщать правительству о любых значительных уязвимостях безопасности в своих продуктах в течение определённого срока.
- Штрафы за несоблюдение. Правительство может наложить значительные штрафы на компании, которые не соблюдают требования безопасности.

Четкое определение ответственности

Необходимо законодательно закрепить:

- Виды ответственности (производителя, оператора, пользователя)
- Механизмы страхования ответственности
- Процедуры возмещения вреда
- Особые правила для автономных систем

Важно разработать гибкую систему, которая будет справедливо распределять ответственность между всеми участниками.

Международная гармонизация

Решение проблем IoT требует международного сотрудничества:

- Разработка единых стандартов (через ITU, ISO, IEEE)
- Гармонизация законодательства
- Создание международных органов по сертификации
- Обмен информацией об угрозах

Перспективным направлением является развитие таких инициатив, как стандарт Matter для умного дома[12], который поддерживают крупнейшие технологические компании.

Заключение

Интернет вещей — это необратимый технологический тренд, который будет только усиливать свое влияние на нашу жизнь. Однако без адекватного правового регулирования развитие IoT несет серьезные риски для общества.

Предложенные в статье меры — разработка специального законодательства, усиление защиты данных, повышение стандартов безопасности, четкое определение ответственности и международная гармонизация — могут стать основой для создания сбалансированной правовой системы.

Реализация этих мер требует совместных усилий законодателей, бизнеса, технических экспертов и общества. Только так можно раскрыть потенциал IoT, минимизировав связанные с ним риски.

[10] The Cybersecurity Strategy. URL:https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (Дата обращения: 21.04.2025).

[11] The UK Product Security and Telecommunications Infrastructure (Product Security) regime. URL: https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime (Дата обращения: 21.04.2025).

[12] Создание фундамента и будущего IoT. URL: https://csa-iot.org/ru/ (Дата обращения: 21.04.2025).

Будущее цифровой экономики во многом зависит от того, насколько эффективно мы сможем решить обсуждаемые правовые проблемы. Это сложная задача, но ее решение необходимо для устойчивого развития технологий и защиты фундаментальных прав человека в цифровую эпоху.

ЛИТЕРАТУРА

1. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»
2. Распоряжение Правительства РФ от 25.03.2020 N 724-р «Об утверждении Концепции обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования»
3. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) «О персональных данных»
4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2025)
5. Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента РФ от 05.12.2016 N 646
6. Chaikovsky, D.S. Improvement of digital economy regulation through formation of big data categorial concepts / D.S. Chaikovsky, V.F. Izotova, E.I. Leskina // European proceedings of social and behavioural sciences: International Scientific and Practical Conference «State and Law in the Context of Modern Challenges» (SLCMC 2021), Саратов, 17 июня 2021 года / Editor(s): Sergey Afanasyev, Alexander Blinov, Sergey Belousov. Vol. 122. — Саратов: European Publisher, 2022. — P. 144–149. — DOI 10.15405/epsbs.2022.01.24.
7. Ковалева, Н.Н. Роль стандартов в правовом регулировании «умных городов» / Н.Н. Ковалева, Д.С. Чайковский, В.Ф. Изотова // Информационное право. — 2021. — № 3. — С. 10–14.
8. Artificial intelligence and social media: selfregulation and government control / N.N. Kovaleva, A.S. Anisimova, Yu.M. Tugusheva, M.A. Danilova // European proceedings of social and behavioural sciences: International Scientific and Practical Conference «State and Law in the Context of Modern Challenges» (SLCMC 2021), Саратов, 17 июня 2021 года / Editor(s): Sergey Afanasyev, Alexander Blinov, Sergey Belousov. Vol. 122. — Саратов: European Publisher, 2022. — P. 347–352. — DOI 10.15405/epsbs.2022.01.56.
9. Optimizing the implementation of university digitalization practices / N.N. Kovaleva, P.V. Eresko, V.F. Izotova, Ye.R. Gafarov // European proceedings of social and behavioural sciences: International Scientific and Practical Conference «State and Law in the Context of Modern Challenges» (SLCMC 2021), Саратов, 17 июня 2021 года / Editor(s): Sergey Afanasyev, Alexander Blinov, Sergey Belousov. Vol. 122. — Саратов: European Publisher, 2022. — P. 353–359.
10. Забайкин, Ю.В. Идентификация Интернета вещей в аспектах правового регулирования // Ю.В. Забайкин, Д.А. Лунькин // Вопросы российского и международного права. — 2023. — Т. 13, № 4-1. — С. 322–328. — DOI 10.34670/AR.2023.39.54.058.
11. Саранчук, Ю.М. Безопасность интернета вещей: вопросы совершенствования правового регулирования и ответственности субъектов экосистемы / Ю.М. Саранчук, М.С. Азаров // Advances in Law Studies. — 2020. — Т. 8, № 3. — С. 26–30. — DOI 10.29039/2409-5087-2020-8-3-26-30.
12. Пахаев, Х.Х. Обзор угроз безопасности Интернета вещей / Х.Х. Пахаев, Т.Г. Айгумов, Э.М. Абдулмукминова // Инженерный вестник Дона. — 2022. — № 10(94). — С. 260–271.
13. Соколовская, И.Э. Интернет вещей: безопасность и конфиденциальность в системе «Человек — технология» / И.Э. Соколовская // Научное мнение. — 2021. — № 11. — С. 69–79. — DOI 10.25807/22224378_2021_11_69.
14. Ермаков, С.А. Обзор существующих процедур контроля доступа в контексте обеспечения безопасности систем Интернета вещей / С.А. Ермаков, А.А. Болгов // Информация и безопасность. — 2022. — Т. 25, № 2. — С. 229–246. — DOI 10.36622/VSTU.2022.25.2.008.

Журнал «Современная наука: актуальные проблемы теории и практики»