Секция «Правовая информатика, информационное и цифровое право»

# «Интернет вещей» и приватность: правовое регулирование обработки персональных данных, собираемых устройствами

**Научный руководитель – Полянский Виктор Владимирович**

***Александрова Анна Сергеевна***
*Аспирант*
Самарский национальный исследовательский университет имени академика С.П. Королева, Самара, Россия
*E-mail: anna.alex2000@yandex.ru*

Стремительный рост числа устройств Интернета вещей (IoT) — от умных гаджетов до промышленных сенсоров — создает беспрецедентные возможности для сбора и обработки персональных данных. По прогнозам аналитических агентств, количество подключенных устройств IoT к 2025 году достигнет почти трех десятков миллиардов, что неизбежно влечет за собой существенное увеличение объемов собираемой информации [4].

Интернет вещей (IoT) — это глобальная сеть физических объектов, «умных» устройств и сенсоров с уникальными идентификаторами, передающих данные через сеть без прямого взаимодействия человека. Многообразие устройств IoT (от «умного дома» до промышленного интернета вещей — IIoT) и их масштаб создают существенные сложности в обеспечении конфиденциальности и защиты данных [2, с.7].

Данные, собираемые устройствами IoT, весьма разнообразны по своему характеру и степени чувствительности. К наиболее распространенным категориям относятся: данные о местоположении, полученные с GPS-трекеров или мобильных устройств; биометрические данные, такие как отпечатки пальцев или распознавание лица, используемые для аутентификации; данные о здоровье, включая показатели сердечного ритма, артериального давления и других параметров, собираемые медицинскими сенсорами; и, наконец, обширные массивы данных о поведении пользователя, собираемые различными приложениями и сервисами IoT. Этот широкий спектр информации, часто относящийся к категории персональных данных, требует особого внимания к вопросам безопасности и защиты от несанкционированного доступа и использования.

Специфика IoT создает определенные проблемы для обеспечения защиты данных. Масштабность сбора данных, связанная с огромным количеством подключенных устройств, делает задачу мониторинга и контроля за безопасностью исключительно сложной. Децентрализованная архитектура IoT, где данные обрабатываются на множестве распределенных устройств и платформ, затрудняет идентификацию оператора, обрабатывающего данные и определение ответственности за обработку и хранение информации. Сложность и многообразие используемых протоколов и интерфейсов увеличивают риск уязвимостей к кибератакам. Кроме того, недостаточная интеграция мер безопасности на уровне отдельных устройств и недостаток стандартизации в области безопасности IoT делают сети уязвимыми для различного рода злонамеренных действий, включая несанкционированный доступ, модификацию данных и DDoS-атаки. Все это в совокупности требует разработки новых подходов к обеспечению безопасности и защиты персональных данных в рамках постоянно расширяющегося пространства IoT.

В России правовое регулирование обработки персональных данных, в значительной степени опирающееся на Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», сталкивается с серьезными трудностями применительно к специфике Интернета вещей (IoT) [1]. Этот закон, разработанный для традиционных моделей обработки информации, не в полной мере учитывает архитектурные особенности IoT-систем.

Во-первых, получение информированного согласия пользователя на обработку данных в IoT-системах часто носит формальный характер из-за сложности технических аспектов и обширности собираемых данных. Обеспечение безопасности данных в распределенной архитектуре IoT затруднено уязвимостями устройств, недостаточной стандартизацией и незаявленным сбором данных (например, анализ местоположения для рекламы без уведомления). Трансграничная передача данных увеличивает риски правового несоответствия и утечек информации.

Во-вторых, отсутствие единого центра контроля и управления потоками данных в распределённых IoT-системах представляет собой серьёзную проблему для защиты персональных данных. Разрозненность устройств и платформ делает практически невозможным полное отслеживание и надзор за обработкой информации.

Из вышесказанного можно выделить три ключевые проблемы, требующие решений.

1) Неясный механизм ответственности в случае нарушения прав пользователей в распределенных IoT-системах, затрудняющий привлечение к ответственности виновных субъектов. Эта проблема усугубляется отсутствием ясных критериев определения ответственности в ситуациях, когда данные обрабатываются несколькими независимыми организациями.

2) Проблема «скрытой» обработки данных, где незаявленный сбор и использование персональных данных происходит без явного согласия пользователей. Это связано с тем, что многие устройства IoT собирают данные, которые не обязательно прямо необходимы для их заявленной функциональности.

3) Отсутствие эффективных механизмов контроля и надзора за безопасностью IoT-устройств, ведущее к распространению уязвимостей и риску масштабных утечек данных. Недостаток стандартизации и сложности сертификации создают благоприятные условия для злоумышленников [3, с.76-78].

Для решения этих проблем необходим комплексный подход. В первую очередь, требуется разработка и внедрение строгих стандартов безопасности для IoT-устройств, включая обязательную сертификацию и механизмы защиты от незаявленного сбора данных. Необходимо активное развитие технологий обеспечения приватности данных, например, федеративного обучения или гомоморфного шифрования, позволяющих минимизировать риски утечки информации [5]. Параллельно, требуется усиление просветительской работы среди пользователей для повышения их осведомленности о рисках и усиление контроля со стороны надзорных органов за соблюдением законодательства в сфере IoT. Наконец, необходимо совершенствование законодательства, включая более четкое определение ответственности и более строгие санкции за нарушение прав пользователей в контексте IoT.

## Источники и литература

1) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс»

2) Глушак, Е. В. Введение в Интернет вещей: учебное пособие / Е. В. Глушак, А. В. Куприянов. — Самара: Самарский университет, 2023. — 104 с

3) Проблемы безопасности Интернета вещей. Учебное пособие – М.: Мир науки, 2021. – Сетевое издание. Режим доступа: https://izd-mn.com/PDF/20MNNPU21.pdf

4) Количество IoT-подключений вырастет в 2025 году до 27 млрд / URL: https://iot.ru/riteyl/kolichestvo-iot-podklyucheniy-vyrastet-v-2025-godu-do-27-mlrd-

5) Федеративное обучение: Совместное машинное обучение без централизованных данных / URL: https://open.zeba.academy/federativnoe-obuchenie-sovmestnoe-mashinnoe-obuchenie-tsentralizovannykh-dannykh/