УДК 34 **DOI: 10.34670/AR.2023.75.92.045**

Развитие права в области IoT

Кучковская Наталья Валерьевна

Кандидат экономических наук, доцент,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, Ленинградский пр., 49;
e-mail: nk2@list.ru

Аннотация

Интернет вещей (IoT) - это технология, которая позволяет устройствам собирать и обмениваться данными между собой через интернет, чтобы автоматически контролировать и управлять различными системами. IoT применяется в различных областях, таких как здравоохранение, промышленность, транспорт и другие. Однако с развитием IoT возникает ряд проблем, связанных с безопасностью и защитой персональных данных. Эта статья будет посвящена развитию права в области IoT, рассмотрим основные проблемы и существующие регуляторные меры. Одной из основных проблем IoT является безопасность. Каждый день появляются новые уязвимости и методы атак на устройства IoT. Хакеры могут взломать устройства, чтобы получить доступ к персональным данным или использовать их в качестве ботнета для совершения кибератак. Кроме того, IoT может быть использовано для шпионажа и нанесения материального ущерба. Еще одной проблемой IoT является защита персональных данных. Устройства IoT могут собирать большие объемы данных, включая конфиденциальные данные о здоровье, финансовые данные и т.д. Поэтому необходимо усиливать правовое регулирование персональных данных, передающихся посредством технологий интернета вещей.

Для цитирования в научных исследованиях

Кучковская Н.В. Развитие права в области IoT // Вопросы российского и международного права. 2023. Том 13. № 4А. С. 350-356. DOI: 10.34670/AR.2023.75.92.045

Ключевые слова

Исследование, Интернет вещей, защита, право, развитие.

Введение

Для защиты прав потребителей и борьбы с проблемами безопасности и защиты данных были разработаны регуляторные меры. В данном разделе мы рассмотрим некоторые из них.

Одной из наиболее важных регуляторных мер, связанных с IoT, является GDPR. GDPR была принята в ЕС в 2016 году и вступила в силу в 2018 году. GDPR устанавливает стандарты защиты данных для организаций, которые собирают, хранят и обрабатывают персональные данные граждан ЕС. GDPR требует от организаций обеспечивать защиту персональных данных, включая устройства IoT.

Еще одной регуляторной мерой, которая может быть использована для улучшения безопасности IoT, являются правила безопасности в Интернете вещей Национального института стандартов и технологий (NIST). НИСТ разработало ряд рекомендаций и практик безопасности, которые организации могут использовать для защиты устройств IoT. Одна из ключевых рекомендаций NIST заключается в том, чтобы организации постоянно отслеживали уязвимости и выпускали обновления программного обеспечения для устройств IoT.

Основное содержание

В США в 2019 году был принят закон о безопасности Интернета вещей (IoT), который требует, чтобы устройства IoT, продаваемые федеральным правительством, отвечали определенным стандартам безопасности. Закон также устанавливает стандарты обеспечения конфиденциальности и защиты персональных данных. Хотя этот закон не распространяется на устройства, которые не продаются федеральным правительством, он является важным шагом в направлении улучшения безопасности IoT.

В России IoT также представляет собой значительный потенциал для улучшения различных областей, однако проблемы безопасности и защиты персональных данных в этой области не менее актуальны, чем в других странах. В данном разделе мы рассмотрим некоторые из основных регуляторных мер, связанных с IoT, которые существуют в России.

Федеральный закон "О персональных данных"

Один из основных законодательных актов, связанных с защитой персональных данных, в России - Федеральный закон "О персональных данных". Этот закон устанавливает правила сбора, использования и распространения персональных данных граждан России. Закон требует, чтобы все организации, которые собирают персональные данные граждан России, были зарегистрированы в Российском реестре операторов персональных данных.

Федеральный Закон "О защите прав потребителей"

Федеральный Закон "О защите прав потребителей" также является важным законодательным актом в России, который имеет отношение к IoT. Закон требует, чтобы все товары и услуги, которые продавцы предлагают потребителям, соответствовали определенным стандартам качества и безопасности.

В России также существуют Правила о защите персональных данных при обработке их в информационных системах персональных данных. Эти правила устанавливают требования к организациям, которые обрабатывают персональные данные граждан России, включая устройства IoT. Организации должны обеспечивать защиту персональных данных, включая устройства IoT, от несанкционированного доступа, утечек и других угроз безопасности.

Концепция безопасности Интернета вещей

В России также разработана Концепция безопасности Интернета вещей, которая устанавливает основные направления работы в области безопасности IoT в России. Концепция определяет основные риски и угрозы, связанные с IoT, а также определяет необходимые меры по их предотвращению и снижению последствий.

Кроме описанных выше регуляторных мер, в области IoT существуют и другие инициативы, направленные на улучшение безопасности и защиты данных. Например, международный стандарт ISO/IEC 27001:2013 устанавливает требования к системам управления информационной безопасностью (ИБ), включая устройства IoT. Этот стандарт может быть использован организациями для разработки и реализации мер по защите персональных данных и обеспечения безопасности IoT.

Также существуют инициативы, направленные на создание более безопасных устройств IoT. Например, группа экспертов Open Connectivity Foundation разработала стандарт OCF Security Profile, который определяет требования к безопасности устройств IoT, включая требования к защите персональных данных и безопасности сети. Этот стандарт может быть использован производителями устройств IoT для создания более безопасных устройств.

Еще одной важной темой в области IoT является защита интеллектуальной собственности. IoT устройства могут собирать большие объемы данных, которые могут содержать конфиденциальную информацию о бизнес-процессах и патентах. Поэтому защита интеллектуальной собственности является важной задачей в области IoT. Существуют инициативы по разработке стандартов и протоколов для защиты интеллектуальной собственности в IoT, например, стандарты Intellectual Property Exchange (IPX) и Trusted Platform Module (TPM).

Ниже приведены некоторые примеры случаев применения права в области IoT в мире:

1. Случай с Nest Labs - в 2014 году компания Nest Labs, производитель устройств умного дома, была подвержена обвинениям в нарушении закона об использовании персональных данных. Компания была обвинена в том, что она собирала данные о пользователях без их ведома и согласия, и использовала эти данные для целей маркетинга. В результате этого дела компания была вынуждена улучшить свои политики в области защиты данных и получить согласие пользователей на сбор и использование их персональных данных.

2. GDPR и камеры видеонаблюдения - с момента введения GDPR в Европейском союзе в 2018 году, было несколько случаев, когда компании были обвинены в нарушении правил GDPR в области использования камер видеонаблюдения. В 2020 году компания "H&M" была оштрафована на €35 миллионов за нарушение GDPR, связанное с использованием камер видеонаблюдения для наблюдения за сотрудниками.

3. Закон о защите Интернета вещей в США - в 2019 году в США был принят Закон о безопасности Интернета вещей (IoT), который устанавливает стандарты безопасности и защиты персональных данных для устройств IoT. Закон также требует, чтобы устройства IoT, продаваемые федеральным правительством, отвечали определенным стандартам безопасности.

4. Законодательные инициативы в Китае - в Китае существуют законодательные инициативы, направленные на улучшение безопасности и защиты данных в области IoT. В 2020 году Китай принял закон "О защите персональных данных", который устанавливает правила для сбора, использования и распространения персональных данных граждан Китая. Кроме того, в 2020 году была принята "Информационная безопасность Цифровой Шелковой дороги", которая устанавливает стандарты безопасности и защиты данных в области IoT.

5. Регуляторные меры в Японии - в Японии существуют регуляторные меры в области IoT,

направленные на улучшение безопасности и защиты данных. В 2020 году Япония приняла закон "О защите персональных данных", который устанавливает правила для сбора, использования и распространения персональных данных граждан Японии. Кроме того, в Японии создана экспертная группа по безопасности IoT, которая разрабатывает рекомендации и стандарты в области безопасности и защиты данных для устройств IoT.

6. Законодательство в Австралии - в Австралии существуют законодательные инициативы в области безопасности и защиты данных в области IoT. В 2020 году Австралия приняла Закон о кибербезопасности, который устанавливает требования к безопасности и защите персональных данных для устройств IoT. Кроме того, Австралийский совет по защите персональных данных (OAIC) разрабатывает рекомендации и руководства по безопасности и защите данных для устройств IoT.

7. Законодательные инициативы в Канаде - в Канаде существуют законодательные инициативы в области безопасности и защиты данных в области IoT. В 2020 году Канада приняла закон "О защите персональных данных", который устанавливает правила для сбора, использования и распространения персональных данных граждан Канады. Кроме того, Канадский совет по безопасности Интернета вещей (IoTAS) разрабатывает рекомендации и стандарты в области безопасности и защиты данных для устройств IoT.

В целом, во многих странах существуют законы и регуляторные меры, направленные на улучшение безопасности и защиты персональных данных в области IoT. Такие меры включают в себя установление стандартов безопасности, правила для сбора и использования персональных данных, а также разработку рекомендаций и руководств по безопасности и защите данных для устройств IoT. Кроме того, проводится работа по созданию более безопасных устройств IoT и обеспечению социальной и этической ответственности в развитии IoT.

IoT представляет собой значительный потенциал для улучшения различных областей, но проблемы безопасности и защиты персональных данных в этой области не менее актуальны, чем в других сферах. Регуляторные меры, такие как законы и стандарты, а также разработка более безопасных устройств IoT, могут помочь улучшить безопасность и защиту данных. Однако необходимо продолжать работу над улучшением стандартов и развитием новых технологий для создания безопасной и защищенной среды для IoT.

Кроме того, важно учитывать и социальные аспекты развития IoT. В силу широкого использования IoT в различных областях, включая здравоохранение, транспорт, производство, энергетику и т.д., могут возникать этические и правовые вопросы, связанные с использованием и обработкой персональных данных, автоматизацией процессов и т.д. Поэтому важно учитывать социальные аспекты развития IoT и проводить общественный диалог, чтобы учесть мнения и интересы различных сторон и обеспечить создание более этичной и справедливой среды для IoT.

Необходимо учитывать различия в правовых регуляторных мерах на разных рынках, что может привести к различиям в требованиях к безопасности и защите данных для устройств IoT, производимых и продаваемых в разных странах. Это может быть вызвано различиями в законодательстве, политических аспектах, экономической ситуации и т.д. Поэтому, при разработке и производстве устройств IoT, необходимо учитывать правовые регуляторные меры на различных рынках и обеспечивать соответствие требованиям в каждой стране.

В целом, IoT представляет собой значительный потенциал для улучшения различных областей и требует совместных усилий государства, бизнеса и общественности для обеспечения безопасности и защиты данных, развития новых технологий и учета социальных аспектов.

Заключение

В России также существуют регуляторные меры, которые направлены на улучшение безопасности и защиты персональных данных в области IoT. Федеральный закон "О персональных данных", закон "О защите прав потребителей" и Правила о защите персональных данных при обработке их в информационных системах персональных данных устанавливают требования к организациям, которые собирают и обрабатывают персональные данные граждан России, включая устройства IoT. Концепция безопасности Интернета вещей определяет основные риски и угрозы, связанные с IoT, и определяет необходимые меры по их предотвращению и снижению последствий.

Однако, как и в других странах, в России необходимо продолжать работу над улучшением стандартов безопасности и защиты данных для IoT, учитывая быстрое развитие технологий и появление новых угроз. Кроме того, необходимо обеспечить более эффективное взаимодействие между государственными органами, бизнесом и общественностью, чтобы совместно работать над созданием безопасной и защищенной среды для IoT в России.

IoT представляет собой значительный потенциал для улучшения различных областей, однако безопасность и защита персональных данных являются серьезными проблемами. Регуляторные меры, такие как GDPR, правила безопасности NIST и закон о безопасности IoT в США, могут помочь улучшить безопасность и защиту данных. Однако, с учетом быстрого развития технологий, необходимо продолжать работу над улучшением стандартов безопасности и защиты данных для IoT.

Библиография

1. Березин И. И. Особенности юридической защиты персональных данных в системах «умный дом» // Мир науки, культуры, образования. 2017. № 4. С. 79-81.
2. Джаннибекова Л. С., Савченко А. В. Анализ угроз и рисков информационной безопасности в системах интернета вещей // Технологии информационной и научной работы. 2019. № 2. С. 80-85.
3. Карташова Е. В., Шаламова М. В. Правовые аспекты использования «умных» технологий в медицине // Научный результат. Серия Медицина и фармация. 2018. Т. 4. № 3. С. 25-29.
4. Курбатов В. Н., Костромина Е. В. Правовое регулирование использования систем интернета вещей в сфере энергосбережения // Экономика и предпринимательство. 2020. № 4-1. С. 234-238.
5. Первова Ю. Ю., Березин И. И. Правовые аспекты использования систем интернета вещей в охране здоровья населения // Вестник Российского государственного университета правосудия. 2020. № 3. С. 100-105.
6. Томсон А. И. Правовые аспекты использования интернета вещей в системе управления производственными процессами // Вестник Московской государственной юридической академии имени О. Е. Кутафина (МГЮА). 2020. № 3. С. 155-160.
7. Шишкин А. А. Правовое регулирование использования систем интернета вещей в транспортной отрасли // Государство и право. 2018. № 10. С. 114-121.
8. Грибова И. Г. Защита персональных данных в интернете вещей: анализ правового регулирования // Вестник Томского государственного университета. Право. 2018. № 46. С. 82-89.
9. Мазуренко В. А. Правовые аспекты использования систем интернета вещей в бизнесе // Вестник Кемеровского государственного университета. 2019. № 4. С. 87-92.
10. Шурчкова М. В., Дарчук Е. В. Правовые аспекты использования интернета вещей в образовании // Инновационная экономика и общество. 2019. № 3. С. 130-133.
11. Шахназарова А. Г., Морозов А. А. Правовое регулирование использования систем интернета вещей в жилищном строительстве // Известия Уральского федерального университета. Серия 2. Гуманитарные науки. 2018. № 2. С. 135-144.
12. Рыбалка А. Н. Правовые аспекты использования интернета вещей в транспортных системах города // Юридическая наука и практика. 2020. № 3. С. 138-141.

Development of IoT law

Natal'ya V. Kuchkovskaya

PhD in Economics, Associate Professor,
Financial University under the Government of the Russian Federation,
125993, 49, Leningradskii ave., Moscow, Russian Federation;
e-mail: nk2@list.ru

Abstract

The Internet of Things (IoT) is a technology that allows devices to collect and exchange data among themselves over the Internet in order to automatically monitor and manage various systems. IoT is used in various fields, such as healthcare, industry, transport and others. However, with the development of IoT, a number of problems arise related to the security and protection of personal data. This article will be devoted to the development of law in the field of IoT, consider the main problems and existing regulatory measures. One of the main problems of IoT is security. New vulnerabilities and methods of attacks on IoT devices appear every day. Hackers can hack into devices to gain access to personal data or use them as a botnet to carry out cyber attacks. In addition, IoT can be used for espionage and material damage. Another IoT problem is the protection of personal data. IoT devices can collect large amounts of data, including sensitive health data, financial data, etc. If this data falls into the wrong hands, it can lead to serious consequences.

For citation

Kuchkovskaya N.V. (2023) Razvitie prava v oblasti IoT [Development of IoT law]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (4A), pp. 350-356. DOI: 10.34670/AR.2023.75.92.045

Keywords

Research, Internet of Things, protection, law, development.

References

1. Berezin I.I. Features of the legal protection of personal data in "smart home" systems // World of science, culture, education. 2017. No. 4. S. 79-81.
2. Dzhannibekova L. S., Savchenko A. V. Analysis of threats and risks of information security in the systems of the Internet of things // Technologies of information and scientific work. 2019. No. 2. S. 80-85.
3. Kartashova E. V., Shalamova M. V. Legal aspects of the use of "smart" technologies in medicine // Research Result. Series Medicine and Pharmacy. 2018. V. 4. No. 3. S. 25-29.
4. Kurbatov V. N., Kostromina E. V. Legal regulation of the use of Internet of things systems in the field of energy saving // Economics and Entrepreneurship. 2020. No. 4-1. pp. 234-238.
5. Pervova Yu. Yu., Berezin I. I. Legal aspects of the use of Internet of things systems in public health protection // Bulletin of the Russian State University of Justice. 2020. No. 3. P. 100-105.
6. Thomson A. I. Legal aspects of using the Internet of Things in the system of production process management // Bulletin of the Moscow State Law Academy named after O. E. Kutafin (MSLA). 2020. No. 3. S. 155-160.
7. Shishkin A. A. Legal regulation of the use of Internet of Things systems in the transport industry // State and Law. 2018. No. 10. P. 114-121.
8. Gribova I. G. Protection of personal data in the Internet of things: analysis of legal regulation // Bulletin of the Tomsk State University. Right. 2018. No. 46. S. 82-89.
9. Mazurenko V. A. Legal aspects of the use of Internet of Things systems in business // Bulletin of the Kemerovo State

University. 2019. No. 4. S. 87-92.
10. Shurchkova M. V., Darchuk E. V. Legal aspects of using the Internet of things in education // Innovative Economics and Society. 2019. No. 3. P. 130-133.
11. Shakhnazarova A. G., Morozov A. A. Legal regulation of the use of Internet of Things systems in housing construction. Bulletin of the Ural Federal University. Series 2. Humanities. 2018. No. 2. P. 135-144.
12. Rybalka A. N. Legal aspects of the use of the Internet of things in the transport systems of the city // Legal Science and Practice. 2020. No. 3. P. 138-141.