УДК 34 **DOI: 10.34670/AR.2023.80.68.026**

Правовой аспект кибербезопасности и IoT в России

Забайкин Юрий Васильевич

Кандидат экономических наук, доцент,
кафедра «Управление бизнесом и сервисных технологий»,
Российский биотехнологический университет,
125080, Российская Федерация, Москва, Волоколамское ш., 11;
e-mail: 79264154444@yandex.com

Лунькин Дмитрий Александрович

Кандидат экономических наук,
Российский государственный геологоразведочный университет,
117485, Российская Федерация, Москва, ул. Миклухо-Маклая, 23;
e-mail: lunkinda@mgri.ru

Аннотация

В современном мире, где все более широкое распространение получает Интернет вещей (IoT), кибербезопасность становится критически важным аспектом защиты данных и конфиденциальности. Каждый день в Интернете появляются новые уязвимости и методы взлома, которые способны причинить непоправимый ущерб как отдельному человеку, так и всему обществу. В этой статье будет рассмотрен правовой аспект кибербезопасности и IoT в России, включая нормативные правовые акты, регулирующие область кибербезопасности и IoT. Кибербезопасность и IoT (Internet of Things) стали важными аспектами в современном мире, в котором все больше устройств и приложений подключаются к интернету и обрабатывают большое количество конфиденциальной информации. Россия не является исключением, и проблема защиты данных и конфиденциальности становится все более актуальной. Кибербезопасность и IoT (Internet of Things) стали важными аспектами в современном мире, в котором все больше устройств и приложений подключаются к интернету и обрабатывают большое количество конфиденциальной информации. Россия не является исключением, и проблема защиты данных и конфиденциальности становится все более актуальной.

Для цитирования в научных исследованиях

Забайкин Ю.В., Лунькин Д.А. Правовой аспект кибербезопасности и IoT в России // Вопросы российского и международного права. 2023. Том 13. № 1А-2А. С. 200-207. DOI: 10.34670/AR.2023.80.68.026

Ключевые слова

Правовой аспект, кибербезопасность, Интернет вещей, исследование, право.

Введение

Правовой аспект кибербезопасности в России регулируется рядом законов и нормативных актов, которые направлены на защиту информации, сетей и систем от несанкционированного доступа, а также на обеспечение безопасности критической информационной инфраструктуры.

Основными нормативно-правовыми актами, регулирующими вопросы кибербезопасности в России, являются:

– Конституция Российской Федерации: закрепляет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
– Уголовный кодекс РФ: содержит статьи, предусматривающие ответственность за незаконный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ (ст. 273), нарушение правил работы компьютерных систем и сетей (ст. 274) и т.д.
– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: определяет основные правила обработки и защиты информации, регулирует деятельность по обеспечению информационной безопасности.
– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»: устанавливает требования к защите критической информационной инфраструктуры, определяет ответственность за ее нарушение.
– Федеральный закон от 27.12.2010 № 403-ФЗ «О противодействии терроризму»: включает положения о защите информационных систем от террористической деятельности.

Помимо указанных законов, регулирование кибербезопасности в России осуществляется через различные подзаконные акты и стратегии, а также международные соглашения и нормы [Колесников, Дорохов, 2015].

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает общие правила для обработки информации в Российской Федерации. В соответствии с этим законом, каждый субъект обработки данных обязан обеспечить защиту информации, содержащейся в информационных системах.

Закон устанавливает требования к защите информации от несанкционированного доступа, использования, изменения и уничтожения. Кроме того, закон включает положения о защите персональных данных, которые должны быть защищены от незаконного доступа и использования [Попов, 2017].

Реализация многих мер безопасности, установленных законодательством, остается на усмотрение производителей устройств IoT, что может привести к снижению уровня защиты данных. Недавно были выявлены уязвимости в устройствах IoT, которые могут быть использованы злоумышленниками для получения доступа к конфиденциальной информации [Хачатурян, 2013].

Для решения проблемы защиты кибербезопасности и IoT в России были приняты ряд правовых мер. Одной из таких мер является создание государственных органов, которые занимаются вопросами кибербезопасности. В 2016 году был создан Федеральный центр кибербезопасности при Федеральной службе безопасности Российской Федерации. Этот центр занимается защитой информационных систем государственных органов, а также осуществляет мероприятия по выявлению и предотвращению кибератак [Козлов, 2014].

Другой мерой по защите кибербезопасности и IoT является обучение населения и

специалистов в области информационной безопасности. В России проводятся многочисленные семинары и тренинги для сотрудников компаний, специализирующихся на разработке и производстве устройств IoT, а также для пользователей этих устройств. Кроме того, в ряде высших учебных заведений России открыты специальности, связанные с кибербезопасностью и IoT.

Еще одной мерой по защите кибербезопасности и IoT в России является проведение аудитов информационных систем и устройств IoT. Аудит проводится для выявления уязвимостей и устранения их до того, как они могут быть использованы злоумышленниками. Аудит информационных систем и устройств IoT проводится как государственными органами, так и частными компаниями.

Были приняты меры по усилению ответственности за нарушение правил кибербезопасности и защиты данных. В России введены штрафы и уголовная ответственность за нарушение правил защиты персональных данных. Кроме того, за нарушение правил кибербезопасности могут быть применены административные и уголовные меры ответственности.

Федеральный закон от 7 июля 2003 года № 126-ФЗ «Об связи» регулирует область связи и телекоммуникаций в России. Этот закон устанавливает требования к качеству услуг связи, а также регулирует правила использования технологий связи, включая IoT. В соответствии с этим законом, провайдеры связи обязаны обеспечивать защиту технических средств связи от несанкционированного доступа и использования. Кроме того, закон содержит положения о защите персональных данных, передаваемых через технические средства связи [Попов, 2015].

Помимо Федерального закона от 27 июля 2006 года № 149-ФЗ и Федерального закона от 7 июля 2003 года № 126-ФЗ, существует ряд других нормативно-правовых актов, которые регулируют область кибербезопасности и IoT в России. В частности, в 2019 году был принят закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части повышения государственной защиты информации» (Федеральный закон от 18 апреля 2019 года № 66-ФЗ), который вводит ряд новых требований к защите информации в России.

В соответствии с этим законом, с 1 июля 2021 года все производители и поставщики технических средств связи, включая устройства IoT, должны предоставлять информацию о защите своих устройств и обеспечивать возможность обновления программного обеспечения для устранения уязвимостей безопасности [Казакова, 2016].

Закон вводит требования к шифрованию данных, передаваемых через технические средства связи, и устанавливает обязательность использования отечественного программного обеспечения для обработки и хранения конфиденциальной информации государственных органов.

Даже при наличии нормативных правовых актов, кибербезопасность и IoT остаются актуальной проблемой в России. Многие устройства IoT, которые используются в России, производятся за рубежом и не всегда соответствуют требованиям российского законодательства. Кроме того, реализация многих мер безопасности, установленных законодательством, остается на усмотрение производителей устройств IoT, что может привести к снижению уровня защиты данных.

Правовые меры по защите кибербезопасности и IoT в России

Для решения проблемы защиты кибербезопасности и IoT в России были приняты ряд правовых мер. Одной из таких мер является создание государственных органов, которые занимаются вопросами кибербезопасности. В 2016 году был создан Федеральный центр

кибербезопасности при Федеральной службе безопасности Российской Федерации.

Этот центр занимается защитой информационных систем государственных органов, а также осуществляет мероприятия по выявлению и предотвращению кибератак.

Другой мерой по защите кибербезопасности и IoT является обучение населения и специалистов в области информационной безопасности. В России проводятся многочисленные семинары и тренинги для сотрудников компаний, специализирующихся на разработке и производстве устройств IoT, а также для пользователей этих устройств. Кроме того, в ряде высших учебных заведений России открыты специальности, связанные с кибербезопасностью и IoT.

Еще одной мерой по защите кибербезопасности и IoT в России является проведение аудитов информационных систем и устройств IoT. Аудит проводится для выявления уязвимостей и устранения их до того, как они могут быть использованы злоумышленниками. Аудит информационных систем и устройств IoT проводится как государственными органами, так и частными компаниями.

Были приняты меры по усилению ответственности за нарушение правил кибербезопасности и защиты данных. В России введены штрафы и уголовная ответственность за нарушение правил защиты персональных данных. Кроме того, за нарушение правил кибербезопасности могут быть применены административные и уголовные меры ответственности.

Однако, несмотря на принятые меры, защита кибербезопасности и IoT остается актуальной проблемой в России. Важно продолжать работу над улучшением законодательства в этой области, а также совершенствовать технологии и методы защиты информации.

Необходимо обеспечить более тесное сотрудничество между государственными органами, частными компаниями и общественными организациями в области кибербезопасности. Кроме того, необходимо проводить более эффективную работу по информированию населения о рисках, связанных с использованием устройств IoT, а также о мерах по защите данных и конфиденциальности.

Важно продолжать работу над улучшением законодательства в этой области, а также совершенствовать технологии и методы защиты информации. Кроме того, необходимо обеспечить более тесное сотрудничество между государственными органами, частными компаниями и общественными организациями в области кибербезопасности. Вместе эти меры могут помочь обеспечить более эффективную защиту кибербезопасности и IoT в России. Защита кибербезопасности и IoT является задачей не только государства и компаний, но и каждого пользователя. Пользователи должны быть более внимательны к своей информационной безопасности и принимать меры по защите своих данных. Это может включать в себя использование надежных паролей, установку антивирусных программ и регулярное обновление программного обеспечения [Котляров, 2012].

Также важно отметить, что защита кибербезопасности и IoT является глобальной проблемой, которая требует сотрудничества между различными странами. Россия активно участвует в международном сотрудничестве в области кибербезопасности, в том числе через участие в международных конференциях и форумах [Голубева, 2017].

Таким образом, защита кибербезопасности и IoT является важной проблемой для России и всего мира. В России приняты ряд правовых мер, направленных на улучшение защиты данных и конфиденциальности. Однако, чтобы достичь более эффективной защиты кибербезопасности и IoT, необходимо продолжать работу над улучшением законодательства, совершенствованием технологий и методов защиты информации, а также обеспечивать более тесное сотрудничество между государственными органами, частными компаниями и общественными организациями в

этой области.

В рамках правового аспекта кибербезопасности в Российской Федерации основное внимание уделяется регулированию и контролю за обеспечением безопасности информационных систем и сетей, а также защите критической информационной инфраструктуры.

Согласно данным на 2023 год, в регулировании кибербезопасности можно выделить следующие ключевые направления:

– Обеспечение суверенитета информационного пространства: в последние годы правительство России уделяет особое внимание развитию собственных технологий и инфраструктуры для обеспечения информационной независимости и устойчивости. Это позволяет им контролировать обмен данными и предотвращать иностранные вмешательства.
– Защита персональных данных: в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», организации обязаны обеспечивать конфиденциальность и защиту персональных данных при их обработке.
– Сотрудничество с международными организациями и партнерами: Россия активно вовлечена в сотрудничество с международными организациями, такими как ООН, Международная организация по стандартизации (ISO) и Совет Европы. Это содействует разработке общих подходов и рекомендаций по обеспечению кибербезопасности на международном уровне.
– Развитие национальной системы образования и подготовки кадров в области кибербезопасности: Усиление требований к кибербезопасности приводит к возрастанию спроса на квалифицированных специалистов в этой сфере. Россия стремится развивать образовательные программы и научные исследования для подготовки высококлассных экспертов в области кибербезопасности.
– Противодействие киберпреступлениям: с учетом постоянного развития киберпространства и появления новых угроз, правоохранительные органы России активно совершенствуют свои методы и под ходы по борьбе с киберпреступлениями.
– Развитие нормативной базы: Правительство России продолжает работу над усовершенствованием законодательства в области кибербезопасности, чтобы адаптировать его к быстро меняющимся реалиям киберпространства. Введение новых нормативных актов и корректировка существующих законов позволяют эффективнее регулировать сферу кибербезопасности и усиливать защиту интересов граждан и организаций.
– Повышение уровня государственного контроля: правительство России укрепляет государственный контроль в области кибербезопасности с помощью различных инструментов, таких как аудиты, лицензирование и сертификация, а также введение обязательных требований к защите информации для критической информационной инфраструктуры.
– Создание механизмов взаимодействия между государственными и частными организациями: в целях более эффективной реализации политики в области кибербезопасности и координации деятельности различных участников, в России создаются механизмы взаимодействия между государственными органами, частным сектором и научно-образовательными учреждениями. Это позволяет объединять усилия в области кибербезопасности и обеспечивать обмен информацией, опытом и технологиями.

Заключение

Кибербезопасность и IoT становятся все более важными аспектами защиты данных и конфиденциальности в современном мире. В России эта область регулируется рядом нормативно-правовых актов, которые устанавливают требования к защите информации, в том числе персональных данных, и технических средств связи, включая устройства IoT. Однако, несмотря на принятые меры, кибербезопасность и IoT остаются актуальной проблемой в России.

Для решения проблемы защиты кибербезопасности и IoT необходимо продолжать работу над улучшением законодательства в этой области, а также совершенствовать технологии и методы защиты информации. Важно также обеспечить более тесное сотрудничество между государственными органами, частными компаниями и общественными организациями в области кибербезопасности, а также проводить более эффективную работу по информированию населения о рисках, связанных с использованием устройств IoT и мерах по защите данных и конфиденциальности. Вместе эти меры могут помочь обеспечить более эффективную защиту кибербезопасности и IoT в России.

Библиография

1. Бирюков Д.В. Правовые аспекты кибербезопасности в России // Вестник Пермского государственного университета. 2013. № 2. С. 87-92.
2. Голубева И.В. Кибербезопасность в России: проблемы и перспективы // Электронный журнал «Экономика и предпринимательство». 2017. Т. 1. № 1. С. 9-15.
3. Казакова О.А. Интернет вещей и проблемы кибербезопасности в России // Право и экономика. 2016. № 3. С. 26-32.
4. Козлов В.А. Кибербезопасность и Интернет вещей: проблемы и перспективы // Безопасность жизнедеятельности. 2014. № 1. С. 39-45.
5. Колесников Д.В., Дорохов В.В. Кибербезопасность в России: проблемы и перспективы // Наука и образование. 2015. № 7. С. 60-66.
6. Котляров В.В. Кибербезопасность в России: современное состояние и перспективы // Вестник Иркутского государственного университета. 2012. № 5. С. 64-69.
7. Курбанов Р.Ш. Кибербезопасность и Интернет вещей: анализ проблем и перспектив // Информационное общество. 2018. № 4. С. 32-36.
8. Мохов А.В. Правовой аспект кибербезопасности в России // Вестник Санкт-Петербургского университета. 2016. Сер. 12. Вып. 1. С. 116-119.
9. Попов А.Н. Кибербезопасность в России: современные вызовы и перспективы // Информационные технологии и право. 2015. № 1. С. 7-15.
10. Попов Н.В. Кибербезопасность и Интернет вещей // Техника и технологии безопасности. 2017. № 1. С. 9-17.
11. Хачатурян В.Х. Правовое регулирование кибербезопасности в России // Право и политика. 2013. № 1. С. 93-98.

Legal aspect of cybersecurity and IoT in Russia

Yurii V. Zabaikin

PhD in Economics, Associate Professor,
Department "Business Management and Service Technologies",
Russian Biotechnological University,
125080, 11, Volokolamsk sh., Moscow, Russian Federation;
e-mail: 79264154444@yandex.com

Dmitrii A. Lun'kin

PhD in Economics,
Russian State Geological Prospecting University,
117485, 23, Miklukho-Maklaya str., Moscow, Russian Federation;
e-mail: lunkinda@mgri.ru

Abstract

In today's world, where the Internet of Things (IoT) is becoming increasingly widespread, cybersecurity is becoming a critical aspect of data protection and privacy. Every day, new vulnerabilities and hacking methods appear on the Internet that can cause irreparable damage to both an individual and the whole society. This article will consider the legal aspect of cybersecurity and IoT in Russia, including regulatory legal acts regulating the field of cybersecurity and IoT. Cybersecurity and IoT have become important aspects in the modern world, in which more and more devices and applications are connected to the Internet and process a large amount of confidential information. Russia is no exception, and the problem of data protection and privacy is becoming more and more urgent. Cybersecurity and IoT become important aspects in the modern world, in which more and more devices and applications are connected to the Internet and process a large amount of confidential information. Russia is no exception, and the problem of data protection and privacy is becoming more and more urgent. To solve the problem of protecting cybersecurity and IoT, it is necessary to continue working on improving legislation in this area, as well as improving technologies and methods for protecting information. It is also important to ensure closer cooperation between government agencies, private companies and public organizations in the field of cybersecurity, as well as to work more effectively to inform the public about the risks associated with the use of IoT devices and data protection and privacy measures.

For citation

Zabaikin Yu.V., Lun'kin D.A. (2023) Pravovoi aspekt kiberbezopasnosti i IoT v Rossii [Legal aspect of cybersecurity and IoT in Russia]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (1A-2A), pp. 200-207. DOI: 10.34670/AR.2023.80.68.026

Keywords

Legal aspect, cybersecurity, Internet of Things, research, law.

References

1. Biryukov D.V. (2013) Pravovye aspekty kiberbezopasnosti v Rossii [Legal Aspects of Cybersecurity in Russia]. *Vestnik Permskogo gosudarstvennogo universiteta* [Bulletin of the Perm State University], 2, pp. 87-92.
2. Golubeva I.V. (2017) Kiberbezopasnost' v Rossii: problemy i perspektivy [Cybersecurity in Russia: problems and prospects]. *Ekonomika i predprinimatel'stvo* [Economics and Entrepreneurship], 1, 1, pp. 9-15.
3. Kazakova O.A. (2016) Internet veshchei i problemy kiberbezopasnosti v Rossii [Internet of Things and Cybersecurity Problems in Russia]. *Pravo i ekonomika* [Law and Economics], 3, pp. 26-32.
4. Khachaturyan V.Kh. (2013) Pravovoe regulirovanie kiberbezopasnosti v Rossii [Legal regulation of cybersecurity in Russia]. *Pravo i politika* [Law and Politics], 1, pp. 93-98.
5. Kolesnikov D.V., Dorokhov V.V. (2015) Kiberbezopasnost' v Rossii: problemy i perspektivy [Cybersecurity in Russia: problems and prospects]. *Nauka i obrazovanie* [Science and education], 7, pp. 60-66.
6. Kotlyarov V.V. (2012) Kiberbezopasnost' v Rossii: sovremennoe sostoyanie i perspektivy [Cybersecurity in Russia: current state and prospects]. *Vestnik Irkutskogo gosudarstvennogo universiteta* [Bulletin of the Irkutsk State University], 5, pp. 64-69.

7. Kozlov V.A. (2014) Kiberbezopasnost' i Internet veshchei: problemy i perspektivy [Cybersecurity and the Internet of Things: Problems and Prospects]. *Bezopasnost' zhiznedeyatel'nosti* [Life Safety], 1, pp. 39-45.
8. Kurbanov R.Sh. (2018) Kiberbezopasnost' i Internet veshchei: analiz problem i perspektiv [Cybersecurity and the Internet of Things: Analysis of Problems and Prospects]. *Informatsionnoe obshchestvo* [Information Society]. 2018. № 4. S. 32-36.
9. Mokhov A.V. (2016) Pravovoi aspekt kiberbezopasnosti v Rossii [Legal aspect of cybersecurity in Russia]. *Vestnik Sankt-Peterburgskogo universiteta* [Bulletin of St. Petersburg University], 12, 1, pp. 116-119.
10. Popov A.N. (2015) Kiberbezopasnost' v Rossii: sovremennye vyzovy i perspektivy [Cybersecurity in Russia: Modern Challenges and Prospects]. *Informatsionnye tekhnologii i pravo* [Information Technologies and Law], 1, pp. 7-15.
11. Popov N.V. (2017) Kiberbezopasnost' i Internet veshchei [Cybersecurity and the Internet of things]. *Tekhnika i tekhnologii bezopasnosti* [Safety engineering and technology], 1, pp. 9-17.