**УДК 004.056.53**

# ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IoT-СИСТЕМ И «УМНОГО» ДОМА

**Данила Павлович Козлов**
студент
thepolarospl@yandex.ru
**Наталия Владимировна Пчелинцева**
старший преподаватель
natas79@mail.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

**Аннотация.** Статья посвящена актуальным вопросам безопасности в Интернете вещей (IoT) и концепции «Умного дома». В ней подробно анализируются основные угрозы и уязвимости, присущие устройствам iOS, а также освещаются современные подходы к обеспечению информационной безопасности, такие как криптографические алгоритмы, многофакторная аутентификация, системы обнаружения вторжений и инструменты мониторинга. Основное внимание уделяется внедрению эффективных мер информационной безопасности в системах «Умный дом» и изучению путей развития технологий защиты данных в рамках Интернета вещей.

**Ключевые слова:** интернет вещей, IoT, безопасность информации, умный дом, криптография, аутентификация, защита данных, кибератаки.

Сегодня концепция Интернета вещей (IoT) и технологии «умного дома» прочно вошли в нашу повседневную жизнь. Международное исследовательское агентство IDC прогнозирует, что к 2025 году количество устройств, подключенных к Интернету вещей, достигнет 40 миллиардов, что свидетельствует о стремительном росте этой тенденции [1]. Объединение устройств Интернета вещей и решений для «умного дома» в единую сеть создает условия для значительного повышения комфорта и рационального использования ресурсов. По мере увеличения количества подключенных устройств растет и количество киберугроз, направленных на нарушение целостности сетевой инфраструктуры и кражу конфиденциальной информации [2].

Одной из главных проблем систем Интернета вещей является слабая встроенная защита большинства массовых устройств, таких как камеры видеонаблюдения, умные замки и датчики освещения. Такое положение дел обусловлено стремлением производителей снизить затраты и быстрее вывести устройства на рынок [3]. В результате возникают типичные уязвимости компонентов Интернета вещей.:

1. Использование ненадежных паролей и незащищенных каналов связи (например, HTTP без SSL/TLS).

2. Слабая защита беспроводных технологий, таких как Wi-Fi, Bluetooth, ZigBee, Z-Wave и подобных, является существенной уязвимостью.

3. Отсутствие своевременного обновления встроенного ПО для устройств.

4. Со стороны пользователей отсутствует достаточное понимание важности мер, направленных на повышение информационной безопасности.

Ярким примером угрозы, исходящей от кибератак, является использование ботнетов (например, Mirai), когда незащищенные устройства Интернета вещей массово заражаются вредоносным кодом и затем осуществляют скоординированную атаку на инфраструктуру компаний или частные сети [4].

Для решения этих задач предлагается ряд подходов, которые можно систематизировать в несколько групп.

Обеспечение безопасности каналов речевого обмена с помощью криптографии – ключевой элемент в повышении безопасности устройств Интернета вещей. Для защиты передаваемой информации используются симметричные и асимметричные алгоритмы шифрования (AES, RSA и ECC). Производители внедряют протоколы TLS и DTLS для шифрования взаимодействия между Интернета вещей и сервером.

Постоянный мониторинг активности IoT-устройств – важное условие в обеспечении кибербезопасности. Системы мониторинга выявляют аномалии в поведении устройств, использование странных сетевых портов и записывают альтернативные протоколы [6]. Среди них IDS (Intrusion Detection System) и IPS (Intrusion Prevention System), к которым относятся Snort и Suricata, блокируют попытки несанкционированного доступа и вредоносных посетителей.

Многофакторная аутентификация - один из способов повышения безопасности «Умного дома». Использование различных факторов для идентификации личности (пароль, биометрические данные, одноразовый код и многие другие) заметно снижает вероятность успешного проникновение в систему злоумышленниками. Биометрические технологии (сканирование отпечатков пальцев, голоса или лица) и аппаратные криптографические ключи, в том числе YubiKey, все чаще внедряются в системы IoT, что повышает их безопасность.

Регулярное обновление ПО закрывают уязвимости в гаджетах от кибератак, вирусов, шпионского ПО и других угроз. Наиболее ответственные разработчики – Samsung SmartThings и Xiaomi Smart Home, они часто выпускают обновления прошивки и сообщают пользователям об обнаруженных уязвимостях [8]. Существуют также специализированные платформы, предназначенные для централизованного отслеживания и управления IoT-уязвимостями, - Forescout IoT Security Platform и Cisco IoT Threat Defense [6].

Развитие Интернета вещей и концепции «Умного дома» сталкивается с проблемами в области информационной безопасности. Но, несмотря на существующие угрозы, использование передовых технологий защиты (криптографию, многофакторную аутентификацию и структуры обнаружения вторжений) эффективно повышает безопасность систем IoT, что помогает повысить доверие клиентов.

Обеспечение безопасности систем IoT требует комплексного подхода на всех этапах их жизненного цикла, от проектирования и усовершенствования до постоянного обновления. Важным направлением является исследование и улучшение алгоритмов защиты в сфере Интернета вещей, чтобы обеспечить безопасное и конфиденциальное использование IoT-технологий.

С развитием технологий IoT можно ожидать уникальные новшества, такие как интеграция с искусственным интеллектом и повышение безопасности данных. В ближайшие годы «умный дом» станет не роскошью, а стандартом.

**Список литературы:**

1. Worldwide Internet of Things Forecast Update, 2025–2030 // IDC, 2024. – URL: https://www.demandsage.com/number-of-iot-devices/

2. Интернет вещей (IoT): угрозы безопасности и конфиденциальности / А. М. Гельфанд, А. А. Казанцев, А. В. Красов, В. Р. Уляшева // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей: в 4х томах, Санкт-Петербург, 24–25 февраля 2021 года / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Том 1 Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 215-220. EDN TFJJHA.

3. Вьющенко О. О., Маслова М. А. Об обеспечении безопасности в сфере интернета вещей // Научный результат. Информационные технологии. 2021. №3.

4. Antonakakis M. et al. Understanding the mirai botnet //26th USENIX security symposium (USENIX Security 17). 2017. С. 1093-1110.

5. Османов А. А. Поддержка безопасности для IoT // Новые информационные технологии как основа эффективного. 2020. С. 102.

6. Bakhshi Z., Balador A., Mustafa J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models //2018 IEEE wireless communications and networking conference workshops (WCNCW). IEEE. 2018. С. 173-178.

7. Ali B., Awad A. I. Cyber and physical security vulnerability assessment for IoT-based smart homes // sensors. 2018. Т. 18. №. 3. С. 817.

8. Feng X. et al. A survey on internet of things security based on smart home //2018 5th Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE). IEEE. 2018. С. 84-91.

**UDC 004.056.53**

## SECURITY TECHNOLOGIES FOR IoT SYSTEMS AND SMART HOMES

**Danila P. Kozlov**
student
thepolarospl@yandex.ru
**Natalia V. Pchelintseva**
senior lecturer
natas79@mail.ru
Michurinsk State Agrarian University
Michurinsk, Russia

**Annotation**. This article is devoted to current security issues in the Internet of Things (IoT) and the concept of the "smart home". It analyzes in detail the main

threats and vulnerabilities inherent in iOS devices, as well as highlights modern approaches to information security, such as cryptographic algorithms, multifactor authentication, intrusion detection systems, and monitoring tools. The main focus is on implementing effective information security measures in smart home systems and exploring ways to develop data protection technologies within the Internet of Things.

**Keywords**: internet of things, IoT, information security, smart home, cryptography, authentication, data protection, cyber attacks.

Статья поступила в редакцию 10.05.2025; одобрена после рецензирования 20.06.2025; принята к публикации 30.06.2025.

The article was submitted 10.05.2025; approved after reviewing 20.06.2025; accepted for publication 30.06.2025.