SECURITY ISSUES IN THE INTERNET OF THINGS (IoT)

Olkhovskaya I.V. (Republic of Uzbekistan)

Olkhovskaya Irina Valeryevna – Senior Lecturer,
DEPARTMENT OF INFORMATION SYSTEMS AND TECHNOLOGIES,
TASHKENT STATE AGRARIAN UNIVERSITY,
REPUBLIC OF UZBEKISTAN, TASHKENT

Abstract: *The article examines current security challenges in the field of the Internet of Things (IoT), including the insufficient level of device protection, limited computational resources, and the lack of unified security standards. It emphasizes the need for a comprehensive approach to ensuring IoT security.*
Keywords: *smart devices, authentication, cyber confrontation, Big Data, biometric data.*

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ИНТЕРНЕТ ВЕЩЕЙ (IOT)

Ольховская И.В. (Республика Узбекистан)

Ольховская Ирина Валерьевна - старший преподаватель,
кафедра « Информационные системы и технологии»
Ташкентский государственный аграрный университет
Республика Узбекистан, г. Ташкент

Аннотация: *в статье рассматриваются актуальные проблемы обеспечения безопасности в сфере Интернета вещей (IoT), недостаточный уровень защиты устройств, ограниченные вычислительные ресурсы, отсутствие единых стандартов безопасности, подчеркивается необходимость комплексного подхода к обеспечению безопасности IoT.*
Ключевые слова: *«Умные» устройства, аутентификация, киберконфронтация, Big Data, биометрические данные.*

Интернет вещей изменяет принципы ведения бизнеса, общественных связей и отношений, сам уклад нашей жизни. «Умные» устройства собирают огромные массивы данных о своих владельцах: аудио- и видеопотоки, геолокацию, параметры окружающей среды, сценарии поведения, расписание присутствия дома и т.д. Контролировать, что именно отправляется производителю, какие аналитические сервисы задействованы и как долго хранятся данные, в большинстве случаев пользователю практически невозможно. Ситуацию усугубляет то, что многие устройства изначально доступны в интернет напрямую. Поисковые системы по устройствам, до сих пор находят десятки тысяч открытых веб-камер, baby-мониторов и систем видеонаблюдения с дефолтными паролями или вовсе без аутентификации.

В 2025 году «интернет вещей» перестал быть теоретической угрозой: от уязвимых камер и роутеров до автомобилей и медицинских имплантов — IoT-экосистема стала одним из ключевых полей киберконфронтации. Массовый характер устройств, слабая безопасность по умолчанию и долгий срок службы создают значимый системный риск. Полностью отказаться от подключенных устройств уже невозможно, но их использование требует осознанного подхода: выбора решений с понятной политикой безопасности, настройки по принципу «минимально необходимого доступа», регулярных обновлений и мониторинга.

К числу наиболее распространённых угроз безопасности IoT относятся несанкционированный доступ к устройствам и данным, перехват информации в беспроводных сетях, подмена управляющих команд, атаки типа «отказ в обслуживании» (DoS), внедрение вредоносного программного обеспечения. Причинами возникновения угроз являются слабые механизмы аутентификации, использование стандартных паролей, отсутствие обновлений ПО и недостаточная защита каналов связи. Реализация политики безопасности IoT представляет собой комплекс мер, направленных на защиту устройств, передаваемых данных и серверной инфраструктуры от внешних и внутренних угроз, она формируется на этапе проектирования системы и определяет правила аутентификации устройств. Важной особенностью IoT является использования энергоэффективных криптографических алгоритмов и оптимизированных механизмов защиты. Одной из проблем, является ограничение скоростей связи устройств между собой, слабая защищённость и отсутствие стандартов безопасности. По мере увеличения числа подключённых к сети устройств, разрастания облачных сервисов и внедрения технологий Big Data кибератаки становятся всё более масштабными и многочисленными, в результате, **наблюдается** ослабление защиты. Современные устройства оснащены множеством сенсоров и микрофонов, могут собирать различную информацию. *Например*:

1) Личные данные: имя, возраст, местоположение, пол, адрес проживания, например, фитнес-трекеры.

2) Биометрические данные: голос, частота сердечных сокращений, температура тела, такие данные могут собирать устройства умных браслетов или колонок.

3) Данные о поведении: предпочтения пользователя, время активности, любимые приложения или маршруты.

4) Технические данные: IP-адрес, MAC-адрес устройства, данные о сети и подключении, например, умные камеры фиксируют изменения в сети и могут автоматически передавать информацию на удаленные серверы.

Зачем устройства собирают эти данные? Производителям нужны данные, чтобы повысить эффективность, адаптировать сервисы под конкретного пользователя и, следовательно, повысить уровень лояльности. Чем больше информации собирает устройство, тем точнее оно предлагает функции, которые нужны пользователю. Существуют риски при использования умных устройств, которые могут случайно или нет записывать частные разговоры или собирать данные без нашего ведома, компании могут использовать данные для создания рекламных профилей, фитнес-трекеры привязываются к приложениям и дают им доступ к информации о вашем здоровье, злоумышленники могут получить доступ к управлению. Усилить безопасность smart - приборов поможет установка дополнительной защитной электроники — миниатюрных компонентов, которые соединяют периферийные устройства с принимающими микроконтроллерами или микропроцессорами, отвечающие за персонализированные сертификаты, безопасное размещение закрытых ключей и управление криптографическими элементами.

Итак, проблемы безопасности в Интернете вещей (IoT) представляют собой одну из наиболее значимых и актуальных задач современной цифровой среды. Массовое внедрение «умных» устройств в различные сферы деятельности сопровождается ростом числа уязвимостей, связанных с ограниченными ресурсами устройств, недостаточным уровнем их защиты, отсутствием единых стандартов и сложностью управления распределённой инфраструктурой. Только при условии обеспечения высокого уровня безопасности возможно устойчивое и безопасное функционирование IoT-инфраструктуры в условиях цифровой трансформации общества.

Список литературы / References

1. *Алюнов А.Н., Ахмад А.* Основы интернета вещей : Учебное пособие. Издательство: КноРус. Москва. 2025 . ISBN: 978-5-406-14467-1.
2. *Ольховская И.В.* Современные тенденции развития интернет вещей //Вестник науки и образования. – 2026. – № 4 (171) -2. – С. 6-8.