УДК 004.89

Т.Е. Мирамов, Н.А. Горбунова
Карагандинский государственный университет им. Е.А. Букетова
Караганда, Казахстан

КИБЕРБЕЗОПАСНОСТЬ В СФЕРЕ ИНТЕРНЕТА ВЕЩЕЙ (IOT): УГРОЗЫ И ЗАЩИТНЫЕ МЕРЫ

Аннотация. *В статье рассматривается анализ текущего состояния кибербезопасности в сфере интернета вещей (IoT), выявлены основные угрозы и риски. Перечисляются возможные защитные меры противодействия угрозам, утечкам информации, предложены стратегии и методы защиты, направленные на предотвращение возможных атак и обеспечение надежной работы систем IoT в современном цифровом мире.*

T.E. Miramov, N.A. Gorbunova
Buketov Karaganda State University
Karaganda, Kazakhstan

CYBERSECURITY IN THE INTERNET OF THINGS (IOT) SPHERE: THREATS AND PROTECTIVE MEASURES

Abstract*. The article examines the analysis of the current state of cybersecurity in the field of the Internet of Things (IoT), identifying the main threats and risks. Possible protective measures to counter threats and information leaks are listed, strategies and methods of protection are proposed aimed at preventing possible attacks and ensuring reliable operation of IoT systems in the modern digital world.*

С развитием современных технологий Интернет вещей (IoT) стал ключевым фактором в повседневной жизни, проникая в различные сферы, от здравоохранения и производства до домашних устройств и транспортных систем. Однако, вместе с широким распространением и использованием IoT, возникают значительные вызовы в области кибербезопасности. Этот аспект становится все более важным, поскольку устройства IoT сопряжены с угрозами безопасности, способными привести к серьезным последствиям, включая утечку данных, нарушение личной жизни, а также угрозы для физической безопасности человека.

Устройства Интернета вещей (IoT) сталкиваются с различными угрозами безопасности, которые могут оказать серьезное воздействие на их функционирование, приватность данных и даже безопасность пользователей. Некоторые из основных угроз включают в себя:

- DDoS-атаки (атаки отказа в обслуживании): Кибератаки, направленные на перегрузку сети устройств IoT трафиком, часто с целью временного отключения сервисов или систем [1].

- Взлом устройств: Недостаточная защита устройств IoT может привести к их физическому или удаленному взлому, что позволяет злоумышленникам получить доступ к данным пользователя, перехватывать управление или даже использовать устройства в качестве точки входа для атак на другие системы.

- Утечка данных и нарушение приватности: Недостатки в защите данных и приватности могут привести к утечкам конфиденциальной информации, такой как личные данные, местоположение или медицинская информация.

- Манипуляция данными: Злоумышленники могут изменять данные, передаваемые устройствами IoT, что может привести к неправильным решениям или даже опасным ситуациям в сфере здравоохранения, автомобильной промышленности и других областях[1].

Устройства Интернета вещей (IoT) сталкиваются с несколькими факторами уязвимости, которые делают их более подверженными угрозам безопасности:

- Недостатки в защите данных: Многие устройства IoT имеют недостаточные меры безопасности, такие как слабые пароли, отсутствие шифрования данных или открытые порты, что делает их уязвимыми для взлома или перехвата данных.

- Недостаток обновлений и поддержки: Многие производители устройств IoT не предоставляют регулярные обновления для исправления уязвимостей, что оставляет устройства подверженными известным угрозам безопасности.

- Отсутствие стандартов безопасности: На сегодняшний день отсутствует общепринятый стандарт безопасности для устройств IoT. Различные производители применяют разные подходы к безопасности, что может привести к разнообразию уязвимостей и сложностей в обеспечении защиты.

- Физические ограничения: Некоторые устройства IoT имеют ограниченные ресурсы (вычислительная мощность, память, энергия), что делает сложным или даже невозможным применение сложных методов защиты, таких как сильное шифрование или сложные алгоритмы аутентификации [2].

Проблема недостатка стандартов безопасности в производстве устройств IoT также является значительной. Отсутствие единого набора стандартов безопасности создает неоднородность в уровне

защиты устройств. Многие производители, стремясь быстро вывести продукт на рынок, уделяют меньше внимания аспектам безопасности, фокусируясь в первую очередь на функциональности и стоимости устройств.

Стандартизация в области кибербезопасности для IoT устройств станет важным шагом к созданию более надежных и безопасных систем. Она поможет унифицировать процессы разработки и производства, а также установить общие требования к защите данных и мерам предотвращения атак.

Для обеспечения безопасности в Интернете вещей (IoT) можно применять ряд технических и организационных мер безопасности:

Шифрование данных: Использование сильного шифрования для защиты передаваемых данных между устройствами IoT и серверами. Это включает применение протоколов шифрования, таких как SSL/TLS, для защиты коммуникаций [3].

Аутентификация и управление доступом: Реализация механизмов аутентификации для подтверждения подлинности устройств и пользователей перед доступом к системе IoT. Использование двухфакторной аутентификации, управление правами доступа и использование сильных паролей.

Мониторинг и обнаружение инцидентов: Установка систем мониторинга, которые позволяют отслеживать активность устройств IoT и обнаруживать потенциальные аномалии или атаки. Это включает в себя системы обнаружения вторжений (IDS) и системы управления событиями безопасности (SIEM).

Обновление программного обеспечения и патчи безопасности: Регулярное обновление программного обеспечения на устройствах IoT для устранения уязвимостей и применения последних исправлений безопасности (патчей).

Физическая безопасность: Защита физического доступа к устройствам IoT, например, через использование физических замков, контроля доступа к серверным помещениям и т.д.

Обучение пользователей: Обучение конечных пользователей основам кибербезопасности, таким как правила сложных паролей, осведомленность об угрозах фишинга и другие методы социальной инженерии.

Стандартизация безопасности: Стимулирование разработки общепринятых стандартов безопасности для устройств IoT, что способствует повышению уровня безопасности за счет обязательных требований к защите данных и средствам обеспечения безопасности [4].

Эти меры могут быть эффективными при правильной реализации и интеграции в экосистему Интернета вещей, обеспечивая более надежную защиту устройств и данных. Тем не менее, важно осознавать, что безопасность IoT является постоянно развивающейся областью, требующей постоянного обновления и улучшения мер безопасности для борьбы с новыми угрозами и рисками.

Обсуждение проблем кибербезопасности в сфере Интернета вещей (IoT) подчеркивает важность борьбы с угрозами, которые могут привести к серьезным последствиям для безопасности, приватности и функционирования устройств и систем IoT.

Как отмечалось, устройства IoT сталкиваются с разнообразными уязвимостями, такими как недостатки в защите данных, недостаток стандартов безопасности, возможности взлома и многие другие факторы. Эти уязвимости оставляют системы IoT открытыми для различных киберугроз, что требует систематического подхода к обеспечению безопасности.

Необходимость дальнейших исследований и развития средств защиты IoT становится критически важной. Необходимо продолжать работу над разработкой более эффективных методов аутентификации, шифрования и обнаружения угроз для усиления защиты устройств IoT. Кроме того, разработка общепринятых стандартов безопасности, а также регулярное обновление и поддержка устройств, играют важную роль в предотвращении атак и обеспечении безопасности IoT.

Для дальнейшего улучшения кибербезопасности в сфере IoT, необходимо:

Продолжать активно исследовать новые угрозы и уязвимости, а также адаптироваться к изменяющимся методам атак.

Развивать и стандартизировать методы защиты и шифрования, обеспечивая более эффективную защиту устройств и данных.

Способствовать образованию и повышению осведомленности об угрозах кибербезопасности IoT у разработчиков, пользователей и производителей.

Формировать стратегии управления рисками и регулярно обновлять практики безопасности в соответствии с изменяющимися угрозами.

Только совместными усилиями индустрии, ученых и правительств можно обеспечить более безопасное и надежное функционирование экосистемы Интернета вещей (IoT) в будущем.

Список использованных источников

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer networks, 54(15), 2787-2805.

2. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer networks, 57(10), 2266-2279.

3. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

4. Römer, K., & Römer, C. (2010). The design space of wireless sensor networks. IEEE Wireless Communications, 11(6), 54-61.

УДК 004

К.В. Муравейко, Н.И. Белодед
Академия управления при Президенте Республики Беларусь
Минск, Беларусь

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В БИЗНЕСЕ

Аннотация. *В современном мире технологии искусственного интеллекта и машинного обучения играют ключевую роль в развитии бизнеса. Эти технологии предоставляют компаниям новые возможности для автоматизации процессов, принятия обоснованных решений и улучшения клиентского опыта.*

K.V. Muraveiko, N.I. Beloded
Academy of Public Administration under the Aegis of the President of the Republic of Belarus
Minsk, Belarus

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN BUSINESS

Abstract. *In the modern world, artificial intelligence and machine learning technologies play a key role in business development. These technologies provide companies with new opportunities to automate processes, make informed decisions and improve the customer experience.*