Удальцов К.Р. Влияние интернета вещей на кибербезопасность: уязвимости подключенных устройств// Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 5(43) с. 46–49

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ВЛИЯНИЕ ИНТЕРНЕТА ВЕЩЕЙ НА КИБЕРБЕЗОПАСНОСТЬ: УЯЗВИМОСТИ ПОДКЛЮЧЕННЫХ УСТРОЙСТВ

Удальцов К.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: 2003.06.10kr@gmail.com

Данная статья исследует влияние Интернета вещей (IoT) на кибербезопасность и предлагает ряд стратегий для улучшения безопасности IoT. Рассматриваются ключевые аспекты, такие как образование пользователей и производителей, развитие технологий киберзащиты, международное сотрудничество и стандартизация. Настоятельная необходимость совместных усилий пользователей, производителей, правительств и международного сообщества для обеспечения безопасного развития Интернета вещей подчеркивается как ключевой момент в минимизации уязвимостей IoT к киберугрозам.

Ключевые слова: Интернет вещей, кибербезопасность, IoT устройства, обучение пользователей, производители IoT, технологии киберзащиты, международное сотрудничество, стандартизация, киберугрозы, уязвимости IoT.

THE IMPACT OF THE INTERNET OF THINGS ON CYBERSECURITY: VULNERABILITIES OF CONNECTED DEVICES

Udaltsov K.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

This article explores the impact of the Internet of Things (IoT) on cybersecurity and suggests a number of strategies to improve IoT security. Key aspects such as the education of users and manufacturers, the development of cyber defense technologies, international cooperation and standardization are considered. The urgent need for joint efforts by users, manufacturers, governments and the international community to ensure the safe development of the Internet of Things is highlighted as a key point in minimizing IoT vulnerabilities to cyber threats.

Keywords: Internet of Things, cybersecurity, iOS devices, user training, It manufacturers, cyber defense technologies, international cooperation, standardization, cyber threats, IoT vulnerabilities.

Интернет вещей (IoT) - это концепция, которая описывает сеть подключенных устройств, способных обмениваться данными между собой без прямого участия человека. Эти устройства могут включать все, начиная от умных домашних приборов и кончая медицинскими устройствами и промышленным оборудованием. Однако с развитием IoT возникают новые вызовы в области кибербезопасности.[1]

1. Увеличение атак на подключенные устройства

В силу того, что большое количество устройств в IoT работает на основе встраиваемых систем и операционных систем, они могут быть более уязвимы к кибератакам. Атаки могут включать в себя взлом устройств, перехват данных или даже использование устройства для организации DDoS-атак на другие системы.

2. Недостатки в конструкции и защите

Многие устройства IoT разрабатываются с упором на функциональность и экономию ресурсов, что может привести к недостаточной защите от киберугроз. [2] Некоторые устройства могут иметь стандартные пароли, слабую или отсутствующую защиту данных, что делает их легкими целями для злоумышленников.

3. Оценка рисков и совершенствование мер безопасности

Для смягчения рисков, связанных с IoT, необходимо провести оценку уязвимостей и реализовать более строгие стандарты безопасности. [3] Меры также могут включать в себя широкое использование шифрования данных, улучшение аутентификации устройств и обновление программного обеспечения для устранения обнаруженных уязвимостей.

4. Обзор законодательства и регулирования

Большинство стран начали разрабатывать законодательство, которое регулирует безопасность устройств IoT. [4] Это включает требования к обязательному внедрению стандартов безопасности, отчетности о нарушениях безопасности и наложении штрафов за недостатки в защите.

Интернет вещей, несомненно, привносит огромные выгоды в современную жизнь, однако необходимо активно бороться с уязвимостями безопасности, чтобы предотвратить серьезные угрозы для частных лиц, организаций и общественной инфраструктуры. [5],Путем улучшения стандартов защиты и юридического регулирования мы можем снизить риски и продолжить развитие IoT в безопасном и устойчивом направлении. Обучение пользователей и производителей [6]

Одним из ключевых аспектов улучшения кибербезопасности IoT является образование и обучение пользователям и производителям. Пользователям необходимо осознавать основы безопасного использования устройств IoT, такие как регулярное обновление программного обеспечения, использование надежных паролей и защита своих домашних сетей. Производители же должны уделять большее внимание интеграции безопасности на ранних этапах разработки устройств.[7]

5. Развитие технологий киберзащиты

С постоянным развитием угроз кибербезопасности IoT необходимо активное совершенствование технологий защиты. [8] Это включает в себя использование искусственного интеллекта и машинного обучения для обнаружения и предотвращения атак, разработку средств мониторинга и обнаружения угроз, а также усовершенствование методов шифрования и аутентификации.

6. Международное сотрудничество и стандартизация

Киберугрозы не ограничиваются границами стран, поэтому международное сотрудничество играет ключевую роль в обеспечении безопасности IoT. Важно развивать международные стандарты безопасности, обмениваться информацией о киберугрозах и совместно реагировать на кибератаки.

Заключение

Все большее количество устройств IoT поглощает нашу повседневную жизнь, делая ее более удобной и эффективной. Однако без должной защиты эти устройства могут стать мишенями для киберпреступников, угрожая нашей конфиденциальности, безопасности и даже физическому благополучию. Совместные усилия пользователей, производителей, правительств и международного сообщества необходимы для обеспечения безопасного развития Интернета вещей и минимизации его уязвимостей к киберугрозам.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
4. Красов А. В. и др. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
6. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
7. Волкогонов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
8. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics"RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.

3. Kazantsev A. A. et al. Creating and managing a Security Operations Center for effective use in real-world environments//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". - 2020. – No. 2. – pp. 86-94.
6. Gelfand A.M. Methods of choosing stegocontainers for data transmission//Regional informatics and information security. – 2020. – pp. 260-262.
7. Volkogonov V. N. et al. Wi-fi network Security Analysis//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 270-275.
8. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.