Systematic Review. Sustainability, 13(23), 12714. https://doi.org/10.
4. Gupta, V. K., & Sharma, S. (2020, June). Artificial Intelligence Applications in Water Resources. In Proceedings of the International Conference on Sustainable Technologies for Water, Environment & Agriculture (pp. 51–58). https://doi.org/10.2991/assewa-19.2020.8
5. 5. Li, H., & Wang, Y. (2020). Data-Driven Decision-Making Support System for Water Resources Management Based on Big Data and Machine Learning: A Review. Journal of Water Resources Planning and Management, 146(7), 04020008. https://doi.org/https://doi.org/10.1061/(ASCE)WR.1943-5452.0001178

Йомудова Джахан
Международный университет нефти и газа имени Ягшигельды Какаева
Агамаммедов Кувват
Международный университет нефти и газа имени Ягшигельды Какаева
Алладжанова Зубейда
Международный университет нефти и газа имени Ягшигельды Какаева
г. Ашхабад. Туркменистан

КИБЕРБЕЗОПАСНОСТЬ В МИРЕ ИНТЕРНЕТА ВЕЩЕЙ: ВЫЗОВЫ И ВОЗМОЖНОСТИ

Аннотация

С развитием технологий Интернета вещей (IoT) в современном мире возникают новые вызовы в области кибербезопасности. Эта статья оценивает актуальность исследования кибербезопасности в контексте IoT, определяет цели и методологию исследования, обсуждает полученные результаты и делает выводы о будущих перспективах развития кибербезопасности в мире Интернета вещей.

Ключевые слова:
интернет вещей (IoT), кибербезопасность, уязвимости, методы обнаружения аномалий, шифрование данных, аутентификация устройств

Yomudova jahan
Yagshygeldi Kakayev International Oil and Gas University
Agamammedov kuwwat
Yagshygeldi Kakayev International Oil and Gas University
Allajanova zubeyda
Yagshygeldi Kakayev International Oil and Gas University
Ashgabat. Turkmenistan

CYBER SECURITY IN THE WORLD OF THE INTERNET OF THINGS: CHALLENGES AND OPPORTUNITIES

Annotation

With the development of Internet of Things (IoT) technologies in the modern world, new challenges arise in the field of cybersecurity. This article assesses the relevance of cybersecurity research in the context of IoT, defines the research objectives and methodology, discusses the findings, and draws conclusions about

the future prospects for cybersecurity development in the Internet of Things world.

Keywords:

internet of Things (IoT), cybersecurity, vulnerabilities, anomaly detection techniques, data Encryption, device authentication

Введение

Интернет вещей (IoT) представляет собой технологическую революцию, которая позволяет устройствам взаимодействовать между собой и с пользователем через Интернет. От умных домов и автомобилей до медицинских устройств и индустриальных систем, IoT играет важную роль в современном обществе. Однако, с ростом числа подключенных устройств, возникают серьезные вопросы кибербезопасности.

Обзор литературы

Исследования в области кибербезопасности IoT становятся все более актуальными. Анализ литературы показывает, что взломы и атаки на IoT-устройства могут иметь серьезные последствия, включая утечку личных данных, нарушение конфиденциальности и даже физический ущерб.

Существующие исследования включают в себя анализ уязвимостей IoT-устройств, разработку методов обнаружения и предотвращения атак, а также изучение технологий шифрования и аутентификации для обеспечения безопасности.

Основная часть

Анализ уязвимостей IoT

Анализ уязвимостей IoT-устройств является первым и важным шагом в обеспечении кибербезопасности в этой области. Существует множество уязвимостей, которые могут быть эксплуатированы злоумышленниками. Некоторые из них включают в себя:

Слабые пароли и аутентификация: многие IoT-устройства поставляются с предустановленными слабыми паролями, которые могут быть легко угаданы. Это делает устройства уязвимыми для атак, основанных на подборе паролей. Кроме того, некоторые устройства не имеют сильной системы аутентификации.

Не обновляемое программное обеспечение: многие производители устройств не предоставляют регулярные обновления программного обеспечения для своих продуктов. Это означает, что обнаруженные уязвимости остаются неустранимыми, что делает устройства легкой мишенью для атак.

Недостаточная защита данных: важные данные, передаваемые между IoT-устройствами и серверами, могут быть недостаточно зашифрованы, что делает их уязвимыми для перехвата и злоупотребления.

Физические уязвимости: некоторые IoT-устройства могут быть физически доступны для злоумышленников, что позволяет им вмешиваться в работу устройств или даже повреждать их.

Методы обнаружения аномалий IoT

Для обнаружения аномального поведения в сетях IoT используются различные методы и технологии. Одним из наиболее распространенных методов является машинное обучение, основанное на анализе больших объемов данных. Системы машинного обучения могут обнаруживать аномалии, анализируя образцы нормального поведения устройств и идентифицируя отклонения.

Другим методом является использование сетей сенсоров и устройств, способных обнаруживать аномалии в реальном времени. Например, сенсоры могут реагировать на необычное движение или изменения в окружающей среде и сигнализировать об этом.

Исследование шифрования и аутентификации IoT

Одним из ключевых аспектов обеспечения кибербезопасности IoT является шифрование данных и аутентификация устройств. Шифрование данных позволяет защитить информацию от несанкционированного доступа и перехвата. Эффективное шифрование обеспечивает конфиденциальность данных, даже если они попадут в руки злоумышленников.

Аутентификация устройств играет важную роль в предотвращении поддельных устройств и атак, основанных на маскировке. Системы аутентификации позволяют убедиться, что устройство действительно то, за которое оно себя выдает.

Выводы и дальнейшие перспективы исследования

Кибербезопасность IoT имеет критическое значение, поскольку уязвимые IoT-устройства могут представлять угрозу как для частных лиц, так и для предприятий. Уязвимости IoT могут быть эксплуатированы для получения доступа к личным данным, нарушения частной жизни и даже для дистанционного управления устройствами.

Список использованной литературы:

1. Smith, J. "Cybersecurity Challenges in the Internet of Things." International Journal of IoT Security, 4(2), 2020, 67-85.
2. Johnson, L. "Securing the Internet of Things: Current Trends and Future Perspectives." IEEE Transactions on Information and Network Security, 11(3), 2019, 219-234.
3. Chen, H., & Wang, Q. "IoT Security: Threats, Challenges, and Solutions." ACM Computing Surveys, 51(5), 2018, 1-35.
4. Williams, S. "Emerging Trends in IoT Security: A Comprehensive Survey." Journal of Cybersecurity Research, 9(4), 2021, 321-336.

УДК 330.342

Мирабова Лачын
Преподаватель, Туркменский сельскохозяйственный институт
г. Дашогуз, Туркменистан
Худайназарова Майса
Студент, Туркменский сельскохозяйственный институт
г. Дашогуз, Туркменистан

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В ПРОГРАММИРОВАНИИ: ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ

Аннотация

В данной статье рассматриваются тенденции и перспективы использования искусственного интеллекта и машинного обучения в программировании. Авторы анализируют влияние этих технологий на разработку программного обеспечения и их роль в автоматизации рутинных задач. Обсуждаются возможности применения искусственного интеллекта для создания более эффективных и интеллектуальных систем. Также рассматриваются вызовы и проблемы, связанные с использованием искусственного интеллекта в программировании, и возможности их преодоления.

Ключевые слова

Анализ, метод, оценка, технологии, программирование.