Impact Factor: 9.2 ISSN-L: 2544-980X

Кибербезопасность в области IoT технологии

Рахматов Расулжон

Ассистент кафедры "Информационная безопасность" Ферганского филиала Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми.

Мирзаев Жамшид Боймуродович

Ассистент кафедры "Информационная безопасность" Ферганского филиала Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми.

Abstract: *Анализируется влияние роста интернета вещей (IoT) на кибербезопасность, идентифицируются угрозы и вызовы, возникающие в связи с этим, и предлагаются стратегии для обеспечения безопасности в экосистеме IoT. Анализируются технические и организационные меры по обеспечению кибербезопасности, включая шифрование данных, авторизацию и аутентификацию, защиту от несанкционированного доступа и мониторинг устройств. Также рассматриваются аспекты сотрудничества между производителями, операторами и пользователями устройств IoT для обеспечения кибербезопасности.*

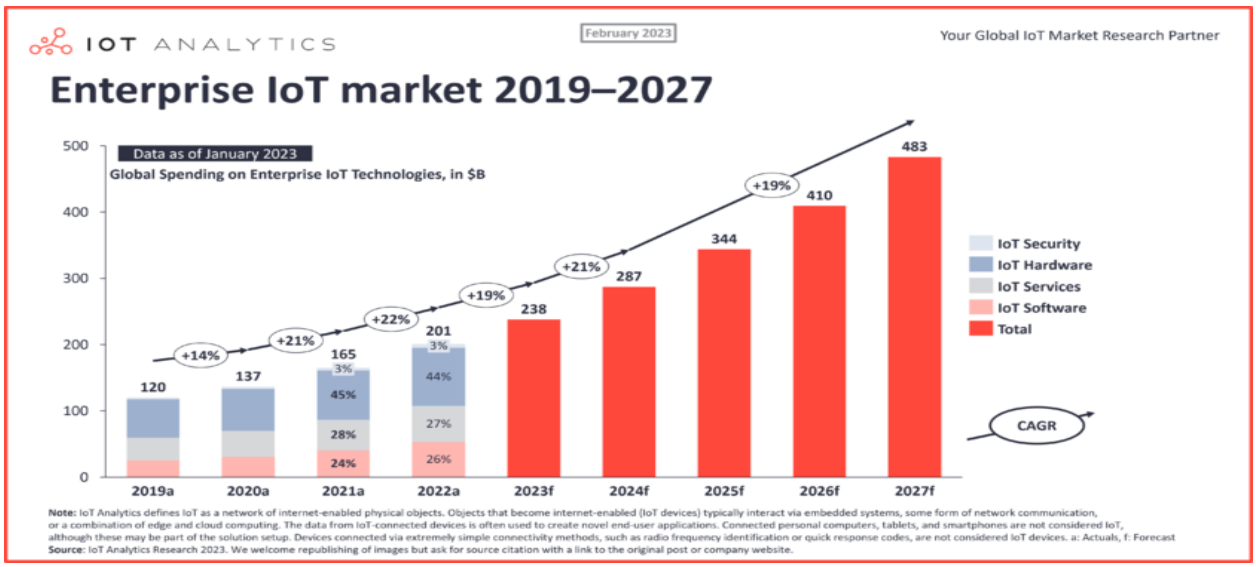
Keywords: *IoT, SQL, кибербезопасность, WPA2 и SSL.*

INTRODUCTION:

Кибербезопасность в области интернета вещей (IoT) становится все более важной с увеличением числа подключенных устройств. IoT технология предоставляет огромные преимущества в различных отраслях, но она также представляет серьезные угрозы для безопасности, так как увеличивает поверхность атаки для злоумышленников.

Рост интернета вещей (IoT) имеет значительное влияние на современное общество и экономику. Одним из главных аспектов влияния IoT является увеличение уровня автоматизации и улучшение оперативной эффективности в различных отраслях, начиная от промышленного производства и здравоохранения, заканчивая сельским хозяйством и умными городами. IoT также способствует повышению уровня комфорта и удобства для конечных пользователей благодаря развитию умных домов, носимых устройств и автомобильной техники. Однако рост IoT также вносит серьезные вызовы в области кибербезопасности. Увеличение количества подключенных устройств увеличивает поверхность атак, предоставляя злоумышленникам больше возможностей для кибератак. Безадежно безопасность устройств IoT также создает угрозу для конфиденциальности и безопасности данных, что является важным аспектом влияния роста IoT. Таким образом, влияние роста интернета вещей (IoT) охватывает

как позитивные, так и негативные аспекты, и требует комплексного подхода для обеспечения безопасности и защиты важных данных.



Анализ

Одной из основных проблем в области кибербезопасности IoT является отсутствие стандартов безопасности. Многие устройства разрабатываются с недостаточным вниманием к безопасности, что делает их уязвимыми для кибератак. Недостаточная защита конфиденциальных данных также представляет серьезную угрозу для пользователей устройств IoT.

Технические и организационные меры по обеспечению кибербезопасности включают в себя различные аспекты, такие как:

Шифрование данных: Защита конфиденциальной информации путем преобразования ее в нечитаемый формат с использованием криптографических алгоритмов.

Авторизация и аутентификация: Установление и проверка идентичности пользователей и устройств, чтобы предотвратить несанкционированный доступ к системам и данным.

Защита от несанкционированного доступа: Реализация механизмов контроля доступа и ограничения привилегий для предотвращения несанкционированного доступа к системам и данным.

Мониторинг устройств: Непрерывный мониторинг активности устройств и сетей для обнаружения подозрительной или аномальной активности, свидетельствующей о возможных киберугрозах.

Организационные меры включают организационную политику безопасности, обучение сотрудников, разработку стандартов безопасности и управление рисками.

Технические и организационные меры по обеспечению кибербезопасности играют критическую роль в предотвращении и обнаружении киберугроз, а также в защите конфиденциальных данных и обеспечении безопасности информационных систем и устройств.

Для обеспечения кибербезопасности в области IoT необходимо применять комплексный подход, включающий в себя шифрование данных, авторизацию и аутентификацию устройств, защиту от несанкционированного доступа, мониторинг и анализ событий, а также обновление программного обеспечения и прошивок.

Безопасность в области IoT также требует сотрудничества между производителями, операторами и пользователями устройств. Производители должны уделить большее внимание вопросам безопасности при разработке устройств, а операторы и пользователи должны быть

осведомлены о методах защиты и следовать bewsecurity по заверении безопасности своих устройств и данных.

В целом, обеспечение кибербезопасности в области IoT является сложной и многогранный задачей, требующей совместных усилий от производителей, операторов и пользователей. Улучшение стандартов безопасности, обмен информацией об угрозах, и непрерывное обновление технологий и практик являются критически важны для преодоления вызовов кибербезопасности в области IoT.

Решение

В последние годы Интернет Вещей стал неотъемлемой частью нашей повседневной жизни, и организации все чаще используют IoT технологии для увеличения эффективности и улучшения пользовательского опыта. Однако, с ростом количества устройств, связанных с Интернетом, возрастает и риск кибератак, которые могут привести к серьезным последствиям. В этой статье мы рассмотрим основные аспекты кибербезопасности в области IoT технологии.

Изначально, кибербезопасность в области IoT технологии должна начинаться с проектирования устройств. Разработчики должны учитывать особенности IoT и создавать устройства с безопасностью во всех аспектах: от аппаратного обеспечения до программного обеспечения. Например, разработчики должны использовать криптографию для защиты данных, управлять доступом к устройствам с помощью паролей, аутентификации и авторизации.

Ряд известных производителей уже имеют примеры устройств, которые были атакованы и использованы как "ботнеты". Устройства могут стать жертвами кибератак при использовании устройств со слабыми паролями или устройств, которые не защищены антивирусами. Кроме того, от того, как устройства будут подключаться к Интернету и взаимодействовать друг с другом, также зависит, насколько безопасными будут они в использовании. Важно, чтобы устройства были защищены от атак по типу переполнения буфера или SQL-инъекции.

Следующий важный аспект кибербезопасности в области IoT технологии - это безопасность компьютерных сетей. Как правило, устройства в сети подключаются к общей точке доступа к Интернету, а значит любой несанкционированный доступ к сети может привести к утечке данных или взлому устройств. Поэтому важно использовать защищенные соединения и протоколы безопасности, такие как WPA2 и SSL, чтобы предотвратить несанкционированный доступ к устройствам и сети.

Другим важным моментом является защита от физических кибератак. Кажется, что загруженный или отсутствующий домофон это простой недостаток, но он также может быть уязвимостью для взлома и ослабления безопасности устройства. Кроме того, запрет на физический доступ к устройству может сделать его более защищенным от взлома или установки вредоносных программ.

Взаимодействие между устройствами в сети IoT может быть сложным и требовать обработки большого количества данных. Это означает, что обработка данных должна быть обеспечена высокой степенью безопасности, включая шифрование всех передаваемых данных, а также защиту от несанкционированного доступа. Также необходимо устанавливать правила доступа для отдельных приложений и устройств.

Кроме этого, устройства должны иметь свои собственные системы мониторинга и противодействия кибератакам, которые включают в себя обнаружение необычной активности и немедленное уведомление администраторов сети. Обнаружение и регистрация всех необычных активностей является одним из основных методов обеспечения безопасности в IoT сетях.

Аспекты сотрудничества между производителями, операторами и пользователями устройств IoT для обеспечения кибербезопасности:

Роль производителей: обсудите важность внедрения безопасности на уровне разработки устройств IoT, включая использование шифрования, механизмов аутентификации и обновлений безопасности.

Роль операторов: рассмотрите меры, которые операторы могут принять для обеспечения безопасности устройств IoT на своих сетях, включая мониторинг активности, обновление программного обеспечения и предоставление обучения пользователям.

Роль пользователей: обсудите важность осведомленности и обучения пользователей об основах кибербезопасности, включая правила сильных паролей, регулярные обновления и осведомленность о потенциальных угрозах.

Наконец, важно понимать, что кибербезопасность - это не статичный процесс, поэтому необходимо регулярно тестировать безопасность устройств и наращивать меры безопасности. Это должно включать проверку уязвимостей и проблем безопасности с помощью автоматических сканеров, а также анализ систем журналирования для обнаружения необычной активности.

Заключение

В заключение, кибербезопасность в области IoT технологии является серьезной проблемой, требующей всеобъемлющих мер безопасности для устройств, сетей и данных, которые они обрабатывают. Многие компании, включая производителей устройств, должны посвятить больше ресурсов и внимания безопасности в IoT технологиях. Безопасность должна быть интегрирована в каждый шаг разработки, производства и эксплуатации устройств, чтобы обеспечить защиту от кибератак, утечек данных и других угроз в области IoT технологии.

Кибербезопасность в области IoT технологии требует совместных усилий со стороны производителей, операторов и пользователей. Эффективное сотрудничество между этими сторонами является ключевым для обеспечения безопасности устройств IoT и предотвращения киберугроз.

Для достижения этой цели, необходимо уделить большее внимание интеграции мер безопасности на уровне проектирования, развития стандартов безопасности для устройств IoT, регулярного обновления программного обеспечения, а также обучения пользователей об основах кибербезопасности.

Кроме того, необходимо активное сотрудничество между производителями, операторами и пользователями для обмена информацией об угрозах, разработки совместных стратегий защиты и реагирования на киберинциденты, а также поддержки усилий по совершенствованию стандартов кибербезопасности в области IoT.

В целом, кибербезопасность в области IoT технологии требует комплексного подхода и взаимодействия между всеми участниками экосистемы IoT для эффективной защиты от киберугроз и обеспечения безопасности устройств и данных.

Использованная литература

1. D.F. To‘xtasinov, R.R. Raxmatov - ELEKTROMOBILLAR VA BOSHQA QURILMALARDA AKKUMULYATORLARDAN SAMARALI FOYDALANISH TADQIQI - ФАРҒОНА ПОЛИТЕХНИКА ИНСТИТУТИ И Л М И Й – Т Е Х Н И К А ЖУРНАЛИ

1. Raxmatov, R. (2023). ELEKTR ENERGIYASINI SAQLASHDA MEXANIK USULLARDAN FOYDALANISH. *Engineering problems and innovations*, 113-114.

2. Raxmatov, R. (2023). SUV ISTE’MOLI XISOBINI OLISH TIZIMLARIDAN REAL-VAQT REJIMIDA FOYDALANISH HAMDA ULARNI BOSHQARISHNING RAQAMLI TIZIMLARINI JORIY ETISH. *Engineering problems and innovations*.

3. Умаров, А., Рахматов, Р., & Худайназаров, У. (2023, October). АНАЛИЗ ДИСКРЕТНОЙ СВЕРТКИ В MATLAB ДЛЯ ОБРАБОТКИ СИГНАЛОВ С ПОМОЩЬЮ ФИЛЬТРОВ. In *Conference on Digital Innovation:" Modern Problems and Solutions"*.

4. Хусанова, М., & Рахматов, Р. (2023, October). ИССЛЕДОВАНИЕ ПРОТОКОЛОВ МОНИТОРИНГА И ОБНАРУЖЕНИЯ МОБИЛЬНЫХ УГРОЗ. In *Conference on Digital Innovation:" Modern Problems and Solutions"*.

5. Джураев, М., Хусанов, Б., Нишонбоева, Ю., Рахматов, Р., & Мамажонов, К. (2021). Система мониторинга водных ресурсов с цифровыми технологиями. *Общество и инновации*, *2*(4/S), 538-544.

6. Nishonboyeva Y., Abdullayev A., Raxmatov R. (2022). Sug`orishda suv zaxiralaridan foydalanishning avtomatlashtirilgan boshqaruvi *Образование и наука в XXI веке*, *4*(25), 80-83.

7. Raxmatov, R. (2023). SUV RESURSLARINI BOSHQARISHDA IOT TEXNOLOGIYALARINING AHAMIYATI. *Journal of technical research and development*, *1*(2), 87-90.

8. Рахматов, Р., Мирзаев, Ж., & Худайназаров, У. (2023, October). THREAT INTELLIGENCE AND NETWORK SECURITY. In Conference on Digital Innovation:" Modern Problems and Solutions".

9. Мирзаев, Ж., Худайназаров, У., & Тожматов, Д. (2023, October). NETWORK SECURITY MONITORING IN CLOUD ENVIRONMENTS. In Conference on Digital Innovation:" Modern Problems and Solutions".

10. Dostonbek, T., & Jamshid, M. (2023). Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems. Central Asian Journal of Theoretical and Applied Science, 4(4), 93-98.

https://iot-analytics.com