УДК 004.056

Маткаримов А.И.

Преподаватель,

Туркменский государственный институт экономики и управления

Туркменистан, г. Ашхабад

Аллеков А.

Преподаватель,

Туркменский государственный университет имени Махтумкули

Туркменистан, г. Ашхабад

БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ В ИНТЕРНЕТЕ ВЕЩЕЙ

Аннотация: *В этой статье рассматривается вопрос безопасности и конфиденциальности в контексте Интернета вещей. Обсуждается актуальная проблема, основные угрозы и риски нарушения защиты данных. Анализируются текущие подходы и методы безопасности, предлагаются рекомендации по улучшению защиты информации.*

Ключевые слова: *Интернет вещей, безопасность, конфиденциальность, защита данных, угрозы.*

Интернет вещей (Internet of Things, IoT) - это сеть физических объектов, которые оснащены встроенными технологиями для взаимодействия друг с другом и с внешней средой. Интернет вещей является частью более широкой концепции Индустрии 4.0, которая предполагает внедрение цифровых технологий и автоматизации в производство и повседневную жизнь.

История интернета вещей начинается с изобретения радио в начале 20 века. С тех пор технологии связи и обработки данных развивались, и в настоящее время интернет вещей стал возможным благодаря развитию беспроводных сетей, сенсоров, микроконтроллеров и облачных вычислений.

Одной из особенностей интернета вещей является то, что он позволяет объединять различные устройства и системы в единую сеть, что позволяет им обмениваться данными и координировать свои действия. Это может быть полезно в различных областях, таких как умный дом, логистика, здравоохранение и т.д.

Потенциал интернета вещей огромен. Он может улучшить качество жизни людей, повысить эффективность производства и снизить затраты на ресурсы. Однако, для того чтобы полностью реализовать этот потенциал, необходимо решить множество проблем, связанных с безопасностью, конфиденциальностью и управлением данными.

Конфиденциальность Интернета вещей — это особые соображения, необходимые для защиты информации людей от воздействия в среде IoT . Эти шаги необходимы, поскольку в условиях Интернета вещей практически любому физическому или логическому объекту или объекту может быть присвоен уникальный идентификатор и возможность автономного взаимодействия через Интернет или аналогичную сеть.

Поскольку конечные точки или « вещи » в среде Интернета вещей передают собранные данные автономно через Интернет и обычно отображают эти данные в мобильных приложениях, они также работают совместно с другими конечными точками и взаимодействуют с ними. Функциональная совместимость вещей необходима для функционирования Интернета вещей, чтобы, например, сетевые элементы умного дома работали вместе бесперебойно.

Данные, передаваемые данной конечной точкой, сами по себе могут не вызывать каких-либо проблем с конфиденциальностью. Например, интеллектуальный счетчик, используемый для удаленного мониторинга и сбора данных для потребителя и его коммунальной компании, является обычным явлением и обычно безвреден. Однако когда даже фрагментированные данные с нескольких устройств Интернета вещей собираются, сопоставляются и анализируются, они могут дать конфиденциальную информацию, например, о местонахождении людей или образе жизни.

Идея сетевых устройств и других объектов является относительно новой, особенно с точки зрения глобальной связи и автономной передачи данных, которые являются центральными для Интернета вещей. Таким образом, риски безопасности не всегда учитывались при проектировании продукта, что может сделать даже предметы повседневного обихода уязвимыми.

Скептицизм и подозрительность в отношении систем Интернета вещей часто коренятся в проблемах кибербезопасности и конфиденциальности. Потребители чувствуют, что конфиденциальность их данных находится под угрозой; они беспокоятся как о компаниях, которым поручено защищать их данные, так и о злоумышленниках.

Следующие риски конфиденциальности по-прежнему препятствуют реализации полного потенциала Интернета вещей:

1. Лишние данные. Во всем мире существуют миллиарды подключенных устройств, которые генерируют огромные объемы данных всего за один день. У тех, кто действует недобросовестно, есть много целей и возможностей поставить под угрозу конфиденциальность потребителей. В результате производителям устройств IoT и компаниям, использующим эти устройства, приходится нелегко обеспечить общественное доверие.

2. Вторжение в личное пространство. Хакеры могут атаковать незащищенное устройство или сеть Интернета вещей, чтобы получить доступ к личной информации (PII) или другой конфиденциальной информации о потребителях. Производители устройств и организации, которые используют эти устройства, также имеют доступ к данным PII и должны принимать меры предосторожности для предотвращения несанкционированного доступа и неправильного использования.

3. Частный обмен данными. Производитель устройства может указать мелким шрифтом, как он передает данные о потребителях третьим лицам. Если потребители не читают юридическую документацию, прилагаемую к их датчикам, подключенным автомобилям и другим устройствам, их конфиденциальные данные могут по незнанию просматриваться и использоваться этими третьими лицами.

Тот факт, что подключенные к Интернету устройства могут работать с высокой производительностью в удаленных местах, во многих случаях полезен и даже критичен. Но это также означает, что хакеры и киберпреступники придумывают новые, изощренные тактики взлома этих устройств. Атаки типа «отказ в обслуживании» и вредоносное ПО — это методы, которые хакеры используют для компрометации данных устройств Интернета вещей.

Отсутствие тестирования и обязательных обновлений программного обеспечения как до, так и во время развертывания Интернета вещей делает многие организации уязвимыми для атак. Если производители устройств Интернета вещей не обращают внимания на проблемы безопасности, когда предприятия и потребители доверяют им поставку высокозащищенных продуктов и интеллектуальных устройств, они могут быть ошеломлены злоумышленниками. Если производители будут обеспечивать регулярное обновление программного обеспечения и встроенного ПО, со временем их устройства будут иметь меньше уязвимостей безопасности данных.

Еще одна проблема безопасности, влияющая на конфиденциальность IoT, — это эффект «подвижного движения» в различных отраслях, таких как поставщики медицинских услуг, страховые компании и производители автомобилей. Компании внедряют новые технологии, такие как Интернет вещей, в рамках более широкой трансформации Индустрии 4.0 , не подвергая их тщательной проверке. Например, организация может быстро настроить сеть Интернета вещей, не оценивая ресурсы, необходимые для обслуживания и защиты сети и ее устройств Интернета вещей в долгосрочной перспективе.

Наконец, недостатки в экосистеме безопасности IoT могут оказаться более фундаментальными, если производители будут производить устройства без вычислительной мощности, необходимой для встроенной безопасности. Некоторые устройства созданы для выполнения основных функций, таких как обработка данных, без внимания к безопасности. Будущие взломы и утечки данных, вероятно, привлекут внимание к необходимости встроенной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. "Интернет вещей: практическое руководство", Владимир Осьмак, 2018

2. "Интернет вещей: революция в бизнесе", Ричард Гилберт, 2017

4. "Интернет вещей: новое поле для инноваций", Майкл Портер, Джеймс Хеппельманн, 2015

5. "Интернет вещей: будущее уже здесь", Доминик Пратт, 2014

6. "Безопасность Интернета вещей: практическое руководство", М.В. Зацепин, 2017

7. "Интернет вещей: безопасность и конфиденциальность", А.В. Алферов, 2018

8. "Интернет вещей: конфиденциальность данных", Е.А. Сидорова, 2021

Matkarimov A.
Lecturer,
Turkmen State Institute of Economics and Management
Turkmenistan, Ashgabat

Allekov A.
Lecturer,
Magtymguly Turkmen State University
Turkmenistan, Ashgabat

DATA SECURITY AND PRIVACY ON THE INTERNET OF THINGS

Abstract: *This article examines the issue of security and privacy in the context of the Internet of Things. The current problem, the main threats and risks of data security violations are discussed. Current security approaches and methods are analyzed and recommendations for improving information security are offered.*

Keywords: *Internet of things, security, privacy, data protection, threats.*