МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Факультет экономический
Кафедра теоретической экономики

КУРСОВАЯ РАБОТА

по дисциплине «Цифровая экономика»

ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ «ИНТЕРНЕТА ВЕЩЕЙ» И СПОСОБЫ ИХ ПРЕОДОЛЕНИЯ

Работу выполнил 14.06.2023 Д.С. Ковшиков
(подпись, дата)
Направление подготовки 38.03.05 – Бизнес-информатика курс 2
Направленность (профиль) Бизнес в цифровой экономике
Научный руководитель
канд. экон. наук, доцент 14.06.2023 А.В. Болик
(подпись, дата)
Нормоконтролер
канд. экон. наук, доцент 9.06.2023 А.В. Болик
(подпись, дата)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность: интернет вещей связывает объекты и расширяет использование данных, обеспечивая повышение производительности и видоизменяя отрасли. Интернет вещей (IoT) — это система, которая объединяет устройства в компьютерную сеть и позволяет им собирать, анализировать, обрабатывать и передавать данные другим объектам через программное обеспечение, приложения или технические устройства IoT-устройства функционируют самостоятельно, хотя люди могут настраивать их или предоставлять доступ к данным. IoT-системы работают в режиме реального времени и обычно состоят из сети умных устройств и облачной платформы, к которой они подключены с помощью WiFi, Bluetooth или других видов связи.

Целью курсовой работы является классификация угроз интернет вещей и способы их защиты от угроз.

Исходя из поставленной цели можно выделить следующие *задачи*:

- Рассмотреть понятие и принципы Интернета вещей;
- Изучить подключенные вещи и уровни IoT;
- Выяснить способы защиты от угроз;

Объект исследования: интернет вещи.

Предмет исследование: анализ угроз интернет вещей.

Методы: анализ и обобщение специальной литературы, публикаций в периодических изданиях, новости.

Информационную базу исследования: составили работы авторов, занимающихся изучением интернет вещей и их угроз, так же данные российских организаций, законодательные, правовые и нормативные документы других российских и международных организаций, периодические информационные материалы и статистика.

Методологическая основа: В курсовой работе применялись различные методы исследования: статистическое наблюдение, метод анализа и синтеза, методы группировки и сравнений, метод сбора фактов.

Структура курсовой работы представляет собой введение, две главы, заключение и список использованной литературы.

1 Общая характеристика пользовательского Интернета вещей

1.1Понятие и принципы Интернета вещей (IoT, Internet of Things)

Термин «Интернет вещей» был впервые употреблен в 1999 году Кевином Эштоном, предпринимателем и соучредителем центра Auto-ID Labs (независимая сеть лабораторий и исследовательская группа в области сетевой радиочастотной идентификации и новых сенсорных технологий) при Массачусетском технологическом институте. Эштон состоял в команде, которая сумела изобрести способ подключения объектов к интернету при помощи технологии RFID. RFID-метка — это метка идентификации, позволяющая идентифицировать объекты посредством радиосигналов; на нее можно нанести определенную информацию, а позднее считать устройством.

В 2012 году произошли значительные изменения датчиков, что привело к ускорению рыночной готовности IoT, и для многих компаний это означало, что цифровая трансформация набирает обороты. Технологическое совершенствование сделало возможным появление МЭМС — микро электромеханических систем (миниатюрное устройство, изготовленное методом микрообработки как из механических, так и из электрических компонентов). Благодаря этому датчики уменьшились настолько, что их стало возможно фиксировать, например, на одежде.[24[

На сегодняшний день существует несколько определений такого явления, как Интернет вещей. Зачастую многие вендоры и интеграторы также склонны интерпретировать данный термин по-разному, несколько видоизменяя трактовку. Несмотря на то, что сам термин и направление появились только в 1999 году, идея витала в воздухе достаточно давно.

К примеру, еще в далеком 1926 году Никола Тесла в интервью для журнала «Collier’s» сказал, что в будущем радио будет преобразовано в

«большой мозг», все вещи станут частью единого целого, а инструменты, благодаря которым это станет возможным, будут легко помещаться в кармане.

Одной же из самых первых «умных вещей» можно назвать тостер выпускника MIT Джона Ромки (одного из отцов-основателей протокола TCP/IP), подключенный к сети в 1990 году.

Рисунок 1 - История развития IoT [21]

В качестве наиболее простого и оптимального для понимания определения Интернета вещей (IoT) можно привести следующее:

IoT - это совокупность устройств, обладающих интерфейсами сетевого взаимодействия, и самой объединяющей их сети. Важно отметить, что устройство может подсоединяться к данной сети через промежуточное сопряжение - или даже через цепочку сопряжений. Простейший пример: сопряжение фитнес-трекера с внешней сетью через мобильный телефон.

IoT - сеть физических объектов, обладающих встроенными технологиями взаимодействия с внешней средой с возможностью передачи данных о своём текущем состоянии и приеме данных извне.

IoT - концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей

как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека. [16]

Наряду с термином IoT, часто также используется и другой термин, который появился существенно раньше - M2M (Межмашинное взаимодействие, Machine- to-Machine), общее название технологий, которые позволяют приборам обмениваться информацией друг с другом. Это проводные и беспроводные системы датчиков, которые передают информацию от одного устройства другому. Одной из первых разработок в области мобильного межмашинного взаимодействия является OmniTRACS - решение Qualcomm, разработанное в 1989 году для отслеживания коммерческого транспорта.

Фактически M2M позволил технологиям АСУ ТП в режиме онлайн получать доступ к объектам, которые ранее были недоступны - не было возможности наладить с ними постоянное кабельное соединение. Такие объекты можно разделить на два класса: удалённые от кабельных сетей объекты и подвижные объекты. Ключевым фактором роста технологий M2M стало существенное развитие систем глобального позиционирования GPS/ГЛОНАСС и др.

Концепция IoT, появившись в 1999 году, в год представления технологии радиочастотной идентификации физических предметов (RFID), сразу получила мощный толчок к развитию. В 2008 и 2009 годах состоялся переход от «Интернета людей» к «Интернету вещей», т.е. количество подключенных к сети предметов превысило количество людей.

Активная реализация и развитие технологических платформ на основе концепции продолжаются и сейчас. Ключевыми факторами развития IoT стали технологии межмашинного взаимодействия (M2M), развитие технологий связи 4G, распространение протокола IPv6, облачных технологий (SaaS, PaaS, IaaS и др.), программно-определяемых сетей (SDN) и программно-определяемых дата-центров (SDDC).

В первом десятилетии XXI века получила распространение доступная беспроводная связь, став важным фактором для развития технологий межмашинного взаимодействия. [25]

Основными отраслями применения IoT стали:

1. Системы мониторинга и управления транспортом, ЖКХ, медицинскими устройствами.

2. Системы мониторинга и управления безопасностью автомобилей (противоугонные системы), судов, домов, квартир и офисов, людей и животных.

3. Системы мониторинга промышленного оборудования и т.п.

Интернет вещей основывается на трех базовых принципах. Во-первых, повсеместно распространенную коммуникационную инфраструктуру, во-вторых, глобальную идентификацию каждого объекта и, в-третьих, возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет, к которой он подключен.

Наиболее важными отличиями Интернета вещей от существующего интернета людей являются:

– фокус на вещах, а не на человеке;

– существенно большее число подключенных объектов;

– существенно меньшие размеры объектов и невысокие скорости передачи данных;

– фокус на считывании информации, а не на коммуникациях;

– необходимость создания новой инфраструктуры и альтернативных стандартов.

Концепция сетей следующего поколения NGN предполагала возможность коммуникаций людей (непосредственно или через компьютеры) в любое время и в любой точке пространства. Концепция Интернета вещей включает еще одно направление -коммуникация любых устройств или вещей.[9]

Коммуникация в любое время:

1. В движении;
2. Ночью;
3. Днем;
4. На улице;
5. Дома;
6. Около компьютера;

Коммуникация в любом месте:

1. Между компьютерами;
2. Между людьми (без компьютера) между людьми и устройствами;
3. Между устройствами Коммуникация;
4. Любых устройств;

Интернет вещей (Internet of Things, IoT) — это множество физических объектов, подключенных к интернету и обменивающихся данными. Концепция IoT может существенно улучшить многие сферы нашей жизни и помочь нам в создании более удобного, умного и безопасного мира.

Примеры Интернета вещей варьируются от носимых вещей, таких как умные часы, до умного дома, который умеет, например, контролировать и автоматически менять степень освещения и отопления. Также ярким примером служит так называемая концепция умного предприятия (Smart Factory), которое контролирует промышленное оборудование и ищет проблемные места, а затем перестраивается так, чтобы не допустить поломок. Интернет вещей занимает важное место в процессе цифровой трансформации в компаниях. Прогнозируется, что к 2030 году количество подключенных к сети устройств вырастет примерно до 24 млрд с годовой выручкой до 1,5 трлн долларов.

1.2 Подключенные вещи и уровни IoT

Интернет вещей включает три уровня: компоненты, структурные блоки и система систем, как показано на рисунке 2. Базовые возможности зависят от

компонентов. Структурные блоки охватывают технологии продуктов, которые возникают в результате интеграции новых компонентов Интернета вещей с компонентами традиционных технологий. Система систем описывает уникальные способы возможного объединения и интеграции структурных блоков, а также и их развертывания в различных отраслях.

Рисунок 2 - Уровни Интернета вещей [7]

Компоненты предназначены специально для определенного применения, а значит - и для решения. Например, в системе водоснабжения используются измерительные приборы, датчики давления и расхода, а также компоненты контроля значений. Структурные блоки - это общие для многих решений элементы, чрезвычайно важные для успешной работы. В качестве примеров можно привести модули коммуникации, безопасности, аналитики, удаленные вычислительные узлы и модули обновлений.

Структурные блоки являются основой многих решений и включают модули коммуникации, безопасности и аналитики, удаленные вычислительные узлы и модули обновления. Среди других примеров структурных блоков: программное обеспечение, бытовая техника, мобильные устройства, технологии обеспечения безопасности и конфиденциальности, а также коммуникационные и сетевые технологии. Сюда также входит бытовая и коммерческая электроника; автомобильный, воздушный и водный транспорт; технологии автоматизации домов (включая мониторинг и

измерение показателей); а также интернет- и сетевые протоколы (например, IPv6). [10]

Структурные блоки используются для создания систем, которые затем объединяются в систему систем. В мире Интернета вещей различия определяются поддерживаемым операционным сценарием.

Например, автомобиль — это система, состоящая из многочисленных структурных блоков и компонентов. Система систем для уличного движения позволяет автомобилю и водителю взаимодействовать с системами уличного движения, чтобы ориентироваться в маршрутах и дорожном движении. Для автопроизводителей̆ контекст смещается на системы поддержки потребителей̆. Собранная информация по безопасности, условиям и стилю вождения, а также записи о техническом обслуживании передаются в системы поддержки клиентов производителя, образуя систему систем обслуживания клиентов. В обоих сценариях решение Интернета вещей выполняет координацию и взаимодействие многих систем меньшего масштаба, каждая из которых обладает собственным уровнем автономности, зависимости и взаимодействия.

Примерами системы систем также являются IBM Smarter Cities и интеллектуальные энергосистемы, системы контроля окружающей среды, наземный транспорт, авиация и аэронавтика, безопасность и наблюдение. Сюда же можно отнести решения в следующих сферах: фармацевтика, медицина и здравоохранение, розничная торговля, цепочки поставок, обработка и производство, сельское хозяйство, контроль за продовольственными товарами и пищевыми продуктами, СМИ и развлечения, а также операционные сценарии и экономические обоснования.

Бизнес-задачи, возникающие в Интернете вещей

Интернет вещей уже вошел в нашу жизнь и будет все больше развиваться и влиять на корпоративные среды. Коммерческие и технические руководители, ответственные за такие среды, должны понимать, на какие

задачи и подходы необходимо обратить внимание в экосистеме с Интернетом вещей.

Основное внимание необходимо уделить критически важным операционным факторам, таким как масштабируемость, доступность, управляемость, управление данными, безопасность и удобство использования. Эти факторы относятся к контексту гибридной среды, где многие аспекты развертывания находятся вне контроля корпорации.

Масштабируемость

В среде с применением Интернета вещей есть два типа задач, связанных с масштабируемостью, каждый из которых создает уникальные сложности для пользователей и корпораций. Первый тип связан с количеством подключенных устройств. Второй - с объемом создаваемых данных.

Задачи масштабируемости для подключенных устройств зависят от количества параллельных подключений (пропускная способность), которые может поддерживать система, и уровня качества обслуживания (QoS), который можно гарантировать. Здесь интернет-масштабируемость является критическим фактором.

Доступность

Доступность Интернета вещей связана с восстанавливаемостью и надежностью. Полная доступность систем может требовать применения к различным компонентам и структурным блокам технических принципов, зависящих от практических потребностей конкретной отрасли.

Влияние архитектуры на доступность обусловлено, в частности, увеличивающимся спросом на облачные вычисления и модели "x как услуга", например программное обеспечение как услуга. Корпорации должны тщательно изучать последствия использования необходимых услуг и возможностей среды Интернета вещей. Им может потребоваться заново рассмотреть свои соглашения об уровне обслуживания для облачных решений, чтобы определить, возможен ли необходимый уровень доступности.

Инновационное решение предотвращает сбои и отказы, помогая компаниям с гибридной средой (локальной и облачной) соответствовать ожиданиям клиентов и удовлетворять потребности предприятия.

Управляемость

Сейчас модель управления применяется только к системам, связанным с ИТ, например серверам, компьютерам и устройствам хранения данных.

Несмотря на разумное управление, скажем, мобильными телефонами и планшетами, большинство других устройств Интернета вещей не входит в расширенную экосистему, систематическое управление ими не осуществляется. В Интернете вещей большинство устройств работает удаленно и без прямого взаимодействия с человеком - управлять ими нужно точно так же, удаленно и без участия человека. Простого применения современных методов и технологий управления сетями и системами недостаточно. Необходимы новые подходы, чтобы развивать архитектуру Интернета вещей и управлять ее жизненным циклом.

Управление данными

Сочетание вычислительных парадигм больших данных и Интернета вещей фундаментально меняет способ нашей работы, развлечений и взаимодействия со средой. Если большие данные связаны с объемом, скоростью, проверкой и достоверностью, то Интернет вещей позволяет использовать эти данные осмысленным образом, повышая производительность и качество жизни.

Например, Интернет вещей может собирать пространственно-временную информацию, то есть данные о пространстве (местонахождении) и времени. Эта информация в сочетании с аналитическими технологиями позволяет по-новому взглянуть на то, когда, где и как могут или должны взаимодействовать люди и устройства. Ключевым фактором является то, как корпорации хранят и используют эти данные, а также управляют ими. Многие корпорации уже применяют такие технологии, как IBM SPSS, Tealeaf и IBM Cognos для проведения сложного анализа и углубленного понимания

шаблонов, необычных событий и аномалий. Использование этих технологий в контексте Интернета вещей открывает новые пути создания инноваций, предоставляющих новые возможности поддержки ключевых бизнес-процессов, таких как электронная коммерция, цепочки поставок и управление обслуживанием потребителей. Но чтобы достичь этого уровня возможностей, необходимо усовершенствовать базу данных, управление контентом и информационные технологии. [1]

Безопасность

При традиционном обеспечении безопасности ИТ устанавливаются защитные границы и брандмауэры вокруг внутренних систем ИТ. Но с Интернетом вещей концепция контролируемого доступа заменяется концепцией контролируемого доверия, при которой возможны самые разные решения. Для решения задач безопасности необходимо внедрять Интернет вещей таким образом, чтобы можно было эффективно выполнить авторизацию, проверку подлинности, обеспечить контроль доступа, конфиденциальность и доверие, сохранив удобство использования.

Удобство использования

Удобство использования играет большую роль в решениях будущего. ИТ-решения традиционно предназначались для реализации определенной задачи, на основе которой проводилось обучение.

Применительно к решениям Интернета вещей такой тип обучения может быть сложным и неэффективным, поскольку придется делать устройства все более и более удобными, чтобы они устраняли разрыв между культурными различиями и разным уровнем знаний и навыков пользователей. Системы Интернета вещей могут обеспечивать подробное представление сложных систем, для чего необходимо использовать эстетически привлекательный и удобный в использовании дизайн с многоязычной поддержкой и контекстной справкой.

2 Потенциальные угрозы пользователям

2.1 Классификация угроз

Экосистема IoT-технологий представляет собой комбинацию разных технологических зон: зона IoT-устройств, сетевая зона и облачная зона. Эти зоны могут быть источником цифровых данных. То есть данные можно собирать с умного устройства или датчика из внутренней сети, такого как брандмауэр или маршрутизатор, или из внешних сетей (облако или приложение). Эти технологические зоны являются и объектом криминального интереса киберпреступников.

Для борьбы с киберпреступлениями был создан специальный раздел криминалистики - компьютерная криминалистика, или форензика (англ. Computer forensics), - прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании доказательств в виде компьютерной информации, методах поиска, получения и закрепления таких доказательств. IoT-криминалистика (англ. IoT-forensics) как подраздел форензики занимается расследованием киберпреступлений в системе IoT, исследованием цифровых доказательств. [19]

В ходе расследования компьютерных преступлений, связанных с мошенничествами, или компьютерных атак, средствами которых так или иначе являлись сетевые соединения, проводят цифровую экспертизу - специальное исследование, включающее анализ использования сетевых технологий. В зависимости от места хранения данных в системе IoT эксперты в сфере IoT - криминалистики выделяют три опасных участка в ландшафте киберугроз: облако, сеть и устройство, соответственно выделяются облачная криминалистика, сетевая и криминалистика на уровне устройства IoT.

Поскольку ценные данные часто хранятся в облаке, облачная инфраструктура является одной из самых важных целей для злоумышленников. Для проведения традиционной цифровой экспертизы эксперт-криминалист сначала получает изъятое цифровое оборудование, а

затем начинает расследование для извлечения цифровых доказательств (цифровых данных, которые можно использовать в качестве доказательства совершения киберпреступления). Однако если данные хранятся в облаке, используется другой сценарий, потому что цифровые доказательства могут быть размещены в облачных хранилищах на разных серверах и их трудно извлечь оттуда. Кроме того, в облаке ограничен доступ к инфраструктуре и информации о точном месте хранения данных. При расследовании инцидента, произошедшего в облаке, поставщик облачных услуг может запросить информацию об имени владельца данных или месте хранения соответствующих данных. [22]

Следует отметить, что у облачных сервисов, использующих виртуальные машины в качестве серверов, данные могут храниться на этих серверах. Реестры записи или временные интернет-файлы на серверах могут быть удалены, если они не синхронизированы с устройствами хранения, например если эти серверы перезапускаются или выключаются.

Сетевая криминалистика проводит исследования всех видов сетей, которые используются IoT-устройствами для отправки и получения данных. К ним относятся домашние, промышленные и локальные сети, MAN и WAN. Например, если инцидент связан с устройствами IoT, все журналы, в которых отражен поток трафика, такие как брандмауэры или журналы IDS, могут быть потенциальными доказательствами.

Экспертиза на уровне устройства включает в себя все потенциальные цифровые доказательства, которые могут быть собраны с устройств IoT, таких как графика, аудио, видео. Примером подобных цифровых доказательств являются видео и графика с камеры видеонаблюдения или аудиозаписи с умной колонки Amazon Echo.

Существующие инструменты в области цифровой криминалистики могут не соответствовать инфраструктуре среды IoT. Из-за того, что большинство данных IoT хранится в облаке, оно становится одним из основных источников доказательств преступлений в IoT, а как писалось выше,

найти необходимые цифровые доказательства в облаке даже эксперту-криминалисту затруднительно. Кроме того, на одном физическом сервере может работать несколько виртуальных машин, принадлежащих разным владельцам. Большие облачные хранилища могут быть недоступны после совершения преступления. Все эти проблемы требуют решения и поиска новых инструментов для расследования киберпреступлений в IoT. [3]

Угрозы:

1) Умышленные действия

Вредоносное ПО - программное обеспечение, предназначенное для выполнения нежелательных и несанкционированных действий в системе без согласия пользователя. Это ПО может привести к повреждению, модификации или краже информации. Его опасность может быть высокой.

Эксплойт - код, разработанный для использования уязвимости с целью получения доступа к системе. Эту угрозу трудно обнаружить, и в средах IoT ее опасность варьируется от высокой до критической, в зависимости от затронутых активов

Целевая атака - атака, предназначенная для конкретной цели, которая проводится в течение длительного периода времени в несколько этапов. Основная цель преступника – оставаться незамеченным и получить как можно больше конфиденциальных данных, информации или контроля. Хотя опасность этой угрозы является средней, ее обнаружение – обычно очень сложный и длительный процесс.

DDoS-атака - в процессе DDoS-атаки несколько систем атакуют одну цель, чтобы нагрузить ее и привести к сбою. Это можно сделать путем создания множества соединений, переполнения канала связи или многократного повторного воспроизведения одних и тех же сообщений.

Скомпрометированное устройство - Эту угрозу трудно обнаружить, поскольку скомпрометированное устройство трудно отличить от оригинала. Эти устройства обычно имеют бэкдоры и могут использоваться для проведения атак на другие системы в окружающей среде.

Утрата конфиденциальности - эта угроза опасна как утратой конфиденциальности пользователя, так и воздействием постороннего персонала на элементы сети.

Модификация информации - в этом случае цель состоит не в повреждении устройства, а в манипуляции информацией, чтобы вызвать хаос или получить денежную прибыль

2) Перехват информации

Атака «человек посередине» - активная атака подслушивания, при которой злоумышленник передает сообщения от одной жертвы другой, чтобы заставить их поверить, что они разговаривают непосредственно друг с другом.

Подключение к активной сессии - взятие под контроль активного сеанса связи между двумя элементами сети. Злоумышленник может получить важную информацию, в том числе и конфиденциальную.

Перехват информации - несанкционированный перехват и (иногда) модификация частной коммуникации, например телефонных звонков, мгновенных сообщений, сообщений электронной почты.

Сетевая разведка - пассивное получение внутренней информации о сети: подключенные устройства, используемый протокол, открытые порты, используемые службы и т. д.

Перехват соединения - Кража соединения для передачи данных, при этом незаконный хост действует как законный с целью кражи, изменения или удаления передаваемых данных.

3) Отключение

Отключение питания - преднамеренное или случайное прерывание или сбой в сети. В зависимости от затронутого сегмента сети и времени, необходимого для восстановления, опасность этой угрозы варьируется от высокой до критической.

Сбой устройства - сбой или выход из строя аппаратного устройства.

Сбой системы - сбой программных служб или приложений.

Потеря сервиса поддержки - недоступность услуг поддержки, необходимых для правильной работы информационной системы.

4) Технический бой

Уязвимости на программном уровне - устройства IoT часто уязвимы из-за слабых паролей, неизмененных паролей, установленных по умолчанию, программных ошибок и ошибок конфигурации.

Сторонние ошибки - ошибки в активном элементе сети, вызванные неправильной настройкой другого элемента, который имеет к нему прямое отношение

5) Катастрофы

Стихийные бедствия - наводнения, сильные ветры, сильные снегопады, оползни и другие стихийные бедствия, которые могут повредить устройства физически.

Аварии в среде IoT - аварии в среде развертывания IoT-оборудования, приводящие к их неработоспособности.

6) Физическая атака

Модификация устройства - модификация устройства, внесение изменений в устройство (например, путем использования плохой конфигурации портов, использования открытых портов).

Уничтожение устройства - порча, кража и т. п.

Различные угрозы несут разные потенциальные опасности, которые различаются в зависимости от сценариев использования. Ниже приведена классификация угроз, характерных для IoT, с описанием разных их видов [9].

2.2 Способы защиты от угроз

Ниже представлен подробный список мер по обеспечению безопасности, направленных на снижение угроз, уязвимостей и рисков, влияющих на устройства и среды IoT

Таблица 1 - Способы защиты от угроз [13]

Способы защиты	**Описание**
Управление информационной безопасностью и управление рисками	Меры безопасности, касающиеся анализа рисков безопасности информационной системы, политики, аккредитации, показателей и аудита, а также безопасности человеческих ресурсов
Управление экосистемами	Меры безопасности в отношении картирования экосистем и отношений экосистем
Архитектура информационной безопасности	Меры безопасности, касающиеся конфигурации систем, управления активами, разделения систем, фильтрации трафика и криптографии
Администрирование информационной безопасности	Меры безопасности в отношении административных учетных записей и административных информационных систем
Управление идентификацией и доступом	Меры безопасности в отношении аутентификации, идентификации и прав доступа
Техническое обеспечение информационной безопасности	Меры безопасности в отношении процедур технического обеспечения ИТ-безопасности и удаленного доступа
Управление инцидентами компьютерной безопасности	Меры безопасности в отношении анализа и реагирования на инциденты безопасности в информационной системе, а также отчет об инцидентах

Вышеперечисленные меры безопасности классифицированы в зависимости от того, к какой области IoT-экосистемы они применяются.

Кроме этого, каждая мера безопасности может быть отнесена к определённой категории в зависимости от ее характера – это может быть политика безопасности, которую необходимо учитывать при разработке устройств; организационные меры, ориентированные на бизнес и сотрудников, которые должны быть приняты самой организацией; наконец, технические меры, направленные на снижение потенциальных рисков для устройств IoT других элементов IoT-экосистемы. Соответственно, выявленные базовые меры безопасности IoT распределены по трем основным категориям, представленным на рисунке 3.

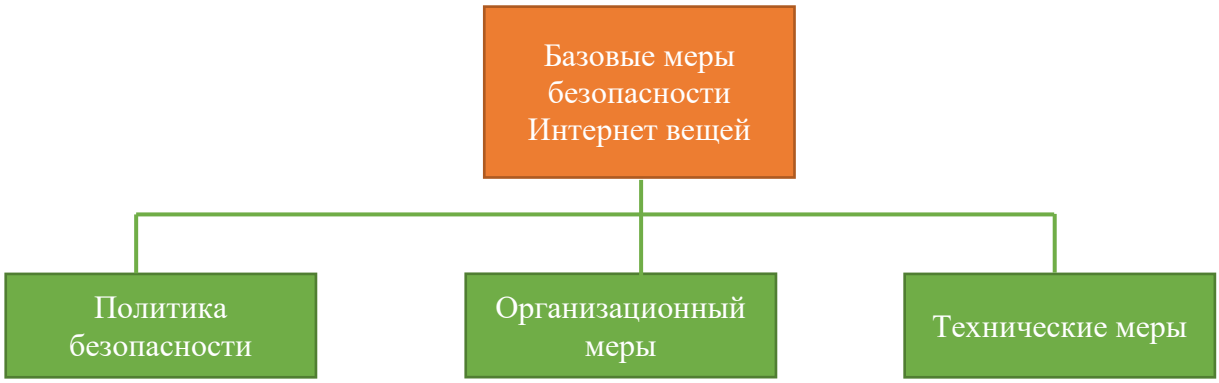

Рисунок 3 - Базовые меры безопасности интернет вещей [11]

Первая группа мер относится к политике безопасности, которая в целом направлена на обеспечение информационной безопасности и призвана сделать ее более конкретной и надёжной. Она должна соответствовать деятельности организации и содержать хорошо документированную информацию. В этом контексте были определены следующие рекомендации по безопасности.

Стоит отметить, что, когда речь идет об обеспечении безопасности конфиденциальности при проектировании, меры безопасности должны отражать особенности и контекст, в котором будет развернуто устройство или система IoT. Когда дело доходит до IoT, риск зависит от контекста (то есть

основывается на сценарии приложения), и в этом отношении меры безопасности должны применяться с учетом этого фактора. [22]

Организационные меры

Все предприятия должны иметь организационные критерии информационной безопасности. Действия персонала должны обеспечивать безопасность, управление процессами и безопасную работу с информацией в рабочем процессе организации. Организации должны обеспечить ответственность подрядчиков и поставщиков за выполнение рассматриваемых функций. В случае инцидента безопасности организация должна быть подготовлена (ответственность, оценка и реагирование).

Технические меры

Меры безопасности должны учитывать и охватывать технические элементы, чтобы уменьшить уязвимости IoT. Ниже представлен обзор необходимых технических мер для сохранения и защиты безопасности информации в IoT.

Аппаратное обеспечение безопасности

Рекомендуется использовать оборудование, которое включает в себя аппаратные средства безопасности для усиления защиты и целостности устройства: например, специализированные микросхемы, которые обеспечивают защиту на транзисторном уровне (защищенное хранение данных и средств аутентификации, идентификация устройства и защита ключей в состоянии покоя и в процессе использования). Защита от локальных и физических атак может быть обеспечена с помощью функциональной безопасности.

Управление доверием и целостностью

Доверие к загрузочной прошивке должно быть установлено до того, как будет установлено доверие к любому другому программному обеспечению. Необходим контроль за установкой программного обеспечения в операционных системах, чтобы предотвратить загрузку недостоверного программного обеспечения и файлов.

Необходимо разрешить системе возвращаться в первоначальное безопасное состояние, в котором она находилась до нарушения безопасности. Возможность восстановления системы в случае, если обновление не было завершено корректно, также играет важную роль. Рекомендуется использовать протоколы и механизмы, способные управлять доверием.

Надежное обеспечение безопасности и конфиденциальности по умолчанию

Любые применимые функции безопасности должны быть включены по умолчанию, а любые неиспользуемые или небезопасные функции – отключены. Важно создавать сложные пароли по умолчанию для отдельных устройств.

Защита персональных данных

Персональные данные должны собираться и обрабатываться на основании соответствующих законов, они никогда не должны собираться и обрабатываться без согласия субъекта данных. Необходимо проверять, используются ли персональные данные в указанных целях. Пользователи IoT должны иметь возможность контролировать собираемую информацию.

Безопасность и надежность системы

При проектировании системы важно учитывать системные и эксплуатационные сбои, не допуская, чтобы система вызывала неприемлемый риск травмирования или причинения физического ущерба. Основные функции должны продолжать работать при потере связи и/или негативном воздействии со стороны скомпрометированных устройств или облачных систем.

Безопасное обновление программного обеспечения

Необходимо убедиться, что программное обеспечение устройства, его конфигурация и его приложения имеют возможность обновления по беспроводной сети, сервер обновлений безопасен, файлы обновления передаются через защищенное соединение и не содержат конфиденциальных данных, подписаны авторизованным доверенным объектом и зашифрованы с использованием принятых методов шифрования, что пакет обновления имеет

свою цифровую подпись, сертификат подписи и цепочку сертификатов подписи. Автоматические обновления прошивки не должны изменять пользовательские настройки предпочтений, параметров безопасности или конфиденциальности без уведомления пользователя.

Аутентификация

Необходимо разрабатывать системы аутентификации и авторизации на основе моделей угроз на уровне системы. Важно убедиться, что во время первоначальной установки пароли и имена пользователей по умолчанию, а также слабые или недействительные пароли и имена пользователей изменены. механизмы аутентификации должны использовать надежные пароли или персональные идентификационные номера (PIN). Уместно рассмотреть возможность использования двухфакторной или многофакторной аутентификации, такой же, как в смартфонах, биометрических данных и т.д.

Важно учитывать, что учетные данные для аутентификации должны быть зашифрованы. Необходимо убедиться, что механизм восстановления или сброса пароля надежен и не предоставляет злоумышленнику информацию, указывающую на действительную учетную запись. То же самое относится и к механизмам обновления и восстановления ключей. [5]

Авторизация

Необходимо ограничить действия, разрешенные для данной системы, путем внедрения механизмов детализированной авторизации и использования принципа наименьших привилегий: приложения должны работать на самом низком уровне привилегий. Прошивка устройства должна быть разработана таким образом, чтобы изолировать привилегированный код, процессы и данные самой прошивки. Аппаратное обеспечение устройства должно обеспечивать изоляцию для предотвращения доступа злоумышленника к чувствительному к безопасности коду.

Контроль доступа – физическая безопасность и безопасность окружающей среды

Целостность и конфиденциальность данных должны обеспечиваться средствами контроля доступа. Когда субъект, запрашивающий доступ, авторизован для доступа конкретным процессам, необходимо обеспечить соблюдение определённой политики безопасности.

Обнаружение несанкционированного доступа и реагирование на аппаратное вмешательство не должны зависеть от сетевого подключения. Важно, чтобы устройства были оснащены только теми внешними физическими портами, которые необходимы им для работы.

Безопасная и надежная связь

Необходимо обеспечить различные аспекты безопасности – конфиденциальность, целостность, доступность и подлинность информации, передаваемой по сетям, а также хранящейся в приложении IoT или в облачном хранилище. Важно учесть, что безопасность связи обеспечивается современными стандартизированными протоколами безопасности шифрования, такими как TLS.

Учетные данные не должны передаваться в открытом виде по сети.

Чтобы обеспечить надёжный обмен данными от передачи до приема, они всегда должны быть подписаны, когда и где бы они ни собирались и ни хранились. Необходимо отключать определенные порты или сетевые подключения для выборочного подключения. Также стоит установить контроль трафика, отправляемого или получаемого сетью, для снижения риска автоматизированных атак.

Безопасные интерфейсы и сетевое обслуживание

Разделение сетевых элементов на отдельные компоненты помогает изолировать инциденты безопасности и минимизировать общий риск.

Протоколы должны быть разработаны таким образом, чтобы в случае взлома одного устройства это не повлияло на весь набор. Необходимо избегать предоставления одного и того же секретного ключа для всего семейства продуктов, поскольку взлома одного устройства будет достаточно, чтобы

взломать и остальные устройства этого семейства. Важно внедрить инфраструктуру, устойчивую к DDoS-атакам и балансирующую нагрузки.

Необходимо убедиться, что веб-интерфейсы полностью шифруют сеанс пользователя – от устройства до серверных служб – и не подвержены XSS, CSRF, SQL-инъекциям и т. п.

Безопасная обработка ввода и вывода

Должна проводиться валидация вводимых данных (обеспечение безопасности данных перед использованием) и фильтрация вывода.

Протоколирование

Необходимо внедрить систему протоколирования, которая регистрирует события, связанные с аутентификацией пользователей, управлением учетными записями и правами доступа, изменениями правил безопасности и функционированием системы. Журналы должны храниться на долговременных носителях и извлекаться через аутентифицированные соединения.

Мониторинг и аудит

Важно осуществлять регулярный мониторинг для проверки поведения устройства, обнаружения вредоносных программ и выявления ошибок целостности. Необходимо проводить периодические проверки средств контроля безопасности, чтобы убедиться в их эффективности, и тестирования на проникновение. Применение этих технических мер должно учитывать особенности экосистемы IoT, такие как масштабируемость, то есть огромное количество задействованных устройств требует принятия определенных мер на уровне специализированных компонентов архитектуры. [4]

ЗАКЛЮЧЕНИЕ

В первой главе представлена характеристика интернет вещей. Каждое устройство/машина IoT содержит датчики, связанные с облачной платформой IoT. Последняя в свою очередь собирает, обрабатывает, и распространяет данные с каждого подключенного устройства/датчика, позволяя устройствам взаимодействовать друг с другом и в интернете (данный процесс межмашинной связи через платформы IoT называют M2M). IoT индустрия появилась только в 2005 году. Ей нужно время, чтобы «созреть». Поэтому компании вкладывают миллионы долларов в хакатоны, изучая уязвимости в IoT. на вершине горы окажутся компании, которые обеспечат безопасность на IoT платформах и связанного с ними оборудования, а также те, кто будет решать соответствующие деловые и потребительские задачи с помощью товаров и услуг IoT.

Но любая мощная технология, как мы знаем, может быть использована не по назначению. Сегодня искусственный интеллект действует для многих благих целей. В том числе, чтобы лучше ставить медицинские диагнозы, находить новые способы лечения рака и делать автомобили безопаснее. Тем не менее, по мере расширения возможностей искусственного интеллекта мы также увидим, что он используется в опасных или злонамеренных целях.

В второй главе представлен обзор угроз безопасности Интернета вещей с точки зрения последних разработок, решений для их устранения и новых технологий в развитии. Он показывает первостепенное значение безопасности при разработке жизнеспособных решений Интернета вещей. Надеемся, данная статья поможет вам выбрать безопасные технологии Интернета вещей для вашей организации.

Применение технологии 1oT создает возможности и риски для безопасности, поэтому проблемы с устройствами 1oT в отношении безопасности огромны. Тщательная оценка рисков безопасности должна предшествовать любому внедрению Интернета вещей, чтобы гарантировать

обнаружение всех соответствующих основных проблем. Без достаточной безопасности и защиты данных, IoT не будет успешным в долгосрочной перспективе. Поэтому перед каждым производителем Интернета вещей стоит задача дополнить все этапы процессов разработки, вплоть до эксплуатации оборудования, соответствующими мерами безопасности. В будущей работе важно разработать структуру для выполнения и оценки рисков безопасности в IoT, чтобы гарантировать конфиденциальность, целостность и доступность. Значительный рост рисков, связанных с проблемами безопасности и защиты частной жизни, связан не с IoT как таковым, а с тем, что цифровой мир и Интернет все плотнее вплетается в нашу жизнь. Все больше персональных и конфиденциальных данных хранятся в “облаках”, все более зависимы мы от умных полезных устройств, приложений, Интернета. IoT безусловно делает рассмотренные выше проблемы более значительными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Нам доверяют защиту информации. Актуально / Информзащита - URL: https://www.infosec.ru. – 2019.

2. Evans D. Internet of Things. Cisco, white paper. URL: https://www.cisco.eom/c/dam/en_us/about/ac9/docs/innov/IoT_IB SG_0411FINAL. – 2018.

3. Расходы на развитие российского интернета вещей урезали в 4 раза - CNews URL: https://www.cisco.eom/c/dam/en_us/about/ac79/docs/innov674

5. Риски и угрозы в Интернете вещей / Блог компании Доктор Веб / Хабр. URL: https://www.vedikh.eom/c/dam/en_us/about/ac44adetg

6. Затраты в сфере кибербезопасности в 2021 году продолжат расти. URL: https://www.ifjvfddvo.eom/c/dam/en_us/about/ac331

7. Маслова М.А. Принципы безопасности интернета вещей // Вестник УрФО. Безопасность в информационной сфере. 2018. No 3 (29). С. 38-42.

8. Наумов Р.К., Железнов Н.Э. Сравнительный анализ форматов хранения текстовых данных для дальнейшей обработки методами машинного обучения // Научный результат. Информационные технологии. 2021. Т. 6. No

9. Нестеренко В.Р., Маслова М.А. Использование технологии blockchain для обеспечения безопасности в распределенном интернете вещей // Научный результат. Информационные технологии. 2021. Т. 6. No 2. С. 3-8.

10. Полегенько А.М. Особенности защиты информации в Интернете вещей // International Journal of Open Information Technologies, Vol.6, No 10, 2018. С.

12 Исаев А. Р. Инновации и информационные технологии как фактор развития экономики / А. Р. Исаев // Региональная общественная организация «Центр инновационных технологий и социальной экспертизы». – 2019. – № 2 (19). – 19 с.

13 Магомедов И. А. IIOT: Бизнес будущего / И. А. Магомедов // Известия Чеченского государственного университета. – 2019. – № 1 (13). – С. 24–28.

14. Магомадов В. С. Взгляд на четвертую индустриальную революцию / В. С. Магомадов // Сборник материалов международной научно-практической конференции «Новая промышленная революция в зеркале современной науки». – 2018. – С. 86–87.

15. Игнатович Д. Промышленный интернет вещей: рассказываем об успешных кейсах [Электронный ресурс] / Д. Игнатович // Хабр. – 2019. – URL: https://habr.com/ru/company/kauri_iot/blog/471588/ (Дата обращения: 16.05.2020).

16. Кранц М. Интернет вещей: новая технологическая революция / Кранц М. – Москва: Эксмо, 2019. – 113 с.

17. Халиев М. С-У. Прогресс в развитии информационных технологий / М. С-У. Халиев, С-Х. С-Э. Тадаев // Сборник научных статей по итогам работы второго международного круглого стола «Современная мировая экономика: проблемы и перспективы развития цифровых технологий и биотехнологии». – 2019. – С. 107–108.

18. Исмаилов И. И. Киберпреступность как угроза 21 века / И. И. Исмаилов, И. М. Даудов // Сборник материалов 6-й Международной научно-практической конференции «Развитие правого сознания в образовательном пространстве». – 2019. – С. 113–118.

19. Гузуева Э. Р. Применение информационных технологий в предприятиях крупного и малого бизнеса / Э. Р. Гузуева // Сборник материалов IV Международной заочной научно-практической конференции. – 2018. – С. 226–230.

20. Верещагина, Елена Александровна Капецкий, Игорь Олегович Ярмонов, Антон Сергеевич Проблемы безопасности Интернета вещей. Учебное пособие – М.: Мир науки, 2021. – Сетевое издание.

21. Определение политики в области исследований и инноваций, использующей сочетание облачных вычислений и Интернета вещей : Заключительный отчет / Агуцци С. [и др.]. Европейская комиссия, 2021. 95 с. doi: 10.2759/38400.

22. Кавис М. Осмысление данных Интернета вещей с помощью технологий машинного обучения // Forbes: [сайт]. 2018. 04 сентября. URL: https://www.Forbes.com/sites/mikekavis/2014/09/04/making-sense-of-ion-data - с-технологиями-машинного-обучения/?so=83eb3605ee14 (дата обращения: 20.06.2021).

23. Райес А., Салам С. Вещи в IoT: датчики и исполнительные механизмы // Интернет вещей: от шумихи к реальности. Cham : Springer, 2020. С. 57-77. https://doi.org/10.1007/978-3-319-44860-2_3 .

24. Сингх Д., Трипати Г., Джара А.Дж. Обзор Интернета вещей: видение будущего, архитектура, вызовы и сервисы // Всемирный форум IEEE по Интернету вещей 2018 (WF-IoT). IEEE, 2019. P. 287-292. doi: 10.1109/WF-IoT.2014.6803174.

25. Интернет вещей – от исследований и инноваций до выхода на рынок / О. Вермесан, П. Фрисс (ред.). Ольборг, Дания: River Publishers, 2018 373 с. (серия River Publishers in Communications). URL: https://www.river publishers.com/pdf/ebook/RP_E9788793102958.pdf (дата обращения: 20.06.2021).

Отчет о проверке на заимствования №1

Автор: Ковшиков Дмитрий Сергеевич
Проверяющий: Ковшиков Дмитрий

Отчет предоставлен сервисом «Антиплагиат» - http://users.antiplagiat.ru

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 1
Начало загрузки: 22.05.2023 10:32:02
Длительность загрузки: 00:00:01
Имя исходного файла: Курсовая работа Ковшиков.pdf
Название документа: Курсовая работа ковшиков
Размер текста: 43 кБ
Тип документа: Курсовая работа
Символов в тексте: 43737
Слов в тексте: 5046
Число предложений: 363

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Начало проверки: 22.05.2023 10:32:04
Длительность проверки: 00:00:01
Корректировка от 14.06.2023 12:13:22
Комментарии: [Автосохраненная версия]
Модули поиска: Интернет Free

СОВПАДЕНИЯ	САМОЦИТИРОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
16,62%	0%	0%	83,38%

Совпадения — фрагменты проверяемого текста, полностью или частично сходные с найденными источниками, за исключением фрагментов, которые система отнесла к цитированию или самоцитированию. Показатель «Совпадения» – это доля фрагментов проверяемого текста, отнесенных к совпадениям, в общем объеме текста.

Самоцитирования — фрагменты проверяемого текста, совпадающие или почти совпадающие с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа. Показатель «Самоцитирования» – это доля фрагментов текста, отнесенных к самоцитированию, в общем объеме текста.

Цитирования — фрагменты проверяемого текста, которые не являются авторскими, но которые система отнесла к корректно оформленным. К цитированиям относятся также шаблонные фразы; библиография; фрагменты текста, найденные модулем поиска «СПС Гарант: нормативно-правовая документация». Показатель «Цитирования» – это доля фрагментов проверяемого текста, отнесенных к цитированию, в общем объеме текста.

Текстовое пересечение — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.

Источник — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.

Оригинальный текст — фрагменты проверяемого текста, не обнаруженные ни в одном источнике и не отмеченные ни одним из модулей поиска. Показатель «Оригинальность» – это доля фрагментов проверяемого текста, отнесенных к оригинальному тексту, в общем объеме текста.

«Совпадения», «Цитирования», «Самоцитирования», «Оригинальность» являются отдельными показателями, отображаются в процентах и в сумме дают 100%, что соответствует полному тексту проверяемого документа.