DOI: 10.46548/CIT-2021-0034-0007

Л.Г. Когельман

УГРОЗЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Россия, г. Пенза, Пензенский государственный технологический университет

The Internet of Things (IoT) is used to provide communication with numerous devices. It is a system in which objects embedded in various devices interact with another object through a wireless communication medium to exchange and transmit information without human interaction. These devices are vulnerable to vulnerability attacks due to the simple and open nature of such networks. Therefore, security is the biggest problem in this technology. Attention to IoT security threats is crucial to promote the development of the Internet of Things. The purpose of the paper is to outline the various security problems faced by the Internet of Things environment and the existing mechanisms used to protect it. The article focuses on the security features of the Internet of Things, such as security requirements, as well as solutions that need to be applied to avoid these security threats.

ВВЕДЕНИЕ Интернет вещей (IoT) играет важную роль в повседневной жизни каждого человека. Он позволяет передавать данные от человека к объекту, от объекта к объекту или от объекта к объектам. Приложения интернета вещей используются во многих областях, таких как мониторинг окружающей среды, домашняя автоматизация, транспорт, медицинские системы, системы здравоохранения и т.д. Эволюция интернета вещей - одно из важнейших событий предыдущего периода времени. Такие технологии, как беспроводные сенсорные сети (БСС) и RFID-метки, ускоренно развиваются при увеличении масштабов развития интернет-технологий [1]. Появилось огромное количество возможных атак и угроз безопасности IoT. Эти угрозы еще не широко известны, и без надлежащей защиты устройств интернета вещей с большей вероятностью они будут использованы в атаках, преследующих вредоносные цели [2]. Поэтому важно понимать угрозы, вызовы и решения для безопасности IoT.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ

a. Потенциальные злоумышленники и их мотивы.

Системы, основанные на IoT, управляют большим объемом информации, которую можно использовать для различных сервисов, что делает парадигму интернета вещей интересной мишенью для множества злоумышленников, таких как случайные хакеры, хактивисты, киберпреступники и т.д. Потенциальные злоумышленники могут быть заинтересованы в краже конфиденциальной информации, такой как данные о местоположении, номера кредитных карт, пароли финансовых счетов и т.д. путем взлома устройств интернета вещей. Кроме того, они могут даже попытаться скомпрометировать компоненты интернета вещей, такие как пограничные узлы, чтобы начать атаки на организацию. Более того, технологии и машины быстро развиваются, что приводит к угрозам и проблемам конфиденциальности. Интеллектуальные устройства взаимодействуют и обмениваются данными друг с другом в сети. Если какое-либо устройство будет повреждено, вся инфраструктура окажется под угрозой. Таким образом, безопасность в последние годы имеют большое значение [1]. И необходимо установить некоторые требования к безопасности, потому что, например, в случае взлома промышленного устройства на карту может быть поставлено производство вместе с важнейшими данными.

b. Определение безопасности в сфере интернета вещей.

В таблице 1 обобщены требования к безопасности. Ключевое различие между

защитой и атакой на безопасность заключается в том, что защита - это то, что отвечает всем требованиям безопасности, в то время как атака на безопасность - это атака, которая, как правило, угрожает, по крайней мере, одному из требований безопасности [1].

Таблица 1. Требования к безопасности

Требования	Определение	Сокращение
Конфиденциальность	Обеспечение доступа к информации только авторизованным пользователям	C
Целостность	Обеспечение полноты, точности и отсутствие несанкционированного манипулирования данными	I
Доступность	Обеспечение доступности всех системных служб по запросу авторизованного пользователя	A
Подотчетность	Способность системы привлекать пользователей к ответственности за их действия	AC
Проверяемость	Способность системы осуществлять постоянный мониторинг всех действий	AU
Надежность	Способность системы проверять личность и устанавливать доверие к третьей стороне	TW
Неотрицание	Способность системы подтверждать возникновение/ отказа от совершения действия	NR
Приватность	Обеспечение соблюдения системой политики конфиденциальности и предоставление отдельным лицам возможности контролировать свою личную информацию	P

А. Определение конфиденциальности в рамках Интернета вещей.

В связи со значительным увеличением использования и эффективности электронной обработки данных, в наши дни конфиденциальность информации стала ключевой проблемой. Конфиденциальность в сфере интернета вещей можно разделить на три категории:

- осведомленность о рисках конфиденциальности, связанных с интеллектуальными вещами и услугами, окружающими субъекта данных,
- индивидуальный контроль за сбором и обработкой личной информации окружающими интеллектуальными вещами,
- осведомленность и контроль за последующим использованием и распространением личной информации этими субъектами любому субъекту за пределами сферы личного контроля субъекта [2].

В сценарии "умный дом" домашнее хозяйство субъекта может быть описано как личная сфера субъекта и могут отличаться в зависимости от ситуации. Конфиденциальность, как правило, различается по восприятию и требованиям в зависимости от конкретного человека, что приводит к неясному пониманию личной информации. Поэтому при разработке новых систем и услуг необходимо учитывать тщательную оценку чувствительности соответствующей информации и соответствующих требований пользователей.

УГРОЗЫ БЕЗОПАСНОСТИ

А. Беспроводная сенсорная сеть (БСС):

БСС легко подвержены атакам на безопасность интернета вещей из среды передачи информации, используемой для вещания. Некоторыми из основных угроз БСС

являются:

1. Физические атаки: Сенсорное устройство должно быть реализовано в каждом объекте для достижения их полной работоспособности. Однако трудно физически защитить устройства, а также остановить несанкционированный физический доступ. Хакер может вносить изменения в доступные данные узла/датчика, тем самым подвергая риску функционирование всей сенсорной сети [3,4].

2. Репликация узла: В этой атаке существующий идентификатор узла датчика копируется в ту же сеть, что и новый датчик, что приведет к дублированию, вызывающему неправильную маршрутизацию пакетов, запись ложных показаний датчика или отключение сети, тем самым нарушая производительность сенсорной сети [5].

3. Выборочная пересылка: В БСС предполагается, что все узлы получают сообщения в пункт назначения. Вредоносный узел выборочно пересылает пакеты в этой атаке. Он может просто отбросить определенные сообщения, не пересылая их. Трудно идентифицировать злоумышленника, так как он, как правило, изменяет пакеты, исходящие от нескольких определенных узлов, и затем сообщение пересылается на другие узлы, тем самым ограничивая подозрения в модификациях вредоносного узла [5] [2].

4. Атака «червоточина». Это критическая атака, при которой злоумышленник записывает пакеты в определенном месте сети, а затем туннелирует их в другое место. Этот процесс может осуществляться выборочно. Более того, при туннелировании стандарт маршрутизации управляющих сообщений может быть нарушен [2].

5. Атака Сибиллы. Эта атака была введена в контексте одноранговых сетей. Это происходит, когда компьютер захвачен, и хакер утверждает, что у него несколько удостоверений личности, и противник может находиться более чем в одном месте одновременно.

Один узел представляет несколько идентификаций в сети, что приводит к значительному снижению эффективности отказоустойчивости, такой как распределенное хранилище, неравномерность и многолучевость [5].

6. Атака «Воронка». Злоумышленник захватывает узел внутри сети и пытается привлечь весь трафик с соседних узлов. Этот процесс может быть осуществлен с использованием алгоритма маршрутизации и привлечением других узлов. Противник запускает множество серьезных атак, включая выборочную пересылку пакетов, модификацию сообщений или удаление пакетов [5] [2].

7. Атака «Отказ в обслуживании». Сервисы становятся недоступными для законных пользователей, а их запросы уничтожаются путем заполнения их запросами от злоумышленника, что приводит к отказу во всех услугах, отправленных законными пользователями [2].

8. Подслушивание: Злоумышленник прослушивает информацию во время передачи данных между двумя узлами по сети. Информация остается прежней, но ее конфиденциальность нарушена. Злоумышленник может использовать эту информацию против пользователя [5] [2].

B. Радиочастотная идентификация (RFID):

Некоторые типы атак на технологию RFID заключаются в следующем:

1. Изменение физических данных: Злоумышленник физически получает теги, а затем данные изменяются. Индукция неисправности используется для изменения физических данных. Индукция сбоя - это процесс изменения данных при их записи или обработке, который может быть выполнен с использованием микроскопов для лазерной резки или небольшой заряженной иглы, приводящий к несоответствию между данными, хранящимися на метках, и объектами, к которым прикреплены эти метки. RFID-метка,

прикрепленная к изготовленному изделию, дает неверную информацию об изделии. Из-за этой атаки прослеживаемость тегов снижается [2].

2. Клонирование тегов: Исходный тег заменяется новым, и в него копируется исходный идентификатор тега (id). Если для RFID-меток нет физической защиты доступа, то злоумышленник может легко заменить исходную метку новой [5].

3. Замена тегов: Популярная атака, при которой заменяются теги двух разных продуктов. Это происходит в розничных магазинах, где ценник с высокой ценой обменивается на ценник с низкой ценой, так что дорогостоящий товар приобретается по более низкой цене. [5] [2].

4. Атака на отказ в обслуживании: Когда считыватель RFID запрашивает информацию у метки, он получает идентификационный идентификатор метки, а затем сравнивает его с идентификатором, хранящимся в его базе данных. Как считыватель RFID, так и база данных сервера уязвимы для DoS-атаки, в результате, когда эта атака происходит, метка не может отправить свою идентификацию считывателю. Таким образом, соединение между тегом и считывателем не будет стабильным и, в свою очередь, приведет к прерыванию обслуживания исследования. [5.

РЕШЕНИЯ ДЛЯ УГРОЗ БЕЗОПАСНОСТИ

А. Решения по обеспечению безопасности для беспроводных сенсорных сетей (БСС) Некоторые из решений, касающихся беспроводных сенсорных сетей, заключаются в следующем:

1. Общие ключи. Функция безопасности, которая, как правило, имеет огромное значение в БСС, является управление ключами. Оказалось, что БСС уникальны по этой характеристике из-за их размера, мобильности и ограничений мощности. Традиционно использование одного из многих протоколов с открытым ключом приводит к созданию ключа. Обычно, применение простой ключевой инфраструктуры для любой сети обеспечивает защиту от атак извне. Однако известно, что глобальный ключ не обеспечивает никакой устойчивости сети, а попарные ключи не являются масштабируемым решением [13].

2. Защищенная группировка. БСС состоит из большого количества небольших узлов, которые являются компактными и автоматизированными устройствами. Узлы датчиков необходимы для соединения узлов вместе. Для выполнения конкретной задачи важно, чтобы члены группы могли безопасно общаться друг с другом, даже несмотря на то, что может также использоваться общая безопасность. Исключения для решений делаются, когда более мощные узлы отвечают за защиту члена статических групп [19].

3. Шифрование. Сенсорные сети в основном работают в общественных или неопределенных зонах по изначально ненадежным беспроводным каналам. Таким образом, для устройства несущественно подслушивать или даже добавлять сообщения в сеть. Традиционным способом решения этой проблемы является применение таких методов, как коды аутентификации сообщений, схемы шифрования с симметричным ключом и криптография с открытым ключом [13].

4. Безопасное объединение данных. Сенсорные сети и методы объединения данных, как правило, уязвимы для целого ряда атак, включая атаки типа "отказ в обслуживании". Наиболее важной проблемой в сетях является большой трафик данных, который возникает из-за увеличения объема передачи данных. Чтобы снизить накладные расходы и сетевой трафик, сенсорные узлы объединяют измерения перед отправкой их на базовую станцию. Этот тип данных привлекает злоумышленника [21. Достоверность сгенерированных данных будет снижена, если злоумышленник получит контроль над узлом агрегирования и решит игнорировать отчет или создаст ложный отчет. В результате необходимо учитывать сеть в целом. Основной целью в этой области является использование устойчивых функций, которые должны быть способны

обнаруживать и сообщать о поддельных отчетах, каким-либо образом демонстрируя подлинность данных. Однако все еще может потребоваться усовершенствование в этой области, например, объем данных, который генерируется интерактивным алгоритмом [21] [19].

5. SPINS. Протоколы безопасности для сенсорных сетей: SPINS оптимизированы для сред с ограниченными ресурсами и беспроводной связи. У SPINS есть несколько основных блоков, благодаря которым он предлагает множество свойств безопасности, таких как аутентификация данных, свежесть данных, семантическая безопасность, низкие затраты на связь и защита от воспроизведения [22].

6. TinySec. Архитектура безопасности на канальном уровне: TinySec может быть включен в приложения сенсорной сети, поскольку они небольшие и имеют общий пакет безопасности, и поэтому он включен в официальный выпуск TinyOS. Двумя специальными параметрами безопасности, которые поддерживает tinysec, являются аутентифицированное шифрование (tinysecae) и только аутентификация (tinysecauth). С помощью аутентифицированного шифрования TinySec шифрует полезную нагрузку данных и аутентифицирует пакет с помощью MAC. В режиме только аутентификации TinySec аутентифицирует весь пакет с помощью MAC, но полезная нагрузка данных не зашифрована [12].

B. Решения по обеспечению безопасности для радиочастотной идентификации (RFID).

Физический метод.

1) «Убийство» меток. Принцип, используемый для этого метода, заключается в отключении функции тега, чтобы прекратить отслеживание тега и его носителя, это то, что обычно делается в супермаркете. Преимущество команды "убить" заключается в потере тегов. Например, информация о теге будет бесполезна после продажи товара. Это не удобно для послепродажного обслуживания и дальнейшего понимания продукта. Более того, если идентификационный номер убийства (PIN-код) будет раскрыт, человек с дурными намерениями может совершить кражу из супермаркета [11].

2) Сеть Фарадея. Согласно теории электромагнитного поля, контейнер, изготовленный из проводящего материала сети Фарадея, не дает проникнуть в сеть Фарадея внешним радиоволнам и наоборот. Размещение метки в контейнере, изготовленном из проводящего материала, скорее всего, предотвращает сканирование метки, т. е. пассивная метка не может принимать сигнал, а инициативная метка не может посылать сигнал. Таким образом, использование принципа сети Фарадея может помешать нарушителю конфиденциальности сканировать информацию тега. Например, если монета вставлена в RFID-метку, используя принцип сети Фарадея, можно предотвратить сканирование ее нарушителем конфиденциальности [11].

3) Останавливающая метка. Принцип, лежащий в основе использования специального остановочного тега, заключается в том, чтобы вмешиваться в алгоритм предотвращения столкновений, что означает, что корреспонденту отправляются одни и те же данные ответа, чтобы тег был защищен [9].

Протокол безопасности RFID.

Механизм безопасности с использованием программного обеспечения, основанный на технике секретного кода, удобнее пользователям, чем механизмы аппаратной безопасности, основанные на физических методах. Хотя в последнее время было предложено множество протоколов безопасности RFID, большинство из них имеют различные недостатки.

В 2003 году Вайда и др. предложили упрощенный протокол аутентификации по тегам. Это сбалансированное решение, которое учитывает и производительность, и

безопасность. Злоумышленник может быть в состоянии раскрыть протокол, если он владеет значительными вычислительными ресурсами [12].

Sarma и др. предложили протокол блокировки хэша, который использует metaID для замены реального идентификатора тега, чтобы информация не отслеживалась и не просачивалась. Однако механизм динамического обновления идентификатора отсутствует. MetaID сохраняется неизменным, и в него не вносится никаких изменений. Более того, идентификатор отправляется обычным текстом по небезопасному каналу. Таким образом, наиболее вероятно, что протокол может быть атакован поддельным именем или ретранслирован [12].

Вайс и др. предложили протокол случайной блокировки хэша, который использует механизм запроса-ответа, основанный на случайных числах. Идентификатор тега, прошедший проверку подлинности, отправляется обычным текстом по небезопасному каналу. Таким образом, протокол также может быть атакован под вымышленным именем или повторно передан и отслежен. Поскольку объем данных, передаваемых между тегом и считывателем, велик, перспектива применения не так велика [12].

Предложен протокол LCAP, который также является протоколом типа запрос-ответ. Идентификатор тега динамически обновляется после каждой операции. Для протокола требуется только два дискретных вычисления. Сложность алгоритма снижается, поскольку он делит идентификатор на две части, т. е. левую и правую. Поскольку он состоит только из идентификатора метки и однонаправленной хэш-функции, он очень хорошо отвечает требованиям RFID-системы. Поскольку идентификатор тега отправляется только в том случае, если он проходит аутентификацию и обновляется после каждой операции, протокол LCAP может эффективно предотвращать отслеживание и утечку информации. Идентификатор тега обновляется после получения сообщения об обновлении идентификатора и сообщения, прошедшего аутентификацию, по окончании каждого разговора. К этому времени справочная база данных уже обновила соответствующий идентификатор. Хотя протокол LCAP является удовлетворительным протоколом аутентификации для недорогой RFID-системы, он не подходит для общей вычислительной среды распределенной базы данных, поскольку синхронизация базы данных представляет потенциальную скрытую угрозу безопасности [12].

Таблица 2. Угрозы и решения безопасности БСС

Угрозы	Решения
Физическая атака и обратное проектирование	Механизм, устойчивый к несанкционированному доступу
Проблема целостности данных	Обнаруживает угрозы безопасности в целостности данных, затем приспосабливается к среде с обнаруженными цензурированными изменениями при использовании показателей безопасности
Атака Сивиллы	Продолжение отслеживания количества клонов
Атака «Воронка»	Расшивание заторов
Вредоносный узел	Путем обнаружения вредоносного узла и распространения отдельно в черном списке
DDOS-атака	Механизм маркировки, фильтрации и отбрасывания пакетов
Атака на доступность сети	Безопасная маршрутизация
Подслушивание	Защищенная ретрансляционная связь
Атака криптоанализа	Улучшенная двусторонняя схема аутентификации

	пользователей

Таблица 3. Угрозы и решения безопасности RFID

Угрозы	Решения
Подделка	Клетка Фарадея
Клонирование тегов	Аутентификация идентификатора тега, действительный идентификатор используется для клонирования тега
Подделка	Протокол двусторонней аутентификации
Теги отслеживания	Сверхлегкий протокол взаимной аутентификации
«Убийство» меток	При «убийстве» теги, они не используются повторно

УГРОЗЫ КОНФИДЕНЦИАЛЬНОСТИ

A. Идентификация. Идентификация означает угрозу соединения идентификатора, такого как адрес и имя или псевдоним любого типа, с физическим лицом и информацией о нем. Угроза заключается в подключении личности к определенной конфиденциальности, нарушающей контекст, а также активирует и облегчает другие угрозы. Например, профилирование и отслеживание отдельных лиц или сбор различных источников данных. Угроза идентификации в настоящее время наиболее распространена на этапе обработки информации в серверных службах, где огромные объемы данных собираются в центральном месте вне контроля субъекта. Основной проблемой, с которой приходится сталкиваться при идентификации, является разработка систем интернета вещей, которые предпочитают локальную обработку централизованной, горизонтальное взаимодействие вертикальному, чтобы минимальный объем идентифицирующих данных был доступен за пределами личной сферы пользователя [4].

B. Локализация и отслеживание. Локализация и отслеживание обозначают угрозу определения и документирования местоположения человека во времени и пространстве. Отслеживание требует идентификации для привязки непрерывных локализаций к одному человеку [10]. В настоящее время отслеживание возможно с помощью различных средств, таких как интернет-трафик, GPS или местоположение мобильного телефона. Большинство конкретных нарушений конфиденциальности были выявлены в связи с этой угрозой, например, слежка по GPS, раскрытие личной информации или, как правило, ощущение преследования. В непосредственной физической близости локализация и отслеживание обычно не приводят к нарушениям конфиденциальности, например, любой человек, находящийся в непосредственной близости, может непосредственно наблюдать за местоположением объекта. Таким образом, локализация и отслеживание представляют угрозу главным образом на этапе обработки информации, когда трассировки местоположений строятся вне контроля субъекта. Основными проблемами, с которыми сталкиваются при локализации и отслеживании, являются осведомленность об отслеживании в условиях пассивной концентрации информации, контроль общих данных о местоположении в помещениях и протоколы сохранения конфиденциальности для связи с системами интернета вещей.

C. Профилирование. Профилирование означает угрозу сбора или систематизации информационных досье о физических лицах с целью выявления интересов путем сопоставления с другими профилями и данными. Методы профилирования в основном используются для персонализации в электронной коммерции (рекомендательные системы, информационные бюллетени и рекламные объявления), а также для внутренней оптимизации на основе демографических данных и интересов клиентов [9]. Примерами, когда профилирование приводит к нарушению конфиденциальности,

являются ценовая дискриминация, нежелательная реклама, социальная инженерия или ошибочные автоматические решения, например с помощью Facebook автоматическое обнаружение сексуальных преступников. Сбор и продажа профилей о людях обычно воспринимается как нарушение конфиденциальности. Эти примеры показывают, что угроза профилирования возникает главным образом на этапе распространения, в отношении третьих сторон, но также и в отношении самого субъекта в форме ошибочных или дискриминационных решений. Эти подходы, возможно, могут быть применены к сценариям Интернета вещей, но их следует адаптировать к обычной модели, которая предполагает центральную базу данных и учитывает множество распределенных источников данных, которые ожидаются в IoT. Это требует значительных усилий для повторной калибровки показателей и перепроектирования алгоритмов, как, например, показывает недавняя работа в области дифференциальной конфиденциальности для распределенных источников данных. Сбор данных является одной из основных функций Интернета вещей и основным драйвером его реализации. Таким образом, это рассматривается как самая большая проблема в обеспечении баланса интересов бизнеса в области профилирования и анализа данных с требованиями конфиденциальности отдельных лиц.

D. Нарушение конфиденциальности взаимодействия и презентации. В этой угрозе личные данные передаются через общедоступный канал, а затем раскрываются нежелательным лицам. Многочисленные приложения интернета вещей, такие как производство, инфраструктура, медицинские системы и системы здравоохранения и т.д., нуждаются в многочисленных соединениях внутри пользователя. В этих системах возможно, что детали предоставляются пользователям с помощью использования умных вещей в окружающей среде. Например, с помощью приближающихся методов освещения и телевизионных или настольных экранов, показывающих видео. И наоборот, пользователи доминируют в системах в альтернативной инстинктивной методологии с использованием интеллектуальных вещей в окружающей среде (таких как ощущение и передача интеллектуальных объектов). Тем не менее, многочисленные связи и организационные процедуры по своей сути являются публичными. Таким образом, это создает проблемы с конфиденциальностью при обмене секретной информацией между пользователем и системой. Например, в умных городах человек может задать вопрос о маршруте в конкретную больницу. На такой запрос не следует отвечать (например, отображение маршрута на дороге общего пользования может быть замечено любым, кто проезжает по той же дороге) [4].

E. Переходы жизненного цикла. Конфиденциальность нарушается, когда интеллектуальные объекты раскрывают свои секретные данные на протяжении всего процесса изменения управления доменами в их жизненном цикле. Эта проблема замечена в отношении изображений и видео, которые обычно видны на камерах и других новых устройствах. Поскольку нарушения конфиденциальности в жизненном цикле в первую очередь обусловлены собранной информацией, это зависит от уровня информации эталонной модели интернета вещей. Жизненный цикл многих продуктов для обслуживания клиентов даже сейчас рассчитан на то, чтобы постоянно покупать продукт. Интеллектуальные объекты могут создавать атрибуты для более увлекательного жизненного цикла, который будет включать обмен, кредитование, предоставление и бесценное распоряжение. Поэтому мы признаем необходимость в адаптируемых результатах, которые, несомненно, создадут некоторые проблемы. Некоторые преобразования жизненного цикла (например, совместное использование смарт-объекта требует закрепления секретных деталей на временной стадии). Секретные детали могут быть раскрыты, и фактический владелец может продолжать последовательно использовать устройство [4].

F. Атака на инвентаризацию. Это определяется как несертифицированный сбор данных о реальности и функциях персональных устройств. Взаимосвязь устройств интернета вещей рассматривается как одна из важных развивающихся функций интернета вещей. Интеллектуальные объекты считаются доступными для запроса через Интернет с идентификацией всех интернет-протоколов. Уполномоченные организации могут запрашивать информацию отовсюду (например, у сертифицированных пользователей и владельцев системы), в то время как неавторизованные организации могут запрашивать и нарушать это, чтобы организовать подробную запись вещей в определенной области (например, офисное здание, общественные учреждения, промышленная зона и т. д.). Несмотря на то, что интеллектуальные объекты могут легко определять авторизованные и неавторизованные организации, для определения их категории и представления можно использовать отпечатки скорости передачи данных этих организаций и другие редкие спецификации. С ожидаемой эскалацией технологии БСС процедуры снятия отпечатков также могут быть продемонстрированы (например, тайный слушатель в месте проживания жертвы) [4].

Для предотвращения атак на инвентаризацию в IoT мы выделяем две специализированные проблемы: прежде всего, интеллектуальный объект должен иметь возможность проверять запросы и отвечать на эти запросы уполномоченными организациями, чтобы предотвращать атаки на гибкую инвентаризацию. Во-вторых, методологии, которые защищают здоровье от снятия отпечатков пальцев, будут запрошены для защиты и предотвращения пассивных атак на инвентаризацию, основанных на передаче отпечатков пальцев смарт-объекта [10].

G. Связь. В этой угрозе ранее отдельные системные устройства соединяются вместе (например, раскрывается сбор информации, относящейся к различным данным, которые никогда не раскрывались ранее неизвестным источникам). Пользователи не знают о превосходной оценке и потере данных, когда все различные данные и разрешения собраны вместе. Другим примером нарушения конфиденциальности с помощью связи является быстрое расширение предоставленных неизвестных данных [4]. Угрозы связи будут усугубляться в процессе эволюции интернета вещей в первую очередь по двум причинам. Во-первых, параллельное соединение соединит системы разных организаций для создания диверсифицированной системы, предоставляющей новые услуги, которые ни одна система никогда не предоставляла самостоятельно. Во-вторых, постоянная взаимосвязь такой вещи постепенно потребует гибкого обмена информацией и обслуживания между различными людьми.

РЕШЕНИЯ ДЛЯ СОХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ.

Было предложено несколько подходов для решения проблем конфиденциальности и соображений конфиденциальности поставщиков услуг.

A. Криптографические методы и манипулирование информацией.

Криптография по-прежнему является наиболее доминирующей. Практически все предлагаемые решения не могут предложить адекватных протоколов безопасности из-за ограниченного объема хранилища и вычислительных ресурсов [6].

B. Осведомленность о конфиденциальности или осведомленность о контексте.

Решения для повышения осведомленности о конфиденциальности были в основном ориентированы на приложения отдельных лиц, которые предоставляют своим пользователям базовую информацию о конфиденциальности, чтобы интеллектуальные устройства, такие как носимые фитнес-устройства, смарт-телевизоры и системы мониторинга состояния здоровья, могли собирать персональные данные о них. Например, в исследовании было предложено, чтобы платформа под названием SeCoMan вела себя как доверенная третья сторона для пользователей, поскольку приложениям может быть недостаточно доверена информация о местоположении [7].

C. Контроль доступа. Контроль доступа является одним из эффективных решений, используемых в сочетании с шифрованием и информированием о конфиденциальности. Это дает пользователям возможность управлять своими собственными данными. Примером такого подхода является CapBAC [9], предложенный Скарметой, Эрнандесом и Морено. По сути, это распределенный подход, при котором умным вещам самим разрешается принимать решения об авторизации.

D. Минимизация данных. Принцип минимизации данных означает, что поставщики услуг Интернета вещей должны ограничить или уменьшить концентрацию персональных данных до того, что имеет непосредственное отношение. Они также должны хранить данные только до тех пор, пока это необходимо для выполнения целей услуг, предоставляемых технологией. Существуют и другие предлагаемые решения, которые не подпадают под предыдущие четыре категории, такие как автостоп. Это новый подход к обеспечению анонимности пользователей, которые предоставляют свои местоположения. Приложения для автостопа обрабатывают интересующее местоположение [10].

ЗАКЛЮЧЕНИЕ И ПРЕДЛАГАЕМОЕ РЕШЕНИЕ.

IoT - это новая технология, которая добилась значительного прогресса в стандартизации технологий. Интернет вещей дает огромные преимущества в бизнесе, академическом секторе, а также для самих людей. Информация в IoT передается с RFID-меток или датчиков, которые содержат конфиденциальную информацию, защищенную от любого несанкционированного доступа [6]. Следовательно, безопасность и конфиденциальность очень важны для защиты систем интернета вещей. В этой работе рассматриваются основные угрозы и их соответствующие решения в IoT путем определения различных областей, чувствительных к атакам на безопасность. Современные проблемы следует рассматривать как расширяющуюся возможность, которая включает в себя намерения по обеспечению безопасности на ранней стадии разработки и успешное применение регламентированных мер безопасности на этапе производства. В качестве будущей перспективы защиты интернета вещей могут быть разработаны более совершенные системы безопасности, которые смогут решать проблемы конфиденциальности во всех областях. Необходимы дальнейшие исследования для разработки и проектирования соответствующих механизмов безопасности, устойчивых к различным типам атак. Поэтому пользователи, организации и разработчики должны объединиться и найти выдающееся решение для защищенной среды интернета вещей.

Тем не менее, манипулирования данными пользователя можно полностью избежать, если пользователь только делится необходимой информацией в нужное время и удаляет остальную часть своей информации, тем самым ускоряя процесс, повышая его эффективность и защищая его от угроз конфиденциальности, обсуждаемых в статье.

1. Mosenia and N.K. Jha, (2016, September). “A comprehensive study of Internet of Things.” In Emerging Topics in Computing. pp. 586-602. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/7562568 (Дата обращения: 05.10.2021).

2. Md. Husamuddin and M. Qayyu. “Internet of Things: A study on Security and Privacy Threats.” In Second International Conference on Anti-Cyber Crimes (ICACC), 2017. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/7905270 (Дата обращения: 12.09.2021).

3. J. H. Ziegeldoorf, O.G. Morcon, and K. Wehrle, (2017, May). “Privacy in the Internet of Things: Threats and challenges.” In *Journal of Computing and Machinery.* 7(1), pp. 110-119. [Электронный ресурс] // Режим доступа: https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf (Дата обращения: 15.08.2021).

4. Когельман Л.Г. Безопасность и атаки в беспроводных сенсорных сетях/ Труды международного симпозиума «Надежность и качество» - Пенза, ПГУ, 2019, Том: 1, с. 90-92.

5. K. Raju and V. Bapauji. “Internet of Things (IoT): Security and privacy threats.” In IEEE International Conference Robot Autom, 2016. [Электронный ресурс] // Режим доступа: https://www.researchgate.net/publication/305302451 (Дата обращения: 22.09.2021).

6. H. Feng and W. Fu. “Study of recent development about privacy and security of the Internet of Things.’ In IEEE International Conference on Web Information Systems and Mining, 2, pp. 91-95, 2010. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/5662804/ (Дата обращения: 25.10.2021).

7. A. H. Celdran, F. J. G. Clemente, M. G. Perez and G. M. Perez. “SeCoMan: A semantic-aware policy framework for developing privacy- preserving and context-aware smart applications.” In IEEE Systems Journal, 10(3), pp. 1111-1124, 2016 [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/6718051 (Дата обращения: 27.10.2021).

8. A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno. “A decentralized approach for security and privacy challenges in the internet of things.” In IEEE World Forum on Internet of Things (WF-IoT), pp. 67-72. IEEE, 2014. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/6803122 (Дата обращения: 23.06.2021).

9. M. Daud, Q. Khan, and Y. Saleem. “A study of key technologies for IoT and associated security challengers.” In International Symposium on Wireless Systems and Networks, 2017. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/8250042 (Дата обращения: 27.10.2021).

10. N. Aleisa and K. Renaud, “Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion),” unpublished. [Электронный ресурс] // Режим доступа: https://arxiv.org/ftp/arxiv/papers/1611/1611.03340.pdf (Дата обращения: 05.10.2021).

11. Khattab, Z. Jeddi, E. Amini,. And M. Bayoumi. “RFID Security Threats and Basic Solutions.” In *RFID Security: A lightweight paradigm.* Switxerland: Analog Circuits and Signal Processing, 2017, ch. 2, pp. 2741. [Электронный ресурс] // Режим доступа: https://link.springer.com/chapter/10.1007/978-3- 319-47545-5_2 (Дата обращения: 25.10.2021).

12. Q. Wang, X. Xiong, W. Tian and L. He. “Low-cost RFID: Security problems and solutions.” In the International Conference on Management and Service Science, 2011. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/5998331 (Дата обращения: 25.10.2021).

13. Jain, K. Kant and M. R. Tripathy. “Security solutions for Wireless Sensor Networks.” In Second International Conference on Advanced Computing & Communication Technologies, 2012, pp. 430-433. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/6168407 (Дата обращения: 14.07.2021).

14. M. Dabbagh and A. Rayes. “Internet of Things security and privacy” in Internet of Things from hype to reality. [Электронный ресурс] // Режим доступа: https://www.researchgate.net/publication/309375790 (Дата обращения: 22.10.2021).

15. Harpal, G. Tejpal and S. Sharma. “A survey article on attacks and security goals in Wireless Sensor Networks.” In Second International Conference on Communication and Electronics Systems, 2017, pp. 683-686. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/8321166 (Дата обращения: 29.10.2021).

16. Tyagi, J. Kusshwah and M. Bhalla. “Threats to security of Wireless Sensor Networks.” In Seventh International Conference on Cloud Computing, Data Science & Engineering - Confluence, 2017, pp. 402-405. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/7943183 (Дата обращения: 18.10.2021).

17. M. Frustaci, P. Pace and G. Aloi. “Securing the IOT world: issue and perspectives.” IEEE Conference on Standards for Communications and Networking CSCN), 2017, pp. 247-251. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org/document/7888545 (Дата обращения: 12.09.2021).

18. Z. Ren, X. Liu, Runguo and T. Zhang. “Security and Privacy on Internet of Things.” Seventh IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), 2017, pp. 140-144. [Электронный ресурс] // Режим доступа: https://ieeexplore.ieee.org.library.pmu.edu.sa/document/8076530 (Дата обращения: 11.10.2021).

19. W. Al Shehri. “A survey on Security in Wireless Sensor Networks.” International Journal of Network Security & Its Applications (IJNSA), 9(1), 2017, pp. 25-32. [Электронный ресурс] // Режим доступа: http://aircconline.com/ijnsa/V9N1/9117ijnsa03.pdf (Дата обращения: 04.10.2021).

20. M. Saraogi. "Security In Wireless Sensor Networks." pp. 1-12. [Электронный ресурс] // Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.5923 &rep=rep1&type=pdf (Дата обращения: 03.10.2021).

21. K. Sharma, M.K. Ghose, D. Kumar, R. P. K. Singh and V. K. Pandey. “A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks”. In International Journal of Advanced Science and Technology (IJAST), 17, 2010, pp. 31-44. [Электронный ресурс] // Режим доступа: http://modul.repo.mercubuana-yogya.ac.id/modul/files/openjournal/JoumalOfDesign/4_263.pdf (Дата обращения: 14.10.2021).

22. Md. A. Hamid, M.d. Mamun-Or-Rashid, and C. S. Hong. “Routing Security in Sensor Network: Hello Flood Attack and Defense” In IEEE ICNEWS, 2006, pp. 77-81. [Электронный ресурс] // Режим доступа: http://networking.khu.ac.kr/layouts/net/publications/data/Routing%20Security %20in%20Sensor%20Network%20HELLO%20Flood%20Attack%20and%20 Defense.pdf (Дата обращения: 11.10.2021).