Обзор и анализ стандартов и протоколов в области Интернет вещей. Современные методы тестирования и проблемы информационной безопасности IoT

Н.А. Наралиев, Д.И. Самаль

***Аннотация*— IoT – это целая экосистема, который содержит в себе интеллектуальные устройства оснащенными сенсорами (датчиками), обеспечивающие удаленное управление, хранение, передачу и безопасность данных. Интернет вещей (IoT) – представляет собой инновационные решения в различных областях таких, как здравоохранение, страхование, охрана труда, логистика, экология и т.д. Для раскрытия полного потенциала использования IoT – устройств необходимо решить множество проблем связанные со стандартами обеспечение безопасности, архитектуру построение экосистемы, каналы и протоколы подключения устройств. Сегодня в мире крупные организации, такие как NIST, IEEE, ISO/IEC и другие делает огромные усилия в решении вопросов стандартизации, безопасности и архитектуры разрабатываемых устройств.**

Анализ последних научных исследовательских работ в области решении вопросов информационной безопасности и конфиденциальности данных IoT – устройств показал положительные результаты, но, однако эти методы и подходы основаны на традиционных методах безопасности сети. Разработка и применение механизмов безопасности IoT- устройств является сложной и неоднородной задачей. В связи с этим обеспечение информационной безопасности и защиты конфиденциальных данных, а также доступность IoT - устройств является основной целью написания данной статьи.

Учитывая вышесказанное, возникает множество вопросов связанной с состоянием безопасности IoT - устройств, а именно: Какие на сегодня существуют стандарты и протоколы для IoT? Какие требования предъявляются для обеспечения информационной безопасности IoT – устройств? Какие механизмы обеспечения безопасности IoT – устройств существуют? Какие методы тестирования IoT – устройств существует?

Производители и разработчики IoT – устройств не уделяют достаточного внимания вопросам обеспечения безопасности. С развитием кибератак, векторы атак становятся все более совершенными и нацеленными на несколько элементов инфраструктуры одновременно. Инфраструктура IoT обычно включает в себя миллионы подключенных объектов и устройств, которые хранят и обмениваются конфиденциальной информацией. Сценарии кражи и мошенничества, такие как взлом и подделка личных данных, представляют собой серьезную угрозу для таких устройств IoT. Большинство IoT – устройств использует общедоступный интернет для обмена данными, что делает их уязвимыми для кибератак. Современные подходы к обеспечению информационной безопасности часто предлагают решения отдельных проблем, когда многоуровневые подходы предлагают повышенную устойчивость к кибератакам.

***Ключевые слова*— iot, cybersecurity, кибератака, интернет вещей, защита информации, беспроводные технологии, LoraWAN.**

I. Введение

В сегодняшнем мире, в котором быстрыми темпами набирают свою популярность умные устройства «Интернет вещей», выполняющие роль помочь в решении наших повседневных задач в различных областях применения. Все умные устройства, взаимосвязанные друг с другом, работают через выход в глобальную сеть – интернет. Количество подключенных датчиков и устройств Интернета вещей в мире в 2018 году составила 21 млрд., а к 2022 году превысит 50 млрд., на рисунке 1, об этом говорится в исследовании компании Juniper Research. [1].

Информационная безопасность – является одним из наиболее важных аспектов развертывания и внедрения интернет вещей в реальном мире. На сегодняшний день количество инцидентов, связанных с технологиями IoT увеличивается, что требует разработки новых стандартов и систем защиты против кибератак. Известные атаки на системы IoT такие как спуфинг, анализ и изменения трафика, манипуляция конфиденциальной информацией, инъекции кода, и несанкционированный доступ.

Статья получена 9 июля 2019. Рекомендована оргкомитетом Международной научно-практической конференции «Современные информационные технологии и ИТ-образование».

Наралиев Нишонали Анорматович, Белорусский государственный университет информатики и радиоэлектроники, аспирант, nishonali@gmail.com

Самаль Дмитрий Иванович, кандидат технических наук, доцент, Белорусский государственный университет информатики и радиоэлектроники, samal@bsuir.by.

С ростом масштабов рынка Интернет вещей, компании, выпускающие умные устройства, стремятся в быстром маркетинговом ходе выпускать как можно быстрее продукты, а на разработку адекватной защиты и безопасности устройств уделяют меньше внимание. В связи этим многие продукты сегодня не устойчивы перед различными векторами вредоносных атак, что привело к использованию злоумышленниками как платформа для организации мощнейших кибератак.

Информационная безопасность и доступность IoT – устройств является постоянно растущей проблемой на сегодняшний день, в связи с малым количеством исследований по этому направлению, и малым количеством реализованных стандартов, которые могли бы решить актуальные задачи безопасности устройств.

Рис. 1 - Рост подключенных устройств в мире, млрд.

Основные проблемы обеспечения безопасности IoT - устройств, такие как предотвращение потери контроля, доступность работы, а также нарушения информации о клиентах и данных компаний, вызывает необходимость внедрения тестирования проникновение (penetration testing) умных устройств перед выпуском на рынок.

II. Интернет вещей

Термин «Интернет вещей» сегодня несет очень много определений, например, как описывает как одна из лидеров рынка корпоративных приложений SAP, Internet of Things – это мир, в котором физические объекты органично интегрируются в информационную сеть, и где эти физические объекты могут активно участвовать в бизнес-процессах. При помощи интернета сервисы могут взаимодействовать с этими «умными объектами», изменять их состояние и запрашивать любую связанную с ними информацию, с учетом вопросов безопасности и конфиденциальности. Или International Data Corporation (IDC) — аналитическая компания, специализирующаяся на исследованиях рынка информационных технологий, дает следующее понятие [2]. Internet of Things – это сеть сетей с уникально идентифицируемыми конечными точками, которые общаются между собой в двух направлениях по протоколам TCP/IP для обмена данными через каналы глобальной сети Интернет без человеческого вмешательства [3].

Устройствами входящие в интернет вещей, — любые автономные устройства, датчики, сенсоры, подключённые к интернету, которые могут отслеживаться и/или управляться удалённо.

Экосистема интернета вещей — все компоненты, которые позволяют бизнесу, правительствам и пользователям присоединять свои устройства IoT, включая пульты управления, панели инструментов, сети, шлюзы, аналитику, хранение данных и безопасность. [4]

Рынок Интернета вещей очень перспективно развивается в сферах, таких как услуги ЖКХ, энергетика, логистика, медицина, безопасность, ритейл, банковская сфера, сельское хозяйство, промышленность.

Архитектура Internet of Things

Для понимания сложности существующих решений в области интернет вещей, необходимо наличие архитектуры, которая обеспечивает основные компоненты и их взаимосвязи. На рисунке 2 представлена эталонная архитектура интернет вещей, разработанная сектором стандартизации Международного союза электросвязи (ITU-T) Y.2060 [5].

Рис.2. Эталонная архитектура IoT

Предложенная эталонная архитектура Международного союза электросвязи детализирует фактические используемые физические компоненты экосистему IoT. Данная архитектура отображает детально каждый уровень архитектуры, которые должны были соединены, интегрированы, управляемы и предоставлены приложениям.

III Стандарты и протоколы интернет вещей

Создание оптимальной архитектуры безопасности IoT устройств необходимо в первую очередь в производственных объектах или смарт - городах, которые соединены в единую платформу, и далее уже на потребительском уровне. Создаваемая безопасность должна отслеживать по отдельности все устройства подключенной к сети, предупреждать о злонамеренном доступе или защищать либо отключить устройства по мере необходимости. Поэтому разработка и использование стандартов для интернет вещей являются крайне важными.

Наиболее активная работа на всех уровнях Интернет вещей идет в области стандартизации. На сегодняшний день разработкой стандартов занимается крупные организации, такие как IEEE (Institute of Electrical and Electronics Engineers) и ISO/IEC (International Electrotechnical Commission) [6,7].

В середине 2014 года первая рабочая группа IEEE P2413 начал разработку «Стандарт архитектурной основы для Интернета вещей (IoT)», в котором основным вопросам данной группы было обеспечения надежности и безопасности устройств.

В декабре 2015 году была создана Межведомственная рабочая группа по стандартизации в области кибербезопасности, целью которой является координация вопросов в области кибербезопасности международном уровне [8]. Данный стандарт описывает цели, риски и угрозы в отношении кибербезопасности IoT. Национальный институт стандартов и технологий (NIST) на основе этого проекта предлагает разделить Интернет вещей на 5 функциональных областей [9]:

1. Подключенные устройства;
2. IoT потребительского класса;
3. Медицинское оборудование и устройства, используемые в сфере здравоохранения;
4. «Умные» здания;
5. «Умное» производство (в том числе, АСУ ТП).

Для каждой области должны быть разработаны свои стандарты с учетом их особенностей.

Вопросы в области стандартов для интернет вещей хотя уже достигли значительного прогресса, но впереди предстоит более глубокие исследование в следующих направлениях: защита личной информации пользователей IoT, архитектура и коммуникации и т.д. Ниже в таблице 1 представлены стандарты IEEE связанные с Internet of Things. [10-21].

Таблица 1. Стандарты IEEE для Internet of Things

IEEE 802.15.4 ™ -2011	Стандарт IEEE для локальных и городских сетей - Часть 15.4: Беспроводные персональные сети с низкой скоростью (LR-WPAN)

IEEE 802.15.4f ™ -2012	Стандарт IEEE для локальных и городских сетей. Часть 15.4: Беспроводные персональные сети с низкой скоростью (LR-WPANs). Физический уровень системы активной радиочастотной идентификации (RFID)
IEEE 802.16 ™ -2012	Стандарт IEEE для воздушного интерфейса для широкополосных систем беспроводного доступа
IEEE 802.16p ™ -2012	Стандарт IEEE для воздушного интерфейса для систем широкополосного беспроводного доступа. Поправки: усовершенствования для поддержки приложений «машина-машина»
IEEE 1609.2 ™ -2013	Стандарт IEEE для беспроводного доступа в автомобильных средах - Службы безопасности для приложений и управленческих сообщений
IEEE 1703 ™ -2012	Стандарт IEEE для локальной сети / глобальной сети (LAN / WAN) Протокол связи узла в дополнение к таблицам данных конечных устройств коммунальной промышленности
IEEE 1888 ™ -2011	Стандарт IEEE для вездесущего сетевого протокола управления сетью
IEEE 1902.1 ™ -2009	Стандарт IEEE для протокола длинной длины волны беспроводной сети
IEEE 1905.1 ™ -2013	Стандарт IEEE для конвергентной цифровой домашней сети для гетерогенных технологий
IEEE 2200 ™ -2012	Стандартный протокол IEEE для управления потоками в медиа-клиентских устройствах
IEEE 2030.5 ™ -2013	IEEE Принятие стандарта Smart Energy 2.0 стандарта протокола приложений
IEEE 21451-7 ™ -2011	Стандарт IEEE для интерфейса интеллектуального преобразователя для датчиков и приводов - Преобразователи в системы радиочастотной идентификации (RFID) Протоколы связи и преобразователи

IV Беспроводные протоколы для интернета вещей

Спектр существующих протоколов обеспечения связи как беспроводные, так и проводные образует экосистему IoT – устройств, обеспечивая сетевое соединения и связь с приложениями. Важнейшую роль в обеспечении беспроводной передачи данных в Интерне вещей играют такие факторы, как отказоустойчивость пропускной способности, адаптивность и совместимость, эффективная передача данных в условиях низкой скорости, реконфигурации и масштабируемость при использовании и организации сети. Для использования в Интернет вещей существует несколько типов беспроводных сетей, таких как:

- Low Power Short Range Networks – энерго-эффективные сети малого радиуса действия;
- Low Power Wide Area Networks (LPWAN) – энерго-эффективные сети большого радиуса действия;
- Cellular Network – технологии, основанные на использовании стандартов сотовых сетей в лицензируемом диапазоне.

Преимуществам протоколов связи LPWAN является низкая требовательность к аппаратным средствам, энерго-эффективная сеть дальнего радиуса действия для датчиков и небольших устройств и в обслуживании очень дешевые, а срок службы без замены батареи должен составлять 10 и более лет. В таблице 2 перечислены стандарты LPWAN сетей, которым характерны эти преимущества [22].

Таблица 2. Стандарты LPWAN сетей

Стандарт LPWAN	RMPA от Ingenu	LoRaWan от Link Labs	LTE-M	Weightless от Nwave	UNB от SigFox	NB-Fi от WAVIoT
Частота	2,4 ГГц	868 МГц	1,8–2,7 ГГц	868 МГц	868 МГц	868 МГц
Максимальная дальность	15 000 м	10 000 м	640 м	4000 м	10 000 м	16 600 м
Ширина полосы пропускания узла	1 МГц	125 кГц	192 кГц	200 Гц	100 Гц	100 Гц
Скорость передачи данных	2 Кбит/с	0,3-50 Кбит/с	1 Мбит/с	100 бит/с	100 бит/с	10-100 бит/с
Беспроводной способ обновления	да	да	неясно	да	нет	да
Режимы шлюза	полудуплекс	полудуплекс	дуплекс	только передача	полудуплекс	дуплекс
Кол-во устройств на шлюз	500 000	40 000	20 000	50 000	50 000	более 1 млн
Шифрование	128 бит	128 бит	128–256 бит	не предусмотрено	128 бит	256 бит
Срок службы батареи	10 лет	10 лет	5 лет	10 лет	10 лет	10 лет
Год выхода на рынок	2010	2014	2020	2013	2010	2011
Сайт	ingenu.com	link-labs.com	3gpp.org	nwave.io	sigfox.com	waviot.com

Пример построения экосистемы с использованием технологии связи IoT, которые обеспечивают обмен информацией и управляющими командами приведен на рисунке 3 [23].

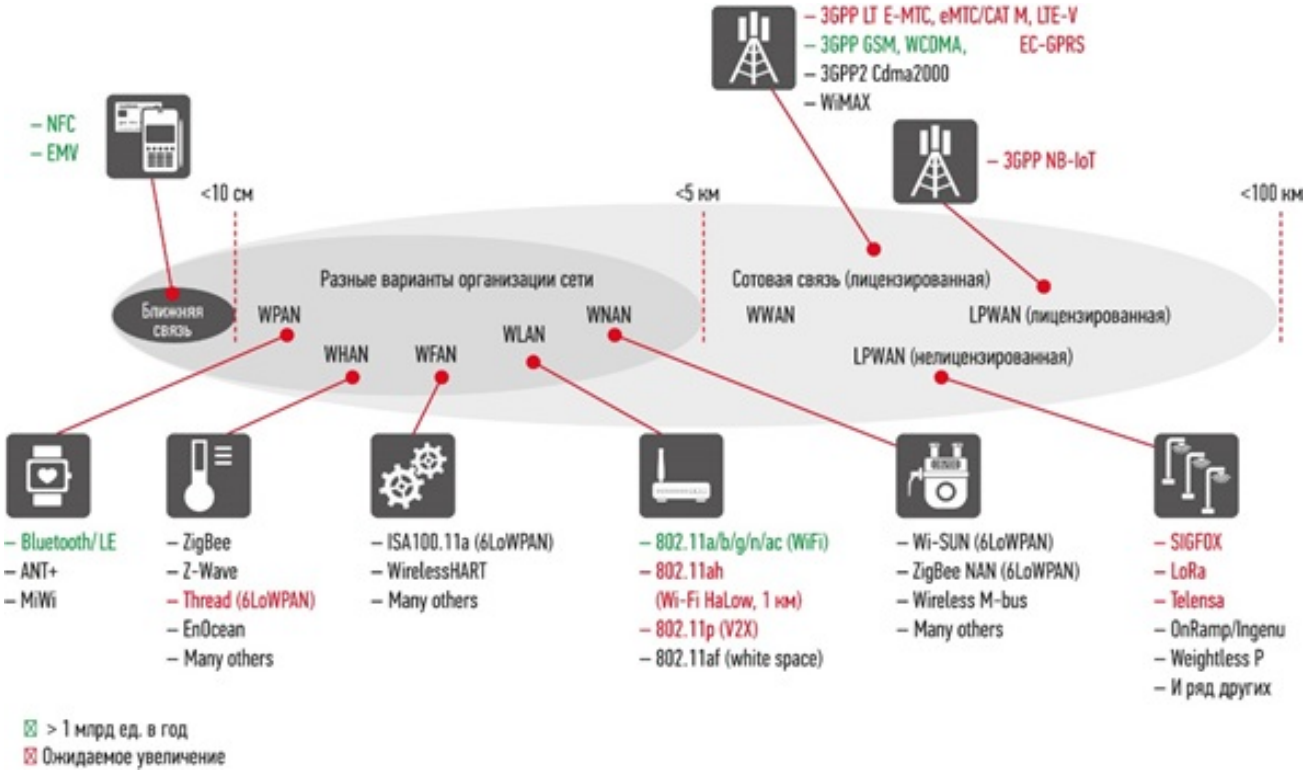

Рис. 3. Пример экосистемы IoT

Протоколы решают различные задачи по обеспечению необходимых требований: скорости передачи, радиуса действия, частотного диапазона, уровня энергопотребления и безопасности. Варианты комбинаций этих условий объясняют многообразие протоколов беспроводных соединений «умных» устройств

V Проблемы и требования, предъявляемые к информационной безопасности интернет вещей

“IoT открывает двери, для многих злоумышленников которые хотят использовать слабые стороны IoT-устройств для получения доступа и перехвата конфиденциальной информации, которая будет использоваться для их собственной выгоды.

Обеспечение безопасности умных устройств, оснащенные датчиками и проводами, должны брать на себя ответственность производители, выпускающие интеллектуальные устройства. При этом соблюдая все требования обеспечения безопасности работы устройств, внедряя лучшие практические решения в области информационной безопасности и проводить качественное тестирование по существующим векторам атак. Производители смарт-устройств должны обеспечить поддержку обновлений программного обеспечения или сертификатов безопасности, даже после завершения разработки и продажи. Но большинство производителей во многих случаях игнорируют обеспечение безопасности своих смарт-устройств, что становиться основной причиной нарушений безопасности IoT.

Некоторые подтверждающие факты, например, IoT-устройств может иметь скрытую учетную запись, в которой обычный пользователь не может изменить пароль или удалить, используют стандартные протоколы подключения, т.к. это учетная запись недоступна ни через веб-интерфейс, ни через мобильный клиент, но злоумышленник может получить к ней доступ, используя другие протоколы как Telnet или SSH. Использование такого рода подключения может дать злоумышленникам возможность, например, просмотр видеопоток, изменения прошивок или же создание компрометации других устройств.

С использованием известных протоколов, таких как TCP, ICMP, HTTP, UPD, DNS и др., злоумышленники осуществляют различные DDoS-атаки, отправляя поток ложных запросов на умные устройства, в целях блокировки или отказ в обслуживание ресурса жертвы. Ресурсами жертвы может быть один из элементов ИТ – инфраструктура как канал связи, маршрутизатор, различные firewall, серверы база данных или приложения.

Одна из известных DDoS – атак с использование IoT-устройства ботнет «Mirai», использовав лишь 100 000 устройств, атаковал DNS-провайдера Dyn, последствии привели к глобальным перебоям в работе интернета в мире [24]. Данная атака мощностью 1,2 Тб/с была осуществлена ботнетом, состоящим из 100 тысяч умных устройств. Ботнет Hajime, обнаруженный в октябре 2016 года специалистами Rapidity Networks, пользуется методом заражения, похожим на Mirai. Ботнет BrickerBot, который, как и Mirai, заражает ПО BusyBox, был обнаружен экспертами компании Radware в апреле 2017 года [25]. Пользуясь верительными данными, установленными по умолчанию в сервисе SSH, а также ошибочными конфигурациями и

известными уязвимостями, ботнет пытается устраивать перманентные атаки на отказ в обслуживании против устройств Интернета вещей. BrickerBot портит прошивки устройств, удаляет на них файлы и меняет сетевые настройки [26].

Если производители на этапе производства и разработки будут внедрять тестирование проникновения на IoT-устройств, то уязвимости будут обнаружены и исправлены до их эксплуатации.

С выпуском новых IoT-устройств все еще остается проблема обеспечения конфиденциальности, целостности и доступности данных, которые являются основными замедлителями широкомасштабного применения IoT. С ростам количества подключенных устройств к интернету, означает, что появятся новые модели и векторы угроз. Государственные органы, регулирующие стандарты в области обеспечения конфиденциальности и защиты информации должны пересмотреть свои принципы и создать новые стандарты с учетом появления новых устройств, используемых как в бытовом, так и промышленном секторе. На рисунке 4 показаны базовые требования к безопасности Интернет вещей.

Рис. 4. Требования к безопасности Интернет вещей

Механизм обеспечение безопасности интернет вещей

Каждое разрабатываемое IoT-устройство состоит из различных датчиков, протоколов подключения и т.д., которые подвергаются воздействию различных угроз атак. К примеру, неавторизованный доступ, анализ или изменение трафика, подмена сертификатов и обновление прошивок на устройствах.

Обеспечение механизма безопасности устройств должно рассматривается в каждом создаваемых IoT проектах В целях защиты экосистемы интернет вещей необходимо задействовать механизмы безопасности на разных уровнях разработки и внедрения IoT-устройств. Механизм обеспечения безопасности показан на рисунке 5 [27].

Рис. 5. Механизм обеспечения безопасности IoT.

VI Методы тестирования IoT – устройств

В настоящее время разрабатываемые умные устройства подключается к сети и массовое развёртывание создает экосистему - IoT. Большинство устройств в сети IoT являются гетерогенными по своей природе и подключены к различным сетям или системам, обмениваются данными по сети, и это создает некоторые проблемы, которые сталкивается Интернет вещи [28]:

- Доступность устройств.
- Идентификация: все устройства должны быть однозначно идентифицируемы.
- Совместимость устройств.
- Связь с сетью.
- Целостность данных, распределенных по сети.
- Конфиденциальность данных, передаваемых по сети.
- Аутентификация: информация должна использоваться совместно с аутентифицированным лицом / приложением.
- Авторизация.
- Корректность.
- Надежность.

Для решения вышеперечисленных проблем и обеспечения системы, делая ее более надежной и доступной, необходимо придерживаться стандартов обеспечения безопасности, и внедрения процесса тестирования на этапе разработки и выпуска устройств.

Методы тестирования умных устройств касаются функционирования самих устройств, взаимодействия с сетями и безопасностью. Проблемы тестирования выходят за рамки самих устройств и датчиков, и возникают другие вопросы, связанные с обработкой больших объемов данных. На сегодняшний день не существует единого подхода и стандарта тестирования Интернет вещей.

Цель тестирования устройств крайне важна в связи с дальнейшей эксплуатацией в работе. Существуют четыре области тестирования интернет вещей на этапе проектирования и разработки (рисунок 6).

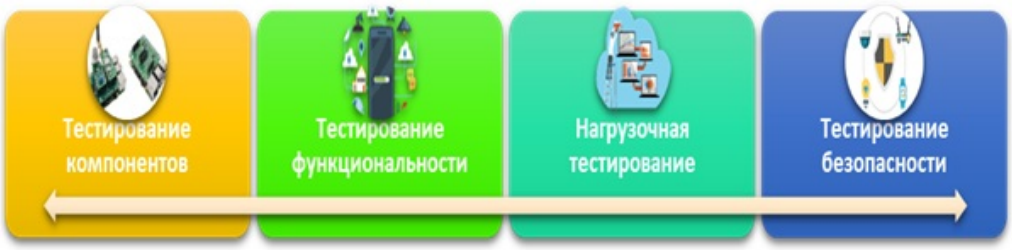

Рис. 6. Области тестирования интернет вещей

Использование методов тестирования программного обеспечения применяются для выявлений нарушений безопасности в коде, исполнении функции программного обеспечение и целостности работы, при проверке соответствия реальным и ожидаемым результатам работы программы. Наиболее широко используемые методы тестирования: модульное, интеграционное, приемочное и тестирование системы.

На этапе тестирования обнаруживается множество критических ошибок, включая проблемы безопасности и производительности, которые невозможно обнаружить на уровне единицы. Подходы к тестированию IoT – устройств существенно будет отличаться в зависимости от разработанной архитектуры при проектировании системы.

Большое количество подключенных устройств в сети, означает ряд большинство проблем при эксплуатации. Для тестирования архитектуры IoT – решения существуют несколько подходов:

1. Тестирование юзабилити – важно обеспечить бесперебойную работу и приятный пользовательский интерфейс для пользователей устройств. Благодаря множеству умных устройств различной формы, функций и форм, подключаемых через IoT, применения тестирование на удобство становится решающим [29].
2. Тестирование безопасности – в среде IoT пользователи, полагающихся на безопасность обмена и хранения данных, критически важно тестирование безопасности, включая аутентификацию пользователей, проверку конфиденциальности данных и шифрование, стандартов сетевой безопасности и т.д.
3. Функциональное тестирование – тестирование функционирования программного обеспечения, работающего в устройствах и сервисах крайне важно. Тестирование в реальном режиме - лучший способ обнаружить проблемы, которые может обнаружить конечный пользователь, когда они используют приложение или устройства.
4. Тестирование масштабируемости – симулируют различные сценарии возникновения пиковых нагрузок вовремя использование сервисами или платформой IoT, чтобы проверить готовность приложения к критическим ситуациям, и адаптироваться к внезапным изменениям без потери производительности.
5. Тестирование совместимости – существует множество типов устройств, которые будут подключены к системе IoT. Эти устройства имеют разнообразную конфигурацию аппаратно – программного обеспечения, версий протокола связи и доступности. В связи этим необходимо важно проверить совместимость в системе IoT [30].
6. Тестирование надежности – проверка компонентов IoT таких как датчики, платы, соединения, эксплуатация в различных условиях окружающей среды.
7. Тестирование сети – обеспечивая точное покрытие, определение пропускной способности, время задержки кадра и надежности сети, что имеет решающее значение для ее развертывания и последующей оптимизации. Тестирование приложения IoT в различных сетевых подключениях и протоколах соединений для обеспечения бесшовной связи на платформе IoT [31].
8. Тестирование базы данных – позволит минимизировать риски при внедрении системы в эксплуатацию. В процессе тестирования базы данных проверяется работа базы данных приложения на предмет соответствия функциональным и нефункциональным требованиям.
9. Тестирование производительности – представляет собой класс тестов, применяемых для количественного измерения характеристик объекта системы, связанных с производительностью, включая продолжительность выполнения процедур, время отклика, надежность и другие параметры, время отклика датчиков или приложения находится в пределах указанного предела. Кроме того, проверка эффективности чтения, записи и скорости извлечения данных является одним из ключевых аспектов тестирования производительности в IoT [32]

VII Заключение

С развитием технологии IoT, вопрос обеспечения безопасности представляет серьезную угрозу для сети Интернет, поскольку на большинстве IoT – устройств не реализованы механизмы обеспечения безопасности. Рост вредоносного ПО и ботнетов с каждыми годами растет. Следовательно, чтобы защитить системы от такого вредоносного ПО и улучшить механизмы защиты, необходимо разрабатывать единые стандарты для обеспечения безопасности. В данной статье представлен обзор стандартов, разрабатываемых крупными организациями, такими как NIST, IEEE, ISO/IEC и другие для IoT – устройств для решения вопросов обеспечения безопасности и защиты информации. Также в статье описывается спектр существующих протоколов обеспечения связи, беспроводные протоколы и примеры построения экосистем IoT – устройств. Были рассмотрены

рекомендации по организации методов тестирования IoT-устройств. Описаны механизмы обеспечения безопасности интернет вещей по уровням. Изученные стандарты для обеспечения информационной безопасности необходимо будет соблюдать во время разработки и производства IoT - устройств.

Следует отметить что, количество стандартов и рекомендаций по обеспечению информационной безопасности интернет вещей в настоящее время недостаточно. Необходимо учитывать всю серьезность проблемы новых векторов атак на умные устройства, в связи с этим, регулирование решения вопросов обеспечения безопасности выпускаемых умных устройств должно взять на себя государство, с внесениями соответствующих изменений в национальную нормативно-правовую систему, которая включает в себя вопросы о защите информации на всех уровнях.

В будущем (в дальнейшей работе планируется рассматривать) будем рассматривать обзор и анализ ботнет-сетей, атакующие IoT – устройств, связанные с ними сигнатуры, которые находятся в публичном доступе. Также планируется провести тесты на проникновение (pentest) IoT – устройствам, по известным протоколам и методами.

Библиография

[1] Интернет вещей, IoT, M2M мировой рынок http://www.tadviser.ru/index.php/Статья:Интернет_вещей,_IoT,_M2M_(мировой_рынок)

[2] IDC https://ru.wikipedia.org/wiki/International_Data_Corporation

[3] IoT https://strij.tech/publications/tehnologiya/chto-takoe-internet-veschey.html

[4] IoT ecosystem https://www.intel.ru/content/www/ru/ru/internet-of-things/ecosystem.html

[5] Рекомендация МСЭ-Т Y.2060 для интернета вещей (IoThttps://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=ru

[6] IEEE Internet of Things https://iot.ieee.org/

[7] International Electrotechnical Commission https://www.iec.ch/

[8] Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) https://csrc.nist.gov/publications/detail/nistir/8200/draft

[9] NIST: Internet of Things https://www.nist.gov/topics/internet-things-iot

[10] IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) http://standards.ieee.org/findstds/standard/802.15.4-2011.html

[11] IEEE 802.15.4f-2012 - IEEE Standard for Local and metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 2: Active Radio Frequency Identification (RFID) System Physical Layer (PHY) http://standards.ieee.org/findstds/standard/802.15.4f-2012.html

[12] IEEE 802.16-2012 - IEEE Standard for Air Interface for Broadband Wireless Access Systems http://standards.ieee.org/findstds/standard/802.16-2012.html

[13] IEEE 1609.2-2013 - IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages http://standards.ieee.org/findstds/standard/1609.2-2013.html

[14] http://standards.ieee.org/findstds/standard/802.16p-2012.html

[15] IEEE 1703-2012 - IEEE Standard for Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables http://standards.ieee.org/findstds/standard/1703-2012.html

[16] IEEE 1888-2011 - IEEE Standard for Ubiquitous Green Community Control Network Protocol http://standards.ieee.org/findstds/standard/1888-2011.html

[17] IEEE 1902.1-2009 - IEEE Standard for Long Wavelength Wireless Network Protocol http://standards.ieee.org/findstds/standard/1902.1-2009.html

[18] IEEE 2200-2012 - IEEE Standard Protocol for Stream Management in Media Client Devices http://standards.ieee.org/findstds/standard/2200-2012.html

[19] http://standards.ieee.org/develop/project/1905.1.html

[20] IEEE 2030.5-2013 - IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard http://standards.ieee.org/findstds/standard/2030.5-2013.html

[21] IEEE 21451-7-2011 - Information technology--Smart transducer interface for sensors and actuators--Part 7: Transducers to radio frequency identification (RFID) systems communication protocols and transducer electronic data sheet (TEDS) formats http://standards.ieee.org/findstds/standard/21451-7-2011.html

[22] E. Morin, M. Maman, R. Guizzetti, and A. Duda, “Comparison of the device lifetime in wireless networks for the internet of things,” IEEE Access, vol. 5, pp. 7097–7114, 2017

[23] LPWAN: умная сеть будущего https://ichip.ru/lpwan-umnaya-set-budushhego.html

[24] Технологии IoT, сгруппированные по рабочему диапазону покрытия http://controlengrussia.com/besprovodny-e-tehnologii/putivoditel-iot-1/

[25] Ботнет Mirai использовался для мощной DDoS-атаки на компанию Dyn https://habr.com/company/eset/blog/313444/

[26] BrickerBot превращает IoT-гаджеты в «кирпич» https://habr.com/post/402995/

[27] BrickerBot Permanent Denial-of-Service Attack https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A

[28] Long Chen, Security Management for The Internet of Things, Electronic Theses and Dissertations, 2017

[29] Безопасность «Интернета вещей»: существующие проблемы и их решение http://www.controlengrussia.com/internet-veshhej/bezopasnost-interneta-veshhej/

[30] Тестирование юзабилитов https://qalight.com.ua/baza-znaniy/yuzabiliti/

[31] Типы тестирования программного обеспечения https://geteasyqa.com/ru/qa/software-testing-types/

[32] Тестирование производительности: последовательность тестов, измеряемые показатели, правила подачи нагрузки http://software-testing.ru/library/testing/performance-testing/2685-test-perfomance

[33] Тестирование производительности Комплексная проверка на всех этапах жизненного цикла ПО. http://www.a1qa.ru/performance-testing/

[34] В. Чанг, М. Рамачандран, «На пути к обеспечению безопасности данных с помощью среды принятия облачных вычислений», IEEE Trans. Услуги Comput. том 9, нет 1, с. 138-151, январь / февраль. 2016.

[35] Угрозы интернета вещей и возможные методы защиты https://os.kaspersky.ru/2019/03/13/ugrozy-interneta-veshhey-i-vozmozhnye-me/

Review and analysis of standards and protocols in the field of Internet of Things. Modern testing methods and problems of information security IoT

N.A. Naraliyev, D.I. Samal

***Abstract*— IoT is a whole ecosystem that contains intelligent devices equipped with sensors (sensors) that provide remote control, storage, transmission and security of data. The Internet of Things (IoT) is an innovative solution in various areas such as healthcare, insurance, labor protection, logistics, ecology, etc. To unleash the full potential of using IoT devices, it is necessary to solve many problems related to standards, security, architecture, ecosystem construction, channels and device connection protocols. Today in the world, large organizations such as NIST, IEEE, ISO / IEC, and others make enormous efforts in addressing the issues of standardization, security, and the architecture of developed devices.**

Analysis of recent scientific research in the field of solving information security issues and data privacy of IoT devices showed positive results, but these methods and approaches are based on traditional methods of network security. The development and application of security mechanisms for IoT devices is a complex and heterogeneous task. In this regard, ensuring information security and the protection of sensitive data, as well as the availability of IoT devices, is the main purpose of writing this article.

Given the above, many questions arise related to the security status of IoT devices, namely: What are the current standards and protocols for IoT? What are the requirements for ensuring information security of IoT devices? What security mechanisms do IoT devices have? What methods of testing IoT devices exist?

Manufacturers and developers of IoT devices do not pay enough attention to security issues. With the development of cyber-attacks, attack vectors are becoming more sophisticated and aimed at several infrastructure elements at the same time. IoT infrastructure typically includes millions of connected objects and devices that store and share confidential information. Scenarios of theft and fraud, such as hacking and falsifying personal data, pose a serious threat to such IoT devices. Most IoT devices use the public Internet to exchange data, which makes them vulnerable to cyber-attacks. Modern approaches to information security often offer solutions to individual problems, when multi-level approaches offer increased resistance to cyber-attacks.

***Keywords*— iot, cybersecurity, cyber-attack, Internet of things, information security, wireless technologies, LoraWAN.**

REFERENCES

[1] Internet of Things, IoT, M2M global market http://www.tadviser.ru/index.php/Article: On-line media_, _IoT,_M2M_(world_market)
[2] https://ru.wikipedia.org/wiki/International_Data_Corporation
[3] https://strij.tech/publications/tehnologiya/chto-takoe-internet-veschey.html
[4] https://www.intel.ru/content/www/ru/ru/internet-of-things/ecosystem.html
[5] ITU-T Recommendation Y.2060 for the Internet of Things (IoThttps: //www.itu.int/ITU-T/recommendations/rec.aspx? Rec = 11559 & lang = en
[6] IEEE Internet of Things https://iot.ieee.org/
[7] International Electrotechnical Commission https://www.iec.ch/
[8] International Cybersecurity Standardization for Internet of Things (IoT) https://csrc.nist.gov/publications/detail/nistir/8200/draft
[9] NIST: Internet of Things https://www.nist.gov/topics/internet-things-iot
[10] IEEE Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) http://standards.ieee.org/findstds/standard/802.15.4-2011.html
[11] IEEE 802.15.4f-2012 - IEEE Standard for Local and Metropolitan area networks-- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 2: Active Radio Frequency Identification (RFID) System Physical Layer (PHY)) http://standards.ieee.org/findstds/standard/802.15.4f-2012.html
[12] IEEE 802.16-2012 - IEEE Standard for Broadband Wireless Access Systems http://standards.ieee.org/findstds/standard/802.16-2012.html
[13] IEEE 1609.2-2013 - http://www.ieee.org/findstds/standard/1609.2-2013.html
[14] http://standards.ieee.org/findstds/standard/802.16p-2012.html
[15] IEEE 1703-2012 - IEEE Standard for Local Area Area Networks / Wide Area Network (LAN / WAN) Industry Data Center Device Data Tables http://standards.ieee.org/findstds/standard/1703 -2012.html
[16] IEEE 1888-2011 - IEEE Standard for Ubiquitous Green Community Control Network Protocol http://standards.ieee.org/findstds/standard/1888-2011.html
[17] IEEE 1902.1-2009 - IEEE Standard for Long Wavelength Wireless Network Protocol http://standards.ieee.org/findstds/standard/1902.1-2009.html
[18] IEEE 2200-2012 - IEEE Standard Protocol for Stream Management in Media Client Devices http://standards.ieee.org/findstds/standard/2200-2012.html
[19] http://standards.ieee.org/develop/project/1905.1.html
[20] IEEE 2030.5-2013 - IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard http://standards.ieee.org/findstds/standard/2030.5-2013.html
[21] IEEE 21451-7-2011 - Information technology - Transducers electronic data sheet (TEDS) http: // standards.ieee.org/findstds/standard/21451-7-2011.html
[22] E. Morin, M. Maman, R. Guizzetti, and A. Duda, IEEE Access, vol. 5, pp. 7097–7114, 2017
[23] LPWAN: smart network of the future https://ichip.ru/lpwan-umnaya-set-budushhego.html
[24] IoT technologies grouped by working coverage range http://controlengrussia.com/besprovodny-e-tehnologii/putivoditel-iot-1/
[25] The Mirai botnet was used for a powerful DDoS attack on the Dyn company https://habr.com/company/eset/blog/313444/
[26] BrickerBot turns IoT gadgets into “brick” https://habr.com/post/402995/
[27] BrickerBot Permanent Denial-of-Service Attack https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A
[28] Security Management for the Internet of Things, Electronic Theses and Dissertations, 2017

[29] Security of the “Internet of Things”: existing problems and their solutions http://www.controlengrussia.com/internet-veshhej/bezopasnost-interneta-veshhej/
[30] Testing usability https://qalight.com.ua/baza-znaniy/yuzabiliti/
[31] Types of software testing https://geteasyqa.com/en/qa/software-testing-types/
[32] Performance testing: test sequence, measurable indicators, rules for submitting the load http://software-testing.ru/library/testing/performance-testing/2685-test-perfomance
[33] Performance Testing Comprehensive testing at all stages of the software life cycle. http://www.a1qa.ru/performance-testing/
[34] V. Chang, M. Ramachandran, “Towards Ensuring Data Security Using the Cloud Computing Environment”, IEEE Trans. Comput services. Volume 9, no 1, p. 138-151, January / February. 2016
[35] Threats of the Internet of Things and possible methods of protection https://os.kaspersky.com/2019/03/13/ugrozy-interneta-veshhey-i-vozmozhnye-me/