УДК 004.77 **DOI: 10.18413/2518-1092-2021-6-3-0-5**

Вьющенко О.О.
Маслова М.А.

ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ В СФЕРЕ ИНТЕРНЕТА ВЕЩЕЙ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: doctorsten2@yandex.ua, mashechka-81@mail.ru

Аннотация
Стремительное развитие Интернета вещей (IoT) и его возможности по виду услуг сделали его одной из быстрорастущих технологий, оказывающих огромное влияние как на социальную жизнь, так и на деловую среду человека. Широкое распространение подключенных устройств в IoT создало огромный спрос на надежную безопасность в ответ на растущий спрос миллиардов подключенных устройств и услуг по всему миру. Но при этом число угроз продолжает расти с каждым днем, а атаки увеличиваются как по количеству, так и по сложности. Так же растет число злоумышленников и инструменты, которыми они пользуются, постоянно усовершенствуются и становятся все более эффективными. Следовательно, необходимо постоянная защита от угроз и уязвимостей для IoT. В данной статье проведем анализ развития IoT, рассмотрим существующие угрозы, атаки на IoT, а также методы защиты устройств от угроз и уязвимостей для IoT.
Ключевые слова: интернет вещей (IoT), угрозы, уязвимости, конфиденциальность, злоумышленники, безопасность.
Для цитирования: Вьющенко О.О., Маслова М.А. Об обеспечении безопасности в сфере интернета вещей // Научный результат. Информационные технологии. - Т.6, №3, 2021. С. 33-39. DOI: 10.18413/2518-1092-2021-6-3-0-5

Viushchenko O.O.
Maslova M.A.

ABOUT ENSURING SECURITY IN THE FIELD OF THE INTERNET OF THINGS

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: doctorsten2@yandex.ua, mashechka-81@mail.ru

Abstract
The rapid development of the Internet of Things (IoT) and its capabilities in terms of services have made it one of the fastest-growing technologies that have a huge impact on both social life and the business environment of a person. The widespread adoption of connected devices in the IoT has created a huge demand for reliable security in response to the growing demand of billions of connected devices and services around the world. But at the same time, the number of threats continues to grow every day, and attacks are increasing both in number and complexity. The number of attackers is also growing, and the tools they use are constantly being improved and becoming more effective. Therefore, it is necessary to constantly protect against threats and vulnerabilities for IoT. In this article, we will analyze the development of IoT, consider existing threats, attacks on IoT, as well as methods of protecting devices from threats and vulnerabilities for IoT.
Keywords: Internet of Things (IoT), threats, vulnerabilities, privacy, attackers, security.
For citation: Viushchenko O.O., Maslova M.A. About ensuring security in the field of the internet of things // Research result. Information technologies. - T.6, №3, 2021. - P. 33-39. DOI: 10.18413/2518-1092-2021-6-3-0-5

ВВЕДЕНИЕ

Интернет вещей (IoT) все более широко входит в различные аспекты жизнедеятельности современного человека, без которых уже трудно представить современное общество: банковская система, образование, система здравоохранения, маркетинг, домашний обиход, спорт,

машиностроение, внедрения новых продуктов на рынке, хранение информации о человеке как в государстве, так и в частных целях и т.д. Так как внедрение любой технологии IoT в наших домах, на работе, предприятиях открывает двери для новых проблем безопасности, то помимо удобств и развития немаловажным аспектом является защита от угроз и уязвимостей во всех областях внедрения интернет вещей. Пользователи и поставщики должны учитывать и проявлять осторожность в отношении таких проблем безопасности и конфиденциальности путем постоянного анализа, обеспечения контроля, постоянной защиты IoT от злоумышленников [8, 10].

ОСНОВНАЯ ЧАСТЬ

По данным компании Cisco IBSG, уже в 2008 году количество имеющихся подключенных к Интернету устройств тогда уже превышало численность населения Земли и стало рождением Интернета вещей. Через пару лет в 2010 году на одного человека приходилось около 1,8 устройства, подключенного к интернету, что составляло 12 миллиардов устройств, а к 2022 году по прогнозу количество таких устройств превысит 50 миллиардов, что составляет 6.3 устройства на человека. [1, 2]. Началась эра стремительного развития IoT, а также его способности представлять множество разнообразных услуг для человечества и, следовательно, самой быстрорастущей технологией, оказывающей большое влияние на все сферы человеческой деятельности (рис. 1).

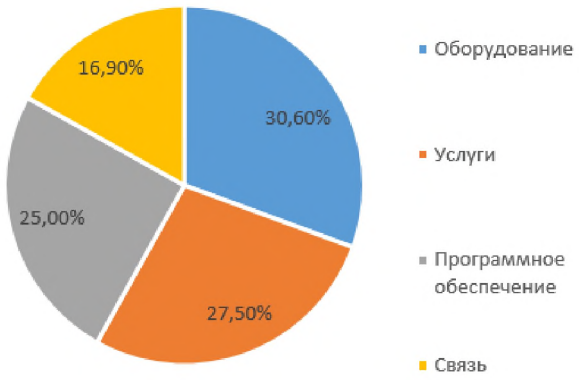

Рис. 1. Структура мирового рынка интернета вещей
Fig. 1. Structure of the global Internet of Things market

Рынок IoT на 2019 г составил 212 млрд. долларов, а по прогнозам к началу 2025 года показатель возрастет до 1,08 трлн. долларов [3].

Изначально аналитики наблюдая за вредоносными программами получали статистические данные с достаточно низкой активностью программ, которые были направлены на техническое обеспечение IoT. Например, специалисты «Доктор Веб» в 2016 г за четыре месяца зарегистрировали 730 000 атак, через год их уже было в 29 раза больше - 24 000 000, к 2018 г их количество насчитывало уже 99 000 000, в 2019 г лишь за первое полугодие было совершено 73 000 000 атаки [4]. Т.е. видно, что рост атак, взломов и заражения устройств постоянно набирает все больших оборотов и всего лишь за три года возросло на 13497%. Динамика обнаружения ханипотами атак представлена на рисунке 2.

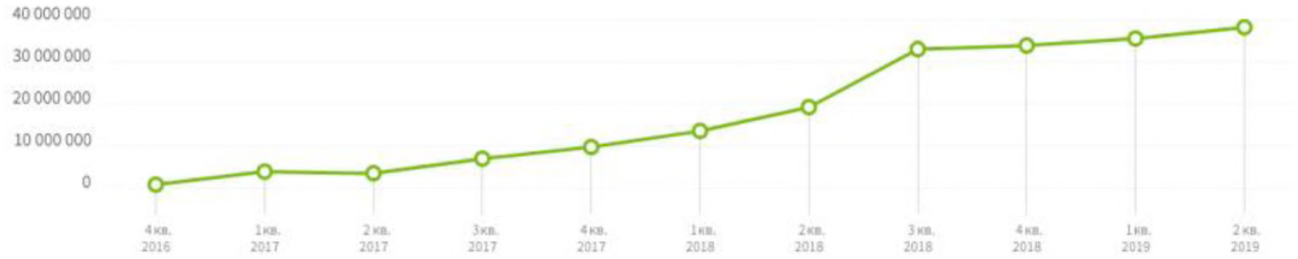

Рис. 2. Зафиксированные ханипотами атаки на устройства IoT
Fig. 2. Attacks on loT devices recorded by honeypots

Помимо роста угроз и атак, также растет число злоумышленников, желающих на этом заработать. Постоянно усовершенствуется инструменты, которые они используют в работе. Для того, чтобы IoT работало качественно и без сбоев необходимо постоянно усовершенствовать его защиту как от существующих, так и ново появляющихся угроз, и уязвимостей. [5].

Затраты на обеспечение безопасности в сфере Интернета вещей из года в года растет, так как увеличивается число атак и злоумышленников. В 2014 г - 231,86 млн долл, 2015 - 281,54 млн долл., 2016 - 348,32 млн долл, 2018 - 547,2 млн долл. Т.е. с 2014 по 2018 года затраты на безопасность выросли почти в 2,5 раза (см. рис. 3) [6].

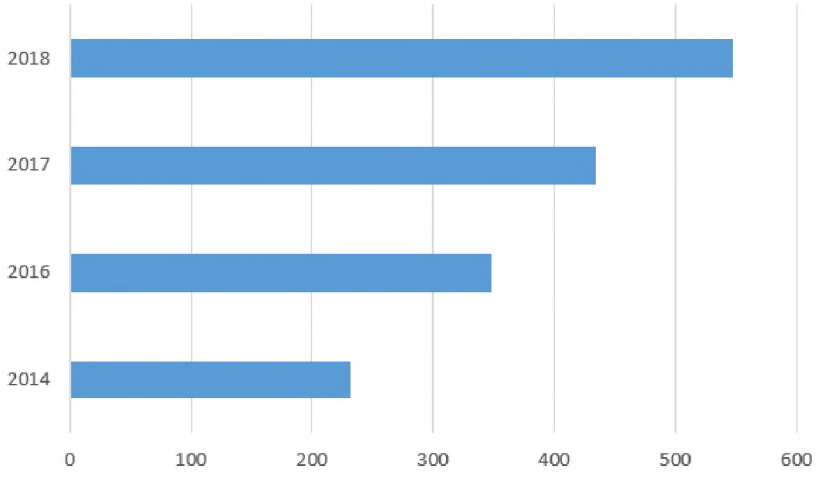

Рис. 3. Затраты на безопасность в сфере loT, в млн долл.
Fig. 3. IoT security costs, in millions of US dollars

Безопасность определяется как процесс защиты объекта от физического повреждения, несанкционированного доступа, кражи или потери путем поддержания высокой конфиденциальности и целостности информации об объекте и предоставления информации об этом объекте в случае необходимости. Требования безопасности в среде IoT не отличаются от любых других систем информационно-коммуникационных технологий. Следовательно, для обеспечения безопасности IoT необходимо поддержание наивысшей внутренней ценности как материальных объектов (устройств), так и нематериальных (услуг, информации и данных).

Киберугрозы могут быть запущены против любых активов и объектов IoT, вызывая как ущерб, так и выводя из строя работу системы как частично, так и полностью, что может привести к серьезному экономическому ущербу как предприятия, так и обычного пользователя, не говоря уже об опасности для населения планеты в целом. Очень часто производятся атаки на такие объекты, как: системы связи, отопления, освещения, физической безопасности, кондиционирования, а также домашних устройств и приборов. Например, информация, собранная с датчиков, встроенных в системы отопления или освещения человека, может сообщить

злоумышленнику, когда кто-то находится дома или вне дома. Атаки так же могут быть направлены на крупные предприятия или заводы, с целью обогатиться или нанести ущерб конкуренту, например, отключения света или сбой в массовом производстве продукции. Можно тогда представить размер причинённого ущерба.

Поэтому вопросы безопасности и конфиденциальности становятся все более актуальными для пользователей и поставщиков в связи с их переходом на IoT. Обеспечение безопасности подразумевает защиту как устройств IoT, так и служб от несанкционированного доступа как изнутри устройств, так и извне. Безопасность должна защищать службы, аппаратные ресурсы, информацию и данные как при переходе, так и при хранении [7].

Рассмотрим, какие ключевые проблемы существуют с устройствами и службами IoT: конфиденциальность данных, приватность и доверие. Конфиденциальность данных является основательной проблемой в устройствах и службах IoT., т.к. доступ к данным может получить не только пользователь, но и авторизованный объект. Для этого необходимо решить две важные задачи: механизм контроля доступа и авторизации и, механизм аутентификации и управления идентификацией (IdM). Устройство IoT должно иметь возможность проверить, что организация (физическое лицо или другое устройство) авторизована для доступа к службе. Авторизация помогает определить, разрешено ли лицу или устройству получать услугу после идентификации. Контроль доступа -это контроль доступа к ресурсам посредством предоставления или отказа в предоставлении средств с использованием широкого спектра различных критериев. Аутентификация и контроль доступа важны для установления безопасного соединения между устройствами и службами. Основная проблема, которую необходимо решить в данном случае - это упростить создание, понимание и управление правил контроля доступа.

Что касается аутентификации и управления идентификацией, она имеет решающее значение в IoT, поскольку несколько пользователей, объектов/вещей и устройств должны аутентифицировать друг друга с помощью надежных служб. Необходимо понять, как найти решение для безопасной обработки личности пользователя, вещей/объектов и устройств. Приватность является важной проблемой в устройствах и сервисах IoT из-за повсеместного характера его среды, так как объекты подключены, а данные передаются и обмениваются через Интернет. Одним из важнейших задач, которые необходимо решить является конфиденциальность при сборе данных, обмене, управлением ими, а также их безопасность.

Но существует множество уязвимостей, которые дают возможность злоумышленнику производить атаки, запускать в действие различные команды и, следовательно, получать несанкционированный доступ к данным и файлам. Они содержаться в аппаратных, программных частях системы, политиках и процедурах, которые используются в системах и конечно в пользовательских системах [4].

Существует несколько основных компонент в IoT - это системное программное обеспечение и системное оборудование. Данное оборудование имеет ряд конструктивных недостатков, которые требуют больших усилий для их исправления. Например, аппаратные возможности очень трудно идентифицировать и исправить, даже если уязвимость была идентифицирована из-за совместимости оборудования, возможности взаимодействия и усилий, которые требуются для исправления. В свою очередь уязвимости программного обеспечения могут находиться в:

- программном обеспечении управления (например, человеческий фактор или сложность ПО);
- прикладном программном обеспечении;
- операционных системах и т.д.

Технические же уязвимости -это человеческие слабости. Часто для получения результата необходимо иметь четкие данные и требования, а их непонимание влияет на начало проекта без плана, плохую коммуникацию между разработчиками и пользователями, нехваткой ресурсов, навыков и знаний, а также неспособность управлять и контролировать систему.

Рассмотрим уровни аппаратной безопасности:

1) Установка корня доверия (RoT), является базовой защитой от руткитов и подразумевает загрузку с аппаратной аутентификацией и гарантирует, что источник первой выполняемой инструкции не может быть изменен. Он является основой этапа процесса загрузки и участвует в дальнейшем запуске системы - от BIOS до ОС и приложений. RoT играет важную роль в установлении безопасной связи, когда ряд вещей взаимодействуют в неопределенной среде Интернета вещей и в нем следует учитывать два аспекта доверия: доверие к взаимодействиям между сущностями и доверие к системе с точки зрения пользователей. [4]. Надежность устройства IoT зависит от компонентов устройства, включая аппаратное обеспечение, такое как: процессор, память, датчики и исполнительные механизмы, программные ресурсы (аппаратное ПО, ОС, драйверы и приложения, источник питания). Для установления доверия пользователей/служб, необходимо создать эффективный механизм определения доверия в динамичной и совместной среде IoT.

2) Управление ключами и TPM (Trusted Platform Module) - это открытый и закрытый ключи, которые являются одним из наиболее часто используемых стандартов защиты аппаратных ключей. Они обеспечивают безопасность системы и для их защиты необходимо подобрать подходящий механизм управления. Спецификация TPM была создана Trusted Computing Group и является частью ISO и IEC. Обычно его используют для хранения, защиты и администрирования ключей в таких случаях, как корень доверенной загрузки, шифрование диска, аппаратная и программная аутентификация и управление паролями. TPM может генерировать хэш проверенной конфигурации оборудования или ПО для обнаружения сторонних вмешательств во время выполнения. Эта технология также используется для генерации хэшей SHA-1 и SHA-256, блочного шифрования AES, асимметричного шифрования и генерации случайных чисел [4]/

3) Безопасность хранения данных. Многие устройства lоT используют постоянное хранилище на граничном узле или маршрутизаторе/шлюзе. Узлы также должны где-то хранить свои данные. В случае потери устройства безопасность данных является ключевой задачей предотвращения установки вредоносного ПО и защиты конфиденциальной информации. Например, большинство устройств хранения (жесткие диски, флэш-накопители) имеют технологию шифрования и безопасности. Но помимо шифрования, также необходимо позаботиться о безопасности выводимых из эксплуатации дисков с безопасным процессом стирания данных с запоминающего устройства. Можно ознакомиться с инструментами безопасного уничтожения контента, описанной в документах лаборатории NIST в специальной публикации NIST 800-88 для безопасного стирания [1].

4) Криптография - это шифрование, конфиденциальность, которые являются обязательными для устройств IoT и помогают защитить связь, защищая прошивку и процесс аутентификации. Шифрование включает в себя три основные категории: шифрование с отрытым ключом (предназначен для шифрования и обмена сообщениями, таких как Elliptic Curve, PGP, RSA, TLS и S/MIME), криптографическое шифрование (привязывает данные произвольного размера к битовой строке, использует односторонние хэши, например, MD5, SHA1, SHA2 и SHA3) и симметричное шифрование (используют алгоритмы RC5, DES, 3DES и AES) [2, 9].

ЗАКЛЮЧЕНИЕ

Исходя из рассмотренного, видно, что как поставщикам, так и конечным пользователям необходимо постоянно работать над качеством безопасности интернета вещей. Для будущих стандартов важно: устранить недостатки существующих механизмов безопасности IoT; постоянно проводить мониторинг появляющихся угроз IoT; учитывать вероятность последствия угроз для IoT; своевременно определять подходящие механизмы безопасности для контроля доступа, аутентификации, управления идентификацией и гибкой системы управления доверием; защищать аппаратную, программную части, а также политики и процедуры используемые как в общих, так и пользовательских системах; постоянно повышать уровень надежности и защиты аутентификации

и управления идентификацией. Все это необходимо рассматривать на ранних этапах разработки продукта, помогая выявить основные проблемы в области безопасности IoT и обеспечивая лучшее понимание угроз и их атрибутов, исходящих от различных злоумышленников, а также постоянно проводить проверки на наличие новых угроз и совершенствовать их защиту.

Список литературы

1. Нам доверяют защиту информации. Актуально / Информзащита - URL: https://www.infosec.ru.
2. Evans D. Internet of Things. Cisco, white paper. URL: https://www.cisco.eom/c/dam/en_us/about/ac79/docs/innov/IoT_IB SG_0411FINAL.
3. Расходы на развитие российского интернета вещей урезали в 4 раза - CNews URL: https://www.cnews.ru/articles/2021-03-30_rashody_na_razvitie_rossijskogo.
4. Кожевникова И.С. Тенденции безопасности интернет-вещей // Молодой ученый. 2017. № 13 (147). С. 11-14.
5. Риски и угрозы в Интернете вещей / Блог компании Доктор Веб / Хабр. URL: https://habr.com/ru/company/drweb/blog/460433/
6. Затраты в сфере кибербезопасности в 2021 году продолжат расти. URL: https://3dnews.ru/1030514/zatrati-v-sfere-kiberbezopasnosti-v-2021-godu-prodolgat-rasti.
7. Маслова М.А. Принципы безопасности интернета вещей // Вестник УрФО. Безопасность в информационной сфере. 2018. № 3 (29). С. 38-42.
8. Наумов Р.К., Железков Н.Э. Сравнительный анализ форматов хранения текстовых данных для дальнейшей обработки методами машинного обучения // Научный результат. Информационные технологии. 2021. Т. 6. № 1. С. 40-47. DOI: 10.18413/2518-1092-2021-6-1-0-5.
9. Нестеренко В.Р., Маслова М.А. Использование технологии blockchain для обеспечения безопасности в распределенном интернете вещей // Научный результат. Информационные технологии. 2021. Т. 6. № 2. С. 3-8. DOI: 10.18413/2518-1092-2021-6-20-1.
10. Полегенько А.М. Особенности защиты информации в Интернете вещей // International Journal of Open Information Technologies, Vol.6, No 10, 2018. С. 41-45.

References

1. We are trusted to protect information. Actual / Informzashchita - URL: https://www.infosec.ru.
2. Evans D. Internet of Things. Cisco, white paper. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IB SG_0411FINAL.
3. Expenses for the development of the Russian Internet of Things were cut by 4 times - CNews. URL: https://www.cnews.ru/articles/2021-03-30_rashody_na_razvitie_rossijskogo.
4. Kozhevnikova I.S. Security Trends in Internet of Things // Young Scientist. 2017. № 13 (147). P. 11-14.
5. Risks and Threats in the Internet of Things / Doctor Web Blog / Habr. URL: https://habr.com/ru/company/drweb/blog/460433/.
6. Cybersecurity costs will continue to rise in 2021. URL: https://3dnews.ru/1030514/zatrati-v-sfere-kiberbezopasnosti-v-2021 -godu-prodolgat-rasti.
7. Maslova M.A. Security principles of the Internet of Things // Bulletin of the Ural Federal District. Security in the Information Sphere. 2018. № 3 (29). P. 38-42.
8. Naumov R.K., Zhelezkov N.E. Comparative analysis of text data storage formats for further processing by methods of machine learning // Research result. Information technologies. - T.6, №1, 2021. - P. 40-47. DOI: 10.18413/2518-1092-2021-6-1-0-5.
9. Nesterenko R.V., Maslova M.A. Using blockchain technology to ensure security in the distributed internet of things // Research result. Information technologies. - T.6, №2, 2021. - P. 3-8. DOI: 10.18413/2518-1092-2021-6-2-0-1.
10. Polegen'ko A.M. Features of information protection in the Internet of Things // International Journal of Open Information Technologies, Vol.6, No 10, 2018. P. 41-45.

Вьющенко Олег Олегович, студент четвертого курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Маслова Мария Александровна, старший преподаватель кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности

Viushchenko Oleg Olegovich, fourth-year student of the Department Information security, Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, senior lecturer of the Department Information security, Institute of Radioelectronics and Information security