ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.75, 004.77

РАЗРАБОТКА КОМПЛЕКСА МЕР БЕЗОПАСНОСТИ ПРИМЕНИТЕЛЬНО К ИНТЕРНЕТУ ВЕЩЕЙ

Величко Денис Дмитриевич,
ФБОУ ВО «Калужский государственный университет им. К.Э. Циолковского», магистрант кафедры «Информатики и информационных технологий», г. Калуга, denys97.velichko@mail.ru.

Аннотация

В статье рассматриваются вопросы безопасности устройств, относящихся у Интернету вещей, в общем, и системам «Умный дом» в частности. Приводится и декомпозируется общая сетевая инфраструктура, определяются информационные потоки между устройствами, пользователями и администраторами. Определяются характерные виды уязвимостей и соответствующие им виды атак, предлагаются методы противодействия.

Ключевые слова: интернет вещей, умный дом, уязвимость, атака, противодействие атакам.

DEVELOPMENT OF A SET OF SECURITY MEASURES APPLICABLE TO THE INTERNET OF THINGS

Denis D. Velichko,
Kaluga State University named after K.E. Tsiolkovski, student of the Department of Informatics and information technologies, Kaluga city, denys97.velichko@mail.ru.

ABSTRACT

The article deals with the security issues of devices related to the Internet of Things, in general, and Smart Home systems in particular. The general network infrastructure is given and decomposed, information flows between devices, users and administrators are determined. The characteristic types of vulnerabilities and the corresponding types of attacks are determined, methods of counteraction are proposed.

Keywords: Internet of Things, Smart home, vulnerability, attack, counteraction to attacks.

1. Введение. Интернет вещей, в общем, и системы «Умный дом», в частности, состоят из вычислительных устройств, цифровых или механических машин, которые могут передавать и получать данные по вычислительным сетям без необходимости взаимодействия с человеком. Кроме того, многие из этих устройств могут работать независимо в рамках существующей инфраструктуры Интернета [1, 2] В настоящее время проблемы безопасности Интернета вещей растут по мере того, как устройства становятся все более распространенными и автоматизированными [3-9].

2. Цель исследования. Целью исследования является определение методов (мер безопасности) противодействия угрозе безопасности, которые следует использовать для устройств Интернета вещей.

Для этого были выделены следующие задачи:

1. Определить информационные потоки между участниками сетей Интернета вещей для получения общей схемы сетевого взаимодействия.

2. Разбить сетевую инфраструктуру на зоны доверия и уточнить информационные потоки как на уровне устройств, в частности, так и на уровне сети, в целом.

3. Предложить классификацию, охватывающую большинство устройств Интернета вещей, и определить, какие общие устройства используются как на индивидуальном, так и на коммерческом уровнях.

4. Определить виды уязвимостей и соответствующие им виды атак.

В результате решения задач 1-4 становится возможным выполнить сопоставление вида атаки, области атаки, цели атаки и уязвимостей и предложить меры безопасности для устройств Интернета вещей по областям.

3. Материалы и методы исследования.

3.1. Определение информационных потоков между участниками сетей Интернета вещей.

Для определения информационных потоков между участниками сетей Интернета вещей следует установить, каким образом то или иное устройство участника получает доступ к сети Интернета вещей.

После выполнения подключения локальный/удаленный пользователь получает доступ к интерфейсу приложения. Каждому сеансу локального/удаленного пользователя в целях обеспечения безопасности сопоставляется своя виртуальная машина; сеансы выполняются на сервере приложений. База данных будет содержать информацию об учетных записях пользователей, а также другие пользовательские данные и журналы использования. Отметим, что удаленные пользователи не могут получить доступ к локальным сетям и подключение осуществляется к облачному шлюзу для доступа к серверу приложений. Локальные и удаленные администраторы могут получать доступ к административному интерфейсу для просмотра аналитических данных, полученных с сервера приложений, и выполнения обслуживания.

Общая схема сети, представленная на рисунке 1, визуализирует потоки данных, которыми обмениваются пользователи, администраторы и устройства, и позволяет представить общую модель угрозы безопасности. Используя эту схему, можно разложить модель сети, чтобы определить зоны доверия в среде Интернета вещей.

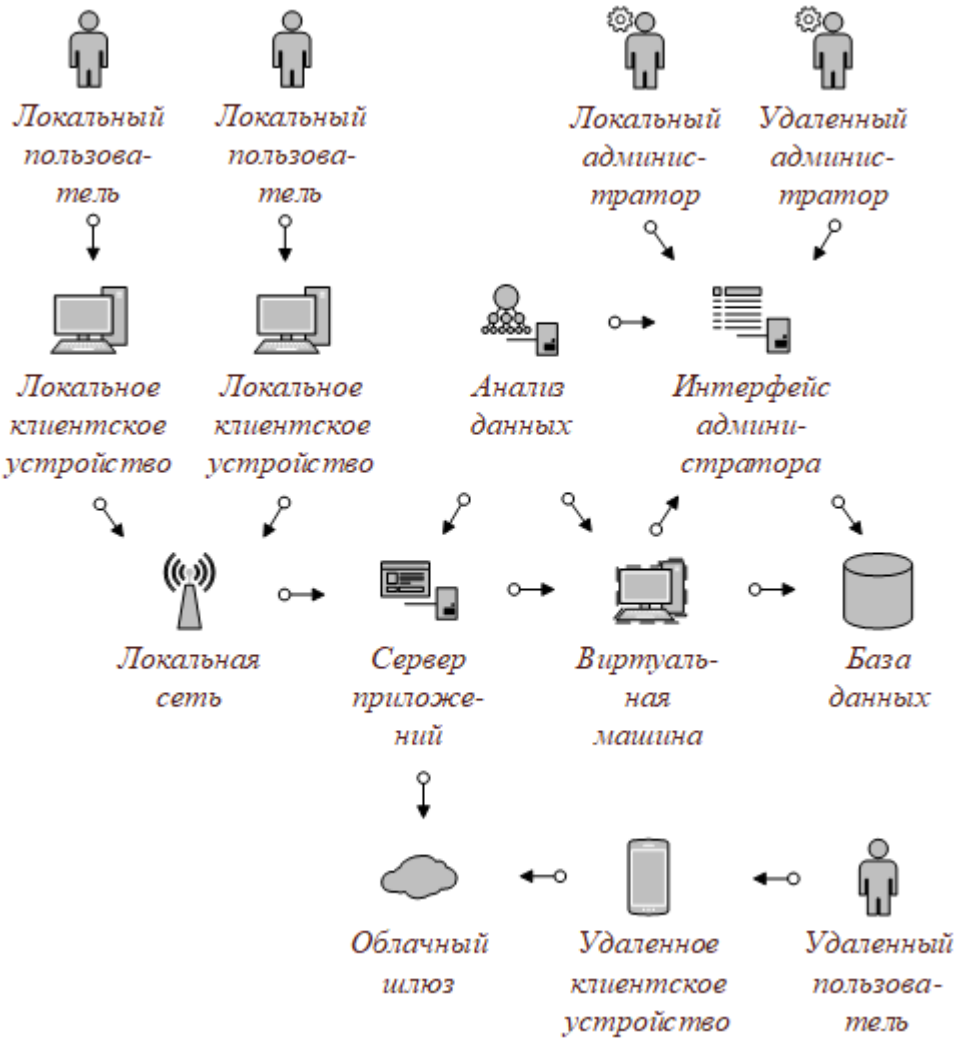

Рисунок 1 – Общая схема сетевого взаимодействия и информационных потоков для сетей Интернета вещей

3.2. Определение зон доверия в сетевой инфраструктуре. Выделим основные компоненты сетевой инфраструктуры для Интернета вещей:

1. *Компонент «Устройство» (пользователя или администратора)* – любое устройство, с которым может взаимодействовать пользователь (компьютер, смартфон, IP-камера видеонаблюдения, «умный» кардиостимулятор, «умные» часы и т.п.), имеют те или иные операционные системы, подключаются к локальной сети или сети Internet в подавляющем большинстве посредством беспроводных технологий. Следовательно, основное внимание необходимо уделить уязвимостям удаленного доступа этих устройств.

2. *Компонент «Полевой шлюз»* представляет собой устройство или программное обеспечение (в том числе серверное); безопасно пересылает данные между центром обработки данных и устройствами пользователей и администраторов; обнаруживает и управляет подключенными к «внутренней части» системами «Умного дома» (освещение, вентиляция, температурный режим и т.п.). В настоящее время полевые шлюзы являются высокомасштабируемыми устройствами и производятся Dell, Intel и др. компаниями.

Следовательно, полевые шлюзы подвержены, в первую очередь, уязвимости физического вторжения.

3. *Компонент «Облачный шлюз»* с точки зрения безопасности в первую очередь предназначен для изоляции от сетевого трафика подключенных к нему устройств и полевых шлюзов. Следовательно, компонент «Облачный шлюз» позволяет оперативно реализовать меры по снижению уязвимости физического вторжения и сокращает количество возможных атак в сети за счет уменьшения поверхности атаки.

Исходя из вышесказанного, разложение сетевой инфраструктуры на зоны доверия осуществляется исходя из определения, что каждая зона представляет собой периметр безопасности, в котором действует та или иная форма контроля доступа.

В качестве зон доверия определены:

1. *Локальный пользователь + устройство (Зд1);*
2. *Удаленный пользователь + устройство(Зд2);*
3. *Полевой шлюз (Зд3);*
4. *Облачный шлюз (Зд4);*
5. *Клиентская сторона приложения + виртуальная машина (Зд5)*;
6. *Серверная сторона приложения + База данных + Аппаратное обеспечение (Зд6);*
7. *Анализ данных (Зд7);*
8. *Администратор + устройство администратора (Зд8);*
9. *Шлюз администратора (Зд8).*
10. *Интерфейс администратора (Зд10).*

Тогда потоки данных, возникающие между зонами доверия:

1. *Зд1 ↔ Зд3*;
2. *Зд2 → Зд4*;
3. *Зд3 → Зд4*;
4. *Зд5, Зд6, Зд7→ Зд10*;
5. *Зд8 → Зд9*;
6. *Зд5, Зд6 → Зд7*

При входе пользователя или администратора на соответствующее устройство, это устройство аутентифицируется через процессы входа в систему и в дальнейшем может получить доступ к локальной сети или сети Интернет. Пользователь входит в облачное приложение, используя назначенное имя пользователя, пароль и при необходимости «второй фактор» аутентификации. Таким образом, данные, которые перемещаются между зонами, нуждаются в подтверждении целостности, которая может быть достигнута с помощью шифрования или применения виртуальных машин на серверах приложений (см. Рисунок 1).

3.3. Классификация устройств Интернета вещей по областям применения. В таблице 1 приведена предлагаемая классификация устройств Интернет вещей по областям применения, а именно: домашнее использование (системы «Умный дом), здравоохранение, транспорт, коммерция, финансы и машиностроение.

Каждое устройство относится к области применения в соответствии с пользовательскими приложениями. Кроме того, выделены продукты/экосистемы продуктов или устройства, использующиеся в основном отдельными людьми и образующие потребительский сектор, и применяемые отдельными компаниями или целыми отраслями и образующие коммерческий сектор.

Таблица 1 – Классификация устройств по областям использования

Область применения	*Примеры продуктов, систем или устройств*	*Потребительский сектор*	*Коммерческий сектор*
Домашнее использование	Amazon Alexa, Google Home, Amazon Echo, Cortana, Nest Thermostat, Nest Camera, Philips Hue	+	
Здравоохранение	Умный кардиостимулятор, Fitbit, Умная инсулиновая помпа	+	
Транспорт	Система автоматического торможения, Система автономного управления транспортным средством, Система мониторинга парка транспортных средств	+	+
Коммерция	Система Point of Sale, Система управления запасами, Система автономных сетей магазинов самообслуживания		+
Финансы	ATM, Venmo, Сбербанк		+
Промышленность	Система SCADA, PLC		+

1. К области *«Домашнее использование»* относятся продукты/устройства потребительского сектора, некоторые из которых содержат системы искуственного интеллекта и могут управлять другими устройствами Умного дома/Интернета вещей. Например, для устройств управления освещением Philips Hue или устройств управления температурой Nest имеется возможность централизованного интеллектуального управления с помощью умного шлюза и мобильного приложения. Большинство этих устройств не имеют высокого стандарта безопасности, что подразумевает наличие уязвимых мест сетевой инфраструктуры и возможность получения несанкционированного доступа ко всей сети.

2. К области *«Здравоохранение»* в настоящее время относятся продукты/устройства преимущественно потребительского сектора: интеллектуальные медицинские датчики, системы комплексного удаленного мониторинга, а также ассимиляции медицинских устройств. Например, широкое распространение получили умные кардиостимуляторы с возможностью подключения по Bluetooth или WiFi и передачей данных в ЦОД

медицинского учреждения и далее лечащему врачу. Отдельно следует отметить, что эти устройства производят большое количество данных, управление которыми может стать проблемой для ИТ-отдела ЦОД. Исходя из вышесказанного, передаваемые по беспроводным протоколам данные (особенно для сетей среднего радиуса действия) должны быть должным образом защищены.

3. К области *«Транспорт»* относятся продукты/устройства как потребительского, так и коммерческого сектора. В настоящее время электронные блоки управления, предназначенные для получения данных с датчиков и управления движением автомобиля (удерживание полосы движения, автоматическое торможение, распознавание дорожных знаков, определение положения транспортного средства и т.п.), а также головные мультимедийные устройства современных автомобилей содержат встроенное ПО, которое можно обновлять «по воздуху» и получать к нему доступ через облачные технологии. Это, например, позволяет производителям обновлять настройки, влияющие на топливную экономичность, загрязнение воздуха и т.п.

Данные устройства имеют более высокий уровень безопасности, обеспечиваемый производителем. Отметим, что в случае проникновения в инфраструктуру и в дальнейшем перехвата управления транспортным средством, изменения/нарушения алгоритмов функционирования датчиков или электронного бортового устройства могут повлечь возникновение опасности не только для владельца автомобиля, но и для всех участников дорожного движения.

4. К областям *«Коммерция»* и *«Финансы»* относятся продукты/устройства, разрабатываемые для использования в коммерческом секторе: интеллектуальные турникеты пропуска и терминалы точек продаж, датчики сбора, хранения и передачи данных о потребителях товаров (движение и точки останова в магазине), автономные сети магазинов самообслуживания, системы управления запасами; системы таргетированной рекламы, банковские терминалы и т.п. При этом программные продукты финансовой области тесно связаны с персональными устройствами потребителей услуг: клиенты проводят банковские транзакции с домашних (компьютеры, ноутбуки), мобильных (планшеты, смартфоны) и носимых умных устройств (фитнес-трекеры, умные часы), невидимые платежи за транспортные и ресторанные услуги (по примеру Uber, Dine and Dash, Dash Replenishment Service и др.).

Исходя из вышесказанного, торговые учреждения, банки и финансовые учреждения собирают информацию о клиентах, попадающую под действие Закона о защите персональных данных; любой тип утечки данных может привести к серьезным проблемам как для учреждения, так и для клиента. При этом точками несанкционированного проникновения и получения доступа в подавляющем большинстве являются оконечные и сетевые устройства потребителей услуг.

5. К области *«Промышленность»* относятся продукты/устройства, используемые в коммерческом секторе: системы управления производством (ICS), диспетчерский контроль и сбор данных (SCADA) и программируемые логические контроллеры (PLC). Данные системы предназначены либо для управления отдельным производственным оборудованием или включенным в состав технологических процессов, либо для обеспечения комфорта и безопасности персонала. Имеют высочайшую отказоустойчивость, однако системы управления, в основном, основаны на устаревших технологиях, и их достаточно сложно обновлять и исправлять. Отметим, что получение

несанкционированного доступа к устройствам данной области может повлечь выход из строя целых промышленных, сельскохозяйственных, транспортных, коммунальных инфраструктур и угрозу безопасности жизнедеятельности большого число людей.

3.4. Определение уязвимостей и атак для устройств Интернета вещей.

Ниже приведены известные уязвимости [10-16] для устройств и Интернета вещей, которые могут использоваться для проведения различных атак. Уязвимость определяется как недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации [17]. Атака – как целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [17].

Были определены следующие виды характерных уязвимостей:

1. *Жестко закодированный пароль (Уз1)*.
2. *Слабый или стандартный пароль (Уз2)*.
3. *Ошибка внедрения команд (Уз3)*.
4. *Открытые порты (Уз4)*.
5. *Отсутствие блокировки учетной записи (Уз5)*.
6. *Незашифрованные сервисы (Уз6)*.
7. *Небезопасный или вредоносный веб-интерфейс (Уз7)*.
8. *Небезопасные сетевые сервисы (Уз8)*.
9. *Небезопасный облачный интерфейс (Уз9)*.
10. *Перечисление учетных записей (Уз10)*.
11. *Межсайтовый скриптинг (Уз11)*.
12. *Переполнение буфера (Уз12)*.
13. *Удаление физического хранилища (Уз13)*.
14. *Отсутствует авторизация (Уз14)*.

На основе видов уязвимостей были определены характерные успешно выполняемые виды атак на устройства Умного дома и Интернета вещей [10-16]:

1. *Отказ в обслуживании (DoS) (А1)*.
2. *Ботнет (А2)*.
3. *Программы-вымогатели (А3).*
4. *Социальная инженерия (А4).*
5. *Атака «Человек посередине» (MITM)* (*А5*).
6. *Спуфинг (А6)*.
7. *Повышение привилегий (EOP) (А7).*
8. *Троянский конь SCADA систем (А8).*
9. *Mirai (А9).*
10. *Червь (А10).*
11. *Анализ пакетов (А11).*
12. *Атака через прокси SShowDowN (А12)*.

4. Результаты и их обсуждение. Исходя из выше представленного материала проведено сопоставление вида атаки, области атаки, цели атаки и уязвимостей для Интернета вещей. Результаты представлены в таблице 2. Она позволяет, определяя наиболее распространенные атаки, определить конкретные уязвимости, которые используют атаки, и найти способы защиты от них. В частности, обнаруживая, где происходит атака в сетевой архитектуре, таблица 2 позволяет легко выяснить, что подвергается атаке.

Были определены следующие возможные меры безопасности [18-26] для известных уязвимостей устройств Умного дома и Интернета вещей:

1. *Тайм-аут аккаунта (Мб1).*
2. *Блокировка учетной записи (Мб2).*
3. *Двухфакторная аутентификация (Мб3).*
4. *Сложность пароля (Мб4).*
5. *Настройка портов устройства (Мб5).*
6. *Управление обновлениями (Мб6).*
7. *Обнаружение / предотвращение вторжений (Мб7).*
8. *Шифрование данных (Мб8).*
9. «*Воздушный зазор» сетей передачи данных (Мб9).*
10. *Физическая безопасность (Мб10).*
11. *Защита от DoS-атак (Мб11).*
12. *Журналирование событий (Мб12).*
13. *Внешнее резервное копирование данных (Мб13).*
14. *Антивирусная защита (Мб14).*
15. *Тестирование на проникновение (Мб15).*
16. *Дезинфекция ввода (Мб16).*
17. *Подпись кода (Мб17).*
18. *Самозащита приложения во время выполнения (RASP) (Мб18).*

Таблица 2 – Виды атак с указанием их локализации, объектов, статуса и уязвимостей

Вид атаки	*Локализация атаки*	*Объект атаки*	*Статус данных*	*Уязвимость*
А1	Сервер	Сервер	Передача	Уз5, Уз9, Уз14
А2	Устройство пользователя	Устройство	Передача	Уз9, Уз10
А3	Устройство пользователя	Накопитель информации	-	Уз1, Уз2, Уз3, Уз6, Уз8, Уз9, Уз11, Уз12, Уз14
А4	Пользователь	Устройство	-	Уз13
А5	Вычислительная сеть	Пакет	Передача	Уз6, Уз7, Уз8, Уз9, Уз13

А6	Вычислительная сеть	Пакет	-	Уз6, Уз7, Уз8, Уз9
А7	Устройство пользователя	Устройство	-	Уз4
А8	Устройство пользователя	Устройство	Передача	Уз7, Уз11, Уз13
А9	Устройство пользователя	Устройство	Передача	Уз9, Уз10
А10	Устройство пользователя	Устройство	-	Уз9
А11	Вычислительная сеть	Пакет	Передача	Уз6, Уз8, Уз9
А12	Устройство пользователя	Устройство	Передача	Уз9, Уз10

В таблице 3 приведено итоговое сопоставление уязвимостей устройств Интернета вещей по областям применения и вида атак, использующих уязвимости, а также рекомендованы меры безопасности, ведущие к закрытию уязвимостей.

Таблица 3 – Сопоставление уязвимостей, атак и мер безопасности для областей применения устройств Интернета вещей

Область применения → Уязвимость	Уязвимость → Атака	Меры безопасности → Закрытая уязвимость
Домашнее использование → *Уз2, Уз3, Уз4, Уз6, Уз8, Уз9, Уз13*	*Уз9 → А2* *Уз2, Уз3, Уз4, Уз6, Уз8, Уз9 → А3* *Уз6, Уз8, Уз9, Уз13 → А6* *Уз4 → А7* *Уз13 → А8* *Уз9 → А9* *Уз9 → А10* *Уз6, Уз8, Уз9 → А11* *Уз9 → А12*	*Мб4 → Уз2, Уз10* *Мб8 → Уз6, Уз7, Уз13* *Мб5 → Уз4, Уз8* *Мб9 → Уз9* *Мб7 → Уз3, Уз7*
Здравоохранение → *Уз2, Уз3, Уз6, Уз7, Уз8, Уз9*	*Уз2, Уз3, Уз6, Уз8, Уз9 → А3* *Уз6, Уз7, Уз8, Уз9 → А5* *Уз7 → А8* *Уз9 → А10*	*Мб17 → Уз3, Уз7* *Мб8 → Уз6, Уз7, Уз13* *Мб5 → Уз4, Уз8* *Мб7 → Уз3, Уз7* *Мб9 → Уз9*
Транспорт → *Уз3, Уз4, Уз6, Уз7, Уз8, Уз9, Уз11, Уз12*	*Уз3, Уз6, Уз8, Уз9, Уз11, Уз12 → А3* *Уз4 → А7* *Уз9 → А10*	*Мб7 → Уз3, Уз7* *Мб9 → Уз9* *Мб5 → Уз4, Уз8* *Мб6 → Уз12* *Мб16→ Уз11*
Коммерция → *Уз3, Уз4, Уз6, Уз9, Уз12, Уз13*	*Уз3, Уз6, Уз12 → А3* *Уз6, Уз13 → А5* *Уз13 → А8* *Уз9 → А10*	*Мб7 → Уз3, Уз7* *Мб6 → Уз12* *Мб8 → Уз6, Уз7, Уз13* *Мб9 → Уз9* *Мб10→ Уз6*

Финансы → → *Уз2, Уз3, Уз4, Уз6, Уз9, Уз12, Уз13*	*Уз9 → А1* *Уз2, Уз3, Уз6, Уз9, Уз12 → А3* *Уз13 → А4* *Уз6, Уз9, Уз13 → А5* *Уз6, Уз9 → А6* *Уз9 → А10*	*Мб9 → Уз9* *Мб4 → Уз2, Уз10* *Мб6 → Уз12* *Мб8 → Уз6, Уз7, Уз13* *Мб7 → Уз3, Уз7*
Промышленность → → *Уз2, Уз3, Уз4, Уз6, Уз8, Уз9, Уз11, Уз12, Уз13*	*Уз9 → А2* *Уз2, Уз3, Уз6, Уз8, Уз9, Уз12 → А3* *Уз13 → А4* *Уз13 → А8* *Уз9 → А10*	*Мб9 → Уз9* *Мб4 → Уз2, Уз10* *Мб8 → Уз6, Уз7, Уз13* *Мб5 → Уз4, Уз8* *Мб7 → Уз3, Уз7* *Мб11 → Уз7, Уз11, Уз13*

Для устройств области «Домашнее использование» в первую очередь следует рекомендовать применение мер *Сложность пароля (Мб4), Настройка портов устройства (Мб5)*, Шифрование *данных (Мб8)*, «*Воздушный зазор» сетей передачи данных (Мб9)*, которые могут быть реализованы за счет встроенных возможностей самих устройств. Реализация меры *Обнаружение / предотвращение вторжений (Мб7)* влечет за собой дополнительные финансовые расходы и требует соответствующей квалификации пользователя.

Основная проблема устройств области «Здравоохранение» заключается в том, что на этих устройствах часто отсутствует какая-либо аутентификация для входа в систему, так как это устройства сетей ближнего радиуса действия (Bluetooth, NFC). Выполнение мер *Настройка портов устройства (Мб5)*, Обнаружение */ предотвращение вторжений (Мб7), Шифрование данных (Мб8)*, «*Воздушный зазор» сетей передачи данных (Мб9)* для этих устройств в настоящее время затруднительна, поэтому производителям следует обязательно выполнять меру *Подпись кода (Мб17)*. Это позволяет пользователю быть уверенными в происхождении программного обеспечения.

Для устройств областей применения «Транспорт», «Коммерция», «Финансы» и «Промышленность» в настоящее время возможно выполнение всех предложенных мер безопасности либо производителем устройств, либо пользователем (область применения «Транспорт») или квалифицированным специалистом в области информационной безопасности.

Заключение. С дальнейшим развитием, усложнением и распространением устройств Интернета вещей, а также программного обеспечения, ориентированного на Интернет вещей, необходимо обеспечивать надежную защиту от существующих и будущих атак. Предлагаемые меры безопасности устройств Интернета вещей являются в определенной мере комплексными и обеспечивают снижение рисков их внедрения по областям применения.

Список литературы.

1. Эванс Д. Интернет вещей. Как изменится вся наша жизнь на очередном витке развития Всемирной сети [Электронный ресурс] // Официальный сайт компании Cisco Systems: [сайт]. [2011]. URL://https://www.cisco.com/c/dam/global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf (дата обращения: 20.10.2021).
2. Калинин А. С. Интернет вещей. Принципы, технологии, перспективы развития [Электронный ресурс] // Молодой ученый. 2019. № 2 (240). С.341-342. URL:https://moluch.ru/archive/240/55473/ (дата обращения: 21.10.2021).
3. Власенко А. В. Безопасность интернета вещей [Электронный ресурс] // Молодой ученый. 2021. №21(363). С.86-89. URL:https://moluch.ru/archive/363/81232/ (дата обращения: 26.10.2021).
4. Черняк Л. Интернет вещей: новые вызовы и новые технологии [Электронный ресурс] // Открытые системы. 2013. №4. URL:http://www.osp.ru/os /2013/04/13035551. (дата обращения: 26.10.2021).
5. Нефедова М. Уязвимость в ZigBee ставит IoT-устройства под удар [Электронный ресурс] // Хакер. Факультет компьютерной опасности: [сайт]. [2015]. URL: https://xakep.ru/2015/08/10/zigbee-devices-problems/ (дата обращения: 27.10.2021).
6. Нефедова М. Автомобиль Tesla можно угнать, заразив смартфон его хозяина Malware [Электронный ресурс] // Хакер. Факультет компьютерной опасности: [сайт]. [2015]. URL:https://xakep.ru/2016/11/25/tesla-android-hack/ (дата обращения: 27.10.2021).
7. Информационная безопасность интернета вещей (Internet of Things) [Электронный ресурс] // TRADVISER. Государство. Бизнес. Технологии: [сайт]. [2011]. URL: https://www.tadviser.ru/Статья: Информационная_безопасность_интернета_вещей_(Internet_of_Things) (дата обращения: 27.10.2021).
8. Леонов А. В. Понятие «доверия» в Интернете вещей [Электронный ресурс] // Молодой ученый. 2015. №7(87). С.58-61. URL:https://moluch.ru/archive/87/16981/ (дата обращения: 28.10.2021).
9. Звягинцев Б. И. Обеспечение неприкосновенности частной жизни в беспроводных медицинских нательных вычислительных сетях [Электронный ресурс] // Молодой ученый. 2015. № 12 (92). С.183-186. URL: https://moluch.ru/archive/92/20436/ (дата обращения: 29.10.2021).
10. Петровский А. Эффективный хакинг для начинающих и не только. 3-е изд. М: Майор, 2001. 164 с.
11. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие. М.: Издательство МГТУ м. Н. Э. Баумана, 2016. 250, [2] с.
12. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы. СПб.: Символ-Плюс, 2009. 560 с.

13. Konheim A. Computer Security and Cryptography. USA: John Wiley & Sons, 2006. 522 p.
14. Graves K. Official Certified Ethical Hacker Review Guide: Exam 312-50 1st Edition. Duesseldorf: Sybex, 2007, 264 p.
15. Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. England: O'Reilly, 2017, 240 p.
16. Gupta A. The IoT Hacker's Handbook. A Practical Guide to Hacking the Internet of Things. Walnut, CA, USA: Apress, 2019. 320 p.
17. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов: [сайт]. [2016]. URL: https://docs.cntd.ru/document/1200123702 (дата обращения: 25.10.2021).
18. Михайлов Д., Жуков И. Защита мобильных телефонов от атак. М.: Фойлис, 2011. 192 с.
19. Security in the Internet of Things : A review // Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. 2012. P. 648-651.
20. Рекомендации по безопасности для развертывания Интернет вещей Azure (IoT) [Электронный ресурс] // Официальный сайт компании Microsoft: [сайт]. URL:https://docs.microsoft.com/ru-ru/azure/iot-fundamentals/security-recommendations (дата обращения: 24.11.2021).
21. Забула С. Как усилить безопасность интернета вещей (IoT) в организации [Электронный ресурс] // Anti-malware: [сайт]. [2021]. URL:https://www.anti-malware.ru/practice/solutions/How-to-strengthen-IoT-security (дата обращения: 26.11.2021).
22. Сексембаева М.А. Особенности обеспечения безопасности в промышленном Интернете вещей // E-SCIO. 2019. №5(32). С.383-395.
23. Орешкина Д. Эталонная архитектура безопасности интернета вещей (IoT). Часть 1 [Электронный ресурс] // Anti-malware: [сайт]. [2017]. https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 (дата обращения: 23.11.2021).
24. Орешкина Д. Эталонная архитектура безопасности интернета вещей (IoT). Часть 2 [Электронный ресурс] // Anti-malware: [сайт]. [2017]. https://www.anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2 (дата обращения: 24.11.2021).
25. IoT Security Maturity Model (SMM): Description and Intended Use [Электронный ресурс] // Industry IoT Consortium: [сайт]. [2020]. URL:https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf (дата обращения: 05.11.2021).
26. IoT Security Maturity Model (SMM): Practitioner's Guide [Электронный ресурс] // Industry IoT Consortium: [сайт]. [2020]. URL:

https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf (дата обращения: 15.11.2021).

References.

1. Evans D. Internet veshchej. Kak izmenitsya vsya nasha zhizn' na ocherednom vitke razvitiya Vsemirnoj seti [Electronic resource] // Oficial'nyj sajt kompanii Cisco Systems: [site]. [2011]. URL://https://www.cisco.com/c/dam /global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf (date of access: 20.10.2021). (in Russian).
2. Kalinin A. S. Internet veshchej. Principy, tekhnologii, perspektivy razvitiya [Electronic resource] // Molodoj uchenyj. 2019. № 2 (240). P.341-342. URL:https://moluch.ru/archive/240/55473/ (date of access: 21.10.2021).
3. Vlasenko A. V. Bezopasnost' interneta veshchej [Electronic resource] // Molodoj uchenyj. 2021. №21(363). P.86-89. URL:https://moluch.ru/archive/363 /81232/ (date of access: 26.10.2021). (in Russian).
4. Chernyak L. Internet veshchej: novye vyzovy i novye tekhnologii [Electronic resource] // Otkrytye sistemy. 2013. №4. URL:http://www.osp.ru/os /2013/04/13035551. (date of access: 26.10.2021). (in Russian).
5. Nefedova M. Uyazvimost' v ZigBee stavit IoT-ustrojstva pod udar [Electronic resource] // Haker. Fakul'tet komp'yuternoj opasnosti: [site]. [2015]. URL: https://xakep.ru/2015/08/10/zigbee-devices-problems/ (date of access: 27.10.2021). (in Russian).
6. Nefedova M. Avtomobil' Tesla mozhno ugnat', zaraziv smartfon ego hozyaina Malware [Electronic resource] // Haker. Fakul'tet komp'yuternoj opasnosti: [site]. [2015]. URL:https://xakep.ru/2016/11/25/tesla-android-hack/ (date of access: 27.10.2021). (in Russian).
7. Informacionnaya bezopasnost' interneta veshchej (Internet of Things) [Electronic resource] // TRADVISER. Gosudarstvo. Biznes. Tekhnologii: [site]. [2011]. URL: https://www.tadviser.ru/Stat'ya:Informacionnaya_bezopasnost' _interneta_veshchej_(Internet_of_Things) (date of access: 27.10.2021). (in Russian).
8. Leonov A. V. Ponyatie «doveriya» v Internete veshchej [Electronic resource] // Molodoj uchenyj. 2015. №7(87). P.58-61. URL:https://moluch.ru /archive/87/16981/ (date of access: 28.10.2021). (in Russian).
9. Zvyagincev B. I. Obespechenie neprikosnovennosti chastnoj zhizni v besprovodnyh medicinskih natel'nyh vychislitel'nyh setyah [Electronic resource] // Molodoj uchenyj. 2015. № 12 (92). P.183-186. URL: https://moluch.ru /archive/92/20436/ (date of access: 29.10.2021). (in Russian).
10. Petrovskij A. Effektivnyj haking dlya nachinayushchih i ne tol'ko. 3-e izd. Moscow: Major, 2001. 164 p. (in Russian).

11. Bondarev V.V. Vvedenie v informacionnuyu bezopasnost' avtomatizirovannyh sistem: uchebnoe posobie. Moscow: BMSTU Publishing, 2016. 250, [2] p. (in Russian).
12. Satton M., Grin A., Amini P. Fuzzing: issledovanie uyazvimostej metodom gruboj sily. Saint-Petersburg: Simvol-Plyus, 2009. 560 p. (in Russian).
13. Konheim A. Computer Security and Cryptography. USA: John Wiley & Sons, 2006. 522 p.
14. Graves K. Official Certified Ethical Hacker Review Guide: Exam 312-50 1st Edition. Duesseldorf: Sybex, 2007, 264 p.
15. Smith S. The Internet of Risky Things: Trusting the Devices That Surround Us. England: O'Reilly, 2017, 240 p.
16. Gupta A. The IoT Hacker's Handbook. A Practical Guide to Hacking the Internet of Things. Walnut, CA, USA: Apress, 2019. 320 p.
17. GOST R 56546-2015. Zashchita informacii. Uyazvimosti informacionnyh sistem. Klassifikaciya uyazvimostej informacionnyh sistem [Electronic resource] // Elektronnyj fond pravovyh i normativno-tekhnicheskih dokumentov: [site]. [2016]. URL: https://docs.cntd.ru/document/1200123702 (date of access: 25.10.2021). (in Russian).
18. Mihajlov D., ZHukov I. Zashchita mobil'nyh telefonov ot atak. Moscow: Fojlis, 2011. 192 p. (in Russian).
19. Security in the Internet of Things : A review // Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. 2012. P. 648-651.
20. Rekomendacii po bezopasnosti dlya razvertyvaniya Internet veshchej Azure (IoT) [Electronic resource] // Oficial'nyj sajt kompanii Microsoft: [site]. URL:https://docs.microsoft.com/ru-ru/azure/iot-fundamentals/security-recommendations (date of access: 24.11.2021). (in Russian).
21. Zabula S. Kak usilit' bezopasnost' interneta veshchej (IoT) v organizacii [Electronic resource] // Anti-malware: [site]. [2021]. URL:https://www.anti-malware.ru/practice/solutions/How-to-strengthen-IoT-security (date of access: 26.11.2021). (in Russian).
22. Ceksembaeva M.A. Osobennosti obespecheniya bezopasnosti v promyshlennom Internete veshchej // E-SCIO. 2019. №5(32). P.383-395. (in Russian).
23. Oreshkina D. Etalonnaya arhitektura bezopasnosti interneta veshchej (IoT). Chast' 1 [Electronic resource] // Anti-malware: [site]. [2017]. https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 (date of access: 23.11.2021). (in Russian).
24. Oreshkina D. Etalonnaya arhitektura bezopasnosti interneta veshchej (IoT). Chast' 2 [Electronic resource] // Anti-malware: [site]. [2017]. https://www.anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2 (date of access: 24.11.2021). (in Russian).
25. IoT Security Maturity Model (SMM): Description and Intended Use [Э Electronic resource] // Industry IoT Consortium: [site]. [2020].

URL:https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf (date of access: 05.11.2021).

26. IoT Security Maturity Model (SMM): Practitioner's Guide [Electronic resource] // Industry IoT Consortium: [site]. [2020]. URL: https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf (date of access: 15.11.2021).