**УДК 004.738.5**
**ББК 32.372**
**Ч18**

*Спасибо за помощь в подготовке книги*
*Юрию Владимировичу Потапову,*
*техническому директору ООО «Евроинтех»*

**Чанцис Ф., Стаис И., Кальдерон П., Деирменцоглу Е., Вудс Б.**
Ч18 Практический хакинг интернета вещей / пер. с англ. Л. Н. Акулич. – М.: ДМК Пресс, 2022. – 480 с.: ил.

**ISBN 978-5-97060-974-3**

Устройств, управляемых через интернет, с каждым годом становится больше, но не все грамотно оценивают сопутствующие риски. Из этой книги читатель узнает, каким образом подключать умную технику у себя дома и на предприятиях, чтобы наилучшим образом себя обезопасить. Авторы подробно описывают уязвимости в сфере интернета вещей (IoT), моделируют угрозы и представляют эффективную методологию тестирования умных устройств – от инфузионной помпы до беговой дорожки. Практические упражнения научат вовремя распознавать угрозы и предотвращать атаки злоумышленников.

Издание будет полезно тестировщикам безопасности, системным администраторам, а также разработчикам и пользователям IoT-систем.

УДК 004.738.5
ББК 32.372



ISBN 978-1-7185-0090-7 (англ.)
ISBN 978-5-97060-974-3 (рус.)

# СОДЕРЖАНИЕ

## Часть II ВЗЛОМ СЕТИ

# Об авторах

**Фотиос (Фотис) Чанцис** (@ithilgore) работает над безопасным и надежным общим искусственным интеллектом (AGI) в OpenAI. Прежде он занимал должность главного инженера по информационной безопасности в Mayo Clinic, где проводил техническую оценку безопасности медицинских устройств, систем клинической поддержки и критически важной инфраструктуры здравоохранения. С 2009 года входил в основную команду разработчиков Nmap, написал Ncrack под руководством Гордона «Федора» Лайона, автора исходной версии Nmap, в ходе инициативной программы Google Summer of Code. Впоследствии выступал наставником в проекте Nmap во время Google Summer of Code 2016 и 2017 года, создал видеокурс по Nmap. Исследование сетевой безопасности Фотиса Чанциса включает использование TCP Persist Timer (вы можете найти его статью по теме, опубликованную в Phrack № 66) и изобретение скрытой атаки со сканированием портов путем злоупотребления протоколом XMPP. Фотис участвовал в различных конференциях по безопасности, включая DEF CON. Основные его работы представлены на его сайте *https://sock-raw.org/*.

**Иоаннис Стаис** (@Einstais) – старший исследователь в области ИТ-безопасности и руководитель красной команды CENSUS S.A. – компании, предлагающей специализированные услуги в области кибербезопасности клиентам по всему миру. Иоаннис участвовал более чем в 100 проектах по оценке безопасности, включая оценку протоколов связи, сетевых и мобильных банковских услуг, платежных систем NFC, банкоматов и систем точек продаж, критически значимого медицинского оборудования и решений MDM. Получил степень магистра в области компьютерных систем в Афинском университете. В настоящее время исследования Иоанниса сосредоточены на разработке алгоритмов машинного обучения для улучшения анализа уязвимостей, на усовершенствовании фреймворков для исследования уязвимостей методом грубой силы и изучении современных угроз мобильным и веб-приложениям. Иоаннис Стаис представлял свои исследования на конференциях по безопасности, таких как Black Hat Europe, Troopers NGI и Security BSides Athens.

## О соавторах

**Паулино Кальдерон** (@calderpwn) – автор публикаций и международный спикер, более 12 лет работающий в области безопасности сетей и приложений. Он выступает на конференциях по безопасности и вместе со специалистами Websec – фирмы, основанной им в 2011 году – консультирует компании из списка Fortune 500, а свободное от работы время проводит в блаженном отдыхе на пляжах Косумеля (Мексика). Паулино – большой почитатель программного обеспечения с открытым исходным кодом и участвовал во многих проектах, включая Nmap, Metasploit, OWASP Mobile Security Testing Guide (MSTG), OWASP Juice Shop и OWASP IoT Goat.

**Евангелос Деирменцоглу** (@edeirme) – специалист по информационной безопасности, интересующийся решением масштабных проблем защиты. Руководил работой по обеспечению кибербезопасности финансового технологического стартапа Revolut. Член Сообщества свободно распространяемого ПО с 2015 года; внес вклад в разработку Nmap и Ncrack. В настоящее время пишет диссертацию по кибербезопасности, уделяя особое внимание анализу исходного кода, который он применял в работе со многими крупными поставщиками технологий США, компаниями из списка Fortune 500, финансовыми и медицинскими учреждениями.

**Бо Вудс** (@beauwoods) – научный сотрудник по инновациям в области кибербезопасности в Атлантическом совете, лидер движения I Am The Cavalry. Основатель и генеральный директор Stratigos Security; входит в правление ряда некоммерческих организаций. В своей работе, которая призвана наладить контакт между сообществами, занимающимися исследованием безопасности, и сообществами публичных политик, он стремится к тому, чтобы любая сетевая технология, способная укрепить безопасность человека, заслуживала доверия. В прошлом сотрудник Управления по санитарному надзору за качеством пищевых продуктов и медикаментов США, главный управляющий консультант Dell SecureWorks. Последние несколько лет проводит консультации в сфере энергетики, здравоохранения, автомобилестроения, авиации, железнодорожного транспорта и интернета вещей; сотрудничает с исследователями кибербезопасности, разработчиками ИТ-политик и Белым домом. Является автором ряда публикаций, часто выступает на публичных мероприятиях.

## О техническом обозревателе

**Аарон Гусман** (Aaron Guzman) – один из авторов «Руководства по тестированию безопасности интернета вещей», технический руководитель группы безопасности Cisco Meraki. В рамках проектов OWASP IoT и Embedded Application Security возглавляет инициативы с открытым исходным кодом, которые повышают осведомленность о стратегиях защиты интернета вещей и тем самым снижают порог входа в отрасль защиты IoT для специалистов. Аарон Гусман – сопредседатель рабочей группы Cloud Security Alliance по IoT и технический рецензент ряда книг по безопасности интернета вещей. Имеет широкий опыт публичных выступлений, проводя презентации на конференциях, тренинги и семинары по всему миру. Следите за исследованиями Аарона в Твиттере: @scriptingxss.

# ВСТУПИТЕЛЬНОЕ СЛОВО

Современные программы безопасности предназначены для борьбы с традиционными угрозами на предприятии. Но технологии развиваются с такой скоростью, что выявлять утечку данных организации становится все труднее.

Рождение интернета вещей в одночасье превратило традиционные производственные предприятия в компании по разработке программного обеспечения. Они начали комбинировать интегрированное аппаратное обеспечение и ПО для повышения эффективности своих продуктов, обновлений, простоты использования и ремонтопригодности. Используемые, как правило, в важных инфраструктурах – дома или в корпоративных сетях, – эти устройства предоставили новый ряд функций и приспособлений, облегчающих нашу жизнь.

Однако эти «черные ящики» принесли нам и новые испытания. Созданные специалистами, продумывающими лишь техническую сторону, они почти не интегрируются в систему безопасности. Они подвергли нашу жизнь новым угрозам и предоставили входы в инфраструктуру, которой раньше не было. Такие устройства до сих пор практически не отслеживаются и содержат ряд уязвимостей, так что мы часто не замечаем вторжения в их работу. При выявлении угроз организации подобные устройства не принимаются в расчет – часто их даже не отмечают в списке оборудования, подлежащего внутренней проверке безопасности.

«Практический хакинг интернета вещей» – это не просто очередная книга по безопасности: здесь обсуждается философия тестирования безопасности и показывается, как нам нужно изменить свое отношение к подключению техники у себя дома и на предприятиях, чтобы наилучшим образом себя обезопасить. Многие компании-производители не учитывают вопросов безопасности при разработке, а в результате создаваемые системы очень уязвимы для атак. Такие

устройства можно найти почти в каждой сфере нашей жизни. Интернет вещей влияет на все отрасли и компании, создавая риск, с которым большинство организаций не в состоянии справиться.

Большинство людей не вполне понимает, какие риски таят в себе устройства интернета вещей. Принято считать, что раз они не содержат конфиденциальной информации, то и не критичны для компании. На самом деле злоумышленники используют эти устройства в качестве скрытых каналов в сети, которые остаются незамеченными в течение долгого времени и ведут непосредственно к уязвимым данным. Приведу пример из личной практики. Недавно я участвовал в расследовании инцидента на крупном производственном предприятии. Мы обнаружили, что злоумышленники проникли в организацию через программируемый логический контроллер (ПЛК). Один из заводов-производителей привлекал стороннего подрядчика для изготовления устройств, и злоумышленники получили доступ к системам этого подрядчика. В результате более двух лет они могли распоряжаться всей информацией о клиентах и данными компании, о чем никто не догадывался.

ПЛК был точкой входа в остальную часть сети и в конечном счете открывал прямой доступ ко всем системам исследований и разработок компании, которые содержали большую часть интеллектуальной собственности и уникальных данных. Атака была обнаружена только потому, что один из злоумышленников по небрежности сбросил имена пользователей и пароли контроллера домена, что вызвало случайный сбой системы, потребовавший расследования.

Авторы книги «Практический хакинг интернета вещей» в первую очередь фокусируются на понимании рисков и уязвимостей, моделируя угрозы и описывая эффективную методологию тестирования устройств интернета вещей. Книга повествует о хакинге оборудования, сети, радио и всей инфраструктуры интернета вещей, а также о том, как анализировать выявленные риски путем технической оценки устройств. При описании методов тестирования устройств, входящих в систему интернета вещей, подробно рассказывается, что нужно для создания программы тестирования в организации и как проводить проверку. Эта книга призвана изменить методы оценки безопасности в большинстве организаций и помочь лучше понять риски – тестирование устройств интернета вещей рассматривается как часть этого процесса.

Рекомендую книгу всем техническим специалистам, которые производят устройства интернета вещей, а также всем, кто пользуется таковыми дома или на предприятии. Поскольку безопасность систем и защита информации сегодня важны как никогда, актуальность этой книги очевидна. Я искренне рад ее появлению, учитывая, какая работа за этим стоит, и уверен, что она поспособствует разработке более безопасной инфраструктуры интернета вещей в будущем.

Дэйв Кеннеди,
основатель TrustedSec, Binary Defense

# ПРЕДИСЛОВИЕ

Наша зависимость от технологий растет более быстрыми темпами, чем наша способность защитить их. Технологии, которые, как мы знаем, не застрахованы от вторжения злоумышленников, каждый день везут нас на работу, обслуживают медучреждения, наблюдают за нашими домами… Как доверять этим устройствам, если они не вполне надежны?

Аналитик по кибербезопасности Керен Элазари сказала, что хакеры – это «иммунная система цифровой эры». Нам нужны технически подкованные люди, которые могут выявлять уязвимости и информировать и защищать общество от ущерба, связанного со взломом интернет-систем. Никогда еще эта работа не была настолько актуальна: слишком немногие располагают необходимыми знаниями, навыками и инструментами[1].

Эта книга призвана укрепить иммунную систему общества, чтобы лучше защитить всех нас.

## Подход, принятый в книге

Хакинг в сфере интернета вещей – очень широкая тема, и в книге используется практический подход к ней. Мы фокусируемся на концепциях и методах, которые помогут вам быстро приступить к тес-

---

[1] Россия принимает активное участие в развитии международной экосистемы интернета вещей. В феврале 2022 г. официально опубликован первый международный стандарт промышленного интернета вещей, разработка которого велась по инициативе «Ростелекома» на базе технического комитета (ТК) по стандартизации 194 «Кибер-физические системы» Росстандарта при поддержке Минпромторга России. Стандарт станет платформой для развития Национальной технологической инициативы (НТИ) и цифровой экономики. Его утверждение состоялось на уровне ключевых организаций — Международной организации по стандартизации и Международной электротехнической комиссии (ISO/IEC). *https://iotas.ru/media/day_theme/1365/*.

тированию реальных систем, протоколов и устройств интернета вещей. Мы специально выбрали для примера инструменты и уязвимые устройства, широко распространенные и доступные по цене, чтобы вы могли практиковаться самостоятельно.

Мы также подготовили образцы кода и эксплойты, с которыми вы можете поэкспериментировать. Они доступны на веб-сайте книги по адресу *https://nostarch.com/practical-iot-hacking/*. Для удобства изучения некоторые упражнения сопровождаются образами виртуальных машин. В некоторых главах мы ссылаемся на популярные примеры с открытым исходным кодом, которые легко найти в интернете.

Перед вами не руководство по применению средств для взлома интернета вещей – книга не охватывает все аспекты безопасности интернета вещей, поскольку для этого понадобился бы труд куда большего масштаба. Поэтому мы взяли для рассмотрения самые основные методы взлома оборудования, включая взаимодействие с UART, $I^2C$, SPI, JTAG и SWD. Мы анализируем различные сетевые протоколы интернета вещей, уделяя особое внимание тем, которые не просто важны, но и мало исследовались ранее. Среди них UPnP, *WS-Discovery*, mDNS, DNS-SD, RTSP / RTCP / RTP, LoRa / LoRaWAN, Wi-Fi и Wi-Fi Direct, RFID и NFC, BLE, MQTT, CDP и DICOM. Также мы обсуждаем реальные примеры, с которыми сталкивались в ходе профессионального тестирования.

## Для кого предназначена эта книга

Не существует двух людей с одинаковыми воззрениями и опытом. Между тем анализ устройств интернета вещей требует навыков практически во всех областях, потому что эти устройства сочетают в себе вычислительную мощность и возможности подключения в самом разном рабочем окружении. Мы не можем предугадать, какие главы и фрагменты книги читатель сочтет наиболее интересными. Но полагаем, что предоставление этих знаний широким слоям населения обеспечит больший контроль пользователей над стремительно цифровизирующимся миром.

Мы написали книгу для тех, кто профессионально занимается взломом и проникновением в системы (так называемых тестировщиков безопасности), но ожидаем, что она будет полезна и другим людям:

- **исследователь систем безопасности** может использовать книгу как справочник, разбираясь с незнакомыми протоколами, структурами данных, компонентами и концепциями инфраструктуры интернета вещей;
- **системный администратор** предприятия узнает, как лучше защитить рабочую среду и активы своей организации;
- **менеджер по продукции** ознакомится с новыми ожиданиями клиентов в отношении устройств интернета вещей и сможет учесть это при разработке, уменьшив стоимость продукта и сократив время его вывода на рынок;

- **специалист по оценке безопасности** откроет для себя новые навыки, чтобы лучше обслуживать клиентов;
- **любознательный студент** найдет знания, которые помогут ему выстроить карьеру в области, связанной с защитой людей.

Настоящая книга написана в расчете на то, что читатель умеет работать с командной строкой Linux, знаком с сетевыми концепциями TCP/IP и кодированием. При необходимости вы можете обратиться к дополнительным материалам по взлому аппаратного обеспечения, таким как книга *The Hardware Hacking Handbook* (Colin O'Flynn, Jasper van Woudenberg; готовится к выходу в издательстве No Starch Press). Ссылки на дополнительную литературу вы встретите ниже в некоторых главах.

## Kali Linux

В большинстве упражнений, представленных в книге, используется Kali Linux – самый популярный дистрибутив Linux для тестирования на взлом. Kali поставляется с различными инструментами командной строки, каждому из которых мы уделим внимание при освещении определенных тем. Если вы не разбираетесь в операционной системе, рекомендуем прочитать книгу OccupyTheWeb. Linus Basics for Hackers (No Starch Press, 2019) и изучить материалы на сайте *https://kali.org/*, а также пройти бесплатный курс *https://kali.training/*.

Чтобы установить Kali, воспользуйтесь инструкциями на сайте *https://www.kali.org/docs/installation/*. Для установки подойдет любая актуальная версия, однако имейте в виду, что большинство упражнений для версий Kali, обновляемых в период с 2019 по 2020 год. Вы можете попробовать старые образы Kali на *http://old.kali.org/kali-images/*, если у вас возникли проблемы с установкой какого-либо инструмента. В новых версиях Kali по умолчанию устанавливаются не все инструменты, но вы можете добавить их с помощью метапакета kali-linux-large. Чтобы установить его, введите в терминале команду:

```
$ sudo apt install kali-linux-large
```

Мы также рекомендуем запускать Kali на виртуальной машине. Подробные инструкции вы найдете на веб-сайте Kali, а на различных онлайн-ресурсах рассказывается, как это сделать с помощью VMware, VirtualBox или других технологий виртуализации.

## Структура книги

Книга состоит из 15 глав, которые условно разделены на пять частей. В основе своей главы независимы друг от друга, но в некоторых из них приводятся ссылки на инструменты или концепции, представленные

выше. Поэтому, хотя мы стремились сделать большинство глав автономными, рекомендуем читать книгу последовательно.

**Часть I «Угрозы в мире интернета вещей»**

**Глава 1 «Безопасность интернета вещей»** – это своеобразный пролог: здесь рассказывается, почему важна безопасность интернета вещей и каковы особенности хакинга в этой сфере.

**Глава 2 «Моделирование угроз»** объясняет, как моделировать атаки на системы интернета вещей и какие распространенные угрозы вы можете обнаружить, на примере инфузионной помпы и ее компонентов.

**Глава 3 «Методология тестирования безопасности»** предоставляет базовые знания для комплексной оценки безопасности вручную на всех уровнях систем интернета вещей.

**Часть II «Взлом на уровне сети»**

**Глава 4 «Оценка сети»** показывает, как выполнять переключение VLAN в сетях IoT, идентифицировать устройства IoT в сети и взломать механизм аутентификации MQTT с помощью Ncrack-модуля.

**Глава 5 «Анализ сетевых протоколов»** посвящена методологии работы с незнакомыми сетевыми протоколами. Рассматривается процесс разработки анализатора Wireshark и модуля Nmap Scripting Engine для протокола *DICOM*.

**Глава 6 «Использование сети с нулевой конфигурацией»** исследует сетевые протоколы, используемые для автоматизации развертывания и настройки систем IoT. Описываются атаки на UPnP, mDNS, DNS-SD и WS-Discovery.

**Часть III «Взлом аппаратной части системы»**

**Глава 7 «Уязвимости портов UART, JTAG и SWD»** посвящена внутренней работе UART и JTAG/SWD. Вы узнаете, как определить на плате контакты UART и JTAG и взломать защиту микроконтроллера STM32F103 с помощью UART и SWD.

**Глава 8 «SPI и $I^2C$»** объясняет, как использовать два протокола шины с различными инструментами для атаки на встроенные устройства IoT.

**Глава 9 «Взлом прошивки»** показывает, как извлечь и проанализировать прошивку для организации доступа через бэкдор, а также изучить распространенные уязвимости в процессе обновления прошивки.

**Часть IV «Взлом радиоканалов»**

**Глава 10 «Радио ближнего действия: взлом rFID»:** злоупотребление RFID демонстрирует различные атаки на системы RFID, такие как чтение и клонирование карт доступа.

**Глава 11 «Bluetooth Low Energy (BLE)»** на примере простых упражнений показывает, как атаковать протокол Bluetooth Low Energy.

**Глава 12 «Радиоканал среднего дальности: взлом Wi-Fi»** освещает атаки на беспроводных клиентов через Wi-Fi, способы злоупотребления Wi-Fi Direct и распространенные атаки на точки доступа Wi-Fi.

**Глава 13 «Радио дальнего действия: LPWAN»** содержит основы изучения протоколов LoRa и LoRaWAN, показывая, как захватывать и декодировать эти типы пакетов, и освещает распространенные атаки на них.

**Часть V «Атаки на экосистему IoT»**

**Глава 14 «Взлом мобильных приложениий»** рассматривает распространенные угрозы, проблемы безопасности и методы тестирования мобильных приложений на платформах Android и iOS.

**Глава 15 «Взлом умного дома»** представляет практическое воплощение многих идей, рассматриваемых на протяжении книги, с описанием методов обхода умных дверных замков, подавления сигналов в беспроводных системах сигнализации и просмотра изображения с IP-камер. Кульминация главы – рассмотрение реального примера перехвата контроля над умной беговой дорожкой.

В **приложении «Инструменты для взлома интернета вещей»** содержится список популярных инструментов для атак на устройства, входящие в систему интернета вещей, – как рассмотренных в книге, так и других распространенных средств.

## Контакты

Мы всегда заинтересованы в получении отзывов и готовы ответить на любые ваши вопросы. Вы можете использовать адрес электронной почты errata@nostarch.com, чтобы уведомлять нас об ошибках, когда вы их обнаружите, и ithilgore@sock-raw.org для общих отзывов.

# ЧАСТЬ I

## УГРОЗЫ В МИРЕ ИНТЕРНЕТА ВЕЩЕЙ

# 1

# БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ

Если вы проживаете в многоквартирном доме, то вас наверняка окружают предметы *интернета вещей* (the Internet of Things – IoT). По улице ежечасно проносятся сотни «компьютеров на колесах», каждый из которых напичкан датчиками, процессорами и сетевым оборудованием. Многоэтажные здания утыканы множеством антенн и тарелок, подключенных к интернету и объединяющих в сеть персональных помощников, умные микроволновые печи, термостаты. Где-то в вышине мобильные центры обработки и хранения данных передают информацию на скорости сотни километров в час, оставляя след данных шире, чем инверсионный след самолета. Посетите завод, больницу или магазин электроники – и вас удивит, насколько широко распространились устройства, работающие по интернету.

Учитывая, что даже специалисты очень по-разному трактуют понятие «интернет вещей», в данной книге мы будем подразумевать под ним физические устройства, имеющие функциональность компьютера, способные передавать данные по сети и не требующие взаимодействия человека с компьютером. Некоторые люди дают устройствам интернета описательное и в принципе верное определение: «почти компьютеры, но не совсем». Нередко к названию устройства интерне-

та вещей добавляют слово «умный» – например, «умная микроволновая печь», – несмотря на то, что многие считают это неоправданным. (Смотрите статью Lauren Goode «Everything is connected, and there's no going back». *The Verge, 2018*. Вряд ли в скором времени появится более авторитетное определение интернета вещей.)

Для хакеров инфраструктура интернета вещей – это мир возможностей: миллиарды соединенных друг с другом устройств, передающих и раздающих данные, создают огромную площадку для проведения экспериментов, изготовления, использования систем и их выведения на предельные значения. И прежде чем погрузиться в технические детали хакинга и защиты интернета вещей, мы поговорим о безопасности интернета вещей как таковой – проанализируем правовые, практические и личные ее аспекты.

## Почему важна защита интернета вещей?

Возможно, вы в курсе статистики: к 2025 году появятся десятки миллиардов новых устройств интернета вещей, благодаря чему мировой ВВП увеличится на десятки триллионов долларов. Но это произойдет, только если все пойдет по плану и новые устройства будут раскуплены моментально. Пока же мы видим, что проблемы безопасности, защиты, конфиденциальности данных и надежности сдерживают распространение. Проблемы безопасности могут влиять на покупку не меньше, чем цена устройства.

Медленное развитие индустрии интернета вещей обусловлено не только экономическими причинами. Устройства интернета вещей могут облегчить жизнь во многих сферах. В 2016 году на автодорогах США погибло 37 416 человек, и, по данным Национального управления безопасностью движения на трассах, в 94 % случаев причиной был человеческий фактор. Автономный транспорт мог бы радикально снизить число аварий и сделать дороги безопаснее – при условии, что он будет надежным.

В других сферах нашей жизни мы также ожидаем преимуществ от внедрения инновационных технологий. Например, кардиостимуляторы, ежедневно отправляющие данные врачу, могут значительно уменьшить смертность от сердечных приступов. Тем не менее в дискуссии, проведенной Обществом сердечного ритма, доктор министерства по делам ветеранов США отметила, что ее пациенты отказываются от устройств-имплантов, опасаясь взлома. Многие работники производства, сотрудники госорганов и исследователи безопасности полагают, что из-за кризиса доверия развитие жизненно важных технологий задержится на годы или десятилетия.

Естественно, когда технологии активно внедряются в нашу жизнь, мы должны твердо знать (а не просто предполагать), что они оправдают доверие. Согласно исследованию отношения потребителей к интернету вещей, инициированному правительством Великобритании, 72 % респондентов были убеждены, что в таких устройствах

уже предусмотрена система защиты. Между тем для солидной части производителей безопасность устройств интернета вещей является второстепенным фактором.

В октябре 2016 года состоялись атаки ботнета Mirai, вызвавшие озабоченность правительства Соединенных Штатов и других государств. Эти возрастающие серии атак были направлены на сотни тысяч недорогих устройств, используемых в личных целях, и использовали распространенные пароли заводских настроек, наподобие **admin**, **password** и **1234**. В конечном счете это повлекло за собой *распределенную атаку на отказ в обслуживании* (Distributed Denial of Service, DDoS), направленную на систему доменных имен (Domain Name System, DNS) провайдера Dyn, обслуживающего многих американских гигантов, таких как Amazon, Netflix, Twitter, the Wall Street Journal, Starbucks и др. Атака на клиентов, доход и репутацию длилась более восьми часов.

Многие посчитали, что это дело рук хакеров, работающих на другие государства. За Mirai вскоре последовали атаки WannaCry и NotPetya, совокупный ущерб от которых составил триллионы долларов – в том числе из-за взлома систем интернета вещей, используемых на объектах жизнеобеспечения и на производстве. У правительства появился повод задуматься, насколько хорошо оно защищает своих граждан. По своей сути WannaCry и NotPetya представляли атаки с целью вымогательства, запускавшие эксплойт EternalBlue, нацеленный на компьютерную уязвимость в Windows – реализацию сетевого протокола прикладного уровня SMB (Server Message Block). К декабрю 2017 года, когда выяснилось, что Mirai разработала и привела в действие группа подростков, правительства всех стран осознали, что проблему безопасности интернета вещей следует тщательно изучить.

Возможны три подхода к безопасности интернета вещей: оставить все как есть, оснастить ненадежные устройства системой защиты или обязать производителей предусматривать такую защиту изначально. В случае сценария со статус-кво использование интернета вещей будет наносить обществу регулярный ущерб. Добавление защитных функций после покупки приведет к появлению новых компаний, которые заполнят нишу, не занятую производителями, а в итоге покупатель вынужден будет переплачивать. Третий сценарий – встраивание защиты при производстве оборудования – наилучший для потребителей с точки зрения устранения проблем и рисков, и ценообразование тоже является наиболее эффективным.

Воспользуемся примером из прошлого, чтобы показать, как могут работать эти три сценария, особенно два последних. К примеру, в зданиях Нью-Йорка часто предусматривался наружный путь эвакуации при пожаре. За счет этого возрастали стоимость эвакуации и ущерб для людей, оказавшихся внутри (см. статью «How the Fire Escape Became an Ornament», опубликованную в Atlantic). Сегодня путь эвакуации прокладывается внутри зданий, и люди защищены лучше, чем когда-либо прежде. Точно так же и внутренняя защита устройств интернета вещей принесет возможности, которых не дадут внешние решения, такие как установка обновлений и новых аппаратных средств,

моделирование угроз, изоляция компонентов, – обо всем этом вы прочтете в книге.

Обратите внимание на то, что вышеприведенные варианты не являются взаимоисключающими – рынок интернета вещей может поддерживать все три сценария.

## Чем защита интернета вещей отличается от традиционной ИТ-защиты?

Технология интернета вещей имеет ряд ключевых отличий от более привычных нам информационных технологий (ИТ). Движение I Am The Cavalry, глобальная гражданская инициатива по защите научного сообщества, сравнивает то и другое на научной основе, и результаты этого сопоставления мы приведем ниже.

*Последствия* от ошибок в защите интернета вещей в ряде случаев могут повлечь гибель людей. Кроме того, они могут подорвать репутацию компании или целой отрасли, а также веру в то, что правительство способно защитить граждан методом контроля и регулирования. Например, атака WannaCry, прерывающая обслуживание медучреждений на несколько дней, угрожает жизни пациентов, для которых важен строгий график приема лекарств, а также предрасположенных к инсульту или инфаркту.

*Злоумышленники*, совершающие атаки, руководствуются разными мотивами, преследуют разные цели, используют неоднородные методы и возможности. Некоторые не стремятся поставить под угрозу жизнь и здоровье людей, другие, напротив, охотно к этому прибегают. Так, больницы часто подвергаются атакам с целью получения выкупа, потому что потенциальный вред пациентам увеличивает вероятность и скорость выплат.

*Технические параметры* устройств интернета вещей, включая систему защиты, создают ограничения, которых нет у обычного компьютерного оборудования. Например, размер и мощность кардиостимулятора не позволяют применять подходы классической ИТ-защиты, рассчитанные на более крупные и мощные устройства.

Устройства интернета вещей часто действуют в специфическом *контексте* и *окружении,* в частности в быту, где ими распоряжаются люди, не обладающие знаниями или ресурсами, необходимыми для надежного хранения и эксплуатации. Вряд ли можно ожидать от водителя автомобиля с интеллектуальным управлением самостоятельного обновления системы, например установки антивируса. Также маловероятно, что рядовой потребитель сможет оперативно и грамотно отреагировать на возникшую проблему безопасности. Но мы ожидаем подобных действий от предприятия.

*Экономически* производство интеллектуального оборудования стремится к максимальному удешевлению самих устройств и их компонентов, в результате чего последующее добавление средств защиты представляется затратным. Многие такие устройства нацелены на

покупателей с ограниченным бюджетом, у которых к тому же отсутствует опыт в выборе и настройке подобной техники. Кроме того, расходы, обусловленные уязвимостью устройств, часто несут не те, кто непосредственно ими пользуется. Например, ботнет Mirai воспользовался стандартными паролями прошивки – большинство пользователей не догадывается, что нужно сменить пароль, установленный производителем, или не знают, как это сделать! Mirai обошелся экономике Соединенных Штатов в миллиарды долларов, выбрав в качестве мишени стороннего поставщика DNS, который сам не оперировал ни одним из устройств, пострадавших от атаки.

*Время* проектирования, разработки, внедрения, эксплуатации и вывода из эксплуатации устройств часто измеряется десятилетиями. Время отклика также может возрастать в зависимости от параметров устройства, контекста и рабочего окружения. Например, часто ожидается, что интернет-управляемое оборудование на электростанции прослужит без замены более 20 лет. Но атаки на украинского поставщика электроэнергии вызвали сбои в работе системы через несколько секунд после того, как злоумышленники перехватили управление инфраструктурой предприятия.

## *В чем особенность взлома интернета вещей?*

Поскольку безопасность интернета вещей существенно отличается от безопасности в сфере ИТ, для взлома систем интернета вещей требуются другие методы. Такие системы обычно включают отдельные устройства и датчики, мобильные приложения, облачную инфраструктуру и сетевые протоколы связи. К числу последних относятся протоколы сетевого стека TCP/IP (например, mDNS, DNS-SD, UPnP, WS-Discovery и DICOM), а также протоколы, используемые в радиосистемах ближнего действия (например, NFC, RFID, Bluetooth и BLE), среднего радиуса действия (например, Wi-Fi, Wi-Fi Direct и Zigbee) и дальнего действия (например, LoRa, LoRaWAN и Sigfox).

В отличие от традиционных тестов безопасности тестирование безопасности интернета вещей подразумевает проверку и зачастую разборку оборудования, работу с сетевыми протоколами, обычно не встречающимися в других средах, анализ управления устройством через мобильные приложения и изучение взаимодействия устройств с веб-службами, размещенными в облаке, через API-интерфейсы. Все эти частности будут обсуждаться в других главах.

Для примера рассмотрим умный дверной замок. На рис. 1.1 изображена стандартная схема умных запирающих устройств. Умный замок управляется с мобильного приложения потребителя через Bluetooth с низким энергопотреблением (Bluetooth Low Energy, BLE), и приложение обменивается данными с серверами умного замка в облаке (или, как иногда говорят, с чужим компьютером), используя API, работающий по протоколу HTTPS. В этой схеме умный замок зависит от мобильного устройства пользователя с выходом в интернет, который обеспечивает прием любых сообщений от облачного сервера.

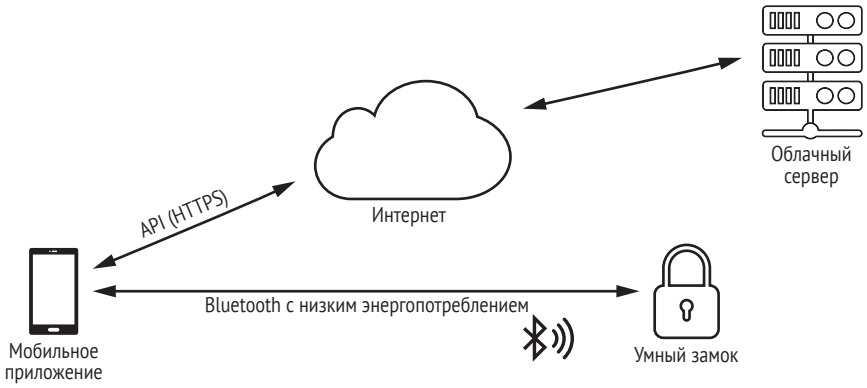


*Рис. 1.1. Система «умный замок»*

Все три компонента (замок, мобильное приложение и облако) взаимодействуют и полагаются друг на друга, создавая систему интернета вещей, предоставляющую широкое поле для атак. Представьте, что произойдет, если вы аннулируете цифровой ключ для гостя Airbnb с помощью этой умной системы блокировки. От имени владельца помещения и устройства «умный замок», мобильное приложение может отправить в облако сообщение, отменяющее ключ гостя. Естественно, совершая это действие, вам необязательно находиться рядом с запираемым помещением и замком. После того как на сервер поступает сигнал об отмене, сервер отправляет умному замку специальное сообщение для обновления списка контроля доступа (Access Control List, ACL). Если злоумышленник переключит свой телефон в режим авиаполета, то умный замок не сможет использовать его в качестве ретранслятора для получения этого обновления с сервера и предоставит доступ к вашей квартире.

Простая атака, описанная выше – обход аннулирования, – это наглядный пример уязвимости, с которой вы можете столкнуться при хакинге интернета вещей. Ограничения, обусловленные использованием небольших и недорогих устройств с низким энергопотреблением, еще больше повышают уязвимость этих систем. Так, вместо использования криптографии с открытым ключом, которая требует значительных ресурсов, устройства интернета вещей обычно полагаются только на симметричные ключи для шифрования своих каналов связи. Эти криптографические ключи зачастую неуникальны и запрограммированы в прошивке или оборудовании, благодаря чему злоумышленники могут извлечь их, а затем повторно использовать на других устройствах.

## *Методики, стандарты и инструкции*

Традиционный подход к решению проблем безопасности заключается в реализации стандартов. За последние несколько лет люди пытались решать проблемы безопасности интернета вещей, применяя

множество методик, правил и других документов. Хотя стандарты предназначены для консолидации отраслей вокруг общепринятых передовых практик, обилие регламентирующих документов создает раздробленную картину, вызывая разногласия по поводу того, что и как делать. Но мы можем извлечь большую пользу из рассмотрения различных стандартов и методик, даже если признаем, что нет единого мнения о наилучшем способе защиты IoT-устройств.

Во-первых, разграничим документы, касающиеся *внутреннего устройства*, и документы, определяющие *функционал*. Эти два аспекта взаимосвязаны, поскольку техническая оснащенность расширяет возможности пользователей в плане безопасности. И напротив, то, что в конструкции устройства не заложено, ограничивает функционал: например, исключает безопасное обновление программного обеспечения, надежность предоставляемых данных, изоляцию и сегментацию в пределах устройства, своевременные оповещения о сбоях. *Инструкции,* предоставляемые производителями, отраслевыми учреждениями или государственными органами, могут сочетать в себе оба типа пояснительных документов.

Во-вторых, проведем различие между *методическими рекомендациями* и *стандартами*. Первые регламентируют категории задач, а вторые – процессы и спецификации для выполнения этих задач. То и другое важно, но методические материалы более актуальны и широко применимы, поскольку стандарты безопасности быстро устаревают и сфера их действия зачастую ограничена. В то же время некоторые стандарты чрезвычайно полезны и определяют основные компоненты технологии интернета вещей, например, для взаимодействия, такие как IPv4 и Wi-Fi. Сочетание методик и стандартов может привести к эффективному управлению технической инфраструктурой.

В настоящей книге мы по мере необходимости будем ссылаться на методики и стандарты, чтобы предоставить разработчикам и пользователям инструкции по устранению возможных проблем в работе описываемых нами инструментов, технологий и процессов. Вот примеры стандартов, инструкций и методических материалов:

- **стандарты.** Европейский институт телекоммуникационных стандартов (European Telecommunications Standards Institute, ETSI), основанный в 1988 году, ежегодно выпускает более 2000 стандартов. Его техническая спецификация по кибербезопасности интернета вещей содержит условия разработки безопасных IoT-устройств. Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) и Международная организация по стандартизации (International Organization for Standardization, ISO) публикуют ряд стандартов, которые поддерживают защиту устройств интернета вещей;
- **рекомендательные материалы.** В международное массовое движение I Am The Cavalry (основано в 2013 году) входят участники сообщества исследователей безопасности. Разработанная им Клятва Гиппократа для интеллектуальных медицинских

устройств (рис. 1.2) описывает цели и возможности проектирования и разработки медицинского оборудования. Многие из изложенных здесь принципов были включены в нормативные критерии Управления по санитарному надзору за качеством пищевых продуктов и медикаментов для одобрения медицинских изделий. Среди других методик – методические рекомендации по безопасности в киберпространстве Национального института стандартов и технологий США, применимые в том числе к владению и эксплуатации IoT-устройств, рекомендации по безопасности интернета вещей Cisco и методика контроля безопасности интернета вещей (IoT Security Controls Framework) Альянса облачной безопасности (Cloud Security Alliance);


*Рис. 1.2. Клятва Гиппократа для интеллектуальных медицинских устройств, методические рекомендации по использованию интернета вещей*

- **инструкции и справочные материалы.** Открытый проект безопасности веб-приложений (The Open Web Application Security Project, OWASP), запущенный в 2001 году, вышел далеко за рамки деятельности одноименной организации. Его списки «топ-10» стали мощным подспорьем для разработчиков программного обеспечения и отдела ИТ-закупок и используются для повышения уровня безопасности в различных проектах. В 2014 году был опубликован первый список «топ-10», относящийся к сегменту интернета вещей (рис. 1.3). Последняя его версия (на момент написания статьи) приходится на 2018 год.


*Рис. 1.3. Топ-10 рисков в области интернета вещей: справочный документ Открытого проекта безопасности веб-приложений*

Другие инструкции и справочные материалы включают в себя Базовый план Национального института стандартов и технологий США в отношении интернета вещей, ресурсы по обновлению и укреплению безопасности Национального управления по телекоммуникациям и информации США (National Telecommu-

nications and Information Administration, NTIA) в отношении интернета вещей, Базовые рекомендации Европейского агентства по сетевой и информационной безопасности (European Network and Information Security Agency, ENISA) в части защиты интернета вещей, Рекомендации и оценку безопасности интернета вещей Международной ассоциации глобальной системы мобильной связи (Global System for Mobile Communications' Association, GSMA) и Рекомендации Фонда безопасности интернета вещей (IoT Security Foundation).

## Пример: обнаружение проблемы безопасности, связанной с интернетом вещей, составление отчета и информирование

Хотя в основе своей эта книга посвящена техническим аспектам, следует отметить и некоторые другие факторы, влияющие на исследование безопасности интернета вещей. Эти факторы, по опыту, включают компромиссы, неизбежные при раскрытии уязвимости, и то, что следует учитывать специалистам по защите, производителям, и широкой общественности в этой связи. В примере ниже будет описано успешное исследование безопасности интернета вещей. Расскажем, как оно проводилось и что привело к удачному исходу.

В 2016 году Джей Рэдклифф, исследователь безопасности, у которого диагностирован диабет I типа, обнаружил три уязвимости в устройстве инсулиновой помпы Animas OneTouch Ping и сообщил об этом производителю. Работа по тестированию началась за несколько месяцев до этого: он купил устройства, построил тестовую лабораторию и определил вероятные угрозы. Кроме того, Джей обратился за консультацией к юристу, чтобы убедиться, что тестирование не противоречит государственному и региональному законодательству.

Основная цель Джея заключалась в защите пациентов, поэтому он подал свой отчет в соответствии с политикой раскрытия уязвимостей производителя. По электронной почте, телефону и в личных беседах Джей обсудил технические детали, возможные последствия проблемы и шаги, необходимые для их устранения. Переговоры продолжались несколько месяцев, в течение которых Рэдклифф продемонстрировал использование слабых мест в работе устройства и предоставил проверочный код.

Позже, узнав, что производитель не планирует внедрять какие-либо технические исправления до выпуска новой модели помпы, Джей публично раскрыл информацию об уязвимости, но со следующей оговоркой: «Если кто-либо из моих детей заболеет диабетом и медицинский персонал порекомендует поставить им помпу, я без колебаний выберу модель OneTouchPing, пусть она и не идеальна» – см. *https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/*.

Джей почти год работал над тем, чтобы найти уязвимость и устранить ее. Он должен был представить свою работу на крупной конференции после того, как производитель уведомит пациентов, для которых это важно. Многие пациенты использовали почту как основной источник получения информации, а почтовая рассылка была запланирована только после этого доклада. Джей принял непростое решение отменить свое выступление на конференции, чтобы пациенты могли узнать о проблеме от своего врача или компании, а не из новостной статьи.

Вы можете извлечь ряд уроков из ситуаций, с которыми имеют дело опытные исследователи безопасности, такие как Джей.

- *Они учитывают возможную реакцию на их изыскания.* Джей не только заблаговременно прояснил юридические аспекты, но и постарался, чтобы его тестирование не повредило кому-либо за пределами лаборатории. Кроме того, он позаботился о том, чтобы пациенты узнали о технических проблемах от людей, которым они доверяют, что снизит тревогу и не повлечет отказ от использования технологий, спасающих жизнь.
- *Они информируют о проблеме, но не вмешиваются в процесс принятия решений.* Джей понял, что производитель не захотел тратить большие средства на обновление старых устройств и сосредоточился на создании новых продуктов, которые позволят спасти еще больше людей и облегчат их жизнь. Вместо того чтобы настаивать на исправлении старых моделей, он прислушался к мнению производителя.
- *Они подают пример.* Джей, как и многие другие исследователи в области здравоохранения, наладил долгосрочные отношения с пациентами, регулирующими органами, врачами и производителями. До известной степени это означало отказ от общественного внимания и оплачиваемых проектов, а также необходимость проявить исключительное терпение. Но результаты говорят сами за себя. Ведущие производители выпускают самые безопасные медицинские устройства из когда-либо существовавших, привлекая исследовательское сообщество к таким мероприятиям, как Biohacking Village на конференции DEF CON.
- *Они знают закон.* Исследователям безопасности долгое время приходилось сталкиваться с обвинениями в правонарушениях. Часто это были необоснованные выпады, но в ряде случаев повод имелся. Притом что эксперты все еще разрабатывают стандартизованный язык регулирования программ по раскрытию информации и поиску уязвимостей, до судебных исков в адрес исследователей, раскрывающих информацию, дело доходило редко (если вообще доходило).

# Мнения экспертов: навигация в среде интернета вещей

Мы обратились к нескольким признанным экспертам в области права и государственной политики, чтобы проинформировать читателей о темах, которые традиционно не освещаются в книгах о исследованиях безопасности. Харли Гейгер упоминает два закона, действующих в отношении исследователей безопасности в США, а Дэвид Роджерс рассказывает, какие меры по повышению безопасности устройств интернета вещей принимаются в Великобритании.

## *Законы хакинга интернета вещей*

**Харли Гейгер, директор по общественной политике компании Rapid7**

Пожалуй, два наиболее важных федеральных закона, влияющих на исследования в области интернета вещей, – это Закон о защите авторских прав в цифровую эпоху (Digital Millennium Copyright Act, DMCA) и Акт о компьютерном мошенничестве и злоупотреблении (Computer Fraud and Abuse Act, CFAA). Давайте рассмотрим эти мрачноватые законы.

Во многих оценках безопасности интернета вещей отмечается обход слабых средств защиты ПО, но Закон о защите авторских прав в цифровую эпоху в большинстве случаев запрещает обход *технологических мер защиты* (Technological protective measures, TPM), таких как шифрование, требования аутентификации и кодирование региона, в целях доступа к произведениям, защищенным авторским правом (например, к программному обеспечению), без разрешения владельца авторских прав. Для этого перед проверкой безопасности требуется получить разрешение от производителей программ, которыми оснащены устройства интернета вещей – *в том числе и те, которыми вы владеете!* К счастью, существует специальное исключение для благонадежного тестирования безопасности, позволяющее исследователям игнорировать технологические меры защиты и не просить разрешения правообладателя. Глава Библиотеки Конгресса допустил это исключение по запросу сообщества исследователей безопасности и его союзников. По состоянию на 2019 год исследование, отвечающее Закону о защите авторских прав в цифровую эпоху, соответствует следующим критериям:

- проводится на устройстве, приобретенном на законных основаниях (например, авторизованном владельцем компьютера);
- выполняется исключительно с целью тестирования или исправления уязвимостей в системе защиты устройства;
- не наносит вред окружающей среде (к примеру, не может проводиться на АЭС или перегруженной магистрали);
- информация, полученная в результате исследования, используется в первую очередь для повышения безопасности или защиты

устройств, компьютеров или их пользователей (а, например, не в целях пиратства);

- исследование не нарушает другие законы, включая, но не ограничиваясь Актом о компьютерном мошенничестве и злоупотреблении.

Существует два исключения, из которых только одно обеспечивает реальную защиту. Это более серьезное исключение должно обновляться каждые три года главой Библиотеки Конгресса США, и степень защиты при его обновлении может меняться. В результате могут раскрываться некоторые из наиболее важных в правовом аспекте результатов исследований. Самая последняя версия исключения в Законе о защите авторских прав в цифровую эпоху, применимая к тестированию безопасности (2018 год), доступна по ссылке *https://www.govinfo.gov/content/pkg/FR-2018-10-26/pdf/2018-23241.pdf#page=17/*.

Акт о компьютерном мошенничестве и злоупотреблении тоже используется часто; как вы могли заметить, он фигурирует в вышеприведенной цитате из Закона защиты авторских прав в цифровую эпоху. Этот акт является главным федеральным законом США о борьбе с хакерскими атаками, и, в отличие от Закона о защите авторских прав в цифровую эпоху, он не описывает меры защиты тестирования безопасности. Указанный акт обычно распространяется на доступ к чужим компьютерам, а также вредоносные действия в их отношении без разрешения *их владельца* (а не владельца авторских прав на программное обеспечение, как в случае с DMCA). Что, если устройство интернета вещей выделила вам компания, в которой вы работаете, или школа, а вы решили без их ведома исследовать это устройство на предмет надежности? Суды все еще спорят по этому поводу. Это одно из спорных мест в Акте о компьютерном мошенничестве и злоупотреблении, который, к слову, был принят более 30 лет назад. Тем не менее, если вы вторгаетесь в устройство интернета вещей, которое принадлежит вам или которое вам предоставил для тестирования его владелец, вы, скорее всего, в ладу с законом – как DMCA, так и CFAA. С чем вас и поздравляем.

Но подождите! С исследованиями безопасности интернета вещей могут быть связаны и многие другие законы, особенно государственные законы о хакинге, которые могут трактоваться еще шире и более расплывчато, чем Акт о компьютерном мошенничестве и злоупотреблении. (Интересный факт: в законе штата Вашингтон о хакинге предусмотрена особая правовая защита для так называемых белых шляп, или этичных хакеров.) Не стоит думать, что к вашему исследованию безопасности интернета вещей не возникнет претензий только потому, что оно проводится в строгом соответствии с законом DMCA и актом CFAA – хотя для начала это уже неплохо!

Если вы запутались в многочисленных законах и боитесь что-то нарушить, то вы не одиноки. Законы на эту тему сложны, они представляют головоломку даже для острых умов юристов и государственных чиновников, – но в то же время ведется интенсивная кропотливая работа по уточнению и усилению правовой защиты исследований

в области безопасности. Ваш голос и опыт работы с неоднозначными законами, сдерживающими ценные исследования безопасности интернета вещей, могут сослужить полезную службу в дебатах о реформировании DMCA, CFAA и других законов.

## *Роль правительства в безопасности интернета вещей*

**Дэвид Роджерс, генеральный директор Copper Horse Security, автор Кодекса надлежащей практики Великобритании, кавалер Ордена Британской империи, врученного за заслуги в области кибербезопасности**

Перед правительством стоит нетривиальная задача: защищать общество и вместе с тем способствовать процветанию экономики. Хотя правительства разных стран не дерзали вмешиваться в безопасность интернета вещей, опасаясь затормозить инновации, такие события, как появление ботнетов Mirai, WannaCry и NotPetya, заставили законодательные и регулирующие органы пересмотреть свою политику невмешательства.

Одним из решений государственного масштаба стало, в частности, введение британского *Кодекса надлежащей практики*. Впервые опубликованный в марте 2018 года, этот документ призван сделать Соединенное Королевство самым безопасным местом для жизни и ведения бизнеса в интернете. Государство признало, что инфраструктура интернета вещей имеет огромный потенциал, но и таит в себе огромные риски, поскольку производители не могут защитить потребителей и граждан. В 2017 году экспертная консультативная группа, состоящая из представителей различных отраслей, правительств и академических кругов, приступила к изучению проблемы. В дополнение были организованы обсуждения со многими участниками сообщества исследователей безопасности, включая такие организации, как I Am The Cavalry.

В Кодексе изложены 13 принципов, которые в целом должны поднять планку кибербезопасности не только для технических устройств, но и экосистемы. Он применяется к разработчикам мобильных приложений, поставщикам облачных услуг, операторам мобильной связи, а также розничным продавцам. Такой подход перекладывает бремя обеспечения безопасности с потребителей на организации, которые лучше оснащены и заинтересованы в решении проблем с безопасностью на более ранних этапах жизненного цикла устройств.

Полный текст Кодекса доступен по ссылке *https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/*. Самыми неотложными задачами являются следующие: 1) недопущение применения паролей, устанавливаемых по умолчанию; 2) принятие и реализация политики раскрытия уязвимостей; 3) обеспечение доступности обновлений программного обеспечения для устройств. Автор охарактеризовал эти пункты как *критерии защищенности*; если продукт интернета вещей не соответствует этим требованиям, в оставшейся части он, вероятно, также имеет изъяны.

Подход, используемый в Кодексе, учитывает международную значимость проблемы, поскольку мир интернета вещей и цепочка поставок интеллектуальных устройств – это явления глобального порядка. Кодекс поддержали десятки компаний по всему миру, и в январе 2019 года Европейский институт стандартов по телекоммуникациям (ETSI) одобрил его под названием Техническая спецификация ETSI 103 645.

Дополнительную информацию о политике разных государств в данной сфере вы найдете в Базе данных политик кибербезопасности интернета вещей на сайте I Am The Cavalry: *https://iatc.me/iotcyberpolicydb/*.

## *Взгляд пациентов на безопасность медицинских устройств*

Проектирование и разработка IoT-устройств может вынудить производителей идти на нелегкие для них компромиссы. Исследователи безопасности, которые сами пользуются медицинским оборудованием такого типа, в частности Мари Мо и Джей Рэдклифф, хорошо знают, какие компромиссы имеются в виду.

### Мари Мо, @mariegmoe, SINTEF

Я исследователь безопасности и пациент, находящийся под наблюдением врачей. Каждый импульс моего сердца генерирует техническое устройство – кардиостимулятор, установленный у меня внутри. Восемь лет назад я очнулась на полу после падения. Перед этим в работе моего сердца наступила пауза – достаточно долгая для того, чтобы потерять сознание. Теперь, чтобы сердечный ритм не нарушался и подобных пауз не возникало, мне нужен кардиостимулятор. Этот маленький аппарат отслеживает каждый импульс и посылает прямо в мое сердце небольшой электрический сигнал, чтобы оно продолжало биться. Но как я могу доверять своему сердцу, если его приводит в действие программа, работа которой для меня непрозрачна?

Кардиостимулятор мне устанавливали в экстренном порядке. Это была критическая мера, так что не было возможности отказаться от импланта. Но у меня было время задать наводящие вопросы. К удивлению врачей, я начала расспрашивать о потенциальных уязвимостях программного обеспечения, установленного в кардиостимуляторе, и о возможностях взлома этого жизненно важного устройства. Ответы оказались неудовлетворительными. Медицинские работники не смогли ответить на технические вопросы о компьютерной безопасности; многие даже не задумывались над тем, что работа аппарата управляется программным кодом, а производитель имплантата предоставляет весьма скудную техническую информацию.

Итак, я затеяла исследовательский проект; за последние четыре года я узнала довольно много о безопасности устройства, с которым теперь живу. Выяснилось, что многие мои опасения, касающиеся

кибербезопасности медицинских устройств, оправданны. Я узнала, что в проприетарном ПО, созданном с использованием подхода «безопасность через неизвестность», порой неудачно реализованы защита и конфиденциальность. Я узнала, что унаследованная технология в сочетании с дополнительными возможностями подключения означает увеличение поверхности атаки и, следовательно, повышение вероятности возникновения проблем, влияющих на безопасность пациентов. Хакеры вроде меня взламывают устройства не с целью посеять страх или причинить боль пациентам. Моя мотивация – исправить обнаруженные недостатки. Для этого критически важно сотрудничество всех заинтересованных сторон.

Я хочу, чтобы производители медицинских устройств серьезно относились ко мне и к другим исследователям, когда мы просим их сообщать о проблемах кибербезопасности, действуя в интересах пациентов.

Во-первых, мы должны признать, что проблемы кибербезопасности угрожают здоровью людей. Замалчивание обнаруженных уязвимостей или отрицание их существования не обезопасит пациентов. Меры по обеспечению прозрачности, такие как создание открытых стандартов для протоколов защищенной беспроводной связи, публикация согласованной политики раскрытия уязвимостей, в которой исследователям предлагается в корректной форме сообщать о проблемах, и выпуск рекомендаций по кибербезопасности для пациентов и врачей заставляют верить, что производитель серьезно относится к этим проблемам и работает над их устранением. Таким образом, я и мой врач можем быть уверены, что медицинские риски и побочные эффекты, связанные с кибербезопасностью, не превышают общих рисков, обсуловленных моей личной ситуацией.

Решение на будущее – прозрачность и лучшее сотрудничество с пониманием и сочувствием.

### Джей Рэдклифф (Jay Radcliffe), @ jradcliffe02, Thermo Fisher Scientific

Я хорошо помню тот день, когда мне поставили диагноз «диабет». Это был мой 22-й день рождения. У меня были типичные симптомы диабета I типа: сильная жажда и потеря веса. Тот день изменил мою жизнь. Я один из редких людей, которые могут сказать, что мне повезло с диагнозом. Диабет открыл мне мир медицинских устройств, подключенных к интернету. К тому времени я уже любил разбирать и чинить вещи – это был просто новый способ проявить свои природные задатки и навыки. Невозможно описать, что чувствует человек, к телу которого подключают аппарат, контролирующий основные жизненные функции. Другое неописуемое чувство – знать, что он функционирует благодаря беспроводному подключению и имеет уязвимости. Я радуюсь любой возможности сделать медицинские устройства более устойчивыми к вредоносному воздействию, в том числе сетевому. Эта техника критически важна для поддержания здоровья и жизни людей. Инсулиновые помпы, кардиостимуляторы

и другие кардиоустройства, стимуляторы спинного мозга, нейростимуляторы и бесчисленное множество других устройств меняют жизнь людей к лучшему.

Подобные приборы часто подключаются к мобильным телефонам, а затем к интернету – так они могут информировать врачей и лиц, осуществляющих уход, о состоянии здоровья пациента. Но возможность подключения сопряжена с риском. Наша задача как специалистов в области безопасности – помочь пациентам и врачам понять эти риски, а производителям – выявить их и контролировать. Хотя сами компьютеры, возможности подключения и меры безопасности сильно изменились за последние несколько десятилетий, в законодательстве Соединенных Штатов не появилось ничего существенно нового в отношении исследований безопасности, проводимых с добрыми намерениями. (Ознакомьтесь с законами, действующими в вашем регионе, – они могут отличаться.) К счастью, нормативные формулировки, исключения и реализации изменились в лучшую сторону – благодаря работе хакеров, ученых, компаний и компетентных чиновников. Для подробного рассмотрения юридических аспектов компьютерной безопасности может потребоваться несколько томов заумного текста, написанного опытными юристами, так что эта книга не место для такого обсуждения. Но в целом, если вы владеете медицинским устройством и проживаете на территории США, исследовать безопасность этого устройства законно, по крайней мере в пределах вашей собственной сети.

## Заключение

Сфера интернета вещей стремительно развивается. Количество, типы и способы использования этих «вещей» меняются быстрее, чем удается опубликовать новые книги о них. К тому времени, как вы прочтете эти строки, появится еще какая-нибудь новинка, о которой мы пока ничего не знаем. Тем не менее мы уверены: эта книга содержит ценные ресурсы и ссылки, которые позволят вам развивать свои навыки независимо от того, что вам придется тестировать через год или десятилетие.