Содержание

Введение. Вездесущий компьютер 7

Часть I. Тенденция 25

Глава 1. Компьютеры по-прежнему уязвимы 30

Глава 2. Пропатчивание — неработающая модель безопасности 51

Глава 3. Узнавать, кто есть кто в интернете, становится все труднее 64

Глава 4. Незащищенность предпочитают все 80

Глава 5. Риски становятся катастрофическими 111

Часть II. Решения 139

Глава 6. Как выглядит безопасный интернет+ 148

Глава 7. Как мы можем защитить интернет+ 170

Глава 8. Обеспечивать безопасность должно правительство 206

Глава 9. Смена приоритетов: правительство должно перейти от киберагрессии к обеспечению кибербезопасности 231

Глава 10. План Б: что может произойти на самом деле 261

Глава 11. Что такое «плохая политика»? 279

Глава 12. К надежному, устойчивому и демилитаризованному интернету+ 303

Заключение. Настало время объединить политику и технологию 315

Благодарности 329

Примечания 332

Введение

Вездесущий компьютер

Подумайте о трех инцидентах и скрытом в них смысле.

Инцидент первый. В 2015 г. два специалиста по кибербезопасности вмешались в электронную систему управления автомобилем Jeep Cherokee[1]. Сделали они это, находясь от машины на расстоянии 10 миль*, с помощью связанной с ней через интернет мультимедийной системы. Камеры наружного наблюдения зафиксировали искаженное ужасом лицо водителя мчащегося по хайвею авто, у которого «произвольно» включался-выключался кондиционер, сменялись радиопрограммы, то и дело начинали работать дворники и в конце концов заглох двигатель. Так как айтишники всего лишь демонстрировали уязвимости системы, а не покушались на убийство водителя, они не пытались управлять тормозами или вращать руль, хотя и это было им по силам.

Аналогичные трюки хакеры проделывали и с рядом других автомоделей. Взламывали электронную систему управления через диагностический порт[2]. Проникали туда через DVD-плеер[3]. Вскрывали навигационную систему OnStar[4] и компьютеры, встроенные в автопокрышки[5].

Самолеты тоже уязвимы. Нет, взломщики не предпринимали атак, подобных той, что была совершена в отношении Jeep Cherokee, однако, по их утверждениям, у коммерческих

* 16,09 км. — *Прим. ред.*

авиалайнеров имеются слабые места, например мультимедийная система[6] или система связи с землей[7]. Долгие годы производители самолетов отвергали саму вероятность взлома. Тем не менее в 2017 г. Министерство внутренней безопасности США, не раскрывая подробностей, продемонстрировало дистанционное проникновение в системы Boeing 757[8].

Инцидент второй. В 2016 г. взломщики удаленно «взорвали» кибербоеприпас под названием Crash Override, отключив таким образом высоковольтную электроподстанцию «Северная»*. Атака с применением Crash Override отличалась[9] от произошедшего годом ранее нападения на диспетчерский пункт «Прикарпатьеоблэнерго». Тогда тоже случился блэкаут, но нападение по преимуществу осуществлялось в ручном режиме: хакеры получили доступ к системе через вредоносную программу, после чего, дистанционно управляя компьютерами в диспетчерском пункте, отключили электричество. Одному из операторов удалось заснять происходящее[10].

Подстанция «Северная», как уже упоминалось, была отключена автоматически — с помощью программы Crash Override. Потребители электроэнергии отделались легким испугом: техники перевели подстанцию в автономный режим и через час с небольшим восстановили подачу электричества вручную. Имеют ли американские электростанции такие же системы переключения на ручное управление, не говоря уже о специалистах, умеющих их применять, — неизвестно.

Программа Crash Override — оружие. За счет модульной структуры ее можно модифицировать под конкретную задачу или цель — газопровод, станцию водоочистки и т. п. Программа содержит «заряды»[11], которые не стали задействовать на «Северной». Тем не менее подстанцию могли раз за разом включать и выключать, в результате чего оборудование вышло бы из строя, а подача электроэнергии стала бы невозможной

* Оригинальное название подстанции — Пивнична. — *Прим. ред.*

в ближайшие дни или даже недели. Применение такого оружия — проверка его возможностей. К такому выводу можно прийти, если учесть, что за последние годы хакеры, не причиняя ущерба, взломали стратегически важные системы более чем 20 американских электростанций[12].

Инцидент третий. В один из выходных 2017 г. неизвестные по всему миру вскрыли 150 000 принтеров. Выявив незащищенное оборудование, вредоносная программа заставила его печатать рисунки в ASCII-формате, издевательские и провокационные сообщения[13]. Чуть ранее в том же году по инициативе хакеров принтеры ряда американских университетов множили антисемитские листовки[14]. Такие акты вандализма, увы, не редкость.

В отношении 3D-принтеров атаки не проводились, но это не основание считать биооборудование менее уязвимым. Наихудшие последствия взлома обычного принтера — непредвиденные расходы и раздражение. Но если атаку направят на биопринтеры, уровень угрозы возрастет многократно. 3D-оборудование, которое все еще совершенствуется, обладает огромным потенциалом: с его помощью планируется синтезировать и «собирать» вирусы, нацеленные на уничтожение раковых клеток или на излечение других заболеваний конкретного пациента[15]. А теперь представьте, что биопринтеры получили широкое применение в больницах, аптеках и врачебных кабинетах. Хакеру, получившему необходимые инструкции и удаленный доступ к одному из 3D-устройств, по силам заставить его печатать смертоносный вирус. По силам дать команду одному-единственному принтеру напечатать множество таких вирусов или массе принтеров размножить небольшую партию вирусов. Если вирус поразит значительное количество людей, получит широкое распространение и окажется стойким, мы столкнемся с самой настоящей пандемией. С самым настоящим кибергейтом.

Отчего стали возможны подобные инциденты? Водителю автомобиля 1998 г. выпуска не грозило, что некто, находящийся от него на расстоянии в несколько миль, вмешается в процесс

управления. То же самое можно сказать и применительно к работникам электростанций в 1998 г. Современные транспортные средства и стратегические объекты уязвимы. То же в скором времени можно будет сказать и в адрес биопринтеров. А все потому, что все это, по сути, — компьютер. Уязвимым постепенно становится все, потому что все постепенно становится компьютером. Если выражаться точнее, то компьютером, подключенным к интернету.

Духовка — компьютер, предназначенный для приготовления пищи. Холодильник — компьютер для охлаждения и сохранения продуктов. Фотоаппарат — компьютер, оснащенный объективом с затвором. Банкомат — компьютер с деньгами внутри. Современные лампы —компьютеры, излучающие свет, после того как человек самостоятельно или с помощью другого компьютера нажмет на кнопку включения.

Некогда автомобиль представлял собой механическое устройство, снабженное парой-тройкой компьютеров. Сегодня это система из 20–40 компьютеров, оборудованная четырьмя колесами и двигателем. Вы нажимаете на педаль тормоза и считаете, что физически останавливаете автомобиль, но на самом деле посылаете электронный сигнал тормозам.

Телефон превратился в мощный компьютер в 2007 г., когда на рынке появился iPhone. Теперь смартфон — постоянный спутник человека. Префикс «смарт»* в слове «смартфон» — а мы используем его для обозначения компьютеризованных, подключенных к интернету устройств, — означает, что в процессе работы устройство собирает, обрабатывает и передает данные. Имеет смысл считать умным и телевизор, ведь он постоянно собирает сведения о привычках пользователя с целью оптимизировать процесс взаимодействия.

Скоро умные устройства будут встраивать в наш организм. Современные кардиостимуляторы[16] и инсулиновые помпы[17] — наглядное тому подтверждение. Умными становятся таблетки

* От англ. smart — умный. — *Прим. пер.*

и всевозможные медицинские изделия[18]. Умные контактные линзы будут не только информировать об остроте зрения, но и примутся отслеживать уровень глюкозы, а также диагностировать заболевания глаз, скажем, глаукому[19]. Фитнес-трекеры уже стали умными, а их способность наблюдать за состоянием человеческого организма постоянно развивается[20].

Предметы обихода все умнеют и умнеют. Можно купить умный ошейник для собаки[21] или умную игрушку для кошки[22], а еще умную ручку[23], умную зубную щетку[24], умную кофейную чашку[25], умную секс-игрушку[26], умную куклу Барби[27], умную рулетку[28] и умный датчик полива растений[29]. Можно купить даже умный мотоциклетный шлем, который в случае аварии автоматически вызовет «скорую помощь» и сообщит о происшествии родным и близким[30].

Мы свидетели начала эпохи умных домов. Виртуальная помощница Alexa* и ее двоюродные «сестры» готовы предоставить информацию по любому запросу. Существуют умные термостаты[31], умные розетки[32] и умные бытовые приборы. Можно купить умные напольные весы[33], умный унитаз[34] и умные лампочки[35]. Можно приобрести умную кровать[36], которая проанализирует особенности сна и диагностирует нарушения. Можно установить на дверь умный замок[37], а ремонтникам или сотрудникам службы доставки предоставить одноразовый код для прохода.

В офисах и на предприятиях такие умные устройства представляют собой единую сеть с камерами видеонаблюдения и датчиками движения, что обеспечивает бóльшую эффективность всех систем — освещения, климат-контроля, лифтов и т. п. Городские службы все чаще отдают предпочтение умным энергетическим сетям и транспортным системам, что в скором времени позволит им управлять бытовыми приборами и другими домашними устройствами и тем самым оптимизировать расход

* В России распространены другие голосовые помощники, например Алиса. — *Прим. ред.*

электроэнергии. С этой же целью развивается сеть умных беспилотных автомобилей, автоматически направляющихся туда, где в них действительно есть нужда.

Городские власти начинают встраивать умные датчики в дорожное полотно и в уличные фонари[38]. Это позволяет регулировать движение с учетом пробок, сокращать время прибытия сотрудников полиции и медицинских служб к месту происшествия, повышать эффективность работы муниципальных и коммунальных служб — оптимизировать маршруты мусоровозов, оперативно ликвидировать выбоины. Очень скоро умные билборды станут распознавать лица и демонстрировать проходящим мимо них людям персональную рекламу[39].

Силовая подстанция представляет собой компьютер, который распределяет электроэнергию, и — как многие другие современные устройства — он подключен к интернету. Программа-вирус Crash Override не проникала внутрь подстанции «Северная» — она скрывалась в щите управления, находящемся за много миль от объекта и соединенным с ним через интернет.

Этот технологический сдвиг произошел буквально за последнее десятилетие. Если раньше мы имели дело с вещами со встроенными компьютерами, то теперь живем среди компьютеров с присоединенными к ним вещами. В компьютер превращается все больше вещей. Происходящее легко не заметить, ведь мы, разумеется, не приобретаем автомобиль или холодильник в качестве компьютера. Мы покупаем их ради назначения — как транспортное средство или агрегат для сохранения продуктов. Но все это компьютер, что важно осознавать, поскольку речь идет о безопасности.

Меняется и концепция интернета. Мы больше не «заходим в чаты», не «загружаем электронную почту» — мы «серфим в интернете». Эти речевые обороты быстро устаревают, и через несколько лет выражение «я захожу в интернет» будет иметь примерно тот же смысл, что при включении тостера фраза «я захожу в электросеть».

Повсеместная цифровая взаимосвязь различных устройств называется интернет вещей (Internet of Things — IoT)[40]. Этот маркетинговый термин очень точно отражает реальность. Сотрудники фирмы Gartner, специализирующейся на изучении рынка информационных технологий, так охарактеризовали это понятие: «Интернет вещей — это сеть физических объектов, каждый из которых наделен встроенной системой обмена данными, позволяющей им взаимодействовать между собой или с внешней средой». Подразумевается, что через интернет эти устройства взаимодействуют с нами, друг с другом и другими компьютерными приложениями.

Масштабность событий, происходящих в цифровом мире, поражает воображение. В 2017 г. мы знали о 8,4 млрд устройств, подключенных к интернету (преимущественно компьютеры и телефоны)[41], что на треть больше, чем за год до этого, а к 2020 г. их число составит от 20 до 75 млрд — в зависимости от того, чьей оценке вы доверяете*[42].

В основе явления — стремление производителей различных приборов и устройств наделять их разумом и благодаря этому добиваться конкурентного преимущества. Более того, количество компьютеров будет возрастать прямо пропорционально уменьшению их размера и снижению цены.

Стиральная машина — это компьютер, который делает чистой одежду. Производители стиральных машин не пренебрегают возможностью оснастить изделия доступными по цене компьютерами. Следовательно, приобретать стиральную машину, не связанную с интернетом, будет все сложнее.

Два года назад я безуспешно пытался купить новый автомобиль без поддержки интернета. Опция была стандартной для машин с необходимыми мне характеристиками. По мере

---

* Приведенные статистические данные и прогнозы действительны для 2018 г. — года написания книги. В действительности к 2021 г. число активных умных вещей достигло 10 млрд; https://dataprot.net/statistics/iot-statistics/. — *Прим. ред.*

удешевления упомянутых технологий подобное будет происходить повсеместно. В итоге устройство для подключения к интернету станет неотъемлемой частью любого изделия.

Сегодня сама идея о том, чтобы стиральная машина имела связь с интернетом, кажется надуманной. И совершенно невозможно представить, что к интернету способна подключиться, скажем, футболка[43]. Между тем в ближайшем будущем это будет в порядке вещей. Компьютеры становятся мощнее, меньше, дешевле, и все, что потребуется для того, чтобы одежда с поддержкой интернета стала нормой, — это довести стоимость микропроцессора до такого уровня, чтобы она стала ниже, чем выгода для розничного продавца от автоматического отслеживания запасов до продажи и автоматического отслеживания использования после нее. Буквально десятилетие — и мы, скорее всего, не сможем купить футболку без датчиков. Более того, мы будем считать вполне естественным, что стиральная машина, общаясь с крутящейся внутри нее одеждой, самостоятельно определяет оптимальный цикл стирки и расход моющего средства. Впоследствии производитель стиральных машин начнет продавать производителям одежды информацию о том, что мы носим (или больше не носим).

Перед какой бы аудиторией мне ни доводилось выступать, всегда находились те, кто спрашивал: «Зачем?» Они понимали, зачем снижать потребление электроэнергии, но были не в состоянии осознать, зачем подключать к интернету кофейник или зубную щетку. «Тренд “Все умное” официально признан глупым», — гласил заголовок газетной статьи от 2016 г., посвященной одной из первых попыток подключить холодильник к интернету[44].

Ответ на вопрос «зачем» прост: таковы требования рыночной экономики. По мере того как стоимость компьютеризированных устройств снижается, их предельная выгода (как с точки зрения функциональности, так и с точки зрения результатов наблюдений), необходимая для оправдания компьютеризации, тоже

уменьшается. Для пользователя выгода от компьютеризации может заключаться в наличии дополнительных свойств у приобретаемого товара, для производителя товара — в возможности с его помощью изучать рынок и пользовательскую базу. При этом производители электронных устройств, внедряемых в большинство товаров, отказываются от специализированных микросхем в пользу универсальных, массовых и более дешевых чипов. Ну а поскольку встроенные компьютеры становятся стандартизированными, производителям дешевле включить связность, чем пренебречь ей. Другими словами, дешевле «забросать» город датчиками, чем извлечь те из дорожного полотна.

В тотальной компьютеризации есть и свои преимущества — некоторые из них для нас уже очевидны, остальные мы увидим только после того, как количество компьютеров достигнет критической массы. Интернет вещей проникнет в нашу жизнь на всех ее уровнях, и я не думаю, что нам по силам повлиять на уже запущенный процесс. Происходит фундаментальный сдвиг, масштабный и всеобъемлющий: все превращается в единую гиперсвязанную систему, в которой подключенные к одной сети вещи взаимодействуют между собой.

И в основе всего лежит интернет вещей. Возьмем интернет вещей или, если посмотреть шире, киберфизические системы. Добавим к ним миниатюризацию сенсоров, контроллеров и трансмиттеров, затем — автономные (независимые) алгоритмы, машинное обучение и искусственный интеллект (ИИ). Приложим немного облачной вычислительной среды с соответствующим увеличением возможностей хранения и обработки данных. Не забудем включить в перечень интернет, всепроникающую компьютеризацию и широкую доступность высокоскоростного беспроводного подключения. И, наконец, дополним картину робототехникой. В итоге мы получим единый глобальный интернет, который оказывает на мир непосредственное физическое воздействие. Это интернет, который чувствует, думает, действует[45].

У процесса нет выраженного направления. Мы видим тенденции, которые в процессе развития пересекаются и усиливают друг друга. Так, например, в робототехнике используются автономные алгоритмы. В дронах заложены принципы интернета вещей, автономности и мобильной вычислительной среды. В умных рекламных щитах сочетаются механизм персонализации и интернет вещей. Устройство, регулирующее объем воды, проходящей через плотину, функционирует на основе киберфизических систем, облачной вычислительной среды и деятельности автономных агентов. Мы предпочли бы полагать по-другому, но люди — один из элементов большинства этих систем. Мы предоставляем информацию для компьютеров и принимаем результаты их работы (соглашаемся с ними). Пользуемся их автоматизированной функциональностью. Обеспечиваем взаимодействие между системами, которые пока недостаточно умны для того, чтобы отсечь нас от себя. Перемещаем эти системы, по крайней мере, те из них, которые не способны перемещаться самостоятельно. Влияем на них, а они влияют на нас. Велика вероятность, что со временем мы превратимся в виртуальных киборгов, даже если физиологически останемся людьми.

Следует дать имя этой новой системе. Она больше чем интернет, больше чем интернет вещей. На самом деле она — интернет + вещи. Если выражаться точнее, она — это интернет + вещи + мы. Или, короче, интернет+[46]. Честно говоря, я не собирался придумывать термин, но не могу найти понятие, определяющее совокупность всех этих тенденций. Поэтому пусть хотя бы в этой книге будет интернет+.

Конечно, слова «умный» и «думающий» применительно к неодушевленному предмету имеют переносный смысл. Но меня они вдохновляют сильнее, чем все остальные. Бóльшая часть интернета вещей не очень-то и умна и останется таковой еще очень долго. И все же в интеллектуальном плане система постоянно развивается. Маловероятно, что в обозримом будущем компьютеры станут разумными, но при решении определенных задач они уже

проявляют рациональность. Интернет+ становится мощнее благодаря построенным нами взаимосвязям. Однако одновременно он становится и менее защищенным. Давайте разберемся, почему так происходит и что мы можем с этим сделать.

История запутанная, и я поделил ее на две части. В части I я описываю текущее состояние компьютерной безопасности — с технической, политической и экономической точки зрения, — а также тенденции, которые привели к такому положению дел. Компьютеры уменьшаются в размерах и при этом оказывают все большее воздействие на физический мир, но, в принципе, пока остаются все теми же компьютерами, за которыми мы работали в течение нескольких десятилетий. Проблемы технической безопасности никуда не делись. Как и политические проблемы — мы преодолевали их раньше и преодолеваем сейчас. Но по мере того, как компьютеры и средства коммуникации проникают в приборы, отрасли промышленности — одна за другой — приобретают черты компьютерной промышленности (отрасли, производящей компьютеры). Компьютерная безопасность вскоре станет обязательным предметом, и ее азы будут изучаться и применяться повсеместно. Но вот что нам точно известно о компьютерах, вне зависимости от того, частью чего они являются — автомобилей, силовых подстанций или биопринтеров, — они уязвимы. Они могут подвергнуться атаке со стороны преступников, программистов-любителей, представителей государственной власти и вообще кого угодно, располагающего достаточными техническими возможностями.

В главе 1 мы кратко охарактеризуем технические причины уязвимости интернета. В главе 2 рассмотрим главный способ поддержания безопасности в компьютерных системах — пропатчивание* уязвимостей в случае их обнаружения, а также поговорим о том, почему это не сработает применительно к интернету+. Глава 3

* Пропатчивание — автоматизированное устранение обнаруженных проблем. — *Прим. ред.*

посвящена тому, как мы показываем, кто мы в интернете, и как мы можем это скрыть. В главе 4 рассказывается о политических и экономических силах, поощряющих информационную незащищенность, — капитализме слежки (наблюдения), киберпреступности, кибервойне, а также об агрессивных методах работы корпораций и государств, использующих незащищенность в своих целях. И, наконец, в главе 5 мы поговорим о риске, почему он растет и из-за чего может принять непоправимый характер.

«Кибергейт» — это гипербола, но мы уже живем в мире, где атаки на компьютеры становятся причиной автомобильных аварий и вывода из строя электростанций. И то и другое может повлечь за собой катастрофические последствия, привести к огромным жертвам. Добавим к этому взломы компьютерных систем самолетов, медицинских приборов и ряда стратегически важных объектов и в итоге получим устрашающий сценарий, над которым есть причина поразмыслить.

Если вы знакомы с моими книгами и статьями, следите за моим блогом, то знаете, что в своих работах и публикациях я поднимаю большинство тем, которые раскрываются в части I этой книги. Если эти вопросы вам незнакомы, то после прочтения первых пяти глав вы будете прекрасно ориентироваться в теме.

Проблема защищенности интернета+ заключается в том, что мы привыкли к безопасности. За защиту компьютеров и сетевых данных отвечал рынок. Такой подход работал, пока проблема не приобрела иные масштабы. Если компьютер подвергался атаке, терялась важная информация или некто похищал ваши персональные данные. Приятного мало, плюс возникали непредвиденные траты, тем не менее случившееся не имело трагических последствий. Теперь, когда все превращается в компьютер, взлом системы представляет непосредственную опасность для жизни и имущества. Хакеры способны устроить автоаварию, выключить кардиостимулятор или вывести из строя городскую энергосистему. А это уже катастрофа.

В части II я говорю об изменениях в политике, необходимых для обеспечения защищенности интернета+. Главы 6, 7 и 8 посвящены тому, с помощью чего и как усиливается защищенность интернета+, а также кто это делает. Все это не ново и не сложно, но дьявол кроется в деталях. Я надеюсь, что к главе 8 вы осознаете, что «кто» — это правительство. Да, есть значительный риск в том, чтобы отдавать решение проблемы информационной безопасности на откуп правительству, но этому нет равноценной альтернативы. Та степень защиты интернета+, которую мы наблюдаем сейчас, — результат плохо отрегулированных бизнес-инициатив и действий правительства, для которого развитие интернета находится в большем приоритете, чем его безопасность. Одна из мер защиты, предложенных мной в главе 8, — создание нового правительственного агентства, которое координировало бы действия властей с действиями других ведомств и консультировало бы их по вопросам защищенности интернета+ и технологий. Вы можете со мной не согласиться, и это хорошо, потому что необходимо дискутировать и обсуждать эту проблему.

Глава 9 носит общий характер. Чтобы заручиться доверием граждан, правительство должно отдавать предпочтение обороне интернета+, а не нападению (наступлению) с его помощью. Я объясняю, как это сделать. С практической точки зрения маловероятно, что большинство изменений, которые я предлагаю в главах 6–9, будут приняты в обозримом будущем. Поэтому в главе 10 я стараюсь оставаться реалистом и рассуждаю о том, что произойдет и как на это следует реагировать как США, так и другим странам. В главе 11 я выдвигаю несколько предложений относительно направлений в сегодняшней политике, которые существенно снизят защищенность интернета+. Глава 12 опять-таки более общая и посвящена тому, как нам создать такой интернет+, где доверие, стойкость и мир станут нормой, и как это будет выглядеть. По сути, я привожу доводы в пользу того, что хорошее правительство творит добро. Это может быть трудной задачей,

особенно в строго либертарианской, компактной с точки зрения управления и настроенной против регулирования компьютерной индустрии, но это очень важно. В 2017 г. даже консервативный *The Economist* опубликовал материал, поддерживающий как контроль за умными вещами, так и ответственность, лежащую на них[47]. Мы часто слышим жалобы, что правительство делает ошибки, работает спустя рукава, да попросту встает на пути технического прогресса. Гораздо реже обсуждается, каким образом руководство страны управляет рынками, защищает физических лиц и сдерживает напор корпораций. Одной из главных причин сегодняшней незащищенности интернета+ я считаю отсутствие контроля со стороны государства (правительства). По мере того как риски приближаются к критическим отметкам, требуется все большее включение руководства страны в процесс защиты интернета+.

Заканчиваю книгу я обращением к политикам и экспертам в области технологий. Я призываю их к действиям. Политические дискуссии в своей основе являются техническими. Мы нуждаемся в политиках, которые разбираются в технологиях, и нам необходимо вовлечь в политику таких экспертов. Нужно сформировать пул специалистов, ратующих за интересы общества. А эта проблема гораздо шире, чем защищенность интернета+. Но я призываю к действиям в конкретной области технологий, поскольку разбираюсь именно в ней.

Кроме того, я поднимаю некоторые дополнительные темы.

Гонка вооружений в области безопасности. Зачастую безопасность полезно рассматривать как технологическую гонку вооружений между атакующей и обороняющейся сторонами. Атакующая сторона разрабатывает новую технологию, а обороняющаяся отвечает контртехнологией. Или обороняющаяся сторона разрабатывает технологию защиты, вынуждая атакующую сторону придумывать новые пути и методы ее преодоления. Понимание того, как эта гонка вооружений разворачивается в интернете+, критически важно для его защищенности.

Доверие. Хотя мы зачастую не думаем об этом, доверие — базис функционирования общества на всех его уровнях. В интернете также все строится на доверии. Мы доверяем компьютерам, программному обеспечению (ПО) и интернет-сервисам. Доверяем сегментам сети, которые не способны увидеть, и рабочим процессам в используемых устройствах. Осознание того, как мы сохраняем это доверие и как оно может быть подорвано, также важно для понимания защищенности интернета+.

Сложность (запутанность). В этой проблеме сложно и запутанно все: технологии, политика, взаимодействие технологий и политики. Добавим сюда экономику и социологию. Эти области знания многомерны, с течением времени они лишь усложняются. Проблему защищенности интернета+ принято называть wicked problem, поскольку ее трудно или даже невозможно решить. Имеется в виду не дьявольская сущность проблемы, а ее завуалированный характер и — как результат — сложное или вообще отсутствующее решение. О выработке разумного решения и говорить не приходится.

В книге затрагивается множество вопросов по теме, которые раскрываются схематически. Огромное количество сносок — одновременно и список рекомендуемой литературы, и приглашение к ее прочтению. Перечень был уточнен в конце апреля 2018 г. Он есть и на веб-сайте книги (https://www.schneier.com/ch2ke.html). На сайте https://www.schneier.com/ вы найдете ежемесячный бюллетень, а также ежедневно обновляемый блог по упомянутой тематике и остальные мои работы.

Поднятые в книге проблемы я оцениваю с метауровня, будучи, по сути, технологом, а не политиком и даже не политическим аналитиком. Именно поэтому я могу рассказать о технологическом подходе к решению проблем с защищенностью интернета+. Могу дать рекомендации, какую политику необходимо проводить, чтобы найти, выработать и реализовать эти технологические решения. Но я не пишу о поиске политических решений. Не могу рассказать, как получить необходимую

поддержку, или как вводить политические изменения, или даже о том, насколько они осуществимы. Признаюсь, книге этого действительно недостает.

Отмечу также, что я рассматриваю проблему с точки зрения американца. Большинство примеров взяты из реалий моей жизни, и бóльшая часть рекомендаций дается применительно к Соединенным Штатам. Во-первых, это то, что я знаю лучше всего. Во-вторых, я убежден, что у США уникальный опыт развития не по плану и — благодаря территории и положению на рынке — эта страна как никакая другая способна изменить ситуацию к лучшему. Несмотря на то что освещение международных проблем и геополитических аспектов защищенности интернета не было целью этой книги, я так или иначе затронул эти вопросы. В то же время на эту тему есть отличная работа под названием «Темная сеть: Война за киберпространство» (*The Darkening Web: The War for Cyberspace*)[48].

Проблема защищенности интернета непрерывно эволюционирует и неизбежно находит отражение в каждой публикации на аналогичную тему. Я помню, как в марте 2014 г. заканчивал книгу «Данные и Голиаф» (*Data and Goliath*). Мне думалось, что она выйдет через полгода, и я надеялся, что за это время не произойдет ничего такого, что повлияет на ее нарратив. То же самое чувство я испытываю и сегодня. Тем не менее я верю, что главное событие, из-за которого мне пришлось бы переписать эту книгу, не произойдет. Конечно, появятся свежие истории и примеры, но ландшафт, который я описываю, скорее всего, останется неизменным на протяжении многих лет.

Будущее защищенности интернета+, или кибербезопасности, если вам по душе такая терминология, — это неисчерпаемая тема, и вопросы, поднятые и раскрытые в большинстве глав этой книги, могли бы послужить основой для новых работ. Надеюсь, что, копая не столько вглубь, сколько вширь, помогу читателям составить представление о реальном положении дел, предоставлю им возможность осознать существующие

проблемы и предложу некий план действий. Цель я вижу в том, чтобы вовлечь как можно более широкую аудиторию в дискуссию по теме защищенности интернета+ и подготовить читателей к обсуждению поставленной проблемы на более глубоком уровне. В ближайшие несколько лет мы примем важные решения, даже если они будут сводиться к тому, чтобы не предпринимать никаких действий.

От рисков никуда не деться. И они никак не связаны с тем, насколько развита инфраструктура той или иной страны или насколько авторитарно ее правительство. Не ослабевают они и по мере того, как мы решаем глобальные проблемы, одна из которых — неэффективная политическая система Соединенных Штатов. Не исчезнут риски и под воздействием изменений на рынке. Преодолеваем же мы их лишь постольку, поскольку решили сделать это и согласились с политическими, экономическими и социальными издержками наших решений.

Мир создан из компьютеров, и нам нужно их защитить. Для этого следует начать думать иначе. В 2017 г. на конференции по безопасности интернета бывший председатель Федеральной комиссии связи (Federal Communications Commission — FCC) Том Уилер поддел экс-госсекретаря Мадлен Олбрайт, язвительно заметив, что «мы сталкиваемся с проблемами XXI века, обсуждаем их в терминах XX века и предлагаем решения XIX века»[49]. Он был прав. Нужно действовать эффективнее. От этого зависит наше будущее.

Миннеаполис (штат Миннесота),
Кембридж (штат Массачусетс), апрель 2018 г.

Часть I

Тенденция

Пару лет назад мне понадобилось заменить термостат. Я много путешествую, поэтому в свое отсутствие хотел экономить электричество. Новый термостат представлял собой подключенный к интернету компьютер, которым можно управлять со смартфона. Переключать программы, следить за температурой — и все удаленно. Очень удобно.

В то же время обнаружилось, что при использовании термостата могут возникнуть проблемы. В 2017 г. некий хакер хвастался в интернете, что удаленно взломал умный термостат Heatmiser (у моего устройства другой производитель)[1]. Другая группа кибервзломщиков продемонстрировала возможности вируса-вымогателя, созданного для атаки на термостаты двух популярных американских брендов (опять же, моего среди них нет), и потребовала определенную сумму в биткойнах за его деактивацию[2]. Если хакеры сумели внедрить вирус-вымогатель, то они могли бы включить термостат в сеть ботов и использовать его для атаки на другие интернет-сайты. Это был исследовательский проект, в ходе которого ни один термостат не пострадал, а все инженерные коммуникации остались в целости и сохранности. Однако опасность, что в любой момент могут атаковать именно мой термостат и это повлечет за собой непредсказуемые последствия, сохраняется.

Когда речь заходит о безопасности интернета+, нужно помнить о двух вещах.

Вещь первая: принципы обеспечения безопасности наших компьютеров и смартфонов становятся принципами обеспечения безопасности абсолютно всего. Поэтому, когда вы задумываетесь о незащищенности ПО, уязвимости входа в систему, аутентификации, обновлений, то есть о том, что мы будем обсуждать в части I, — все это относится не только к компьютерам и телефонам, но и к термостатам, автомобилям, холодильникам, имплантированным слуховым аппаратам, кофейникам, уличному освещению, дорожным знакам и вообще ко всему. Компьютерная безопасность становится всеобщей безопасностью.

Вещь вторая: уроки, извлеченные из практической реализации принципов компьютерной безопасности, касаются абсолютно всего. За последние несколько десятилетий специалисты в сфере компьютерной безопасности столкнулись с совершенно новым явлением — цифровой гонкой вооружений, многое узнали о природе компьютерных сбоев и осознали важность устойчивости системы (обо всем этом мы обязательно поговорим). Ранее подобного рода уроки имели отношение исключительно к компьютерам. Сейчас они имеют отношение абсолютно ко всему.

Проблема обеспечения компьютерной безопасности приобрела иные масштабы. Риски, связанные с проникновением интернета во все сферы нашей жизни, поистине огромны. Реальной угрозой нашего времени становится техническая возможность удаленно воздействовать на любые системы, будь то GPS-навигация мирового судоходства[3], двигатели самолетов[4] и автомобилей[5], электростанции, заводы по переработке токсичных отходов, медицинские приборы[6], что неизбежно спровоцирует сбой в этих системах и приведет к гибели множества людей. На карту поставлена безопасность наций и целых государств. Не к столь катастрофичным, но оттого не менее значимым последствиям способно привести вмешательство хакеров

в процесс электронного голосования на выборах, атака на умные дома с целью нанести ущерб имуществу конкретных людей[7], взлом банковской системы ради экономического коллапса.

Цифровая безопасность — это гонка вооружений между атакующей и обороняющейся сторонами. Подумайте о борьбе между рекламодателями и противниками рекламы. Если вы используете блокировщик рекламы (по всему миру так поступают около 600 млн человек)[8], то наверняка заметили, что некоторые сайты применяют программы — антиблокировщики рекламы, которые препятствуют ознакомлению с контентом до тех пор, пока вы не отключите антибаннер[9]. Подумайте о борьбе между спамерами, разрабатывающими новые методы принудительной рассылки навязчивой рекламной информации, и компаниями — их противниками[10]. Мошенничество с кликами — примерно то же самое: жулики используют различные трюки, чтобы убедить крупные компании, такие как Google, в том, что по ссылкам на платные рекламные объявления переходят реальные люди и что Google задолжал деньги мошенникам, тогда как Google пытается их вычислить. Никогда не прекращается гонка вооружений в области мошенничества с кредитными картами: атакующая сторона совершенствуется в методах взлома кредиток, а компании, их выпускающие, совершенствуют способы защиты. Нападениям со стороны хакеров подвергаются и банкоматы: военные действия ведутся с помощью скиммеров, миниатюрных устройств, которые крадут информацию с «пластика»[11], с помощью камер, считывающих ПИН-коды, а также удаленным способом — через интернет[12].

Следовательно, чтобы разобраться с безопасностью интернета+, нам следует осознать, насколько в принципе сегодня защищен интернет. Следует выявить и проанализировать технологические, экономические, политические и криминальные тенденции развития цифрового мира и благодаря этому понять, что ожидает нас в ближайшем будущем.

Глава 1

Компьютеры по-прежнему уязвимы

Соблюдение требований безопасности — это всегда компромисс. Иногда компромисс между безопасностью и удобством эксплуатации, время от времени — между безопасностью и функциональностью, а бывает, что компромисс между безопасностью и быстродействием. Наше стремление к комфорту, выбор в пользу него в ущерб безопасности — одна из главных причин уязвимости компьютеров. Справедливости ради стоит признать, что обеспечение безопасности компьютеров, как и информационной системы в целом, — задача поистине сложная.

В 1989 г. эксперт по безопасности интернета Юджин Спаффорд произнес знаменитую фразу: «Единственный по-настоящему безопасный компьютер — тот, что выключен, залит бетоном и под круглосуточной вооруженной охраной находится в герметичном помещении, стены которого обшиты свинцовыми листами. Но даже тогда меня одолевают сомнения»[1]. С тех пор прошло несколько десятков лет, однако почти ничего не изменилось.

Слова об уязвимости правдивы как по отношению к персональным компьютерам, изолированным от интернета, так и по отношению к устройствам, встроенным в приборы и подключенным к сети. Не так давно бывший директор

Национального центра кибербезопасности США Род Бекстром сделал следующее умозаключение: 1) всё, что подключено к интернету, уязвимо; 2) к интернету подключается всё; 3) всё становится уязвимым[2].

Защита компьютера настолько сложна, что у каждого исследователя в области безопасности на этот счет существует собственный афоризм. Вот мое изречение от 2000 г.: «Безопасность — это процесс, а не вещь»[3].

Тому есть множество причин.

Бóльшая часть ПО написана плохо и ненадежна

Я играю в Pokémon GO, и приложение часто сбоит — вылетает. Работа его крайне нестабильна, но не то чтобы подобное было чем-то из ряда вон выходящим. Каждому из нас приходилось сталкиваться с аналогичной проблемой либо при работе на компьютере, либо в процессе пользования смартфоном. Чтобы защитить хранящиеся в устройствах данные, мы создаем резервные файлы или используем системы, которые делают это автоматически. И даже тогда мы рискуем потерять важную информацию. Мы привыкли снисходительно относиться к издержкам «общения» с техникой такого типа, а потому, не ожидая от нее идеальной работы и внутренне готовясь к сюрпризам разного рода, пусть даже таковые нас совсем не радуют, перезагружаем компьютеры, когда те зависают.

Большинство компьютеров снабжены плохим ПО, потому что за редким исключением рынок не поощряет высококачественные программы. «Хорошо, быстро, дешево — выберите любые две из трех составляющих». Выбросить на рынок недорогую и быстро сделанную программу куда проще, чем корпеть над созданием качественного продукта. Что примечательно, на протяжении какого-то времени большинство из нас считает плохо написанное ПО достаточно хорошим.

Такой подход прижился в области компьютерных технологий и проявился на всех ее уровнях. Для среднестатистической

компании гораздо важнее получить продукцию с опережением графика и в рамках бюджета, нежели приобрести качественное ПО. Университеты с большей вероятностью ограничатся кодом, который едва работает, чем приобретут надежную программу. И мы как потребители ПО чаще всего не готовы платить дополнительные деньги за его улучшение.

Современные программы содержат мириады ошибок, некоторые из них — неотъемлемая часть сложного ПО[4] (подробнее об этом позже), однако большинство возникает на начальном этапе создания программы и не исправляется в процессе разработки. Соответственно, к потребителю ПО поступает с ошибками. Способность работать с некачественным кодом свидетельствует о нашем мастерстве.

В 2002 г. руководство компании Microsoft всерьез задумалось над тем, чтобы свести к минимуму количество уязвимостей в системе безопасности своих программ, и на улучшение процесса разработки ПО ушло целое десятилетие[5]. Продукты Microsoft все еще несовершенны — это за пределами существующих на сегодняшний день технологических возможностей, — но качество их намного выше среднего уровня. Компания Apple славится своим высококачественным ПО[6]. Как и Google. Некоторые небольшие, но критически важные сегменты ПО с самого начала отличались высоким уровнем исполнения. Например, программы для авионики написаны в соответствии с очень жесткими стандартами качества. Также и в НАСА: контроль за качеством ПО космических челноков обязателен[7].

Столь разное отношение к вопросам безопасности ПО у ИТ-специалистов разных отраслей продиктовано мерой ответственности и степенью рисков. Стратегически важные сферы имеют и более высокую степень защиты. Именно поэтому в НАСА действуют консервативные стандарты гарантии качества. На бытовом же уровне, пользуясь такими относительно высококачественными операционными системами, как Windows, macOS, iOS и Android, мы постоянно их обновляем и пропатчиваем.

Некоторые ошибки (баги) в ПО, безусловно, — уязвимости в системе безопасности, чем не преминут воспользоваться атакующие. Например, ошибка переполнения буфера позволяет злоумышленнику захватить контроль над компьютером и принудить его выполнять произвольные команды[8]. И таких багов множество. Точное количество не поддается исчислению. Мы не знаем, сколько ошибок следует рассматривать в качестве уязвимостей и сколько уязвимостей можно потенциально использовать[9]. На эту тему ведется самый настоящий диспут. Я твердо уверен, что большие программные системы содержат тысячи уязвимостей, а для взлома достаточно всего одной. Иногда ее просто найти, иногда — нет.

И хотя уязвимостей много, нельзя сказать, что они равномерно распределены по программе. Есть такие, которые выявить легко, и такие, которые выявить трудно. Инструменты, автоматически обнаруживающие и устраняющие или исправляющие целые классы уязвимостей, существенно повышают безопасность ПО. Очевидно, что, если кто-то выявил уязвимость, велика вероятность, что вскоре ее обнаружит (или уже обнаружил) другой. Heartbleed — большая брешь в безопасности интернета. Эту ошибку упускали из виду целых два года[10], зато открыли с разницей в несколько дней два исследователя, действующих независимо друг от друга. Уязвимости Spectre и Meltdown в компьютерных чипах существовали по меньшей мере лет десять, пока в 2017 г. их не обнаружили сразу несколько человек[11]. Я не нахожу объяснения этому феномену, поэтому ограничимся констатацией того факта, что параллельное обнаружение уязвимостей — это реальность. К этому вопросу мы вернемся в главе 9, когда будем говорить о правительствах, накапливающих программные уязвимости с целью шпионажа и создания кибероружия.

Взрывное увеличение числа устройств, взаимодействующих с интернетом вещей, означает, что количество программ, строк кодов, а значит, ошибок и уязвимостей станет расти

в геометрической прогрессии. Сохранение же дешевизны умных вещей — это привлечение к их созданию малоквалифицированных программистов, плохая отладка процесса разработки ПО и частое повторное использование кодов, то есть в случае широкого распространения уязвимости вред от нее будет огромным[12].

Чтобы обезопасить устройства, которые мы используем в повседневной жизни (компьютеры, телефоны, автомобили, медицинские приборы, системы управления домом), от вторжения хакеров, недостаточно находить и устранять уязвимости в ПО. Нужно подходить к процессу создания ПО с совершенно других позиций. За этим будущее системы безопасности.

Когда создавался интернет, вопрос о его безопасности даже не поднимался

В апреле 2010 г. часть мирового интернет-трафика (15%) изменила направление и прошла через серверы в Китае. Длилось это около 18 минут[13]. Мы не знаем, произошло ли это по распоряжению тамошнего правительства с целью протестировать возможности перехвата или хакеры действовали по собственной инициативе, зато знаем, как действовали атакующие: они нарушили протокол динамической маршрутизации (Border Gateway Protocol — BGP).

Протокол этот определяет, как интернет распределяет трафик по кабелям и соединительным узлам между интернет-провайдерами, странами и континентами. Чтобы система работала, аутентификация не требуется, а еще все безоговорочно доверяют любой информации о скорости и перегрузке каналов связи[14]. Поэтому BGP можно манипулировать. Из секретных документов, обнародованных работавшим на правительство [Соединенных Штатов] Эдвардом Сноуденом, мы узнали, что Агентство национальной безопасности США (АНБ) использует эту лазейку, чтобы «прослушивать» определенные потоки данных[15]. В 2013 г. некая компания сообщила о 38 случаях, когда интернет-трафик перенаправлялся на маршрутизаторы белорусских или исландских провайдеров[16]. В 2014 г. турецкое

правительство использовало этот способ, чтобы подвергнуть цензуре отдельные сегменты интернета. В 2017 г. трафик нескольких основных американских операторов связи был ненадолго перенаправлен к неизвестному интернет-провайдеру[17]. Не думайте, что подобные атаки практикуют исключительно службы государственных органов: в 2008 г. на Defcon* было продемонстрировано, что это может сделать кто угодно[18].

В самом начале эры интернета мерами его защиты были действия, предотвращающие физические атаки на сеть. Благодаря этому отказоустойчивая архитектура интернета обрабатывала сбои или повреждения серверов и соединений, но не справлялась с систематическими атаками на базовые протоколы. Многие из них остаются незащищенными до сих пор. Не обеспечивается безопасность в строке «от кого» в электронной почте: кто угодно может выдать себя за кого угодно. Отсутствует безопасность в службе доменных имен (Domain Name Service — DNS), которая переводит интернет-адреса из понятных человеку названий в воспринимаемые компьютером адреса, а также в протоколе сетевого времени (Network Time Protocol — NTP), призванном синхронизировать процессы. Небезопасны и оригинальные протоколы языка разметки гипертекста HTML (HyperText Markup Language), лежащие в основе работы Всемирной паутины, и даже протокол защищенной передачи гипертекстовых данных https (HyperText Transfer Protocol Secure). Атакующим по силам нарушить любой.

Протоколы разрабатывались в 1970-е — начале 1980-х гг., когда предполагалось, что интернет будет использоваться рядом исследовательских организаций, но не для решения глобальных или критически важных задач. Профессор Массачусетского технологического института и один из создателей раннего интернета Дэвид Кларк вспоминает: «Не нужно считать, что мы

* Defcon — крупнейшая в мире ежегодная конференция хакеров, проходит в Лас-Вегасе. — *Прим. пер.*

не задавались вопросом безопасности. Мы осознавали, что есть люди, которым не следует доверять, и полагали, что сможем исключить их из процесса пользования интернетом»[19]. Действительно, именно так все и было.

Еще в 1996 г. бытовало мнение, что безопасность — сфера ответственности конечных точек, то есть компьютеров, за которыми сидят люди, а не самой сети. Вот что было написано в том же 1996 г. в рекомендациях Инженерного совета интернета (Internet Engineering Task Force — IETF) — организации, определяющей стандарты индустрии: «Желательно, чтобы интернет-операторы защищали приватность и аутентичность трафика, но это не требование архитектуры. Конфиденциальность и аутентификация — ответственность конечных пользователей, она должна реализовываться в протоколах, которые они используют. Конечные точки не должны зависеть от конфиденциальности или добросовестности операторов. Последние могут выбрать предоставление определенного уровня защиты, но это вторично по отношению к ответственности конечных пользователей по защите самих себя»[20].

И это неправильно. В главе 6 мы поговорим о сквозной сетевой модели, при которой сеть не должна нести ответственность за безопасность, как предписывал IETF. Но люди настолько привыкли не учитывать обстоятельства, что не приняли в расчет даже аспекты безопасности, которые имело смысл включать только в сеть.

Исправить ситуацию оказалось очень сложно. Еще в 1990-е гг. IETF, чтобы предотвратить атаки, выпустил предложения по укреплению безопасности BGP, но те оказались уязвимы в части коллективного принятия безопасной системы. Дело в том, что защищенная система будет эффективной и экономически выгодной, если ее примет достаточное количество сетей. Те же, кто включается первым, несет финансовые издержки. Результатом такой ситуации становится ложный стимул: каждый предпочитает подождать и предоставить другим возможность стать первым[21]. В результате мы имеем то, что имеем: спустя 20 лет

после того, как мы впервые заговорили о проблеме безопасности интернета, решения по-прежнему нет.

Аналогичным образом обстоит дело с модулями безопасности службы доменных имен — DNSSEC* (Domain Name System Security Extensions). Это обновление, которое решило бы проблемы безопасности протокола DNS. С тех пор как 20 лет назад технологическое сообщество приняло решение внедрить это обновление, дело с места не сдвинулось: все выжидают, когда большинство сайтов примут DNSSEC и тем самым подтвердят его эффективность[22].

Многофункциональность компьютеров означает, что против нас могут использоваться любые методы

Помните телефоны, какие стояли в доме у родителей или у бабушки с дедушкой? Те аппараты разрабатывались и изготавливались как телефон, и их функции не выходили за рамки возможностей, заложенных производителем. Сравните их с устройством в вашем кармане. Это не совсем телефон — это компьютер с телефонным приложением. И, как вы знаете, он умеет намного больше, чем обеспечивать аудиокоммуникацию. Он и фотографирует, и снимает видео, и позволяет обмениваться сообщениями, и читать электронные книги, и много чего еще. Выражение «для этого есть приложение» нельзя использовать по отношению к старомодному телефону, зато вполне естественно произнести в адрес компьютера, который умеет совершать телефонные звонки.

Можно провести аналогию с книгоизданием допечатной поры и после изобретения печатного станка Иоганном Гутенбергом в 1440 г. С того времени технология только совершенствовалась: сначала станок был механическим, а потом — электромеханическим. Тем не менее он оставался только печатным станком. Независимо от усилий того, кто на нем работал, станок

* DNSSEC — набор расширений протокола DNS, которые позволяют минимизировать атаки, связанные с подменой DNS-адреса при разрешении доменных имен. — *Прим. пер.*