ВЗЛОМАТЬ ВСЁ

КАК СИЛЬНЫЕ МИРА СЕГО ИСПОЛЬЗУЮТ УЯЗВИМОСТИ СИСТЕМ В СВОИХ ИНТЕРЕСАХ

Книга о новых силах, способных подорвать энергию и целостность современного мира.

Стивен Пинкер

БРЮС ШНАЙЕР

ЛЕГЕНДАРНЫЙ ЭКСПЕРТ ПО КИБЕРБЕЗОПАСНОСТИ

Брюс Шнайер

Взломать всё. Как сильные мира сего используют уязвимости систем в своих интересах

«Альпина Диджитал»

2023

Шнайер Б.

Взломать всё. Как сильные мира сего используют уязвимости систем в своих интересах / Б. Шнайер — «Альпина Диджитал», 2023

ISBN 978-5-96-148999-6

Классический образ хакера – это специалист ИТ высочайшего класса, который знает несколько языков программирования, разбирается в устройстве систем безопасности и в два счета подберет пароль к вашему почтовому ящику. Он изучает системы для того, чтобы найти в них уязвимости и заставить работать в своих интересах. Однако взламывать можно не только компьютеры, но и социальные системы: от налогового законодательства до финансовых рынков и политики. В своей книге легендарный криптограф, специалист по кибербезопасности и преподаватель Гарварда Брюс Шнайер рассказывает о том, как могущественные, но неизвестные публике хакеры помогают богатым и влиятельным людям становиться еще богаче и манипулировать сознанием людей. Кроме того, он приводит огромное количество примеров хаков социальных систем: взломов тарифных планов для междугородних звонков, банкоматов, программ лояльности пассажиров, манипуляций на рынке элитной недвижимости и многих других. Прочитав ее, вы узнаете, как замечать взломы, и уже не сможете смотреть на мир по-прежнему.
Для кого Для тех, кто хочет лучше понимать, как богатые и влиятельные люди меняют правила под себя и управляют общественным сознанием.

ISBN 978-5-96-148999-6

Содержание

Брюс Шнайер
Взломать всё. Как сильные мира сего используют уязвимости систем в своих интересах

В книге упоминаются социальные сети Instagram и/или Facebook – продукты компании Meta Platforms Inc., деятельность которой по реализации соответствующих продуктов на территории Российской Федерации запрещена как экстремистская.

Переводчик *Михаил Белоголовский*
Научный редактор *Артем Деркач*
Редактор *Даниэль Орлов*
Главный редактор *С. Турко*
Руководитель проекта *А. Деркач*
Корректоры *М. Стимбирис, М. Смирнова*
Верстка *А. Абрамов*
Художественное оформление и макет *Ю. Буга*

* * *

ВЗЛОМАТЬ ВСЁ

КАК СИЛЬНЫЕ МИРА СЕГО ИСПОЛЬЗУЮТ УЯЗВИМОСТИ СИСТЕМ В СВОИХ ИНТЕРЕСАХ

БРЮС ШНАЙЕР

ПЕРЕВОД С АНГЛИЙСКОГО

альпина
ПАБЛИШЕР

Москва
2023

Предисловие

Говорят, что вода[1] никогда не бежит в гору.
Никогда не бежала, никогда не побежит.
Но если у тебя достаточно денег,
В законах природы всегда найдется лазейка.
И вот уже ручеек течет вверх по склону.

ДЖИМ ФИТТИНГ, песня «Water Never Runs Uphill» из репертуара группы Session Americana

Компания Uncle Milton Industries продает детские муравьиные фермы с 1956 г. Ферма представляет собой конструкцию из двух листов прозрачного пластика, соединенных между собой с зазором в 6 мм, запаянную с трех сторон, а с четвертой – имеющую крышечку. Идея заключается в том, чтобы заполнить это узкое пространство песком, запустить туда муравьев и с комфортом наблюдать, как они роют туннели.

Однако в самом наборе никаких муравьев нет. Довольно сложно сохранить их живыми, пока коробка лежит на магазинной полке, да к тому же наверняка существуют правила безопасности, касающиеся детей, игрушек и насекомых. Поэтому в комплекте с чудо-фермой идет почтовая карточка, на которой вы можете указать свой адрес, отправить ее в компанию, и через некоторое время вам доставят пробирку с живыми муравьями.

Большинство людей, впервые увидевших эту карточку, удивляются самому факту, что компания высылает клиентам пробирки с муравьями. Но моей первой мыслью было: «Вот это да! Я могу сделать так, что компания отправит пробирку с муравьями любому человеку, чей адрес я укажу».

Специалисты по кибербезопасности смотрят на мир иначе, чем большинство людей. Обычно, когда человек видит перед собой некую систему, он сосредоточивается на том, как она работает. Профессионал в сфере кибербезопасности, видя ту же систему, первым делом пытается понять, как можно вывести ее из строя, а точнее, как использовать сбой системы, чтобы заставить ее вести себя непредвиденным образом и делать такое, чего система в принципе не должна делать, но что способно дать хакеру определенное преимущество.

Это и есть взлом – разрешенные системой действия, которые подрывают цель или замысел самой системы. В точности, как отправка пробирок с муравьями компанией Uncle Milton Industries людям, для которых это стало бы полной неожиданностью.

Я преподаю курс кибербезопасности в Гарвардском институте государственного управления, больше известном как школа им. Кеннеди. В конце первого занятия я даю аудитории неожиданное задание[2] к нашей следующей встрече: через два дня каждый студент должен будет записать по памяти первые сто цифр числа пи. «Я понимаю, нет смысла надеяться, что вы запомните сотню случайных цифр за такой короткий срок, – говорю я им. – Поэтому рассчитываю, что вы будете хитрить. Единственное условие – не попадайтесь».

Спустя два дня аудитория гудит от возбуждения. Большинство студентов прибегают к старым уловкам, записывая цифры мелким почерком на клочках бумаги или наговаривая число на диктофон в надежде незаметно пронести наушник. Но кое-кто проявляет невероятную изобретательность. Один студент, к примеру, использовал невидимые чернила и очки, в которых цифры проявлялись. Другой написал искомое число на китайском языке, которого я, увы, не знаю. Третий закодировал цифры разноцветными бусинами и сделал из них ожерелье. Еще один запомнил несколько первых и последних цифр из сотни, а остальные взял из головы, полагая, что я не стану проверять всю последовательность. Но больше всего меня поразил случай, когда студент по имени Ян, потратив на это кучу времени, делая долгие паузы между

цифрами, записал весь необходимый ряд. Он закончил, когда все уже сдали ответы. Помню, как и я, и другие студенты смотрели на него, не понимая, как именно он это делает. Неужели парень действительно вычисляет в уме бесконечный ряд? Но все оказалось намного проще: хитрец запрограммировал телефон, и тот вибрировал в его кармане, передавая каждую цифру азбукой Морзе.

Смысл подобного задания вовсе не в том, чтобы превратить добросовестных студентов в жуликов. На лекциях я всегда напоминаю, что за списывание в Гарварде полагается исключение. Дело в другом: если они собираются заниматься государственной политикой в области кибербезопасности[1], они должны думать как жулики и воспитывать в себе хакерское мышление.

Моя книга рассказывает историю хакерства, сильно отличающуюся от того, что преподносят на эту тему фильмы, телепередачи и пресса. Вы не найдете подобной информации в книгах, посвященных взлому компьютерных систем или защите от хакерских атак. Это история о вещах куда более распространенных, фундаментально присущих человеку и гораздо более древних, нежели компьютер. Это история о деньгах и власти.

Настоящими прирожденными хакерами являются дети. Они взламывают системы инстинктивно, просто потому что не до конца понимают их правила и общий замысел. (В этом они схожи с системами искусственного интеллекта, о которых мы поговорим в конце книги.) Но хакингом вполне осознанно занимаются и весьма состоятельные люди. В отличие от детей или искусственного интеллекта они понимают и правила, и контекст. С детьми их роднит другое – многие не готовы признать, что правила, созданные для всех, применимы и к ним. Превыше всего они ставят собственные интересы, а в результате то и дело взламывают всевозможные системы.

Моя история хакерства выходит за рамки того, что делают с компьютерными системами скучающие подростки, конкурирующие правительства или не слишком радивые студенты, отлынивающие от учебы. Я также не беру во внимание представителей контркультуры. Хакер, который мне интересен, работает на крупную корпорацию, выборное должностное лицо или, к примеру, на хедж-фонд, находя лазейки в правилах финансовой игры, позволяющие выкачивать из системы дополнительную прибыль. Хакинг как таковой является неотъемлемой частью деятельности любого правительственного лоббиста. Благодаря хакингу социальные сети удерживают нас на своих платформах.

В моей книге хакинг – это то, чем занимаются богатые и влиятельные люди, нечто, что укрепляет существующие структуры власти.

В качестве примера приведу историю Питера Тиля. Roth IRA – это легальный пенсионный счет, разрешенный законом с 1997 г. Он предназначен для инвесторов среднего класса и имеет ограничения как на уровень дохода инвестора, так и на сумму инвестиций. Но миллиардер Питер Тиль, один из основателей PayPal, умудрился найти лазейку[3]. Используя этот пенсионный счет, он купил 1,7 млн акций собственной компании по цене $0,001 за акцию, превратив $2000 в $5 млрд, навсегда освобожденных от налогов.

Хакерство часто служит ответом на вопрос, почему правительство не в состоянии защитить нас от корпоративных или чьих-то личных интересов, подкрепленных могуществом и деньгами. Хакерство является одной из причин, по которой мы чувствуем бессилие перед государственной машиной. Богатые и влиятельные люди нарушают правила, чтобы увеличить свое богатство и власть, – это и есть хакерство. Они постоянно работают над поиском новых хаков, а также над сохранением найденных лазеек, чтобы извлечь из них максимальную прибыль. И это очень важный момент. Дело не в том, что богатые и влиятельные люди – непре-

[1] Автор использует здесь забавное сленговое выражение cybersexcurity (*букв. киберсексуальное любопытство*), созвучное с термином cybersecurity. – *Прим. пер.*

взойденные взломщики, а в том, что их с меньшей вероятностью за это накажут. Зачастую их хаки просто становятся общественной нормой. Чтобы исправить такое положение дел, необходимы изменения на уровне официальных институтов, но все осложняет очевидный факт: официальные лидеры – это те самые люди, которые подтасовывают карты не в нашу пользу.

Любая система может быть хакнута. В настоящее время взломаны уже многие крупные системы, и ситуация становится только хуже. Если мы не научимся контролировать этот процесс, наши экономические, политические и социальные системы начнут давать все более ощутимые сбои. В конце концов они просто рухнут, поскольку перестанут эффективно служить целям, для которых были предназначены, а люди потеряют к ним доверие. И это уже происходит. Скажите, что вы чувствуете, когда думаете о том, как Питеру Тилю сошла с рук неуплата налога на миллиардный прирост капитала?

Однако, как я покажу в дальнейшем, хакинг не всегда разрушителен. При должном использовании он является одним из способов эволюции и совершенствования систем. Именно так развивается общество. А точнее сказать, именно так люди развивают общество, не разрушая до основания то, что уже было построено. Взлом может быть и орудием светлой стороны. Фокус заключается в том, чтобы понять, как поощрять «хорошие» взломы, предотвращать «плохие» и отличать одни от других.

В дальнейшем хакерство станет еще более разрушительным, поскольку мы интенсивно внедряем искусственный интеллект (ИИ) и автономные системы. Все это компьютерные системы, и рано или поздно они будут взломаны, как и любые, им подобные. Системы ИИ уже влияют на социальные процессы, к примеру принимая решения о выдаче кредитов, найме и условно-досрочном освобождении; их взломы неизбежно повлекут серьезные экономические и политические последствия. Но еще более важным является факт, что в основе ИИ лежат процессы машинного обучения, а значит, не за горами то время, когда хакерами станут сами компьютеры.

Если заглянуть еще чуть дальше в будущее, можно увидеть, как системы ИИ начнут самостоятельно выискивать новые возможности для хакинга. Это изменит все. До сих пор хакерство было исключительно человеческим занятием. Хакеры – обычные люди, и потому общие для людей ограничения распространяются и на процесс взлома. Но скоро эти ограничения будут сняты. ИИ начнет хакать не только наши компьютеры, но и наши правительства, наши рынки и даже наши умы. ИИ будет взламывать системы с такой скоростью и мастерством, что самые крутые хакеры покажутся дилетантами. Читая эту книгу, держите в уме концепцию ИИ-хакинга – к ней мы вернемся в заключительной части.

Время, когда для нас критически важным стало умение распознавать взломы и защищаться от них, наступило. И помочь в этом могут специалисты по кибербезопасности. Вот почему эта книга так актуальна именно сейчас.

Однажды, уже не помню когда и где[4], я услышал такое высказывание по поводу математики: «Дело не в том, что математика может решить все мировые проблемы. Просто мировые проблемы было бы легче решать, если бы все чуть больше разбирались в математике». Думаю, то же самое справедливо и в отношении безопасности. Дело не в том, что хакерский подход способен решить все мировые проблемы. Просто мировые проблемы было бы проще решать, если бы все лучше разбирались в вопросах информационной безопасности.

Так что поехали.

Часть I
Хакинг для «чайников»

1
Что такое хак

«Хакинг», «хакер», «хак» или «взлом» – эти термины перегружены множеством смыслов[5], но четкого понимания, что же за ними стоит, как правило, нет. Определение, которое я даю понятию «хак», не является исчерпывающим и не претендует на незыблемую истинность. Но меня оно устраивает. Цель этого определения – показать, что мыслить как хакер полезно для лучшего понимания различных систем, причин их потенциальных сбоев и способов сделать системы более устойчивыми.

Определение

Хак[6] (*англ.* hack, hak – взлом)

1. Хитроумное, непредвиденное использование системы, которое: а) подрывает правила или нормы самой системы – б) за счет людей, так или иначе затронутых ее деятельностью.

2. Некое действие, допускаемое системой, недокументированное и не предусмотренное ее разработчиками.

Хакинг и мошенничество – не одно и то же. Иногда хак может иметь признаки мошенничества, но только в особых случаях. Мошенник всегда нарушает правила, делая то, что система недвусмысленно запрещает. Ввод чужого имени и пароля на сайте без разрешения владельца профиля, сокрытие части дохода при заполнении налоговой декларации или копирование чужих ответов на экзаменационном тесте – все это виды мошенничества. Ни одно из этих действий не попадает под определение хака.

Хак не является ни усовершенствованием, ни улучшением, ни инновацией. Усовершенствование – это когда вы тренируете свою подачу в теннисе и возвращаетесь на корт лучшим игроком. Улучшение имеет место, когда Apple добавляет новую функцию в iPhone. Инновация возникает, если вы обнаружили неизвестный ранее метод использования электронной таблицы. Иногда, впрочем, хак может являться инновацией или улучшением, например когда вы взламываете свой iPhone, чтобы добавить функции, которые Apple не одобряет, но все-таки это не одно и то же.

Хакинг нацелен на систему, чтобы обратить ее против самой себя, не нарушая целостности. Если я разобью окно вашей машины и заведу ее, замкнув провода зажигания, это нельзя назвать хаком. Если же я придумаю, как обмануть автомобильную систему бесключевого доступа, чтобы открыть дверь и включить зажигание, – то это уже хак.

Разница очевидна. Хакер – не тот, кто обводит вокруг пальца жертву. Хакер находит изъян в правилах системы и заставляет ее делать то, что системе делать не положено. Тем самым он обводит вокруг пальца саму систему и, соответственно, ее разработчиков.

Хак подрывает смысл системы, нарушая ее правила или нормы. Это именно «игра с системой». Хакерство занимает промежуточное положение между мошенничеством и инновациями.

«Хак» – термин во многом субъективный. Часто можно услышать: «Я скажу, хак это или не хак, лишь когда увижу своими глазами». О чем-то можно с уверенностью сказать, что это хак. О чем-то – что это точно не хак. Но есть довольно много явлений, которые находятся

в серой зоне между этими двумя полюсами. Навык скорочтения – это не хак. Невидимые глазу микроточки, тайно наносимые принтером, чтобы идентифицировать ваш документ, – определенно хак. Но вот CliffsNotes[2]… Здесь я не берусь утверждать.

Хак всегда сделан с умом. Часто он вызывает сдержанное восхищение (порой вкупе с праведным гневом) и реакцию типа «Круто, хотел бы и я додуматься до этого», даже если речь идет о вещах принципиально вам чуждых. Такая реакция характерна даже в тех случаях, когда в роли хакеров выступают отъявленные злодеи. Моя книга 2003 г.[7] Beyond Fear («За пределами страха») начинается с подробного объяснения, почему теракт 11 сентября «поражал воображение». Террористы нарушили неписаные правила угона самолетов. До них захват самолета подразумевал полет в заданную точку, политические требования, переговоры с правительствами и полицией и в большинстве случаев мирное урегулирование ситуации. То, что террористы сделали 11 сентября, чудовищно, но нельзя не признать изобретательность их хака. Они использовали оружие, разрешенное службами безопасности аэропортов, и превратили гражданские самолеты в управляемые ракеты, в одностороннем порядке переписав нормы авиационного терроризма.

Хакеры и их деятельность заставляют по-новому взглянуть на системы, из которых выстроен наш мир. Они разоблачают то, что мы принимаем как должное, зачастую ставя в неловкое положение сильных мира сего, а иногда заставляя людей платить непомерную цену. Если не брать в расчет терроризм, можно сказать, что люди любят хакеров, потому что они умны. Макгайвер[3] был хакером. Фильмы о побегах из тюрьмы и хорошо спланированных ограблениях полны умных хаков: «Мужские разборки», «Большой побег», «Мотылек», «Миссия невыполнима», «Ограбление по-итальянски», «11-», «12-», «13 друзей-» и «8 подруг Оушена».

Хак всегда оригинален. «Разве это разрешено?», «Я и не знал, что так можно!» – вот обычная реакция людей на очередной хак. Со временем правила и общественные нормы меняются, а с ними меняются и представления о том, что является хаком. Все хаки в итоге либо подпадают под запрет, либо становятся разрешенными действиями. Соответственно, то, что еще недавно считалось хаком, перестает им быть. Когда-то вам приходилось хакать свой смартфон, чтобы превратить его в беспроводную точку доступа; сегодня точка доступа является стандартной функцией iOS и Android. Напильник в торте, переданном в тюрьму сообщнику, изначально был хаком, но теперь это стандартный сюжетный ход, заставляющий тюремщиков быть начеку.

В 2019 г. кто-то использовал дрон[8], чтобы доставить мобильный телефон и марихуану в тюрьму штата Огайо. В то время я бы назвал это хаком, но сегодня запуски дронов рядом с тюрьмами в некоторых штатах напрямую запрещены, и подобный трюк перестал быть хаком. Недавно я прочитал о том, как некто использовал удочку[9], чтобы перебросить контрабанду через стену тюрьмы, а также о коте[10], пойманном в тюрьме Шри-Ланки с грузом наркотиков и SIM-карт. (За кота не волнуйтесь, он сбежал.) Все это определенно хаки.

Хаки часто бывают законными. Поскольку они следуют букве закона, но нарушают то, что мы называем «духом закона», незаконными они становятся только в том случае, если существует некое всеобъемлющее правило, прямо их запрещающее. Когда бухгалтер находит лазейку в налоговых правилах, это, как правило, законно, если нет более общего правила, запрещающего такое действие.

---

[2] CliffsNotes – изначально серия брошюр с кратким изложением и готовым анализом литературных произведений. Чтение подобных брошюр экономит студентам время, но снижает качество образования. Сегодня сайт https://cliffsnotes.com по тому же принципу предлагает базовые сведения из разных областей знаний. – *Прим. пер.*

[3] Ангус Макгайвер – секретный агент, герой популярных американских телесериалов. Будучи талантливым ученым и тонким психологом, Макгайвер в любых экстремальных ситуациях полагается исключительно на смекалку, знания и складной швейцарский нож. – *Прим. пер.*

В итальянском языке есть слово для обозначения такого рода вещей – furbizia, то есть изобретательность, которую итальянцы проявляют, чтобы обойти бюрократические препоны и неудобные законы. В хинди есть похожее слово, подчеркивающее ловкость и находчивость при решении проблем, – jugaad. В бразильском португальском эквивалентом является gambiarra.

Хаки бывают моральными и аморальными. Некоторые полагают, что если какая-то деятельность или поведение не противоречат закону, то они по умолчанию являются нравственными, но, конечно, мир устроен гораздо сложнее. Точно так же, как существуют аморальные законы, существуют и моральные преступления. Большинство хаков, которые мы будем обсуждать в этой книге, технически законны, но противоречат самому духу закона. (А законы – это лишь один из типов систем, которые можно взломать.)

Слово «хак» в своем нынешнем значении появилось на свет[11] в 1955 г. в Клубе технического моделирования железных дорог MIT[4] и быстро перекочевало в зарождающуюся область компьютерных наук. Первоначально оно описывало способ решения проблем, предполагающий сообразительность, новаторство и находчивость, без какого-либо криминального или даже соревновательного подтекста. Но к 1980-м гг. «хакингом» все чаще стали называть взлом систем компьютерной безопасности. Хакнуть компьютер означало заставить его сделать не просто что-то новое, а нечто такое, чего он делать не должен.

На мой взгляд, от компьютерного хакинга до хакинга экономических, политических и социальных систем всего один шаг. Все эти системы – не что иное, как наборы правил или норм, а значит, они точно так же уязвимы для взлома, как и компьютерные системы.

И это не новость. Люди взламывали системы общественного устройства на протяжении всей истории.

[4] MIT – Массачусетский технологический институт. – *Прим. ред.*

2
Системы и хакинг

Хакнуть можно любую систему, но сравнение между собой различных типов систем, например налогового кодекса и компьютерного кода, полезно для выявления их характерных особенностей и понимания того, как именно работает хак в каждом конкретном случае. Налоговый кодекс – это не программное обеспечение, он исполняется не на базе компьютера. Однако вы все равно можете считать его «кодом» в компьютерном смысле этого слова, серией алгоритмов, которые принимают входные данные (финансовую информацию за год) и выдают результат (сумму начисленного налога).

Налоговый кодекс невероятно сложен. Существует огромное количество нюансов, исключений и особых случаев, возможно, не для большинства из нас как физических лиц, но для богатых людей и разного рода предприятий. Он состоит из правительственных законов, административных постановлений, судебных решений и юридических заключений. В него также входят законы и нормативные акты, регулирующие деятельность корпораций и разнообразных партнерств. Дать достоверную оценку размерам налогового кодекса затруднились даже эксперты, по крайней мере, когда я их об этом спросил. Непосредственно налоговый кодекс[12] занимает около 2600 страниц. Нормативные акты и постановления Налогового управления увеличивают этот объем примерно до 70 000 страниц. Законы, касающиеся корпоративных структур и партнерств, не менее сложны, поэтому я предположу, что в общей сложности налоговый кодекс США занимает 100 000 страниц или 3 млн строк. Объем кода Microsoft Windows 10[13] составляет около 50 млн строк. Довольно странно сравнивать количество строк текста и строк компьютерного кода, но подобное сравнение все равно полезно. В обоих примерах высокий уровень сложности во многом связан с тем, как разные части кода взаимодействуют друг с другом.

Любой компьютерный код содержит *баги*. Баги – это ошибки в спецификации, ошибки программирования, ошибки, возникающие на разных этапах создания программного обеспечения, порой столь же обыденные, как опечатка или типографская неточность. Современные программные приложения, как правило, содержат сотни, если не тысячи багов. Баги есть во всем без исключения программном обеспечении, которое вы сейчас используете на компьютере, на телефоне и на любых устройствах интернета вещей (IoT) у вас дома или на работе. То, что все это программное обеспечение прекрасно работает большую часть времени, говорит о том, насколько малозаметными и несущественными могут быть баги. Вы вряд ли столкнетесь с ними в ходе обычного использования устройств, но они есть. Точно так же они имеются и в налоговом кодексе, со многими частями которого вы просто никогда не сталкивались.

Некоторые баги создают дыры в безопасности. Под этим я подразумеваю нечто очень конкретное: злоумышленник может преднамеренно вызвать баг, чтобы добиться нежелательного для разработчиков и программистов эффекта. На языке компьютерной безопасности мы называем такие баги «уязвимостями».

В налоговом кодексе тоже есть свои баги. Это могут быть ошибки в написании налоговых законов: ошибки на уровне слов, за которые проголосовал конгресс, а президент подписал в виде закона. Это могут быть ошибки в интерпретации налогового кодекса. Это могут быть просчеты, допущенные на этапе разработки законов, или непреднамеренные упущения того или иного рода. Они могут возникать из-за огромного количества способов взаимодействия различных частей налогового кодекса друг с другом.

Недавний пример – Закон о сокращении налогов и занятости от 2017 г. Этот закон был разработан в спешке, в закрытом режиме и принят без должного рассмотрения законодателями и даже без корректуры. Некоторые его части были написаны от руки, и просто

невозможно представить себе, что голосовавшие за или против принятия этого закона точно знали его содержание. В результате в текст вкралась ошибка, из-за которой пособия по смерти военнослужащих были отнесены к трудовым доходам. Следствием этой ошибки стало то, что члены семей погибших неожиданно получили налоговые счета[14] на суммы свыше $10 000. Это типичный баг.

Однако он не является уязвимостью, поскольку никто не может воспользоваться этой ошибкой, чтобы уменьшить свои налоговые счета. Но некоторые ошибки в налоговом кодексе являются уязвимостями. Например, существовал корпоративный налоговый трюк под названием «Двойной ирландский с голландским сэндвичем» – уязвимость, возникшая в результате взаимодействия налоговых законов ряда стран, которую в итоге устранили ирландцы.

Вот как это работало[15]. Американская компания передавала активы ирландской «дочке», которая взимала с нее огромные роялти с продаж клиентам в США. Это заметно снижало налоги компании в Штатах, а ирландские налоги на роялти были существенно ниже. Затем, используя лазейку в ирландском законодательстве, компания переводила прибыль на счета фирм в налоговых гаванях, таких как Бермуды, Белиз, Маврикий или Каймановы острова, чтобы освободить ее от налогов. Вторая ирландская компания, также облагаемая низким налогом, создавалась для продаж европейским клиентам. Наконец, использовалась еще одна уязвимость и в цепочке возникала голландская компания-посредник, с помощью которой прибыль перегоняли обратно в первую ирландскую компанию и далее в офшор. Эта схема особенно популярна у высокотехнологических компаний, которые передают права интеллектуальной собственности своим иностранным «дочкам», а те, в свою очередь, укрывают денежные активы в налоговых гаванях.

Именно таким образом Google, Apple и другие технологические гиганты избегают уплаты справедливой доли налогов в США, несмотря на то что являются американскими компаниями. Это определенно не предусмотренное законодателями использование налоговых кодексов трех стран, хотя стоит отметить, что Ирландия намеренно придерживалась мягких налоговых правил, чтобы привлечь американские компании. И это очень выгодная ситуация для хакеров. По оценкам, только в 2017 г. американские компании уклонились от уплаты налогов[16] в США почти на $200 млрд, разумеется, за счет остальных налогоплательщиков.

В налоговом мире баги и уязвимости называются лазейками, а их использование злоумышленниками – стратегией ухода от налогов. Тысячи профессионалов – налоговые юристы и бухгалтеры из числа тех, кого в мире компьютерной безопасности мы называем «черными шляпами»[5], – скрупулезно исследуют каждую строку налогового кодекса в поисках уязвимостей, которые можно было бы использовать для собственной выгоды.

Мы знаем, как исправлять баги в компьютерном коде. Во-первых, мы можем использовать различные инструменты для их обнаружения еще до того, как код будет закончен. Во-вторых, уже после того, как код начнет работать, мы можем выискивать, а самое главное – быстро устранять баги различными способами.

Эти же методы применимы и к налоговому кодексу. Налоговое законодательство 2017 г. ограничило вычеты по налогу на имущество[17]. Это положение вступило в силу только в 2018 г., поэтому кое-кто придумал хитрый хак – досрочно уплатить налог на недвижимость за 2018 г. в 2017 г. Незадолго до конца года налоговое управление США вынесло решение о том, в каких случаях это было законно, а в каких нет, и приняло исправления в Налоговый

[5] «Черные», «белые» и «серые шляпы» – устоявшаяся классификация хакеров по их мотивации. Взята из голливудских вестернов, где положительные персонажи носили белые шляпы, отрицательные – черные, а неоднозначные, соответственно, серые. «Черные шляпы» из мира хакеров движимы корыстными целями: финансовой выгодой, местью или идеологическими мотивами. «Белые шляпы» работают в интересах компаний и взламывают их системы, чтобы устранить недостатки. «Серые шляпы» ищут уязвимости в системах без разрешения их владельцев, но и без злого умысла. – *Прим. пер.*

кодекс для защиты от подобных действий. В большинстве случаев они были сочтены незаконными.

Однако зачастую все не так просто. Некоторые лазейки прописаны в законе и не могут быть исключены из него в мгновение ока. Принятие любого налогового законодательства – это всегда большая проблема, особенно в США, где оно обсуждается с особым пристрастием. Ошибку с подоходным налогом для семей военнослужащих, возникшую в 2017 г., начали исправлять лишь в 2021 г. И до сих пор конгресс не устранил ее: пока исправлена только еще более старая ошибка, которая взаимодействовала с ошибкой 2017 г., а ее окончательное устранение будет завершено в 2023 г. (И это еще довольно легкий случай, поскольку все признают, что ошибка имеет место.) У нас нет возможности править налоговый кодекс с той же оперативностью, с которой мы устраняем баги в программном обеспечении.

Есть и другой вариант: уязвимость остается в системе и постепенно становится частью обычного порядка вещей. Многие налоговые лазейки прекращают свое существование именно так. Иногда их принимает Налоговое управление США, иногда суды подтверждают их законность. Уязвимости могут не совпадать с целями налогового законодательства, но текст закона позволяет их использовать. Иногда они даже задним числом легализуются конгрессом после того, как за них заступятся избиратели. Все это и есть процесс развития систем.

Хак подрывает замысел системы. Какой бы юрисдикцией ни обладала управляющая система, она либо блокирует хак, либо разрешает его – явно или неявно, просто не предпринимая ответных действий.

3
Что такое система

Хакер соблюдает правила системы, но нарушает ее дух и замысел.

Для того чтобы хак состоялся, должна быть система правил, которую можно взломать. Поэтому мне нужно сделать отступление и уточнить, что означает понятие «система», по крайней мере в том смысле, в каком я его использую.

> **Определение**
>
> Система (*англ.* system). Сложный процесс, ограниченный набором правил или норм, предназначенный для достижения одного или нескольких желаемых результатов.

Текстовый процессор, с помощью которого я набрал этот абзац, представляет собой систему: электронные сигналы, ограниченные набором программных правил, предназначенных для создания текста. Слова появились на экране – это и есть мой желаемый результат. Создание этой книги как продукта – результат уже другой системы, процессы которой включают в себя дизайн страниц, их печать, сшивание в определенном порядке, наложение суперобложки и транспортировочную упаковку. Каждый из этих процессов выполняется в соответствии с набором четких правил. Две эти системы, а также ряд других приводят к созданию бумажной книги, которую вы держите в руках, или электронного файла, который вы читаете на своем устройстве либо воспроизводите для прослушивания. Это верно независимо от того, собраны элементы системы под одной крышей или разбросаны по всему миру. Это верно независимо от того, является ли результат реальным или виртуальным, бесплатным или дорогостоящим, выпущенным ограниченной партией или общедоступным. В процессе всегда будут задействованы одна или несколько систем.

Всякая система имеет правила. Ими могут быть законы, правила игры, неформальные правила группы или процесса, негласные социальные правила. Когнитивные системы тоже следуют законам – законам природы.

Хак – это всегда то, что позволяет сама система. И под словом «позволяет» я имею в виду нечто конкретное. Дело не в том, законен ли хак, социально приемлем или этичен, хотя все это может быть ему свойственно. Речь идет о том, что система, как она создана, не препятствует взлому самой себя. Система допускает хак непреднамеренно, случайно, но эта случайность является следствием того, как она была спроектирована. В технических системах это обычно означает, что осуществить взлом позволяет программное обеспечение, в социальных системах – что правила или законы, управляющие системой, не запрещают взлом напрямую. Вот почему мы используем слово «лазейка» для описания хаков.

Исходя из сказанного, хакингу подвержены системы, участники которых заранее договорились – явно или неявно – соблюдать общий набор правил. Иногда внутренние правила системы не совпадают с законами среды, в которой она существует. Я понимаю, что это сбивает с толку, поэтому объясню на примере. Компьютер управляется набором правил в виде запущенного на нем программного обеспечения. Хакнуть компьютер означает так или иначе обойти эти правила. Но помимо этого существуют внешние по отношению к компьютеру законы, которые потенциально регулируют то, что с ним можно делать и чего нельзя. К примеру, в США Закон о компьютерном мошенничестве и злоупотреблениях квалифицирует большинство форм взлома как уголовное преступление. (Обратите внимание, что происходит: взламывается компьютерная система, но более общая правовая система защищает ее.) К слову, довольно спорный момент, насколько общим должен являться такой закон, ведь

в своем нынешнем виде он создает ловушку, поскольку любой взлом компьютера считается незаконным.

Профессиональный спорт регулируется четким набором правил и потому часто становится мишенью хакеров. Собственно говоря, любые законы в юридическом смысле – не что иное, как набор правил, а значит, их тоже можно взламывать.

В некоторых системах внутренними правилами являются сами нормативно-правовые акты или, по крайней мере, они и обеспечивают существование этих правил. Далее, когда мы будем знакомиться с хакингом финансовой и правовой систем, мы увидим, что незначительные опечатки или слишком запутанные формулировки в законопроектах, контрактах, судебных заключениях способны открыть путь всевозможным эксплойтам[6], которые не были предусмотрены составителями законов и судьями.

Обратите внимание на одну очень важную вещь: правила не обязательно должны быть явными. В нашем мире существует множество систем, особенно социальных, которые ограничены нормами. Нормы менее формальны, чем правила; часто неписаные, они, тем не менее, определяют поведение. Мы все время ограничены социальными нормами, причем для разных ситуаций они разные. Даже политика регулируется нормами в той же степени, что и законом, чему мы неоднократно становились свидетелями в последние годы, когда в США нарушались норма за нормой.

Мое определение системы включает в себя слово «предназначенная», что подразумевает наличие проектировщика – того, кто определяет желаемый результат. Это важный элемент определения, но на самом деле он верен лишь отчасти.

В случае с компьютерами взламываемые системы намеренно создаются человеком или организацией, а значит, успешный хакер оставляет с носом конкретных разработчиков системы. Это также верно для разнообразных сводов правил, установленных каким-нибудь руководящим органом: корпоративных процедур, спортивных правил или конвенций ООН.

Однако многие системы, которые мы будем обсуждать в этой книге, не имеют индивидуальных разработчиков. Рыночный капитализм проектировался не кем-то одним – это результат труда многих людей, приложивших руку к его эволюции на протяжении немалого времени. То же самое относится и к демократическому процессу; в США это проявляется как сочетание Конституции, законодательства, судебных решений и социальных норм. Поэтому, когда хакер замахивается на социальные, политические или экономические системы, он намеревается переиграть целую комбинацию факторов, куда входят обособленные друг от друга разработчики системы, социальный процесс, посредством которого система развивалась, и социальные нормы, управляющие этой системой.

Наши с вами когнитивные системы развивались с течением времени тоже без участия проектировщика. Неотъемлемой частью биологических систем является эволюция: постоянно возникают новые способы применения систем существующих, старые системы перепрофилируются, а ненужные – атрофируются. Но нас в первую очередь интересует *цель* той или иной биологической системы. Какая цель у селезенки? А у миндалевидного тела? Эволюция – это способность системы «проектировать» себя без участия проектировщика. Поэтому живые системы мы будем изучать, начиная с их функций в организме или экосистеме, даже если никто не ставил для них цель.

Хакинг – это естественный результат системного мышления. Системы пронизывают практически все сферы нашей жизни. Системы лежат в основе нашего общества. Они становятся не только все более многочисленными, но и все более сложными по мере усложнения самого общества. И хакинг систем становится все более важным условием их развития.

---

[6] Эксплойт (exploit, sploit; *проф. сленг)* – программа, использующая конкретную уязвимость ПО или создающая условия для исполнения другого кода, который в обычных условиях неисполним. – *Прим. пер.*

По сути, если вы хорошо и глубоко понимаете систему, вам нет нужды играть по правилам, придуманным для всех остальных. Вместо этого вы можете искать и находить недостатки и упущения в этих правилах. В какой-то момент вы замечаете, что те или иные ограничения, которые система накладывает на вас, не вполне справляются со своей задачей. И тогда вы взламываете систему. Если же при этом вы еще богаты и влиятельны, то, скорее всего, проделка сойдет вам с рук.

4
Жизненный цикл хака

С точки зрения компьютерной безопасности хак состоит из двух частей: уязвимости и эксплойта.

Уязвимость – это особенность системы, которая позволяет ее взломать. Для компьютерной системы она может быть ошибкой или упущением в проекте, спецификации или непосредственно в самом коде. Это может быть чем-то незначительным, как пропущенная скобка, или, наоборот, чем-то важным, как свойство архитектуры программного обеспечения. В любом случае взлом становится возможен лишь благодаря уязвимости. Механизм, посредством которого эту уязвимость используют, называется эксплойтом.

Если вы заходите на сайт, передающий ваше имя пользователя и пароль в незашифрованном виде, – это уязвимость. Программа, которая отслеживает интернет-соединения, фиксирует ваше имя пользователя и пароль, а затем применяет их для получения доступа к вашей учетной записи – это эксплойт. Если программное обеспечение позволяет видеть личные файлы другого пользователя, она содержит уязвимость, а эксплойтом станет другая программа, с помощью которой это можно будет сделать. Если есть возможность открыть дверной замок без ключа – это тоже уязвимость. Эксплойтом в данном случае послужит любой инструмент, подходящий на роль отмычки.

В качестве примера приведу историю EternalBlue. Это кодовое название эксплойта для операционной системы Windows, который работал на АНБ (Агентство национальной безопасности) в течение как минимум пяти лет, вплоть до 2017 г., когда его выкрали у агентства русские. EternalBlue использует уязвимость, допущенную Microsoft в протоколе Server Message Block (SMB), ответственном за обмен данных между клиентом и сервером. То, каким образом был закодирован SMB, давало возможность злоумышленнику отправить через интернет тщательно подготовленный исполняемый код, запустить его выполнение на принимающем компьютере под управлением Windows и таким образом получить над этим компьютером контроль. Строго говоря, АНБ могло использовать EternalBlue для удаленного управления практически любым компьютером, подключенным к интернету, на котором установлена операционная система Windows.

Процесс хакинга часто бывает распределенным между несколькими участниками, каждый из которых обладает специфическими навыками, однако под словом «хакер» подразумевают их всех, что вносит изрядную путаницу. Как минимум, существуют три группы участников. Во-первых, это творцы – те, кто используют свое любопытство и опыт для обнаружения возможности взлома и создания эксплойта. В случае с EternalBlue уязвимость обнаружил специалист из АНБ, а ирландскую налоговую лазейку – эксперт по налогам, который кропотливо изучал законодательства разных стран и их взаимодействие. Во-вторых, это те, кто применяют эксплойт на практике. В АНБ это были сотрудники, которые использовали эксплойт против конкретных целей, а в бухгалтерской фирме – бухгалтеры, реализующие стратегии ухода от налогов конкретных корпораций.

Такие хакеры используют для взлома чужой творческий потенциал, и в компьютерном мире мы в шутку окрестили их «скрипт-кидди» – детишками, не ведающими, как работают программы, лежащие в основе того или иного хака. Эти ребята не слишком умны и креативны, чтобы создавать новые хаки, но они вполне справляются с запуском программ-скриптов, которые автоматически высвобождают результаты чужого творчества.

И, наконец, есть организации или конкретные люди, которые являются заказчиками. Откройте новости: АНБ хакает иностранную сеть, Россия – США, а Google – налоговый кодекс. Важно это понимать, поскольку мы еще не раз будем говорить о том, как богатые и влиятель-

ные люди хакают разнообразные системы. Да, богатство и власть сами по себе не являются непременным условием появления продвинутых хакеров, но они открывают доступ к такого рода услугам. США, Россия и Google могут себе позволить нанимать самых одаренных и с их помощью успешно взламывать системы.

Когда мы говорим о хакинге, то применительно к хаку используем глаголы «создать» и «обнаружить». Если быть точным, обнаруживают уязвимость, а затем создают эксплойт, но слово «обнаружить» нравится мне куда больше, поскольку оно акцентирует внимание на том факте, что возможность взлома скрыта в самой системе и присутствует в ней еще до того, как кто-нибудь догадается о ее существовании.

Что именно будет происходить после обнаружения хака, зависит от того, кто его обнаружил. Как правило, такой человек или организация используют хак в своих интересах. В компьютерном мире это может быть хакер с преступными намерениями, национальная разведывательная служба вроде АНБ или нечто среднее между ними. В зависимости от того, кто и как начинает использовать хак, другие потенциальные бенефициары могут узнать о нем или не узнать. Но у них всегда остается шанс обнаружить его самостоятельно, потратив недели, месяцы или годы.

В ряде систем выгода, которую может приносить хак, определяется тем, как часто и насколько публично им пользуются. Обнаруженная уязвимость в банковской системе может использоваться преступниками «по-тихому», время от времени и оставаться для банка слепой зоной в течение многих лет. Хорошие хаки в сфере Налогового кодекса, как правило, распространяются очень быстро, поскольку становятся объектом продажи[18]. Искусная психологическая манипуляция может стать достоянием общественности, как только о ней заговорит достаточное количество людей, а может и оставаться неизвестной широкому кругу на протяжении многих поколений.

В любом случае рано или поздно наступает момент, когда система реагирует. Взлом можно нейтрализовать, если исправить базовую уязвимость. Под этим подразумевается, что есть кто-то, способный обновлять систему с целью устранять уязвимости или каким-то иным образом делать их непригодными для использования. Нет уязвимости – нет взлома. Все просто.

Контроль над целевой системой и ответственность за процессы ее обновления очевидны в случае, например, операционных систем, таких как Windows, или любых других крупных программных пакетов, за которыми стоит разработчик. Microsoft и Apple сделали исправление своих систем обязательным регулярным процессом.

Программы с открытым исходным кодом или с публичным доменом тоже относятся к этой категории: за ними обычно стоят конкретные люди или организации, а их код находится на всеобщем обозрении. Однако в отношении недорогого программного обеспечения для устройств IoT обновления как метод устранения уязвимостей работают уже не так хорошо. Большая часть подобного ПО разрабатывается с минимальной нормой прибыли, а команды программистов собираются под проект, после чего расформировываются. Но что еще хуже, многие устройства IoT в принципе не поддаются исправлению. И дело вовсе не в том, что это некому сделать: во многих IoT-устройствах компьютерный код встроен не в программное, а в аппаратное обеспечение, то есть невозможность его исправить заложена в самой природе этих устройств. Проблема усугубляется по мере того, как компании прекращают производство моделей или уходят с рынка, оставляя после себя миллионы осиротевших устройств, подключенных к интернету.

В целом в технических системах уязвимости часто исправляют сразу после их обнаружения. Это далеко не так просто в случае систем социальных, о которых пойдет речь в этой книге. Обновление Налогового кодекса, например, требует многолетнего законодательного процесса. Люди, получающие выгоду от хака, могут успешно лоббировать против любых изменений в законе. Часто возникают законные разногласия по поводу того, приносит ли тот или иной

хак пользу обществу, что еще больше затрудняет устранение уязвимостей. И, как мы увидим далее, богатые люди, наделенные властью, имеют колоссальное влияние на процессы решения подобных проблем, которые номинально являются демократическими.

Если взломанная система не будет исправлена вовремя, то хак становится частью ее правил. Так рождается новая норма. Поэтому то, что начинается как взлом, может вскорости стать чем-то привычным и легитимным. Такова была судьба многих нетехнических хаков, о которых пойдет речь в этой книге.

5
Вездесущность хакинга

Какой бы закрытой ни была система, уязвимости будут присутствовать в ней всегда, а следовательно, и возможность взлома. В 1930 г. австро-венгерский математик Курт Гёдель доказал, что все математические системы либо неполны, либо имеют внутренние противоречия. На мой взгляд, это утверждение справедливо не только для математических систем, но и в более широком смысле. В любых системах существуют несоответствия и упущения, которыми можно воспользоваться. В частности, системы правил вынуждены балансировать на тонкой грани между полнотой и доступностью, связанные языковыми ограничениями и возможностями понимания. Соедините это с естественной человеческой потребностью в преодолении разнообразных границ, а также с тем фактом, что уязвимости для любой системы – это неизбежность, и вы поймете, что хакеры есть везде.

Club Penguin – детская онлайн-игра компании Disney, просуществовавшая с 2005 по 2017 г. Общение детей с незнакомцами в интернете справедливо вызывает беспокойство их родителей, поэтому Disney создала режим Ultimate Safe Chat, который запрещал свободный ввод текста, ограничивая игроков заранее подготовленным списком реплик. Идея заключалась в том, чтобы оградить детей от буллинга и контакта с потенциальными педофилами. Но дети есть дети, они хотят общаться друг с другом несмотря ни на что. Поэтому они просто хакнули это ограничение, изображая буквы и цифры фигурками своих аватаров.

Дети – прирожденные хакеры. Они не понимают намерений, которые стоят за системой, и, как следствие, не видят ее ограничений, что свойственно взрослым. Дети видят проблему комплексно и могут хакнуть систему, даже не осознавая, что делают. Нормы, а уж тем более законы имеют на них куда меньшее влияние, чем на их родителей. Проверка правил на прочность – это всегда признак независимости.

Подобно Club Penguin, многие детские онлайн-игры вводили ограничения на высказывания в чате, чтобы предотвратить саму возможность травли и любого преследования. Дети взломали их все без исключения[19]. Чтобы обойти модераторов и фильтры ненормативной лексики, дети используют такие уловки, как намеренные ошибки в написании, например PHUQ вместо fuck you, разделение ключевой информации на несколько высказываний, чтобы ни одно из них не нарушало правил, и акростих, шифруя свои послания начальными буквами разрешенных фраз. Некоторые сайты запрещали пользователям вводить цифры – в ответ на это дети стали использовать слова: win вместо one (один), too вместо two (два), tree вместо three (три) и т. д. Тот же прием с созвучными искажениями применялся и для нанесения оскорблений: lose her означало looser (неудачник), a stew putt – stupid (дурак).

Школы пытаются ограничить использование учениками школьных компьютеров, в ответ на это ученики их взламывают. Успешные хаки такого рода распространяются моментально. После того как в школах одного из округов ограничили количество сайтов, которые разрешено посещать ученикам, те быстро сообразили, что VPN позволяет обойти ограничения и к тому же сделать это скрытно. Когда в другом районе заблокировали доступ к чатам, дети тут же нашли решение и стали общаться с помощью общего файла Google Doc.

Этот прием не нов. У него даже есть название – *фолдеринг*[20]. В разное время его использовали для сокрытия информации экс-глава ЦРУ генерал Петреус, руководитель избирательной компании Дональда Трампа 2016 г. Пол Манафорт и террористы, устроившие атаку 11 сентября 2001 г. Все они понимали, что могут избежать слежки, если будут пользоваться одним почтовым ящиком со своими сообщниками и писать друг другу письма, сохраняя их в виде неотправленных черновиков.

Во времена моего детства существовали хаки для обхода правил телефонной системы. Если вы слишком молоды, чтобы помнить такое, я объясню. Человек звонил на телефонную станцию, вызывал оператора, сообщал ему, кто он такой, и говорил, что хочет сделать междугородний групповой звонок. Оператор звонил по указанному номеру и спрашивал абонента, согласен ли тот принять групповой звонок за свой счет. Групповые звонки стоили весьма недешево. Но поскольку оператор сам инициировал звонок другой стороне, информация могла быть передана ей еще до того, как начинала взиматься плата. Итак, мы делали запрос группового звонка, оператор спрашивал указанного абонента – как правило, кого-то из наших родителей, – согласен ли тот принять групповой звонок, родители отвечали «нет», а затем перезванивали нам уже по стандартным, не таким дорогим тарифам. Подобные трюки можно было сделать и более эффективными. В некоторых семьях был даже список имен, которыми звонивший представлялся оператору в зависимости от ситуации; к примеру, имя Брюс могло означать «прибыл благополучно», Стив – «перезвоните» и т. д. (Оператор не знал настоящего имени звонившего.) Даже сегодня люди пользуются телефонными хаками, чтобы обойти правила тарификации. В Нигерии это называется «подмигнуть»[21]: звонишь кому-нибудь и кладешь трубку до того, как он успеет ответить. В Индии в первой половине 2010-х гг. такие хаки тоже были широко распространены[22], поскольку стоимость звонков на сотовые и стационарные телефоны заметно отличалась. Все эти хаки предназначены для подрыва телефонных систем, чтобы обмениваться информацией, не платя за эту привилегию.

Домашнее обучение во время пандемии[23] COVID-19 пробудило хакерские способности во многих школьниках. Один сообразительный ученик переименовал себя в «Reconnecting…» и просто выключил видеосвязь, чтобы учитель думал, что у него проблемы с подключением. В марте 2020 г., в первые месяцы пандемии, власти Китая полностью закрыли город Ухань, а его школы перевели на дистанционное обучение. В ответ на это ученики стали заваливать приложение DingTalk, через которое осуществлялся образовательный процесс, отзывами с одной звездой[24], надеясь, что таким образом оно будет удалено из магазинов приложений. (Увы, это не сработало.)

Системы всегда существуют по определенным правилам, а значит, имеют тенденцию быть жесткими. Они ограничивают наши возможности, и это устраивает далеко не всех. Поэтому мы и взламываем системы. Как только вы лучше поймете, что такое системы и как они работают, вы начнете замечать их повсюду. И точно так же повсюду начнете видеть последствия хакинга.

Само по себе это не означает, что абсолютно все системы взломаны. Вспомните Гёделя[25]. Среди юристов есть поговорка: «Все контракты неполны». Контракты исполняются не потому, что они жестко препятствуют нарушению сторонами договорных условий, а потому, что, как правило, имеют место доверие и благонамеренность. Если же дела идут плохо, существуют системы арбитража[26] и судебного разбирательства. Да, это может показаться наивным и идеалистичным, но именно благодаря системам, основанным на доверии, и функционирует наше общество. Мы не требуем от наших соглашений абсолютной защиты, потому что: 1) этого невозможно достичь, 2) любая попытка будет слишком долгой и громоздкой и 3) нам это попросту не нужно.

То же самое справедливо и в отношении прочих систем. Систему заставляет работать вовсе не ее предполагаемая неуязвимость, а все та же комбинация доверия и судебного разбирательства. Несмотря на то что мы говорим здесь о хаках и хакерах, все это в значительной степени является исключением из правил. Большинство людей не взламывают системы, и системы основную часть времени справляются со своими функциями. И когда взломы все-таки происходят, у нас есть системы для борьбы с ними. Это и есть устойчивость. Это то, на чем держится общество. Именно так люди справлялись с хакерством на протяжении тысячелетий.

Не все системы одинаково подвержены взлому. Далее, по мере изложения, вы познакомитесь с характеристиками систем, которые делают их более или менее уязвимыми для хакеров. Самыми уязвимыми являются сложные системы с большим количеством правил, хотя бы в силу того, что в них скрыто больше непредвиденных последствий. Сложность – злейший враг безопасности[27]. Это безусловно верно в отношении систем компьютерных, но справедливо и для таких систем, как налоговый кодекс, финансовые рынки и искусственный интеллект. В целом чем более гибкими социальными нормами и правилами ограничена система, тем более она уязвима для взлома, поскольку оставляет больше возможностей для интерпретации и, следовательно, содержит в себе больше лазеек.

С другой стороны, хакинг систем менее критичных, менее масштабных и, возможно, в чем-то экспериментальных причинит куда меньше вреда. Поэтому лучше позволить этим системам развиваться благодаря хакерам, чем тратить время и силы на защиту от них. Если беспечно позволить хакнуть, к примеру, процесс проектирования и строительства моста, ошибка может привести к катастрофе. Но допускать такие виды взлома, которые приводят к появлению новых, неожиданных способов использования интернета, имеет смысл.

Хакинг – естественная часть человеческого бытия. Он повсеместен и, как мы увидим, является важным фактором эволюционного процесса – непрерывного, бесконечного и способного создавать формы, как выразился Дарвин, «самые прекрасные и изумительные». Ну или же самые нелепые и ужасные.

Часть II
Основные виды хакинга и защита от него

6
Хакинг банкоматов

Для начала рассмотрим различные виды взломов систем, ограничения которых наиболее очевидны. Это создаст хорошую основу для понимания хакинга систем более сложных: политических, социальных, экономических и когнитивных.

Что такое банкомат? Это компьютер с наличными деньгами внутри. Он подключен к банковской сети через интернет (пару десятилетий назад это было обычное телефонное соединение и модем) и работает под управлением операционной системы Windows. Конечно же, его можно взломать.

В 2011 г. австралийский бармен по имени Дэн Сондерс выяснил, как снимать в банкоматах деньги, которых у тебя нет. Как-то поздно вечером, подойдя к банкомату, он неверно ввел сумму для перевода между своими счетами, случайно завысив ее. К удивлению Сондерса, перевод прошел, а банкомат выдал наличные, которых у него не было на счете, причем без регистрации операции системой. Это стало возможным из-за уязвимости в программном обеспечении банкомата, которое регистрировало переводы между счетами, в сочетании с другой уязвимостью – временной задержкой списаний и зачислений, произведенных посредством банкоматов в ночное время. Однако Сондерс ничего об этом не знал. Он обнаружил хак совершенно случайно и просто понял, что может воспроизвести результат.

В течение следующих пяти месяцев Сондерс снял в австралийских долларах сумму, эквивалентную $1,1 млн[28]. Его так и не смогли поймать. В какой-то момент он сам решил прекратить порочную практику: почувствовал себя виноватым, прошел курс терапии, а затем сделал публичное признание. За полгода банк так и не смог понять, где он теряет столько денег.

Давайте на секунду прервемся и поговорим о том, с какого рода деянием мы имеем дело. Кража денег из банка всегда незаконна. Но в этом случае взломана не банковская система, а система банкоматов и специальное программное обеспечение, написанное для них. Сондерс случайно наткнулся на способ использования этих систем, не предусмотренный их создателями. Иначе говоря, системы сами позволили нарушить заложенные в них правила. А это не что иное, как типичный хак.

Эволюция атак на банкоматы и принимаемых банками ответных мер наглядно иллюстрирует гонку вооружений между хакерами и различными институтами безопасности. Более того, здесь прослеживается несколько важных тем, к которым мы будем возвращаться на протяжении всей книги. Во-первых, системы – это не что-то изолированное: они состоят из более мелких подсистем и сами являются частью систем более крупных. Во-вторых, банкоматы – это не только программное обеспечение, но и «железо»: в процессе использования физического объекта под названием «банкомат» задействованы клиенты и удаленная банковская сеть. Хакеры могут атаковать любой из этих аспектов системы.

Конец ознакомительного фрагмента.

Комментарии

1.
Massimo Materni (1 May 2012), "Water never runs uphill / Session Americana," YouTube, https://www.youtube.com/watch?v=0Pe9XdFr_Eo.

2.
Это упражнение придумал не я. См.: Gregory Conti and James Caroland (Jul-Aug 2011), "Embracing the Kobayashi Maru: Why you should teach your students to cheat," IEEE Security & Privacy 9, https://www.computer.org/csdl/magazine/sp/2011/04/msp2011040048/13rRUwbs1Z3.

3.
См.: Justin Elliott, Patricia Callahan, and James Bandler (24 Jun 2021), "Lord of the Roths: How tech mogul Peter Thiel turned a retirement account for the middle class into a $5 billion tax-free piggy bank," ProPublica, https://www.propublica.org/article/lord-of-the-roths-how-tech-mogul-peter-thiel-turned-a-retirement-account-for-the-middle-class-into-a-5-billion-dollar-tax-free-piggy-bank.

4.
Если кто-нибудь в курсе, пожалуйста, напишите мне.

5.
См.: Finn Brunton has assembled a list of "significant meanings" of the term. Finn Brunton (2021), "Hacking," in Leah Lievrouw and Brian Loader, eds., Routledge Handbook of Digital Media and Communication, Routledge, pp. 75–86, http://finnb.net/writing/hacking.pdf.

6.
Недавно скончавшемуся хакеру Джуд Милхон (Святая Джуд) нравилось другое определение: «Взлом – это умный обход установленных ограничений, независимо от того, установлены они вашим правительством, вашей собственной личностью или законами физики». Jude Milhon (1996), Hackers Conference, Santa Rosa, CA.

7.
Bruce Schneier (2003), Beyond Fear: Thinking Sensibly About Security in an Uncertain World, Copernicus Books.

8.
Lauren M. Johnson (26 Sep 2019), "A drone was caught on camera delivering contraband to an Ohio prison yard," CNN, https://www.cnn.com/2019/09/26/us/contraband-delivered-by-drone-trnd/index.html.

9.
Selina Sykes (2 Nov 2015), "Drug dealer uses fishing rod to smuggle cocaine, alcohol and McDonald's into jail," Express, https://www.express.co.uk/news/uk/616494/Drug-dealer-used-fishing-rod-to-smuggle-cocaine-alcohol-and-McDonald-s-into-jail.

10.
Telegraph staff (3 Aug 2020), "Detained 'drug smuggler' cat escapes Sri Lanka prison," Telegraph, https://www.telegraph.co.uk/news/2020/08/03/detained-drug-smuggler-cat-escapes-sri-lanka-prison.

11.
Jay London (6 Apr 2015), "Happy 60th birthday to the word 'hack,'" Slice of MIT, https://alum.mit.edu/slice/happy-60th-birthday-word-hack. – Прим. ред.

12.
Dylan Matthews (29 Mar 2017), "The myth of the 70,000-page federal tax code," Vox, https://www.vox.com/policy-and-politics/2017/3/29/15109214/tax-code-page-count-complexity-simplification-reform-ways-means.

13.
Microsoft (12 Jan 2020), "Windows 10 lines of code," https://answers.microsoft.com/en-us/windows/forum/all/windows-10-lines-of-code/a8f77f5c-0661-4895-9c77-2efd42429409.

14.
Naomi Jagoda (14 Nov 2019), "Lawmakers under pressure to pass benefits fix for military families," The Hill, https://thehill.com/policy/national-security/470393-lawmakers-under-pressure-to-pass-benefits-fix-for-military-families.

15.
The New York Times (28 Apr 2012), "Double Irish with a Dutch Sandwich" (infographic), https://archive.nytimes.com/www.nytimes.com/interactive/2012/04/28/business/Double-Irish-With-A-Dutch-Sandwich.html.

16.
Niall McCarthy (23 Mar 2017), "Tax avoidance costs the U.S. nearly $200 billion every year" (infographic), Forbes, https://www.forbes.com/sites/niallmccarthy/2017/03/23/tax-avoidance-coststhe-u-s-nearly-200-billion-every-year-infographic.

17.
US Internal Revenue Services (27 Dec 2017), "IRS Advisory: Prepaid real property taxes may be deductible in 2017 if assessed and paid in 2017," https://www.irs.gov/newsroom/irs-advisory-prepaid-real-property-taxes-may-be-deductible-in-2017-if-assessed-and-paid-in-2017.

18.
Помню, как читал об одной налоговой лазейке, которая была показана потенциальным покупателям только после того, как они подписали соглашение о неразглашении, и даже тогда им не сообщили всех деталей. Хотелось бы ссылку на эту историю.

19.
Stephanie M. Reich, Rebecca W. Black, and Ksenia Korobkova (Oct 2016), "Connections and communities in virtual worlds designed for children," Journal of Community Psychology 42, no. 3, https://sites.uci.edu/disc/files/2016/10/Reich-Black-Korobkova-2014-JCOP-community-in-virtual-worlds.pdf.

20.
Steven Melendez (16 Jun 2018), "Manafort allegedly used 'foldering' to hide emails. Here's how it works," Fast Company, https://www.fastcompany.com/40586130/manafort-allegedly-used-foldering-to-hide-emails-heres-how-it-works.

21.
Cara Titilayo Harshman (22 Dec 2010), "Please don't flash me: Cell phones in Nigeria," North of Lagos, https://northoflagos.wordpress.com/2010/12/22/please-dont-flash-me-cell-phones-in-nigeria.

22.
Atul Bhattarai (5 April 2021), "Don't pick up! The rise and fall of a massive industry based on missed call," Rest of World, https://restofworld.org/2021/the-rise-and-fall-of-missed-calls-in-india.

23.
Tribune Web Desk (14 May 2020), "Students find 'creative' hacks to get out of their Zoom classes, video goes viral," Tribune of India, https://www.tribuneindia.com/news/lifestyle/students-find-creative-hacks-to-get-out-of-their-zoom-classes-video-goes-viral-84706.

24.
Anthony Cuthbertson (9 Mar 2020), "Coronavirus: Quarantined school children in China spam homework app with 1-star reviews to get it off app store," Independent, https://www.independent.co.uk/life-style/gadgets-and-tech/news/coronavirus-quarantine-children-china-homework-app-dingtalk-a9387741.html.

25.
Kimberly D. Krawiec and Scott Baker (2006), "Incomplete contracts in a complete contract world," Florida State University Law Review 33.

26.
Bruce Schneier (2012), Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons.

27.
Bruce Schneier (19 Nov 1999), "A plea for simplicity: You can't secure what you don't understand," Information Security, https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html.

28.
Jack Dutton (7 Apr 2020), "This Australian bartender found an ATM glitch and blew $1.6 million," Vice, https://www.vice.com/en_au/article/pa5kgg/this-australian-bartender-dan-saunders-found-an-atm-bank-glitch-hack-and-blew-16-million-dollars.