Содержание

Часть IV
ХАКИНГ ПРАВОВЫХ СИСТЕМ

Часть V
ХАКИНГ ПОЛИТИЧЕСКИХ СИСТЕМ

Часть VI
ХАКИНГ КОГНИТИВНЫХ СИСТЕМ

Часть VII
ХАКИНГ И СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

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*, 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

---

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

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 — непревзойденные 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*… 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

---

* 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.*

что они умны. Макгайвер* 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

---

* 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.*

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.

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* 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.

---

* MIT — Массачусетский технологический институт. — *Прим. ред.*

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.

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 подпи-

сал 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 облага-

емая 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»*, — скрупулезно исследуют каждую строку налогового кодекса в поисках

* «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.*

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 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*, 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

---

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

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. 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 рабо-

тают 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 влиятельные 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 поль-