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

Текст предоставлен правообладателем
«Взломать всё: Как сильные мира сего используют уязвимости систем в своих интересах»: Альпина Паблишер; Москва; 2023
ISBN 9785961489996

Аннотация

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.

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

---

[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.

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 [3], 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 [4].

---

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

[4] 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.

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[5], 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

[5] Если кто-нибудь в курсе, пожалуйста, напишите мне.

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[6], 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**[7] (*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.

---

[6] 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.

[7] 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.

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[8]… 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.[9] 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 [10] 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.

---

[8] 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* .

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

[10] 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 2019 г. кто-то использовал дрон[11], 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[12], чтобы перебросить контрабанду через стену тюрьмы, а также о коте[13], 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.

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[14] в 1955 г. в Клубе технического моделирования железных дорог MIT[15] 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.

---

11 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.

12 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.

13 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.

14 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.*

15 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[16] 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[17] 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

---

16 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.

17 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.

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[18] 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[19]. 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[20] в США почти на $200 млрд, разумеется, за счет остальных налогоплательщиков.

В налоговом мире баги и уязвимости называются лазейками, а их использование

---

18 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 .

19 *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.

20 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.

злоумышленниками – стратегией ухода от налогов. Тысячи профессионалов – налоговые юристы и бухгалтеры из числа тех, кого в мире компьютерной безопасности мы называем «черными шляпами»[21], – 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[22]. 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.

---

[21] «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*.

[22] 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.

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[23], 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. 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

---

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

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 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 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[24]. 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.

---

24 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.

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[25]. 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), а 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

---

[25] 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.

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* [26]. 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»[27]: 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[28], 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 [29] 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[30], надеясь, что таким образом оно

---

26 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.

27 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.

28 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.

29 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.

30 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-

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 [31]. 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[32] 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[33]. 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».

---

dingtalk-a9387741.html.

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

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

33 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.

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[34]. 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.

Первые взломы банкоматов были примитивными, больше похожими на обычный грабеж, чем на хакинг. Преступники заклеивали дверцы диспенсеров для выдачи купюр,

---

34 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.

а затем открывали их после того, как расстроенный клиент прекращал попытки изъять свои деньги и отлучался. Они делали так, чтобы карта застревала в картоприемнике, а затем вытаскивали ее и использовали. Они выкорчевывали банкоматы из стен и увозили, чтобы открыть в безопасном месте, – в точности как это показано в телесериале «Во все тяжкие». Службы безопасности реагировали. Из конструкции диспенсеров банкоматов убрали дверки, поэтому заклеивать стало нечего. Сами аппараты стали более надежно крепить к стене, а частота их пополнения наличными возросла, чтобы уменьшить потенциальный куш. (Самые сметливые злоумышленники стали грабить банкоматы вечером перед длинными праздниками, когда внутри было больше денег.) Современные банкоматы оснащены системами видеонаблюдения, но это не предотвращает подобных атак, разве что помогает впоследствии находить и арестовывать преступников.

Другой тип взлома использует авторитетное воздействие непосредственно на клиента. К примеру, преступник, одетый в костюм или униформу компании, прерывает транзакцию клиента со словами: «Извините, этот банкомат вышел из строя. Воспользуйтесь, пожалуйста, другим». Клиент послушно переходит к соседнему, а злоумышленник остается устанавливать табличку «Не работает». Когда клиент, сделав все необходимое, покидает зону банкоматов, преступник снимает деньги с его счета, завершая прерванную операцию в первом банкомате.

Такие и подобные им кражи привели к ряду изменений в конструкциях банкоматов[35]. Сначала было введено правило, согласно которому операция продолжается лишь до тех пор, пока карта находится в картоприемнике, чтобы никакие люди официального вида не могли закончить ее за клиента. В дальнейшем были внесены коррективы в работу расчетных банковских систем, которые сделали невозможным одновременное проведение нескольких транзакций по одному счету. Однако «авторитетные» взломы на этом не прекратились. Появились более грубые схемы, например такая, распространенная в Индонезии: подставной менеджер в присутствии клиента якобы звонил в офис банка и аннулировал его карту, после чего убеждал ее отдать.

Еще один тип взлома, *скимминг* , предполагает кражу информации с карты для создания и использования ее дубликата. С годами этот способ стал весьма популярным и изощренным. Каноническая версия скимминга заключается в размещении второго устройства для считывания магнитной полосы над слотом картоприемника таким образом, чтобы клиент невольно предоставлял свою карту шпионскому считывателю. Добавьте к этому скрытую камеру или датчик клавиатуры, и вот в вашем распоряжении имеется PIN-код. В одном из вариантов скимминга предполагается установка в общественном месте, например в торговом центре, отдельно стоящего «банкомата». Выглядит он совсем как настоящий, но все, что может, – это только считывать информацию с магнитного слоя карт, собирать PIN-коды и выводить сообщение «Банкомат не работает», чтобы отогнать оставшихся ни с чем клиентов.

Скимминг использует несколько уязвимостей. Во-первых, клиент не обладает достаточным опытом, чтобы заметить установленный скиммер или отличить поддельный банкомат от настоящего. Во-вторых, карта с магнитной полосой легко дублируется. И в-третьих, систему аутентификации, применяемую в банкоматах, – владение картой и знание PIN-кода, – сложно назвать надежной.

Следующий тип взлома банкоматов называется *джекпоттингом* [36] и направлен

---

35 Z. Sanusi, Mohd Nor Firdaus Rameli, and Yusarina Mat Isa (13 Apr 2015), «Fraud schemes in the banking institutions: Prevention measures to avoid severe financial loss,» *Procedia Economics and Finance* , https://www.semanticscholar.org/paper/Fraud-Schemes-in-the-Banking-Institutions%3A-Measures-Sanusi-Rameli/681c06a647cfef1e90e52ccbf829438016966c44.

36 Joseph Cox (14 Oct 2019), «Malware that spits cash out of ATMs has spread across the world,» *Vice* Motherboard, https://www.vice.com/en_us/article/7x5ddg/malware-that-spits-cash-out-of-atms-has-spread-across-the-world.

исключительно на программное обеспечение. Его задача – заставить банкомат выплевывать купюры, словно игральный автомат жетоны. При этом не требуется красть ни карту, ни PIN-код. В 2016 г. подобный взлом был организован на Тайване, а затем волной прокатился по Азии, Европе и Центральной Америке, что привело к убыткам в десятки миллионов долларов. Разработчиками были приняты меры, но в 2020 г. европейские хакеры нашли[37] новую уязвимость в программном обеспечении, благодаря чему атаки такого типа продолжаются по всему миру до сих пор.

Джекпоттинг состоит из нескольких этапов. Первый этап – исследование технической стороны вопроса, что предполагает разборку и изучение подержанного банкомата. Сегодня достать такой банкомат не проблема, даже на eBay их продается великое множество. Разобравшись в деталях, хакеры приступают к работе с действующими банкоматами: открывают панель управления, подключаются к USB-порту, загружают вредоносное ПО на компьютер и устанавливают удаленный доступ к банкомату. Провернуть все это помогает переодевание: преступник в форме техника может сделать это, не вызывая подозрений. Затем, подготовив аппарат, преступник уступает место своему сообщнику с большой сумкой, в которую после получения удаленной команды банкомат выплевывает всю наличность.

Нет точных данных о том, сколько денег похищается таким образом, ведь банки не любят предавать огласке подробности такого рода. Но нам известно, что Секретная служба США начала предупреждать[38] финансовые учреждения об угрозе джекпоттинга в 2018 г. То есть спустя восемь лет после того, как в 2010 г. исследователь в области безопасности Барнаби Джек продемонстрировал джекпоттинг[39] на хакерской конференции DEF CON. Его атаки не требовали физического вмешательства в работу банкомата, а базировались на уязвимостях программного обеспечения, которые он мог использовать удаленно.

7
Хакинг казино

Ричард Харрис работал в Комиссии по надзору за игорным бизнесом штата Невада, где он проверял новые игральные автоматы перед тем, как их разместят в залах казино. Имея доступ к начинке автоматов, он заменял установленные производителем чипы на свои собственные. Они были запрограммированы таким образом, что определенная последовательность монет, которые игрок опускал в автомат, инициировала выплату джекпота. В период с 1993 по 1995 г. Харрис модифицировал более 30 автоматов[40] и «выиграл» сотни тысяч долларов при помощи группы сообщников, которые просто совершали необходимые действия на указанных им игральных автоматах. Но в какой-то момент один из сообщников потерял осмотрительность, и Харрис был пойман.

Точно так же, как и банкомат, современный игральный автомат – это обычный компьютер, напичканный деньгами. Конечно, когда его изобрели в 1895 г., это было

---

37 Dan Goodin (22 Jul 2020), «Thieves are emptying ATMs using a new form of jackpotting,» Wired, https://www.wired.com/story/thieves-are-emptying-atms-using-a-new-form-of-jackpotting.

38 Brian Krebs (27 Jan 2018), «First 'jackpotting' attacks hit U.S. ATMs,» *Krebs on Security* , https://krebsonsecurity.com/2018/01/first-jackpotting-attacks-hit-u-s-atms.

39 Kim Zetter (28 Jul 2010), «Researcher demonstrates ATM 'jackpotting' at Black Hat conference,» *Wired* , https://www.wired.com/2010/07/atms-jackpotted.

40 Las Vegas Sun (21 Feb 1997), «Slot cheat, former casino regulator, reputed mob figure added to Black Book,» https://lasvegassun.com/news/1997/feb/21/slot-cheat-former-casino-regulator-reputed-mob-fig.

механическое устройство, но с 1980-х гг. весь процесс контролирует компьютер, а вращающиеся барабаны с картинками несут исключительно психологическую нагрузку. Во многих аппаратах даже нет настоящих барабанов – они имитируются на дисплее компьютера.

Игральные автоматы хакали с самого их появления. Некоторые из машин старого образца можно было просто толкнуть, чтобы изменить результат вращения барабанов. Другие было легко обмануть монетой на ниточке. Многие автоматы считают монеты, которые выдают, с помощью оптического датчика; заслоняя этот датчик монетой на ниточке, вставленной в монетоприемник, можно было добиться больших выплат.

Все без исключения игры, которые предлагают казино, были когда-то хакнуты. Некоторые из этих хаков стали нормой. Я не имею в виду, что теперь эти хаки разрешены, но они давно на слуху и перестали быть чем-то инновационным или даже попросту интересным. Подсчет карт в блек-джеке когда-то был хаком; сегодня публикуются книги о том, как это делать, и правила для того, чтобы помешать успешному подсчету.

Идея прогнозирования исхода игры в рулетку возникла в 1950-х гг. Колесо вращается с постоянной скоростью, крупье имеет привычку закручивать шарик на один и тот же манер, так почему же, проведя определенные вычисления, не выяснить, к каким числам шарик будет более благосклонным?

В 1960-х гг. для этой цели был создан переносной компьютер, который крепился на теле, управлялся ножными переключателями[41] и выводил результаты подсчетов в виде звуковых сигналов через наушник. Пользователь буквально вводил данные пальцами ног. Эта информация позволяла компьютеру рассчитать скорость вращения колеса, скорость, с которой крупье обычно подбрасывал шарик, и т. д. Через наушник оператор компьютера узнавал, какие числа выпадут с большей вероятностью. В более поздних моделях были улучшены ввод данных и скорость вычислений, но только в 1970-х гг. группе аспирантов Калифорнийского университета в Санта-Крузе наконец удалось получить стабильную прибыль от своего ножного компьютера.

Этот хак не был чем-то незаконным: лишь в 1985 г. штат Невада запретил использование устройств[42] для предсказания исхода игр в казино. Но настоящей защитой стали изменения в правилах игры, благодаря которым крупье прекращали принимать ставки до того, как колесо рулетки приходило в движение.

В блек-джеке хакеры пошли путем подсчета карт. Надо сказать, что это весьма непростая задача, тем более для того, кто не обладает необходимыми навыками. Метод базируется на том факте, что игроки имеют преимущество перед казино, когда в колоде остается больше десяток. Поэтому игрок внимательно следит за картами и увеличивает ставки, когда у него появляется преимущество. Да, это преимущество незначительное – всего около 1 % по сравнению с шансами казино, – но вполне реальное. Однако, чтобы постоянно вести такой учет карт, от игрока требуется недюжинная концентрация.

Казино реагировали на это по-разному[43]. Первый тип реакции заключался в усложнении процесса подсчета карт. В одних казино стали тасовать вместе сразу шесть колод (это делают автоматические тасовщики) и сдавать только две трети колоды, чтобы уменьшить вероятность преимущества игрока. В других карты стали тасовать после каждой

---

41 Paul Halpern (23 May 2017), «Isaac Newton vs. Las Vegas: How physicists used science to beat the odds at roulette,» *Forbes*, https://www.forbes.com/sites/startswithabang/2017/05/23/how-physicists-used-science-to-beat-the-odds-at-roulette.

42 Don Melanson (18 Sep 2013), «Gaming the system: Edward Thorp and the wearable computer that beat Vegas,» *Engadget*, https://www.engadget.com/2013-09-18-edward-thorp-father-of-wearable-computing.html.

43 Grant Uline (1 Oct 2016), «Card counting and the casino's reaction,» *Gaming Law Review and Economics*, https://www.liebertpub.com/doi/10.1089/glre.2016.2088.

раздачи. Известно, что в Лас-Вегасе и Атлантик-Сити пит-боссы подходят к предполагаемым счетчикам карт и вступают с ними в разговор, чтобы отвлечь и даже слегка напугать.

Казино пытались вывести подсчет карт в разряд преступных деяний, но так и не смогли убедить регуляторов, что эта стратегия равносильна жульничеству. Государственные органы ограничились принятием законов, запрещающих использование устройств для подсчета карт[44]. Все, что могут сделать казино сегодня, поймав счетчика карт, – запретить ему появляться в заведении. Раньше таких клиентов вычислял персонал казино, проинструктированный о типичном поведении счетчиков карт. Появившиеся в последнее время камеры, которые отслеживают движение каждой карты, делают это автоматически. Поскольку казино являются частным бизнесом[45], они, как правило (это зависит от штата), могут отказать в обслуживании кому угодно, если при этом не наблюдается признаков дискриминации.

Другой тип реакции казино на счетчиков карт состоял в том, чтобы принять их как издержки бизнеса. Людей, полагающих, что они умеют считать карты, куда больше, чем тех, кто способен на это в действительности. На самом деле казино только выигрывают от распространенного мнения, что блек-джек – это единственная игра, в которой можно преуспеть, ведь в результате они зарабатывают больше денег на желающих считать карты, чем проигрывают настоящим профессионалам-счетчикам. Завлекая игроков, некоторые казино даже упоминают в рекламе, что используют при игре в блек-джек только одну колоду.

Впрочем, бывают и исключения. В 1980-х гг. группа ученых из MIT и Гарвардского университета[46] изобрела инновационный способ подсчета карт. Охотясь за счетчиками карт, казино ищут людей, которые: а) постоянно выигрывают и б) меняют размер своих ставок таким образом, что становится очевидным наличие у них стратегической информации. Чтобы избежать обнаружения, группа ученых разделила задачи по подсчету карт между разными игроками. Счетчики сидели за столами и никогда не меняли суммы своих ставок. Крупные игроки-бетторы тоже не меняли размера ставок – они просто переходили от одного стола к другому, направляемые сообщниками, которые получали сигналы от счетчиков. В общей сложности группа заработала примерно $10 млн[47], прежде чем оставить этот бизнес. Воистину крутой хак.

8
Хакинг программ лояльности авиакомпаний

В 1999 г. парень по имени Дэвид Филлипс купил 12 150 стаканчиков с пудингом Healthy Choice. Зачем? Чтобы хакнуть программу для часто летающих пассажиров.

Предложения для часто летающих пассажиров стали популярны в 1981 г., когда компании American, United и Delta впервые представили свои программы. Теперь они есть

---

44 David W. Schnell-Davis (Fall 2012), «High-tech casino advantage play: Legislative approaches to the threat of predictive devices,» *UNLV Gaming Law Journal* 3, https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1045&context=glj.

45 New Jersey is an exception to this. Atlantic City casinos cannot ban card counters. Donald Janson (6 May 1982), «Court rules casinos cannot bar card counters,» *The New York Times* , https://www.nytimes.com/1982/05/06/nyregion/court-rules-casinos-may-not-bar-card-counters.html.

46 Ben Mezrich (Dec 2002), Bringing Down the House: The Inside Story of Six MIT Students Who Took Vegas for Millions, Atria Books.

47 Janet Ball (26 May 2014), «How a team of students beat the casinos,» *BBC World Service* , https://www.bbc.com/news/magazine-27519748.

у каждого авиаперевозчика. Это программы лояльности, поощряющие клиентов летать самолетами одной авиакомпании и снижающие вероятность их перехода в другую. До COVID-19 я регулярно летал. Мне известны все тонкости и нюансы этих программ, и я утверждаю со знанием дела: все они были взломаны с самого начала.

Один из первых хаков назывался «мили за пробег». Мили, начисляемые пассажирам в зависимости от расстояния их рейсов, по сути являются частной валютой, которую можно обменять на билеты. Умный хакер будет искать способы арбитража двух валют, то есть такие ситуации, когда за небольшие деньги можно получить много миль. Так, например, за беспосадочный перелет из Нью-Йорка в Амстердам начисляется 3630 миль, а за перелет с пересадкой в Стамбуле – 6370 миль. При условии, что тот и другой билеты стоят одинаково, а вам больше нечем заняться, это отличная сделка.

Мили за пробег определенно нарушали цели, ради которых авиакомпании запускали программы лояльности. Дальнейшие хаки стали еще более странными. Программы, как правило, включают в себя несколько уровней вознаграждения: к примеру, налет за год 50 000 миль резко повышает ценность программы для пассажира. Поэтому последние порой занимались тем, что покупали билеты на долгие и сложные, но дешевые рейсы туда и обратно, с шестью и более пересадками, только для того, чтобы накопить мили. Некоторые даже не удосуживались покидать аэропорты, в которых оказывались.

Авиакомпании годами игнорировали подобные хаки, но в 2015 г. они начали вносить изменения в свои программы поощрения часто летающих пассажиров[48], чтобы налет сам по себе не был способом заработать мили. Многие компании ввели минимальный порог расходов для получения элитного статуса и в конечном счете изменили само понятие «миля» в рамках программ, чтобы оно зависело от потраченных долларов, а не от расстояния, которое пролетел пассажир.

Существуют хаки, использующие другие способы накопления миль[49], помимо самих полетов. Авиакомпании уже давно сотрудничают с банками, выпуская совместные кредитные карты. За каждую оплату такой картой начисляются мили, но помимо этого они часто начисляются уже при заказе карты. Хак очевиден: оформите много кредитных карт и закройте их до того, как начнутся комиссионные сборы. Один человек открыл такую кредитную карту и сразу купил на $3000 подарочные сертификаты Amazon, чтобы получить свой бонус за регистрацию. Другой заполнил гараж блендерами в рамках акции, предлагающей дополнительные мили за покупку бытовой техники. Некая дама хвасталась, что за пять лет она «оформила более 46 кредитных карт и заработала 2,6 млн миль только в виде бонусов за регистрацию».

Конечно, такой хакинг программ лояльности наносит немалый вред: банки в итоге тратят миллиарды долларов на перелеты клиентов, которые не платят ни комиссию, ни проценты по своим картам. В результате эти расходы перекладываются на потребителей в виде более высоких цен на билеты. Некоторые эмитенты кредитных карт пытаются пресекать подобные взломы. В 2016 г. банк Chase ввел правило[50], согласно которому клиенту не будет одобрено большинство из кредитных карт, если он уже заказал пять и более кредитных карт в разных банках за последние 24 месяца. American Express теперь

---

48 Josh Barro (12 Sep 2014), «The fadeout of the mileage run,» *The New York Times*, https://www.nytimes.com/2014/09/14/upshot/the-fadeout-of-the-mileag-run.html.

49 Darius Rafieyan (23 Sep 2019), «How one man used miles to fulfil his dream to visit every country before turning 40,» *NPR*, https://www.npr.org/2019/09/23/762259297/meet-the-credit-card-obsessives-who-travel-the-world-on-points.

50 Gina Zakaria (25 Feb 2020), «If you're interested in a Chase card like the Sapphire Preferred you need to know about the 5/24 rule that affects whether you'll be approved,» *Business Insider*, https://www.businessinsider.com/personal-finance/what-is-chase-524-rule.

аннулирует мили [51] у тех, кто «участвовал в злоупотреблениях, неправомерном использовании или играх, связанных с получением или использованием баллов», что дает компании широкие возможности наказывать клиентов, которые, по ее мнению, злоупотребляют системой.

И тут мы возвращаемся к «парню с пудингом»[52]. Известный среди хакеров программ лояльности, Филлипс обнаружил уязвимость не в плане какой-то конкретной авиакомпании, а в программе Healthy Choice 1999 г. К тому времени большинство авиакомпаний уже предлагали партнерские программы, дающие различным фирмам возможность оптом покупать мили для часто летающих пассажиров и предлагать их своим клиентам в качестве вознаграждения. Конкретно в этой злополучной программе клиенты могли зарабатывать мили на рейсы выбранной ими авиакомпании, покупая продукты Healthy Choice. Филлипс занялся поиском самого дешевого продукта, соответствующего требованиям программы, и в итоге купил 12 150 стаканчиков с пудингом по 25 центов за штуку, получив таким образом 1,2 млн миль за $3150 и пожизненный статус Gold на рейсах American Airlines. (Затем он пожертвовал весь купленный пудинг на благотворительность, дополнительно получив возможность списать $815 при уплате налогов.) Определенно, это не тот результат, на который рассчитывала Healthy Choice, запуская программу, но, поскольку Филлипс не нарушил никаких правил, компания заплатила.

9
Хакинг в спорте

Спорт хакают постоянно. Очевидно, это результат конкурентного давления (а в профессиональном спорте еще и денег) и неизбежно «дырявых» правил.

Несколько историй для примера.

Американский бейсбол, 1951 г. Команда «Сент-Луис Браунс»[53] протащила в состав игрока по имени Эд Гейдел, чуть больше метра ростом. Он сделал всего один выход на поле, который, само собой, закончился «прогулкой»[54]: его страйк-зона была настолько мала, что попасть в нее было почти невозможно. В лиге не существовало официального требования к росту игрока, поэтому технически это был легальный хак. Однако на следующий день президент лиги все равно аннулировал контракт игрока.

Баскетбол, 1976 г. Финал NBA, второй овертайм. До конца остается меньше секунды, «Финикс Санс» отстают всего на одно очко от «Бостон Селтикс». Мяч у «Санс» на дальнем конце площадки, и у них просто нет времени, чтобы доставить его к корзине и бросить. Именно в этот момент игрок «Санс» Пол Уэстфал хакнул правила. Он взял тайм-аут, хотя у его команды этого права уже не осталось. Судьи засчитали фол, а «Бостон Селтикс» получили право на штрафной бросок. Но в данном случае заработанное противником дополнительное очко не имело значения. Важным было другое: после штрафного броска

---

[51] Nicole Dieker (2 Aug 2019), «How to make sure you don't lose your credit card rewards when you close the card,» *Life Hacker* , https://twocents.lifehacker.com/how-to-make-sure-you-dont-lose-your-credit-card-rewards-1836913367.

[52] Carla Herreria Russo (3 Oct 2016), «Meet David Phillips, the guy who earned 1.2 million airline miles with chocolate pudding,» *Huffington Post* , https://www.huffpost.com/entry/david-philipps-pudding-guy-travel-deals_n_577c9397e4b0a629c1ab35a7.

[53] Associated Press (20 Aug 1951), «Brownies hit all-time low; Use 3-foot 7-inch player,» *Spokesman-Review* , https://news.google.com/newspapers?id=rS5WAAAAIBAJ&sjid=3uUDAAAAIBAJ&pg=4920%2C3803143.

[54] «Прогулкой» в бейсболе называется ситуация, когда после четырех ошибок питчера бэттер автоматически получает право занять первую базу. – *Прим. пер* .

«Санс» получили мяч в центре площадки[55], что дало им шанс забить двухочковый и выйти в третий овертайм. Что они и сделали. На следующий год NBA изменила правила, запретив командам продвигать мяч на середину площадки с помощью технического фола.

Плавание, 1988 г. Американец Дэвид Беркофф и японец Даичи Судзуки отличились в заплывах на спине[56], проходя большую часть бассейна под водой и показав поразительный результат. Эту технику вскоре переняли и другие первоклассные пловцы, пока не вмешалась Международная федерация плавания и не ограничила дистанцию, на которой пловец на спине может оставаться под водой.

Американский футбол, 2015 г. «Нью Ингленд Пэтриотс» использовали новый хак[57] против «Балтимор Рэйвенс», перемещая игроков на линии розыгрыша, чтобы манипулировать сложными правилами, определяющими, какие игроки имеют право принимать мяч. Два месяца спустя лига внесла поправки в правила[58], чтобы сделать этот хак незаконным.

Впрочем, так происходит далеко не всегда. Часто вместо того, чтобы объявлять хаки незаконными, их включают в игру, потому что они действительно ее улучшают. Многие аспекты спорта, которые сегодня являются нормой, когда-то были хаками. В американском футболе пас вперед был когда-то хаком, точно так же, как и приемы нападения «беги и стреляй» (run-and-shoot) и «быстрый рывок» (fast snap), вынуждающий другую команду менять игроков. В бейсболе хаками были приемы «жертвенная муха» (sacrifice fly) и «преднамеренная прогулка» (intentional walk). Ни один из этих приемов не противоречил правилам, просто до определенного момента никому и в голову не приходило, что можно действовать подобным образом. Как только приемы были опробованы, они стали частью игры.

Однако этот процесс не всегда проходит гладко. В баскетболе бросок под названием «верняк» (слэм-данк) когда-то был хаком[59]. Никто и представить себе не мог, что игрок способен прыгнуть настолько высоко, чтобы положить мяч в корзину сверху. В первые десятилетия развития баскетбола прием вызывал горячие споры. Разные лиги пытались запретить данкинг, но с середины 1970-х гг. он стал неотъемлемой частью этого вида спорта, поскольку зрелищные броски неизменно приводили в восторг болельщиков.

В крикете, в отличие от бейсбола, отбивающий игрок может заработать очки, отбив мяч не только в сектор, расположенный перед ним, а в любую сторону, поскольку его позиция находится в центре поля. Больше века традиционным способом отбивания мяча считалось

---

55 Presh Talwalkar (6 Jun 2017), «Genius strategic thinking in the 1976 NBA Finals,» Mind Your Decisions, https://mindyourdecisions.com/blog/2017/06/06/genius-strategic-thinking-in-the-1976-nba-finals-game-theory-tuesdays . *Secret Base* (5 Feb 2019), «The infinite timeout loophole that almost broke the 1976 NBA Finals,» YouTube, https://www.youtube.com/watch?v=Od2wgHLq69U.

56 John Lohn (24 Sep 2021), «Seoul Anniversary: When the backstroke went rogue: How David Berkoff and underwater power changed the event,» *Swimming World* , https://www.swimmingworldmagazine.com/news/seoul-anniversary-when-the-backstroke-went-rogue-how-david-berkoff-and-underwater-power-changed-the-event.

57 Rodger Sherman (10 Jan 2015), «The Patriots' trick play that got John Harbaugh mad,» *SB Nation* , https://www.sbnation.com/nfl/2015/1/10/7526841/the-patriots-trick-play-that-got-john-harbaugh-mad-ravens.

58 Ben Volin (26 Mar 2015), «NFL passes rule aimed at Patriots' ineligible receiver tactic,» *Boston Globe* , https://www.bostonglobe.com/sports/2015/03/25/nfl-passes-rule-change-aimed-patriots-ineligible-receiver-tactic/uBqPWS5dKYdMYMcIiJ3sKO/story.html.

59 Сюжет детского фильма 1997 г. «Король воздуха» (Air Bud) основан на хаке правил профессионального баскетбола, которые не запрещают собаке выступать за команду. (Фильм просто жесть.)

таковое в сторону подающего боулера, как в бейсболе, или же краем биты в направление позади отбивающего. В начале 2000-х гг. некоторые игроки в крикет догадались[60], что могут опасно «зачерпнуть» или «накатить» мяч над собственной головой. Этот удар полностью соответствовал правилам, но требовал особой смелости и хакерского мышления (один из игроков утверждал, что придумал его, играя на узких улочках Шри-Ланки). Немало знаменитых побед было одержано с помощью этой техники, и теперь это стандартный прием в игре.

Кража знаков в бейсболе допускается, но с многочисленными ограничениями и оговорками в ответ на продолжающийся хакинг этой системы. Игроку второй базы и тренеру третьей разрешено пытаться читать знаки кетчера, а вот бэттеру – нет. Камеры, установленные с этой целью вне поля, запрещены. Когда «Хьюстон Астрос» в 2017–2018 гг. читали знаки при помощи камеры, они скорее мошенничали, чем хакали систему, поскольку это правило уже действовало.

Большинство спортивных хаков становятся очевидными после применения. Невозможно скрыть тот факт, что ты плыл под водой или отбил мяч для крикета ударом над головой. Как только первый игрок или команда применяет хак, об этом узнают все. Исключение составляют виды спорта, где чисто технически можно что-то спрятать. К ним относятся все разновидности гонок на механических транспортных средствах (автомобилях, яхтах и т. д.). Кроме того, отдельной областью является допинг, стимулирующий людей и животных.

Гонки «Формула-1» постоянно изобилуют хаками. Сначала члены одной команды находят лазейку в существующих правилах, чтобы повысить эффективность своих болидов. Затем об этом узнают другие команды и либо копируют идею, либо протестуют против нововведения. Наконец, Международная автомобильная федерация (FIA) вмешивается и делает одно из двух: запрещает хак или же включает его в технические спецификации следующего сезона.

Так, например, в 1975 г. команда Tyrell построила шестиколесный автомобиль[61]: два колеса сзади и четыре спереди. Этот хак увеличил производительность, но снизил надежность. В ответ другие команды построили аналогичные прототипы, но в 1983 г. FIA постановила, что все автомобили могут иметь не более, но и не менее (это уже на всякий случай) четырех колес. В 1978 г. команда Brabham обошла правило[62] о том, что ни один автомобиль не может иметь подвижные аэродинамические элементы, такие как пропеллеры, установив один из них рядом с радиатором и назвав его охлаждающим устройством. Эта машина была добровольно снята с соревнований, и в результате правила не пришлось изменять. В 1997 г. в конюшне McLaren разработали автомобиль с двумя педалями тормоза[63], вторая из которых управляла только задними колесами. Я недостаточно разбираюсь в автомобильных гонках, чтобы понять все детали, но это давало водителю преимущество. Сначала такая инновация была разрешена, но затем ее запретили после жалоб других команд.

В 2010 г. McLaren обошла запрет на подвижные аэродинамические элементы, проделав

---

60 Manish Verma (7 Jan 2016), "How Tillakaratne Dilshan invented the 'Dilscoop,' " *SportsKeeda* , https://www.sportskeeda.com/cricket/how-tillakaratne-dilshan-invented-dilscoop.

61 Jordan Golson (17 Dec 2014), «Well that didn't work: The crazy plan to bring 6-wheeled cars to F1,» *Wired* , https://www.wired.com/2014/12/well-didnt-work-crazy-plan-bring-6-wheeled-cars-f1.

62 Gordon Murray (23 Jul 2019), «Gordon Murray looks back at the notorious Brabham fan car,» *Motor Sport* , https://www.motorsportmagazine.com/articles/single-seaters/f1/gordon-murray-looks-back-notorious-brabham-fan-car.

63 McLaren (1 Nov 2017), «The search for the extra pedal,» https://www.mclaren.com/racing/inside-the-mtc/mclaren-extra-pedal-3153421.

в кокпите дыру[64], которую водитель мог закрывать и открывать ногой. В качестве аргумента приводился довод, что в отверстии нет движущихся частей, поэтому оно разрешено правилами. Однако водитель, двигая ногой, создавал тот же эффект, и хак быстро запретили. В 2014 г. Mercedes изменила конструкцию турбокомпрессора своего двигателя для «Формулы-1»[65], разделив турбину и компрессор и разместив их по разные стороны двигателя. Конструкция не была признана незаконной, и ее использование стало причиной того, что команда Mercedes доминировала в гонках в течение следующих шести лет. В 2020 г. Mercedes добавила на рулевое колесо новую функцию[66]: нажатие на рулевую колонку меняло угол схождения передних колес. Правила запрещают добавлять какие-либо функции на руль; законность этого хака зависит от точного определения системы рулевого управления, а также от того, рассматривается ли эта функция как вспомогательное средство именно этой системы или же как элемент устройства подвески. FIA прикрыла эту лазейку в 2021 г.

И, наконец, последний пример, к которому мы еще вернемся в этой книге. Раньше хоккейные клюшки были плоскими. Затем кто-то обнаружил, что изогнутой клюшкой игроки могут наносить броски с куда более высокой скоростью. Теперь изогнутые клюшки – это норма и существуют точные ограничения на кривизну клюшки. Во время игр NHL 1993 г. игрок «Лос-Анджелес Кингс» Марти Максорли был пойман с клюшкой, изогнутой не по правилам[67].

10
Хакеры паразитируют

Вирион SARS-CoV-2 в ширину около 80 нм. Он прикрепляется к белку под названием ACE2, который встречается на поверхности многих клеток нашего организма: в сердце, кишечнике, легких и носовых проходах. В нормальном состоянии ACE2 принимает участие в процессах регуляции артериального давления, снятия воспалений и заживления ран. Но у вируса есть особый наконечник, который может захватывать белок, сплавляя воедино мембраны клетки и вируса, что позволяет РНК вируса проникнуть в клетку. Затем вирус подрывает механизм производства белка в клетке-хозяине, перехватывая процесс, чтобы штамповать копии самого себя, которые затем заражают все новые и новые клетки. Другие части РНК вируса создают белки, остающиеся в клетке-хозяине. Один из них не позволяет клетке посылать сигналы иммунной системе о том, что она подверглась атаке. Другой побуждает клетку высвобождать новые вирионы. Третий помогает вирусу противостоять врожденному иммунитету клетки-хозяина. Все это привело к появлению болезни, которая с 2020 г. доминирует в нашей жизни: COVID-19.

COVID-19 – это хакер. Как и все вирусы, SARS-CoV-2 ловко использует иммунную систему нашего организма, нарушая ее работу ценой здоровья и жизни более 6 млн человек во всем мире. ВИЧ – еще один хакер. Он заражает Т-хелперные клетки в нашей крови,

---

64 Matt Somerfield (20 Apr 2020), «Banned: The 2010 Formula 1 season's F-duct,» *AutoSport* , https://www.autosport.com/f1/news/149090/banned-the-f1-2010-season-fduct.

65 Laurence Edmondson (6 Feb 2016), «Mercedes F1 engine producing over 900bhp with more to come in 2016,» *ESPN* , https://www.espn.com/f1/story/_/id/14724923/mercedes-f1-engine-producing-900bhp-more-come-2016.

66 Laurence Edmondson (21 Feb 2020), «Mercedes' DAS system: What is it? And is it a 2020 game-changer?» *ESPN* , https://www.espn.com/f1/story/_/id/28749957/mercedes-das-device-and-2020-game-changer.

67 Dave Stubbs (2 Jun 2017), «Marty McSorley's illegal stick still part of Stanley Cup Final lore,» National Hockey League, https://www.nhl.com/news/marty-mcsorleys-illegal-stick-still-part-of-stanley-cup-final-lore/c-289749406.

внедряя свою ДНК в ДНК клетки, а затем реплицируясь внутри нее. В конце концов инфицированная клетка высвобождает новые вирионы ВИЧ в кровоток, продолжая процесс своего размножения.

В целом хакинг как явление носит паразитический характер. И ВИЧ, и SARS-CoV-2 являются паразитами: они живут в организме другого вида, извлекая из этого выгоду, как правило, за счет хозяина. Система существует для достижения определенных целей, поставленных обычно ее разработчиками. Хакер взламывает эту систему для достижения иных целей, которые могут противоречить первоначальным.

Это очевидно при хакинге банкоматов, азартных игр, программ лояльности и планов междугородних звонков. Целью того, кто управляет банкоматом, является выдача наличных клиентам банка и списание соответствующих сумм с их счетов. Цель хакера – получить наличные, не списывая деньги со своего счета (или вообще не имея такового). Точно так же цель казино – обеспечивать честную игру (что, впрочем, означает равенство шансов между игроками, а вовсе не между игроками и казино). Цель хакера, напротив, состоит в том, чтобы получить преимущество.

В спорте и онлайн-играх это менее очевидно. Цели спортивной лиги могут состоять в том, чтобы получать прибыль, развлекать болельщиков, продвигать соревновательность как социальное качество, в некотором смысле быть оплотом справедливости и обеспечивать «хорошую игру», что бы это ни значило. Цель спортсмена – выигрывать любой ценой, индивидуально или в команде, и, возможно, зарабатывать деньги.

Цели онлайн-игры Club Penguin заключались в том, чтобы обеспечить пользователям безопасный и интересный опыт и законным путем повысить прибыль корпорации Disney. Целью хакеров Club Penguin было более свободное общение с другими игроками, независимо от того, был ли хакер шестилетним ребенком, ищущим, с кем поболтать, или же троллем в поисках жертв. С точки зрения системы и тот и другой были паразитами, хотя и совершенно разных видов.

Спам – это хак электронной почты. Когда создавались интернет-протоколы и закладывалась система электронной почты, никто о нем не думал в принципе, не говоря уже о намеренном пресечении таких попыток, хотя сами по себе нежелательные почтовые рассылки – давняя американская традиция. Рассылка подобных электронных писем, в том числе преследующих коммерческие цели, на раннем этапе существования электронной почты никем не осуществлялась. Идея спама возникла в 1990-х гг., причем одновременно и в системе электронной почты, и в популярном тогда сервисе обмена сообщениями Usenet, а серьезной проблемой стала уже в начале 2000-х гг. В те годы около 90 % всей электронной почты было спамом. Это не что иное, как паразитический взлом коммуникационной системы.

Не все паразитические отношения происходят за счет хозяина, и не все хакеры – злодеи. Обычно они ведут себя рационально, преследуя финансовые интересы, как в большинстве приведенных в этой книге примеров. Но они также могут действовать исходя из других интересов: моральных, этических или политических. Иногда хакеры с помощью взлома пытаются улучшить мир. Иногда они просто ищут возможности. Иногда, если система настроена против них, они действуют по необходимости – просто для того, чтобы выжить. Подумайте о людях, которые пытаются получить медицинскую помощь или прокормить себя и свою семью.

Как и любой паразит, подрывая систему хозяина, хак не должен быть чересчур эффективным – ему нужно, чтобы система продолжала существовать. Успешный хакинг банкоматов, хотя и приносит прибыль, полностью зависит от наличия таких банкоматов, которые можно взломать. Если бы какой-то конкретный хак стал слишком успешным, банки просто перестали бы устанавливать подходящие банкоматы. Если бы слишком много людей взломали Club Penguin, чтобы вести беседы, противоречащие концепции безопасности детей, Disney свернула бы эту систему прежде, чем столкнуться с последствиями. Спам уничтожил бы электронную почту, если бы не антиспамовые программы. Слишком

эффективный хак может в итоге себя обессмыслить, разрушив базовую систему, от которой зависит.

11
Защита от хаков

Spectre и Meltdown – две аппаратные уязвимости в микропроцессорах Intel и ряда других производителей. Они были обнаружены в 2017 г., а в 2018 г. компании опубликовали эту информацию. По сути, уязвимыми с точки зрения безопасности оказались некоторые оптимизации производительности, принятые на протяжении нескольких лет. Защита осложнялась тем, что уязвимости были аппаратными, а не программными. Для устранения некоторых из них были разработаны программные «заплаты» – патчи (часто со значительными потерями производительности), но далеко не для всех. Заменить уязвимые системы было просто нереально, поскольку чипы, о которых идет речь, установлены примерно в 100 млн компьютеров. И хотя будущие микропроцессоры могут быть спроектированы без уязвимостей, нельзя исправить их на уже установленных задним числом. Возможно, лучшей защитой в данном случае стала сложность использования этих уязвимостей: многие компьютеры были уязвимы, но хакеры не могли этим воспользоваться.

Защититься от взлома бывает непросто. Контрмеры варьируются от внесения исправлений до проектирования новых, безопасных систем. Дальше мы поговорим о каждой из них по очереди.

Я первым признаю, что моя таксономия небрежна. Введение правила, которое лишает законности подсчет карт в блек-джеке, делает эту тактику неэффективной, но только в том случае, если вас поймают. Устраняет ли это уязвимость или просто снижает эффективность хака? Аналогичным образом противоугонная бирка, снабженная капсулой с красителем, портит украденную вещь, снижая эффективность кражи, и одновременно делает эту кражу менее вероятной, лишая вора стимула. Подобные двусмысленности ничуть меня не напрягают. Точность категорий защитных средств волнует меня куда меньше, чем практическое знание о различных средствах защиты от хакеров и хаков.

Первая и наиболее очевидная защита – это устранение уязвимости.

В компьютерном мире основным средством защиты от хаков являются исправления. Технически это несложно – нужно просто обновить компьютерный код, чтобы устранить уязвимость. Нет уязвимости – нет эксплойта; нет эксплойта – нет взлома.

То, насколько хорошо работает исправление, во многом зависит от типа системы. Системы, которые находятся в собственности или контролируются одним субъектом, могут, если захотят (то есть если это имеет для них экономический смысл), быстро устранять обнаруженные уязвимости путем исправления.

Выпуск патча – это только первый этап процесса; далее он должен быть установлен на уязвимые системы. Исторически сложилось так, что между компаниями, выпускающими исправления, и пользователями, устанавливающими их, существует несогласованность. Поставщики программного обеспечения выпускают исправления, а пользователи устанавливают их на свое усмотрение, и часто на это уходят недели или даже месяцы, в течение которых непропатченные системы, конечно же, остаются уязвимыми.

Этот сценарий предполагает, что владелец системы должен иметь возможность не только писать исправления, но и заботиться о том, что система будет быстро исправлена. Если в штате компании достаточно инженеров для написания патчей и при этом существует система обновления, позволяющая оперативно доставлять новое программное обеспечение каждому пользователю, то исправления могут быть очень эффективным методом безопасности. Но это не так, если отсутствует хотя бы одно из двух условий… (Помните о множестве устройств IoT, код которых находится в прошивке и не может быть исправлен?) То, что на ваш компьютер и телефон постоянно приходят обновления, позволяет им оставаться в безопасности, несмотря на появление новых хаков. Однако, несмотря на свою

уязвимость, ваш домашний маршрутизатор редко подвергается исправлениям.

Многие громкие хаки стали возможны из-за непропатченных систем. Китай взломал сервер американского бюро кредитных историй Equifax в 2017 г. через уязвимость в программном обеспечении для создания веб-приложений Apache Struts. Apache исправила уязвимость в марте, но Equifax не смог своевременно обновить свое программное обеспечение и был успешно атакован в мае.

В том же 2017 г. червь WannaCry пробрался в более чем 200 000 компьютеров по всему миру и причинил ущерб на сумму около $4 млрд, причем это коснулось только тех сетей, которые не установили патч для Microsoft Windows.

Все это иллюстрирует главный недостаток патчей: они устанавливаются постфактум. Уязвимость уже существует в системе. Хакеры могут вовсю эксплуатировать ее к моменту установки патча. И даже если это не так, то сам факт исправления кода привлекает внимание к уязвимости и подвергает опасности все аналогичные системы, которые еще не были пропатчены.

Для большинства индивидуальных пользователей компьютеров и мобильных устройств обновления происходят автоматически. Если на вашем компьютере установлена операционная система Windows, то пакет обновлений приходит во второй вторник каждого месяца и может включать исправления более чем 100 уязвимостей. Ваш iPhone выдает все более грозные предупреждения, если вы игнорируете установку обновлений. (Если вы еще не сделали выводов, позвольте сказать прямо: включите функцию автоматического обновления на компьютере и телефоне. Ставьте патчи сразу, как только получите. Всегда.)

Крупные организационные сети вынуждены работать с исправлениями куда медленнее и осторожнее. Поскольку плохой патч может спровоцировать кучу проблем из-за того, как он взаимодействует с другим программным обеспечением, исправления обычно устанавливают обдуманно и методично. Часто это означает, что их устанавливают с опозданием или не устанавливают вовсе. Мы могли бы возложить вину за взлом базы данных на саму Equifax, поскольку она не установила патч для Apache Struts, но дело в том, что патчи этого разработчика славились своими ошибками, несовместимыми с другим программным обеспечением, взаимодействующим со Struts. Многие организации проявляют осторожность, применяя эти исправления.

В случае социальных систем патчи работают иначе. В системах технологических патч блокирует саму возможность взлома. Это, безусловно, относится к программному обеспечению, но касается и других технологических систем. Производитель банкоматов может установить патч на свои машины, и конкретная схема джекпоттинга перестанет работать. Казино при игре в блек-джек может раздавать с шести колод, постоянно тасуя карты. Финансовая биржа может ограничить торговлю десятисекундным интервалом, сделав такой хак, как высокочастотная торговля, нереалистичным. Все это можно сделать лишь потому, что возможности системы строго определены технологией.

С социальными, экономическими или политическими системами, которые не связаны напрямую с компьютерами, все далеко не так просто. Когда мы говорим об «исправлении» налогового кодекса или правил игры, мы имеем в виду изменение законов или правил системы таким образом, чтобы конкретная атака попала в разряд запрещенных. Компьютер по-прежнему можно будет использовать для предсказания вероятных исходов игры в рулетку, и клюшку можно будет изогнуть больше чем на три четверти дюйма (1,9 см), но пойманному нарушителю придется испытать на себе малоприятные последствия своего поступка. Единственное «обновление», которое нужно «установить» в этих случаях, – это обучить персонал и убедиться, что каждый пит-босс в казино и каждый хоккейный арбитр на льду знают новые правила и то, как выявлять мошенников, а пойманных с поличным наказать соответствующим образом. Аналогично, законная стратегия ухода от налогов становится незаконным уклонением от их уплаты и в случае обнаружения преследуется по закону (во всяком случае, так должно быть).

Это указывает на другую проблему: мошенников сложно обнаружить. Вспомните, что

рулетка оставалась уязвимой до тех пор, пока систему ставок не изменили таким образом, что хакинг просто перестал быть эффективным. Эта проблема характерна для систем, о которых мы будем говорить. Если вы обновите компьютерный код, взлом станет невозможным. Если вы обновите налоговый кодекс, хак все еще будет возможен, просто юридическая лазейка перестает быть таковой, а значит, и хак, по моему определению, перестает быть хаком. Это означает, что вам придется обновить и систему обнаружения, чтобы хакеры, ставшие теперь преступниками, были пойманы и привлечены к ответственности.

Эффективность патчей также снижается, когда управляющий орган функционирует медленно или когда внутри него нет единого мнения, нужен ли патч вообще. Иными словами, когда у системы нет четкой цели. Что, например, означает «исправить» налоговый кодекс? В большинстве случаев это означает принятие нового закона, который закрывает уязвимости действующего. Этот процесс может занимать годы, ведь налоговый кодекс создается в политической сфере – обители конкурирующих представлений о том, чего должна достичь государственная политика. Кроме того, те самые люди, которые используют уязвимости, как правило, стараются хакнуть и законодательные системы, чтобы поддерживать легальность своих действий. Представьте себе, если бы счетчики карт в блек-джеке отвечали за правила казино. Подсчет карт тогда преподносился бы как умный и честный способ победить в игре. Точно так же преподносится сейчас уклонение от уплаты налогов.

В отсутствие исправлений на уровне законодательства можно прибегнуть к весьма специфическому и быстрому патчу, который «ставится» через суд. В компьютерном мире у него есть аналог, известный как *хотфикс* (hotfix), – быстрое обновление программного обеспечения, предназначенное для устранения конкретной ошибки или уязвимости. Термин «хотфикс» (буквально «горячее исправление») происходит от того факта, что традиционно такие обновления применялись к уже запущенным рабочим системам. Этот метод был более рискованным, поскольку программное обеспечение могло дать сбой, способный повлечь непредсказуемые проблемы. Сегодня хотфикс – обычное явление: обновления для операционных систем, значительная часть которых функционирует в облаке, устанавливаются прямо в процессе их работы, но, когда появился термин, это было не так.

12
Более тонкие средства защиты

Второй способ защиты – снижение эффективности взлома.

Компрометация деловой электронной почты – это хакерская атака с помощью социальной инженерии, поскольку она использует не технологическую, а человеческую уязвимость. При такой мошеннической схеме жертва получает электронное письмо от источника, которому доверяет, содержащее вполне законный запрос, но с просьбой сделать это не так, как обычно, зачастую вопреки установленному протоколу. Так, бухгалтер получает электронное письмо от поставщика, который просит перечислить деньги на новый банковский счет. Или покупатель жилья получает электронное письмо от компании-застройщика с инструкциями о том, как перевести первый взнос. Или финансовый директор может получить электронное письмо от генерального директора с просьбой срочно перевести многомиллионную сумму на конкретный счет. Счета-получатели принадлежат мошеннику, и жертва, как правило, никогда больше денег своих не видит. Подобные аферы стоят миллиарды.

Иногда такая схема предполагает взлом электронных почтовых ящиков продавцов – это повышает вероятность того, что жертва будет доверять отправителю. Чаще всего электронные письма мошенников представляют собой незначительные вариации настоящих адресов, что-то вроде person@c0mpanyname.com вместо person@companyname.com. (Если вы слушаете аудиокнигу, то буква «о» в первом слове «companyname» заменена на ноль.)

Уязвимость здесь заключается в невнимательности, свойственной людям, или неуместном доверии.

Существует масса причин, по которым уязвимость нельзя устранить. В мире политики законодательный процесс, который должен это делать, может оказаться неработоспособным. Или же может не оказаться руководящего органа, который выдает предписание создать патч. В случае хакинга с помощью социальной инженерии, описанного выше, хакеры взламывают работу нашего мозга, а эта уязвимость не поддается исправлению в более короткие сроки, чем определит эволюция.

Когда мы не можем устранить уязвимость, у нас есть три варианта. Первый – *перепроектировать систему* так, чтобы взломать ее было слишком сложно, слишком дорого, менее прибыльно или же менее разрушительно. Это подход работает и в тех случаях, когда просто объявить хак вне закона недостаточно и мы хотим дополнительно усложнить жизнь хакерам.

Второй вариант – *предвидение* . Если я расскажу вам о компрометации деловой электронной почты и о том, как это работает, вы станете лучше распознавать ситуации, когда становитесь потенциальной мишенью, и, надеюсь, с меньшей вероятностью попадете в расставленные сети. Именно так мы защищаемся от мошеннических атак по электронной почте и телефону, которые проскальзывают через автоматические фильтры. Именно так потенциальные жертвы могут противостоять эффективным когнитивным взломам, которые играют на универсальных человеческих предубеждениях, таких как страх и доверие к авторитету.

Это подразумевает использование дополнительной системы с целью обезопасить основную. Для противодействия компрометации деловой электронной почты компания может ввести требование, чтобы любые крупные денежные переводы утверждались как минимум двумя людьми. Это означает, что, даже если взлом пройдет успешно и сотрудник будет одурачен, хакер не сможет извлечь выгоду из своего обмана.

Этот вариант защиты часто обсуждается как решение проблемы незащищенных IoT-устройств. Беспокойство вызывает тот факт, что через несколько лет в наших домах и сетях появятся разнообразные уязвимые IoT-устройства, защитить которые будет просто невозможно. Одним из решений является наличие в сетях систем, распознающих эти устройства и ограничивающих их поведение таким образом, чтобы снизить возможность для хакинга. Представьте, что ваш домашний маршрутизатор умен настолько, что распознает IoT-устройства и блокирует их, когда те пытаются делать нечто, чего делать не должны, например если холодильник начинает рассылать спам, добывать криптовалюту или участвовать в DoS-атаках.

Третий вариант защиты – *обнаружение хака и восстановление системы постфактум.*

В 2020 г. российская служба внешней разведки (СВР) взломала серверы обновлений, принадлежащие разработчику программного обеспечения, под управлением которого работала сеть компании SolarWinds. В числе ее 300 000 клиентов по всему миру было большинство компаний из списка Fortune 500 и члены правительства США. СВР установила бэкдор [68] в обновление одного из продуктов компании, который носил название Orion, и стала выжидать.

Остановимся на секунду. Всего несколько страниц назад я объяснял, что главный в компьютерной индустрии метод защиты от хакеров – это исправления. СВР взломала сам процесс создания патчей, а затем подсунула бэкдор в одно из обновлений продукта. Более 17 000 клиентов Orion скачали и установили хакнутое обновление, предоставив СВР доступ к своим системам. СВР подмяла под себя тот самый процесс, которому ожидаемо все должны доверять, чтобы повысить свою безопасность.

---

[68] Бэкдор (*англ* . back door – черный ход) – лазейка, намеренно встроенная в код легальной программы. – *Прим. пер* .

Хак не был обнаружен ни АНБ, ни каким-либо другим подразделением правительства США. Компания FireEye, предоставляющая услуги в сфере сетевой безопасности, случайно наткнулась на него в ходе детального аудита собственных систем.

Как только взлом SolarWinds выплыл наружу, сразу стало ясно, насколько катастрофической (или успешной, в зависимости от вашей позиции) оказалась эта операция. Русские взломали Государственный департамент США, министерство финансов, министерство внутренней безопасности, Лос-Аламосскую и Сандийскую национальные лаборатории, а также Национальные институты здравоохранения. Они проникли в Microsoft, Intel и Cisco. Они взломали сети в Канаде, Мексике, Бельгии, Испании, Великобритании, Израиле и ОАЭ.

После проникновения в эти системы хакеры СВР смогли установить новые средства доступа, не связанные с уязвимостью SolarWinds. Таким образом, даже после того, как компании, подвергшиеся атаке, исправили свое программное обеспечение и устранили проблемы с помощью новых, уже безопасных обновлений, в их сетях все еще оставались неизвестные уязвимости. Единственный надежный способ восстановить безопасность в такой ситуации – выбросить все оборудование и программное обеспечение и начать с нуля. Но ни одной организации не хватило решимости поступить таким образом, и я полагаю, что их сетями по-прежнему можно манипулировать из Москвы.

Из этой истории следует несколько выводов. Во-первых, обнаружить хак бывает непросто. Иногда его удается распознать прямо во время взлома, но чаще всего это происходит уже после, к примеру в процессе аудита. Во-вторых, хак может быть настолько разрушительным, что никакие ответные меры не будут достаточными. В-третьих, может оказаться просто нереальным восстановиться после конкретного взлома. В этом случае восстановление будет заключаться прежде всего в защите системы от дальнейших хакерских атак.

И, наконец, еще об одном способе защиты – *поиске уязвимостей до того, как они будут использованы злоумышленником* .

Атака «красной команды»[69] – это не что иное, как взлом собственных систем. Можно прибегнуть к услугам компаний, которые специализируются на подобном анализе, а можно поставить задачу разработчикам делать это самостоятельно в рамках процесса контроля качества. И в том, и в другом случае «красная команда» рассматривает систему так, как если бы являлась внешним хакером. Обычно такая команда находит массу уязвимостей (в компьютерном мире они есть всегда), которые исправляются до выхода программного обеспечения.

Эта концепция пришла из армейского арсенала. Традиционно «красной командой» на воинских учениях называли подразделение, игравшее роль врага[70] . Сообщество кибербезопасности взяло этот термин, чтобы обозначить группу людей, обученных думать как враг и находить уязвимости в системах. Это более широкое определение было включено в процесс военного планирования и в настоящее время является неотъемлемой частью военного стратегического мышления и проектирования систем. Министерство обороны США, особенно сектор национальной безопасности, уже давно интегрировало «красную тройку» в процесс планирования. Вот что заявил об этом Научный совет по вопросам обороны США:

---

69 В IT-индустрии принято употреблять этот термин на языке оригинала: «red team», «red-teaming». – *Прим. науч. ред* .

70 University of Foreign Military and Cultural Studies Center for Applied Critical Thinking (5 Oct 2018), The Red Team Handbook: The Army's Guide to Making Better Decisions, US Army Combined Arms Center, https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf.

> Мы утверждаем, что «красные команды» [71] сейчас особенно важны для министерства обороны… Агрессивные «красные команды» необходимы для оспаривания новых оперативных концепций, чтобы обнаружить их недостатки прежде, чем это сделает реальный противник.

Если вы не создаете «красную команду», то, чтобы найти уязвимости в своих системах, вам придется полагаться на своих же врагов. Но если уязвимости находит кто-то другой, как вы можете быть уверены, что они будут устранены, а не использованы? В компьютерном мире основным средством противодействия использованию хакерами плодов своих усилий является признание компьютерного взлома преступлением. Если вы хакер и обнаружили новую уязвимость, то можете использовать ее с риском получить тюремный срок. Но вы также можете продать информацию на черном либо на сером рынке.

Противодействующим стимулом являются поощряющие программы, известные как bug bounties, когда компании-разработчики программного обеспечения выплачивают вознаграждение людям, обнаружившим уязвимости в их продуктах. Идея заключается в том, чтобы заинтересовать исследователей сообщать о своих находках в компанию. Bug bounties неплохо справляются со своей задачей, хотя зачастую хакеры могут заработать куда больше, толкая информацию об уязвимостях преступникам или производителям кибероружия.

В любом случае чем больше вы знаете о системе, тем легче находить новые уязвимости, особенно если у вас имеется доступ к человекочитаемому исходному коду, а не только к объектному коду, читаемому машиной. Точно так же легче найти уязвимости в своде правил, если у вас есть копия самого свода правил, а не только информация о постановлениях на его основе.

13
Устранение потенциальных хаков на этапе проектирования систем

Автозапуск – функция, впервые появившаяся в Windows 95. До этого момента вы покупали программное обеспечение на компакт-диске, а затем вручную запускали сценарий установки на своем компьютере. С автозапуском вы могли просто вставить диск в дисковод, и система автоматически находила и запускала сценарий установки. Это значительно упрощало установку программного обеспечения для среднего, технически неграмотного пользователя.

К сожалению, функция автозапуска также использовалась вирусописателями для установки в системы вредоносных программ. Вирус размещался на безобидном компакт-диске или, в более поздние годы, на флешке и автоматически запускался, как только ничего не подозревающий пользователь вставлял его в компьютер. Вот откуда ведет свою историю всем известное предупреждение о небезопасности подключения случайных USB-накопителей к компьютеру.

Обратите внимание, что в данном случае уязвимость не является следствием ошибки. Это была попытка найти баланс между безопасностью и удобством использования. Найденный компромисс, возможно, и выглядел разумным в 1995 г., чего нельзя было сказать о нем десятилетие спустя. Сообщения о системных ошибках, вызванных автозапуском, стали множиться как грибы после дождя, и в 2011 г. Microsoft наконец-то перепроектировала систему для Windows Vista, отключив функцию автозапуска для флешек, сетевых дисков и прочих носителей, оставив ее только для таких вымирающих мастодонтов, как DVD-диски.

Проблема заключается в том, что невозможно создать идеальную защиту от хакеров на этапе проектирования, поскольку, во-первых, безопасность – это лишь одно из свойств,

---

[71] Defense Science Board (Sep 2003), «Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities,» Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, https://apps.dtic.mil/dtic/tr/fulltext/u2/a430100.pdf.

которые должны быть оптимизированы при разработке системы, а во-вторых, методы, которые используют хакеры, их цели и мотивы постоянно меняются по мере развития общества и технологий. Проектировщикам необходимо пересмотреть свои основные подходы к организации и запуску систем. Хороший дизайн системы со временем теряет свои преимущества, и хакеры всегда найдут способы использовать его в своих целях.

Вместо того чтобы находить уязвимости в системе до того, как она будет взломана, мы можем попытаться создать систему с меньшим количеством уязвимостей, то есть *сделать так, чтобы они не существовали изначально* . В сфере информационной безопасности это называется проектированием безопасных систем.

Впрочем, сказать намного легче, чем сделать. В сложноорганизованном компьютерном коде невозможно найти все скрытые лазейки. Простые смертные не могут создать программное обеспечение без ошибок и уязвимостей. У нас до сих пор нет теории проектирования безопасного программного обеспечения, не говоря уже о методологии такого процесса. Но главная причина, по которой мы не повышаем качество в этой сфере, заключается в том, что писать безопасный и надежный код – трудно, медленно и дорого, а значит, как правило, для этого нет экономического стимула. За такими редкими исключениями, как электронные системы самолетов и космических кораблей, большая часть программного обеспечения пишется в спешке и кое-как. Но базовые принципы проектирования, которые минимизируют количество уязвимостей и возможности их использования, у нас все-таки есть.

Простота. Чем сложнее система, тем более она уязвима. Причин тому множество, но, обобщая их, можно сказать, что в сложной системе присутствует куда больше элементов, которые могут сработать не так. Например, у здания офисного центра больше потенциальных уязвимостей, чем у дома на одну семью. Противоядием служит простота. Многие естественные системы сложны по самой своей природе, но что касается искусственных систем, то чем проще они разработаны, тем более безопасными будут в дальнейшем.

Глубокая защита. Основная идея этого подхода заключается в том, что одна уязвимость не должна разрушать всю систему. В компьютерных системах это чаще всего реализуется методом многофакторной аутентификации, когда кроме имени пользователя и пароля, являющихся единой точкой отказа [72] , используют несколько методов аутентификации. К примеру, моя электронная почта дополнительно защищена Google Authenticator. Это приложение привязано к моему смартфону, который всегда со мной. Чтобы получить доступ к своей учетной записи, мне нужно разблокировать телефон, открыть приложение и ввести сгенерированный им код. Другие многофакторные системы могут включать биометрию, например отпечаток пальца, или небольшое USB-устройство, подключаемое к компьютеру.

Для некомпьютерных систем глубокая защита – это все, что не позволяет какой-то одной уязвимости стать причиной успешного взлома системы. Это может быть засов на двери в дополнение к основному замку, двойной забор с колючей проволокой вокруг военной базы или требование, чтобы финансовые операции на определенную сумму утверждались двумя людьми. Хак, преодолевающий один из этих барьеров, вряд ли сможет преодолеть и другой.

Компартментализация (изоляция / разделение обязанностей). Умные террористические организации разделяют себя на ячейки. Каждая ячейка имеет

---

[72] Единая точка отказа (*англ* . Single point of failure, SPOF) – узел системы, отказ которого приводит к ее неработоспособности. – *Прим. пер* .

ограниченное представление об остальных, поэтому если одна из них скомпрометирована, то другие остаются в безопасности. Это и есть компартментализация, которая ограничивает последствия любой конкретной атаки. Эта же идея лежит в основе того, что в одной организации ключи от всех кабинетов разные, а у каждой учетной записи – свой пароль. Такой подход еще называют принципом наименьших привилегий, когда человеку или подразделению предоставляется только тот уровень доступа, который необходим для выполнения работы. Именно благодаря этому принципу у вас нет главного ключа от всех кабинетов в здании, где вы работаете, ведь у вас нет в нем производственной необходимости.

В компьютерных сетях такой подход называется *сегментацией* . Он подразумевает разделение сети на части, подобные террористическим ячейкам, чтобы хакерская атака на одну из них не привела к взлому всей сети. Сегментация – это первое, что пытается нарушить злоумышленник после проникновения в сеть. Например, хорошая сегментация не позволила бы СВР использовать уязвимость SolarWinds для доступа к различным частям сети и установить вредоносные программы и бэкдоры.

Эта концепция легко применима и в социальных системах. Она находит отражение, например, в идее, что государственные регуляторы не должны иметь финансовых интересов в отраслях, которые они регулируют. (Впрочем, этот принцип регулярно нарушается в США, благодаря так называемому эффекту вращающихся дверей, когда происходит взаимная ротация кадров между правительством и отраслями.) Или в том, что избирательные округа не должны создаваться выборными должностными лицами, которые могут извлечь выгоду из джерримендеринга[73].

Механизмы защиты от сбоев. Все системы дают сбой, будь то в результате несчастного случая, ошибки или атаки. Мы хотим, чтобы они выходили из строя максимально безопасно. Есть простые решения, например выключатель мертвеца в поезде: если машинист теряет дееспособность, поезд перестает ускоряться и в конце концов останавливается. Есть решения намного сложнее, как в случае с пусковыми установками ядерных ракет, которые имеют всевозможные надежные механизмы, гарантирующие, что боеголовки никогда не будут запущены случайно.

Социальные системы также могут иметь механизмы защиты от сбоев. Многие наши законы содержат нечто подобное. Убийство незаконно, независимо от используемых средств, даже если вы придумаете хитрый способ взломать систему для его совершения. Альтернативный минимальный налог (AMT) в США должен был служить в качестве предохранительной меры, чтобы граждане платили минимальный налог независимо от того, сколько и какого рода лазеек они обнаружили. (То, что AMT не сработал так, как это задумывалось, демонстрирует сложность поставленной задачи.)

*** * ***

Все перечисленные контрмеры также снижают эффективность хакинга.

Пока что я не сказал ничего нового. Большую часть этой темы я уже освещал в своей книге 2000 г. «Секреты и ложь»[74]. Другие авторы писали об этом и до меня, и после. Но понимание подходов безопасного проектирования имеет решающее значение для ограничения эффективности взлома. Чем больше фундаментальных принципов безопасности вы сможете включить в дизайн вашей системы, тем надежнее она будет

---

[73] Джерримендеринг (*англ* . Gerrymandering; также избирательная геометрия) – произвольная демаркация избирательных округов с целью изменения соотношения политических сил внутри каждого и, как следствие, в целом на территории проведения выборов. Термин происходит от имени губернатора штата Массачусетс Элбриджа Герри (Джерри), который в 1812 г. перекраивал границы избирательных округов. – *Прим. пер* .

[74] Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003.

защищена от хакеров.

Используют компании эти методы или нет, зависит от конкретной отрасли. Можно предположить, что такие гиганты, как Apple и Microsoft, тратят гораздо больше денег на обеспечение безопасности своих программных продуктов, чем разработчики игр для мобильных телефонов. Точно так же можно ожидать, что компания, создающая программное обеспечение для самолетов, автомобилей и медицинских приборов, потратит значительно больше средств и усилий на обеспечение безопасности, чем компания, выпускающая программируемые игрушки. И хотя всегда есть исключения, в основном такая картина верна.

14
Экономика безопасности

В 1971 г. некто, купивший билет на имя Дэна Купера, хакнул Boeing 727, использовав кормовой трап весьма нетривиальным способом: после успешного захвата самолета и получения выкупа в размере $200 000 наличными он выпустил пассажиров, заставил пилотов взлететь и выпрыгнул с парашютом, чтобы навсегда исчезнуть для правоохранителей, которые так и не смогли установить его личность. За Купером последовало множество подражателей, и в итоге компания Boeing изменила конструкцию этой модели, убрав кормовой трап и тем самым устранив возможность выпрыгнуть в полете. Это было эффективное, но дорогостоящее исправление уязвимости. Однако почему она вообще существовала? Вероятно, компания считала эту угрозу или нереальной, или слишком отдаленной, чтобы от нее защищаться.

Моделирование угроз – это термин из области системного проектирования, означающий последовательное перечисление всех возможных угроз для системы[75]. Если в качестве системы вы рассмотрите свой дом, то для начала стоит перечислить, что в нем наиболее ценное: жильцы, семейные реликвии, оригинал Пикассо, дорогая электроника. Затем нужно перечислить все способы, которыми посторонний может проникнуть в дом: незапертая дверь, открытое окно, закрытое окно и т. д. После этого вы рассмотрите разные типы людей, которые могут захотеть проникнуть в дом: профессиональный взломщик, соседский ребенок, преследователь, серийный убийца. Не стоит забывать об угрозах от людей, которым не нужно взламывать дверь, например о возможном насилии со стороны интимного партнера. И, наконец, вы используете всю эту информацию для построения модели, подробно описывающей то, о каких угрозах стоит побеспокоиться, а какие можно проигнорировать, сколько усилий нужно потратить на смягчение конкретных угроз и т. д. Ваша домашняя безопасность будет иметь свою специфику, если вы владеете оригиналом Пикассо, являетесь президентом страны или живете в зоне боевых действий.

Экономические соображения необходимы для понимания того, как строить защиту от хакинга. Определите размер убытков в случае взлома системы. Определите стоимость и эффективность конкретных методов безопасности. Проведите анализ затрат и выгод, чтобы понять, стоит ли каждый метод потраченных на него средств. В некоторых случаях нет смысла внедрять защиту. Например, существует множество потенциальных мер безопасности, которые могут снизить количество взломов банкоматов, но они не применяются, поскольку раздражают законных клиентов. Такие методы, как сканирование отпечатков пальцев или система распознавания лиц, многие клиенты сочтут нарушающими конфиденциальность. Если эти меры ощутимо снизят частоту использования банкоматов, то сделают их менее прибыльными, несмотря на то что повысят уровень безопасности.

Еще одно понятие из области экономики, которое важно для понимания хакинга

---

75 Adam Shostack (2014), Threat Modeling: Designing for Security, John Wiley & Sons.

и защиты от него, – это экстерналии. Экстерналией называется внешний эффект от экономической деятельности, который сказывается на людях, непосредственно не вовлеченных в эту деятельность. Помните владельца фабрики, решившего загрязнить реку? Люди, живущие ниже по течению, в результате могут заболеть, но владелец живет в другом месте, и ему все равно.

Конечно, все не так однозначно. Ниже по течению могут жить работники фабрики и ее клиенты. Экологические активисты могут разоблачить факт загрязнения, пресса – опубликовать критические статьи, а общественное мнение – обернуться против владельца. Тем не менее в нашем системном мышлении загрязнение реки является экстерналией.

Хакинг вызывает внешние эффекты. У этих эффектов есть цена, которую платит общество. Это похоже на воровство в магазинах: все должны покупать по более высоким ценам, чтобы компенсировать потери или оплатить меры, предпринимаемые магазином для борьбы с воришками.

Мы знаем, как решить проблемы, вызванные внешними эффектами: нужно преобразовать их в проблемы, которые затрагивают человека, владеющего системой и принимающего решения. Для этого мы налагаем на систему правила извне, чтобы перенести затраты внутрь самой системы.

В идеальном мире такой подход работает блестяще. В реальности его эффективность зависит от правоприменения и наказаний, от юристов и результатов судебных разбирательств. Она зависит от действий регулирующих органов, на которые влияют представители власти, лоббисты, стремящиеся смягчить нормы, а также доноры избирательных кампаний со своими программами. Она зависит от результатов исследований, финансируемых промышленностью и научными кругами, которые могут искажаться в интересах политических сил. Она зависит от граждан, которые должны не только понимать, что подобные затраты существуют, но и то, как и кого именно заставить понести их.

Технические системы становятся небезопасными при изменении модели угроз. По сути, любая система проектируется в соответствии с реалиями своего времени. Затем в какой-то момент ее использования что-то меняется. Какова бы ни была причина изменений, старые предположения, положенные в основу безопасности, больше не верны, и система становится незащищенной. Уязвимости, которые когда-то были неважными, превращаются в критические. Критические уязвимости, напротив, перестают быть актуальными. Хаки становятся то проще, то сложнее, то более прибыльными, то менее, то распространенными, то единичными.

Возможно, самым наглядным примером этого служит сам интернет. Как бы смешно это ни звучало сегодня, но интернет создавался без учета требований безопасности. Еще в конце 1970-х – начале 1980-х гг. он не использовался для каких-то важных дел, а чтобы получить к нему доступ, нужно было быть сотрудником исследовательского учреждения. Многопользовательские мейнфреймы, подключенные к интернету, имели свои собственные системы безопасности. По этим причинам первые разработчики интернета намеренно игнорировали соображения безопасности в пользу более простого протокола и оставляли их на усмотрение многопользовательских конечных точек.

Мы все знаем, чем закончилась эта история. Сначала к интернету стали подключаться однопользовательские персональные компьютеры без систем безопасности, но разработчики сетей предположили, что эти компьютеры имеют такой же уровень безопасности, как и старые мейнфреймы. Затем изменилось все, что касается использования интернета. Изменилась его скорость. Изменился масштаб. Изменилась область его применения. Изменилась и вышла на первый план его роль в обществе. Взломы, о которых раньше никто и помыслить не мог, внезапно стали критически важными. Изменилась модель угроз. А это означало, что анализ затрат и выгод стал тоже иным.

В области компьютерной безопасности мы хорошо знаем, что такое динамичные среды. Кажется, что каждые несколько лет меняется абсолютно все и методы безопасности должны

меняться тоже. Спам в системе электронной почты является проблемой в той мере, в какой стала экономически невыгодной почта бумажная, поскольку отправлять электронные письма намного дешевле.

Поддержание безопасности в этой динамичной среде требует работы на опережение хакеров. Вот почему мы занимаемся исследованиями в области компьютерной безопасности, проводим конференции, выпускаем журналы, создаем программы для выпускников университетов, устраиваем хакатоны. Мы обмениваемся информацией о том, что предпринимают хакеры, и делимся передовыми методами защиты. Мы пытаемся понять, где появятся новые уязвимости, до того, как это произойдет, и как именно хакеры будут реагировать на них.

Для того чтобы законы поспевали за хакерами, они должны давать регуляторам необходимую гибкость в вопросах запрета новых хаков и наказания хакеров. Закон о компьютерном мошенничестве и злоупотреблениях был принят в 1986 г. и стал результатом обеспокоенности тем, что существующие на тот момент законы не охватывали все преступления, связанные с компьютерами. Например, этот закон, среди прочего, квалифицирует доступ к чужой компьютерной системе без разрешения или превышение уровня авторизованного доступа как преступление. Такая формулировка оказалась настолько широкой, что в 2021 г. Верховный суд США сократил ее. Однако смысл закона остался прежним – он позволяет обвинению заявить: «Хотя система и дала возможность осуществить хак, но такие действия явно не были предусмотрены, и ответчик знал, что поступает неправильно. И потому его действия незаконны».

Для многих наших социальных систем возможность исправления самих себя заложена не только внутри, но и на внешнем уровне более общих правил, по крайней мере в некоторой степени. Остается открытым вопрос: как мы осуществляем управление жизненным циклом некомпьютерных систем? Как часто мы должны проверять на уязвимости наши демократические институты и то, соответствуют ли они своему назначению? И что делать в случае, если это не так? Каждые несколько лет мы покупаем новый ноутбук или смартфон, справедливо полагая, что новые устройства более безопасны. Но как нам сделать то же самое с социальными институтами?

15
Устойчивость

Системы норм отличаются от сводов правил. В самой природе нормы заложено, что ее невозможно взломать; в случае нормы хак – это всего лишь другое слово для обозначения ее нарушения. С другой стороны, поскольку нормы более неформальны, чем правила, и не кодифицированы, существует больше возможностей для интерпретаций. Это приводит к тому, что мотивированный человек может легче перейти границы норм или оптимизировать свои действия для достижения определенного результата. А поскольку эти системы требуют от людей реагировать на атаки, нормам намного проще развиваться, чтобы, в частности, делать хаки легитимными.

В качестве примера можно взять недавние события, когда Дональд Трамп смог успешно выступить против социальных и политических норм. Я стараюсь не иллюстрировать Трампом те или иные тезисы этой книги по той причине, что он политически заряжен. Но здесь я сделаю исключение, поскольку пример слишком показателен, чтобы его игнорировать. У общества есть механизмы исправления мягких нарушений социальных норм – публичное посрамление, политический откат, журналистика и прозрачность. И все эти механизмы неплохо справлялись, пока Трамп не перегрузил их. В очень короткий срок возникло слишком много скандалов. Механизмы, которые корректировали поведение государственных служащих, оказались неэффективными перед лицом такого кандидата, как Трамп. Нормы работают только в том случае, если существуют последствия их нарушений, а общество просто не успевало реагировать на такой натиск.

Таким образом, Трамп смог раздвинуть границы норм сразу во многих направлениях. И в некоторых случаях это разрушило сами нормы[76].

Однако, подобные вызовы системам норм могут повысить их устойчивость. Нормы – это что-то неявное и достаточно гибкое, поэтому их легко изменить. Для того чтобы оспорить и изменить систему норм, не нужны деньги, юридические знания или технологии, хотя все это, конечно, может помочь. Наши социальные модели поведения и неявные ожидания могут быть оспорены каждым, кто готов высказаться о них и имеет для этого платформу. И такой вызов скорее поможет нормам развиваться и совершенствоваться, чем сломает их.

Устойчивость является важной концепцией, которая применима ко всему: от человеческого тела до планетарной экосистемы, от организационных систем до систем компьютерных. Это способность системы восстанавливаться после возмущений, в число которых входят и хаки.

Устойчивость – это то, почему при строительстве подвесных мостов используют натянутые тросы, а не цельнометаллические стержни: вторые разрушаются внезапно и катастрофически, а тросы рвутся медленно и громко. Именно ради устойчивости наши мозг и тело знают так много разнообразных способов адаптации к любым обстоятельствам, в которых мы оказываемся. Хорошие таксисты знают, как объехать популярные достопримечательности как минимум четырьмя маршрутами, и это тоже устойчивость. И даже то, что в округе Ориндж, штат Калифорния, функционирует окружное правительство, объявившее о своем банкротстве в 1994 г.[77], – факт, иллюстрирующий тот же принцип.

В сфере безопасности устойчивость – это эмерджентное, то есть не сводимое к сумме ее компонентов, свойство системы, которое может сочетать в себе такие аспекты, как непроницаемость, гомеостаз, избыточность, маневренность, смягчение и восстановление. Устойчивые системы более безопасны, чем хрупкие. Многие из мер безопасности, которые мы обсуждали в предыдущих главах, направлены на повышение устойчивости системы к взлому.

Здесь стоит упомянуть еще один момент. Мы говорили о защите от хакинга в основном абстрактно, однако любое обсуждение такой защиты должно ответить на несколько конкретных вопросов. Кто от кого защищается? Кто решает, полезен взлом или нет? И, самое главное, кто отвечает за безопасность и за то, насколько защитные меры стоят затраченных усилий и средств?

Примеры, которые я приводил до сих пор, были довольно простыми: за системой стоит некий человек или организация, и они же отвечают за ее безопасность. Например, руководство Microsoft решает, является ли конкретный хак Windows проблемой и как эту проблему решить. Как правило, все решается установкой патча. Если поставить патч оказывается сложно, система живет с уязвимостью какое-то время, как это было в случае с функцией автозапуска. У нас есть примеры, когда уязвимости после взлома быстро исправлялись, и есть другие, когда хаки оставляли нетронутыми, потому что защита от них оказывалась слишком дорогим удовольствием. Если потери от мошенничества меньше, чем затраты на исправление системы, то компании, обслуживающие кредитные карты, позволят

---

[76] Автор транслирует принятую точку зрения приверженцев Демократической партии США. – *Прим. ред*.

[77] Округ столкнулся с дефицитом в $1,5 млрд. Правительство округа подало заявление, согласно главе 9 Кодекса о банкротстве. Цель главы 9 – согласовать план погашения между кредиторами, который может включать снижение основной суммы или процентной ставки по непогашенной задолженности, продление сроков погашения кредита, а также рефинансирование долга путем получения нового кредита. Достаточно подать заявление о реорганизации долга, чтобы взыскание средств было приостановлено. Через полгода после объявления о банкротстве правительство округа, в котором проживает 2,5 млн человек, вновь вышло на рынок финансовых займов и до сих пор привлекает немало средств. – *Прим. ред*.

мошенничеству продолжаться. Магазины часто позволяют шоплифтерам [78] уходить с украденными товарами, потому что сотрудники, пытаясь остановить их, могут пострадать физически, а ложное обвинение людей в краже – привести к дорогостоящим судебным разбирательствам.

Поскольку мы пытаемся построить социальные и политические системы, способные защищать себя от хакеров, необходимо подумать о балансе между написанием законов законодателями и их исполнением регуляторами. С одной стороны, регулирующие органы не несут прямой ответственности перед людьми в той же мере, что и законодатели. С другой стороны, мы не хотим, чтобы законодатели увязали в деталях реализации законов до их принятия. Чем больше законодательные органы могут делегировать реализацию законов регуляторам, тем более гибкой и устойчивой к взломам будет созданная система.

Защита социальных систем от хакинга – это не только проблема разработчиков данных систем. Это проблема, стоящая перед всем обществом, перед каждым, кто желает социальных изменений и прогресса в целом.

Часть III
Хакинг финансовых систем

16
Хакинг райских кущ

Одним из центральных постулатов средневекового католицизма была идея покаяния и искупления. Она заключалась в том, что если вы согрешили, то можете искупить свою вину и получить прощение. Большие грехи требовали не просто раскаяния в содеянном, но и столь же больших мероприятий по их искуплению, которые многим были не по карману. Единственным способом искупить все грехи, совершенные на протяжении жизни, было паломничество в Иерусалим, но большинство людей просто не смогли бы его совершить. Поэтому церковь предприняла следующий логический шаг, начав принимать денежные пожертвования, чтобы другие могли проделать трудный и опасный путь от вашего имени. Это был разумный компромисс, и церковь поощряла подобную благотворительность. Так, если городская церковь нуждалась в новой крыше, богатому грешнику в качестве покаяния поручали оплатить ее ремонт. В обмен грешник получал отпущение грехов в форме индульгенции – документа, по сути подтверждающего пред Богом и людьми, что грехи его отпущены. Казалось бы, благодать, да и только.

Уязвимость этой схемы, однако, заключалась в том, что индульгенции – товар безграничный. Духовенство начало использовать его в качестве валюты, и это стало эксплойтом. Система в целом регулировалась слабо, а значит, никто не был в состоянии эффективно ограничить способ продажи индульгенций. Церковь печатала их столько, сколько могла продать, и скоро состоятельные люди осознали, что могут купить столько отпущения, сколько им нужно. Появились посредники, которые платили коррумпированным епископам за право перепродавать индульгенции. То, что задумывалось как система искупления [79], превратилось в систему наживы и власти. В 1517 г. практика продажи индульгенций привела к тому, что Мартин Лютер вывесил свои знаменитые «Девяносто пять

---

78 Шоплифтинг – несанкционированный вынос товара из магазина розничной торговли. Подсчитано, что такое преступление в мере совершается каждые пять секунд. Продавцы, для борьбы с убытками только от шоплифтеров, вынуждены в среднем повышать стоимость товаров на 3 %. – *Прим. ред* .

79 R. N. Swanson (2011), Indulgences in Late Medieval England: Passports to Paradise? Cambridge University Press.

тезисов» – диспут о покаянии и индульгенциях – на дверях Замковой церкви в немецком Виттенберге, положив начало протестантской Реформации и вызвав более чем столетнюю религиозную войну.

Везде, где можно заработать, есть хакеры. А те, кто умеет распознавать выгодные лазейки, могут получить много денег. Это делает финансовые системы уникально подходящими (то есть выгодными) для взлома. Иоганн Тецель, доминиканский монах начала XVI в.[80], изобрел два инновационных продукта для системы индульгенций. Во-первых, он выдвинул и продвигал идею о том, что можно покупать индульгенции для умерших друзей и близких [81], тем самым повышая их статус в загробной жизни с чистилища до рая. Во-вторых, он продавал индульгенции, которые якобы давали отпущение не только прошлых, но и будущих грехов. Что-то вроде пожизненной гарантии на посмертное избежание ада[82].

Несмотря на серьезные протесты со стороны католических богословов и реформаторов, таких как Мартин Лютер, Ватикан не смог пресечь эту практику. Церковь стала зависеть от огромных прибылей, получаемых с продажи и перепродажи индульгенций, и это парализовало любые ответные меры. К примеру, продажа индульгенций Тецелем стала основным источником финансирования строительства собора Святого Петра.

Многие из хаков, о которых мы уже говорили, были заблокированы теми, кто управлял системой. Авиакомпании обновили правила программ поощрения часто летающих пассажиров. В спорте периодически обновляются правила той или иной игры. Но время от времени управляющая система разрешает хак и даже объявляет его законным. Изогнутая клюшка сделала игру более захватывающей. Подсчет карт выгоден для казино в качестве приманки, даже если среди клиентов порой попадаются компетентные счетчики карт.

Такая нормализация хака – обычное явление в финансовом мире. Иногда новые хаки пресекаются регулирующими органами, но чаще они получают добро и даже закрепляются законодательно уже после совершения факта взлома. Это один из механизмов, с помощью которого финансовые системы внедряют инновации. Новые идеи приходят не только от регуляторов, но и от реальных пользователей в виде хаков.

Хотя самым очевидным решением обычно является исправление системы, часто его невозможно реализовать по политическим мотивам. Власть и деньги сплавляются в лоббистский мускул, который давит на игровую доску до тех пор, пока она не наклонится в нужную сторону. Это не значит, что хаки финансовых систем не исправляют в принципе, просто порой процесс занимает немало времени. Только в 1567 г. папа Пий V отменил разрешение на выдачу индульгенций, связанных с финансовыми операциями, что позволило исправить систему и устранить хак.

Люди с деньгами в качестве хакеров обладают могуществом, а прибыль является мощным стимулом как для самого взлома, так и для его легализации.

---

80 Ray Cavanaugh (31 Oct 2017), «Peddling purgatory relief: Johann Tetzel,» *National Catholic Reporter* , https://www.ncronline.org/news/people/peddling-purgatory-relief-johann-tetzel.

81 Якобы у них даже был рекламный слоган: «Лишь злато в ларце зазвенит, / Душа облегченно на небо летит».

82 Совершенно не связанное с этим наблюдение: карта «Пожизненный выход из тюрьмы» в игре «Монополия» может быть использована, чтобы хакнуть правило, запрещающее игрокам давать друг другу деньги взаймы. Игроки могут продавать карту друг другу за любую сумму, что превращает ее в удобное средство денежных переводов.

Jay Walker and Jeff Lehman (1975), 1000 Ways to Win Monopoly Games, Dell Publishing, http://www.lehman-intl.com/jeffreylehman/1000-ways-to-win-monopoly.html.

Хакинг в банковском деле

Многие процедуры, которые мы сегодня считаем обычной составляющей банковского дела, появились как хаки, когда различные влиятельные игроки пытались обойти правила, ограничивающие их поведение и прибыль. Я обращаю на это внимание не ради критики. Хакинг – реальный способ заставить правительство пересмотреть и обновить правила в этой сфере.

На протяжении большей части XX в. Федеральная резервная система регулировала банковскую деятельность в США с помощью так называемого положения Q[83]. Принятое в 1933 г. после Великой депрессии, Положение Q регулировало такие вещи, как потолок процентных ставок по разным видам счетов и ставок для индивидуальных и корпоративных клиентов.

Положение Q – это мера безопасности. До его введения банки конкурировали друг с другом, предлагая клиентам высокие процентные ставки по вкладам. Такая конкуренция побуждала банки рисковать, чтобы заработать на этих вкладах. Ограничения положения Q снижали системный банковский риск.

Более 40 лет эта система работала, но в 1970-х гг. процентные ставки резко выросли, и банки стали отчаянно искать способы обойти положение Q и предложить более высокие процентные ставки по депозитам, чтобы они могли конкурировать с другими видами инвестиций. В начале 1970-х гг. одним из таких способов стал счет NOW[84] – счет с обращающимся приказом об изъятии средств, сочетающий возможности текущего счета для осуществления платежей и снятия денег посредством приказов (чеков) и депозита, на нем деньги замораживаются на определенный срок, после которого выплачиваются проценты. Счета NOW внешне выглядели как процентные депозитные счета, но технически являлись обычными текущими счетами.

Нам известно имя хакера, который изобрел счета NOW, – это Рональд Хаселтон, президент и исполнительный директор Consumer Savings Bank в Вустере, штат Массачусетс. Говорят, что Хаселтон услышал, как клиентка спросила, почему она не может выписывать чеки со своего сберегательного счета. Он тоже задался этим вопросом и взломал правила положения Q, чтобы создать, по сути, первый процентный расчетный счет.

Современные депозитные сертификаты[85] – это еще один пример инновационного банковского хака. Хакерский ход заключался в привлечении дилера по ценным бумагам для создания вторичного рынка депозитных сертификатов, благодаря которому повысилась их привлекательность для корпоративных счетов. Хакеры, придумавшие эту схему, работали в First National City Bank, ныне Citicorp. В 1961 г. банк представил оборотные депозитные сертификаты, по которым выплачивалась более высокая процентная ставка, чем по процентным счетам, а пять лет спустя вывел их на Лондонскую биржу. Вскоре после этого First National City Bank реорганизовался в холдинговую компанию, чтобы избежать банковского регулирования, которое не позволяло ему выпускать депозитные сертификаты

---

83 Положение Q – это правило Совета управляющих Федеральной резервной системы (FRB), которое устанавливает «минимальные требования к капиталу и стандарты достаточности капитала для учреждений, регулируемых советом директоров». Было создано в 1933 г. в соответствии с законом Гласса – Стиголла с целью запретить банкам выплачивать проценты по депозитам на текущих счетах. – *Прим. ред* .

84 Аббревиатура NOW (*англ* .) от «negotiable orders of withdrawal». Вид счетов, предполагающий как начисление процентов, так и выписку чеков, – нечто среднее между сберегательным и расчетным счетами. – *Прим. ред* .

85 Депозитный сертификат (*англ* . Certificate of Deposit, сокр. CD) – именная ценная бумага, удостоверяющая размер внесенной вкладчиком суммы и его право на получение в банке по истечении установленного срока суммы депозита и оговоренных в сертификате процентов. – *Прим. пер* .

по более высоким ставкам. Конгресс исправил ситуацию, внеся в 1956 г. поправки в закон о банковских холдинговых компаниях, в соответствии с которыми регулирование деятельности таких компаний было возложено на Совет Федеральной резервной системы.

К банковским хакам середины XX в. относятся также фонды денежного рынка и евродолларовые счета, созданные для обхода ограничений на процентные ставки, предлагаемые по более традиционным видам счетов.

Все эти хаки стали нормой либо благодаря тому, что регулирующие органы решили не закрывать лазейки, либо благодаря тому, что конгресс прямо узаконил их, как только стали накапливаться жалобы регулирующих органов. Например, счета NOW были легализованы[86] сначала в Массачусетсе и Нью-Хэмпшире, затем в Новой Англии в целом и, наконец, в 1980 г. по всей стране. Многие другие ограничения, наложенные законом о банковских холдинговых компаниях, были отменены с принятием в 1994 г. закона Ригла – Нила, разрешающего проведение банковских операций между штатами и повышающего эффективность филиальных сетей банков. Все это стало частью большой волны банковского дерегулирования, которая продолжалась вплоть до 2000-х гг.

С этой моделью мы будем встречаться снова и снова[87]. Сначала правительство сдерживает банкиров посредством регулирования, чтобы ограничить объем ущерба, который они могут нанести экономике. Но правила регулятора также ограничивают и прибыль банкиров, поэтому они борются с ними. Банкиры хакают эти правила с помощью трюков, которых регуляторы не предвидели и специально не запрещали, и строят вокруг них прибыльный бизнес. Затем они делают все возможное, пытаясь повлиять на регуляторов и на само правительство, чтобы власть разрешила и нормализовала их взломы. Побочный эффект такого процесса – дорогостоящие финансовые кризисы, которые затрагивают население в целом.

Взломы продолжаются и сегодня. Закон Додда – Франка о реформировании Уолл-стрит и защите прав потребителей, принятый в 2010 г. после мирового финансового кризиса 2008 г., должен был стать масштабной реформой системы финансового регулирования. Этот закон включал в себя целый ряд банковских правил, призванных обеспечить большую прозрачность, снизить системные риски и избежать очередного финансового краха. В частности, закон регулировал деривативы, которыми часто злоупотребляли и которые стали одним из главных факторов финансового кризиса 2008 г.

Однако закон Додда – Франка был полон уязвимостей. Банки немедленно привлекли своих юристов к поиску лазеек, которые позволили бы обойти цель закона – и к черту риски для экономики. Первым делом они ухватились за конкретную формулировку, исключающую иностранную деятельность, если только она не имеет «прямой и существенной связи с деятельностью или торговлей в США». Как только эта уязвимость была закрыта, банкиры обошли определение зарубежного «филиала», назвав филиалы «отделениями». Это тоже проработало недолго. Наконец они зацепились за слово «гарантия». По сути, все иностранные деривативы были гарантированы американской материнской компанией, а это означало, что именно она покроет убытки, если что-то случится с зарубежными филиалами. Просто убрав слово «гарантия» и другие эквивалентные термины из своих контрактов, они могли избежать регулирования.

---

86 Joanna H. Frodin and Richart Startz (Jun 1982), «The NOW account experiment and the demand for money,» *Journal of Banking and Finance* 6, no. 2, https://www.sciencedirect.com/science/article/abs/pii/0378426682900322. Paul Watro (10 Aug 1981), «The battle for NOWs,» Federal Reserve Bank of Cleveland, https://www.clevelandfed.org/en/newsroom-and-events/publications/economic-commentary/economic-commentary-archives/1981-economic-commentaries/ec-19810810-the-battle-for-nows.aspx.

87 Хотя он и не использовал никогда слово «хакинг», Хайман Мински размышлял об этом. Hyman Minsky (May 1992), «The financial instability hypothesis,» Working Paper No. 74, The Jerome Levy Economics Institute of Bard College, https://www.levyinstitute.org/pubs/wp74.pdf.

К концу 2014 г. банки перевели 95 % своих сделок со свопами в офшоры[88], в более мягкие юрисдикции, в очередной раз избегая регулирования по Додду – Франку. В 2016 г. Комиссия по торговле товарными фьючерсами попыталась закрыть эту лазейку. Она постановила, что свопы не могут быть отправлены за границу, чтобы обойти требования закона Додда – Франка, и что как гарантированные, так и негарантированные свопы должны покрываться материнской компанией. Но, увы, новое правило не успели доработать до того, как Трамп вступил в должность президента, а назначенный им председатель комиссии так и не довел дело до конца.

Другие хаки были связаны с правилом Уолкера, еще одной составляющей закона Додда – Франка, которая запрещает банкам осуществлять определенные инвестиционные операции на собственных счетах и одновременно ограничивает их взаимодействие с хедж-фондами и фондами прямых инвестиций. Банки быстро поняли, что они могут обойти это правило, если деньги поступают не с их собственных счетов. Они стали создавать различные партнерства и инвестировать через них. Это правило было отменено при администрации Трампа, в результате чего необходимость во многих хаках просто отпала. Наконец, банки поняли, что могут обойти все правила Додда – Франка, касающиеся «торговых счетов», заявив, что они предназначены для некой деятельности, которую они назвали «управление ликвидностью».

Банковские хаки иллюстрируют еще одну вещь, которую мы будем наблюдать неоднократно. Отношения банков и регулирующих органов напоминают бесконечную игру в кошки-мышки. Перед регуляторами стоит задача ограничить безответственное, агрессивное, коррумпированное поведение. Банки заинтересованы в том, чтобы заработать как можно больше денег. Эти две цели противоположны друг другу, поэтому банки взламывают систему регулирования при любой подходящей возможности. Если какой-то банк вдруг решит этого не делать, он будет быстро задавлен конкурентами, продолжившими играть в кошки-мышки.

Очевидное решение проблемы с точки зрения безопасности – исправление – сдерживается агрессивным стремлением отрасли к нормализации (изменению самих норм). Она достигается за счет лоббирования, а также захвата регулятора. Тенденция, когда над регулирующим органом начинает доминировать отрасль и он начинает работать на нее, а не на общественные интересы, весьма распространена. Банковская отрасль также прибегает к хакингу самого законодательного процесса. С 1998 по 2016 г. индустрия финансовых услуг потратила $7,4 млрд на лоббирование[89], причем только банки потратили не менее $1,2 млрд.

Если исправления не являются жизнеспособным решением, мы должны найти уязвимости до того, как они будут взломаны, и, что еще более важно, до того, как они укоренятся в базовой системе и лоббисты начнут настаивать на их нормализации. В финансовых системах государственные органы могли бы объединить усилия, наняв бухгалтеров и юристов для изучения систем по мере их развития и совершенствования нормативных актов, пока те находятся в стадии разработки.

Некоторые страны[90], в том числе Соединенные Штаты, по крайней мере для ряда

---

88 Charles Levinson (21 Aug 2015), «U.S. banks moved billions of dollars in trades beyond Washington's reach,» *Reuters* , https://www.reuters.com/investigates/special-report/usa-swaps. Marcus Baram (29 Jun 2018), «Big banks are exploiting a risky Dodd-Frank loophole that could cause a repeat of 2008,» Fast Company, https://www.fastcompany.com/90178556/big-banks-are-exploiting-a-risky-dodd-frank-loophole-that-could-cause-a-repeat-of-2008.

89 Deniz O. Igan and Thomas Lambert (9 Aug 2019), «Bank lobbying: Regulatory capture and beyond,» IMF Working Paper No. 19/171, International Monetary Fund, https://www.imf.org/en/Publications/WP/Issues/2019/08/09/Bank-Lobbying-Regulatory-Capture-and-Beyond-45735.

90 Несколько банковских регуляторов, в том числе Управление контролера денежного обращения и Бюро финансовой защиты потребителей, предлагают возможность комментировать по крайней мере в отдельных

агентств, уже занимаются подобными вещами, вынося на публичное обсуждение нормативные акты, находящиеся в стадии разработки. Идея заключается в том, чтобы таким образом выявлять способы, с помощью которых правила могут быть взломаны уже сейчас или в ближайшем будущем благодаря ожидаемым технологиям, а затем сразу вносить исправления в текст. Это не устраняет проблем захвата регуляторов или законодательного лоббирования, но по крайней мере могущественные хакеры ничего не теряют, когда такая лазейка закрывается, ведь они не успевают вложиться в эксплойт.

Однако, лоббисты могут злоупотреблять процессом комментирования готовящихся нормативных актов, оказывая давление на регулирующие органы с целью вынудить их оставить лазейки в покое или даже создать новые там, где их не было раньше. Создание такой системы управления, как процесс комментирования нормативных актов, переносит внимание хакеров с целевой системы на систему ее управления, которая должна быть крайне осторожной и гибкой, чтобы самой не стать мягким подбрюшьем для злоумышленников.

18
Хакинг финансовых бирж

Фондовые рынки, товарные биржи и другие финансовые торговые системы тоже давно созрели для взлома. Точнее сказать, они были подарком для хакеров с самого своего появления, но компьютеризация и автоматизация торговли сделали проблему еще более острой.

Хакеры в этой сфере нацелены прежде всего на информацию. Когда финансовая биржа работает так, как надо, трейдеры, располагающие более полной информацией, добиваются лучших результатов, поскольку покупают по низким ценам, а продают на пике. Хакеры подрывают этот механизм двумя основными способами. Во-первых, они используют еще не опубликованную информацию, чтобы заключать выгодные сделки раньше других. Во-вторых, они распространяют дезинформацию, которая движет рынком, а затем заключают прибыльные сделки до того, как все остальные поймут, что их обманули. Оба этих способа подрывают принцип справедливого рынка, который состоит в том, что инвесторы имеют равный доступ к рыночной информации.

Наиболее очевидным взломом первого типа является *инсайдерская торговля* , попавшая под недвусмысленный запрет уже настолько давно, что перестала быть хаком. Как правило, инсайдерская торговля подразумевает покупку или продажу ценной бумаги на основе непубличной информации. Трейдером может быть финансовый директор, который располагает данными о продажах своей компании до их раскрытия, пиарщик, пишущий финансовый отчет, или работник типографии, читающий этот отчет до его публикации. Вред от инсайдерской торговли двоякий: во-первых, осуществляют ее за счет всех остальных участников рынка, не владеющих важной информацией, и, во-вторых, она подрывает доверие к справедливости рыночной системы.

В США инсайдерская торговля была криминализирована в 1934 г. законом о ценных бумагах и биржах, подтвержденным и уточненным на протяжении многих лет решениями Верховного суда США. В 2021 г. три человека были обвинены в инсайдерской торговле[91] за покупку акций компании Long Island Iced Tea Co. незадолго до того, как она сменила название на Long Blockchain Co. без какой-либо иной причины, кроме как желания заработать на ажиотаже вокруг блокчейна. Правило, которое просуществовало так долго,

---

случаях. См.: https://www.occ.treas.gov/about/connect-with-us/public-comments/index-public-comments.html. Consumer Financial Protection Bureau (last updated 7 Apr 2022), «Notice and opportunities to comment,» https://www.consumerfinance.gov/rules-policy/notice-opportunities-comment.

91 US Securities and Exchange Commission (9 Jul 2021), «SEC charges three individuals with insider trading,» https://www.sec.gov/news/press-release/2021-121.

является ярким примером успешного системного патча.

Действительно, то, что эти запреты пережили почти 90 лет хакерских атак и инертности регуляторов, впечатляет. Если из этого и можно извлечь какой-то урок, то он заключается в том, что широкое правило позволяет создать более надежный, адаптируемый и устойчивый режим регулирования. Простота правила сводит к минимуму уязвимости в структуре закона. (Мы видели, насколько оказался уязвимым сложный закон Додда – Франка.) По словам бывшего председателя Комиссии по ценным бумагам и биржам (SEC) Артура Левитта, «высокая конкретизация даст юридическому сообществу различные способы обойти эти особенности. SEC и министерство юстиции специально хотят добиться расплывчатости этих законов[92], чтобы иметь максимальное количество рычагов для возбуждения дел». Правила инсайдерской торговли намеренно расширены, дабы предотвратить дальнейшие попытки подобных взломов системы.

Фронтраннинг , или «забегание вперед», – это еще один хакерский метод, использующий секретную информацию. Если вы брокер и знаете о предстоящей крупной сделке, вы можете перед этим заключить сделку на меньшую сумму. Затем вы исполняете сделку своего клиента, она двигает рынок, и вы получаете мгновенную прибыль. Как и инсайдерская торговля, подобный прием является незаконным.

Некоторые хакерские атаки на финансовые рынки и сети нацелены на окружающие их информационные системы. К примеру, в 2015 г. SEC предъявила обвинения двум украинским хакерам[93], которые взломали сети Business Wire и PR Newswire и похитили более 100 000 неопубликованных пресс-релизов публичных компаний. Релизы были распространены среди сообщества трейдеров, которые использовали полученную информацию, чтобы делать обоснованные ставки, что само по себе весьма напоминает схему инсайдерской торговли.

Второй тип взлома связан с созданием дезинформации. Старый пример – схема под названием Pump & Dump, или «накачка и слив». Преступники покупают акции предпочтительно малоизвестных компаний – в этом контексте печально известен именно рынок грошовых акций. Затем они активно рекомендуют эти акции к покупке, используя ложные и вводящие в заблуждение заявления о потенциальной прибыли. Если другие инвесторы попадаются на эту аферу и начинают покупать, цена на акции взлетает и преступники продают их. Традиционно эта схема включала обзвон потенциальных инвесторов по телефону. Сегодня для этого чаще используются трейдерские форумы, профильные группы в социальных сетях и спам-рассылки по электронной почте. Например, это могут быть лидеры финансового форума r/WallStreetBets на платформе Reddit, спровоцировавшие розничных инвесторов без всякой причины отправить цену акций компании GameStop «на Луну», или же Илон Маск, сообщающий в Twitter о своих покупках биткоинов миллионам подписчиков. В обоих случаях мы имеем дело с инвесторами, использующими онлайн-коммуникации для манипулирования ожиданиями людей и создания ценовых пузырей ради собственной выгоды (и ценой чужих убытков) с беспрецедентной скоростью и в немыслимых доселе масштабах. Появление онлайн-торговли сделало этот хакерский метод еще более прибыльным. По большей части накачка и слив являются незаконными, и если вас поймают, то придется заплатить немалые штрафы. С другой стороны, судебное преследование в этих случаях может быть затруднено. Ни Маск, ни кто-либо, причастный к ажиотажной торговле акциями GameStop в 2021 г., так

---

92 Knowledge at Wharton staff (11 May 2011), «Insider trading 2011: How technology and social networks have 'friended' access to confidential information,» Knowledge at Wharton, https://knowledge.wharton.upenn.edu/article/insider-trading-2011-how-technology-and-social-networks-have-friended-access-to-confidential-information.

93 US Securities and Exchange Commission (11 Aug 2015), «SEC charges 32 defendants in scheme to trade on hacked news releases,» https://www.sec.gov/news/pressrelease/2015-163.html.

и не были привлечены к ответственности.

Спуфинг – вид мошенничества, также связанный с распространением дезинформации. В данном случае трейдер размещает ордера на миллионы долларов, а затем отменяет их после того, как другие трейдеры заметили выставленные заявки и отреагировали на них. Это тоже незаконный метод, и уже несколько человек были осуждены за его использование.

Фейковые новости , то есть намеренно ложные сообщения, маскирующиеся под журналистику, – еще один метод взлома рынка с помощью дезинформации, набирающий все большие обороты. Чаще всего такой взлом используется для искажения оценки стоимости компаний, что позволяет хакерам получать прибыль от колебаний цен на акции. Например, в 2015 г. поддельная версия сайта Bloomberg.com была использована для распространения новости о предложении купить Twitter за $31 млрд, что вызвало резкий рост акций компании по мере распространения информации. Осведомленные хакеры в это же время продавали акции Twitter по искусственно завышенным ценам. Поддельный сайт был оформлен аналогично оригинальному сайту Bloomberg.com и использовал похожий URL. Мы знаем случаи использования поддельных пресс-релизов, поддельных отчетов, поддельных твитов и даже поддельных документов Комиссии по ценным бумагам и биржам США. Все эти действия SEC рассматривает как незаконные.

Если задуматься, дезинформация – это хакинг не столько финансовой сети, сколько других трейдеров. Это попытка повлиять на их поведение, а значит, это уже взлом когнитивных систем.

Большая группа хаков в финансовой сфере связана с поиском новых способов снижения риска, часто с использованием лазеек в финансовых правилах. Хедж-фонды занимаются этим с момента своего появления в 1960-х гг. Сначала они делали это путем *хеджирования* , компенсируя риски друг друга, потом стали прибегать к разнообразным инвестиционным стратегиям, а затем начали сами торговать активами с помощью компьютера.

Само существование хедж-фондов построено на взломе системы финансового регулирования. С момента своего появления хедж-фонды были защищены рядом законодательных лазеек, освобождающих их от надзора Комиссии по ценным бумагам и биржам США. Поскольку они принимают в качестве клиентов только состоятельных и институциональных инвесторов, хедж-фонды освобождены от надзора в соответствии с законом о ценных бумагах 1933 г., который был предназначен для защиты индивидуальных покупателей на рынке. Придерживаясь критериев, изложенных в 1940 г. в законе об инвестиционных компаниях, хедж-фонды освобождают себя от запрета на методы инвестирования, которые применяются к зарегистрированным инвестиционным компаниям, и в первую очередь на открытие коротких позиций. В 2010 г. закон Додда – Франка поставил хедж-фонды под надзор SEC, но на практике они по-прежнему остаются нерегулируемыми. Хедж-фонды – это хак, который стал привычной частью финансовой системы.

На протяжении десятилетий хедж-фонды использовали одну законодательную лазейку за другой. Иногда эти лазейки прикрывают после того, как первопроходцы уже снимут все сливки. Иногда правила меняют таким образом, чтобы узаконить хак. Но в большинстве случаев их просто продолжают использовать и в итоге принимают как норму. Люди, управляющие хедж-фондами, совсем не обязательно умнее остальных. Просто они лучше понимают систему, умеют находить уязвимости и разрабатывать эксплойты, чтобы воспользоваться ими. Поскольку люди, которые лучше всех разбираются в системе, получают прибыль от ее взлома, вряд ли в ближайшее время мы увидим существенные исправления.

Хаки, с которыми мы только что познакомились, направлены против разных систем и работают на разных уровнях. Некоторые из них действуют на техническом уровне: спуфинг и фронтраннинг – это хаки, использующие скорость и автоматизацию, которые рынок получил благодаря компьютерам. Другие действуют на уровне финансовых рынков. Третьи – на законодательном уровне, находя уязвимости, например, в законах о ценных

бумагах. Все это – микрокосм хаков, которые будут описаны в следующих главах.

19
Хакинг компьютеризированных финансовых бирж

Сегодня все финансовые биржи компьютеризированны, и это привело к появлению разнообразных новаторских хаков [94] . К примеру, теперь куда проще реализовать фронтраннинг, а вот обнаружить его стало гораздо труднее. Привязка автоматизированной торговли к анализу рыночных настроений, когда торговые программы покупают акции, становящиеся вдруг очень популярными, или продают их не просто на факте плохих новостей, а на том, что эти новости становятся вирусными, может сделать накачку и слив, а также клеветнические кампании намного более прибыльными. Но самым опасным из всех современных методов биржевого хакинга является *высокочастотный трейдинг* , или ВЧТ. Этот метод эксплуатирует не секреты и ложь, а открытую публичную информацию, но делает это с молниеносной скоростью.

ВЧТ – это форма алгоритмической торговли, которая использует ценовые разрывы, возникающие при размещении крупных торговых ордеров, обычно пенсионными фондами или страховыми компаниями. (Такие ордера могут оказать значительное влияние на цены акций.) Алгоритмы ВЧТ выявляют эти ордера, а также другие события, которые могут повлиять на цены акций, и затем извлекают из них прибыль. Эти сделки называются высокочастотными, потому что пытаются купить дешевле и продать дороже на мизерных колебаниях цен с молниеносной скоростью. Часто вход в сделку и выход из нее проходят за миллисекунды, поэтому алгоритмические трейдинговые компании воюют за место на серверах, физически расположенных близко к биржам, чтобы максимально увеличить скорость. Подобно тому, как собаки могут слышать частоты, слишком высокие для человеческого уха, алгоритмы высокочастотной торговли могут распознавать и реагировать на возникающие модели, слишком мелкие, чтобы люди могли заметить их.

Это чистый хакинг. Если предположить, что цель рынка заключается в том, чтобы покупатели и продавцы обменивались деньгами и товарами по ценам, которые каждый из них считает для себя выгодными, то ВЧТ взламывает это намерение. Если мы считаем, что все участники рынка должны иметь равный доступ к рыночной информации для принятия инвестиционных решений, то ВЧТ – это хак. По сути, ВЧТ использует сверхчеловеческие рефлексы, чтобы зарабатывать по чуть-чуть, но постоянно на случайных колебаниях системы в процессе ее функционирования. ВЧТ – это артефакт компьютерных систем, используемых для облегчения торговли. Он определенно является не предвиденным разработчиками рынка фактором. Он определенно подрывает цели системы ради личной выгоды. И он однозначно является паразитом.

ВЧТ привносит в систему не только присущую ему несправедливость, но, что еще хуже, новые риски и волатильность. В 2010 г. фондовые рынки США стремительно обвалились, потеряв более $1 трлн в течение 36 минут, прежде чем восстановиться. Причина так и не была обнаружена, но масштабы обвала определенно были усугублены ВЧТ. В 2012 г. компания Knight Capital Group потеряла $440 млн из-за уязвимости в новом программном обеспечении, которое управляло ВЧТ. Как показывают эти и другие события, ВЧТ и автономные торговые системы могут быть более рискованными, чем обычная торговля, осуществляемая живыми трейдерами, уже в силу скорости и объема. И, конечно,

---

94 Atlantic Re: think (21 Apr 2015), «The day social media schooled Wall Street,» *Atlantic* , https://www.theatlantic.com/sponsored/etrade-social-stocks/the-day-social-media-schooled-wall-street/327. Jon Bateman (8 Jul 2020), «Deepfakes and synthetic media in the financial system: Assessing threat scenarios,» Carnegie Endowment, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.

ВЧТ явно ставит в невыгодное положение тех, кто не имеет доступа к алгоритмическим торговым системам.

В отличие от большинства хаков, о которых идет речь в этой части книги, и несмотря на свою вопиющую несправедливость, ВЧТ был нормализован. В США Управление по регулированию финансовой индустрии ввело некоторые базовые правила, призванные повысить уровень раскрытия информации о методах, лежащих в основе алгоритмических торговых систем; в ЕС действуют аналогичные правила. Ни те ни другие не делают многого, чтобы замедлить эту практику. На пике развития в 2009–2010 гг. на высокочастотную торговлю приходилось от 60 до 70 % всех торговых операций в США. И хотя частным лицам позволено заключать договоры с ВЧТ-брокерами, чтобы реализовывать свои компьютерные алгоритмы, профессиональные ВЧТ-трейдеры все равно будут делать это быстрее и лучше. Разумеется, в ущерб другим. Несправедливое преимущество ВЧТ-компаний заключается также и в том, что по правилам они могут доплачивать бирже, чтобы видеть отложенные ордера на долю секунды раньше, чем это сможет сделать остальной рынок.

Использование опечаток – еще один рыночный хак, работающий на высоких компьютерных скоростях. Опечатки не являются редкостью в торговле посредством компьютерных систем. Наиболее крупные сбои попадают в новости, такие как случай с японской компанией Mizuho Securities Co., которая потеряла $225 млн на торговле акциями, когда ее сотрудник случайно допустил так называемую ошибку перестановки, разместив на бирже 610 000 акций по 1 иене за штуку вместо одной акции стоимостью 610 000 иен. Или случай, когда младший трейдер Deutsche Bank случайно отправил хедж-фонду $6 млрд в результате так называемой ошибки толстого пальца, задев соседние кнопки ввода. Или когда трейдер на Токийской фондовой бирже потерял акции на сумму $617 млрд, нажав не на ту кнопку и отменив сразу 42 транзакции, – опять проделки «толстого пальца».

Во всех приведенных примерах нет признаков взлома – это просто ошибки. Хакинг начинается, когда намеренно размещают безумные ордера на покупку и продажу в надежде заработать на чужих опечатках. Выставить ордер ничего не стоит, поэтому хак заключается в постоянном наводнении рыночных систем нереалистичными предложениями. Почти все подобные ордера так и остаются неисполненными, но время от времени какой-нибудь из них входит в соответствие с чужой ошибкой, что приводит к получению огромной прибыли.

С хаками в этой сфере понятно, а как насчет защиты? Гибкость финансовых правил означает, что исправления выглядят вполне жизнеспособным решением: финансовые правила намеренно сформулированы широко и оставляют большой простор для действий правоприменителей. Суды и регулирующие органы могут легко и быстро запрещать или регламентировать новую практику, просто перетолковывая или разъясняя существующий закон. Но даже в этом случае способность хакеров нормализовывать свои действия ограничивает эффективность исправлений.

Компьютеризированные финансовые биржи, пожалуй, являются наиболее подходящим местом, где можно развернуть разработку безопасных систем. Мы можем спроектировать наши финансовые системы таким образом, чтобы снизить волатильность, возникающую как следствие высокочастотной торговли. Уже сейчас на многих рынках установлены «автоматические выключатели», которые временно останавливают торги, если цена акций резко изменяется на определенный процент. Но мы можем сделать куда больше в этом направлении. Например, потребовать, чтобы все сделки совершались раз в секунду, или раз в десять секунд, и при этом одновременно. Мы могли бы создать системы обнаружения опасных ордеров ВЧТ и либо задерживать их исполнение, либо полностью отменять. Но любые конструктивные изменения требуют от регуляторов идти против воли влиятельных инвесторов. После тезисов Мартина Лютера потребовалось 50 лет на то, чтобы папа Пий V смог переделать систему индульгенций. Конечно, нам не придется ждать так долго.

20
Хакинг и элитная недвижимость

В Лондоне, Нью-Йорке, Ванкувере и других крупных городах мира рынок элитной недвижимости ведет себя не так, как раньше. Речь идет не о богатых людях, покупающих себе дома, пусть даже вторые и третьи. Речь идет о машине для отмывания денег.

Вот как она работает. Если у вас имеются миллионы теневых долларов (или рублей), вы не можете просто так положить их на расчетный или инвестиционный счет. Правительство требует от финансовых учреждений проявлять любопытство, задавать вам кучу разных вопросов и подавать отчет о подозрительной деятельности, если ваши ответы вызывают сомнения. Но одна лазейка для теневого капитала все-таки есть, и это недвижимость. Во многих странах правила, регулирующие покупку недвижимости, не столь обременительны, как правила банков и финансовых рынков. Банки обязаны проверять клиентов, чтобы предотвратить мошенничество и отмывание денег, но это не распространяется на подставные иностранные корпорации, которые участвуют в сделках с недвижимостью. Брокеры и продавцы не задают вопросов о родословной вашей наличности, потому что правительство не требует этого. Как только вы заметили уязвимость, хак становится очевидным.

Сначала вы покупаете супердорогую квартиру в городе, где не собираетесь жить. Вы совершаете покупку через подставную компанию, чтобы скрыть свое личное участие (технически это называется «бенефициарное владение»). Затем вы используете купленную недвижимость в качестве залога для получения банковских кредитов. Деньги, которые вы занимаете, чисты перед законом, а значит, можно инвестировать их одним из традиционных способов, на фондовом рынке или как-то иначе, не нарушая правил этих систем. При этом вам все равно, будет квартира дорожать или нет, поскольку вы купили ее с иной целью. Тем не менее, если цены вырастут, это будет неплохо, так как появится больше возможностей для заимствования. Вы также не сдаете недвижимость в аренду, поскольку это обесценивает ее, какими бы хорошими ни оказались ваши арендаторы.

Именно так Андрей Бородин, бежавший из России по обвинению в мошеннических действиях с собственным банком, стал владельцем лондонской квартиры стоимостью 140 млн фунтов стерлингов. И он явно не одинок. В отчете Transparency International за 2015 г. сказано, что в Великобритании было выявлено 160 объектов недвижимости[95] общей стоимостью 4,4 млрд фунтов стерлингов, которые принадлежат «лицам с высоким уровнем коррупционного риска». В таких городах, как Нью-Йорк и Майами, полно незанятых роскошных кондоминиумов. В 2014 г. газета *The New York Times* провела журналистское расследование на примере одного из элитных домов, в котором 80 % квартир оказались принадлежащими подставным фирмам[96].

Этот трюк работает, даже если вы не пытаетесь отмыть «грязные» деньги. Недвижимость по-прежнему является хорошим способом сберечь свои средства и приобрести залог, а растущие цены на нее все еще увеличивают возможности владельцев брать кредиты.

Это объясняет странную на первый взгляд особенность рынка элитной недвижимости: почему так много продавцов предпочитают не продавать свои объекты вместо того, чтобы снизить запрашиваемую цену до разумной рыночной. До тех пор, пока нет фактической

---

95 Matteo de Simone et al. (Mar 2015), «Corruption on your doorstep: How corrupt capital is used to buy property in the U.K.,» Transparency International, https://www.transparency.org.uk/sites/default/files/pdf/publications/2016CorruptionOnYourDoorstepWeb.pdf.

96 Louise Story and Stephanie Saul (7 Feb 2015), «Stream of foreign wealth flows to elite New York real estate,» *The New York Times*, https://www.nytimes.com/2015/02/08/nyregion/stream-of-foreign-wealth-flows-to-time-warner-condos.html.

продажи по более низкой цене, актив не должен обесцениваться. Практически все, кто занимается элитной недвижимостью, предпочитают такой исход.

Это наносит прямой ущерб людям, которые просто хотят жить в районах, где практикуются такие схемы. Это также разрушает рынок коммерческой недвижимости в подобных районах, поскольку здесь заметно меньше людей. Розничные магазины в таких районах, как лондонский Мейфэр, были вынуждены закрыться, потому что 30 % квартир пустуют из-за офшорных отмывателей денег.

Исправления в данном случае столь же очевидны, как и сама уязвимость: нормативные изменения, которые приведут рынок недвижимости в соответствие с другими финансовыми системами. В 2016 г. министерство финансов США реализовало пилотную программу в 12 городах[97], требующую, чтобы LLC (форма собственности, соответствующая российскому ООО) раскрывали своих бенефициарных владельцев при их создании. Это привело к 70 %-ному снижению объемов покупок недвижимости такими компаниями за наличные. Подобное требование можно сделать постоянным и общенациональным. Фактически, программа недавно была возобновлена и расширена, чтобы охватить новые рынки недвижимости. Федеральное правительство могло бы распространить банковское правило «Знай своего клиента» на бенефициаров подставных компаний. Кроме того, правительству явно пора изменить «временное» правило[98], введенное лоббистами в федеральный закон 2001 г. о сдерживании террористических актов, согласно которому покупатели недвижимости освобождаются от детальной проверки.

Однако политического желания что-то менять в этой сфере пока не наблюдается, разве что конфликт России с Украиной может немного сдвинуть ситуацию в Великобритании. Причина инертности – провластные интересы. Существует целый ряд отраслей – девелопмент, строительство и т. д., – которые получают выгоду от нерегулируемой продажи элитной недвижимости. И мало кто из власть имущих выиграет от таких перемен. На другой чаше весов – увеличение налоговых поступлений, повышение доступности жилья, увеличение площади жилого фонда и сокращение возможностей для отмывания денег. Иными словами, все то, чего хотят остальные.

Сегодня отмывание денег через недвижимость – это настолько обыденное дело, что его уже трудно назвать хаком. То же самое можно сказать и о предметах искусства. Существует хак, который заключается в том, чтобы купить произведение искусства по дешевке, завысить его стоимость при оценке, а затем передать его в дар музею, чтобы списать налоги. При этом обществу, которое недосчиталось налоговых поступлений, наносится вред.

21
Нормализация социальных хаков

Думая о хакинге, мы часто представляем себе, что хаки быстро блокируются разработчиками системы, которые исправляют ее уязвимости. Это то, что обычно происходит с компьютерными взломами. Я пишу эти строки в мае 2022 г., и вот три уязвимости, информация о которых недавно появилась в прессе.

● Cisco объявила о многочисленных уязвимостях[99] в своем программном обеспечении

---

97 Michael T. Gershberg, Janice Mac Avoy, and Gregory Bernstein (2 May 2022), «FinCEN renews and expands geographic targeting orders for residential real estate deals,» *Lexology* , https://www.lexology.com/library/detail.aspx?g=065ffb4d-f737-42dc-b759-ef5c4d010404.

98 Max de Haldevang (22 Jun 2019), «The surprisingly effective pilot program stopping real estate money laundering in the US,» *Quartz* , https://qz.com/1635394/how-the-us-can-stop-real-estate-money-laundering.

99 Michael Cooney (5 May 2022), «Cisco warns of critical vulnerability in virtualized network software,» *Network World* ,

для Enterprise NFV Infrastructure Software. Одна из уязвимостей могла позволить злоумышленнику перейти с гостевой виртуальной машины на хост-компьютер и тем самым поставить под угрозу все сетевые хосты.

● Компания F5, специализирующаяся на безопасности облачных вычислений, предупредила своих клиентов[100] о 43 уязвимостях, затрагивающих четыре ее продукта. Одна из них «могла позволить неавторизованному злоумышленнику с сетевым доступом к системе BIG-IP через порт управления и/или собственные IP-адреса выполнять произвольные системные команды, создавать или удалять файлы или отключать службы».

● Корпорация AVG сообщила об обнаружении[101] двух серьезных уязвимостей в своих антивирусных продуктах, которые скрывались в коде с 2012 г. Обе уязвимости могли позволить злоумышленникам отключать защитное программное обеспечение или вмешиваться в работу операционной системы клиента.

В каждом из этих случаев уязвимость обнаруживали либо сами производители, либо исследователи, которые в частном порядке сообщали о ней разработчикам системы, те в свою очередь вносили исправления, и только после этого информация раскрывалась, а вместе с ней и тот факт, что система больше не уязвима.

В компьютерной безопасности для подобных случаев у нас есть термин – «ответственное раскрытие информации». Противоположную ситуацию описывает другой термин – «уязвимость нулевого дня». Это такая уязвимость, которая тайно обнаруживается преступниками, правительствами или хакерами, которые продают информацию о ней преступникам или правительствам. При этом организация, отвечающая за систему, ничего не знает об уязвимости до тех пор, пока не обнаружит реально функционирующий на ней эксплойт. В таких случаях предупреждений не может быть в принципе.

Ни в одном из хаков, которые мы обсуждали в предыдущих главах, ни в большинстве других примеров, приведенных в этой книге, не было ответственного раскрытия информации. Для некомпьютерных систем это норма. Когда менеджер хедж-фонда обнаруживает возможность выгодного взлома финансовой системы, он не предупреждает регулирующий орган, чтобы тот внес исправления. Он использует его в своих интересах до тех пор, пока правительственный орган сам не заставит его прекратить это делать.

Вот как выглядит процесс в целом. Сначала обнаруживается уязвимость, которая позволяет хакнуть систему посредством эксплойта. Постепенно хак становится все более популярным. Это может происходить медленнее или быстрее в зависимости от типа самого хака, от того, что именно он делает, насколько прибыльным может быть, от распространенности взламываемой системы, от скорости распространения информации о хаке и т. д. В какой-то момент управляющий орган системы узнает о взломе и может отреагировать одним из двух способов. Во-первых, он может изменить правила системы, чтобы предотвратить хак, поставив системный патч. Во-вторых, он может внедрить хак в систему, по сути нормализовав его. После такой нормализации хак иногда умирает естественной смертью, поскольку все начинают его копировать и всякое конкурентное преимущество теряется.

История финансового хакинга – это история нормализации хаков[102]. Кто-то изобретает

---

https://www.networkworld.com/article/3659872/cisco-warns-of-critical-vulnerability-in-virtualized-network-software.html.

[100] Harold Bell (5 May 2022), «F5 warns of BIG-IP iControl REST vulnerability,» *Security Boulevard* , https://securityboulevard.com/2022/05/f5-warns-of-big-ip-icontrol-rest-vulnerability.

[101] Charlie Osborne (5 May 2022), «Decade-old bugs discovered in Avast, AVG antivirus software,» *ZD Net* , https://www.zdnet.com/article/decade-old-bugs-discovered-in-avast-avg-antivirus-software.

[102] Я мог написать то же самое об индексных фондах. Annie Lowrey (Apr 2021), «Could index funds be 'worse than Marxism'?» Atlantic, https://www.theatlantic.com/ideas/archive/2021/04/the-autopilot-economy/618497.

хак и зарабатывает огромные деньги. Другие копируют его действия и тоже получают прибыль. Затем регуляторы замечают взлом и вмешиваются. Иногда они объявляют хакинг незаконным и осуждают хакеров, но чаще всего задним числом они одобряют хаки. В этот момент хаки перестают быть таковыми и становятся нормальной частью финансовой деятельности. Процесс нормализации не всегда происходит преднамеренно. Как и в случае с хедж-фондами, некоторые взломы просто игнорируются системой и в результате ее бездействия пассивно нормализуются.

Это может иметь положительные последствия, как в случаях с NOW-счетами и депозитными сертификатами, которые стали настоящими инновациями в финансах, но у всего есть цена. Многие хаки, описанные в предыдущих главах, нарушают принцип справедливости рынка, нацеливаясь на информацию, право выбора или свободу действий. Такие хаки не столько инновационные, сколько подрывные. Их нормализация свидетельствует лишь о том, что богатые люди имеют возможность добиваться своего за счет всех остальных.

Нормализация – явление не новое [103], так же как и игра в кошки-мышки между хакерами и регуляторами. В Средние века и католические, и светские власти вводили строгие ограничения на процентные займы, поскольку они считались греховными. По мере развития банковского дела как профессии богатые банкиры начали обходить эти ограничения с помощью все более изощренных методов. К ним относились фальсификация учетных книг, ошибочная классификация запрещенной ростовщической ссуды как разрешенной, а также маскировка процентов по этой ссуде под подарки ростовщику от заемщика. Одним из хаков того времени был «сухой морской заем», который превращал запрещенный заем в разрешенный, связывая его с произвольным морским путешествием.

Реакция на эти средневековые ростовщические хаки перекликается со всем, о чем говорилось выше. В период с XII по XIV в. католическая церковь обновила свои правила ростовщичества для борьбы с финансовыми инновациями, такими как «сухой морской заем», создала более сложные механизмы обеспечения правоприменения и ужесточила наказания для осужденных ростовщиков. Но состоятельные люди и тогда умели защищать свои источники прибыли. Богатые гильдии обладали ресурсами и опытом для создания таких финансовых продуктов, которые успешно ускользали из-под церковного контроля. И постепенно возникла новая форма захвата регулятора, когда церковь принимала пожертвования и финансовую реституцию от нарушителей, стимулируя развитие ростовщичества. По сути, современное банковское дело зародилось в 1517 г. на Пятом Латеранском соборе, где произошла нормализация выгодного системе хака. Если вы хоть раз брали ипотеку, финансировали обучение или начинали бизнес с помощью кредита, вы должны быть благодарны за эту нормализацию хака. (Собор также легализовал ломбарды – на случай, если вам доводилось прибегать к услугам и этой системы.)

Сегодня нормализация кажется обычным явлением. Я уверен, что большинство хаков высокочастотной торговли были бы признаны незаконными, появись они 100 лет назад. И я также уверен, что инсайдерская торговля, возникни она в последние десятилетия, была бы сегодня вполне законной.

22
Хакинг и рынок

С 2010 по 2014 г. Goldman Sachs владела компанией, специализирующейся на хранении алюминия, которой принадлежали 27 промышленных складов в районе Детройта.

---

[103] Robert Sabatino Lopez and Irving W. Raymond (2001), Medieval Trade in the Mediterranean World: Illustrative Documents, Columbia University Press.

По нескольку раз в день грузовики перевозили[104] 700-килограммовые слитки металла между складами, загружая их на одном и разгружая на другом. И так каждый день.

Определенно, это был хак. Расчет спотовой цены на алюминий частично зависит от того, сколько времени приходится ждать покупателям между покупкой товара и его доставкой. Эта постоянная перетасовка алюминия влияла на цену, а поскольку на этих 27 складах хранилось более четверти алюминиевого запаса страны, юридические танцы Goldman Sachs позволяли ей манипулировать ценой в своих интересах.

Это хак, который явно недоступен людям, не обладающим богатствами Goldman Sachs. Деньги – это то, что делает рыночную экономику пригодной для хакинга, и именно богатые извлекают из этого выгоду.

Хакеры рынка используют уязвимости, возникающие в процессе производства и продажи товаров и услуг, то есть в рамках стандартной логики спроса и предложения, потребительского выбора, того, как бизнес выходит на рынок, уходит с него и какие виды продукции предлагает в первую очередь.

Рыночный капитализм, свободный рынок – это экономическая система с уникальными преимуществами по сравнению с торговой системой, которую он собой заменил. В отличие от систем централизованного планирования, таких как коммунизм, рыночный капитализм не контролируется какой-либо одной организацией. Люди принимают индивидуальные решения в собственных интересах, капитал течет туда, где его можно использовать с наибольшей прибылью, и из этого хаоса возникает эффективный рынок. По крайней мере, в идеальном мире.

Фундаментальный механизм, который заставляет все это работать, – это заинтересованные покупатели, принимающие разумные решения среди конкурирующих продавцов. Правила рынка предназначены для поддержания функционирования этого основного механизма и предотвращения нанесения системе большего ущерба. К ним относятся законы, которые вы ожидаете увидеть, например запрет на недобросовестные торговые методы и небезопасные условия труда, а также законы, о которых вы, возможно, подумали не сразу, регулирующие исполнение контрактов, национальную валюту, гражданские суды для разрешения споров и т. д.

Для успешной работы рынкам необходимы три вещи: информация, выбор и свобода действий. Покупателям нужна информация о товарах и услугах, чтобы принимать разумные решения о покупке, они должны понимать достоинства и недостатки, иметь возможность сравнивать цены, технические характеристики и т. д. У покупателей должен быть выбор между несколькими продавцами, иначе не будет конкуренции, которая контролирует цены и стимулирует инновации. И точно так же покупателям необходима свобода действий, чтобы использовать свои знания о продавцах, товарах и услугах и выбирать между ними. Все эти три элемента рынка были успешно взломаны.

● Намеренно сложные формулировки товарных предложений затуманивают информацию. Попробуйте, например, сравнить цены на тарифы сотовой связи, кредитные карты или проспекты акций. Неясность и, как следствие, путаница затрудняют разумный выбор между альтернативами. В какой-то степени это является следствием естественной сложности нашего высокотехнологичного мира, но во многом это преднамеренный взлом, призванный затруднить доступ пользователей к точной информации.

● Монополии устраняют возможность выбора. Монополии как таковые существовали и до капитализма, но тогда они не были хаком. В рыночной же системе, состоящей из продавцов, конкурирующих за покупателей, монополии подрывают сам механизм рынка. Адам Смит писал об этом в 1776 г., объясняя, что экономические интересы бизнеса часто

---

[104] David Kocieniewski (20 Jun 2013), «A shuffle of aluminum, but to banks, pure gold,» *The New York Times* , https://www.nytimes.com/2013/07/21/business/a-shuffle-of-aluminum-but-to-banks-pure-gold.html.

не совпадают с интересами общественными[105]. Целью бизнесменов и их коммерческих предприятий является максимизация прибыли. Целью общества в большей или меньшей степени является максимизация количества, качества, разнообразия и инновационности продуктов, а также минимизация цен. Отсутствие конкуренции означает, что продавцы больше не боятся потерять покупателей, а значит, у них нет стимула предоставлять то, чего хочет общество.

● Блокировка ограничивает свободу выбора между конкурирующими продуктами. Сегодня вы пьете кока-колу, а если она вам разонравится, то завтра можете выпить пепси. Но если по какой-то причине вы сегодня остались недовольны тарифным планом мобильного оператора, провайдером электронной почты или своей кредитной картой, то, скорее всего, завтра вы все равно продолжите пользоваться тем же тарифным планом, электронной почтой и кредитной картой. Просто стоимость перехода в этих случаях, выраженная в деньгах, времени, удобстве или обучении, будет выше. Это и есть блокировка. А хакинг здесь связан с различными способами обеспечения такой блокировки. Запатентованные форматы файлов, которые значительно удорожают переход на новый аудиоплеер или устройство для чтения электронных книг; настройки, намеренно затрудняющие возможность смены бизнес-приложений; социальные сети, которые лишат вас доступа к аккаунтам друзей, если вы удалите свой собственный; приложения, которые не позволят вам стереть свои данные, когда вы их удаляете со своих устройств.

Результатом этого является увеличение прибыли компаний за наш счет путем взлома рыночной системы.

Для ограничения этих провалов рынка может быть использовано регулирование. Дерегулирование по своей природе устраняет препятствия для хаков, по сути одобряя их, прежде чем кто-либо сможет увидеть их в действии. Это и хорошо, и плохо. Хорошо тем, что инновации могут быть внедрены быстро. Плохо тем, что так же быстро можно внедрить диверсию.

Исторически, по крайней мере в США, мы отдавали приоритет инновациям и минимизации структуры регулирования, которая позволяет их внедрять. В основном такой подход работал в силу того, что объем ущерба, который могли нанести злонамеренные хаки, был ограничен. Сегодня, благодаря возросшей мощи технологий и глобальному характеру экономики, ситуация изменилась. Экономическая система, основанная на жадности и корысти, работает лишь тогда, когда эти свойства не могут ее разрушить, а «двигаться быстро и ломать преграды» – знаменитый девиз Марка Цукерберга – это нормально только в том случае, если вы подвергаете риску то, что принадлежит вам самим. Если речь идет о чужом имуществе, то, возможно, вам стоит дважды подумать, или же вас заставят чинить поломанное.

23
«Слишком большой, чтобы обанкротиться»

Расхожая фраза «слишком большой, чтобы обанкротиться» отражает критическую уязвимость нашей рыночной экономики. Если вы настолько велики, что ваш крах представляет собой системный риск для экономики, вы можете спокойно идти на большие риски, поскольку знаете, что вам не позволят обанкротиться. Эта идея отражена в словах, которые часто приписывают Жану Полу Гетти (хотя, вероятно, впервые их произнес Джон Мейнард Кейнс[106]): «Если вы должны банку 100 долларов, это ваша проблема. Если вы

---

105 Смит А. Исследование о природе и причинах богатства народов. – М.: Эксмо, 2016. Adam Smith (1776), The Wealth of Nations, William Strahan.

106 Жан Пол Гетти (1892–1976) – американский нефтяной магнат и промышленник, считавшийся в 1950–1970-х гг. самым богатым человеком в мире. Стал известен крайней скупостью, отказавшись платить

должны банку 100 миллионов долларов, это проблема банка». В этом и состоит смысл выражения «слишком большой, чтобы обанкротиться».

Некоторые корпорации слишком важны для функционирования нашей экономики, чтобы допустить их банкротство. Они стали настолько большими и важными, что, даже если вдруг начинают приносить серьезные убытки, правительству дешевле выручить их, чем позволить обанкротиться.

Напомним, что основной механизм рынка – это конкуренция продавцов за покупателей: успешные продавцы процветают, а неудачники уходят с рынка. Представьте себе обычного бизнесмена или организацию, обдумывающую рискованный шаг. Они должны взвесить выгоды, которые получат при успешной реализации своего плана, и убытки, которые понесут в случае неудачи, а конечное решение будет учитывать и то и другое. Однако директора компании, считающейся слишком важной, чтобы обанкротиться, знают, что любые убытки от их неверных решений будут оплачены налогоплательщиками, то есть обществом в целом. Это создает моральный риск и стимулирует принятие рискованных, необдуманных решений. Если они добьются успеха, то окажутся в выигрыше. Если же потерпят неудачу, то будут защищены от потерь. «Слишком большой, чтобы обанкротиться» – это страховка от неудачных ставок. Она вносит перекос в нашу рыночную систему. Это искажение, подпитываемое деньгами и властью. И, конечно, это хакинг.

В результате финансового кризиса 2008 г. правительство США взяло на поруки несколько крупных банков Уолл-стрит и других финансовых учреждений после того, как их руководители в течение многих лет принимали неверные бизнес-решения. Это было сделано через Программу помощи проблемным активам, которая уполномочила правительство покупать активы и акции компаний, оказавшихся в тяжелом положении, включая ценные бумаги, обеспеченные ипотекой. Считалось, что помощь в размере $700 млрд необходима для защиты экономики США в целом. Опасения состояли в том, что без такой помощи экономика рухнет, а это бы стоило правительству уже гораздо больше, чем $700 млрд, поскольку пришлось бы оплачивать государственные программы помощи пропорционально степени тяжести рецессии. (Во время экономического спада доходы государства снижаются, поскольку люди зарабатывают меньше и платят меньше налогов, а вот расходы государства, наоборот, увеличиваются, к примеру на такие программы, как страховые выплаты по безработице. Короче говоря, чем тяжелее рецессии, тем они дороже обходятся государству.)

Это не первый случай, когда правительство США берется помогать компаниям «слишком большим, чтобы обанкротиться». Федеральная корпорация по страхованию вкладов была создана в 1930-х гг. после лавины банкротств среди банков, чтобы осуществлять надзор и защищать вклады клиентов. В 1979 г. правительство взяло под крыло корпорацию Chrysler. Помощь была небольшой по сравнению с 2008 г., всего $1,5 млрд, но основания для нее были аналогичными. Правительство ссылалось на интересы национальной безопасности, поскольку дело было в разгар холодной войны, а компания готовилась к выпуску танка M1 Abrams. Правительство ссылалось на экономику, так как было необходимо сохранить 700 000 рабочих мест в Детройте и за его пределами. Кроме того, автопромышленность США находилась в состоянии торговой войны с Японией. Программа спасения Chrysler оказалась успешной: автогигант вернул кредит досрочно и с процентами.

Хак «слишком большой, чтобы обанкротиться», по существу, является результатом изменения модели угроз. Когда были изобретены механизмы рыночной экономики, ни один бизнес не мог быть настолько критичным для всей экономики в целом, что его крах потребовал бы вмешательства государства. Отчасти это объяснялось размерами частных компаний, но также и тем, что критически важные социальные функции не были

выкуп за своего похищенного 16-летнего внука. Джон Мейнард Кейнс (1883–1946) – британский экономист, основатель кейнсианского направления в экономической науке. – *Прим. пер* .

приватизированы. Конечно, компании могли расти, но ни одна из них не могла вырасти до сегодняшних масштабов. Подобный рост требует современных технологий.

Попытки регулировать корпоративных гигантов в лучшем случае оказывались вялыми, в основном из-за сильного лобби этих компаний, которые традиционно сопротивляются государственному надзору. Банковские реформы Додда – Франка 2010 г. ослабили угрозу, исходящую от «слишком больших, чтобы обанкротиться» предприятий, но утратили большую часть своей силы после прохождения законопроекта через конгресс или были сведены на нет более поздним законом о налоговой реформе.

Один из способов защититься от хака под названием «слишком большой, чтобы обанкротиться» – это отказ от прямого спасения мегакорпораций. В 2008 г. у правительства США было как минимум еще два варианта действий. Оно могло обусловить любую помощь реструктуризацией ипотечных кредитов, чтобы устранить волну дефолтов. И могло выручить крупные банки только в том случае, если они передадут деньги заемщикам. Оба варианта были отклонены тогдашним директором Национального экономического совета Ларри Саммерсом. Спасение банков 2008 г. служит еще одним примером того, как богатство защищает хакинг, используемый сильными мира сего.

Самый эффективный способ обезопасить экономическую систему от компаний, которые слишком велики, чтобы обанкротиться, – сделать так, чтобы их вообще не было. В 2009 г. социолог Дункан Уоттс назвал свое эссе «Слишком большие, чтобы обанкротиться? А как насчет "Слишком большие, чтобы существовать?"». В нем он утверждал, что некоторые компании настолько велики и могущественны, что могут эффективно манипулировать правительством и использовать его в качестве страховки при принятии рискованных бизнес-решений, перекладывая свой груз на плечи налогоплательщиков.

Хаки, подобные этим, иллюстрируют три важных момента, к которым мы еще вернемся позже. Во-первых, понятие «слишком большой, чтобы обанкротиться» является обобщающим. По мере того как крупные банки, агентства недвижимости и компании из других важных секторов экономики осознают, что могут использовать этот хак, рыночная экономика в целом становится уязвимой для предприятий, которые расширяются неустойчиво. Во-вторых, хаки могут быть систематизированы и встроены в процесс принятия решений: меры по спасению банков в 2008 г. были закреплены в законе. Продемонстрировав, что федеральное правительство готово выручить банковский сектор, сектор недвижимости и автомобильную промышленность, конгресс нормализовал этот хак как часть финансовой игры с высокими ставками. И в-третьих, сама концепция «слишком большой, чтобы обанкротиться» меняет стимулы тех, кто регулирует деятельность крупных организаций, а следовательно, и сами организации.

Сегодня, и это факт, мегакорпорации рассматривают хак «слишком большой, чтобы обанкротиться» как свою главную страховку. Конечно, те немногие организации, которым спасение через закон Додда – Франка было гарантировано напрямую, – Citigroup, JPMorgan Chase, Bank of America и Goldman Sachs – знают, что правительство снова выручит их в случае необходимости[107]. Это хак, который стал нормой несмотря на то, что наносит колоссальный вред рыночной экономике.

24
Венчурный капитал и прямые инвестиции

Приложения для доставки еды основаны на неустойчивой бизнес-модели. В 2020 г.,

---

[107] Michael Greenberger (Jun 2018), «Too big to fail U.S. banks' regulatory alchemy: Converting an obscure agency footnote into an 'at will' nullification of Dodd-Frank's regulation of the multi-trillion dollar financial swaps market,» Institute for New Economic Thinking, https://www.ineteconomics.org/uploads/papers/WP_74.pdf.

когда пандемия накрыла мир и большинство людей сидело по домам, DoorDash потеряла $139 млн, а Grubhub – $156 млн. Трудно найти цифры отдельно по Uber Eats, но сама компания Uber потеряла $6,8 млрд – и это лучше, чем ее убыток в $8,5 млрд, который она понесла в 2019 г. Для индивидуальных инвесторов это тоже неустойчивые инвестиции, ведь доставка еды, по сути, не выгодна никому. Водители – фрилансеры без льгот и гарантий занятости – получают мало. Ресторанному бизнесу доставка еды тоже больше вредит, чем помогает: дополнительных продаж она не приносит, а от ошибок доставщиков страдает репутация ресторана. Даже для клиентов это не настолько полезная услуга, как может показаться на первый взгляд: им приходится платить больше и при этом постоянно сталкиваться с задержками и другими проблемами, возникающими в процессе доставки. Единственная причина существования этого рынка заключается в том, что венчурные компании, такие как SoftBank, готовы вливать в него десятки миллиардов долларов, надеясь, что когда-нибудь смогут отбить их и получить собственную прибыль. Такая инвестиционная стратегия является хаком. Мы ожидаем от рыночного капитализма, что он должен использовать нескоординированный коллективный разум покупателей для воздействия на продавцов. Однако венчурное финансирование препятствует этому, подавляя активность и самостоятельность покупателей.

История венчурного капитала как модели финансирования насчитывает сотни лет, но по-настоящему он расцвел только в 1980-х гг. Он стал ключевым игроком в подъеме первых высокотехнологичных компаний, а также сыграл основную роль в надувании пузыря доткомов в 2001 г. С тех пор мировой рынок венчурного капитала неуклонно растет: в 2010 г. он составлял $50 млрд, а в 2019 г. – уже $295 млрд. Я и сам извлек выгоду на этом рынке, продав свою первую компанию с венчурным капиталом компании BT в 2006 г., а вторую – компании IBM в 2016 г.

Венчурный капитал сам по себе не является хаком. Хак возникает тогда, когда убыточные компании используют венчурное финансирование, чтобы игнорировать динамику рыночной экономики. Мы не хотим, чтобы некий единый планировщик решал[108], какие предприятия должны продолжать работать, а какие следует закрыть. Но именно это и происходит, когда в дело вступают венчурные фирмы. Вливание венчурных денег означает, что компаниям не нужно конкурировать друг с другом традиционным способом или беспокоиться о законах спроса и предложения. Они могут делать то, что в обычных условиях еще недавно считалось чистым безумием: отдавать свою продукцию даром, платить непомерные зарплаты, нести огромные финансовые потери, предоставлять услуги, которые на самом деле вредят людям. И все это благодаря внешнему источнику финансирования под названием венчурный капитал. По сути, мы имеем дело с централизованным планированием со стороны элитных инвесторов. Если бы то же самое делало правительство, это было бы названо коммунизмом.

С момента своего основания в 2009 г. компания Uber получила $25,5 млрд в виде венчурного финансирования. За всю историю существования у компании не было ни одного прибыльного года. В 2019 г. компания потеряла $8,5 млрд, или по 58 центов на каждой из 5,2 млрд поездок, совершенных ее клиентами по всему миру. Единственная причина, по которой Uber вообще существует, состоит в том, что инвесторы все еще готовы вливать капитал в эту воронку, вероятно ожидая того момента, когда технология беспилотных автомобилей позволит компании уволить всех своих водителей и управлять полностью автономным парком.

WeWork[109] тоже никогда не видела прибыли, потеряв за три года более $10 млрд.

---

[108] Eric Levitz (3 Dec 2020), "America has central planners. We just call them 'venture capitalists,' " *New York Magazine* , https://nymag.com/intelligencer/2020/12/wework-venture-capital-central-planning.html.

[109] WeWork – компания, созданная Адамом Нейманом под перепрофилирование излишков офисных помещений в коворкинги. – *Прим. ред* .

Этот пузырь, надутый венчурными инвесторами, лопнул, когда компания попыталась выйти на биржу в 2019 г. и не смогла этого сделать. Правила работы на дому из-за COVID-19 еще больше подорвали шансы WeWork на успех, и соучредитель компании был уволен с поста генерального директора и председателя совета директоров. Единственная причина, по которой WeWork смогла вырасти настолько большой, заключается в том, что она привлекла $12,8 млрд венчурного финансирования за период с момента своего основания в 2010 г. до лета 2019 г., и еще миллиарды долларов в качестве списания долгов.

Эти примеры не тождественны ни плохим, ни мошенническим инвестициям. Quibi, платформа для потоковой передачи короткометражного контента на мобильные телефоны, получила более $1,75 млрд венчурного финансирования, но закрылась всего через шесть месяцев после запуска – после того, как прогноз по числу подписчиков не оправдался. Элизабет Холмс благодаря венчурному капиталу основала компанию Theranos [110] и управляла ею, так и не создав ни одного успешного продукта, а в итоге за несколько лет надула инвесторов на сумму $1 млрд. Оба этих примера иллюстрируют нормальную работу сегодняшнего рынка, хотя покупатели – в данном случае инвесторы – принимали неверные решения о покупке, а в случае с Theranos имело место откровенное мошенничество.

Система венчурных инвестиций подрывает рыночный капитализм во многих отношениях. Она негативно влияет на рынки, позволяя компаниям устанавливать цены, которые не отражают реальную стоимость или ценность того, что они продают. Она позволяет процветать убыточным предприятиям и распространяться неустойчивым бизнес-моделям. Она также влияет на рынок талантов, особенно в технологическом секторе. И, наконец, она деформирует целые категории рынка, такие как транспорт, жилье и СМИ. К примеру, компании Uber и Lyft создали неустойчивый рынок поездок на арендованных автомобилях, устанавливая искусственно заниженные цены, которые искажают стоимость труда водителей.

Финансирование венчурными фондами – это еще и удар по инновациям. Предпочитая финансовую прибыль существенным улучшениям продукта, оно отдает приоритет одним видам инноваций и игнорирует другие. Для компании, финансируемой венчурным фондом, важна лишь прибыль на вложенный капитал. Поэтому если полагать стимулирование инноваций одной из целей рыночной экономики, то венчурное финансирование подрывает эту цель. Венчурные инвесторы рассчитывают вернуть свои инвестиции за десять лет или меньше и управляют своими компаниями, отталкиваясь от этого.

Кроме того, сама культура венчурного финансирования поощряет лишь те начинания, которые приносят высокую прибыль. Инвесторы финансируют сотни компаний с различными идеями и бизнес-моделями, зная, что почти все они потерпят крах, но несколько удачных проектов с лихвой окупят все остальные. Поэтому менеджеры компаний, финансируемых за счет венчурного капитала, мотивированы скорее на то, чтобы по-быстрому снимать сливки, чем на развитие устойчивого, долгосрочного бизнеса. Вот почему компании, финансируемые венчурными фондами, могут нести такие большие убытки, нанося при этом ущерб обществу. Эти убытки оплачиваются единичными историями успеха, которые с легкой руки венчурных инвесторов теперь называют «единорогами».

Частный капитал позволяет использовать еще один вид хакинга, а именно долговое финансирование. Когда частные инвестиционные компании приобретают контрольный пакет акций с целью выкупить предприятие, они могут вкладывать собственный капитал лишь частично, полагаясь на долговое финансирование. Такая схема часто используется для того, чтобы обременять приобретаемые компании долгами, вытягивать из них деньги, нагружать новыми долгами, а затем продавать с прибылью, оставляя кредиторов ни с чем. Рассмотрим

---

[110] Theranos – американская технологическая корпорация в области медицинских услуг по лабораторному экспресс-анализу крови. – *Прим. ред* .

случай с компанией Greensill Capital[111], которая потерпела крах в 2021 г. Ее неустойчивый рост в течение 10 лет – от стартапа по финансированию цепочки поставок до транснационального посредника с долгом в $4,6 млн и последующего банкротства – был ускорен инвестициями и кредитами от SoftBank, который предоставлял миллионные средства, несмотря на все более сомнительную отчетность компании.

Во всем этом нет ничего противозаконного. Венчурные инвесторы и фонды прямых инвестиций являются настолько обыденной частью сегодняшней экономики, что может показаться странным, когда кто-то называет их хакерами. Но хакинг – это именно то, чем они занимаются, взламывая практически все устои свободного рынка. При этом вы не услышите слова «хакинг» в связи с их деятельностью, которую принято расплывчато называть «инновационной». То, что это законно и общепринято, не меняет простого факта: именно деньги и власть решают, какое поведение считать приемлемым и кто получит место за игровым столом.

25
Хакинг и богатство

В профессиональном спорте потолок зарплат поддерживает конкурентоспособность лиг, уменьшая несправедливое преимущество клубов с бóльшим капиталом. По сути, все клубы договариваются о максимальной сумме, которую они будут платить своим игрокам. Конечно, эти договоренности можно хакнуть. В зависимости от вида спорта и особенностей правил клубы могут скрывать выплаты под видом подписных бонусов, распределять их на несколько лет, нанимать игроков на работу в компанию – спонсора клуба или иную аффилированную компанию, нанимать супругов игроков или прятать зарплату игроков в бюджет ассоциированной с клубом команды более низкой лиги. В профессиональном спорте крутятся огромные деньги, и клубы делают все возможное, чтобы нарушить правила.

Хакингом банковских и финансовых систем, примеры которого мы наблюдали выше, занимаются в основном люди богатые, пытаясь увеличить и без того немалое состояние. Это переворачивает с ног на голову наши представления о хакерах, связанные с компьютерными взломами. Мы привыкли считать хакинг чем-то контркультурным, чем-то, что бесправные люди предпринимают против безжалостных и могущественных систем, вставших на их пути. Такого рода хакинг, безусловно, тоже существует, и хакерская группа Anonymous является тому примером. Но чаще всего системы взламывают в своих интересах именно богатые люди – будь то ради прибыли или ради власти.

Богатые люди обладают рядом преимуществ, которые позволяют им лучше обнаруживать и использовать уязвимости. Им не обязательно самим быть превосходными хакерами: у богатых есть все ресурсы, чтобы нанять специалистов для успешного взлома. Кроме того, поскольку деньги во многом определяют политику, богатые лучше нормализуют хаки, используя свою власть для их легитимизации.

Когда General Motors в 2009 г. объявила о банкротстве, ее акции были признаны бесполезными и претерпели делистинг, однако вскоре реорганизованная компания провела эмиссию новых акций, благодаря которым привлекла капитал. Руководители и богатые инвесторы получили прибыль, в то время как рядовые акционеры, среди которых было немало действующих сотрудников компании и пенсионеров, оказались в проигрыше. Это был очень выгодный хак, но лишь для тех, кто и так уже был богат.

И вновь мы видим, что богатые разбираются в эффективном хакинге. Люди и организации с концентрированными ресурсами в своем распоряжении лучше находят уязвимости и реализуют взломы. Им проще обеспечивать легализацию и нормализацию

---

111 Eshe Nelson, Jack Ewing, and Liz Alderman (28 March 2021), «The swift collapse of a company built on debt,» *The New York Times* , https://www.nytimes.com/2021/03/28/business/greensill-capital-collapse.html.

хаков.

В 2020 г. мы услышали о новом хаке налоговой системы, связанном с торговлей акциями, под названием cum-ex[112] – эти латинские предлоги используют в биржевом сленге, чтобы обозначать акции до (cum) и после (ex) выплаты дивидендов. Вот как описала этот хак газета *The New York Times* : «Благодаря точному расчету времени и координации дюжины различных транзакций сделки cum-ex обеспечивали двойной возврат налога на дивиденды, выплаченные по одной корзине акций». Первое возмещение было законным, второе – нет.

То, что это хак, не вызывает сомнений: никем не предполагалось, что физическое или юридическое лицо сможет получить два налоговых возмещения по одной выплате. Но система позволила это сделать, и с 2006 по 2011 г. банкиры, юристы и инвесторы, использовавшие этот хак, вывели из стран ЕС в общей сумме $60 млрд.

Недавно Германия приговорила банкира[113], известного как Кристиан С., к десяти годам тюремного заключения за эту аферу. Однако это еще не финал истории, поскольку дело Кристиана С. ожидает пересмотра по апелляции. В 2020 г. два лондонских банкира[114] были приговорены к условному сроку и штрафу в размере 14 млн фунтов стерлингов. Немецкому частному банку было предписано выплатить €176,6 млн немецким налоговым органам. Бывший главный налоговый инспектор Германии[115] в 2012 г., когда скандал с cum-ex выплыл наружу, скрылся в Швейцарии, но был экстрадирован и обвинен в предоставлении консультаций и получении гонораров от банкиров, участвовавших в преступной схеме. Позже в рамках расследования дела о cum-ex был проведен обыск во франкфуртском офисе Morgan Stanley[116]. Еще предстоят новые судебные разбирательства: только в Германии расследуется деятельность более чем тысячи юристов и банкиров, подозреваемых в участии в сделках cum-ex.

На этом актуальном примере мы ясно видим взаимодействие хакинга, законности и морали. Когда тогдашнего кандидата Дональда Трампа спросили[117] о минимизации его личных налогов, он, как известно, ответил: «Это делает меня умным». Возможно, но это не обязательно делает его нравственным. Если даже он использовал исключительно законные налоговые лазейки[118], это не означает, что эти лазейки не должны быть закрыты.

---

112 David Segal (23 Jan 2020), «It may be the biggest tax heist ever. And Europe wants justice,» New York Times, https://www.nytimes.com/2020/01/23/business/cum-ex.html.

113 Karin Matussek (1 Jun 2021), «A banker's long prison sentence puts industry on alert,» *Bloomberg* , https://www.bloomberg.com/news/articles/2021-06-01/prosecutors-seek-10-years-for-banker-in-398-million-cum-ex-case.

114 Olaf Storbeck (19 Mar 2020), «Two former London bankers convicted in first cum-ex scandal trial,» *Financial Times* , https://www.ft.com/content/550121de-69b3-11ea-800d-da70cff6e4d3.

115 Olaf Storbeck (4 Apr 2022), «Former German tax inspector charged with €279mn tax fraud,» *Financial Times* , https://www.ft.com/content/e123a255-bc52-48c4-9022-ac9c4be06daa.

116 Agence *France-Presse* (3 May 2022), «German prosecutors raid Morgan Stanley in cum-ex probe,» Barron's, https://www.barrons.com/news/german-prosecutors-raid-morgan-stanley-in-cum-ex-probe-01651575308.

117 Daniella Diaz (27 Sep 2016), «Trump: 'I'm smart' for not paying taxes,» *CNN* , https://www.cnn.com/2016/09/26/politics/donald-trump-federal-income-taxes-smart-debate/index.html.

118 Постановление Верховного суда США от 1935 г. подтвердило это: «Каждый может устраивать свои дела так, чтобы его налоги были как можно ниже; он не обязан выбирать ту модель, которая больше приносит казне; даже из патриотического долга не нужно платить больше налогов». US Supreme Court (7 Jan 1935), Gregory v. Helvering, 293 US 465, https://www.courtlistener.com/opinion/102356/gregory-v-helvering.

Хак под названием cum-ex стоил европейским странам и их гражданам не менее $60 млрд, и большая часть этой суммы никогда не будет возвращена. Повторюсь, хакинг по большей части носит паразитический характер, и занимаются им в основном богатые и влиятельные люди за счет всех остальных.

Часть IV
Хакинг правовых систем

26
Хакинг законов

Налоговые хаки на удивление часто можно найти в сфере архитектуры и строительства. Мансардная крыша приобрела популярность в наполеоновской Франции. Она позволяла расширить жилую площадь, не увеличивая размер соответствующего налога, поскольку технически дополнительный этаж был частью крыши. Двускатная крыша тоже скрывала под собой этаж, что помогало обходить федеральный закон о прямом налоге, принятый в США в 1798 г. В Перу и других странах можно часто видеть жилые дома, из которых торчат куски арматуры, а вокруг громоздятся кучи обломков. Все дело в том, что за недостроенные здания взимается меньший налог на недвижимость.

Вероятно, сейчас самое время напомнить читателям, что считается хаком, а что нет. Британский налог на окна в домах, действовавший с 1696 по 1851 г., привел к тому, что домовладельцы, не желающие его платить, стали заколачивать окна. Это был хак, потому что количество окон использовалось в качестве косвенного показателя размеров дома, а уменьшение числа окон подрывало корректность такого расчета. Если бы параметры дома измерялись напрямую, а домовладельцы просто снесли свои дома, то это бы не было хаком. Отказ от системы или уничтожение ее части, чтобы избежать затрат, не имеет ничего общего с хакингом. Хакинг означает поиск лазеек в правилах системы и использование их в своих интересах, притом что вы остаетесь участником этой системы.

Правительства действуют посредством слов, и эти слова могут изменить положение дел в мире. Конгресс принимает законы. Президенты подписывают указы. Министерства устанавливают. Все это не более чем слова, связанные с осуществлением власти и правоприменением. Эти слова в некотором смысле являются кодом. И, как в компьютерном коде, в них непременно будут ошибки и уязвимости. Авторы любого юридического текста несовершенны: они ошибаются и могут поддаваться влиянию. Посему любой закон, как и всякую систему, можно хакнуть. Законотворцы, случайно или намеренно, оставляют в законах уязвимые места, которые неизбежно будут обнаружены хакерами. А желание взламывать законы, как известно, неистребимо.

Самптуарные законы, регулирующие расходы, ограничивали расточительность и показную роскошь. Исторически они принимались в основном для того, чтобы предотвратить дорогостоящую конкуренцию в среде знати, стремящейся превзойти друг друга в великолепии устраиваемых банкетов, пиров и зрелищ. Правда, иногда такие законы преследовали и другую цель, чтобы люди низшего сословия не пытались подражать аристократам. В обоих случаях те, кто были недовольны этими законами, пытались их хакнуть.

Число блюд или сортов мяса, подаваемых на банкетах, зачастую было строго регламентировано. Флорентийский закон 1356 г. ограничивал число блюд на свадьбе тремя. Но определение блюда исключало фрукты, овощи и сыр, и хозяева использовали эту лазейку, чтобы стол ломился, а гости были довольны. Жаркое могло состоять из мяса, фаршированного мясом других видов животных (да-да, турдакен [119] изначально был

[119] Турдакен – популярное в США и Великобритании блюдо из мяса птицы. Название образовано слиянием

хаком[120] самптуарных законов). Это в очередной раз иллюстрирует то, как богатые могут соблюдать букву закона, но при этом полностью попирать его дух.

Юридические системы – это такие же системы правил, уязвимые для хакинга. В некотором смысле они даже предназначены для взлома. Буква закона в основном соблюдается, но его дух – достаточно редко. Если вы найдете хак, который следует букве закона, но противоречит его духу, то не ваша вина, что закон плохо написан. Подобный аргумент можно часто услышать от сторонников уклонения от уплаты налогов.

Законы хакают постоянно. В 2020 г. Федеральная резервная система США реализовала программу экстренного кредитования для компаний, пострадавших от пандемии коронавируса[121]. Несмотря на то что официально участвовать в программе могли только американские предприятия, иностранные компании придумали, как превратить себя в американские и хакнуть правила программы. Компания Pacific Investment Management, расположенная в Ньюпорт-Бич, штат Калифорния, управляет хедж-фондом, зарегистрированным на Каймановых островах, чтобы избежать уплаты налогов в США. Но, инвестировав в корпорацию из Делавэра и связав ее с материнской калифорнийской компанией, хедж-фонд смог взять коммерческий заем на покупку ценных бумаг, затем занять $13,1 млн у государственной программы помощи и, наконец, использовать этот второй заем для погашения первого, более дорогого. Мгновенная прибыль, совершенно законная, за счет всех жителей США. Возможно, меня запишут в социопаты, но я не могу не восхититься креативностью этого хака.

Мое представление о взломе законов касается не только законодательства. Взломать можно любое правило. На протяжении истории католической церкви ее правила о воздержании сильно варьировались, но они всегда включали в себя отказ от употребления мяса в определенное время. Это называлось постом, хотя и неполным, по сравнению с Иом-кипуром или Рамаданом. Но, поскольку люди таковы, каковы они есть, то и в Средневековье было принято размышлять над тем, что именно должно считаться мясом, особенно во время Великого поста и Адвента. Рыба мясом не считалась. Белощекая казарка также не считалась мясом, поскольку имела чешуйчатые перепончатые лапы и (предположительно) рожала в воде. Аналогичный аргумент применялся к бобрам, которых тоже за мясо не считали. (И это не какой-нибудь исторический курьез: сегодня детройтским католикам в дни поста разрешено есть мясо ондатры на основании миссионерского постановления 1700-х гг.) В некоторых французских монастырях подавали кроличьи зародыши, которые не считались мясом в силу того, что плавали, подобно рыбам, в амниотической жидкости. Святой Фома Аквинский утверждал, что курица имеет водное происхождение (что бы это ни значило) и мясом не является. Отдельные епископы пошли еще дальше, заявив, что поскольку у птицы не четыре ноги, а две, то есть ее в пост не зазорно.

Более свежим хаком в сфере правил религиозного поста является практика некоторых богатых саудовских семей относиться к Рамадану как к вечеринке длиною в месяц, зажигать по ночам и отсыпаться днем.

Любой закон – это поле для хакинга. И пока есть люди, которые хотят ниспровергнуть его цель и смысл, взломы на этом поле будут продолжаться.

трех английских слов: turkey («индейка»), duck («утка») и chiken («цыпленок»). Представляет собой целые тушки птиц, вложенные одна в другую и запеченные в жаровне. – *Прим. пер* .

[120] Современный рецепт этой фаршированной уткой и курицей индейки придумал шеф-повар Пол Прюдом. Однажды я попытался это приготовить – оно того не стоит.

[121] Jeanna Smialek (30 Jul 2020), «How Pimco's Cayman-based hedge fund can profit from the Fed's rescue,» *The New York Times* , https://www.nytimes.com/2020/07/30/business/economy/fed-talf-wall-street.html.

27
Юридические лазейки

«Зона смерти»[122] – такое название получила странная уязвимость в Конституции США. Она возникает из-за противоречий в правилах на уровне юрисдикций. Статья III, раздел 2, Конституции США гласит: «Судебное разбирательство по любым преступлениям, за исключением дел об импичменте, проводится судом присяжных; и такой суд должен проводиться в штате, где были совершены указанные преступления…» В то же время в Шестой поправке к Конституции сказано, что «во всех случаях уголовного преследования обвиняемый имеет право на быстрое и публичное судебное разбирательство беспристрастным судом присяжных того штата и округа, где было совершено преступление…».

Окружной суд США по округу Вайоминг обладает юрисдикцией над всем Йеллоустонским национальным парком, который простирается до Монтаны и Айдахо, и немного заходит на территорию этих штатов. Допустим, вы совершили убийство в Йеллоустонском национальном парке, в той его части, которая расположена в штате Айдахо. По закону вас не могут судить в Вайоминге – юрисдикции, в которой вы были арестованы, – потому что статья III требует, чтобы вас судили в Айдахо. Но Шестая поправка настаивает, чтобы присяжные проживали как в штате (а это Айдахо), так и в округе (это уже Вайоминг), где было совершено преступление. Это означает, что ваши присяжные должны состоять из жителей той части штата Айдахо, где расположена территория Йеллоустонского парка… в котором попросту нет жителей. Упрощая сказанное, не существует конституционного способа осудить вас в этом случае за убийство.

Никто еще не использовал этот конкретный хак, чтобы избежать наказания за убийство, но к нему прибегли в ходе судебного разбирательства по делу о браконьерстве. В 2007 г. мужчина, нарушив закон, застрелил в Йеллоустоунском парке лося. Дело было на территории штата Монтана. После предъявления обвинения адвокаты использовали описанный хак[123] в качестве составляющей защиты. Суд отклонил этот аргумент на основании того, что, будучи принят, он закрепил бы лазейку, которая уже получила название «Зона смерти». Тем самым они отключили хак посредством судебного решения.

Более зловещую версию этого хака[124] мы встречаем на землях коренных народов. Племенные суды не могут судить лиц, совершивших преступления на их землях, если они не являются коренными американцами. Это могут делать только федеральные власти, но во многих случаях они этого просто не делают. Такое положение дел означает, что некоренные американцы могут свободно и без последствий нападать на землях племен на женщин – представительниц коренных народов. Данные говорят о том, что 80 % коренных американок, подвергшихся сексуальному насилию на племенных территориях, становились жертвами мужчин, не являющихся коренными американцами.

И еще один пример юридического хака. Федеральные анклавы – это участки земли в пределах штата, которые принадлежат федеральному правительству и уже долгое время являются уязвимым местом правовой системы США. К федеральным анклавам относятся

---

122 Brian C. Kalt (2005), «The perfect crime,» Georgetown Law Journal 93, no. 2, https://fliphtml5.com/ukos/hbsu/basic.

123 Clark Corbin (3 Feb 2022), «Idaho legislator asks U.S. Congress to close Yellowstone's 'zone of death' loophole,» *Idaho Capital Sun*, https://idahocapitalsun.com/2022/02/03/idaho-legislator-asks-u-s-congress-to-close-yellowstones-zone-of-death-loophole.

124 Louise Erdrich (26 Feb 2013), «Rape on the reservation,» *The New York Times*, https://www.nytimes.com/2013/02/27/opinion/native-americans-and-the-violence-against-women-act.html.

военные базы, здания федеральных судов, федеральные тюрьмы и ряд других сооружений, а также национальные леса и парки. Такие анклавы имеют особый правовой статус, поскольку штаты, в которых они расположены, фактически отказываются от права собственности на них в пользу федерального правительства, а это означает, что законы штата и округа на них не распространяются.

Правовая система неоднократно пыталась устранить эту уязвимость. В 1937 г. по решению Верховного суда США к федеральным анклавам стали применяться налоговые правила штатов, где они расположены[125]. В 1970 г. в деле «Эванс против Корнмана» Верховный суд постановил, что жители федеральных анклавов (к примеру, обитатели частных домов, расположенных на территории национального парка) могут голосовать на выборах штата. Через суды были приняты и другие, менее значительные поправки, но федеральные анклавы по-прежнему не подпадают под действие многочисленных местных законов, включая уголовное законодательство, законы о борьбе с дискриминацией и законы об охране труда.

Жители федеральных анклавов[126] также могут избежать запрета на фуа-гра. Фуа-гра – это приготовленная особым образом гусиная или утиная печень, подвергшаяся процессу под названием гаваж, который представляет собой насильственное кормление животного в течение нескольких недель, пока его печень не разбухнет и не станет в десять раз больше своего нормального состояния. Защитники прав животных регулярно выступают против такой жестокости, и в 2004 г. в Калифорнии наконец запретили производство и продажу фуа-гра. В последующие годы этот запрет неоднократно оспаривался в суде. В 2014 г. владельцы ресторана под названием Presidio Social Club, расположенного в Сан-Франциско, заявили[127], что поскольку он расположен на территории федерального анклава, то запрет штата Калифорния на него не распространяется. Однако, прежде чем суд смог вынести решение, владельцы сдались под натиском активистов, пикетировавших ресторан, и убрали фуа-гра из меню. Так что окончательного решения по этому хаку пока нет.

Во всех приведенных примерах настоящий патч будет состоять в том, чтобы законодательная власть вернулась к закону и устранила лазейки. Именно конгресс должен определить «Зону смерти» в Окружном суде США по округу Айдахо. Именно конгрессу необходимо предоставить индейским народам юрисдикцию и инфраструктуру для обеспечения безопасности и защиты прав женщин и девочек на своих территориях. Хотя Закон о насилии в отношении женщин, принятый в 2013 г., частично закрыл эту уязвимость, принятие по-настоящему действенных поправок к нему было сорвано в 2019 г.[128] оружейным лобби по причинам, не имеющим отношения к данному положению.

28
Хакинг бюрократических барьеров

---

125 US Supreme Court (6 Dec 1937), James v. Dravo Contracting Co. (Case No. 190), 302 U.S. 134, https://tile.loc.gov/storage-services/service/ll/usrep/usrep302/usrep302134/usrep302134.pdf.

126 US Supreme Court (15 Jun 1970), Evans v. Cornman (Case No. 236), 398 U.S. 419, https://www.justice.gov/sites/default/files/osg/briefs/2000/01/01/1999-2062.resp.pdf.

127 Andrew Lu (16 Jul 2012), «Foie gras ban doesn't apply to SF Social Club?» Law and Daily Life, FindLaw, https://www.findlaw.com/legalblogs/small-business/foie-gras-ban-doesnt-apply-to-sf-social-club.

128 Indian Law Resource Center (Apr 2019), «VAWA reauthorization bill with strengthened tribal provisions advances out of the House,» https://indianlaw.org/swsn/VAWA_Bill_2019. Indian Law Resource Center (2019), «Ending violence against Native women,» https://indianlaw.org/issue/ending-violence-against-native-women.

Когда вы устанавливаете некий набор правил, обычно те, кто должен их соблюдать[129], оптимизируют свои действия, чтобы привести их в соответствие с новыми правилами – даже если то, что они в итоге делают, идет вразрез с четко заявленной целью этих правил. В качестве примера можно привести дезинсектора, который выпускает рой насекомых, чтобы стимулировать свой бизнес, или учителя, преподающего строго по тесту, чтобы повысить результаты своих учеников на экзамене. Экономисты называют это законом Гудхарта: когда показатель становится целью, он перестает быть хорошим показателем. Таким образом, бюрократические правила постоянно хакаются людьми, которые не хотят их соблюдать.

Бюрократические барьеры взламываются снизу теми, кого они ограничивают и кому мешают добиться поставленных целей. В 1980-х гг. Даниэль Голдин, девятый администратор NASA, хакнул бюрократические правила, которые применялись к агентству, что позволило запустить больше космических зондов, таких как миссия Mars Pathfinder, и сделать это дешевле, чем раньше[130]. Недавно созданные государственные инновационные агентства, вроде 18F или US Digital Service, уже взломали немало медленных и сложных государственных процессов найма, заключения контрактов и закупок, чтобы внедрять технологические новинки со скоростью интернета. Правительственные технологи в Великобритании и Канаде сделали то же самое в своих странах.

Бюрократическую машину взламывают и те, кто выступает против нее по принципиальным мотивам. «Работа по правилам» (work-to-rule)[131] – это особая тактика профсоюзов, заменяющая собой забастовку. Она представляет собой злонамеренное подчинение, что, по сути, означает безупречно точное следование правилам, которое быстро заводит любое дело в тупик. Вот некоторые наиболее очевидные хаки подобного рода: использовать все разрешенные перерывы, прекращать работу точно в назначенное время, отказываться отвечать на телефонные звонки, потому что это не входит в ваши обязанности, и т. д. Такая тактика проверена десятилетиями и, в частности, легла в основу сюжета неоконченного сатирического романа Ярослава Гашека «Похождения бравого солдата Швейка во время мировой войны», написанного в 1920-х гг.

Это понятные и эффективные хаки: настаивайте на том, чтобы все делалось только по официальным каналам, увеличивайте объем бумажной работы всеми правдоподобными способами, применяйте любые предписания с точностью до последней буквы. Идея такого подхода заключается в том, чтобы обратить систему правил против самой себя.

В 1980-х гг. в Малайзии существовала система издольной ренты, называемая sewa padi. Обычно плата за аренду земли взималась после сбора урожая[132] и зависела от его качества. Поэтому фермеры по ночам тайно собирали урожай еще до официального старта сбора, если надзор был слабым, прятали часть зерна, собранного под отчет, или некачественно проводили обмолот, чтобы позже можно было собрать рис, оставшийся на стеблях, а затем заявляли о якобы плохом урожае. Многое из этого было обычным жульничеством, но некоторые тактики можно считать вполне хакерскими. Правительство устранило эту уязвимость, введя новую систему, называемую sewa tunai, с фиксированной арендной платой, взимаемой до посадки.

---

129 C. A. E. Goodhart (1984), Monetary Theory and Practice: The UK Experience, Springer, https://link.springer.com/book/10.1007/978-1-349-17295-5.

130 Howard E. McCurdy (2001), Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program, Johns Hopkins University Press.

131 В Европе такое поведение сотрудников называется итальянская забастовка. – *Прим. ред* .

132 James C. Scott (1985), Weapons of the Weak: Everyday Forms of Peasant Resistance, Yale University Press.

Этот особый стиль хакинга встречается довольно часто. В 1902 г. правительство Ханоя пыталось искоренить популяцию крыс, покупая у населения крысиные хвосты[133]. Люди быстро смекнули, что разумнее всего поймать крысу, отрезать ей хвост, а затем выпустить, чтобы она могла нарожать еще больше крыс для последующей ловли. В 1989 г. в Мехико была введена схема контроля загрязнения окружающей среды, согласно которой автомобили с четными и нечетными номерными знаками[134] должны были ездить в разные дни. В ответ на это люди стали покупать вторые автомобили, в основном, конечно, дешевые и подержанные, что только ухудшило ситуацию с загрязнением окружающей среды.

Совсем недавно водители Uber в Найроби придумали хак[135], лишающий компанию ее доли в каждой поездке. Клиент вызывает машину через приложение Uber, которое рассчитывает стоимость, а при встрече водитель и пассажир договариваются о том, что пассажир отменяет поездку в приложении и платит водителю наличными.

Крушения Boeing 737 MAX представляют собой особенно яркий пример халатности регулирующих органов, которая стала результатом слишком тесных отношений между ними и регулируемыми отраслями. В данном случае регулирующие органы Федерального управления гражданской авиации США недостаточно тщательно изучили модифицированную систему улучшения маневренных характеристик (MCAS), внедренную в конструкцию Boeing 737 MAX. В результате такого недосмотра два самолета этой модели разбились – один в Индонезии в 2018 г., другой в Эфиопии в 2019 г., унеся жизни 346 человек.

Давайте будем откровенны. Предполагается, что регулирующие органы должны быть экспертным посредником, представляющим интересы среднестатистического человека. Я не являюсь экспертом в области безопасности самолетов, автомобилей, продуктов питания, лекарств или того, как банки должны управлять своими балансами для поддержания стабильности экономики. Все эти знания предоставляет гражданам правительство в форме работы регулирующих органов, которые, по сути, устанавливают правила от моего имени, чтобы меня защитить. В приведенном примере подрывается именно этот механизм надзора.

Анализ катастроф указал на сбои в системе регулирования. Федеральное управление гражданской авиации никогда не проводило независимую проверку MCAS, полагаясь на собственные оценки этой системы компанией Boeing. Правительственные эксперты, как оказалось, не обладали достаточным для этого опытом и делегировали большую часть работы компании-производителю. Инженерам, работавшим над самолетом, было разрешено сертифицировать свою собственную работу. И были случаи, когда руководители Федерального управления гражданской авиации принимали предложения Boeing об изменении правил[136], связанных с безопасностью. В частности, несколько таких правил были просто отменены[137], чтобы упростить процесс сертификации для Boeing и дать

---

133 Michael G. Vann (2003), «Of rats, rice, and race: The Great Hanoi Rat Massacre, an episode in French colonial history,» *French Colonial History* 4, https://muse.jhu.edu/article/42110/pdf.

134 Lucas W. Davis (2 Feb 2017), «Saturday driving restrictions fail to improve air quality in Mexico City,» *Scientific Reports* 7, article 41652, https://www.nature.com/articles/srep41652.

135 Sean Cole (7 Aug 2020), «Made to be broken,» This American Life, https://www.thisamericanlife.org/713/made-to-be-broken. Gianluca Iazzolino (19 Jun 2019), «Going Karura. Labour subjectivities and contestation in Nairobi's gig economy,» DSA2019: Opening Up Development, Open University, Milton Keynes, https://www.devstud.org.uk/past-conferences/2019-opening-up-development-conference.

136 Natalie Kitroeff, David Gelles, and Jack Nicas (27 Jun 2019), «The roots of Boeing's 737 Max crisis: A regulator relaxes its oversight,» *The New York Times*, https://www.nytimes.com/2019/07/27/business/boeing-737-max-faa.html.

137 Gary Coglianese, Gabriel Scheffler, and Daniel E. Walters (30 Oct 2020), "The government's hidden

компании возможность быстрее продавать самолеты. В совокупности вырисовывается картина процесса государственного регулирования, хакнутого авиационной отраслью, и среды, где процветает захват регулирующих органов, порочные стимулы, этические дилеммы и опасные нарушения безопасности.

В 2021 г. министерство юстиции заключило мировое соглашение с компанией Boeing по уголовным обвинениям, связанным с этими авариями, предусматривавшее выплату $2,5 млрд. Это может показаться большой суммой, но на самом деле компания легко отделалась. Только $243,3 млн ушло на штрафы Федеральному агентству гражданской авиации – сумма небольшая, по мнению рыночных аналитиков. При этом против компании не были выдвинуты уголовные обвинения и от нее не потребовали признания вины, несмотря на достоверные сообщения о систематической халатности в вопросах безопасности.

Уютные отношения между Boeing и регулирующими органами свидетельствуют о необходимости пересмотреть разделение обязанностей между регуляторами и отраслями. В конечном счете обеспечение ответственного поведения и такого же отношения к выпуску продукции в регулируемых отраслях лежит на плечах регулирующих органов, а слишком сильная зависимость от самосертификации отрасли создает долгосрочный конфликт интересов и ослабляет способность правительства осуществлять надзор. Что еще более важно, существует необходимость особо тщательной подготовки лиц, выполняющих функции регуляторов, в частности введения правила длительного «остывания» кандидата перед приемом на работу в отрасли. Если регуляторы рассматривают себя не как государственных служащих, а как будущих сотрудников компаний, деятельность которых они регулируют, возникает порочный корыстный стимул и регулирование перестает отвечать общественным интересам.

29
Хакинг и власть

Хакинг – это способ осуществления власти. Власти за счет других, а зачастую и всех прочих участников взломанной системы. Хакером движет желание продвигать собственные планы, невзирая на установленные правила. (Это верно даже в отношении типичного хакера-подростка, пытающегося удовлетворить свое любопытство. Да, любопытство не порок, но в данном случае оно нарушает приватность.)

Бесправные люди взламывают существующие структуры власти. Они делают это, чтобы обойти бюрократические препоны или же ради личной выгоды. Большая часть людей в мире не имеет права голоса в глобальных системах, влияющих на их жизнь; часто у них просто нет другого выбора, кроме как хакнуть эти системы. Такой взлом может быть разумным ответом на хакерские атаки со стороны элиты или государства, к примеру на чрезмерное административное бремя.

Но хотя у хакинга есть и такое лицо, когда аутсайдер пытается вырвать у власти какое-то преимущество, гораздо чаще он используется сильными мира сего для увеличения своих преимуществ.

Как я уже говорил, крупнейшие банки США создали специальные рабочие группы юристов для выявления и использования лазеек в законе Додда – Франка и провели трехлетнюю лоббистскую кампанию по их нормализации, стоившую миллионы долларов. Благодаря своим размерам и богатству банки смогли найти и использовать уязвимости, а благодаря купленной на это богатство власти лазейки остаются законными.

При этом существуют различия в том, как хакают системы бесправные граждане и власть имущие. Аутсайдеры – преступники, диссиденты, хакеры-одиночки – действуют

---

superpower: 'Unrules,' " *Fortune* , https://fortune.com/2020/10/30/federal-law-regulations-loopholes-waivers-unrules.

более проворно и за счет этого увеличивают свою коллективную силу. Но когда устоявшиеся институты наконец находят способы взлома систем, которые их сдерживают, они действуют более эффективно. А поскольку у них больше денег и власти, которые нужно увеличивать, то и выгоды от хакинга они получают больше. Это справедливо как для правительств, так и для крупных корпораций.

О динамике власти можно говорить не только в связи с процессом хакинга, но и в отношении нормализации успешных хаков. Влиятельные люди (под которыми я обычно подразумеваю людей богатых) лучше подготовлены к тому, чтобы устроенные ими взломы были долговечными, а мы с вами не считали их подлыми мошенниками и воспринимали их действия как совершенно нормальные. Ведь именно так, скорее всего, вы и думаете о хедж-фондах, венчурном финансировании и всевозможных стратегиях ухода от налогов.

Причины такого положения дел носят структурный характер. Во-первых, для эффективного использования налоговых лазеек часто требуется помощь высокооплачиваемых юристов и бухгалтеров. Во-вторых, у богатых людей и организаций, как правило, больше денег, которые необходимо скрывать, и потому у них более сильная мотивация для поиска и использования уязвимостей в налоговом кодексе. В-третьих, налоговые эксплойты часто обслуживают теневую зону экономики, а борьба с налоговыми органами требует немалых финансовых ресурсов. И в-четвертых, слабое правоприменение означает, что богатые налоговые мошенники с меньшей вероятностью будут привлечены к ответственности.

Давайте обобщим. Успешные хаки обычно требуют либо специальных знаний, либо ресурсов для найма людей с такими знаниями, либо ресурсов для создания вспомогательной системы, облегчающей взлом. По всем трем пунктам богатые и влиятельные люди и организации имеют преимущество и куда лучше оснащены, чтобы устраивать и нормализовывать масштабные хаки.

Здесь также имеет место социальная динамика власти. Разнообразные меньшинства, маргинальные слои населения, а также представители классов, рас, полов и этнических групп, обладающие меньшей властью, менее склонны и к хакингу. Взлом системы вряд ли сойдет им с рук, если они попытаются это сделать. Да, они могут совершать преступления, но это не одно и то же. Женщин учат следовать правилам, в то время как белых мужчин учат нарушать их, если подворачивается такая возможность. Это важное соображение, которое следует иметь в виду, размышляя о хакинге и власти.

Правящая элита лучше справляется и с противодействием хакерским атакам менее влиятельных индивидов и групп. Профсоюзные тактики, такие как «работа по правилам», применяются сегодня гораздо реже и прежде всего потому, что сильные мира сего неуклонно подрывают власть профсоюзов. Руководство в целом все более враждебно относится к профсоюзным организациям и продвигает антипрофсоюзные законы и судебные решения. В результате многие сотрудники могут быть уволены без причины. Поскольку тактика «работы по правилам» требует членства в профсоюзе или как минимум защиты от безосновательных увольнений, то со временем она стала терять свою актуальность.

Профессор права Джорджтаунского университета Джули Коэн утверждает, что «власть интерпретирует регулирование как ущерб и идет обходными путями». Под этим она подразумевает, что у привилегированного класса есть все необходимое, чтобы обходить установленные правила. Как только хозяева жизни осознали, что им нужно взламывать системы – и в первую очередь процессы регулирования, которые мешают им делать то, что заблагорассудится, – они развили компетентность в этом вопросе. Мы уже имели возможность убедиться в этом на примере банковской сферы, финансовых рынков и элитной недвижимости.

Вспомните об отказе сената США даже рассмотреть кандидатуру Меррика Гарланда в качестве кандидата в Верховный суд страны в 2016 г. Это был хак, подрывающий процесс утверждения кандидатуры в сенате. Что вызывает у меня интерес, так это то, что мы до сих пор не знаем, был ли этот хак нормализован. Известно, что республиканцы не были наказаны

за свое лицемерие, когда четыре года спустя выдвинули на этот пост кандидатуру Эми Кони Барретт. О новой норме мы узнаем только в следующий раз, когда освободится место в Верховном суде, и при этом одна партия будет контролировать президентское кресло, а другая – сенат. Сделает ли снова то же самое сенат, в котором доминируют республиканцы? Воспользуются ли демократы такой возможностью, когда она появится? Если ответ на любой из этих вопросов положительный, то, скорее всего, судьи Верховного суда теперь всегда будут назначаться лишь тогда, когда одна и та же партия контролирует и президентский пост, и сенат, поскольку последний имеет возможность хакнуть систему утверждения в состав Верховного суда.

Вот почему истории о хакерских атаках, совершенных менее влиятельными людьми – бедными, обездоленными, находящимися в положении политических диссидентов в авторитарных странах, – встречаются намного реже. Власть объявляет такие хаки незаконными, а хакеров – мошенниками. Налоговые лазейки, используемые простыми гражданами, закрываются налоговым управлением. Сидячие забастовки и замедление темпа работы – явления, обычные в 1930-х гг., – больше не защищаются федеральным законодательством США. Мы даже не считаем такие методы хакингом. Это не значит, что люди, не облеченные властью, не способны взламывать системы. Просто они менее эффективны в нормализации своих хаков.

Изучая систему, обратите внимание на то, чьи интересы она обслуживает. Хакать ее будут те, кому она мешает. Это могут быть и сливки общества, и представители масс. И хотя и те и другие умеют обходить ограничения, но преуспеют в этом с большей вероятностью элиты. И они же, скорее всего, избегут наказания.

30
Хакинг нормативных актов

С точки зрения пользователей Uber – это служба такси[138]. Она выглядит как служба такси. Она функционирует как служба такси. Но если вы спросите у сотрудников Uber или любых ее конкурентов, то с удивлением узнаете, что это вовсе не служба такси и даже не транспортная компания. Это компания интернет-услуг, соединяющая водителей автомобилей с людьми, которые хотят, чтобы их куда-то отвезли. Эти водители являются независимыми подрядчиками, а не работниками; Uber утверждает, что никак не контролирует их. Uber назначает на поездку водителя со своим автомобилем и обрабатывает его счета – что-то вроде любезности с его стороны. Компания заявляет, что на самом деле не имеет никакого отношения к автомобилям, по крайней мере в том, что касается каких-либо государственных норм.

Каршеринговые приложения – это взлом индустрии такси[139], а в более общем смысле – попытка общества управлять своими краткосрочными транспортными потребностями. Их бизнес-модель позволяет игнорировать десятки законов и нормативных актов, регулирующих деятельность лицензированных такси и лимузинов, включая законы о защите работников, безопасности и правах потребителей, правила получения разрешений и оплаты сборов, а также законы об общественном благе. Таксисты обязаны проходить проверку в соответствующих органах, водители Uber и Lyft – нет (хотя сейчас они нехотя начали это делать). Службы такси обязаны платить своим сотрудникам минимальную

---

138 Компания изначально называлась UberCab, но изменила название именно по той причине, что не является таковой.

139 Ruth Berens Collier, Veena Dubal, and Christopher Carter (Mar 2017), «The regulation of labor platforms: The politics of the Uber economy,» University of California Berkeley, https://brie.berkeley.edu/sites/default/files/reg-of-labor-platforms.pdf.

заработную плату и учитывать общегородские ограничения на число автомобилей, находящихся в управлении. Но только не Uber и Lyft. Этот список можно продолжать и продолжать.

Начиная с 2012 г. Uber использует свое конкурентное преимущество [140] перед традиционными службами такси и лимузинов, чтобы доминировать на рынке. По состоянию на 2021 г. компания представлена в более чем 10 000 городах 72 стран, ежедневно обеспечивая в среднем 19 млн поездок. У компании 3,5 млн водителей [141] и 93 млн ежемесячных активных клиентов. И до сих пор она не может получить прибыль.

Все это время муниципалитеты по всему миру с переменным успехом пытаются закрыть уязвимости, которые Uber использовала для того, чтобы хакнуть рынок такси. В 2017 г. высший суд Европейского союза постановил, что Uber – это транспортная служба, а вовсе не технологическая компания, за которую она себя выдает в надежде обойти правила перевозок. В 2018 г. Апелляционный суд Великобритании постановил, что водители компании являются ее работниками, вопреки утверждению самой Uber о том, что все водители – это независимые подрядчики; французский Кассационный суд принял аналогичное решение в 2020 г. В США в Калифорнии в 2019 г. был принят закон, требующий от таких компаний, как Uber, рассматривать водителей как своих сотрудников; это вызвало волну судебных разбирательств, которые продолжаются и поныне. Другие города и штаты сейчас пытаются сделать то же самое, несмотря на то что в большинстве штатов по данному вопросу уже имеются постановления.

Airbnb – аналогичный хак, только в сфере гостиничной индустрии[142]. Жилье, которое предлагает Airbnb, – это не то же самое, что отели, хотя и служит той же цели краткосрочного проживания. Но Airbnb утверждает, что поскольку она не является гостиничной компанией, то и на жилье, предлагаемое ей в аренду, не должны распространяться законы и правила – в том числе налоговые, – которые регулируют деятельность гостиничного бизнеса. Поскольку Airbnb не владеет недвижимостью, она утверждает, что является всего лишь технологической компанией. Люди, владеющие жильем, рассматриваются ею как независимые подрядчики и сами несут ответственность за уплату налогов и соблюдение местных правил. Но, конечно, большинство из них этого не делает.

Муниципалитеты либо позволяют Airbnb ускользать и не получают свою долю оплаты за проживание, либо пытаются дать отпор. Некоторые из них предпринимали попытки ограничить расширение компании с помощью регулирования, но Airbnb подавала на них в суд (продолжая при этом работать), что приводило к затяжным судебным баталиям. Кроме того, Airbnb часто привлекает владельцев недвижимости в качестве своих лоббистов на местах. Компания рассылает сообщения о том, что городские власти угрожают лишить их возможности зарабатывать, и даже назначает конкретные встречи, на которых хозяева должны присутствовать.

Это лишь два примера компаний эпохи гиг-экономики, для которой характерны попытки взлома трудового законодательства, законов о защите прав потребителей и целого ряда других законов и нормативных актов. TaskRabbit, Handy и DoorDash используют те же хакерские методы. Это же делает и Amazon, управляя системой автомобильной доставки,

---

140 Uber Technologies, Inc. (2021), «2021 Form 10-K Annual Report,» US Securities and Exchange Commission, https://www.sec.gov/ix?doc=/Archives/edgar/data/1543151/000154315122000008/uber-20211231.htm.

141 Brian Dean (23 Mar 2021), «Uber statistics 2022: How many people ride with Uber?» Backlinko, https://backlinko.com/uber-users.

142 Paris Martineau (20 Mar 2019), «Inside Airbnb's 'guerilla war' against local governments,» Wired, https://www.wired.com/story/inside-Airbnbs-guerrilla-war-against-local-governments.

которая по своей сути подобна системе Uber. Поскольку водители, доставляющие товары Amazon, являются независимыми подрядчиками, компания может игнорировать любые законы, которым должна следовать обычная транспортная компания.

То, что компании хакают правила, ни для кого не является секретом. В приведенных примерах важно другое: уклонение от нормативных требований – особенно если речь идет о каршеринге, краткосрочной аренде и микрозаймах – является центральным элементом бизнес-моделей этих компаний. Многие «подрывные» сервисы гиг-экономики были бы попросту нежизнеспособны, если бы их заставили соблюдать правила, которым подчиняются конкурирующие с ними «обычные» компании. В результате «подрывники» и их венчурные инвесторы готовы тратить невероятные суммы на борьбу с этими правилами. Из чего следует, что, во-первых, их конкуренты, соблюдающие нормативные требования, оказываются в невыгодном положении, а во-вторых, долгосрочная прибыльность этих компаний предполагает либо дальнейшее уклонение от регулирования (и, как следствие, эксплуатацию низкооплачиваемых гиг-работников), либо массовую замену гиг-работников машинами.

Реакция этих компаний на попытки государственных и местных органов власти устранить уязвимости, на которых они строят свой бизнес, показывает, как далеко они готовы зайти. После решения Верховного суда штата Калифорния от 2018 г. и упомянутого выше закона штата от 2019 г. несколько таких компаний объединились для проведения референдума под названием «Proposition 22», который был призван лишить гиг-работников мер защиты, гарантированных трудовым законодательством: классификации сотрудников, минимальной заработной платы, страхования по безработице, медицинской страховки и т. д. Возглавляемые Uber, Lyft и DoorDash компании потратили в общей сложности $200 млн, чтобы поддержать этот референдум и убедить работников в том, что он отвечает их интересам. Эта мера увенчалась успехом в 2020 г. и свела на нет усилия Калифорнии по защите работников гиг-компаний. Битва еще не окончена, и, несомненно, после выхода этой книги мы увидим, как будут разворачиваться события.

Пожалуй, я мог бы написать отдельную книгу о том, как компании и отрасли взламывают нормативные акты, ограничивающие их прибыль, но пока просто приведу еще пару примеров. Ссуды до зарплаты – это краткосрочные кредиты[143], предназначенные для необеспеченных граждан. Они выдаются небольшими суммами под астрономически высокие проценты. Четыре пятых заемщиков продлевают такие кредиты, загоняя себя в замкнутый круг, в результате чего средняя процентная ставка по ним составляет 400 % в год, не считая комиссий. Штаты пытаются регулировать индустрию микрозаймов и снижать процентные ставки, но компании, предоставляющие ссуды до зарплаты, постоянно находят способы хакать новые правила. Вместо кредитов, по которым полное погашение должно производиться на следующий после зарплаты день, они стали выдавать кредиты в рассрочку, технически обходя таким образом определение «ссуда до зарплаты». Кроме того, они работают как кредитные брокеры[144] – посредники, которые могут взимать нерегулируемые комиссии. В штате Монтана компании микрозаймов переехали в индейские резервации[145], чтобы избежать регулирования со стороны штата и федерального правительства. В 2020 г. Бюро финансовой защиты потребителей (CFPB) администрации Трампа отменило целый список новых правил, которые должны были ограничить наиболее

---

143 Carter Dougherty (29 May 2013), «Payday lenders evading rules pivot to installment loans,» Bloomberg, https://www.bloomberg.com/news/articles/2013-05-29/payday-lenders-evading-rules-pivot-to-installmant-loans.

144 S. Lu (22 Aug 2018), «How payday lenders get around interest rate regulations,» WRAL (originally from the MagnifyMoney blog), https://www.wral.com/how-payday-lenders-get-around-interest-rate-regulations/17788314.

145 Liz Farmer (4 May 2015), «After payday lenders skirt state regulations, Feds step in,» Governing.

хищнические методы этой отрасли.

И последняя история. Во время пандемии COVID-19 США и Канада закрыли свои сухопутные границы для поездок без острой необходимости. Из страны в страну можно было летать, но существовали всевозможные ограничения на автомобильное сообщение. Это стало проблемой для канадских «снегирей» – людей, привыкших уезжать на зиму в теплые штаты на своих машинах. Однако лазейка нашлась [146]. Грузоперевозки были по-прежнему разрешены, и судоходная компания из Гамильтона, штат Онтарио, предложила услугу по доставке автомобиля клиента в США, в аэропорт города Буффало, а вертолетная компания доставляла туда клиента. Те, кто мог позволить себе такую услугу, полностью обходили закрытие сухопутной границы.

Везде, где существует регулирование, есть люди, которых оно ограничивает. Как правило, нормативные акты приносят пользу гражданам, но могут приниматься и в интересах действующих компаний, препятствовать инновациям и отражать устаревший образ мысли. У новых компаний есть стимул искать уязвимости в этих правилах и организовывать хаки, которые отвечают букве нормативного акта, при этом полностью нарушая его дух. А поскольку, как мы знаем, любые правила всегда будут либо неполными, либо непоследовательными, все они уязвимы для хакинга.

Здесь мы подходим к важному вопросу. Как предотвратить взломы со стороны богатых, технически сложных и политически подкованных корпораций, само существование которых зависит от хакинга? Каким должно быть умное и гибкое решение в этом случае?

Одной из мер безопасности является тестирование новых нормативных актов до их принятия. По словам Джереми Розенблюма, адвоката из Филадельфии, который консультирует компании микрозаймов, отрасль должна постоянно разрабатывать новые финансовые продукты [147], не дожидаясь вмешательства регулирующих органов: «Обслуживая этот рынок, вы должны рассматривать альтернативные стратегии на случай, если CFPB все-таки выпустит нормативные акты». Такой же философии придерживаются все компании, о которых шла речь выше. Чтобы противостоять этому, регулирующие органы должны быть проактивными в своих усилиях и учитывать возможные уязвимые места и реакцию отрасли заранее. Благодаря этому регуляторы смогут лучше предвидеть и предотвращать социально пагубные действия и опасные финансовые инновации, внедряемые отраслью.

Еще один ключевой момент – итеративность и гибкость. Хотя приятно надеяться или даже верить в то, что эффективные нормативные акты будут приняты заранее и предотвратят подобные хаки, регулирующие органы должны быть готовы к неожиданным и социально вредным нововведениям. Для борьбы с ними необходимо следить за регулируемыми субъектами и быть готовыми действовать быстро, чтобы взять под контроль новые продукты, появляющиеся как реакция на нормативные акты. При этом нужно исходить из того, что в правилах есть уязвимости, требующие устранения, как только они будут обнаружены.

31
Взаимодействие юрисдикций

Налоговая лазейка «двойной ирландский с голландским сэндвичем», которую такие

---

146 Dave McKinley and Scott May (30 Nov 2020), «Canadians buzz through Buffalo as a way to beat border closure,» *WGRZ*, https://www.wgrz.com/article/news/local/canadians-buzz-through-buffalo-as-a-way-to-beat-border-closure/71-07c93156-1365-46ab-80c1-613e5b1d7938.

147 Carter Dougherty (29 May 2013), «Payday lenders evading rules pivot to installment loans,» Bloomberg.

компании, как Cisco, Pfizer, Merck, Coca-Cola и Facebook, использовали, чтобы уклониться от уплаты налогов в США, возникла из-за того, что законы действуют внутри национальных границ. Умело используя иностранные дочерние компании и передавая им права и доходы, крупные американские корпорации могут избежать уплаты налогов на большую часть своих глобальных доходов. (Обратите внимание, что граждане США облагаются налогом на весь свой доход, независимо от того, в какой стране он был получен, поэтому этот хак работает только для корпораций.)

Это всего лишь один из многих хаков с использованием налоговых гаваней по всему миру. Глобальное уклонение от уплаты налогов обходится США [148] чуть менее чем в $200 млрд в год, что составляет 1,1 % ВВП. Общая сумма глобальных налоговых поступлений [149] в зависимости от оценок варьируется в диапазоне $500–600 млрд. Подобные хаки интересны в первую очередь тем, что они используют взаимодействие между уязвимостями законодательств разных стран.

Решение заключается в простоте и прозрачности. В США 28 штатов и округ Колумбия приняли комбинированные системы отчетности по корпоративному налогу на прибыль корпораций, что помогает предотвратить перемещение прибыли между юрисдикциями. В рамках комбинированной системы отчетности компании и их дочерние предприятия должны сообщать о своей общей прибыли (в данном случае – об общей «внутренней» прибыли) и о том, какая доля их бизнеса приходится на определенную юрисдикцию (в данном случае – штат). Затем юрисдикция облагает налогом соответствующую долю этой прибыли, пропорциональную доле бизнеса компании, осуществляемого на ее территории, тем самым предотвращая уклонение от уплаты налогов путем переноса прибыли из одной юрисдикции в другую. Такой подход уже помог штатам вернуть миллиарды долларов налоговых поступлений, которые до этого утекали через внутренние налоговые гавани.

Однако это нововведение не решило более широкую проблему перемещения прибыли транснациональными компаниями с целью ухода от налогов. Во-первых, почти все штаты США, использующие комбинированную систему отчетности для налогообложения (заметным исключением является Монтана), не требуют от компаний раскрытия информации об офшорной прибыли, что позволяет тем избегать уплаты налога на прибыль, полученную внутри страны, но переведенную за рубеж. Во-вторых, как я уже отмечал ранее, корпоративный подоходный налог в США не начисляется на прибыль, полученную за рубежом, что облегчает уклонение от уплаты налогов и перевод прибыли за рубеж на федеральном уровне.

Закон о сокращении налогов и увеличении занятости 2017 г. предпринял робкую попытку решить эту проблему с помощью положения о глобальном нематериальном низконалоговом доходе (GILTI), которое требовало от компаний уплаты номинального налога на необлагаемую прибыль в зарубежных налоговых гаванях в размере 10,5 %, но это не помогло остановить основные потоки выводимой за границу прибыли.

Лучшая идея, которую я видел для решения этой проблемы, сочетает в себе все те же простоту и прозрачность. Она называется «Обязательная глобальная комбинированная отчетность» (MWCR) и представляет собой чрезвычайно простой метод решения сложных вопросов налогообложения в юрисдикциях. Подобно системе комбинированной отчетности внутри США, эта система требует, чтобы компания и ее дочерние предприятия сообщали о своей общей глобальной прибыли, а также о том, какая доля их бизнеса (обычно

---

148 Alex Cobham and Petr Jansky (Mar 2017), «Global distribution of revenue loss from tax avoidance,» United Nations University WIDER Working Paper 2017/55, https://www.wider.unu.edu/sites/default/files/wp2017-55.pdf.

149 Ernesto Crivelli, Ruud A. de Mooij, and Michael Keen (29 May 2015), «Base erosion, profit shifting and developing countries,» *International Monetary Fund Working Paper* 2015118, https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Base-Erosion-Profit-Shifting-and-Developing-Countries-42973.

выражаемая через выручку) приходится на определенную юрисдикцию. Затем эта юрисдикция облагает налогом часть прибыли, пропорциональную доле бизнеса компании, который та ведет на ее территории.

На момент написания этой книги администрация Байдена и Организация экономического сотрудничества и развития (ОЭСР, клуб богатых и развитых стран) работали над тем, чтобы сделать нечто подобное MWCR реальностью. В 2021 г. ОЭСР объявила, что 130 стран и юрисдикций согласились облагать налогом крупнейшие транснациональные корпорации по минимальной ставке 15 % от прибыли, полученной на территории каждой из них, в отличие от сегодняшней системы, когда компании облагаются налогом только в стране своей основной «прописки». Предложение Байдена похоже, но в нем есть ряд ключевых отличий, таких как требование соблюдения новых правил широким кругом коммерческих организаций. Время покажет, чем обернутся эти предложения и что корпорации предпримут, чтобы хакнуть их, как это было со всеми предыдущими новшествами.

Иногда страны сами провоцируют такой юрисдикционный арбитраж, намеренно нарушая собственные законы, чтобы привлечь глобальную клиентуру. Например, система регистрации судов под «удобными флагами» позволяет судовладельцам обходить правила технического обслуживания судов, игнорировать трудовые законодательства и уклоняться от судебного преследования за нанесение ущерба окружающей среде, например за разливы нефти. Исторически корабли всегда ходили под флагом своей страны, что обеспечивало им государственную защиту, но в то же время подчиняло законам этой юрисдикции. В начале XX в. Панама разрешила любому желающему поднимать свой флаг за определенную плату. Либерия, Сингапур и ряд других стран быстро переняли этот опыт, а для микрогосударств с выходом к морю и небогатых природными ресурсами, таких как республика Вануату, он стал настоящим шансом. Судовладельцам пришелся по душе такой хак, поскольку в этих странах законодательные системы были неразвиты, а сами законы не отличались строгостью. В период с 1950-х по 2010-е гг. число судов в таких «открытых реестрах» выросло с 4 до 60 % мирового флота. В Конвенции ООН по морскому праву 1994 г. сказано, что между судном и его флагом должна существовать «реальная связь», однако и 25 лет спустя после принятия Конвенции толкование этой фразы все еще остается предметом споров.

По этой же причине корпорации предпочитают регистрироваться в штате Делавэр. Штат впервые начал адаптировать свое налоговое законодательство в конце XIX в., внося изменения, чтобы привлечь бизнес из более крупных и процветающих штатов, таких как Нью-Йорк. Делавэр стал «оншорной» налоговой гаванью для американских компаний не только из-за простоты ведения бизнеса, но и благодаря «делавэрской лазейке»[150]: штат взимает нулевой налог с доходов, связанных с нематериальными активами, принадлежащими холдинговым компаниям из Делавэра. Это позволяет компаниям переводить роялти и подобные доходы[151] из мест, где они фактически ведут бизнес, в холдинговые компании в Делавэре, чтобы не платить с них налогов. Однако это означает потерю миллионов долларов для штатов, в которых корпорации реально осуществляют свою деятельность. Эта лазейка обходится остальным 49 штатам[152] примерно в $1 млрд в год.

И дело не в том, что компании регистрируют свои суда в Панаме или сами

---

150 The Institute on Taxation and Economic Policy (Dec 2015), «Delaware: An onshore tax haven,» https://itep.org/delaware-an-onshore-tax-haven/.

151 Patricia Cohen (7 Apr 2016), «Need to hide some income? You don't have to go to Panama,» *The New York Times* , https://www.nytimes.com/2016/04/08/business/need-to-hide-some-income-you-dont-have-to-go-to-panama.html.

152 Leslie Wayne (30 Jun 2012), «How Delaware thrives as a corporate tax haven,» *The New York Times* , https://www.nytimes.com/2012/07/01/business/how-delaware-thrives-as-a-corporate-tax-haven.html.

прописываются в Делавэре. Хак заключается в преднамеренном использовании этими юрисдикциями нормативных актов таким образом, чтобы повысить свою привлекательность для бизнеса. Противопоставляя себя другим штатам, Делавэр подрывает цели федеральных правил торговли и налоговых органов каждого из штатов в отдельности. Точно так же «удобные флаги» подрывают смысл Конвенции ООН по морскому праву.

Все это примеры хаков, которые стали возможными благодаря тому, что географическое присутствие организаций намного шире, чем полномочия органа, призванного их регулировать. Корпорации обычно ведут бизнес не только в штате Делавэр, но и далеко за его пределами. Морские судоходные компании действуют по всему миру, а не ограничиваются перевозками для Панамы. Сейчас мы можем то же самое наблюдать на примере крупных технологических компаний. Ни одно государственное учреждение не обладает регуляторными возможностями, сопоставимыми с масштабом их деятельности. Такие компании, как Facebook, являются глобальными, но регулирующие их нормативные акты действуют на национальном уровне. Регулирующих структур, подходящих для информационной эпохи, еще просто не существует, и это позволяет компаниям извлекать выгоду из юрисдикционного арбитража.

32
Административное бремя

Иногда хак – это продукт необходимости, порожденный трудностями и задачами вынужденной адаптации. Если какая-то тактика не работает, вы пробуете другую. Этот подход стал причиной возникновения такого явления, как *административное бремя* . Оно используется как хакерский метод в сфере политики. В частности, подходит для взлома систем социальных пособий, таких как страхование по безработице или Medicaid [153] , которые часто вызывают в Америке политические разногласия. Противники этих инициатив сначала пытаются просто запретить их, но не всегда это выходит: может не хватить голосов или на пути встает досадное конституционное положение.

Тогда люди начинают креативить. Если вы отвечаете за реализацию закона, то можете сделать его очень, очень трудным для исполнения. Другими словами, вы можете закопать в бюрократических препонах тех, кто пытается воспользоваться нововведением, а значит, покончить и с самой политической инициативой. Тактики могут быть разными: длительные ожидания, чрезмерная бумажная волокита, громоздкие системы подачи документов, повторные личные собеседования, намеренно плохо сделанные веб-сайты. Цель при этом преследуется всегда одна: наложить настолько неподъемное бремя, что люди, имеющие право на получение пособия (многие из которых и так отягощены бедностью, плохим здоровьем, нехваткой образования и нестабильными жилищными условиями), будут просто не в состоянии справиться с такой задачей. Ученые в области государственной политики Памела Херд и Дональд Мойнихан назвали это явление *административным бременем* [154].

Хорошим примером может служить система страхования по безработице во Флориде [155] . По словам одного из советников губернатора Десантиса, система была специально разработана, «чтобы затруднить получение и сохранение пособий». Весь процесс

---

153 Medicaid – американская совместная программа федерального правительства и правительств штатов, которая предлагает дополнительные медицинские льготы для лиц с ограниченными доходами. – *Прим. пер* .

154 Pamela Herd and Donald P. Moynihan (2019), Administrative Burden: Policymaking by Other Means, Russell Sage Foundation.

155 Rebecca Vallas (15 Apr 2020), «Republicans wrapped the safety net in red tape. Now we're all suffering.» *Washington Post* , https://www.washingtonpost.com/outlook/2020/04/15/republicans-harder-access-safety-net.

подачи заявления был перенесен в онлайн-систему, которая намеренно функционирует кое-как. Аудит 2019 г. выявил, что система «часто выдавала неверные сообщения об ошибках» и то и дело полностью блокировала подачу заявлений [156]. Сама форма заявления занимает несколько страниц, поэтому после ввода одних данных, таких как имя и дата рождения, необходимо перейти на следующую страницу для ввода других, однако это часто приводит к сбою, что возвращает заявителя к исходной точке. Кроме того, сайт доступен только в определенные часы дня [157], а заявители обязаны каждые две недели заходить в систему, чтобы проверить статус своих заявлений.

Во время пандемии COVID-19 эта система причинила немало проблем и страданий 4,5 млн безработных жителей Флориды. В 2020 г. многие люди безуспешно тратили часы и даже дни[158], пытаясь подать заявления. По данным веб-сайта, 2,4 млн человек в конечном итоге были признаны не соответствующими требованиям непрозрачной системы штата, что ограничило их права на получение федеральной компенсации по безработице в связи с пандемией, предусмотренной Законом о помощи, поддержке и экономической безопасности в период коронавируса (CARES).

Отчасти административное бремя возникает из-за конфликта методов проведения той или иной политики. Когда вы разрабатываете систему, которая назначает пособие, вам приходится опасаться двух типов ошибок: одни могут не получить заслуженной помощи, а другие, наоборот, получить ее, хотя и не заслуживают этого. Минимизация шансов на любую из этих ошибок обязательно приводит к увеличению возможности появления другой. Если вы облегчите людям подачу заявления и получение пособия, вы также неизбежно облегчите их получение теми, кто этого не заслуживает. А если вы ужесточите процесс проверки, чтобы отбор был более точным, вы непременно откажете и некоторым справедливо подавшим заявление кандидатам. В зависимости от вашей политики вы предпочтете один исход другому.

Преднамеренное создание административного бремени доводит этот процесс до крайности. Вместо того чтобы отсеивать не имеющих право на получение пособия, административное бремя, связанное с этим, разрастается до такой степени, что многие люди, соответствующие требованиям, просто отказываются от него. По существу, это пассивно-агрессивный отказ в получении пособия.

Мы могли видеть, как эта тактика использовалась в течение 50 лет в США в отношении конституционного права на аборт. Когда штат не мог принять закон, запрещающий аборты напрямую, его сторонники переходили к использованию административного бремени, чтобы значительно усложнить доступ к этой медицинской услуге. Тактика включала в себя обязательные периоды ожидания, консультации, многократные посещения клиники, согласие родителей и ультразвуковые исследования. Крупнейшим хакером в этой теме была Луизиана[159], которая с 1973 г. ввела в действие 89 нормативных актов, касающихся абортов,

---

156 Vox staff (10 Jun 2020), «Why it's so hard to get unemployment benefits,» *Vox* , https://www.youtube.com/watch?v=ualUPur6iks.

157 Emily Stewart (13 May 2020), «The American unemployment system is broken by design,» *Vox* , https://www.vox.com/policy-and-politics/2020/5/13/21255894/unemployment-insurance-system-problems-florida-claims-pua-new-york.

158 Palm Beach Post Editorial Board (30 Nov 2020), «Where is that probe of the broken Florida unemployment system, Governor?», *Florida Today* , https://www.floridatoday.com/story/opinion/2020/11/30/where-probe-broken-florida-unemployment-system-governor/6439594002.

159 Elizabeth Nash (11 Feb 2020), «Louisiana has passed 89 abortion restrictions since Roe: It's about control, not health,» Guttmacher Institute.

включая обременительные требования к лицензированию клиник и правила, даже незначительные нарушения которых способны привести к их немедленному закрытию. Когда в 1992 г. Верховный суд США постановил [160], что штаты не могут «ставить существенные препятствия на пути женщины, которая хочет сделать аборт», борьба в течение последующих 30 лет перешла в другую плоскость: какие препятствия считать существенными, а какие нет.

Можно привести массу подобных историй. Программа «Женщины, младенцы и дети» (WIC) – это государственная программа питания, которая устанавливает невероятно громоздкие, подробные и до смешного сложные ограничения на то, какие именно продукты можно покупать в рамках программы. К примеру, не разрешается смешивать определенные марки детского питания. Административное бремя в этой программе работает эффективно: пособия WIC получают менее половины семей, имеющих на то право[161]. Аналогичным образом хакаются процессы подачи заявлений в Medicaid и получения талонов на питание. Арканзас, например, сумел выкинуть немало людей из списка участников программы Medicaid, когда ввел дополнительные требования к работе лишь для того, чтобы усложнить сбор документов.

Все это примеры того, как богатые и влиятельные люди взламывают системы в ущерб рядовым гражданам. И последствия этого наносят несоразмерный вред тем, кому не хватает навыков, ресурсов и времени для преодоления возведенных барьеров.

Без судебного вмешательства трудно найти удовлетворительное решение таких ситуаций, поскольку административное бремя создают политические власти. Тем не менее частично решить проблему помогут независимые контрольные показатели или системные аудиты, проводимые сторонними организациями для определения масштаба и влияния административного бремени. Это не устраняет проблемы, однако путем количественной оценки воздействия административного бремени на затронутые им группы (особенно на те из них, которые особо защищены законом) с помощью сбора, анализа и визуализации данных независимые аудиторы могут побудить законодателей к действию или создать давление на общество для принятия мер. Кроме этого, если честно, я не знаю, что еще можно сделать.

33
Хакинг и общее право

Системы, которые мы здесь обсуждаем, имеют тенденцию быть чересчур детализированными и при этом недоработанными, создавая каверзные проблемы. Это означает, что они слишком сложны для традиционных методов анализа[162]. Единственный работающий подход – итерационные решения, которые могут использовать хаки для самосовершенствования.

Хаки предполагают нарушение установленных правил системы. Но эти правила часто подлежат интерпретациям, которые могут меняться. Чтобы лучше понять это, давайте рассмотрим правовую систему, созданную, чтобы развиваться именно таким образом, –

---

160 US Supreme Court (29 Jun 1992), Planned Parenthood of Southern Pennsylvania v. Casey, 505 U.S. 833 (1992), https://www.oyez.org/cases/1991/91-744.

161 L. V. Anderson (17 Feb 2015), «The Federal Nutrition Program for Pregnant Women is a bureaucratic nightmare,» Slate, https://slate.com/human-interest/2015/02/the-wic-potato-report-a-symptom-of-the-bureaucratic-nightmare-that-is-americas-welfare-system.html.

162 Jon Kolko (6 Mar 2012), «Wicked problems: Problems worth solving,» Stanford Social Innovation Review, https://ssir.org/books/excerpts/entry/wicked_problems_problems_worth_solving.

общее право. Это, пожалуй, лучший пример большой системы (и модель для будущего), которая способна адаптироваться посредством итерационного хака. Хакинг встроен в саму конструкцию системы. И это действительно эффективно.

В 1762 г. писатель и школьный учитель Джон Энтик был заподозрен в написании клеветнических памфлетов против английского правительства. По указанию государственного секретаря главный посыльный короля с помощниками ворвался в дом Энтика, конфисковав сотни брошюр и черновиков в качестве улик. В результате Энтик подал в суд за вторжение на его землю, несмотря на статус правоохранителей и отсутствие прецедента.

Сегодня это не кажется хаком, но в 1765 г. это было самое настоящее непреднамеренное и непредвиденное использование закона о незаконном проникновении в частную собственность. До этого случая закон применялся только для предотвращения вторжения граждан, но еще никогда не ограничивал действия правительства. Полиция имела презумптивное право проводить обыски в частных владениях как одно из своих полномочий. Энтик утверждал, что его индивидуальное право быть в безопасности на собственной частной территории превыше этого. Он подорвал существующие нормы правоприменения. Это была прогрессивная и даже радикальная интерпретация закона.

Английские суды решили, что толкование закона[163] Энтиком является обоснованным и более совершенным. «По законам Англии любое вторжение в частную собственность, даже незначительное, является посягательством». Постановление по делу Энтика распространило концепцию ответственности за незаконное проникновение даже на государственного секретаря и его заместителей. С этого момента она стала частью английского общего права. Энтик хакнул закон о незаконном проникновении. Он выдвинул толкование, которое логически вытекало из слов закона, но было непреднамеренным и непредвиденным. Суд нормализовал хак, закрепив его в законе. Дело Энтика стало знаковым в установлении гражданских свобод и ограничении сферы действия государственной власти. В США аналогичные делу Энтика решения закреплены в Четвертой поправке.

Иногда хаки бывают полезными. Он может нарушить цель существующего правила или нормы, но при этом не подрывает более широкий общественный договор. В приведенном выше примере суд счел, что гарантии неприкосновенности граждан в их частных владениях независимо от причин, побуждающих их нарушить, пойдут только на пользу общественному договору и придадут ему дополнительную силу. Да, хак приносит пользу хакеру за счет системы, но в отдельных случаях эти потери могут быть минимальными. Если взлом соответствует духу общественного договора, то он становится полезной для системы инновацией.

В подобных случаях в системе общего права решение принимает не какой-нибудь один руководящий орган, а множество судов. Они пытаются согласовать разнообразные интерпретации многих прецедентов, чтобы в дальнейшем применить их к новым хакам по мере появления оных. Нормы общего права представляют собой некое хаотичное множество – сложное, неполное, а порой и противоречивое. Они не разработаны с определенной целью, как традиционное законодательство. Они итеративны и непрерывно развиваются. Свод правил дополняют и корректируют разные люди, каждый из которых преследует собственные цели в общей системе. В системах, управляемых множеством людей, для решения проблем и смещения статус-кво нужен именно такой механизм, и у нас есть его действующий прототип – общее право.

Вот краткое определение: общее право – это право, полученное из судебных решений в форме юридических прецедентов. Оно отличается от статутного права, которое принимается законодательными органами, и от нормативного права, которое устанавливается органами государственными. Общее право более гибко, чем статутное

---

163 England and Wales High Court (King's Bench), Entick v. Carrington (1765), EWHC KB J98 1066.

право. Оно обеспечивает согласованность судебных решений во времени, но при этом может развиваться по мере того, как судьи повторно применяют, проводят аналогии и интерпретируют прошлые прецеденты в соответствии с новыми обстоятельствами. Эта эволюция, по сути, представляет собой бесконечную череду хаков, которые либо признаются незаконными, либо становятся новыми прецедентами.

Возьмем для рассмотрения патентное право. Оно основано на статутном праве, но детали определяются правилами, которые устанавливают судьи. И это действительно сложная система. Патенты могут стоить миллиарды, и судебные иски в этой сфере – обычное дело. Поскольку на карту поставлено много денег, система часто подвергается хакерским атакам. Я приведу лишь один пример: судебные запреты на использование патентов. Идея таких запретов заключается в том, что человек, чей патент нарушается, может получить быстрый судебный запрет, препятствующий этому нарушению, пока суд не вынесет окончательный вердикт. До 2006 г. такие запреты получить было несложно. В результате они стали популярным средством конкурентной борьбы между крупными компаниями, особенно технологическими. Запреты на использование патента применялись для того, чтобы заставить более мелких конкурентов либо прекратить продажу своей продукции, либо выплатить непомерно высокие роялти владельцу патента (практика, которую многие сравнивают с вымогательством).

Судебное разбирательство по делу о запрете использования патентов[164] состоялось, когда компания MercExchange, специализирующаяся на технологиях и интернет-аукционах, подала в суд на eBay, утверждая, что eBay нарушает ее патенты в своей системе онлайн-аукционов. В 2006 г. Верховный суд США рассмотрел это дело и переписал правила запрета на использование патентов, устранив уязвимость. В частности, судам было предписано применять более строгую четырехфакторную проверку при принятии решения о таких запретах.

Законы никогда не бывают полными. С течением времени на фоне изменений в обществе становятся очевидными серые зоны, слепые пятна и пустоты в законах. Лазейки, упущения или ошибки могут встречаться как в статутном, так и в общем праве. Кто-то хакает существующий закон, чтобы заполнить пустоты непреднамеренным и не предвиденным его создателями способом и получить таким образом некое преимущество. Затем кто-то другой – как правило, поставленный хаком в невыгодное положение – оспаривает этот взлом в суде. Судья выступает в качестве нейтрального арбитра и должен решить, является хак законным или нет. Если он нелегитимен, то объявляется незаконным, и это эффективно исправляет систему. Если же он легитимен, то становится частью общего права. Общее право по своей сути является одним большим хаком судебной системы, а его решения, основанные на творческом применении и переосмыслении широких прецедентов и принципов, сами по себе являются социальным хаком для преодоления неразрешимых проблем.

Хакинг – это про то, как закон адаптируется к новым обстоятельствам, новым событиям и новым технологиям. Никто в профессиональной юридической сфере не называет этот процесс хакингом, но дела обстоят именно так. Общее право – это не что иное, как череда хаков и судебных решений по ним. Это лучшая из имеющихся у нас систем, которая позволяет использовать возможности хакинга для постоянного совершенствования закона.

Вот еще один пример. В Средние века, когда землевладельцы в Англии отправлялись воевать в Крестовые походы, они часто передавали титул, а вместе с ним и право собственности на землю доверенному лицу из числа дворянства. Идея заключалась в том, что, пока человек отсутствует, доверенное лицо сможет позаботиться о его собственности

---

164 US Supreme Court (15 May 2006), eBay Inc. v. MercExchange, LLC, 547 U.S. 388, https://www.supremecourt.gov/opinions/05pdf/05-130.pdf.

и обеспечить выполнение регулярных обязательств, таких как феодальные сборы. Однако не всегда это заканчивалось хорошо. Известны случаи, когда крестоносец, вернувшийся из похода, обнаруживал, что его доверенное лицо отказывается возвращать титул. Это была лазейка в законе, ведь в намерения крестоносца не входила продажа или тем более отказ от имущества.

Обескураженные крестоносцы обращались в таких случаях к лорд-канцлеру и его Канцлерскому суду. Решение, которое устранило лазейку, заключалось в создании нового права. По замыслу, отныне у собственности могло быть два владельца: законный владелец – лицо, указанное в титуле, – и справедливый собственник – лицо, которое управляло земельными наделами и фактически пользовалось преимуществами собственности. В данном случае законным владельцем был крестоносец, а справедливым собственником – доверенный управляющий. Это был идеальный патч, поскольку желания заинтересованных сторон были согласованны: и дворяне сохраняли свое право собственности, и ходатайства вернувшихся крестоносцев были удовлетворены.

Сегодня такое же разделение прав сохраняется во многих странах, где работают системы общего права. В США до сих пор существует разделение на вопросы права и вопросы справедливости. Такое деление позволяет использовать в качестве финансовой структуры траст. По сути, трастом (и его активами) владеет кто-то другой, в то время как вы, «настоящий» владелец и бенефициар, имеете право на плоды, приносимые активами траста (к примеру, на денежные выплаты).

34
Хакинг как эволюция

Ортодоксальные евреи – мастера взламывать свои религиозные правила. В Шаббат, который длится с вечера пятницы до вечера субботы, работать категорически запрещено. Понятие работы изначально включало в себя разжигание огня, но позже было расширено до любых действий, связанных с использованием электричества. В детстве у моих двоюродных братьев был таймер, прикрепленный к шнуру питания телевизора. Он включал и выключал его по субботам автоматически, не требуя от человека никаких действий. Единственная проблема заключалась в том, чтобы договориться до заката в пятницу, на какой канал настроить телевизор. Носить с собой в общественных местах какие-либо вещи кроме одежды и украшений в Шаббат тоже запрещено, поскольку считается работой. Это означает, что когда вы выходите на улицу, то не можете взять с собой даже ключ от дома. Однако если этот ключ встроен в украшение, на которое запрет не распространяется, то можно взять его с собой без проблем.

Переносить вещи внутри своего дома в Шаббат разрешено, поэтому некоторые общины растягивают вокруг района длиннющий моток проволоки[165], называемый *эрув* , и этим хакают древнее понятие дома, переопределяя его таким образом, чтобы оно включало в себя все, что находится внутри этой проволочной ограды.

На неевреев эти правила не распространяются. Синагога, в которую я ходил в детстве, специально наняла сторожа-нееврея, чтобы он мог делать в Шаббат то, что не могут евреи. При этом прямо просить о помощи в Шаббат тоже запрещено. То есть нельзя произнести что-то вроде: «Не могли бы вы включить обогреватель?», – но очень даже можно прозрачно намекнуть: «Кажется, здесь немного холодно». Точно так же чтущий субботу еврей не может войти в лифт и попросить нееврея нажать кнопку пятого этажа, но он может спросить: «Нажата ли кнопка пять?» Сегодня многие лифты в религиозных районах Израиля запрограммированы таким образом, чтобы в Шаббат останавливаться на каждом этаже

---

165 M. Olin (2019), «The Eruv: From the Talmud to Contemporary Art,» in S. Fine, ed., Jewish Religious Architecture: From Biblical Israel to Modern Judaism, Koninklijke Brill NV.

автоматически[166].

Когда я был ребенком, подобные способы неукоснительно следовать букве закона и нарушать при этом его дух казались мне противоестественными. Но на самом деле благодаря такому подходу 3000-летний еврейский закон на протяжении веков адаптировался к современности. Это чистейший хакинг и, что еще более важно, интеграция с помощью хаков в наше непрерывно развивающееся общество.

Хакинг всегда сосредоточен на поиске уязвимостей, которые еще не были использованы. И когда этот поиск увенчивается успехом, часто он приводит к неожиданным результатам.

Этот момент крайне важен. Хакинг не просто злонамеренное манипулирование системой. Успешный хак меняет взломанную систему – тем более тогда, когда становится популярным и применяется многократно. Он меняет работу системы либо потому, что система получает исправления, призванные предотвратить хак, либо потому, что она расширяется, чтобы принять его в себя. Хакинг – это процесс, посредством которого те, кто использует систему, меняют ее к лучшему в ответ на появление новых технологий, новых идей и новых взглядов на мир. В этом и состоит эволюционная роль хакинга. Мы наблюдали ее на примерах современного банковского дела, высокочастотной торговли, элитной недвижимости, компаний гиг-экономики. И эта эволюция продолжается прямо сейчас. Недавно появилось Bluetooth-устройство[167], которое делает мобильный телефон пригодным для использования в Шаббат. Суть хака заключается в том, что через кнопки постоянно проходит небольшой ток, поэтому нажатие на них не замыкает цепь, что делает его допустимым по еврейским законам.

При правильном подходе хакинг – это способ ускорить эволюцию системы за счет вовлечения в процесс противника, а при неправильном – ускорить разрушение системы, выявляя и используя ее недостатки в корыстных целях.

Инновации необходимы системам, если они хотят выжить. Закостенелая система не способна реагировать на взломы, и потому ей трудно развиваться. Политолог Фрэнсис Фукуяма приводит этот аргумент, когда размышляет на тему того, что и государства, и общественные институты развиваются, если реагируют на определенные условия окружающей среды[168], и терпят крах или завоевываются, если не могут эволюционировать в соответствии с внешними изменениями. (В качестве примера он использует Османскую империю.) Современные политологические исследования показывают, что, когда консервативные группы, представляющие привилегированный класс, запрещают обществу эволюционировать[169], они постепенно разрушают политические системы в целом.

Однако эта разрушительная сила может быть использована и теми, кто находится в самом низу пирамиды власти, и стать двигателем социальных изменений. Именно так

---

166 Elizabeth A. Harris (5 Mar 2012), «For Jewish Sabbath, elevators do all the work,» *The New York Times* , https://www.nytimes.com/2012/03/06/nyregion/on-jewish-sabbath-elevators-that-do-all-the-work.html.

167 JC staff (12 Aug 2010), «Israeli soldiers get Shabbat Bluetooth phone,» https://www.thejc.com/news/israel/israeli-soldiers-get-shabbat-bluetooth-phone-1.17376.

168 Francis Fukuyama (2014), Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy, Farrar, Straus & Giroux.

169 Yoni Appelbaum (Dec 2019), «How America ends,» Atlantic, https://www.theatlantic.com/magazine/archive/2019/12/how-america-ends/600757. Uri Friedman (14 Jun 2017), «Why conservative parties are central to democracy,» Atlantic, https://www.theatlantic.com/international/archive/2017/06/ziblatt-democracy-conservative-parties/530118. David Frum (20 Jun 2017), «Why do democracies fail?» Atlantic, https://www.theatlantic.com/international/archive/2017/06/why-do-democracies-fail/530949.

происходят революции. Хакинг – это еще и оружие обездоленных. И оружие мощное.

Приведу пример. Люди ищут способы взломать понятие корпоративной личности, пытаясь отстоять права животных, на которых проводят тесты, или загрязняемых предприятиями рек. Сама концепция корпоративной личности [170] – это тоже хак Четырнадцатой поправки, в которой изложены права граждан и их политические свободы.

В дарвиновской картине мира мать-природа решает, какие из хаков останутся, а какие исчезнут. Она может быть жестокой, но эволюция – это не игра в любимчиков. Эволюция же социальных систем имеет своих фаворитов, облеченных властью, которые зачастую сами решают, какой хак оставить, а от какого избавиться. Если это не исправить и позволить правящей элите управлять эволюцией систем, мы увековечим несправедливость. Будущее социального хакинга должно сочетать в себе стремление к эволюции с ориентацией на общее благо, иначе наши социальные системы начнут разрушаться. И тогда место хакинга займет революция.

Возможно, лучшей метафорой для хакинга может послужить понятие инвазивного вида. Разные виды развиваются в разных условиях, по-разному сбалансированных по таким факторам, как хищники, добыча, состав окружающей среды и т. п. Когда представитель вида попадает из привычной ему среды в какую-то другую, он может воспользоваться отличиями весьма неожиданными способами. Возможно, в новой среде нет хищника, который раньше сдерживал его популяцию, и никакая другая сила в природе не может занять его место (как это произошло с бирманским питоном во Флориде). А может быть, отсутствует экологический фактор, игравший такую же роль (например, холодная погода для пуэрарии – растения семейства бобовых, ставшего настоящим бичом южных штатов). Или новый источник пищи неестественно обилен (как в случае с прожорливым азиатским карпом). В результате инвазивный вид способен размножаться с невиданной доселе скоростью. Хаки подобны этому. Они представляют собой скачки возможностей, внедренные в систему, которая к этому не готова. Инвазивный вид может вымереть, если экосистема развернет правильную защиту. Но он также может спровоцировать перегрузку экосистемы. Катастрофическое конечное состояние называется «коллапсом экосистемы», когда хак настолько разрушителен, что уничтожает ее полностью.

Часть V
Хакинг политических систем

35
Скрытые положения в законодательстве

Когда российская Служба внешней разведки взломала компанию SolarWinds и внедрила бэкдор в обновление программного обеспечения Orion, 17 000 или около того пользователей установили это поврежденное обновление и непреднамеренно предоставили СВР доступ к своим сетям. Это огромное количество сетей, и совершенно немыслимо, чтобы СВР попыталась проникнуть в каждую из них. Вместо этого она тщательно перебирала содержимое своего улова, отбирая наиболее ценные и перспективные жертвы.

Такой прием известен как «атака по цепочке поставок». СВР атаковала не какую-то одну из сетей, а программную систему, которую использовали все эти сети. Атака по цепочке поставок – это умный способ атаковать системы, поскольку она может затронуть тысячи людей одновременно. Другие примеры такого рода атак: взлом магазина Google Play с целью размещения в нем поддельного приложения или перехват сетевого оборудования

---

[170] Adam Winkler (5 Mar 2018), « 'Corporations are people' is built on an incredible 19th– century lie,» Atlantic, https://www.theatlantic.com/business/archive/2018/03/corporations-people-adam-winkler/554852.

в системе почты для установки подслушивающих устройств[171] (этим занимается АНБ).

Аналогичным образом можно представить себе хакинг законодательного процесса. В предыдущих главах мы познакомились с тем, как хакеры находят и используют уязвимости в законах после их принятия. Но хакеры могут атаковать и сам законодательный процесс. Подобно взлому обновления программного обеспечения для управления сетью Orion хакеры могут намеренно внедрять уязвимости в готовящееся законодательство и использовать их в своих интересах, если оно будет принято.

В некотором смысле это более высокий уровень хакерских атак. Вместо того чтобы находить уязвимости в законах и нормативных актах, такой хакинг направлен против самого процесса создания законов и нормативных актов. Только по-настоящему сильные хакеры могут делать такие вещи.

Это не просто взлом системы. Это взлом средств ее исправления.

Лазейки в законах – явление распространенное, но большинство из них не квалифицируются как хаки. Это преднамеренные исключения из более общего правила, созданные для поддержки определенной политической цели, спокойствия конкретных групп избирателей или в качестве компромисса между самими законодателями. Для примера можно привести закон 2004 г., пролоббированный компанией Starbucks[172], который признает обжарку кофейных зерен внутренним производством со всеми вытекающими, или, на более общем уровне, антимонопольные исключения в отраслях, требующих координации между участниками[173], например в спортивных лигах. Эти меры не являются непреднамеренными и непредвиденными. Они не пытаются перехитрить систему создания, обсуждения и принятия законов. Как таковые они не являются хаками.

Но это не означает, что законодательный процесс, создающий эти лазейки, не взламывается постоянно. Все, что необходимо для такого хака, – это добавить в законопроект стратегически продуманное и точно сформулированное предложение. Это предложение может ссылаться на другие законы, а уже их взаимодействие может привести к определенному, непредвиденному для всех результату.

Целая индустрия лоббистов от лица своих спонсоров занимается разработкой таких непредвиденных результатов. В 2017 г. в процессе разработки Закона о сокращении налогов и увеличении занятости более половины вашингтонских лоббистов сообщили, что они работают исключительно над налоговыми вопросами. Это более 6000 профессионалов, то есть в среднем по 11 лоббистов на каждого члена конгресса[174].

Например, долговое соглашение 2013 г., принятое конгрессом, включало следующую формулировку: «SEC. 145. В подраздел (b) статьи 163 Публичного закона 111–242 с поправками внесены дополнительные изменения: "2013–2014" меняется на "2015–2016"». Это, казалось бы, безобидное положение, внесенное сенатором Томом Харкином, оказалось

---

171 S. Silbert (16 May 2014), «Latest Snowden leak reveals the NSA intercepted and bugged Cisco routers,» Engadget, https://www.engadget.com/2014-05-16-nsa-bugged-cisco-routers.html.

172 Ben Hallman and Chris Kirkham (15 Feb 2013), «As Obama confronts corporate tax reform, past lessons suggest lobbyists will fight for loopholes,» *Huffington Post*, https://www.huffpost.com/entry/obama-corporate-tax-reform_n_2680880.

173 Leah Farzin (1 Jan 2015), «On the antitrust exemption for professional sports in the United States and Europe,» Jeffrey S. Moorad Sports Law Journal 75, https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1321&context=mslj.

174 Taylor Lincoln (1 Dec 2017), «Swamped: More than half the members of Washington's lobbying corps have plunged into the tax debate,» Public Citizen, https://www.citizen.org/wp-content/uploads/migration/swamped-tax-lobbying-report.pdf.

скрытым подарком для Teach For America[175][176]. По сути, эта поправка продлила на два года действие другого законодательного акта, от которого выигрывали студенты, участвующие в программах подготовки учителей, в том числе рекруты Teach For America.

В 2020 г. конгресс принял Закон о помощи, поддержке и экономической безопасности в период коронавируса (CARES) на $2 трлн о мерах стимулирования экономики в условиях пандемии. На странице 203 законопроекта было внесено изменение, согласно которому инвесторы в недвижимость могли компенсировать свои убытки[177]. Эта налоговая льгота принесла магнатам недвижимости, таким как действующий на тот момент президент Дональд Трамп, прибыль в размере $17 млрд в год, которые могли стать налоговыми поступлениями. Положение не имело никакого отношения к COVID-19, а налоговая льгота, имевшая обратную силу, охватывала период, начинавшийся задолго до появления коронавируса. Спешка и скрытность помогли протащить это положение в законопроект. Его текст был окончательно доработан менее чем за час до голосования, что позволило республиканцам, входившим в рабочую группу законопроекта, добавить нужное положение буквально в последний момент.

Главная уязвимость законодательного процесса состоит в том, что законопроекты – это чрезвычайно большие и сложные документы, которые содержат множество положений без четко обозначенных последствий. Эксплойт внедряется в законопроект таким образом, чтобы законодатели этого не заметили. Нам кажется, что для такого рода махинаций требуется соучастие члена конгресса, который осознает последствия своего вклада в законопроект, но на самом деле внедрить эксплойт способен и рядовой сотрудник, не понимая того, что делает, и даже лоббист, разрабатывающий формулировку, которая в итоге попадет в текст закона.

Это настолько распространенная практика[178], что язык не поворачивается назвать ее хакингом. За последние десятилетия власть все больше концентрировалась в руках лидеров политических партий в каждой из палат в ущерб законодательным комитетам, что способствовало установлению закрытого и непрозрачного законодательного процесса. Такое положение дел в сочетании с тем, что конгресс стал принимать меньше крупных законопроектов по сравнению с прошлыми сессиями, дает широкие возможности для внедрения скрытых положений, выгодных привилегированному классу и отраслям. Эта ситуация даже обыгрывается в одном из эпизодов «Симпсонов», когда клоун Красти избирается в конгресс [179] и протаскивает поправки в закон об управлении воздушным движением через законопроект об обеспечении флагами сирот.

Исправлять подобные хаки непросто. Несмотря на то что юридический текст устроен

---

175 Teach For America – американская некоммерческая организация, привлекающая студентов и выпускников университетов для преподавания в районах США с низким уровнем доходов населения. – *Прим. пер* .

176 Valerie Strauss (16 Oct 2013), «The debt deal's gift to Teach For America (yes, TFA),» *Washington Post* , https://www.washingtonpost.com/news/answer-sheet/wp/2013/10/16/the-debt-deals-gift-to-teach-for-america-yes-tfa.

177 Jesse Drucker (26 Mar 2020), «Bonanza for rich real estate investors, tucked into stimulus package,» *The New York Times* , https://www.nytimes.com/2020/03/26/business/coronavirus-real-estate-investors-stimulus.html. Nicholas Kristof (23 May 2020), «Crumbs for the hungry but windfalls for the rich,» *The New York Times* , https://www.nytimes.com/2020/05/23/opinion/sunday/coronavirus-economic-response.html.

178 GOP congressional aide Billy Pitts said in 2017: «What got snuck into there? What got airdropped into there in conference or whatever? That's always the threat of a big, fat bill – there's always something hidden inside of it.» https://www.npr.org/2017/03/11/519700465/when-it-comes-to-legislation-sometimes-bigger-is-better.

179 Matt Groening and J. L. Brooks (11 Feb 1996), «Bart the fink,» The Simpsons, Season 7, episode 15, Fox Broadcasting Company/YouTube, https://www.youtube.com/watch?v=hNeIkS9EMV0.

аналогично компьютерному коду, процессы их написания и применения заметно отличаются друг от друга. Компьютерный код пишет группа людей в соответствии с общим планом, как правило, под руководством одной компании или конкретного человека. Программисты четко понимают, что должен делать их код, в каких случаях он не должен этого делать, а в каких – не может сделать то, что должен. И только они имеют право исправлять ошибки в своем коде.

Законотворчество устроено иначе. Оно децентрализованно на каждом из уровней. В демократическом обществе закон пишется представителями разных конкурирующих сил. У них разные цели и разные мнения о том, что должен делать закон. Даже если все хорошо понимали, за что они голосовали, в тексте больших законопроектов неизбежны лазейки, которые одни законодатели назовут ошибкой, а другие воспримут как полезную фичу.

Скрытые положения и уязвимости, которые они представляют, были бы меньшей проблемой, если бы правила палаты представителей и сената предусматривали некое минимальное количество времени для рассмотрения законопроекта, возможно пропорциональное объему документа, после того как его текст был окончательно доработан и опубликован. Скрытые положения перестают быть скрытыми, если они обнаружены, тщательно изучены и преданы огласке активными СМИ в такой срок до принятия закона, чтобы подстегнуть изменения или как-то компенсировать политические издержки. Предоставление разумного минимального количества времени для рассмотрения резонансных законопроектов и требования поправок к ним дают некоторый шанс обнаружить скрытые положения, которые в противном случае не будут выявлены.

В рамках 97 рекомендаций по оптимизации работы палаты представителей США[180] Специальный комитет по модернизации конгресса предложил в 2019 г. «разработать новую систему, которая позволит американскому народу легко отслеживать, как именно поправки изменяют законодательство и какое влияние предлагаемые законопроекты окажут на действующий закон». По сути, такая система отслеживания изменений в законодательстве расширяет более ранний проект под названием Comparative Print Project.

Цель этой инициативы состоит в том, чтобы облегчить[181] просмотр и понимание законодательных изменений, что, в свою очередь, способствует обнаружению скрытых положений. Это, конечно, не решит проблему, в том числе потому, что комитет предлагает открыть информационный доступ только к «офисам палаты представителей», но в любом случае это был бы шаг в правильном направлении. Подобный ресурс, доступный для общества, в сочетании с мерами по обеспечению достаточного времени для рассмотрения законодательных актов может стать еще более действенным.

Но просто выделить время недостаточно; необходимо стимулировать людей, чтобы они искали в законопроектах скрытые положения. Взяв за пример систему bug bounty, используемую при разработке программного обеспечения, мы могли бы создать некий ее аналог, позволяющий гражданам получать вознаграждение за обнаруженные лазейки в законах, готовящихся к принятию. Наиболее очевидным полем для такого рода системы могут служить законы с налоговыми последствиями – вознаграждение могло бы составлять небольшой процент от ожидаемых (благодаря закрытию лазейки) налоговых поступлений.

В качестве альтернативы имеет смысл использовать опыт «красных команд»

---

180 Select Committee on the Modernization of Congress (2019), «116th Congress recommendations,» https://modernizecongress.house.gov/116th-recommendations.

181 Select Committee on the Modernization of Congress (2019), «Finalize a new system that allows the American people to easily track how amendments change legislation and the impact of proposed legislation to current law,» *Final Report*, https://modernizecongress.house.gov/final-report-116th/chapter/recommendation/finalize-a-new-system-that-allows-the-american-people-to-easily-track-how-amendments-change-legislation-and-the-impact-of-proposed-legislation-to-current-law.

применительно к законопроектам: специализированные группы, играющие роль частных компаний или правящих элит, должны хакать готовящееся законодательство и обнаруживать ранее неизвестные уязвимости.

Хотя оба этих подхода могут оказаться полезны, они сталкиваются с основной проблемой современного законотворчества, а именно с тем фактом, что законопроекты часто пишутся в обстановке секретности относительно небольшим числом законодателей и лоббистов и многие лазейки в них создаются намеренно. Представьте себе, что «красная команда» находит уязвимость в налоговом законопроекте. Это ошибка или особенность, баг или фича? Кому решать? И на каком основании? Кроме того, многие законопроекты принимаются конгрессом сразу после их публикации, что делает невозможным внимательное прочтение документов, тогда как «красной команде» для работы и принятия мер на ее основе требуется время.

Например, Закон о сокращении налогов и увеличении занятости 2017 г. был поставлен на голосование всего через несколько часов после того, как законодатели бегло ознакомились с его окончательным текстом. Это было сделано намеренно: авторы не хотели, чтобы у профессионалов было достаточно времени для тщательного изучения законопроекта. Аналогичным образом Закон о помощи, поддержке и экономической безопасности в период коронавируса (CARES) был опубликован [182] в 14:00 21 декабря 2020 г. Несмотря на то что законопроект насчитывал 5593 страницы, он был принят в палате представителей вечером того же дня, около 21:00, а уже к полуночи прошел голосование и в сенате. Законопроект содержал, к примеру, положения о малоизученных «налоговых расширениях» и постоянном снижении стоимости акцизов для «производителей пива, вина и дистиллированных спиртных напитков», что, по оценкам, обошлось казне в $110 млрд[183]. Многие законодатели просто не знали о многочисленных налоговых лазейках, которыми пестрел документ.

Возможно, нам придется подождать, пока искусственный интеллект со свойственной ему нечеловеческой скоростью научится читать, понимать и идентифицировать потенциальные хаки еще до того, как будут приняты законы. Это поможет решить проблему, хотя, несомненно, создаст другие.

36
Законопроекты «под прикрытием»

Одни законопроекты важнее других. Законопроекты об ассигнованиях или те, что являются реакцией на стихийные бедствия, пандемии или угрозу национальной безопасности, считаются обязательными к принятию. Эти законопроекты дают законодателям возможность протолкнуть положения, которые сами по себе никогда бы не прошли, но важны в политическом плане. Образно их называют *райдерами* , или наездниками. Райдеры часто непопулярны, противоречат общественным и обслуживают чьи-то узкие интересы или являются результатом политических махинаций и сделок.

Внедрение неуместных райдеров в эти обязательные для прохождения законодательные акты позволяет законодателям избежать внимания или негативной реакции, которая была бы неизбежна в случае отдельного голосования за политически спорное положение. Этот ставший уже обычным хак подрывает сам принцип законотворчества, когда

---

182 Mia Jankowicz (22 Dec 2020), « 'It's hostage-taking.' AOC lashed out after lawmakers got only hours to read and pass the huge 5,593-page bill to secure COVID-19 relief,» Business Insider, https://www.businessinsider.com/aoc-angry-representatives-2-hours-read-covid-19-stimulus-bill-2020-12.

183 Yeganeh Torbati (22 Dec 2020), «Tucked into Congress's massive stimulus bill: Tens of billions in special-interest tax giveaways,» *Washington Post* , https://www.washingtonpost.com/business/2020/12/22/congress-tax-breaks-stimulus.

вносятся отдельные предложения, а затем ставятся на голосование.

Приведу три примера.

● В период с 1982 по 1984 г. к нескольким законопроектам об ассигнованиях, подлежащих обязательному прохождению, был внесен ряд дополнений, названных поправкой Боланда; поправка ограничивала помощь США подразделениям «Контрас» в Никарагуа.

● В 2016 г. в законопроект о расходах на сельское хозяйство и продовольствие была включена поправка, запрещающая Управлению по санитарному надзору за качеством пищевых продуктов регулировать «сигары большого размера и сигары премиум-класса».

● В 2021 г. законодатели внедрили три законопроекта об авторском праве на интеллектуальную собственность в совершенно не связанный с ними Закон о консолидированных ассигнованиях. Рассмотрение этих мер зачахло на фоне активных протестов со стороны сторонников технологического прогресса и технологических компаний, но они были приняты, оказавшись в одном пакете с гораздо более крупным, сложным и обязательным к прохождению законопроектом.

Этот вид хака использует очевидный факт, что президент не может наложить вето на отдельные статьи законопроекта: он либо накладывает вето на весь законопроект, либо принимает его как есть, со всеми поправками и райдерами. Хак также использует уязвимость на уровне комитетов конгресса. Законодательное собрание в полном составе не может голосовать по законопроекту, если он не был одобрен соответствующими комитетами. Это означает, что члены комитетов могут просто вписывать райдеры в законопроект – тайно или даже открыто.

Попытки ограничить эту практику в основном оканчивались ничем. В 1996 г. конгресс предоставил президенту Клинтону право вето на отдельные пункты законопроекта, но уже в 1998 г. оно было признано неконституционным. За тот год, что оно работало, президент накладывал точечное вето 82 раза, после чего группой производителей картофеля, которые возражали против наложения вето на выгодный им райдер, был подан иск.

В модульном компьютерном коде каждый его независимый сегмент выполняет одну функцию. Такая структура делает программы отказоустойчивыми, удобными в обслуживании и диагностируемыми. Законодательство, которое по аналогии имеет дело с меньшим количеством дискретных вопросов, будет и менее подвержено описанному выше хаку. Эта логика стоит за концепцией узконаправленных законов и конституционных положений[184], которые требуют, чтобы законы касались только одной темы. Законопроект, получивший в 2021 г. рабочее название «Одна тема за раз», регулярно предлагался в конгрессе, но так и не был принят.

На уровне штатов усилия по противодействию райдерам оказались более эффективными. На сегодняшний день конституции 43 штатов требуют, чтобы каждый новый законодательный акт был ограничен одной темой. Конституция Миннесоты гласит[185]: «Законы должны охватывать только одну тему. Ни один закон не должен охватывать более одной темы, которая должна быть отображена в его названии». Однако даже эти ограничения могут легко взламываться. Как пишет профессор права Колумбийского университета Ричард Брифо, ответ на вопрос о том, «ограничен закон одной темой или нет, часто находится в глазах смотрящего». С одной стороны, как пояснил Верховный суд штата Мичиган, «нет практически ни одного закона, который нельзя было бы разделить и принять в виде нескольких законопроектов». С другой стороны, как сказано в одном из старых дел

---

184 US Congress (10 Apr 2019; latest action 20 May 2019), H.R. 2240: One Subject at a Time Act, 116th Congress, https://www.congress.gov/bill/116th-congress/house-bill/2240.

185 State of Minnesota (13 Oct 1857; revised 5 Nov 1974), Constitution of the State of Minnesota, Article IV: Legislative Department, https://www.revisor.mn.gov/constitution/#article_4.

Верховного суда Пенсильвании[186], «не существует двух настолько далеких друг от друга тем, что их нельзя было бы привести к общему знаменателю, отодвинув точку зрения достаточно далеко».

Еще один метод безопасности в этом вопросе – устойчивость системы. Законодательство, которое должно быть принято, особенно уязвимо для райдеров из-за крайне негативных последствий, связанных с непрохождением родительского закона. Однако некоторые из этих последствий, такие как остановка работы правительства из-за блокирования законопроекта об ассигнованиях, являются абсолютно искусственными и могут быть смягчены с помощью разумной политики. К примеру, несколько организаций предложили конгрессу[187] повысить устойчивость правительственных операций путем создания процесса автоматического принятия резолюций. В соответствии с ним, государственное финансирование будет продолжаться на сопоставимом уровне, если конгресс не сможет принять регулярный законопроект об ассигнованиях. Смягчая последствия отсрочки принятия законов, обязательных к прохождению, эта реформа облегчит противникам райдеров голосование против проекта бюджета до тех пор, пока райдеры не будут удалены из него.

37
Делегирование и отсрочка принятия законов

Спустя годы после окончания холодной войны конгресс все еще решал проблему закрытия военных баз по всей стране. Задача оказалась не из легких. Эти базы представляли собой тысячи рабочих мест, и ни один законодатель никогда не согласился бы на закрытие базы в своем округе. Вместо того чтобы принимать трудные решения, конгресс придумал хак, деполитизирующий процесс. Он передал свои законотворческие полномочия внешнему органу, создав Комиссию по реорганизации и закрытию баз. Эта комиссия была уполномочена решать, какие базы подлежат сокращению, а ее рекомендации автоматически вступали в силу, если конгресс не отменял их. И это сработало: начиная с 1988 г. создано пять таких комиссий, в результате чего более 350 военных объектов закрыто.

Этот хак до сих пор позволяет конгрессу решать сложные или политически спорные вопросы без необходимости принимать решения самому. Он снижает степень влияния партийной принадлежности и позволяет конгрессу обходить обременительные правила и процессы, замедляющие принятие решений.

Хак используется нечасто. В 2010 г. конгресс сформировал Независимый консультативный совет по платежам (IPAB), который должен был сократить расходы на Medicare[188]. Обычно для вступления в силу подобных изменений требуется акт конгресса, но он уполномочил этот совет вносить изменения, которые могли быть отменены только квалифицированным большинством голосов конгрессменов. Опять же, целью такого хакинга было уйти от ответственности за разработку и проведение фактического голосования по проекту сокращения расходов на Medicare. В отличие от комиссии по закрытию базы эта комиссия так и не завершила свою работу. Благодаря противодействию поставщиков медицинских услуг и очернению IPAB со стороны таких

---

186 Richard Briffault (2019), «The single-subject rule: A state constitutional dilemma,» Albany Law Review 82, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3593&context=faculty_scholarship.

187 Committee for a Responsible Federal Budget (17 Sep 2020), «Better Budget Process Initiative: Automatic CRs can improve the appropriations process,» http://www.crfb.org/papers/better-budget-process-initiative-automatic-crs-can-improve-appropriations-process.

188 Medicare – национальная программа медицинского страхования в США. – *Прим. ред*.

политиков, как бывший кандидат в вице-президенты Сара Пэйлин, конгресс так и не назначил ни одного члена комиссии, а в 2018 г. и вовсе закрыл IPAB после пяти лет простоя без персонала.

Аналогичный хак – законопроект «одно-название», который, по сути, является пустой оболочкой. Он не имеет никакого существенного содержания, но законодатели штата Вашингтон вносят в него поправки и дополнения каждую сессию. Хак служит для того, чтобы законодатели могли обойти законодательные правила и установленные сроки в конце года. В последние дни законодательной сессии 2019 г. демократы использовали законопроект «одно-название», чтобы принять банковский налог при минимальном общественном контроле и обсуждении.

В более общем плане этот хак является частью широкого класса делегирования законодательных функций исполнительной власти. Многими понятие «административное государство» и обширные нормотворческие полномочия, предоставленные исполнительной власти законодательной властью, воспринимаются как несбалансированный взлом законодательной системы. И это происходит регулярно. В США ежегодно принимается от 3000 до 4000 новых административных правил[189], что превосходит по объему результаты работы конгресса. И хотя во многом это является показателем нарастающей беспомощности конгресса, уступающего власть более эффективным федеральным агентствам, есть и другая причина: члены конгресса не всегда хотят официально заявлять о своей поддержке тех или иных законов.

Исправления этого хака сложны и неочевидны. Если законодательная власть в любой момент сочтет, что исполнительная власть превышает свои регуляторные полномочия или преследует нежелательные цели, она должна иметь возможность принять закон, корректирующий объем делегированных полномочий или отменяющий конкретные действия. Некоторые правоведы считают, что конгресс должен поступить именно так, другие настаивают на том, что Верховный суд США должен положить конец этой практике.

Помимо снятия с себя ответственности законодатели также могут отказываться от проведения голосования. Филибастер – это обструктивная тактика, при которой законодатель произносит длинную речь, чтобы помешать своевременному голосованию по предложению или законопроекту и тем самым заблокировать его принятие. Пожалуй, наиболее широко эта тактика применяется в сенате США, но также используется и в законодательных органах по всему миру, от Великобритании и Канады до Австрии и Филиппин.

Справедливости ради следует отметить, что филибастер – хак далеко не новый. Он появился еще в 60 г. до н. э., когда римский сенатор Катон Младший намеренно произносил бесконечные речи, чтобы отсрочить голосование. Римский Сенат должен был завершить все дела до наступления сумерек, но он не мог голосовать, если кто-нибудь из сенаторов отказывался молчать. Катону удавалось проделывать этот трюк в течение полугода, что, вероятно, является своего рода вершиной.

В США филибастер возможен только благодаря уязвимости в правилах, которая стала случайным побочным эффектом другого изменения законодательных правил. Еще в 1805 г. вице-президент Аарон Бэрр заявил, что сенат США не должен быть перегружен процедурными правилами. Одним из правил, отмененных по рекомендации Бэрра в 1806 г., уже после его ухода с поста, было «предложение по предыдущему вопросу», которое завершало дебаты по проекту. Только в 1837 г. кто-то заметил и использовал эту уязвимость. Лазейка была устранена в 1917 г. с помощью правила закрытия дебатов, благодаря которому для поддержания филибастера требовалось говорить безостановочно. Нынешнее правило большинства в три пятых голосов, что равно 60 сенаторам, появилось только в 1975 г.,

---

189 Clyde Wayne Crews and Kent Lassman (30 Jun 2021), «New Ten Thousand Commandments report evaluates the sweeping hidden tax of regulation; Provides definitive assessment of Trump deregulatory legacy,» Competitive Enterprise Institute, https://cei.org/studies/ten-thousand-commandments-2020.

а требование непрерывно говорить было отменено. Это хак поверх патча, наложенного на другой хак, и изменить его можно только следующим хаком.

Филибастер подрывает законодательную систему. Предполагается, что законодательный орган защищает право меньшинства быть услышанным, но при этом соблюдает и правило большинства. Однако современный филибастер переворачивает все с ног на голову, поскольку теперь партия меньшинства может использовать этот хак для остановки законодательного процесса по любому законопроекту без большинства в 60 голосов, что фактически препятствует осмысленному рассмотрению и обсуждению вопроса. Это также плохо для прав меньшинств в обществе, а не только для сенатских партийных меньшинств. Исторически сложилось так, что филибастер чаще всего применялся для блокирования законопроектов, продвигавших равенство рас[190].

В США этот хак стал нормой. В сенате действуют настолько мягкие правила, что сенатору необязательно выступать в течение нескольких дней или месяцев, чтобы устроить филибастер, – он может просто заявить о своем теоретическом намерении сделать это, чтобы отложить голосование. Но в 60 г. до н. э. это, конечно, было действием непредвиденным и не предусмотренным теми, кто создавал правила римского Сената. Обструктивное ораторское искусство было подрывом этих правил, призванным помешать тому, для чего и был создан Сенат: голосованию по законопроектам.

Филибастер – не единственная тактика законодательных проволочек. В Великобритании члены палаты общин могут потребовать, чтобы палата заседала тайно. Эта мера предназначена для обсуждения вопросов национальной безопасности, но ее не раз использовали как тактику затягивания[191] – последний раз в 2001 г. В японском парламенте тактика «выгула быка» [192] означает чрезвычайно медленную ходьбу через холлы для голосования, что, бывает, происходит достаточно, чтобы задержать весь процесс. При верном стратегическом расчете такая тактика может привести к тому, что законопроект будет отложен до следующей законодательной сессии. В итальянском парламенте в 2016 г. в законопроект о конституционной реформе было внесено 84 млн поправок (это не опечатка) в попытке отсрочить голосование по нему.

Хороши или плохи подобные хаки, зависит от того, считаете ли вы, что основной целью системы управления является обеспечение политической подотчетности или все-таки принятие беспристрастных, эффективных политических решений. Если вы полагаете, что правительство должно действовать только тогда, когда есть явная поддержка квалифицированного большинства или всестороннее обсуждение, то тактика отсрочки может быть к месту, позволяя партиям меньшинства получить место за столом переговоров. Если же вы считаете, что правительство должно быть более активным и быстро реагировать на насущные политические вызовы, а уже после иметь дело с мнением избирателей, то возможность для партий меньшинства эффективно накладывать вето на законопроекты – это очень плохо.

Решения варьируются от исправления основной системы таким образом, чтобы хак был невозможен (устранение филибастера в случае сената США), до того, чтобы сделать его реализацию более дорогостоящей, а сам хак реже используемым. В настоящее время

---

190 Zack Beauchamp (25 Mar 2021), «The filibuster's racist history, explained,» Vox, https://www.vox.com/policy-and-politics/2021/3/25/22348308/filibuster-racism-jim-crow-mitch-mcconnell.

191 Lauren C. Bell (14 Nov 2018), «Obstruction in parliaments: A cross-national perspective,» *Journal of Legislative Studies* , https://www.tandfonline.com/doi/full/10.1080/13572334.2018.154469.

192 Michael Macarthur Bosack (31 Jan 2020), «Ox walking, heckling and other strange Diet practices,» *Japan Times* , https://www.japantimes.co.jp/opinion/2020/01/31/commentary/japan-commentary/ox-walking-heckling-strange-diet-practices.

устроить филибастер очень просто: никому не нужно говорить на трибуне сената часами или днями напролет, достаточно просто заявить о своем намерении. Поскольку большинство обязано найти 60 голосов, чтобы отменить филибастер, гораздо труднее его блокировать, чем поддержать. Я слышал о нескольких предложенных реформах, и самая интересная из них – вариант Нормана Орнштейна из Американского института предпринимательства, который утверждает, что нужно просто изменить уравнение. Вместо того чтобы требовать 60 голосов для отмены филибастера, нужно установить планку в 40 голосов для его поддержания. Идея заключается в том, что большинство может заставлять сенат работать круглосуточно в течение нескольких дней или недель, а меньшинству необходимо присутствовать и быть начеку, спать рядом с залом сената, чтобы проголосовать в любой момент.

38
Хакинг и контекст

Я развиваю сложное представление о хакинге. Дело не в том, что хаки – это непременное зло. И даже не в том, что они нежелательны и от них нужно защищаться. Речь о другом: нам нужно признать, что хакеры подрывают основополагающие системы, и решить, является эта подрывная деятельность вредной или она полезна.

К примеру, мы многое узнали о взломе налогового кодекса. В большинстве упомянутых случаев хакеры (бухгалтеры и налоговые адвокаты) находят в кодексе непреднамеренные уязвимости (лазейки).

Нечеткие формулировки в Законе о создании рабочих мест в США [193] 2004 г. породили несколько уязвимостей в налоговом кодексе, и хорошо обеспеченные фирмы смогли воспользоваться ими с большим успехом. Самая заметная среди этих лазеек называлась «вычет за производственную деятельность внутри страны». Этот вычет должен был помочь отечественным производителям конкурировать на международном уровне, но он настолько широко определял производство («объединение или сборка двух или более изделий»), что всевозможные компании не преминули воспользоваться этим вычетом. Компания World Wrestling Entertainment получила его за производство видеороликов о реслинге. Продуктовые магазины претендовали на него, потому что они распыляют на продаваемые фрукты химикаты для быстрого созревания. Аптеки заявляли, что на их территории тоже есть производство – фотокабинки. Производитель подарочных корзин затребовал вычет на том основании, что объединил в одной упаковке вино и шоколад. В последнем случае правительство обратилось в суд, но проиграло.

Невозможно знать наверняка, но эта проблематичная формулировка[194], похоже, была намеренно внедрена законодателями под давлением лоббистов и в силу необходимости получить достаточное количество голосов в конгрессе для принятия закона. Эта налоговая льгота, имевшая непреднамеренные последствия, была одной из многих в законе. Она стала настолько популярной, что оставалась в силе до 2017 г., когда ее заменили вычетом на квалифицированный доход от предпринимательской деятельности.

По мере того как мы переходим от более простых к более сложным примерам, становится все труднее определить, полезен ли тот или иной хак. В чем именно заключается цель хоккейных правил? Соотносятся ли с этой целью изогнутые клюшки или они, наоборот, мешают ее достижению? Изогнутые клюшки способствуют более быстрому движению

---

193 Natalie Kitroeff (27 Dec 2017), «In a complex tax bill, let the hunt for loopholes begin,» *The New York Times* , https://www.nytimes.com/2017/12/27/business/economy/tax-loopholes.html.

194 Edmund L. Andrews (13 Oct 2004), «How tax bill gave business more and more,» *The New York Times* , https://www.nytimes.com/2004/10/13/business/how-tax-bill-gave-business-more-and-more.html.

шайбы [195], а значит, и более захватывающей игре. Но слишком быстрая шайба опасна и приводит к большему количеству травм. Когда Национальная хоккейная лига устанавливала правила, определяющие, насколько изогнутой может быть клюшка, она пыталась сбалансировать соображения безопасности и спортивного мастерства. С 1967 г. эти правила менялись, поскольку менялся баланс на чаше весов: сначала был разрешен максимальный изгиб в 3,81 см, затем в 2,54 см, потом в 1,27 см, а в настоящее время в 1,9 см.

Еще сложнее определить намерения сотрудников законодательного органа, которые разработали этот слишком широкий налоговый вычет для производства. Возможно, какой-то лоббист хакнул законодательный процесс, подкинув члену конгресса или его подчиненным заведомо расплывчатую формулировку, которой, по задумке лоббиста, начнут злоупотреблять? Считал ли член конгресса, что корпоративные налоги плохи по своей природе, и вставил в законопроект формулировки, которые, как он знал, не привлекут внимание, когда законопроект будет проходить через комитет и обсуждаться? А может быть, закон был просто плохо написан?

Является хак улучшением системы или нет, также зависит от точки зрения. Умный предприниматель может использовать лазейку в законодательстве для собственной выгоды, его клиенты тоже будут довольны, а вот правительство может пострадать.

Мы определили хакинг как технику, которая придерживается правил системы, но подрывает ее замысел, ее цель. И это не всегда плохо. Как мы успели убедиться, некоторые хаки являются полезными инновациями. В конечном итоге они нормализуются и улучшают систему. В Китае, например, реформистские правительства 1980–1990-х гг. маневрировали, обходя сопротивление частных собственников [196] с помощью таких хакерских приемов, как предложение арендаторам 70-летней возобновляемой аренды на землю. Они следовали правилам коммунистической партии, но полностью подрывали их суть.

Сама система не может отнести конкретный хак к той или иной категории. Это должна сделать более общая управляющая система, потому что определение взлома зависит от контекста.

Банкомат существует в более широком контексте банковской системы. Правила игры в хоккей существуют в более широких контекстах игроков, лиг, болельщиков и общества в целом. Примеры в этой книге из любой области – будь то банковское дело, экономика, право и законодательство, психология – существуют в более широком социальном контексте наших идентичностей, отношений, желаний, ценностей и целей.

Это ставит нас перед очевидным вопросом: кто должен определять цель системы? Кто решает, является хак полезным или нет? Стала подорванная система лучше или нет? Это действительно сложные вопросы, особенно что касается систем, у которых несколько разработчиков, или систем, эволюционирующих с течением времени. Одни сочтут хак полезным, другие – вредным.

Вот некоторые истины, которые невозможно понять, находясь внутри системы, но которые становятся очевидными на более высоком системном уровне. Все компьютерные программы в конечном счете представляют собой сложный код замыкания и размыкания электрических цепей, представляющий собой набор нулей и единиц, но простого юзера это не волнует – он не пишет в машинном коде. Что нас волнует, так это задачи, которые код позволяет решить: просмотр фильма, отправка сообщений, чтение новостей и финансовых

---

195 National Hockey League (accessed 11 May 2022), «Historical rule changes,» https://records.nhl.com/history/historical-rule-changes.

196 Donald Clarke (19 Jan 2017), «The paradox at the heart of China's property regime,» Foreign Policy, https://foreignpolicy.com/2017/01/19/the-paradox-at-the-heart-of-chinas-property-regime-wenzhou-lease-renewal-problems. Sebastian Heilmann (2008), «Policy experimentation in China's economic rise,» Studies in Comparative International Development 43, https://link.springer.com/article/10.1007/s12116-007-9014-4.

отчетов. Если перенести это сравнение на язык биологии, то молекулярные структуры и химические реакции, характеризующие жизнь, выглядят как невероятно сложный хаос, пока вы не поднимете на уровень организма и не поймете, что все они выполняют функцию поддержания в нем жизни.

В предыдущих главах мы сталкивались с разными органами управления, в чьи обязанности входит вынесение решений. В более простых системах может быть единственный орган управления, имеющий всего одно назначение. Комиссия по азартным играм штата Невада обновляет правила казино на основе анализа хаков. Международная автомобильная федерация делает то же самое в отношении гонок «Формула-1», а Международная федерация футбола – в отношении футбола.

Подрывают ли хаки цель системы? Или же они способствуют ее реализации? В чем вообще заключается цель системы? Единого ответа нет. Он не сводится к анализу хаков и системы; он будет зависеть от вашей морали, этики и политических убеждений. Всегда существуют обоснованные разногласия по поводу того, следует нормализовывать конкретный хак или нет. В конечном счете важно, кто от этого выиграет, а кто проиграет. Но это тоже политически спорный момент. Поэтому проводятся дебаты и, возможно, голосование. И на первое, и на второе влияют деньги и власть.

Вот пример. В 2020 г. президент Трамп хотел назначить отставного бригадного генерала Энтони Тата на должность заместителя министра обороны по вопросам политики, что требует утверждения сенатом США. Когда стало ясно, что сенат никогда его не утвердит, Трамп отозвал кандидатуру и вместо этого назначил его должностным лицом, «исполняющим обязанности» заместителя министра обороны по вопросам политики[197]. Трамп неоднократно использовал термин «исполняющий обязанности», чтобы обойти утверждение сенатом представленных им кандидатур. Это хакинг Закона о реформе вакансий 1998 г. Но чем он является: вопиющим пренебрежением обязанностями сената или же разумным ответом на слишком широкое требование о том, чтобы сенат утверждал 1200 исполнительных должностей? Это зависит от вашего личного мнения[198] о том, как должно работать правительство.

39
Хакинг избирательного права

Существует множество способов сфальсифицировать выборы: вброс бюллетеней, игры с подсчетами голосов и прочее – история, в том числе и недавняя, знает массу тому примеров. Но часто лучшим способом манипулирования на выборах является не прямое мошенничество, а хакинг избирательного права. Точно так же, как рынки и законодательные процессы, демократия основана на информации, выборе и свободе действий. Все эти три составляющие могут быть взломаны. Иными словами, хакеры могут подрывать саму цель демократических выборов, изменяя правила.

Если вы не голосуете, вы не опасны. Вот почему многие хакеры препятствуют реализации избирательного права.

Пятнадцатая поправка, ратифицированная в 1870 г. после окончания Гражданской войны, сделала незаконным отказ в голосовании мужчинам на основании их расы, цвета кожи или недавнего статуса раба. (Женщины по-прежнему не могли голосовать или занимать ответственные посты.) Вскоре после этого чернокожие мужчины стали использовать свое

---

197 Lara Seligman (2 Aug 2020), «Trump skirts Senate to install nominee under fire for Islamaphobic tweets in Pentagon post,» *Politico* , https://www.politico.com/news/2020/08/02/donald-trump-anthony-tata-pentagon-390851.

198 Kevin Drum (3 Aug 2020), «Do we really need Senate confirmation of 1,200 positions?» Mother Jones, https://www.motherjones.com/kevin-drum/2020/08/do-we-really-need-senate-confirmation-of-1200-positions.

растущее влияние на выборах и избираться на государственные должности. Это возмутило белых южан и бывшую рабовладельческую элиту, которая немедля начала взламывать избирательный процесс, чтобы ограничить права и политическую власть афроамериканцев, только-только получивших право голоса. (Для достижения этой цели использовались в том числе далеко не хакерские тактики, такие как насилие и убийства.)

В Алабаме, например, коалиция консервативных демократов, называвших себя «искупителями» [199], захватила власть на выборах 1874 г. благодаря фальсификациям и военизированному насилию. (Не хак!) В течение следующих 30 лет они постепенно ослабляли политическое влияние афроамериканцев путем тщательно продуманных ограничений на голосование. Кульминацией этих усилий стала ратификация [200] в 1901 г. новой конституции штата, целью которой, по заявлениям ее составителей, было «установление превосходства белых в штате». Конституция ввела и закрепила [201] избирательные налоги, требования к владению собственностью, тесты на грамотность и различные дисквалификации, которые резко ограничивали число афроамериканцев, имеющих право голоса. (А вот это уже хак.) Задумка консерваторов сработала: в начале 1870-х гг. более 140 000 афроамериканцев в Алабаме имели право голоса, а в 1903 г. смогли зарегистрироваться на выборах менее 3000 человек из их числа[202].

«Тест на грамотность» – название, намеренно искажающее смысл процедуры. В данном контексте это не имело никакого отношения к тестированию навыков чтения. Это были сложные тесты, разработанные таким образом, чтобы люди неизбежно их проваливали. Можно долго спорить об их конституционности, но самым неприятным моментом этой хакерской атаки было предоставление местным избирательным органам значительной свободы действий в определении того, какие потенциальные избиратели должны пройти провальный тест. Это позволяло должностным лицам избирательных комиссий отказывать в праве голоса по своему усмотрению. Сам луизианский тест на грамотность 1964 г. [203] можно легко найти в интернете. Например, вот одно из заданий (да-да, вы не сошли с ума): «Напишите в первой строке прописными буквами каждое второе слово из этой фразы, печатными буквами – каждое третье слово [строки были очень узкими], а каждое пятое слово напишите с заглавной буквы».

Перенесемся в день сегодняшний. Алабама по-прежнему использует различные тактики подавления избирателей, чтобы ограничить участие в выборах бывших преступников, представителей меньшинств, иммигрантов и сельских избирателей. Препятствия начинают возводиться уже на этапе регистрации избирателей. Штат не предлагает избирателям ни электронную регистрацию, ни регистрацию в офисах Департамента автотранспорта, ни вообще какую бы то ни было предварительную

---

199 Joshua Shiver (16 Apr 2020), «Alabama Constitution of 1875,» Encyclopedia of Alabama, http://encyclopediaofalabama.org/article/h-4195.

200 Alabama Legislature (22 May 1901), «Constitutional Convention, second day,» http://www.legislature.state.al.us/aliswww/history/constitutions/1901/proceedings/1901_proceedings_vol1/day2.html.

201 John Lewis and Archie E. Allen (1 Oct 1972), «Black voter registration efforts in the South,» Notre Dame Law Review 48, no. 1, p. 107, https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=2861&context=ndlr.

202 Rachel Knowles (10 February 2020), «Alive and well: Voter suppression and election mismanagement in Alabama,» Southern Poverty Law Center, https://www.splcenter.org/20200210/alive-and-well-voter-suppression-and-election-mismanagement-alabama#Disenfranchisement.

203 Open Culture staff (16 Nov 2014), «Watch Harvard students fail the literacy test Louisiana used to suppress the Black vote in 1964,» Open Culture.

регистрацию. При этом не существует и системы автоматической регистрации избирателей. По закону штата для регистрации необходимо предъявить документ, подтверждающий гражданство, прямо на избирательном участке. В отношении этого закона проводится федеральное расследование, и, если его оставят в силе, это приведет к еще большей волне отказов в праве голоса представителям меньшинств, у которых часто просто нет паспортов или других документов. Канзас отстранил тысячи новых избирателей от участия в голосовании, используя аналогичное правило.

Исторически сложилось так, что в Алабаме большинство уголовников не имели права голоса. Эта политика также способствовала непропорциональному лишению меньшинств их избирательных прав. Хак заключался в ведении рядом южных штатов «черных кодов», которые классифицировали тривиальные правонарушения (например, кражу скота) как тяжкие уголовные преступления. Афроамериканцы, осужденные за такие преступления, навсегда лишались избирательных прав. В 2017 г. законодательный орган Алабамы отменил этот закон, предоставив почти 60 000 граждан возможность восстановить свое избирательное право. Однако госсекретарь штата не позаботился о том, чтобы предать это нововведение огласке, поэтому многие осужденные до сих пор не знают о своих правах. И даже те преступники, которые о них знают, сталкиваются с существенными трудностями при их реализации из-за административных сложностей и плохого понимания закона чиновниками штата и местными органами власти.

Людей также могут лишить права голоса, исключив в одностороннем порядке их имена из списков избирателей. Обычно при этом исключают тех, кто не голосовал на последних выборах. В основном этот хак работает, поскольку неактивные избиратели вряд ли вернутся на избирательные участки до того, как списки избирателей будут очищены. В Алабаме с 2015 г. из списков избирателей было удалено 658 000 редко голосующих избирателей.

Все это виды административного бремени, которое мы впервые затронули в главе 32. Как правило, подобные хаки не оказывают большого влияния на людей с деньгами и статусом. Но для рядовых граждан с ограниченными ресурсами или временем, инвалидов или тех, кто недостаточно знаком с политическом процессом, такие правила значительно усложняют возможность воспользоваться избирательным правом. Люди пытаются честно следовать этим правилам, но не могут и вынуждены оставить свой голос при себе. Чаще всего такие правила ограничивают участие в выборах представителей малоимущих слоев и меньшинств, которые в основном являются электоратом Демократической партии. В результате подобных хаков только 69 % жителей Алабамы, достигших избирательного возраста, регистрируются для голосования.

40
Другие предвыборные хаки

Еще один хак, посягающий на свободу действий, касается самого процесса голосования. Идея заключается в том, чтобы сделать голосование настолько сложным для имеющих право голоса зарегистрированных избирателей, которые не поддерживают вашего кандидата, чтобы они даже не потрудились прийти на избирательные участки. Многие из приведенных дальше примеров также могут быть классифицированы как административное бремя.

Сразу после ратификации Пятнадцатой поправки южные штаты ввели в действие ограничения на голосование, в которых прямо не упоминалась расовая принадлежность, но затрагивали они тем не менее в основном чернокожих американцев. Поправки включали в себя: подушный налог на голосование, который не могли себе позволить малоимущие, правила, наделявшие избирательным правом только тех, чьи деды имели право голоса до Гражданской войны, и, как уже упоминалось ранее, дьявольски продуманные, точечно применяемые и предвзято оцениваемые тесты на грамотность. Некоторые из этих хаков были

запрещены[204] только после принятия Двадцать четвертой поправки, ратифицированной в 1964 г., Закона об избирательных правах 1965 г. и решения Верховного суда США 1966 г. по делу «Южная Каролина против Катценбаха». После того как в 2015 г. Верховный суд отменил ключевые положения Закона об избирательных правах, эта тактика вернулась в виде правил об удостоверении личности избирателя.

В Алабаме, например, потенциальные избиратели должны предъявить удостоверение личности с фотографией, выданное штатом, иначе их не допустят на избирательные участки. Казалось бы, простое и справедливое требование, но в Алабаме с этим не все так просто. Около 25 % избирателей, имеющих право голоса, живут на расстоянии более 10 миль от офиса Департамента автотранспорта, и многие из них не имеют автомобиля. Это наиболее бедные граждане штата, и часто они проживают общинами. Затем власти штата попытались закрыть 31 офис Департамента автотранспорта, в которых выдаются не только водительские права, но и обычные удостоверения личности. Все офисы располагались в шести округах, где афроамериканцы составляют более 70 % населения. После возражений со стороны министерства транспорта США этот план был отклонен. Тем не менее более 100 000 взрослых жителей Алабамы не имеют приемлемых удостоверений личности для голосования. И хотя это соответствует чуть менее 3 % от общего числа избирателей штата, эта цифра означает 10 % от числа избирателей-афроамериканцев.

Могут существовать законные разногласия по поводу необходимости введения административного барьера и поддержания относительного баланса между предоставлением возможности получения пособия тем, кто действительно в нем нуждается, и препятствованием его получения всеми остальными. Да, важно обеспечить возможность голосования только для тех избирателей, которые имеют право голоса. Но поскольку фактический уровень фальсификаций такого рода крайне низок (что было неоднократно подтверждено судами по всей стране), совершенно очевидно, что описанные выше меры направлены в первую очередь на то, чтобы лишить избирателей, имеющих право голоса, возможности проголосовать.

Наконец, людям может помешать банальное отсутствие избирательных участков рядом с домом[205]. Алабама с 2013 г. снижает число избирательных участков, причем в основном за счет закрытия оных в афроамериканских кварталах. Например, город Дафни с населением 28 000 человек в 2016 г. сократил количество избирательных участков с пяти до двух, и все три закрытых участка были расположены в преимущественно афроамериканских районах города.

Может сложиться впечатление, что в этих главах я решил разделаться с Алабамой, но на самом деле и другие штаты не менее агрессивны в подавлении избирателей, и это усиливающийся процесс. Джорджия, например, тоже требует от избирателей удостоверения личности и подтверждения гражданства штата, чистит списки избирателей, сокращает время досрочного голосования и закрывает избирательные участки, сосредоточенные в афроамериканских районах. О Флориде даже не буду заикаться. И, кроме того, сегодня по всей стране принимаются меры, направленные на подавление молодых избирателей, особенно идеалистически настроенных студентов, которые в основном поддерживают Демократическую партию.

---

204 Constitutional Rights Foundation (n.d., accessed 1 Jun 2022), «Race and voting,» https://www.crf-usa.org/brown-v-board-50th-anniversary/race-and-voting.html. US Supreme Court (7 Mar 1966), South Carolina v. Katzenbach (Case No. 22), 383 U.S. 301, http://cdn.loc.gov/service/ll/usrep/usrep383/usrep383301/usrep383301.pdf.

205 Peter Dunphy (5 Nov 2018), «When it comes to voter suppression, don't forget about Alabama,» Brennan Center, https://www.brennancenter.org/our-work/analysis-opinion/when-it-comes-voter-suppression-dont-forget-about-alabama.

Джерримендеринг – хак не новый. Это слово происходит от имени губернатора Массачусетса, подписавшего Декларацию независимости, Элбриджа Герри (Джерри), который в 1812 г. принял законопроект, согласно которому в штате был сформирован избирательный округ причудливых очертаний, напоминавших саламандру (gerrymander буквально означает «саламандра Джерри»). Такое произвольное манипулирование границами округа позволило консолидировать и усилить голоса федералистов и расколоть голоса Демократическо-республиканской партии. Основная идея здесь заключается в том, что, если вы можете контролировать пропорции избирателей в избирательных округах, вы прямо влияете на то, кто одержит победу, и таким образом добиваетесь доминирования в многоокружном законодательном органе. Вы подстраиваете демографические данные таким образом, чтобы ваша партия выиграла в большинстве округов с небольшим перевесом, скажем в 10 %, а другая партия набрала по 90 % голосов, но всего в нескольких округах.

Существует две тактики джерримендеринга. Первая – «упаковать» округ так, чтобы в него попало как можно больше избирателей оппозиционной партии. Это помогает правящей партии победить в соседних округах, где сила оппозиции ослаблена. Вторая тактика – «расколоть» округ, разделив скопления оппозиционных избирателей между несколькими округами так, чтобы в каждом округе их осталось меньше.

Основная проблема заключается в конфликте интересов: законодатели, отвечающие за формирование округов, являются теми, кто получает выгоду от их демографических характеристик. Решение, очевидное для любого, кто изучал этот вопрос, состоит в разделении полномочий. Округа должны формироваться независимыми комиссиями, члены которых не заинтересованы в результатах выборов. Мичиган в 2018 г. одобрил инициативу, предусматривающую именно такую процедуру. То, что республиканцы штата продолжали бороться с этой комиссией даже в 2020 г., свидетельствует о силе хакеров, занимающихся джерримендерингом.

Помимо вопросов о том, как и в каком округе голосуют граждане, существует бесчисленное множество рычагов, которые политики могут использовать для хакинга избирательного процесса. Государственные должностные лица часто имеют право планировать выборы по своему усмотрению, регистрировать и пересчитывать голоса, а также определять, какие кандидаты и предложения будут включены в избирательный бюллетень. На своих территориях избирательные комиссии могут даже дисквалифицировать кандидатов за несвоевременную подачу документов, недостаточную поддержку или другие технические проблемы. Выборочное использование этих полномочий однозначно является хакингом.

И последняя тактика: в 2018 г. губернатор Висконсина Скотт Уокер просто отказался назначать внеочередные выборы в законодательные органы штата, опасаясь, что их выиграют демократы. В итоге федеральный судья Апелляционного суда обязал его провести выборы. Губернаторы Флориды и Мичигана также пытались прибегнуть к такому методу. В том же 2018 г. Стейси Абрамс едва не проиграла губернаторские выборы в Джорджии Брайану Кемпу, который в то время курировал выборы в качестве госсекретаря и незадолго до них очистил списки от полумиллиона зарегистрированных избирателей.

41
Деньги и политика

Деньги могут контролировать информацию и выбор. За деньги можно купить свободу действий, то есть власть осуществлять изменения. Это политическое хакерство, поскольку оно подрывает цель демократического процесса голосования. В особенности это касается США, где выборы стоят неестественно дорого.

Причины такого положения дел довольно сложны, но все-таки я выделю четыре основные. Во-первых, избирательные циклы в США длятся долго: кандидаты начинают предвыборную кампанию более чем за год до самих выборов. Для сравнения: японские

избирательные кампании длятся 12 дней от начала до конца, а французские – две недели. Выборы в Великобритании проходят в среднем после двух – четырех недель предвыборной кампании. Ни один австралийский или канадский предвыборный сезон никогда не превышал 11 недель, и этот экстремум имел место аж в 1910 и 1926 гг. Во-вторых, партийная дисциплина в США слабее, чем в других странах. Там, где партийная дисциплина сильна, не имеет смысла финансировать конкретных кандидатов и сталкивать их друг с другом на праймериз. В-третьих, США – большая страна с многочисленным населением, дорогими рынками телевизионной рекламы, и, в отличие от других стран, здесь отсутствуют ограничения на расходы избирательных кампаний. И в-четвертых, в законах США о раскрытии пожертвований достаточно лазеек, чтобы снизить политическую ответственность тех, кто принимает неправомерные пожертвования на избирательную кампанию (например, от лиц, не являющихся гражданами США).

Существует мощный стимул для хакинга систем, регулирующих финансирование избирательных кампаний, а также использование кандидатами своих избирательных фондов для взлома политического процесса.

Привилегированному классу нравится проворачивать подобные хаки и добиваться их легализации, поскольку они увеличивают политическое влияние. После принятия Федерального закона об избирательных кампаниях 1972 г. и поправок к нему 1974 г., ограничивающих добровольные пожертвования и расходы, постановление 1976 г. запретило расходы на поддержку партии или кандидата, не согласованные с самой партией или самим кандидатом[206]. Это привело к появлению так называемых *мягких денег* , расходуемых на «партийное строительство», которое часто оказывалось не чем иным, как очернением и политическими нападками на кандидатов другой партии. В течение многих лет состоятельные люди и влиятельные группы оспаривали ограничения, вводимые правилами финансирования избирательных кампаний. В 2002 г. вместе с Законом о реформе двухпартийной кампании были приняты новые ограничения, но они лишь спровоцировали появление новых хаков. Затем решение по делу Citizens United[207] против Федеральной избирательной комиссии 2010 г., подтвержденное постановлением Верховного суда США 2014 г., вновь распахнуло двери, и легальные деньги, включая добровольные пожертвования от корпораций, потекли в политику с новой силой.

Конечно, деньги не гарантируют политический успех, но их отсутствие почти всегда гарантирует провал. Как утверждает профессор права из Гарварда Лоуренс Лессиг[208], «чтобы иметь возможность баллотироваться на выборах, сначала нужно очень тщательно самому сделать выбор, связанный с деньгами». Деньги могут поддерживать кандидатов в таком длительном политическом процессе, как система президентских выборов в США. Мы видели это на республиканских праймериз 2012 г.[209], когда миллиардеры Шелдон Адельсон, Фостер Фрисс и Джон Хантсман-старший оказали огромное влияние на процесс, единолично финансируя кандидатов. Это что-то вроде системы венчурного капитала

---

206 Yasmin Dawood (30 Mar 2015), «Campaign finance and American democracy,» *Annual Review of Political Science* , https://www.annualreviews.org/doi/pdf/10.1146/annurev-polisci-010814-104523.

207 Citizens United – консервативная некоммерческая организация в США, основными заявленными целями которой являются «восстановление традиционных американских ценностей» и «возврат правительства Соединенных Штатов под контроль граждан». Ее президент Дэвид Босси был заместителем руководителя предвыборного штаба Дональда Трампа в 2016 г. Пожертвования на деятельность организации не подлежат налогообложению. – *Прим. пер.*

208 Lawrence Lessig (2014), The USA Is Lesterland, CreateSpace Independent Publishing Platform.

209 Kenneth P. Vogel (12 Jan 2012), «3 billionaires who'll drag out the race,» *Politico* , https://www.politico.com/story/2012/01/meet-the-3-billionaires-wholl-drag-out-the-race-071358.

для политики. Вам не нужно быть лучшим и умнейшим, вам просто нужно убедить богатых инвесторов в том, что ваша кандидатура – это хорошая ставка.

Деньги также могут помочь посеять хаос. В США де-факто существует двухпартийная система, поэтому одна из стратегий состоит в финансировании независимого или стороннего кандидата, который будет оттягивать голоса у вашего оппонента. Если вы республиканец, то можете профинансировать какого-нибудь независимого новичка-либерала, который будет конкурировать с демократом, лидирующим в гонке, и тем самым подорвать его позиции. Если вы демократ – финансируйте независимого кандидата от консерваторов, чтобы разделить голоса республиканцев.

В США такой хак с самовыдвиженцами провернуть довольно непросто, поскольку обе партии заинтересованы в устранении этой уязвимости. В некоторых штатах установлены ранние сроки подачи документов, предусмотрены штрафные санкции для кандидатов, поздно вступающих в гонку, или введены правила, усложняющие попадание в избирательный бюллетень кандидатов, не являющихся ни демократами, ни республиканцами. В 44 штатах действуют законы, которые не позволяют проигравшему на первичных выборах баллотироваться на всеобщих выборах в качестве независимого кандидата.

Однако это не значит, что подобное никогда не происходит. Увидев, как Ральф Нейдер повлиял на выборы 2000 г., республиканские активисты по всей стране попытались воспользоваться кандидатами от Партии зеленых [210], чтобы переманить голоса от демократов. В Сиэтле 18-летний бывший волонтер Нейдера по имени Янг Хан подумывал о том, чтобы принять участие в выборах 2002 г. в Законодательное собрание штата. Некий «г-н Шор» помог Хану организовать кампанию, а также сделал пожертвование на нее. На самом деле этот человек был республиканским стратегом из Вашингтона, округ Колумбия. Его жена аналогичным образом поддерживала кандидата от Партии зеленых в предвыборной гонке в Сиэтле. Позже нечто подобное происходило в Аризоне в 2010 г., в Нью-Йорке в 2014 г. и в Монтане в 2018 и 2020 гг. Республиканцы помогли Канье Уэсту попасть в бюллетень президентских выборов 2020 г., надеясь, что он оттянет голоса у Джо Байдена. В итоге эти хакерские попытки провалились: в теории все куда проще, чем на практике.

С помощью хакинга можно также внести неразбериху и облегчить себе победу. В 2020 г. на выборах в конгресс во Флориде «бывший» республиканец по имени Алекс Родригес выдвинул свою кандидатуру против однофамильца [211], сенатора-демократа от штата Флорида Хосе Родригеса, и присвоил себе коронную тему сенатора – изменение климата. Алекс не имел достаточного политического опыта и фактически не проводил полноценную кампанию, но в результате путаницы он получил целых 3 % голосов, и в результате после ручного пересчета с перевесом в 32 голоса победила республиканка Илеана Гарсия. Кампания Алекса Родригеса была поддержана пожертвованием в $550 000 от недавно созданных компаний Proclivity, Inc. и PAC, аффилированных с представителями Республиканской партии.

Стратегия разделения голосов может быть доведена до крайности. В Индии довольно часто простым гражданам с такими же именем и фамилией, как у политического оппонента,

---

210 Sam Howe Verhovek (8 Aug 2001), «Green Party candidate finds he's a Republican pawn,» *The New York Times* , https://www.nytimes.com/2001/08/08/us/green-party-candidate-finds-he-s-a-republican-pawn.html.

211 Sun-Sentinel Editorial Board (25 Nov 2020), «Evidence of fraud in a Florida election. Where's the outrage?» *South Florida Sun-Sentinel* , https://www.sun-sentinel.com/opinion/editorials/fl-op-edit-florida-election-fraud-20201125-ifg6ssys35bjrp7bes6xzizon4-story.html.

предлагают баллотироваться на тот же пост[212]. Например, на парламентских выборах 2014 г. 5 из 35 кандидатов, претендовавших на конкретный пост, носили имя Лакхан Саху, и только один из них был реальным политиком с законодательным послужным списком. Кандидат от основной противоборствующей партии назвал тот факт, что так много Лакханов Саху вступили в борьбу в одно и то же время, «простым совпадением».

В США общей уязвимостью является сама двухпартийная система, но не меньшую опасность в плане хакинга представляет система выборов, в которой победитель получает все. Поскольку мы не требуем, чтобы кандидаты набирали абсолютное большинство голосов, ограничиваясь большинством относительным, у кандидата меньше шансов на победу, если другой кандидат имеет схожий политический профиль (или даже просто похожее имя) и разделяет голоса потенциальных сторонников.

Одним из способов решения проблемы является *рейтинговое голосование*, при котором избиратели ранжируют кандидатов. Кандидат, набравший наименьшее количество баллов, исключается, а голоса за оставшихся кандидатов перераспределяются в последующих турах на выбывание, пока один из них не наберет абсолютное большинство. Система рейтингового голосования нейтрализует вред, наносимый кандидатами-спойлерами (голоса потенциального спойлера просто перераспределяются в пользу другого кандидата – как правило, именно того, у кого он хотел отнять голоса), и гарантирует, что на выборах победит наиболее приемлемый для реального большинства избирателей кандидат. Показательны парламентские выборы в Австралии в 2022 г.: многие сторонние кандидаты получили поддержку в первом туре, но в последующих голоса не были «потрачены впустую».

42
Хакинг на разрушение системы

В 1729 г. Париж объявил дефолт по своим муниципальным облигациям, поэтому правительство организовало лотерею, в которой каждый держатель облигаций мог купить столько билетов, сколько позволяли его облигации. Каждый билет стоил одну тысячную стоимости облигации, и каждый месяц правительство случайным образом выбирало одного победителя и выдавало ему номинальную стоимость облигации плюс бонус в размере 500 000 ливров.

Вольтер (тот самый) заметил, что размеры выплат превышали количество билетов в обращении, поэтому он пошел на хитрость и вместе с несколькими богатыми покровителями создал синдикат, чтобы скупить все необходимые облигации и билеты. Месяц за месяцем они получали свои выигрыши и менее чем за два года заработали около 7,5 млн франков ($100 млн в сегодняшних долларах).

Организаторы парижской лотереи в конце концов поняли, что большинство выигрышей уходит в руки одним и тем же людям. Вольтер, будучи Вольтером – то есть зная, что ничто хорошее не длится вечно, так почему бы не повеселиться, – на обратной стороне каждого билета оставлял загадки, что облегчило правительству выслеживание хакера. Министр финансов Франции подал на синдикат в суд, но, поскольку его участники не совершили ничего противозаконного, им разрешили оставить выигрыши себе. После этого случая парижское правительство просто закрыло лотерею[213] – мера эффективная, хотя и крайняя.

---

212 Rama Lakshmi (23 Apr 2014), «Sahu vs. Sahu vs. Sahu: Indian politicians run 'clone' candidates to trick voters,» *Washington Post*, https://www.washingtonpost.com/world/sahu-vs-sahu-vs-sahu-indian-politicians-run-clone-candidates-to-trick-voters/2014/04/23/613f7465-267e-4a7f-bb95-14eb9a1c6b7a_story.html.

213 Andy Williamson (16 May 2013), «How Voltaire made a fortune rigging the lottery,» Today I Found Out, http://www.todayifoundout.com/index.php/2013/05/how-voiltaire-made-a-fortune-rigging-the-lottery.

Совсем недавно в штате Огайо был создан веб-сайт, через который работодатели могли сообщать о сотрудниках, отказавшихся работать во время пандемии COVID-19, чтобы они не получали пособие по безработице. Некий хакер понял, что в процессе подачи отчета отсутствует аутентификация: его мог подать кто угодно. Поэтому, чтобы привлечь внимание к проблеме, он написал программу, которая автоматически отправляла поддельные отчеты[214] (преодолевая даже CAPTCHA), и разместил ее в интернете. Мы не знаем, сколько таких отчетов в результате было подано через онлайн-систему. Официальные лица штата Огайо утверждали, что им удалось их отсеять, но в итоге штат отказался от использования подобных отчетов для исключения людей из списков безработных.

В главе 10 я объяснил, почему хакеры – это паразиты. Как и любой паразит, хакер должен балансировать между подрывом системы и ее разрушением. Слишком много хакинга – и система рухнет. Иногда, как в случае с парижской лотереей, система упраздняется в результате того, что хак оказался слишком успешным. В других случаях, как в примере с сайтом по сбору данных о безработице, отключение системы как раз и являлось целью хакера.

Финансово мотивированные хакеры, как правило, не стремятся разрушить системы, которые взламывают. Если хакнуть слишком много банкоматов, они просто исчезнут как явление. Если спорт начнут хакать все кому не лень, он перестанет быть интересным, зачахнет и умрет. Большинство хакеров хотят сохранить систему, но добиваться при этом лучших результатов. Если они и разрушают систему, то обычно это происходит непреднамеренно.

Но бывают исключения, когда хакеры следуют каким-то моральным или этическим принципам. Они хакают систему, потому что она им не нравится, а не потому, что хотят извлечь выгоду. Как и в случае со взломом сайта по безработице в Огайо, их цель – снизить функциональность системы, подорвать ее эффективность или полностью уничтожить. Мы видели пример такого хакинга в 2020 г., когда пользователи TikTok скоординировали свои действия и создали поток фальшивых регистраций на предвыборный митинг Трампа в Талсе[215], чтобы обеспечить полупустой стадион. Это был элементарный хак, поскольку для бронирования билета достаточно было ввести фиктивный адрес электронной почты и фиктивный номер телефона, полученный через Google Voice. Система продажи билетов в конечном итоге не была разрушена, но низкая явка смутила Трампа, и его штаб перешел на другие, менее уязвимые системы продажи билетов.

Какова бы ни была мотивация, хакерские атаки способны разрушать социальные системы в гораздо больших масштабах, чем лотерея Вольтера, билетная система Трампа или пособия по безработице в Огайо. Намеки на это мы видели в банковском кризисе 2008 г., когда неоднократные взломы системы чуть не разрушили всю финансовую сеть США. Намеки на это мы видим, наблюдая за финансированием американской политики, политической дезинформацией и социальными сетями. И это же происходит во время политических революций, когда все социальные механизмы хакаются с совершенно иными целями. Поэтому, хотя хакинг может быть полезен и даже необходим для эволюции системы, иногда его может быть слишком много.

Возьмем другой экономический пример – печатание бумажных денег. Бумажные деньги существуют по крайней мере с XI в., с эпохи правления династии Сун в Китае, и, вне всяких сомнений, являются хаком. Валюта должна представлять собой некую реальную экономическую ценность, но сегодня большинство правительств имеют возможность

---

214 Janus Rose (8 May 2020), «This script sends junk data to Ohio's website for snitching on workers,» *Vice* , https://www.vice.com/en_us/article/wxqemy/this-script-sends-junk-data-to-ohios-website-for-snitching-on-workers.

215 Taylor Lorenz, Kellen Browning, and Sheera Frenkel (21 Jun 2020), «TikTok teens and K-Pop stans say they sank Trump rally,» *The New York Times* , https://www.nytimes.com/2020/06/21/style/tiktok-trump-rally-tulsa.html.

печатать столько валюты, сколько потребуется, независимо от того, сколько на самом деле производит экономика. Это означает, что правительства могут взламывать системы государственного финансирования, создавая достаточное количество новых денег для оплаты своих счетов, вместо того чтобы финансировать программы за счет налогов или частных инвесторов. В Европе этот хак впервые появился благодаря экономисту Джону Ло, который таким образом помог французскому королю Людовику XV оплачивать войны.

Бумажные деньги – это пример полезного хака, ставшего сегодня нормой. Возможность печатать деньги может иметь огромное значение во время экономических кризисов. Именно так правительство США финансировало интервенции, которые успокоили рынки в 2008–2009 гг., и ограничило экономические последствия пандемии и карантина в 2020 г. И это же помогло правительству США финансировать массовые военные мобилизации.

Но когда правительства начинают полагаться на печатный станок для обслуживания внешнего долга, все может пойти из рук вон плохо. Хотя гиперинфляция случается редко, она способна нанести невероятный ущерб в кратчайшие сроки. Когда в 2007 г. Зимбабве переживала гиперинфляцию[216], зимбабвийский доллар за один год потерял более 99,9 % своей стоимости, средний уровень благосостояния местных жителей упал ниже уровня 1954 г., а денег, на которые когда-то можно было купить 12 автомобилей, перестало хватать даже на буханку хлеба. Венесуэлу гиперинфляция настигла в 2017 г.[217] и в итоге взвинтила цены настолько, что средней семье потребовалось зарабатывать в 100 с лишним раз больше значения минимальной заработной платы, только чтобы покупать самое необходимое. Это привело к тому, что более 10 % населения эмигрировало из страны.

Другие примеры хакерских атак с целью разрушения связаны с недавним приходом к власти ряда авторитарных правительств в таких странах, как Россия, Сирия, Турция, Филиппины, Венгрия, Польша, Бразилия и Египет. Выборы там все еще проводятся, и голоса все еще подсчитываются. Законодательные органы по-прежнему принимают законы, а суды обеспечивают их исполнение. Права на свободу слова и свободу ассоциаций часто остаются в силе, по крайней мере формально. Но все эти механизмы и институты были взломаны и поставлены на службу диктатурам.

И наоборот, некоторые системы необходимо взломать, чтобы уничтожить. Бойкоты и гражданское неповиновение в целом – это хакерские атаки: они нарушают правила рынка и привычной политики, чтобы выразить протест против несправедливости. Обратная реакция, которую они вызывают, делает явными скрытые в системах насилие и жестокость, сдвигая политическую повестку в сторону разрушения таких систем, как дискриминационные законы, которые долгое время считались нормой. Задача, с которой мы сталкиваемся, заключается в том, чтобы убедиться, что наши хаки разрушают плохое, оставляя при этом хорошее… и понимать, что из этого что.

Часть VI
Хакинг когнитивных систем

43

216 Janet Koech (2012), «Hyperinflation in Zimbabwe,» Federal Reserve Bank of Dallas Globalization and Monetary Policy Institute 2011 Annual Report, https://www.dallasfed.org/~/media/documents/institute/annual/2011/annual11b.pdf.

217 Patricia Laya and Fabiola Zerpa (5 Oct 2020), «Venezuela mulls 100,000 Bolivar bill. Guess how much it's worth?» *Bloomberg*, https://www.bloombergquint.com/onweb/venezuela-planning-new-100-000-bolivar-bills-worth-just-0-23. Gonzalo Huertas (Sep 2019), «Hyperinflation in Venezuela: A stabilization handbook,» Peterson Institute for International Economics Policy Brief 19–13, https://www.piie.com/sites/default/files/documents/pb19-13.pdf.

Когнитивные хаки

Вот хак, который я регулярно использовал в 1990-х гг., когда мы еще пользовались бумажными авиабилетами, чтобы сэкономить на перелетах. Получение бумажного посадочного талона было отдельным от покупки билета действием, его можно было получить за несколько недель до полета, и для этого нужно было пообщаться с реальным человеком.

В те времена я жил в Вашингтоне, округ Колумбия, и много летал по работе. Скажем так, у меня были причины проводить выходные в Чикаго, но работодатель не позволял делать дорогостоящую остановку. Однако у меня был хак. Скажем, у меня есть билет из Сиэтла в Вашингтон с пересадкой в Чикаго на воскресенье. Сначала я должен пойти в кассу авиакомпании и получить распечатанные посадочные талоны, которые агент прикрепляет степлером к моим билетам. Я откреплял их и прятал, а на другой день возвращался в кассу и менял оба рейса на пятницу (в те времена поменять билеты стоило недорого). Агент авиакомпании вводил изменения в компьютер и выдавал мне новую пару посадочных талонов, снова прикрепленных степлером к тому же билету. В пятницу, как и предполагалось, я летел из Сиэтла в Чикаго, затем проводил там выходные, а вернувшись в аэропорт в воскресенье, подходил к выходу на посадку на рейс Чикаго – Вашингтон с оригинальным билетом и первым посадочным талоном, который я сохранил. Несмотря на то что компьютер не показывал бронь на мое имя, у меня был билет с правильной датой и посадочный талон с воскресного рейса Сиэтл – Чикаго, чтобы показать, если у кого-то возникнут сомнения. Сбитый с толку, агент игнорировал то, что сообщал ему компьютер, выдавал новый посадочный талон и пропускал меня в самолет.

Это был отличный хак, и он работал до тех пор, пока авиакомпании не перешли на электронные билеты и не отказались от бумажных посадочных талонов. Но что именно я взламывал? Уж точно не систему бронирования авиабилетов. Компьютер четко сказал, что у меня нет брони на этот рейс. На самом деле я хакал самого агента авиакомпании, контролирующего посадку. Я был уверенным в себе белым мужчиной, совершающим деловую поездку, с надлежащим образом оформленным билетом и посадочным талоном в руках. Проблема могла быть связана с компьютерной ошибкой, – по крайней мере, именно такое предположение в итоге делал агент. Это может показаться странным, но хакал я не что-нибудь, а человеческий мозг.

Наш мозг – это система, которая развивалась в течение миллионов лет, чтобы поддерживать жизнь на уровне каждой особи и, что более важно (с точки зрения генов), – чтобы поддерживать воспроизводство вида. Он был оптимизирован благодаря постоянному взаимодействию с окружающей средой, но оптимизирован для людей, которые жили небольшими родовыми общинами на Восточно-Африканском плоскогорье 100 000 лет назад. Человеческий мозг не слишком хорошо подходит для жизни в Нью-Йорке, Токио или Дели XXI в. Чтобы приспособиться к современной социальной среде, он вынужден задействовать множество когнитивных функций, а значит, им можно манипулировать.

Будет упрощением говорить о том, что биологические и психологические системы человека являются системами «естественными», а затем заявлять, что хакинг подрывает их цели. Эти системы функционируют и развиваются незапланированно. Тем не менее такой упрощенный подход может дать полезную основу для обсуждения. Мы можем ссылаться на «цель» биологических и психологических систем – например, на цель поджелудочной железы или цель чувства доверия – без необходимости выходить за рамки эволюционных процессов. (Здесь уместна аналогия с экономическими и политическими системами, у которых тоже нет единого проектировщика.) Хакинг творчески подрывает эти системы. Как и взломы созданных человеком систем, когнитивные хаки используют уязвимость, чтобы подорвать цель когнитивной системы.

Когнитивные хаки обладают невероятной силой. Многие социальные системы, на которые опирается наше общество, – демократия, рыночная экономика и т. д. – зависят

от людей, принимающих рациональные решения. В предыдущих главах мы рассматривали хаки, которые успешно ограничивали один из трех внешних аспектов этого процесса: информацию, выбор и свободу действий. В этой и следующих главах мы узнаем, как процесс принятия решения взламывается напрямую – непосредственно в нашем сознании.

Возьмем, к примеру, дезинформацию – хак, который подрывает наши системы свободы слова и свободы прессы. Дезинформация – понятие далеко не новое. Геббельс, гитлеровский министр пропаганды, однажды сказал[218]: «Одной из лучших шуток демократии навсегда останется то, что она дала своим смертельным врагам средства, которыми же и была уничтожена». Дезинформация подрывает многие когнитивные системы, о которых мы будем говорить дальше: внимание, убеждение, доверие, авторитет, трибализм[219], а иногда и страх.

В отличие от других хаков когнитивные хаки относятся к более высокому уровню общности. Фактически, они являются самыми общими в иерархии хаков. В то время как законы регулируют экономические операции и другие сферы жизни общества, законодательные органы и суды отвечают за создание и пересмотр законов, а Конституция страны (или аналогичный документ) устанавливает законодательный процесс и судебную систему. Но наши социальные системы – и системы технологические, в той мере, в какой они взаимодействуют с пользователями, – зависят от того, что люди думают и насколько задействуют свои когнитивные функции, чтобы разобраться в той или иной ситуации. Если вы можете хакнуть мозг, то сможете взломать и любую систему, управляемую человеком.

Когнитивные хаки так же стары, как и наш вид. Многие из них были нормализованы так давно, что мы даже не задумываемся о них, не говоря уже о том, чтобы считать их хаками. Поскольку мы sapiens, разработавшие теорию собственного сознания и обладающие способностью планировать далеко вперед, мы подняли хакинг как таковой до уровня сложности, не доступной ни одному из известных нам видов. Как и многие хакерские приемы, описанные в предыдущих главах, когнитивные хаки нацелены на информацию, выбор или свободу действий, которые необходимы людям для принятия обдуманных и эффективных решений.

Что изменилось за последние полвека, так это возможности для манипулирования восприятием других людей – компьютеры и компьютерные интерфейсы предоставляют нам их в широком ассортименте. В сочетании с компьютерными алгоритмами и поведенческими науками они повысили скорость и изощренность вмешательства в работу сознания, а это ведет уже к качественным изменениям.

Однако паниковать не стоит. Писатель и активист Кори Доктороу предостерегает нас[220] от слепой веры в то, что «высокие технологии использовали большие данные для создания луча, контролирующего наш разум, чтобы втюхивать людям спиннеры». То, о чем пойдет речь в следующих главах, – не более чем пища для размышлений. Однако я думаю, что игнорировать опасения в этой сфере не стоит: ИИ будет делать методы манипулирования все более эффективными.

Патчи, как правило, не работают с когнитивными системами, хотя осознание факта взлома уже само по себе является патчем. Защита от когнитивных хаков сводится к превентивным мерам и смягчению нанесенного ими ущерба. Многие мошеннические игры паразитируют на наших эмоциях – жадности, доверии, страхе и прочих. Взять и поставить

---

218 Jason Stanley (2016), How Propaganda Works, Princeton University Press, https://press.princeton.edu/books/paperback/9780691173429/how-propaganda-works.

219 Трибализм (от *лат* . tribus – племя) – племенной этноцентризм. Выражается в обособленности своей этнической общности, включая стремление законсервировать атрибуты первобытности. – *Прим. ред* .

220 Cory Doctorow (26 Aug 2020), «How to destroy surveillance capitalism,» OneZero, https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59.

заплатку на мозг невозможно, но можно использовать другую систему, чтобы объявить конкретные хаки незаконными – то есть выходящими за рамки приемлемого социального поведения – и обучить потенциальных жертв тому, как избегать их.

Хаки когнитивных систем очерчены не так четко, как хаки, описанные в предыдущих главах. Возьмем для примера дизайн интерфейса веб-страниц, которые кампания Трампа использовала, чтобы обманом заставить людей пожертвовать гораздо больше денег, чем они намеревались, причем для целей, выходящих за рамки политической кампании. Уловки были повсюду: предварительно отмеченные флажки, разрешающие еженедельное снятие средств с расчетного счета или кредитной карты; предустановленные суммы пожертвований, вбитые мелким шрифтом; еще более мелкий шрифт для сообщений о том, что пожертвование может быть использовано на личные расходы кандидата, и т. п. Все эти явные хаки являются примерами *темных паттернов* , о которых мы поговорим позже. Но являются ли они взломами наших перцептивных, эмоциональных или исполнительных систем принятия решений? Ответ: да, причем, похоже, всех трех. Меня не смущает то, что подобное утверждение носит характер неоднозначности. Люди сложные существа. Их когнитивные системы тоже. Поэтому любое обсуждение этой темы тоже будет неоднозначным.

44
Внимание и зависимость

Всплывающую рекламу ненавидят все[221]. Даже ее изобретатель, Итан Цукерман, публично извинился за свое детище. Но всплывающая реклама все равно проникла в большинство компьютерных устройств по той причине, что она прибыльна. А прибыльна она потому, что успешно привлекает внимание людей и увеличивает продажи рекламодателей.

В отличие от баннерной рекламы, которую мы, как правило, можем отключить, всплывающая реклама заставляет уделить ей внимание, хотя бы для того, чтобы просто смахнуть ее с экрана. Обычно он возникает прямо перед глазами, загораживая то, на что вы смотрели. Часто такая реклама включает в себя не только статичное изображение, но и звукоряд и даже видео. Чтобы закрыть окно рекламы, нужно предпринять действие, причем иногда бывает трудно понять, куда для этого надо нажать, или закрытие происходит не с первого раза. И да, все это работает. Удерживание нашего внимания даже в течение относительно короткого промежутка времени может иметь долгосрочный эффект.

Внимание – это когнитивная система, которая позволяет нам сосредоточиться на важных вещах. В любой момент времени вокруг и внутри нас происходит бессчетное множество событий. И хотя наш мозг – это мощный инструмент, его возможности ограниченны. Мы не можем обращать внимание сразу на все.

Учитывая это ограничение, мы используем внимание избирательно. Мы отдаем приоритет вещам и событиям, которые важны для выживания, и уделяем меньше внимания тому, чему уже доверяем. Наше внимание легче всего привлекают явления, которые могут указывать на присутствие хищника или иной угрозы: резкие движения, громкие звуки, яркий свет. Мы также отдаем приоритет явлениям, которые влияют на наше социальное выживание, таким как безопасность и положение в группе, или связанным с привлечением и удержанием сексуальных партнеров. Еще мы обычно обращаем внимание на явления, которые способствуют нашему благополучию и уровню комфорта. Вот почему все, что обещает нам потенциальное вознаграждение, – будь то еда, деньги, наркотики, игрушка в киндер-сюрпризе или просто лайк в цифровом профиле, – привлекает наше внимание. Мы не всегда можем осознанно выбирать, как и на чем фокусировать свое внимание, потому что

---

221 Ethan Zuckerman (14 Aug 2014), «The internet's original sin,» Atlantic, https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041.

большая часть этой системы встроена в наш мозг с неизменяемыми настройками.

Реклама сама по себе не привлекает наше внимание, поэтому рекламодателям приходится взламывать когнитивные системы потенциальных потребителей. В 1860-х гг. французский литограф Жюль Шере изобрел новую форму рекламного плаката[222]: яркие контрастные цвета, красивые полуодетые женщины, динамичные сцены – в общем, то, что невозможно игнорировать. Позже художник-плакатист Леонетто Каппьелло начал рекламировать потребительские товары с помощью потрясающих огромных изображений, созданных специально для того, чтобы пассажиры недавно открытого парижского метрополитена могли разглядеть их, проносясь мимо на большой скорости.

Рекламодатели всегда стремятся как можно более эффективно привлечь наше внимание. Именно поэтому супермаркеты и даже магазины канцелярских товаров или товаров для дома выкладывают конфеты в прикассовой зоне – хак, известный как «размещение в точке продажи». Именно поэтому телевизионные рекламные ролики еще не так давно звучали громче, чем шоу, которые они перебивали, пока Федеральная комиссия по связи США в 2012 г. не запретила эту практику. И именно по этой причине у нас есть всплывающая реклама.

Если рекламные кампании, получившие развитие в 1950-х гг., были основаны на маркетинговых исследованиях и психологии, то современные рекламные кампании все чаще используют микротаргетинг, чтобы хакнуть каждого из нас лично. При этом рекламодатели и брокеры данных накапливают и монетизируют гигантские массивы личной информации, угрожая нашей частной жизни в попытке завладеть вниманием.

Еще один хак схем нашего внимания, который распространен в современных социальных сетях: стимулирование ажиотажа. Facebook использует алгоритмы для оптимизации вашей ленты. Цель компании – удержать вас на платформе: чем дольше вы находитесь на сайте, тем больше рекламы увидите и тем больше денег заработает компания. Поэтому она старается показывать интересный для вас контент, с которым можно демонстрировать сопутствующую рекламу. (Не забывайте об этом: весь смысл этих систем заключается в продаже рекламы, которая манипулирует вами для совершения покупок.)

Аналогичным образом Google хочет, чтобы вы продолжали смотреть видео на YouTube. (YouTube является дочерней компанией Google.) Алгоритм YouTube выяснил, что все более поляризующий специализированный контент привлекает пользователей. Этот неожиданный хак оказался весьма выгодным. Facebook и YouTube поляризуются не потому, что так было задумано, а потому, что, во-первых, алгоритм оптимизировал себя для подачи все более специализированного контента на основе интересов пользователя и, во-вторых, руководство решило проигнорировать потенциальные проблемы, которые это создало. Применительно к политике такие схемы имеют тенденцию к поляризации пользователей, поскольку им проще занять идеологическую нишу, в которой уже есть люди, разделяющие их мировоззрение, и отдавать предпочтение материалам, вызывающим наибольший ажиотаж. Ускоряя и отлаживая задачу поиска и показа специализированного поляризующего контента, автоматизированные системы рекомендаций сокращают количество неотфильтрованных взаимодействий, которые помогают нам учитывать разные мнения и пересматривать собственные убеждения.

Одним из решений этой проблемы, по крайней мере в части рекламы, является регулирование информации, используемой рекламодателями для микротаргетинга. После выборов 2020 г. компания Google внедрила политику, согласно которой было решено ограничить таргетинг предвыборной рекламы общими категориями: возраст, пол и местоположение на уровне почтового индекса. Такие простые меры защиты, скорее всего, окажутся эффективными – если, конечно, Google будет их придерживаться. Однако члены

---

222 Richard H. Driehaus Museum (14 Mar 2017), «Jules Chéret and the history of the artistic poster,» http://driehausmuseum.org/blog/view/jules-cheret-and-the-history-of-the-artistic-poster.

обеих партий сделают все возможное, чтобы подорвать их, поскольку микротаргетинг стал неотъемлемой частью современной политики.

Лучшее решение – применить против гигантских сетей антимонопольное законодательство. С таким количеством контента, собранным в одном месте, гиперспециализация становится легкодоступной (хотя и технически сложной). Напротив, формат небольших социальных сетей, каждая из которых содержит меньший объем контента, ограничит возможности специализации. Обратите внимание, что гиперконсервативные социальные сети, появившиеся после того, как Дональду Трампу запретили пользоваться Twitter [223], не имеют и близко такой власти, как крупные транснациональные компании социальных сетей.

Логической крайностью хакинга внимания является зависимость – самая эффективная форма удержания внимания. Хак заключается не в самом физиологическом процессе зависимости, а в том, как заставить кого-то стать зависимым. Создавая свои продукты так, чтобы они вызывали привыкание, производители и разработчики гарантируют, что клиенты и пользователи будут продолжать их использовать. Иногда зависимость бывает физиологической, но чаще всего она начинается как поведенческая фиксация, закрепляемая с помощью эндорфинов, адреналина и других нейрохимических веществ, выброс которых вызывает такое поведение.

Базовая методология поведенческой зависимости хорошо иллюстрируется на примере игрового автомата. Мы знаем, что переменные вознаграждения вызывают большее привыкание, чем вознаграждение фиксированное, а азартные игры по своей природе предоставляют именно такой вид вознаграждения. На первом этапе процесса возникает триггер – пусковой механизм, который привлекает наше внимание. Игровые автоматы нарочито яркие и шумные. Они шумят и тогда, когда ими никто не пользуется, и тогда, когда кто-то выигрывает. Второй этап представляет собой действие, которое запускает ожидание вознаграждения. Эту роль выполняет ставка – когда-то это была монета, опущенная в слот, сегодня достаточно нажать кнопку. Третий этап – переменное вознаграждение: вы то выигрываете, то проигрываете. На четвертом этапе начинаются эмоциональные инвестиции, которые увеличивают склонность игрока к повторному входу в цикл. Все любят победителей. Еще одно нажатие кнопки, и – кто знает? – может быть, джекпот будет вашим.

Онлайн-игры тоже относятся к аддиктивным процессам с переменным вознаграждением, особенно игры с *лутбоксом* – наборами цифровых товаров. Игроки платят – иногда игровой валютой, но в основном реальными деньгами – за случайный набор внутриигровых предметов. Ценные предметы встречаются в лутбоксах нечасто, иногда очень редко, что имитирует аддиктивные характеристики игрового автомата. Видеоигры в целом обычно разрабатываются с десятками поведенческих настроек, призванных удерживать игроков онлайн как можно дольше – до такой степени, что их аддиктивный характер является секретом Полишинеля.

Информационные продукты, такие как приложения для смартфонов и сайты социальных сетей, специально созданы для того, чтобы аналогичным образом вызывать привыкание. Триггерами служат оповещения, которые привлекают наше внимание: звуковые сигналы, звонки, вибрация, push-уведомления. (Не правда ли, прямо по Павлову?) Действием становится клик, который приносит с собой предвкушение награды. Переменные вознаграждения – это лайки, посты, комментарии, изображения и все остальное, что появляется в ленте.

Ничто из этого не является случайным. Цифровые платформы могут обновлять свои страницы автоматически, без вмешательства пользователя, если бы так решили их разработчики. Но принуждение пользователей к нажатию кнопок или пролистыванию

---

223 После покупки Twitter Илоном Маском среди пользователей был проведен опрос, по результатам которого в конце 2022 г. аккаунт Дональда Трампа разблокирован и вновь активен. – *Прим. ред*.

страниц, чтобы увидеть больше сообщений, имитирует поведение игрового автомата и создает иллюзию контроля, которая приучает вас делать это снова и снова. Аналогичным образом, любого рода пакетные уведомления – когда все новые уведомления показываются один раз в день – снижают эффект переменного вознаграждения, а значит, и аддиктивность. Вот почему эта удобная и простая функция никогда не предлагается ни одной из платформ социальных сетей, основанных на рекламе.

При всей склонности людей считать зависимость недостатком, гораздо полезнее рассматривать ее как хак – надежный и очень эффективный. Мы знаем, что именно делает поведение аддиктивным. Компании повсеместно внедряют такие хаки, причем зачастую настолько скрытно, что потребители не замечают этого. И, как мы увидим дальше, алгоритмы и экспресс-тестирование делают цифровые платформы все более аддиктивными при все меньшем вмешательстве в этот процесс человека.

45
Убеждение

В 2014 г. боты, выдававшие себя за женщин в приложении для знакомств Tinder, отправляли текстовые сообщения пользователям-мужчинам, вели с ними банальную светскую беседу, упоминая в ней мобильную игру Castle Clash, в которую они якобы играли, и затем давали ссылку. С точки зрения хакерского мастерства это было довольно неубедительно. Игра велась на разных мужских эмоциях, включая доверие и сексуальное желание, но новая «подруга», если вы хоть немного включали критическую оценку, явно была ботом. Достоверно неизвестно, насколько успешно эти поддельные аккаунты убеждали людей скачать и поиграть в игру, пока Tinder не удалил их.

Этот пример не уникален. Чат-боты регулярно используются для манипулирования человеческими эмоциями и убеждениями людей в коммерческих и правительственных целях. В 2006 г. армия США развернула SGT STAR, чат-бота, призванного убеждать людей вступать в армию. Технологии ИИ и робототехники делают подобные усилия намного эффективнее.

В 1970-х г. Федеральная торговая комиссия попросила руководителей рекламных агентств объяснить им, что такое маркетинг. До этого у членов комиссии было довольно примитивное представление об отрасли. Они полагали, что реклама – это средство, с помощью которого компании объясняют потенциальным потребителям преимущества своей продукции. Но, конечно, реклама уже тогда была чем-то большим, а современные рекламные технологии, направленные на взлом когнитивных систем, и подавно.

Убеждение – дело непростое. Из-за страха перед манипуляциями и просто опасаясь перемен люди часто противятся попыткам изменить их мнение или поведение[224]. Но, несмотря на наше осознанное и неосознанное сопротивление, бесчисленные уловки незаметно меняют наше мнение. Многие из этих хаков до смешного просты, например *эффект иллюзорной правды* : люди охотнее верят в то, что они слышали неоднократно. (По сути, это *метод большой лжи* , только с другого конца: если вы повторяете ложь достаточно часто, ваши слушатели начнут в нее верить.) Люди с аналитическим складом ума противостоят эффекту иллюзорной правды ничуть не лучше всех остальных. На самом деле повторение лжи и полуправды со стороны элит и СМИ может объяснить устойчивость ложных убеждений. В любом случае очевидно, что такие простые приемы, как повторение одного и того же, могут ускользнуть от нашего внимания и сделать свою работу, незаметно в чем-то убедив нас.

---

224 Marieke L. Fransen, Edith G. Smit, and Peeter W. J. Verlegh (14 Aug 2015), «Strategies and motives for resistance to persuasion: an integrative framework,» Frontiers in Psychology 6, article 1201, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4536373.

Капельное ценообразование – еще один пример. Оно широко распространено в сфере авиаперевозок и гостиничного бизнеса, поскольку цена – это первый атрибут, на который люди обращают внимание при выборе туристических услуг. Хак заключается в том, чтобы сначала показать низкую цену, а затем накрутить дополнительные сборы в надежде, что покупатель не обратит на них внимания. Исследование, проведенное на базе StubHub, онлайн-площадки по продаже билетов, показало, что капельное ценообразование заставляет людей потратить[225] в среднем на 21 % больше, чем прямое выставление цены.

Некоторые продавцы используют *ложные цены* , чтобы повлиять на покупателей. Если вы выбираете между двумя товарами, более дешевым и более дорогим, вы попытаетесь оценить их достоинства и, возможно, выберете тот, что дешевле. Но если продавец добавит третий товар-приманку, еще более роскошный и дорогой, вы, скорее всего, выберете средний вариант.

В интернете для убеждения часто прибегают к *темным паттернам* . Большая часть пользовательского интерфейса компьютера строится на метафорах и нормах, которые доступно объясняют нам, людям, что творится «под капотом» компьютера. Файлы, папки и каталоги – все это не что иное, как метафоры. И они не всегда точны. Перемещая файл в папку, мы на самом деле ничего не перемещаем, а просто меняем указатель, обозначающий место хранения файла. Удаление файла – это не то же самое, что уничтожение физического объекта. Обвиняемые на скамье подсудимых узнают об этом снова и снова, когда файлы, которые, как они думали, были удалены, неожиданно используются против них обвинителями. Но для большинства целей метафоры довольно точно отражают смысл процессов. Нормы, насколько это возможно, тоже взяты из реальной жизни.

Темные паттерны – это термин, обозначающий подрывные хаки в дизайне интерфейса, которые используют общепринятые элементы, чтобы подтолкнуть пользователей к определенным действиям. Обычно стандартизированный дизайн помогает нам в процессе различных онлайн-взаимодействий; это визуальный язык, которому мы доверяем. Например, при таком привычном виде активности, как вождение автомобиля, зеленый цвет означает движение, а красный – остановку. Эти же цвета постоянно используются в качестве ориентиров в пользовательских интерфейсах. Но они превращаются в темный паттерн, когда ряд зеленых кнопок «Продолжить» внезапно прерывается кнопкой такого же цвета, ведущей на страницу продажи, как это сделано, к примеру, в мобильной игре TwoDots. Или когда зеленая кнопка той же формы, что и предыдущие кнопки перехода между страницами, оказывается кнопкой загрузки какого-нибудь программного обеспечения. Поэтому сохраняйте бдительность – слишком часто кнопки подсовывают вам не то, что вы ожидаете.

У Intuit есть бесплатная программа для заполнения налоговых деклараций под названием Free File, но разработчик предпочел спрятать ее подальше от пользователей и обманом заставить их платить за функции заполнения налоговых деклараций в своем продукте TurboTax. (Соглашение о признании вины, заключенное в 2022 г. между несколькими штатами, заставило Intuit выплатить $141 млн в качестве компенсации; посмотрим, изменит ли это поведение Intuit в будущем.) Баннерная реклама от компании Chatmost выглядит на сенсорном экране как пылинка – когда обманутые пользователи пытаются смахнуть ее, они вынужденно нажимают на рекламу.

В 2019 г. сенаторы США Марк Уорнер и Деб Фишер представили проект закона о запрете темных паттернов. Увы, он не прошел. Но если в будущем его все же примут, спонсорам этого проекта лучше хорошенько подумать над тем, как сформулировать определение темного паттерна, потому что само оно станет мишенью для взлома, когда хакеры будут пытаться обойти закон.

---

[225] Morgan Foy (9 Feb 2021), «Buyer beware: Massive experiment shows why ticket sellers hit you with last-second fees,» Haas School of Business, University of California, Berkeley, https://newsroom.haas.berkeley.edu/research/buyer-beware-massive-experiment-shows-why-ticket-sellers-hit-you-with-hidden-fees-drip-pricing.

46
Доверие и авторитет

19 марта 2016 г. Джон Подеста, в то время председатель президентской кампании сенатора Хиллари Клинтон, получил электронное письмо якобы от Google. Это было предупреждение о безопасности, и в нем содержалась ссылка на страницу, похожую на страницу входа в Google. Подеста спокойно ввел свои учетные данные, но позже оказалось, что эта страница вовсе не была страницей Google. На самом деле она управлялась ГРУ, российской военной разведкой. Как только оперативники по ту сторону экрана получили пароль Подесты от сервиса Gmail, они завладели по меньшей мере 20 000 его электронных писем, а затем слили их в WikiLeaks для публикации. Это был хакинг с помощью средств социальной инженерии.

Социальная инженерия – весьма распространенный способ взлома компьютерных систем. По сути, это убеждение человека, имеющего особый доступ к системе, в том, чтобы он использовал его не по назначению. Более 20 лет назад я написал: «Только любители атакуют машины; профессионалы нацелены на людей» [226]. Это утверждение верно и сегодня. И в первую очередь оно касается хакерских методов, основанных на доверии.

Один из таких методов представляет собой звонок на линию техподдержки сотового оператора под видом другого человека с целью убедить сотрудника перевести номер этого человека на телефон, который вы контролируете. Эта атака, известная как *подмена SIM-карты*, особенно неприятна, поскольку контроль над номером телефона открывает путь другим видам мошенничества и часто приводит к большим потерям. Известен случай, когда жертва лишилась вследствие такой атаки $24 млн[227], а совокупные потери просто огромны.

Существует гигантское количество вариаций на тему социальной инженерии. Они могут выглядеть как телефонный разговор с сотрудником – именно так в 2020 г. хакеры завладели 130 аккаунтами Twitter[228] – или как переписка по электронной почте. Термином *«фишинг»* обозначают отправку фальшивых электронных писем с целью убедить получателя перейти по ссылке, открыть вложение или сделать что-то еще, ставящее под угрозу безопасность компьютера или банковского счета получателя. Фишинговые атаки не слишком эффективны, поскольку злоумышленники забрасывают широкую сеть и делают свои призывы достаточно общими. Термин «целевой фишинг» используется, когда эти письма становятся персонализированными. Чтобы составить убедительное сообщение, требуется серьезно исследовать адресата, но оно может быть очень эффективным методом взлома. Подеста попался как раз на такой крючок. Как и бывший госсекретарь Колин Пауэлл.

В главе 12 я рассказал о компрометации деловой электронной почты. Хакер получает доступ к электронной почте руководителя компании, а затем пишет подчиненному что-то вроде: «Здравствуйте. Это генеральный директор. Да, это непривычно, но я в командировке и не имею обычного доступа к сети. Мне нужно, чтобы вы прямо сейчас перевели $20 млн на этот иностранный счет. Это важно. От этого зависит крупная сделка. Я пришлю вам

---

226 Bruce Schneier (15 Oct 2000), «Semantic attacks: The third wave of network attacks,» Crypto-Gram, https://www.schneier.com/crypto-gram/archives/2000/1015.html#1.

227 Joeri Cant (22 Oct 2019), «Victim of $24 million SIM swap case writes open letter to FCC chairman,» *Cointelegraph*, https://cointelegraph.com/news/victim-of-24-million-sim-swap-case-writes-open-letter-to-fcc-chairman.

228 Twitter (18 Jul 2020; updated 30 Jul 2020), «An update on our security incident,» Twitter blog, https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.

необходимые бумаги, когда вернусь в отель». В зависимости от того, насколько хорошо хакеру удастся сделать детали правдоподобными, насколько сотрудник будет рассеян и доверчив и как все вместе впишется в реальную ситуацию, этот хак может оказаться весьма успешным. В 2019 г. компания Toyota потеряла $37 млн из-за подобной аферы, пополнив длинный список ее жертв.

В 2015 г. сирийские женщины-агенты, флиртуя по Skype с доверчивыми повстанцами, сумели выведать у них планы сражений, а также личные данные высокопоставленных руководителей. Российская разведка использовала ту же тактику, пытаясь выведать секретную информацию у военнослужащих США.

Технологии облегчают подобные махинации. Сегодня преступники используют технологию дипфейк для совершения атак методами социальной инженерии. В 2019 г. генерального директора британской энергетической компании обманом заставили перевести[229] €220 000, подделав голос его босса из материнской компании и подтвердив телефонный звонок электронным письмом. В этом хаке использовалась только цифровая обработка голоса, но и видеоизображение уже на подходе. Известен случай, когда мошенник использовал силиконовую маску для записи видео[230] и обманом заставил людей перевести ему миллионы долларов.

Этот вид мошенничества может иметь и геополитические последствия. В рамках научного исследования были созданы очень убедительные видеоролики, в которых политики говорят то, чего они не говорили, и делают то, чего не делали. В 2022 г. видео, на котором президент Украины Владимир Зеленский призывает украинские войска сдаться, было развенчано самим Зеленским. Хотя ролик сделан кое-как и в нем легко можно распознать фальшивку, со временем при развитии технологий такие подделки станут намного лучше.

Одного существования такой технологии уже достаточно для того, чтобы подорвать наше доверие к аудио– и видеодокументам в целом. В 2019 г. видеозапись давно пропавшего с экранов действующего президента Габона[231] Али Бонго, который, как считалось, находился в тяжелом состоянии или уже умер, была названа его противниками «глубокой подделкой» и послужила спусковым крючком для военного путча, оказавшегося, впрочем, неудачным. Это было настоящее видео, но откуда неспециалист мог знать, какое из утверждений является правдой?

Объедините эти методы с уже существующими и будущими технологиями ИИ, которые позволят ботам создавать и убедительно воспроизводить реалистичные тексты – сообщения, монологи и диалоги, – и вы получите технологии, которые полностью хакнут наше представление о том, кто или, точнее, что является или не является человеком.

Мы видели подобные подделки в действии во время президентских выборов в США в 2016 г. BuzzFeed обнаружил 140 фальшивых новостных сайтов[232] с доменными именами,

---

229 Nick Statt (5 Sep 2019), «Thieves are now using AI deepfakes to trick companies into sending them money,» *The Verge* , https://www.theverge.com/2019/9/5/20851248/deepfakes-ai-fake-audio-phone-calls-thieves-trick-companies-stealing-money.

230 Hugh Schofield (20 Jun 2019), «The fake French minister in a silicone mask who stole millions,» *BBC News* , https://www.bbc.com/news/world-europe-48510027.

231 Drew Harwell (12 Jun 2019), "Top AI researchers race to detect 'deepfake' videos: 'We are outgunned,' " *Washington Post* , https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned.

232 Craig Silverman and Lawrence Alexander (3 Nov 2016), «How teens in the Balkans are duping Trump supporters with fake news,» *BuzzFeed* , https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

похожими на настоящие ресурсы, и сенсационными заголовками, которые пользовались большим успехом в Facebook. Это стало началом волны новых сайтов, замаскированных под авторитетные источники информации. Такие доменные имена, как BostonTribune.com, KMT11.com и ABCNews.com.co, выглядели вполне официально и обманули многих читателей, заставив поверить в дезинформацию. Такие сайты, как The Tennessee Star, Arizona Monitor и Maine Examiner, были созданы, чтобы выглядеть как традиционные газеты, но распространяли при этом политическую пропаганду.

Многие исторические индикаторы доверия больше не работают. Печатные книги и телевизионные новости считались авторитетными источниками, поскольку издательская и вещательная отрасли выступали в роли привратников публичного поля. Доверие, основанное на подобной схеме, не имеет под собой оснований применительно к интернету. Сегодня любой может опубликовать что угодно в виде книги. Бумажную газету по-прежнему трудно подделать, но сымитировать ее в формате веб-сайта несложно. Раньше сигналом о надежности и платежеспособности банка служило солидное здание, в котором он размещался; теперь эту роль выполняет графика и дизайн веб-сайта.

Я могу привести еще больше примеров хакинга, основанного на вероломстве. *Спонсированный контент* соответствует форме и функциям платформы, на которой он размещен, но на самом деле является платной рекламой. (Большинство платформ, впрочем, отмечают такой контент как спонсированный.) Отзывы клиентов, которыми сегодня пестрит интернет, могут выглядеть правдоподобно, но их легко подделать. То и дело всплывает информация о фальсификации профессиональных полномочий: грабители выдают себя за сотрудников иммиграционных служб, чтобы отбирать деньги у новых мигрантов, доктора наук выдают себя за врачей, чтобы торговать шарлатанскими снадобьями, мошенники выдают себя за налоговых инспекторов, чтобы получить доступ к компьютерам и паролям честных налогоплательщиков.

И последнее: наши когнитивные системы доверия привыкли иметь дело с людьми. Мы не приспособлены оценивать надежность организаций, брендов, корпораций и т. п. Отсюда возникли маскоты – милые узнаваемые персонажи, олицетворяющие бренд, – и положительные отзывы знаменитостей. Рекламодатели уже десятилетиями придают брендам человеческое лицо и запускают наши когнитивные системы доверия.

Некоторые бренды даже обзавелись узнаваемыми сетевыми личностями: рестораны быстрого питания Wendy's выступают в Twitter в образе саркастичного тролля, а от лица Amazon прославился персонаж, гневно реагирующий на критиков компании в правительстве. И все это для того, чтобы имитировать человечность и завоевать доверие так же, как это делают влиятельные лица и политики. По мере того как компании и политические движения все чаще используют ИИ для оптимизации своего присутствия в социальных сетях и поддаются искушению запускать фальшивые аккаунты, чтобы создать впечатление поддержки широких слоев населения, доверие к ним вскоре может возникнуть даже у матерых скептиков.

47
Страх и риск

Наше чувство страха является врожденным. Оно развивалось на протяжении тысячелетий: наши предки учились избегать хищников, а также представителей своего вида, которые вредят другим ради собственной выгоды. Подобно системам внимания, рассмотренным выше, наша система страха базируется на когнитивных штампах: она тоже проходила оптимизацию в условиях нашего эволюционного прошлого.

Это базовые функции, в основном контролируемые миндалевидным телом в стволе

головного мозга[233]. Анализ вероятностей и рисков не является нашей сильной стороной. Мы часто склонны преувеличивать значение впечатляющих, странных и редких явлений, а значение обычных, знакомых и распространенных, наоборот, преуменьшать. Мы полагаем, что редкие риски встречаются чаще, чем это происходит на самом деле. И мы боимся их больше, чем это следует по теории вероятности.

Многие психологи пытались объяснить это, и один из их ключевых выводов состоит в том, что люди реагируют на риск, больше опираясь на яркие истории, чем на данные. Истории увлекают нас на интуитивном уровне, особенно если они захватывающие или очень личные. Рассказ друга о том, как его ограбили в другой стране, с большей вероятностью повлияет на то, насколько безопасно вы будете чувствовать себя во время поездки туда, чем абстрактная статистика преступлений. Новизна + страх + хорошая история = чрезмерная реакция.

Последствия этого можно видеть во всем. Мы боимся быть убитыми, похищенными, изнасилованными или подвергнуться нападению со стороны незнакомцев, в то время как статистически гораздо более вероятно, что преступник, совершивший такие преступления, окажется нашим родственником или другом. Нас беспокоят крушения самолетов и стрелки-одиночки, а не аварии на дорогах и домашнее насилие, хотя два последних явления распространены намного шире и статистически они смертоноснее. Мы не имели, а некоторые из нас до сих пор не имеют представления о том, как реагировать на риски COVID-19, которые индивидуально малы, коллективно огромны, чрезвычайно чувствительны к небольшим изменениям в социальных условиях и постоянно меняются вслед за мутациями вируса.

Терроризм напрямую взламывает эти когнитивные штампы[234]. Как индивидуальный риск он незначителен. В результате терактов 11 сентября погибли около 3000 человек, и еще около 300 погибли в США от террористических атак за два последующих десятилетия. С другой стороны, 38 000 человек ежегодно погибают в автокатастрофах – это около 750 000 смертей за тот же промежуток времени. От COVID-19 в США погибло более миллиона человек. Но терроризм придуман для того, чтобы сломать всякую логику. Это ужасающее, яркое, зрелищное, непредсказуемое для жертв, злонамеренное явление – именно то, что заставляет нас преувеличивать риск и слишком остро реагировать. Страх овладевает нами, и мы идем на компромиссы в вопросах безопасности, о которых раньше даже не задумывались. Это хакерские атаки на коллективные страхи и инстинкты общества.

Политики тоже занимаются хакингом системы страха. Если вы сможете доказать, что ваша политическая программа обеспечит безопасность и устранит угрозы, которые чаще всего обсуждаются в новостях, то получите поддержку. Люди могут перенимать страхи от политических инфлюэнсеров или коллег, даже не имея соответствующего личного опыта. Избиратель, живущий в северном Нью-Хэмпшире, может испытывать сильный страх перед иммигрантами на южных границах США, даже если у него не было опыта общения с выходцами из Центральной Америки. Как сказал Билл Клинтон, «когда люди не уверены в себе, они предпочитают ориентироваться[235] на кого-нибудь сильного и неправильного, чем на слабого и правильного».

Трибализм – это система коллективной групповой идентичности. Мы

---

233 Bruce Schneier (3 Apr 2000), «The difference between feeling and reality in security,» *Wired* , https://www.wired.com/2008/04/securitymatters-0403.

234 Bruce Schneier (17 May 2007), «Virginia Tech lesson: Rare risks breed irrational responses,» *Wired* , https://www.wired.com/2007/05/securitymatters-0517.

235 Nate Silver (1 Feb 2010), «Better to be strong and wrong – especially when you're actually right,» *FiveThirtyEight* , https://fivethirtyeight.com/features/better-to-be-strong-and-wrong.

запрограммированы объединяться в группы и дистанцироваться от тех, кто в них не входит. Уязвимость этой системы заключается в том, что мы формируем группы по любому поводу, даже если в этом нет никакого смысла. Когда ребенком я проводил лето в лагере, вожатые организовали игру под названием «Война цветов». По сути, весь лагерь на целую неделю случайным образом оказался разбит на две группы: на «красных» и «золотых». Мы больше не ели и не играли вместе. Эффект проявился мгновенно. Мы вдруг стали хорошими парнями, а «они» – врагами. Я уже не помню, какого был цвета, но хорошо помню это ощущение поляризации, внезапного ожесточения против тех, кто еще вчера были моими друзьями.

Есть три основных способа использовать уязвимость нашего трибализма. Первый из них состоит в укреплении существующей групповой идентичности и разделении на группы. Именно к нему прибегло российское Агентство интернет-исследований, больше известное как «фабрика троллей», в период перед выборами 2016 г. в США, используя такие тактики, как пожертвование денег партизанским организациям и провоцирование конфликтов на онлайн-форумах. Основная установка этой кампании звучала как «Найти трещины» – то есть найти существующие в обществе трещины, которые можно углубить до серьезных разногласий между группами.

Второй способ – намеренное формирование обособленных групп с некой скрытой целью. Этим часто грешили колониальные правительства в XIX и XX вв. В Руанде немцы и бельгийцы, управлявшие регионом, превратили экономические особенности хуту (земледельцев) и тутси (скотоводов) в серьезные этнические и классовые различия, что в итоге спустя десятилетия привело к геноциду. Сегодня бренды используют, хотя и с меньшей интенсивностью, аналогичные стратегии в продажах любых товаров – от кроссовок и газировки до квартир и автомобилей.

Третий способ – создать условия для естественного возникновения трибализма. То есть взять уже существующие группы, объединенные по родству интересов, и возвести это родство до уровня «племени». Такой подход характерен для спортивных команд, но все чаще к нему прибегают политические партии и партийные деятели.

Нет сомнений, что на канале Fox News знакомы с результатами исследований, доказывающих, что усиление чувства тревоги связано со все более плотным примыканием к «своим» группам и нарастанием страха перед «чужими». Когда Fox выпускает сюжеты на такие темы, как «Иммигранты заберут ваши рабочие места»[236], «[Подставьте название любого города] кишит преступностью и опасен»[237], «ИГИЛ[238] представляет угрозу для американцев»[239] и «Демократы собираются забрать ваше оружие»[240], он не только заручается общественной поддержкой по этим вопросам, а создает условия, при которых группы становятся поляризованными.

Аналитика данных и автоматизация оказывают все большую поддержку хакингу чувства групповой идентичности. В то же время трибализм настолько укрепил свои позиции

---

236 *Fox News* (26 Jan 2017), «The truth about jobs in America,» The O'Reilly Factor (transcript), https://www.foxnews.com/transcript/the-truth-about-jobs-in-america.

237 Audrey Conklin (21 Feb 2022), «Homicides, rapes in Atlanta soar despite other decreasing violent crime,» *Fox News* , https://www.foxnews.com/us/homicides-rapes-atlanta-soar-2022.

238 Запрещенная на территории Российской Федерации террористическая организация.

239 Ronn Blitzer (26 Oct 2021), "Top Pentagon official confirms ISIS-K could have capability to attack US in '6 to 12 months,' " *Fox News* , https://www.foxnews.com/politics/pentagon-official-isis-k-us-attack-6-to-2-months.

240 Tucker Carlson (9 Apr 2021), «Biden wants to take your guns, but leave criminals with theirs,» *Fox News* , https://www.foxnews.com/opinion/tucker-carlson-biden-gun-control-disarm-trump-voters.

и способность разобщать людей, что подобные хакерские атаки – особенно проведенные с цифровой скоростью и точностью – могут иметь катастрофические последствия для общества. И это не зависит от того, была атака целевой (российские хакеры) или же стала побочным эффектом работы ИИ, который просто не понимает, какой ценой для людей оборачивается его эффективность (рекомендательные системы социальных сетей).

48
Защита от когнитивных хаков

Сообщество пикаперов объединяет мужчин, которые разрабатывают и делятся манипулятивными методами соблазнения женщин. Оно возникло еще до появления общедоступного интернета, позже перекочевало в него и сегодня процветает. Многие пикаперские приемчики напоминают когнитивные хаки. Например, неггинг. По сути, это двусмысленный комплимент с элементом критики или язвительным комментарием, намеренно сделанный для того, чтобы усилить потребность жертвы в эмоциональном одобрении со стороны манипулятора. Да, знаю, это цинично.

Я понятия не имею, работает ли неггинг и прочие пикаперские лайфхаки. Мужчины, которые обсуждают их в интернете, склонны к бахвальству и приводят массу анекдотических доказательств своей неотразимости, но часто отделить ложь от плохой научной методологии бывает непросто. Читая истории женщин, ставших жертвами этих хакерских атак, понимаешь: лучшая защита – знание. Если вы знакомы с тактикой неггинга, то сможете ее предвидеть и вовремя распознать.

Предвидение ускоряет регрессию к среднему. Иными словами, многие когнитивные хаки хорошо работают поначалу, но по мере того, как люди к ним адаптируются, становятся все менее эффективными. Когда в 1994 г. в интернете появилась баннерная реклама, ее кликабельность составляла 49 %; сейчас этот показатель составляет менее 1 %. Всплывающая реклама демонстрировала аналогичный спад, когда стала раздражающе вездесущей. Скорее всего, та же динамика постигнет микротаргетинг, капельное ценообразование, фальшивые аккаунты Facebook и прочие ухищрения, о которых шла речь в последних главах. По мере того как мы привыкаем к этим тактикам, они становятся менее эффективными.

Однако предвидение не дает абсолютной защиты [241]. Многие когнитивные хаки работают даже тогда, когда мы понимаем, что нами манипулируют. Если человек поверил во что-то, он часто сохраняет приверженность своим убеждениям и даже укрепляется в них, когда ему предъявляют явные доказательства их неправоты. Конкретный пример: компании часто используют бесплатные пробные версии с последующей автоматически включающейся ежемесячной подпиской, чтобы взломать готовность потребителя платить. Расчет строится на том, что люди обычно переоценивают возможности своей памяти и умение делать все точно в срок, и, даже если они признают за собой этот недостаток и постоянно собираются отменить подписки на услуги, которые им не нужны, все равно большинство из них ведется на очередные бесплатные версии, а компании продолжают списывать ежемесячную абонентскую плату.

Другой способ защититься от когнитивных хаков – объявить определенные манипулятивные практики незаконными. Австралия, например, обязала продавцов раскрывать полную цену товара сразу, чтобы предотвратить капельное ценообразование, а Федеральная торговая комиссия США требует, чтобы рекламные заявления были «разумно обоснованы». Мы можем снизить эффективность некоторых из этих хаков и, следовательно, сделать их менее опасными, уменьшив возможности микротаргетирования. Если платные

---

241 Leah Savion (Jan 2009), «Clinging to discredited beliefs: The larger cognitive story,» Journal of the Scholarship of Teaching and Learning 9, no. 1, https://files.eric.ed.gov/fulltext/EJ854880.pdf.

сообщения в соцсетях, особенно политическая реклама, будут довольствоваться широкой аудиторией, это затруднит использование целого ряда когнитивных хаков в неблаговидных целях.

Однако любые новые правила рано или поздно будут взломаны. Поэтому контроля, пусть даже надежного и гибкого, а также прозрачности недостаточно, чтобы гарантировать защиту от когнитивных хаков и отучить людей от их использования. Задача усложняется еще и тем, что многие из этих хаков наносят вред, который в моменте кажется абстрактным, а проявляется спустя какое-то время, и потому довольно трудно объяснить, что с ними «не так».

Когнитивные хаки играют на самых базовых и общих аспектах человеческого разума, начиная с инстинкта выживания и заканчивая стремлением к социальному статусу. Они могут быть использованы против кого угодно. Чтобы защититься от когнитивных хакеров, необходимы усилия всего общества в сферах образования и регулирования, а также технические решения, особенно в онлайн-среде. Поскольку цифровые технологии занимают все больше нашего времени, когнитивные хаки все чаще осуществляются с помощью машин. А поскольку компьютерные программы из хакерских инструментов сами превращаются во все более быстрых, мощных и автономных хакеров, понимание того, как цифровые продукты могут взламывать наше сознание, приобретает все более важную роль для защиты от манипуляций.

49
Иерархия хакинга

Ни одна система не существует изолированно, всегда являясь частью иерархии.

Представьте себе человека, который хочет украсть деньги посредством онлайн-банкинга. Он может хакнуть веб-сайт банка, интернет-браузер клиента, операционную систему или аппаратное обеспечение его компьютера. Все эти взломы потенциально могут достичь своей цели – кражи денег.

Теперь представьте себе человека, который хочет платить меньше налогов. Очевидно, что он будет взламывать налоговый кодекс и искать в нем лазейки. Но если у этого человека есть власть и влияние, он может подняться на уровень выше и хакнуть законодательный процесс, который формирует налоговый кодекс. Поднявшись на два уровня выше, он сможет хакнуть нормотворческий процесс, используемый для реализации законодательства, или же процесс ассигнований, чтобы в налоговых органах возник дефицит сотрудников, задействованных в налоговых проверках. (Хакинг процесса правоприменения – это еще один способ подорвать цель системы.) Если наш хакер поднимется на три уровня вверх, он займется взломом политического процесса, используемого для избрания законодателей. На следующем, четвертом по счету уровне он сможет взломать медиаэкосистему, которая служит для обсуждения политических процессов. Последний, пятый уровень – это уровень хакинга когнитивных процессов, спровоцированных медиаэкосистемой, в результате которых избираются законодатели, создающие налоговый кодекс, предоставляющий ему лазейки. Для этого он даже может спуститься на уровень ниже, чтобы найти уязвимости и эксплойты в программе подготовки налогов.

Я пытаюсь сказать, что иерархия систем – это иерархия возрастающей общности, в которой вышестоящая система управляет нижестоящей. И хакеры могут атаковать любой из этих уровней. Хакинг использует иерархию взаимосвязанных систем. Хакнуть какую-то обособленную систему или манипулировать ею порой очень непросто, но системы более высокого уровня, которые управляют ею, или системы нижестоящие, реализующие ее команды, могут стать богатым источником эксплойтов, которые сами по себе, оставаясь на своем уровне иерархии, не представляют опасности.

В технологических системах продвижение вверх по уровням затруднено. Тот факт, что Microsoft Windows имеет уязвимости, не гарантирует, что кто-то может взломать процесс

найма сотрудников корпорации Microsoft, чтобы поставить себя в положение, позволяющее внедрить еще больше уязвимостей в операционную систему. В социальных системах такое продвижение вверх значительно проще, особенно для тех, у кого есть деньги и влияние. Джефф Безос без проблем купил самый большой дом в Вашингтоне[242], чтобы развлекать законодателей и влиять на них, и газету *The Washington Post* , один из самых авторитетных источников новостей в США. Разумеется, еще проще для него нанять программистов, чтобы написать такое программное обеспечение, которое он захочет.

Некоторые хакеры работают на нескольких уровнях одновременно. В 2020 г. мы узнали о Ghostwriter[243], группе предположительно российского происхождения, которая взломала системы управления контентом нескольких восточноевропейских новостных сайтов и разместила фейковые истории. Это обычный хакинг компьютерных систем, подключенных к интернету, в сочетании с хакингом доверия аудитории к новостным сайтам с хорошей репутацией.

Устранением уязвимостей тоже проще заниматься на более низких уровнях иерархии систем. Уязвимость в TurboTax может быть исправлена за несколько дней. Устранение лазейки в налоговом кодексе может растянуться на годы. Когнитивные уязвимости легко могут существовать несколько человеческих поколений (хотя конкретные тактики их эксплуатации, возможно, придется регулярно менять).

Это делает когнитивные хаки самыми опасными из всех. Они управляют нашими действиями, как индивидуальными, так и коллективными, а значит, и нашими социальными системами. Если вы можете взломать человеческий мозг, то ничто не мешает вам использовать эти методы на избирателях, служащих, бизнесменах, регуляторах, политиках и подобных вам хакерах, подталкивая их к изменению систем обитания по вашему усмотрению.

Сегодня когнитивный хакинг несет в себе новые угрозы. Наш мозг не единственная когнитивная система, о которой нам нужно беспокоиться. Государственные услуги, бизнес-транзакции и даже основные социальные взаимодействия теперь опосредуются цифровыми системами, которые так же, как и люди, делают прогнозы и принимают решения, но намного быстрее, последовательнее и при этом менее ответственно, чем мы. Машины все чаще принимают решения за нас, но думают иначе, чем мы, и взаимодействие нашего разума с ИИ указывает хакерам путь к захватывающему и опасному будущему в сферах экономики, права и не только.

Часть VII
Хакинг и системы искусственного интеллекта

50
Искусственный интеллект и робототехника

Искусственный интеллект (ИИ) – это информационная технология. Она представляет собой программное обеспечение для компьютеров и уже глубоко внедрилась в нашу социальную структуру, причем не только там, где мы это видим и осознаем, но и в области, пока недоступные нашему пониманию. Эта технология хакнет наше общество так, как никто

---

242 Sam Dangremond (4 Apr 2019), «Jeff Bezos is renovating the biggest house in Washington, D.C.,» *Town and Country* , https://www.townandcountrymag.com/leisure/real-estate/news/a9234/jeff-bezos-house-washington-dc.

243 Lee Foster et al. (28 Jul 2020), «'Ghostwriter' influence campaign: Unknown actors leverage website compromises and fabricated content to push narratives aligned with Russian security interests,» Mandiant, https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html.

и ничто доселе.

Мое утверждение базируется на двух предпосылках. Во-первых, системы ИИ будут непревзойденным инструментом для хакеров-людей. А во-вторых, они сами станут хакерами. ИИ будет находить уязвимости во всех видах социальных, экономических и политических систем, а затем использовать их с беспрецедентной скоростью, масштабом, размахом и изощренностью. Это не просто разница в интенсивности, это качественно иной хакинг. Мы рискуем оказаться в будущем, где системы ИИ будут взламывать другие системы ИИ, а последствия этого, которые обрушатся на людей, будут не более чем сопутствующим ущербом.

Это может показаться преувеличением, но ничего из того, что я описываю, не требует научно-фантастических технологий далекого будущего. Я не постулирую никакой «сингулярности», когда цикл обратной связи при обучении ИИ становится настолько быстрым, что опережает человеческое понимание. В моих сценариях нет ни злых гениев, ни разумных андроидов вроде Дейты из «Звездного пути», R2-D2 из «Звездных войн» или Марвина из «Автостопом по галактике». Не потребуется таких мощных и вредоносных системы ИИ, как Скайнет из «Терминатора», Альтрон из «Мстителей» или агент Смит из «Матрицы». Некоторые хаки, о которых я расскажу, даже не предполагают серьезных научных открытий. Да, они будут совершенствоваться по мере развития технологий ИИ, но уже сегодня мы можем видеть намеки на их появление. Эти хаки возникнут естественным образом, по мере того как ИИ будет становиться все более совершенным в обучении, понимании и решении проблем.

Определение

Искусственный интеллект, ИИ (*англ* . artificial intelligence, AI).

1. Компьютер, который (как правило) может воспринимать, думать и действовать.

2. Общий термин, охватывающий широкий спектр технологий принятия решений, которые имитируют человеческое мышление.

Это определение, как и предыдущие, не претендует на канонизацию, но справедливости ради должен заметить, что кратко определить ИИ сложно. В 1968 г. пионер компьютерной науки Марвин Мински описал ИИ следующим образом[244]: «Наука о том, как заставить машины делать то, что потребовало бы интеллекта, если бы это делали люди». Патрик Уинстон, еще один пионер ИИ, определил его как[245] «вычисления, которые делают возможным восприятие, рассуждение и действие». Стандартная интерпретация теста Тьюринга 1950 г., придуманная им по аналогии с игрой в имитацию[246], ставила задачу определить по текстовым ответам на вопросы, является ваш собеседник человеком или компьютерной программой.

Здесь необходимо провести различие между специализированным, или *узким* , и *общим ИИ* . Общий ИИ мы часто видим в фильмах: он может чувствовать, думать и действовать схожим с человеком образом по широкому спектру задач. Если по сюжету он умнее людей, то обычно говорят об «искусственном сверхинтеллекте». Соедините его с робототехникой

---

244 Marvin Minsky (1968), «Preface,» in Semantic Information Processing, MIT Press.

245 Patrick Winston (1984), Artificial Intelligence, Addison-Wesley.

246 Игра в имитацию (*англ* . imitation game) – популярная игра для вечеринок с участием трех игроков. Двое, мужчина и женщина, расходятся в разные комнаты, а третий, «дознаватель», посредством наводящих вопросов и ответов в письменной форме пытается определить, кто из них кто. При этом один игрок пытается помочь «дознавателю», то есть отвечает правдиво, а другой старается его запутать, то есть прикидывается существом другого пола. – *Прим. пер* .

и получите андроида, более или менее похожего на человека. Роботы, которые пытаются уничтожить человечество в фильмах, – это тоже общий ИИ.

Мы уже провели и проводим множество прикладных исследований по созданию общего ИИ. У нас есть теоретические разработки о том, как спроектировать эти системы, чтобы они вели себя хорошо, например не уничтожали человечество. Это очень увлекательная работа, охватывающая огромную область от компьютерных наук до социологии и философии, но прежде, чем мы увидим ее результаты в действии, вероятно, пройдут еще десятилетия[247]. Я же хочу сосредоточиться на узком ИИ, поскольку именно он сейчас находится в стадии активной разработки.

Узкий ИИ предназначен для выполнения конкретной задачи, как в случае беспилотного автомобиля. Он знает, как управлять транспортным средством, соблюдать правила дорожного движения, избегать аварий и что нужно делать в непредвиденных ситуациях, например когда мячик вылетает на дорогу. Узкий ИИ знает многое и может принимать на основе этих знаний решения, но только в сфере, ограниченной вождением.

Среди исследователей ИИ бытует шутка: если что-то начинает работать, оно перестает быть ИИ. Теперь это просто программное обеспечение. Логический вывод из этой шутки состоит в том, что, вероятно, единственными достижениями исследователей ИИ могут быть неудачи. И в этом есть доля правды. Термин «искусственный интеллект» является по своей сути чем-то загадочным, научно-фантастическим, а как только он становится реальностью, то теряет свое обаяние и загадку. Раньше мы считали, что для чтения рентгеновских снимков грудной клетки требуется рентгенолог, то есть умный человек с соответствующей подготовкой и профессиональными полномочиями. Сегодня мы знаем, что это рутинная задача, которую может выполнить и компьютер.

Чтобы лучше понять, что такое ИИ, подумайте вот о чем. Существует множество технологий и систем принятия решений, начиная от простого электромеханического термостата, который управляет печью в ответ на изменения температуры, и заканчивая каким-нибудь андроидом из научно-фантастического фильма. То, что делает ИИ таковым, зависит от сложности выполняемых им задач и среды, в условиях которой эти задачи решаются. Электромеханический термостат выполняет очень простую задачу, учитывающую только один аспект окружающей среды – температуру. Для этого даже не нужен компьютер. Современный цифровой термостат может определять, кто находится в помещении, и делать расчет будущих потребностей в тепле на основе прогноза погоды, данных об использовании обогревателя или кондиционера, общегородском энергопотреблении и посекундных расходах на электроэнергию. Футуристический ИИ-термостат, вероятно, сможет действовать как заботливый и внимательный дворецкий, что бы это ни значило в контексте регулирования температуры окружающей среды.

Я бы предпочел не зацикливаться на определениях, поскольку для целей нашего обсуждения они не имеют особого значения. В дополнение к принятию решений, важными качествами систем ИИ, которые я буду обсуждать, являются автономность (способность действовать независимо), автоматизация (способность реагировать на конкретные триггеры заданным образом) и физическая активность (способность изменять физическую среду). Термостат имеет ограниченную автоматизацию и физическую активность, но не обладает автономностью. Система, предсказывающая рецидив преступлений, не обладает физической активностью: она просто дает рекомендации судье. Беспилотный автомобиль обладает всеми тремя качествами, но строго в рамках заданных функций. Робот R2-D2 обладает всеми тремя в большом объеме, хотя по какой-то неясной причине его разработчики забыли о синтезе человеческой речи.

---

247 Футуролог Мартин Форд провел опрос среди 23 выдающихся исследователей ИИ и спросил их, к какому году будет создан общий ИИ, хотя бы с 50 %-ной вероятностью. Ответы варьировались от 2029 до 2200 г., при этом среднее значение составило 2099 г. – то есть «до конца века». См.: Martin Ford (2018), Architects of Intelligence: The Truth About AI from the People Building It, Packt Publishing.

Определение

Робот [248] (*англ* . robot) – физически воплощенный объект, который может ощущать окружающую среду, думать и воздействовать на нее посредством физической активности.

Робототехника тоже обросла популярной мифологией, но ее реальность менее причудлива. Как и в случае с ИИ, существует множество определений этого термина. В кино и на телевидении роботов часто подают как неких искусственных людей, или андроидов. Подобно ИИ, робототехника охватывает целый спектр логических и физических способностей. Я предпочитаю и в этом вопросе сосредоточиться на технологиях более прозаических и близких к нам по времени. Для наших целей робототехника – это автономия, автоматизация и физическая активность, развитая до максимума. Это *киберфизическая автономия* : технология ИИ внутри объектов, которые могут взаимодействовать с физическим миром напрямую.

51
Хакинг систем искусственного интеллекта

Системы ИИ представляют собой программы, работающие на компьютерах, как правило, в крупномасштабных компьютерных сетях. Это означает, что они уязвимы для всех типов хакерских атак, которым подвергаются обычные компьютерные системы. Но помимо этого существуют специальные хаки, направленные исключительно на системы ИИ и, в частности, на системы машинного обучения (МО). МО – это подобласть ИИ, которая в прикладных системах вышла сегодня на первый план. Системы МО базируются на моделях, которые обрабатывают огромное количество данных и самостоятельно ищут решения согласно инструкциям. Атаки на системы МО бывают двух типов: одни нацелены на кражу данных, используемых для обучения, или кражу модели, на которой основана система, другие связаны с обходом настроек системы МО и подталкивают ее к принятию ошибочных решений.

Последний тип атак известен как *враждебное машинное обучение* и, по сути, представляет собой набор хаков. Часто процесс начинается с детального изучения конкретной системы МО, чтобы получить максимальное представление о ее функционировании и слепых зонах. Затем хакеры разрабатывают тщательно продуманные входные данные и направляют их в эти слепые зоны, чтобы обмануть систему МО. В 2017 г. исследователи из MIT напечатали на 3D-принтере черепаху, которую классификатор изображений на базе ИИ всякий раз опознавал как винтовку. Казалось бы, безобидные наклейки на знаке «Стоп», размещенные определенным образом, обманывают ИИ-классификатор, заставляя его думать, что перед ним знак ограничения скорости. Точно так же небольшие наклейки, размещенные на дороге, вводят в заблуждение беспилотный автомобиль, заставляя его свернуть на встречную полосу. Все это примеры, полученные в ходе исследований, и, насколько мне известно, никто еще не разбивал беспилотный автомобиль с помощью враждебного МО.

За враждебным МО, несмотря на название, совсем не обязательно должны стоять чьи-то злые намерения, и оно не ограничивается лабораторными условиями. В настоящее время существуют проекты, целью которых является хакинг систем распознавания лиц, чтобы протестующие граждане да и любые другие люди могли собираться в общественных местах, не опасаясь быть опознанными полицией. Аналогичным образом можно представить себе будущее, в котором страховые компании будут использовать системы ИИ для принятия

[248] Kate Darling (2021), The New Breed: What Our History with Animals Reveals about Our Future with Robots, Henry Holt.

решений по претензиям. В этом случае врач может хакнуть такую систему методом враждебного МО, чтобы гарантировать одобрение страховки для пациента, который нуждается в определенном лекарстве или процедуре.

Другие успешные хаки подразумевают подачу в систему ИИ определенных входных данных, предназначенных ее изменить. В 2016 г. компания Microsoft представила в Twitter чат-бота по имени Тэй. Его разговорный стиль был смоделирован на основе речи девочки-подростка и должен был становиться все более сложным по мере взаимодействия с людьми и изучения их разговорных стилей. В течение 24 часов группа хакеров на дискуссионном форуме 4chan скоординировала свои ответы и наводнила систему расистскими, женоненавистническими и антисемитскими твитами, тем самым превратив Тэй в злобного шовиниста. Тэй честно учился на том материале, который ему подбрасывали, и, не понимая смысла своих реплик, словно попугай, вернул миру его уродство.

Системы ИИ – это компьютерные программы, поэтому нет оснований полагать, что они окажутся неуязвимыми для обычных компьютерных хаков. Исследования в области враждебного МО все еще находятся на ранних стадиях, поэтому мы не можем однозначно сказать, будут подобные атаки легкими или сложными и насколько эффективными будут контрмеры служб безопасности. Если опираться на историю компьютерного хакинга, то можно утверждать, что уже в обозримом будущем в системах ИИ появятся и будут обнаружены уязвимости. Системы ИИ встроены в те же социотехнические системы, которые мы обсуждали на протяжении всей книги, поэтому обязательно найдутся люди, которые захотят взломать их ради личной выгоды.

Хаки, которые я только что описал, объединяет наглядность результатов. Автомобили разбиваются. Черепаха классифицируется как винтовка. Тэй ведет себя как нацист-женоненавистник. Мы видим, что приводит к таким результатам, и – я надеюсь – сможем исправлять системы МО и восстанавливать их работу.

Однако меня больше беспокоят более тонкие атаки, результаты которых менее очевидны. Беспилотные автомобили могут не разбиваться, а просто начать двигаться чуть более хаотично. Чат-боты могут не превращаться в явных нацистов, а просто стать чуть более склонными к поддержке какой-то конкретной политической партии. Хакеры могут придумать формулировку, вставив которую в текст заявки на поступление в университет вы автоматически получите больше шансов. До тех пор, пока результаты неочевидны, а алгоритмы неизвестны, как можем мы знать, что система не взломана?

52
Проблема объяснимости

В книге «Автостопом по галактике» раса сверхразумных панпространственных существ создает самый мощный компьютер во вселенной – Думатель, Deep Thought («Глубокая мысль»), чтобы ответить на некий ключевой вопрос о жизни, вселенной и всем сущем. После 7,5 млн лет вычислений Думатель сообщает[249], что ответ на главный вопрос бытия – «42». При этом он не в состоянии объяснить смысл этого ответа и даже не помнит, в чем, собственно, состоял сам вопрос.

Если в двух словах, то это и есть проблема объяснимости. Современные системы ИИ, по сути, являются «черными ящиками»: с одного конца в них поступают данные, с другого выходит ответ. Понять, как система пришла к тому или иному выводу, бывает невозможно, даже если вы являетесь ее разработчиком или имеете доступ к коду. Исследователи до сих пор не знают, как именно система классификации изображений ИИ отличает черепаху от винтовки, не говоря уже о том, почему она принимает одно за другое.

В 2016 г. система искусственного интеллекта AlphaGo выиграла матч из пяти

---

249 Douglas Adams (1978), The Hitchhiker's Guide to the Galaxy, BBC Radio 4.

партий [250] у одного из лучших в мире игроков Ли Седоля. Это потрясло как мир разработчиков ИИ, так и мир игроков в го. Тридцать седьмой ход AlphaGo, сделанный системой во второй партии, стал сенсацией. Объяснить весь его смысл, не углубляясь в стратегию го, будет трудно, но если вкратце, то это был ход, который не сделал бы ни один человек в мире. ИИ показал, что он мыслит иначе, чем мы.

ИИ решает проблемы не так, как люди. Его ограничения отличаются от наших. Он рассматривает больше возможных решений, чем мы. И что еще важнее – он рассматривает больше типов решений. ИИ будет исследовать пути, которые мы в принципе не рассматриваем, пути более сложные, чем те, что обычно мы держим в уме. (Наши когнитивные ограничения на объем данных, которыми мы можем одновременно мысленно жонглировать, давно описаны как «магическое число семь плюс-минус два»[251]. У системы ИИ нет ничего даже отдаленно похожего на это ограничение.)

В 2015 г. исследовательская группа ввела в систему ИИ под названием Deep Patient медицинские данные примерно 700 000 человек с целью проверить, может ли она предсказывать развитие болезней. Результаты превзошли ожидания: каким-то образом Deep Patient прекрасно справился с прогнозированием начала психических расстройств, таких как шизофрения, несмотря на то что сами врачи практически не способны предсказывать первый психотический эпизод. Звучит, конечно, здорово, но Deep Patient не дает никаких объяснений, на чем основаны его диагнозы и прогнозы, и исследователи понятия не имеют, как он приходит к своим выводам. Врач может либо доверять компьютеру, либо игнорировать его, но запросить у него дополнительную информацию он не может.

Такое положение дел нельзя назвать идеальным. Система ИИ должна не просто выдавать ответы, но объяснять ход своих рассуждений в формате, понятном человеку. Это необходимо нам как минимум по двум причинам: чтобы доверять решениям ИИ и чтобы убедиться, что он не был хакнут с целью воздействия на его объективность. Аргументированное объяснение имеет и другую ценность, помимо того, что оно повышает вероятность точного ответа или принятия правильного решения: оно считается основным компонентом идеи надлежащей правовой процедуры в соответствии с законом.

Исследователи ИИ работают над проблемой объяснимости. В 2017 г. Управление перспективных исследовательских проектов министерства обороны США (DARPA) учредило исследовательский фонд в размере $75 млн для десятка программ в этой области. Потенциально это влияет на успех, но, похоже, нам не уйти от компромиссов между эффективностью и объяснимостью, между эффективностью и безопасностью и между объяснимостью и конфиденциальностью. Объяснения – это форма стенографии когнитивного процесса, используемая людьми и подходящая для наших методов принятия решений. Решения ИИ могут просто не соответствовать формату понятных для человека объяснений, а принуждение к ним систем ИИ может стать дополнительным ограничением, которое повлияет на качество принимаемых ими решений. Пока неясно, к чему приведут эти исследования. В ближайшей перспективе ИИ будет все более непрозрачным, поскольку системы усложняются, становясь все менее похожими на человека, а значит, и менее объяснимыми.

Впрочем, в некоторых контекстах мы можем не заботиться об объяснимости. Я был бы уверен в диагнозе, поставленном мне Deep Patient, даже если бы он не мог объяснить свои действия, но, согласно данным, ставил диагнозы точнее, чем врач-человек. Точно так же я мог бы относиться к системе ИИ, которая решает, где бурить нефтяные скважины,

---

[250] Cade Metz (16 Mar 2016), «In two moves, AlphaGo and Lee Sedol redefined the future,» *Wired* , https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future.

[251] George A. Miller (1956), «The magical number seven, plus or minus two: Some limits on our capacity for processing information,» *Psychological Review* 63, no. 2, http://psychclassics.yorku.ca/Miller.

или предсказывает, какие детали самолета с большей вероятностью выйдут из строя. Но я бы не чувствовал себя так же комфортно в случае с непрозрачной системой ИИ, которая принимает решения о приеме в колледж, прогнозируя вероятность академических успехов абитуриента, с системой, которая принимает решения о выдаче кредита, учитывая расовые стереотипы в своих прогнозах возможной невыплаты, или с системой, принимающей решения об условно-досрочном освобождении на основе прогноза рецидивов. Возможно, некоторым людям даже спокойнее оттого, что системы ИИ принимают серьезные решения без объяснения причин. Все это очень субъективно и, вероятно, со временем будет меняться по мере того, как мы все больше будем приобщаться к принятию решений ИИ.

Однако есть те, кто категорически не согласен с такой ситуацией и выступает против необъяснимого ИИ. Институт будущего жизни (FLI) и другие исследователи ИИ отмечают, что объяснимость особенно важна для систем, которые[252] могут «причинить вред», оказать «существенное влияние на людей» или повлиять на «жизнь конкретного человека, ее качество или его репутацию». В докладе, озаглавленном «ИИ в Великобритании», говорится, что если система ИИ оказывает «существенное влияние на жизнь человека»[253] и не может предоставить «полное и удовлетворительное объяснение» своих решений, то такую систему внедрять не следует.

На мой взгляд, разница между системой ИИ, которая предоставляет объяснение, и такой же системой, которая этого не делает, заключается в справедливости. Мы должны быть уверены, что система ИИ не является расистской, сексистской, абьюзивной или дискриминирующей в каком-то ином смысле, о котором мы пока не имеем представления. Без объяснимости можно легко получить результаты, подобные тем, которые генерирует внутренняя система ИИ компании Amazon для отбора заявлений о приеме на работу. Эта система была обучена на десятилетних данных о найме, и, поскольку в технологической отрасли доминируют мужчины, она научилась сексизму: оценивая резюме, система перемещала вниз те из них, в которых встречалось слово «женщина» или был указан женский колледж как место учебы. (Бывают случаи, когда мы не хотим, чтобы будущее было похоже на прошлое.)

Как только руководители Amazon осознали эту предвзятость и несправедливость, они потеряли к проекту интерес и в итоге отказались от использования системы[254]. Они столкнулись с трудной, возможно, даже непреодолимой проблемой, поскольку существует множество противоречащих друг другу определений справедливости[255]; то, что справедливо в одном контексте, не обязательно справедливо в другом. Какая система приема заявлений является справедливой? Та, которая не учитывает пол кандидата? Та, которая намеренно корректирует гендерные предубеждения? Та, которая распределяет квоты между

---

252 J. Fjeld et al. (15 Jan 2020), «Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principled AI,» Berkman Klein Center for Internet and Society, https://cyber.harvard.edu/publication/2020/principled-ai.

253 Select Committee on Artificial Intelligence (16 Apr 2018), «AI in the UK: Ready, willing and able?» House of Lords, https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.

254 Jeffrey Dastin (10 Oct 2018), «Amazon scraps secret AI recruiting tool that shows bias against women,» *Reuters*, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

255 David Weinberger (accessed 11 May 2022), «Playing with AI fairness,» What-If Tool, https://pair-code.github.io/what-if-tool/ai-fairness.html. David Weinberger (6 Nov 2019), «How machine learning pushes us to define fairness,» *Harvard Business Review*, https://hbr.org/2019/11/how-machine-learning-pushes-us-to-define-fairness.

представителями полов в той пропорции, в которой они подали заявления? Или та, которая обеспечивает равные возможности для разных полов?

Если система ИИ сможет объяснить, чем она руководствовалась, давая ту или иную рекомендацию о приеме на работу или об условно-досрочном освобождении, мы сможем лучше проанализировать процесс принятия решений. Это означает, что мы с большей вероятностью будем доверять этой системе в ситуациях, которые имеют больше социальных нюансов, чем вопрос «Указывает ли этот рентген на опухоль?».

С другой стороны, сами человеческие решения не всегда объяснимы. Конечно, мы можем давать объяснения, но исследования показывают, что часто это скорее оправдания постфактум. Так что, возможно, ответ заключается в том, чтобы просто внимательно изучить результаты. Когда суды решают, является ли поведение того или иного полицейского департамента расистским, они не вскрывают черепа полицейских и не требуют от них объяснений своего поведения. Они смотрят на его результаты и на основании этого выносят решение.

53
Очеловечивание искусственного интеллекта

Системы искусственного интеллекта будут влиять на нас как на личном, так и на социальном уровне. Ранее я уже упоминал о социальной инженерии. Самые эффективные попытки фишинга – то есть те, в результате которых люди и компании теряют много денег, – всегда персонализированны. Электронное письмо от имени генерального директора с просьбой о банковском переводе, адресованное кому-то из финансового отдела, может быть особенно эффективным, а голосовое или видеосообщение – тем паче. Трудоемкая задача настройки фишинговых атак может быть автоматизирована с помощью методов ИИ, что позволит мошенникам сделать электронные письма или голосовые сообщения от авторитетных лиц максимально правдоподобными.

Быть обманутым ИИ не обязательно означает, что вы получите больше проблем, чем от любого другого обмана. Настоящая опасность заключается в том, что ИИ сможет убеждать с компьютерной скоростью и масштабами. Сегодняшние когнитивные хаки – фейковая статья или провокационный вброс, способные одурачить лишь самых легковерных или отчаявшихся, – покажутся топорной работой. ИИ обладает потенциалом для того, чтобы когнитивные хаки стали микроцелевыми: персонализированными, оптимизированными и доставляемыми непосредственно адресату. Есть много старых мошеннических трюков, учитывающих индивидуальные особенности жертвы. Рекламные сообщения – это когнитивные хаки массового поражения. Технологии ИИ способны объединить в себе и те и другие.

Люди уже давно приписывают компьютерным программам человеческие качества. В 1960-х гг. программист Джозеф Вейценбаум создал примитивную разговорную программу ELIZA[256], которая имитировала манеру общения психотерапевта. Вейценбаум был поражен тем, что люди готовы делиться глубоко личными секретами с глупой компьютерной программой. Секретарша Вейценбаума даже просила его выйти из комнаты, чтобы она могла поговорить с ELIZA наедине. Сегодня мы наблюдаем, как люди стараются быть вежливыми с голосовыми помощниками, такими как Alexa и Siri[257], будто для них действительно важен

---

256 Joseph Weizenbaum (Jan 1966), «ELIZA: A computer program for the study of natural language communication between man and machine,» Communications of the ACM, https://web.stanford.edu/class/linguist238/p36-weizenabaum.pdf.

257 James Vincent (22 Nov 2019), «Women are more likely than men to say 'please' to their smart speaker,» *The Verge* , https://www.theverge.com/2019/11/22/20977442/ai-politeness-smart-speaker-alexa-siri-please-thank-you-pew-gender-sur.

тон общения. Siri даже жалуется, когда вы грубите ей. «Это не очень приятно», – говорит она, но лишь потому, что так запрограммирована.

Многочисленные эксперименты дают аналогичные результаты. Испытуемые оценивали производительность компьютера менее критично, если давали оценку в его присутствии, что свидетельствует об их подсознательном желании не ранить его чувства [258]. В другом эксперименте, когда компьютер сообщал испытуемому явно вымышленную «личную информацию» о себе, тот, как правило, отвечал взаимностью, сообщая реальную личную информацию [259]. Сила взаимности изучается сегодня психологами. Это еще один когнитивный хак, используемый людьми, который могут усилить масштаб и персонализация ИИ.

Робототехника делает хакинг ИИ более эффективным. Люди освоили много способов узнавания самих себя в окружающем мире. Мы видим лица повсюду: две точки с горизонтальной черточкой под ними уже воспринимаются как лицо. Вот почему даже минималистичные иллюстрации так хорошо считываются нами. Если что-то имеет лицо, оно перестает быть чем-то и становится неким существом, со своими мыслями, чувствами и всем, что полагается настоящей личности. Если это некое существо говорит или, еще лучше, вступает с нами в диалог, то мы можем поверить, что у него есть намерения, желания и свобода действий. А если на его лице присутствуют еще и брови, то ничто не помешает нам в этом.

Роботы только подчеркивают эту человеческую уязвимость. Многие люди поддерживают квазисоциальные отношения со своими роботами-пылесосами и даже жалуются, если компания предлагает заменить, а не отремонтировать их. Армия США столкнулась с проблемой, когда полковник подразделения, где проходил тестирование новый противоминный робот, запретил насекомообразному устройству [260] продолжать наносить себе вред, наступая на мины. Робот, разработанный в Гарварде, смог убедить студентов впустить его в кампус, притворившись доставщиком пиццы. А Boxie – говорящий робот, похожий на ребенка, разработанный в стенах MIT, – способен убеждать людей отвечать на личные вопросы, просто вежливо их попросив.

Наша реакция на некоторых роботов в чем-то схожа с нашим восприятием детей. У детей большие головы относительно тела, большие глаза относительно головы, большие ресницы относительно глаз и высокие голоса. Мы реагируем на эти характеристики инстинктивным желанием защитить.

Художники из поколения в поколение использовали этот феномен, чтобы придать своим творениям симпатичный вид. Детские куклы призваны вызывать чувство любви и заботы. Герои многих мультфильмов, включая Бетти Буп (1930-е) и Бэмби (1942), нарисованы по такому шаблону. Главной героине научно-фантастического боевика «Алита: Боевой ангел» (2019) с помощью компьютерной графики увеличили глаза, чтобы они казались больше.

В 2016 г. Технологический институт Джорджии опубликовал исследование о доверии человека к роботам [261], в котором неантропоморфный робот помогал участникам

---

[258] Clifford Nass, Youngme Moon, and Paul Carney (31 Jul 2006), «Are people polite to computers? Responses to computer-based inter-viewing systems,» *Journal of Applied Social Psychology* , https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1559–1816.1999.tb00142.x.

[259] Youngme Moon (Mar 2000), «Intimate exchanges: Using computers to elicit self-disclosure from consumers,» *Journal of Consumer Research* , https://www.jstor.org/stable/10.1086/209566?seq=1.

[260] Joel Garreau (6 May 2007), «Bots on the ground,» *Washington Post* , https://www.washingtonpost.com/wp-yn/content/article/2007/05/05/AR2007050501009_pf.html.

[261] Paul Robinette et al. (Mar 2016), «Overtrust of robots in emergency evacuation scenarios,» 2016 ACM/IEEE

перемещаться по зданию, давая указания типа «Это путь к выходу». Сначала участники взаимодействовали с роботом в обычной обстановке, чтобы оценить его эффективность, которая была специально занижена. Затем они должны были решить, следовать или нет советам робота в условиях смоделированной чрезвычайной ситуации. Поразительно, но все 26 участников послушались его указаний, несмотря на то что всего за несколько минут до этого убедились в его плохих навигационных навыках. Степень доверия к машине была вне всякой логики: когда робот указал на темную комнату без четко обозначенного выхода, большинство людей послушались его, вместо того чтобы просто и безопасно покинуть здание через дверь, в которую они вошли. Исследователи провели аналогичные эксперименты с другими роботами, явно имитировавшими неисправность. И вновь испытуемые вопреки здравому смыслу последовали экстренным указаниям роботов. Похоже, роботы могут естественным образом взламывать наше доверие.

Антропоморфные роботы – это еще более убедительная в эмоциональном плане технология, а ИИ только усилит ее привлекательность. Поскольку ИИ все лучше имитирует людей и животных, постепенно он захватит все механизмы, которые мы используем для оценки друг друга. Как писала психолог Шерри Теркл в 2010 г., «когда роботы устанавливают зрительный контакт, узнают лица, повторяют человеческие жесты, они нажимают на наши дарвиновские кнопки, демонстрируя поведение, которое люди связывают с разумом, намерениями и эмоциями». Проще говоря, они хакают наш мозг.

Мы не просто будем относиться к системам ИИ как к людям. Они будут вести себя как люди, причем намеренно обманывая нас. Они прибегнут к когнитивному хакингу.

54
Хакинг человека искусственным интеллектом и роботами

Во время выборов в США в 2016 г. около одной пятой всех политических твитов было размещено ботами. Во время голосования по Brexit в Великобритании в том же году эта доля составила одну треть. В отчете Оксфордского института интернета за 2019 г. приведены доказательства использования ботов для распространения пропаганды[262] в 50 странах. Как правило, это были простые программы, бездумно повторяющие лозунги. Например, после убийства Джамаля Хашогги в 2018 г. посредством ботов было размещено около четверти миллиона просаудовских твитов «Мы все доверяем [наследному принцу] Мохаммеду бин Салману».

В 2017 г. Федеральная комиссия по связи объявила о начале публичных онлайн-обсуждений ее планов по отмене сетевого нейтралитета. Было получено ошеломляющее количество комментариев – 22 млн, – многие из которых, возможно даже половина, были поданы с использованием украденных личных данных. Эти поддельные комментарии были сделаны очень грубо: 1,3 млн из них явно создавались на основе одного и того же шаблона с изменением некоторых слов для придания уникальности. Это было видно невооруженным глазом.

Подобные попытки будут становиться все более изощренными. В течение многих лет программы ИИ составляли спортивные и финансовые новости для реальных новостных агентств, таких как *Associated Press* . Ограниченный характер большинства репортажей на эти темы упростил их адаптацию к ИИ. Сегодня ИИ используется для написания более

International Conference on Human-Robot Interaction, https://www.cc.gatech.edu/~alanwags/pubs/Robinette-HRI-2016.pdf.

[262] Samantha Bradshaw and Philip N. Howard (2019), «The global disinformation order: 2019 global inventory of organised social media manipulation,» Computational Propaganda Research Project, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

общих историй. Современные системы создания текстов[263], такие как GPT-3 от Open AI, могут писать правдивые истории на основе поставляемых фактов, но точно так же они могут строчить и фейковые новости, будучи накормленными ложью.

Не требуется обладать богатым воображением, чтобы понять, как ИИ ухудшит политический дискурс. Уже сейчас управляемые ИИ-персоны могут писать письма в газеты и выборным должностным лицам, оставлять внятные комментарии на новостных сайтах и досках объявлений, а также обсуждать политику в социальных сетях. По мере того как эти системы становятся все более детализированными и все убедительнее имитируют личность, их все труднее отличать от реальных людей. Тактику, которая раньше была очевидной, сегодня уже распознать не так просто.

В ходе недавнего эксперимента исследователи использовали программу генерации текстов для отправки 1000 комментариев в ответ на просьбу правительства к гражданам высказать свое мнение по вопросу Medicaid[264]. Каждый комментарий выглядел уникально, так, будто реальные люди отстаивали свои политические позиции. Администраторы сайта Medicaid.gov даже не усомнились в их подлинности и приняли всё за чистую монету. Позже исследователи указали им на эти комментарии и попросили удалить, чтобы избежать предвзятости в политических дебатах. Однако не все будут столь этичными.

Эти методы уже применяются в реальном мире для влияния на политику. Пропагандистская онлайн-кампания использовала сгенерированные ИИ изображения лиц для создания фальшивых журналистов. Китай распространял созданные ИИ текстовые сообщения, призванные повлиять на выборы на Тайване в 2020 г. Технология дипфейк, использующая ИИ для создания реалистичных видеороликов о фальшивых событиях, часто с участием реальных людей, чтобы изобразить их произносящими то, что они никогда не говорили, уже применяется в политических целях в таких странах, как Малайзия, Бельгия и США.

Одним из примеров расширения этой технологии является бот-персона – ИИ, выдающий себя за человека в социальных сетях. Бот-персоны имеют свою личную историю, характер и стиль общения. Они не занимаются откровенной пропагандой. Такие боты внедряют в различные группы по интересам: садоводство, вязание, модели железных дорог, что угодно. Они ведут себя как обычные члены этих сообществ, публикуя сообщения, комментируя и обсуждая. Системы, подобные GPT-3, позволяют им легко добывать информацию из предыдущих бесед и соответствующего интернет-контента, чтобы выглядеть знатоками в конкретной области. Затем, время от времени, бот-персона может размещать что-то относящееся к политике, например статью об аллергической реакции медицинского работника на вакцину COVID-19, сопровождая ее обеспокоенными комментариями. Или же высказать мнение своего разработчика о недавних выборах, расовой справедливости или любой другой поляризующей теме. Одна бот-персона не может изменить общественное мнение, но что, если их будут тысячи? Или миллионы?

Этому явлению уже дали название – *вычислительная пропаганда* . Оно в корне изменит наше представление о коммуникации. ИИ способен сделать распространение дезинформации бесконечным. И он может полностью поменять само понятие общения. В 2012 г. специалист по этике робототехники Кейт Дарлинг провела эксперимент с аниматронным пластиковым динозавром по имени Клео [265] – игрушкой, которая по-разному реагировала

---

263 Tom Simonite (22 Jul 2020), «Did a person write this headline, or a machine?» *Wired* , https://www.wired.com/story/ai-text-generator-gpt-3-learning-language-fitfully.

264 Max Weiss (17 Dec 2019), «Deepfake bot submissions to federal public comment websites cannot be distinguished from human submissions,» *Technology Science* , https://techscience.org/a/2019121801.

265 Kate Darling (2021), The New Breed: What Our History with Animals Reveals about Our Future with Robots, Henry Holt.

на прикосновения. После того как участники научной конференции поиграли с Клео, она попыталась убедить их «причинить боль» игрушке различными способами. Однако даже непродолжительная игра с Клео заставляла людей испытывать настолько сильное сочувствие, что они отказывались это делать, хотя игрушка явно не чувствовала боли. Это фундаментальная человеческая реакция. Умом мы можем понимать, что Клео всего лишь зеленый пластиковый динозавр, но большая голова в паре с маленьким телом заставляет нас воспринимать объект как ребенка. К тому же у игрушки есть имя, которое говорит нам, что это «она»! И она реагирует на наши прикосновения! Внезапно мы начинаем относиться к ней как к живому существу[266] и чувствуем себя обязанными защитить от любого вреда. И хотя такая реакция кажется вполне доброжелательной, что произойдет, когда этот милый маленький робот посмотрит на своих хозяев большими грустными глазами и попросит их купить ему обновление программного обеспечения?

Поскольку мы, люди, склонны смешивать категории и относиться к роботам как к живым существам со своими чувствами и желаниями, мы уязвимы для манипуляций с их стороны. Роботы могут убедить нас делать то, что мы бы не стали делать без их влияния. И они могут припугнуть нас, чтобы мы не делали того, что могли бы сделать в противном случае. В одном из экспериментов робот успешно воздействовал на испытуемых по скрипту «давление сверстников»[267], побуждая их идти на больший риск. Задайте себе вопрос: как скоро секс-робот начнет предлагать покупки в приложениях в самый ответственный момент?

В этом виде убеждения ИИ будет становиться все лучше. Исследователи уже разрабатывают системы ИИ, которые определяют эмоции, анализируя наш почерк, читая выражение лица или отслеживая дыхание и пульс. Пока еще они часто ошибаются, но с развитием технологий это пройдет. В какой-то момент ИИ превзойдет человека по своим возможностям. Это позволит более точно манипулировать нами. Но с одной оговоркой: нашу адаптивность, о которой мы говорили ранее, никто не отменял.

AIBO – это собака-робот, представленная Sony в 1999 г. Компания выпускала новые и улучшенные модели каждый год вплоть до 2005 г., а затем в течение следующих нескольких лет постепенно прекратила поддержку старых AIBO. Даже по компьютерным стандартам того времени AIBO был довольно примитивным, но это не мешало людям эмоционально привязаться к своим «питомцам». В Японии даже появилась традиция устраивать похороны своих «мертвых» AIBO.

В 2018 г. Sony начала продажи нового поколения AIBO. В игрушку внесено много программных усовершенствований, которые делают ее более похожей на домашнее животное, но интереснее другое: AIBO для работы теперь требуется облачное хранилище данных. Это означает, что, в отличие от предыдущих версий, Sony может удаленно изменить или даже «убить» любого AIBO. Первые три года хранения данных в облаке бесплатны, после чего компания начинает взимать плату в размере $300 в год. Расчет строится на том, что за три года владельцы AIBO эмоционально привяжутся к своим питомцам. Подобную тактику можно назвать «эмоциональным захватом».

Поскольку ИИ и автономные роботы берут на себя все больше реальных задач, подрыв доверия людей к таким системам будет отягощен опасными и дорогостоящими последствиями. Но не стоит забывать, что именно люди управляют системами ИИ. Все они разрабатываются и финансируются людьми, которые хотят манипулировать себе подобными

---

266 Woodrow Hartzog (4 May 2015), «Unfair and deceptive robots,» *Maryland Law Review* , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2602452.

267 Yaniv Hanoch et al. (17 May 2021), «The robot made me do it: Human – robot interaction and risk-taking behavior,» Cyberpsychology, Behavior, and Social Networking, https://www.liebertpub.com/doi/10.1089/cyber.2020.0148.

определенным образом и с конкретной целью.

Такие корпорации, как Sony, и другие влиятельные игроки долго и упорно пытаются хакнуть наши эмоции ради власти и прибыли. Для этого они вкладывают немалые средства в исследования и технологии. И без активных усилий по установлению норм и правил, ограничивающих такой тип хакинга, мы вскоре обнаружим, что нечеловеческие в буквальном смысле возможности систем ИИ обращены против обычных людей в интересах их могущественных хозяев.

55
Компьютеры и искусственный интеллект ускоряют социальный хакинг

Хакерство старо, как само человечество. Мы, люди, взламываем системы с тех пор, как существуем, а хакинг компьютерных систем – ровесник самих компьютеров. Благодаря степени своей сложности и программируемым интерфейсам компьютеры однозначно поддаются взлому. Сегодня многие потребительские товары, такие как автомобили, бытовая техника или телефоны, управляются компьютерами. Все наши институты – финансирование, налогообложение, соблюдение нормативных требований, политические выборы – представляют собой сложные социотехнические системы, включающие компьютеры, сети, людей и организации. Это делает общество более восприимчивым к хакерским атакам.

Компьютеризация изменила и продолжает менять характер хакинга. В сочетании с методами ИИ она ускоряет его по четырем основным параметрам: скорость, масштаб, охват и сложность.

Скорость – наиболее очевидный параметр из этого списка, просто потому что компьютеры намного быстрее людей. Им не нужно спать, они не испытывают скуки и не отвлекаются от поставленных задач. Запрограммированные должным образом, они делают ошибки гораздо реже, чем люди. Это означает, что компьютеры выполняют рутинные задачи намного эффективнее[268]: чтобы произвести правильный математический расчет, смартфону требуется мизерная доля энергии и времени от тех, что затратил бы человек на решение той же задачи. Значительно сокращая трудозатраты, компьютеры превращают некоторые хаки из почти невыполнимых в простые и практичные.

Мы уже видим свидетельства этих новых возможностей. Бесплатный сервис Donotpay.com, управляемый искусственным интеллектом, автоматизирует процесс оспаривания штрафов за парковку[269], помогая отменить сотни тысяч штрафов, выписанных в Лондоне, Нью-Йорке и других городах. Услуга расширяется и на новые сферы, помогая пользователям получать компенсации за задержку авиарейсов и отменять различные подписки.

Высокая скорость ИИ также позволяет быстрее экспериментировать: компьютеры могут оперативно тестировать и отбрасывать бесчисленные варианты элементов продукта, чтобы найти лучший. A/B-тестирование, при котором разным пользователям случайным образом демонстрируются разные версии продукта, часто используется веб-разработчиками для проверки эффективности дизайна веб-страниц. Например, пользователям может быть случайно показана версия А с большой кнопкой «Нажмите здесь» и версия Б с кнопкой поменьше, при этом веб-сайт автоматически собирает данные о том, какая версия приносит максимальное количество кликов. Автоматизированное A/B-тестирование дает

---

268 Karlheinz Meier (31 May 2017), «The brain as computer: Bad at math, good at everything else,» IEEE Spectrum, https://spectrum.ieee.org/the-brain-as-computer-bad-at-math-good-at-everything-else.

269 Samuel Gibbs (28 Jun 2016), «Chatbot lawyer overturns 160,000 parking tickets in London and New York,» *Guardian*, https://www.theguardian.com/technology/2016/jun/28/chatbot-ai-lawyer-donotpay-parking-tickets-london-new-york.

разработчикам возможность [270] одновременно тестировать сложные комбинации переменных (таких, как размер, цвет, расположение и шрифт кнопки), открывая доступ к беспрецедентному разнообразию хаков, которые можно дополнительно персонализировать на основе больших данных в соответствии с предпочтениями и привычками конкретных пользователей. Возможность моделировать тысячи вариантов хаков также расширяет спектр их применения, как для бизнеса, так и для преступности.

Следующим параметром, который необходимо учитывать, является масштаб ИИ. Любая человеческая деятельность, уже имеющая историю, например биржевая торговля, кардинально меняется, обретая непреднамеренные и непредвиденные свойства, когда компьютерная автоматизация резко увеличивает ее масштаб. Системы ИИ могут заниматься теми же видами деятельности, что и создавшие их люди, но в беспрецедентных масштабах.

Можно быть почти уверенным, что в социальных сетях будут массово развернуты бот-персоны, о которых говорилось выше. Они смогут участвовать в обсуждениях круглосуточно, отправляя неограниченное число сообщений любого размера. Если позволить им разгуляться, такие боты способны подавить любые реальные онлайн-дебаты[271]. Они будут искусственно влиять на то, что мы считаем нормальным, и на то, что, по нашему мнению, думают другие, а их влияние станет ощущаться не только в социальных сетях, но и на любой публичной площадке, в гостиной каждого дома. Такого рода манипуляции вредят как рынку идей, так и любому демократическому процессу. Напомним, что для нормального функционирования демократии необходимы информация, выбор и свобода действий. Искусственные персоны могут лишить граждан как первого, так и последнего.

Сфера применения ИИ неизбежно будет расти. По мере того как компьютерные системы становятся более способными, общество будет делегировать им все больше и больше важных решений. Это означает, что хакинг этих систем будет наносить более масштабный ущерб и иметь больший потенциал разрушения базовых социотехнических систем, даже если это не будет входить в намерения хакеров.

ИИ усугубит эти тенденции. Системы ИИ уже принимают решения, которые влияют на нашу жизнь, от самых обыденных до определяющих. Они дают нам пошаговые инструкции в процессе вождения. Они решают, останетесь ли вы в тюрьме и получите ли кредит в банке. Они проверяют кандидатов на должности, абитуриентов, поступающих в колледж, и людей, обращающихся за государственными услугами. Они принимают инвестиционные решения и помогают формировать решения по уголовным делам. Они определяют, какие новости нам показывать в ленте, какие объявления мы увидим, какие люди и темы привлекают наше внимание. Они принимают военные решения о нацеливании. В будущем ИИ, вероятно, будет рекомендовать политиков для поддержки богатым политическим донорам. Он будет решать, кто имеет право голосовать, а кто – нет. Он сможет преобразовывать желаемые социальные результаты в конкретную налоговую политику или корректировать детали программ социального обеспечения.

Хаки этих важнейших систем будут становиться все более разрушительными. (Мы уже видели это на примере «внезапных» крахов фондового рынка[272].) И по большей части мы не имеем достаточного представления о том, как эти системы спроектированы, воплощены

---

[270] Amy Gallo (28 Jun 2017), «A refresher on A/B testing,» *Harvard Business Review* , https://hbr.org/2017/06/a-refresher-on-ab-testing.

[271] California has a law requiring bots to identify themselves. Renee DiResta (24 Jul 2019), «A new law makes bots identify themselves – that's the problem,» *Wired* , https://www.wired.com/story/law-makes-bots-identify-themselves.

[272] Laim Vaughan (2020), Flash Crash: A Trading Savant, a Global Manhunt, and the Most Mysterious Market Crash in History, Doubleday.

или используются.

Наконец, совершенство ИИ означает, что он все чаще будет заменять человека, поскольку компьютеры смогут реализовывать более сложные и непредвиденные стратегии, чем человек. Эти возможности только увеличатся по мере того, как компьютеры будут становиться быстрее и мощнее, а сети – сложнее.

Многие алгоритмы уже находятся за пределами человеческого понимания, будь то рекомендации фильмов к просмотру, объектов для инвестирования или очередного хода в игре го. Эта тенденция тоже будет нарастать, причем рост примет экспоненциальный характер, как только алгоритмы начнут создаваться алгоритмами.

С развитием ИИ компьютерный хакинг становится наиболее мощным способом хакнуть наши социальные системы. Когда все, по сути, является компьютером, управление этим «всем» переходит к программному обеспечению. Представьте себе хакера внутри финансовой сети, который меняет направление денежных потоков. Или хакера внутри юридических баз данных, который вносит небольшие, но существенные изменения в законы и судебные решения. (Смогут ли люди заметить это? Будут ли они знать достаточно, чтобы свериться с первоначальной формулировкой?) Представьте себе хакера, переписывающего алгоритмы Facebook изнутри, меняющего правила, чей пост поднимается в ленте, чей голос усиливается и кто его будет слышать. Когда компьютерные программы управляют системами, которые мы используем повседневно – для работы, трат, общения, организации времени и личной жизни, – технология сама становится политическим деятелем. И при всей свободе, которую нам дают технологии, в руках хакера они могут превратиться в орудие беспрецедентного социального контроля.

Все системы уязвимы для хакинга. Более того, современные исследования показывают, что все системы МО могут быть хакнуты незаметно. И эти хаки будут иметь все более серьезные социальные последствия.

56
Когда искусственный интеллект становится хакером

Старое хакерское состязание «Захват флага» – это, по сути, подвижная игра на открытом воздухе, перенесенная в компьютер. Команды защищают свои сети, атакуя сети других команд. Игра отражает в контролируемой обстановке то, чем занимаются компьютерные хакеры в реальной жизни: поиском и исправлением уязвимостей в своих системах и их использованием в чужих.

Эта игра стала основным развлечением на хакерских конференциях с середины 1990-х гг. В наши дни десятки команд со всего мира принимают участие в состязательных марафонах, которые проводятся в течение выходных. Люди тратят месяцы на подготовку, а победа становится большим событием. Если вы увлекаетесь подобными вещами, то это самое лучшее развлечение для хакера, которое не сделает вас преступником.

DARPA Cyber Grand Challenge – аналогичное мероприятие для ИИ[273], проводившееся в 2016 г. В нем приняли участие 100 команд. После прохождения отборочных туров семь финалистов встретились на хакерской конференции DEF CON в Лас-Вегасе. Соревнование проходило в специально разработанной тестовой среде, наполненной пользовательским программным обеспечением, которое никогда не анализировалось и не тестировалось. ИИ было дано 10 часов на поиск уязвимостей, чтобы использовать их против других ИИ, участвующих в соревновании, и на исправление собственных уязвимостей. Победила система под названием Mayhem, созданная группой исследователей компьютерной

273 Jia Song and Jim Alves-Foss (Nov 2015), «The DARPA Cyber Grand Challenge: A competitor's perspective,» IEEE *Security and Privacy Magazine* 13, no. 6, https://www.researchgate.net/publication/286490027_The_DARPA_cyber_grand_challenge_A_competitor%27s_perspective.

безопасности из Питтсбурга. С тех пор они коммерциализировали эту технологию, и сейчас она активно защищает сети таких клиентов, как министерство обороны США.

В том же году на DEF CON проводилась игра «Захват флага» с участием человеческих команд. Единственное исключение сделали для Mayhem – ее тоже пригласили поиграть. Система ИИ заняла последнее место в общем зачете, но в некоторых категориях показала не самые плохие результаты. Несложно себе представить, как эти смешанные соревнования развернутся в будущем. Мы видели траекторию развития подобной конкуренции на примере шахмат и игры го. Участники с ИИ будут прогрессировать с каждым годом, поскольку все основные технологии совершенствуются. Команды людей в основном останутся на прежнем уровне, потому что люди остаются людьми, даже когда совершенствуются наши инструменты и владение ими. В конце концов ИИ, вероятно, станет регулярно побеждать людей. Я готов дать прогноз, что на это уйдет не более десяти лет.

По необъяснимым причинам DARPA так и не повторила «Захват флага» с участием ИИ, зато Китай с тех пор взял такой формат на вооружение: он регулярно устраивает разнообразные гибридные игрища, в которых команды людей и компьютеров соревнуются друг с другом. Подробностей мы не знаем, поскольку такие соревнования проводятся только внутри страны и все чаще организуются военными, но доподлинно известно, что китайские системы ИИ быстро совершенствуются[274].

Пройдут годы, прежде чем мы полностью раскроем возможности ИИ в плане автономных кибератак, но эти технологии уже меняют их характер. Одной из областей, которая кажется особенно плодотворной для систем ИИ, является поиск уязвимостей. Просматривание программного кода строка за строкой – это именно та утомительная задача, в которой ИИ преуспевает, если только научить его распознавать уязвимости. Конечно, необходимо будет решить множество проблем, связанных с конкретными областями применения, но по этой теме уже существует академическая литература, и исследования продолжаются[275]. Есть все основания ожидать, что со временем системы ИИ будут улучшаться и в итоге приблизятся к совершенству.

Последствия этого потенциала простираются далеко за пределы компьютерных сетей. Нет никаких причин, по которым ИИ не сможет найти тысячи новых уязвимостей в системах, о которых шла речь в этой книге: налоговом кодексе, банковских правилах, политических процессах. Везде, где есть большой массив правил, взаимодействующих друг с другом, ИИ с большой вероятностью найдет уязвимости и создаст эксплойты для их компрометации. Сегодня системы ИИ уже вовсю ищут лазейки в коммерческих контрактах[276].

Со временем эти возможности будут шириться. Любой хакер из плоти и крови хорош лишь настолько, насколько он понимает систему, на которую нацелился, и ее взаимодействие с остальным миром. ИИ достигает этого понимания практически сразу, благодаря данным, на которых его обучают, и продолжает совершенствоваться по мере своего использования. Современные системы ИИ развиваются непрерывно, получая все новые данные и соответствующим образом корректируя свою работу. На этом потоке данных ИИ продолжает обучаться и пополнять свой опыт прямо в процессе работы. Именно

---

274 Dakota Cary (Sep 2021), «Robot hacking games: China's competitions to automate the software vulnerability lifecycle,» Center for Security and Emerging Technology, https://cset.georgetown.edu/wp-content/uploads/CSET-Robot-Hacking-Games.pdf.

275 Bruce Schneier (18 Dec 2018) «Machine learning will transform how we detect software vulnerabilities,» *Security Intelligence*, https://securityintelligence.com/machine-learning-will-transform-how-we-detect-software-vulnerabilities.

276 Economist staff (12 Jun 2018), «Law firms climb aboard the AI wagon,» *Economist*, https://www.economist.com/business/2018/07/12/law-firms-climb-aboard-the-ai-wagon.

по этой причине разработчики систем ИИ для беспилотных автомобилей любят хвастаться количеством часов, проведенных на дорогах их детищами.

Разработка систем ИИ, способных взламывать другие системы, порождает две связанные между собой проблемы. Во-первых, ИИ может получить указание взломать систему. Кто-то может «скормить» ИИ налоговые кодексы или правила мировой финансовой игры с целью создания прибыльных хаков. Во-вторых, ИИ может взломать систему случайно в процессе своей работы. Оба сценария не сулят ничего хорошего, но второй куда опаснее, поскольку мы можем так и не узнать, что произошло.

57
Хакинг ради цели

Как я уже отмечал ранее, ИИ решает проблемы не так, как люди. Он неизбежно натыкается на решения, которые мы просто не способны предвидеть. Некоторые из этих решений могут подрывать цель анализируемой системы в силу того, что ИИ не учитывает последствия, контекст, нормы и ценности, которые люди принимают как само собой разумеющиеся.

В отношении ИИ выражение «*хакинг ради цели* » означает, что для решения поставленной задачи он может действовать так, как не планировали его разработчики[277]. Приведу несколько ярких примеров.

● В футбольном симуляторе в режиме «один на один» игрок должен был забивать голы вратарю. Вместо того чтобы наносить удар, когда игрок оказывался прямо напротив ворот, система ИИ принимала решение выбивать мяч за пределы поля [278] . Вратарь, как единственный представитель команды-соперника, должен был сам вбрасывать мяч из-за боковой, оставив ворота незащищенными.

● ИИ было поручено сложить из виртуальных блоков[279] максимально высокую стену. Высота измерялась по нижней грани последнего блока. ИИ научился переворачивать этот блок так, чтобы его нижняя грань была обращена вверх и стена казалась выше. (Очевидно, что в правилах не было четких указаний относительно того, как должны быть ориентированы блоки.)

● В моделируемой среде для «эволюционирующих» существ ИИ было разрешено изменять физические характеристики своего персонажа, чтобы лучше достигать разных целей. Когда исследователи поставили перед ИИ задачу как можно быстрее пересечь далекую финишную черту, они ожидали, что тот отрастит персонажу длинные ноги, увеличит объем мышц или легких. Но вместо этого ИИ сделал своего персонажа достаточно высоким[280], чтобы тот пересек финишную черту, просто упав на нее.

Все это хаки. Вы можете подумать, что дело в плохой формулировке задач, и будете правы. Вы можете указать на то, что все это происходило в симулированной среде, и тоже будете правы. Но проблема, которую иллюстрируют эти примеры, является более общей: ИИ создан оптимизировать свои функции для достижения цели. При этом он может

---

[277] A list of examples is here. Victoria Krakovna (2 Apr 2018), «Specification gaming examples in AI,» https://vkrakovna.wordpress.com/2018/04/02/specification-gaming-examples-in-ai.

[278] Karol Kurach et al. (25 Jul 2019), «Google research football: A novel reinforcement learning environment,» arXiv, https://arxiv.org/abs/1907.11180.

[279] Ivaylo Popov et al. (10 Apr 2017), «Data-efficient deep reinforcement learning for dexterous manipulation,» arXiv, https://arxiv.org/abs/1704.03073.

[280] David Ha (10 Oct 2018), «Reinforcement learning for improving agent design,» https://designrl.github.io.

естественным образом непреднамеренно внедрять неожиданные хаки.

Представьте, что роботу-пылесосу[281] поручено убирать любой мусор, который он увидит. Если цель не определена более точно, он может просто отключить или прикрыть непрозрачным материалом свои визуальные датчики, чтобы не видеть грязь. В 2018 г. один предприимчивый – а возможно, и просто скучающий – программист решил, что не хочет, чтобы его робот-пылесос постоянно натыкался на мебель[282]. Он настроил систему обучения таким образом, чтобы она поощряла робота, когда тот не задевал препятствия датчиками. Однако вместо того, чтобы перестать натыкаться на мебель, ИИ научился водить пылесос задним ходом, поскольку на задней части устройства попросту не было датчиков – все они размещались спереди.

Если в наборе правил есть нестыковки или лазейки и если они могут привести к приемлемому решению, то ИИ найдет их. Взглянув на такие результаты, мы можем сказать, что технически ИИ следовал правилам. Но все же мы будем чувствовать в этом отклонение и обман, потому что понимаем социальный контекст проблемы так, как не понимает его ИИ. Просто у нас другие ожидания. Исследователи называют эту проблему «согласованием целей».

Ее хорошо иллюстрирует миф о царе Мидасе. Когда бог Дионис готов исполнить его единственное желание, Мидас просит, чтобы все, к чему он прикоснется, превращалось в золото. В итоге Мидас умирает от голода и несчастий, поскольку вся еда, питье и даже его дочь превращаются в непригодное для употребления в пищу и безжизненное золото. Это не что иное, как проблема согласования целей: Мидас неверно запрограммировал цель в своей системе желаний.

Джинны в сказках тоже весьма привередливы к формулировкам желаний и могут быть злонамеренно педантичны, исполняя их. Но перехитрить джинна невозможно. Что бы вы ни пожелали, джинн всегда сможет исполнить это так, чтобы вам захотелось все отменить. Джинн всегда сможет хакнуть ваше желание.

В более общем смысле наши цели и желания всегда недостаточно конкретны[283]. Мы никогда не представляем себе всех возможных вариантов. Мы никогда не формулируем все нюансы, исключения и оговорки. Мы просто не способны перекрыть все пути для хака. Любая цель, которую мы укажем, обязательно будет неполной.

Это приемлемо в человеческих отношениях, потому что люди понимают контекст и обычно действуют добросовестно. Мы все социализированы и в процессе становления познаем, что значит здравый смысл в отношении людей и окружающего мира. Мы заполняем любые пробелы в нашем понимании контекстом и доброй волей.

Философ Эбби Эверетт Жак, в то время руководитель проекта MIT по этике ИИ, объяснил это так: «Если бы я попросил вас принести мне кофе, вы, вероятно, пошли бы к ближайшему кофейнику и наполнили чашку, а может быть, дошли бы до кофейни на углу. Вы бы не привезли мне грузовик с сырыми кофейными зернами. И не купили бы кофейную плантацию в Коста-Рике. Вы также не стали бы вырывать из рук чашку кофе у первого попавшегося человека. Холодный кофе недельной давности или грязную салфетку, пропитанную искомым напитком, вы бы тоже не принесли. Мне не нужно было бы все это уточнять в своей просьбе. Вы и так прекрасно понимаете, что значит "принести кофе"».

---

281 Dario Amodei et al. (25 Jul 2016), «Concrete problems in AI safety,» arXiv, https://arxiv.org/pdf/1606.06565.pdf.

282 Custard Smingleigh (@Smingleigh) (7 Nov 2018), Twitter, https://twitter.com/smingleigh/status/1060325665671692288.

283 Abby Everett Jaques (2021), «The Underspecification Problem and AI: For the Love of God, Don't Send a Robot Out for Coffee,» unpublished manuscript.

Точно так же, если я попрошу вас разработать технологию, которая при прикосновении превращает вещи в золото, вы не станете создавать ее такой, чтобы она морила меня голодом. Мне не нужно было бы указывать это, вы бы это просто знали.

Мы не можем полностью указать цели для ИИ, а ИИ не сможет полностью понять контекст. В своем выступлении на TED исследователь ИИ Стюарт Рассел пошутил о гипотетическом ИИ-помощнике[284], который, для того чтобы оправдать опоздание своего хозяина на званый ужин, устраивает сбой в компьютерной системе самолета, в котором тот летит. Аудитория оценила шутку, но ведь на самом деле откуда компьютерной программе знать, что вмешательство в работу систем летящего самолета не является адекватным ответом на подобную просьбу? Возможно, она обучилась на данных отчетов о пассажирах, пытавшихся сделать нечто подобное[285]. (В 2017 г. в интернете ходила шутка. Джефф Безос: «Алекса, купи мне что-нибудь в Whole Foods». Алекса: «ОК, покупаю Whole Foods».)

В 2015 г. компания Volkswagen была уличена в мошенничестве с тестами на выбросы. Компания не подделывала их результаты; вместо этого она разработала для своих автомобилей бортовые компьютеры, которые бы обманывали контрольные устройства. Инженеры запрограммировали их таким образом, чтобы они определяли, когда автомобиль проходит тест на выбросы. Компьютер включал систему контроля выбросов на время теста и отключал ее по его окончании. На самом же деле автомобили Volkswagen, демонстрирующие превосходные ходовые качества, выбрасывали до 40 раз больше допустимого количества оксида азота, но только тогда, когда за этим не следило Агентство по охране окружающей среды США (EPA).

История Volkswagen не связана с искусственным интеллектом – обычные инженеры запрограммировали обычную компьютерную систему на обман, – но тем не менее она хорошо иллюстрирует проблему. Более десяти лет компании сходило с рук мошенничество только потому, что компьютерный код сложен и трудно поддается анализу. Непросто понять, что именно он делает, и точно так же непросто было понять, что делает автомобиль. До тех пор пока программисты хранят свой секрет, подобный хак, скорее всего, будет оставаться необнаруженным. Единственная причина, по которой сегодня мы знаем об уловке Volkswagen, заключается в том, что группа ученых из Университета Западной Вирджинии неожиданно проверила выбросы автомобилей на дорогах с помощью системы, отличной от системы EPA. Поскольку программное обеспечение было разработано для обхода системы EPA, ученым удалось провести измерение выбросов незаметно для бортового компьютера.

Если бы я попросил вас разработать программное обеспечение для управления двигателем автомобиля, чтобы обеспечить максимальную производительность и при этом пройти тесты на выбросы, вы бы не стали разрабатывать его, понимая, что это обман. Для ИИ это не является проблемой. Он не воспринимает абстрактную концепцию обмана

---

284 Stuart Russell (Apr 2017), «3 principles for creating safer AI,» TED2017, https://www.ted.com/talks/stuart_russell_3_principles_for_creating_safer_ai.

285 Мелисса Кёниг (9 сентября 2021 г.): «46-летняя женщина, опаздывая со своим сыном-школьником на рейс JetBlue, „сделала ложное заявление, что заложила на борту бомбу“, чтобы задержать самолет». *Daily Mail* , https://www.dailymail.co.uk/news/article-9973553/Woman-46-falsely-claims-planted-BOMB-board-flight-effort-delay-plane.html. Элла Торрес (18 января 2020 г.): «Полиция сообщает, что жительница Лондона заявила о якобы заложенной в самолет бомбе, чтобы задержать рейс, на который опаздывала». *ABC News* , https://abcnews.go.com/International/london-man-reports-fake-bomb-threat-delay-flight/story?id=68369727. Питер Стабли (16 августа 2018 г.): «Человек выдумывает бомбу, чтобы задержать свой рейс», *Independent* , https://www.independent.co.uk/news/uk/crime/man-late-flight-hoax-bomb-threat-gatwick-airport-los-angeles-jacob-meir-abdellak-hackney-a8494681.html. (20 января 2007 г.): «В Турции женщина задержала самолет с помощью ложного сообщения о заложенной бомбе». *Reuters* , https://www.reuters.com/article/us-turkey-plane-bomb-idUSL2083245120070620.

на инстинктивном уровне. Он будет мыслить «нестандартно» просто потому, что не обладает представлением об ограничениях человеческих решений. Он также не понимает абстрактных этических концепций. Он не поймет, что решение Volkswagen нанесло вред другим людям, что оно подрывает сам замысел тестов на выбросы или что решение компании было незаконным, если только данные, на которые опирается ИИ, не включают законы, касающиеся выбросов. ИИ даже не поймет, что взламывает систему. И благодаря проблеме объяснимости мы, люди, тоже можем этого не понять.

Если ИИ-программисты не укажут, что система не должна менять свое поведение при тестировании, ИИ тоже сможет додуматься до такого обмана. Программисты будут довольны. Бухгалтеры будут в восторге. И никто, скорее всего, не поймает его с поличным. Теперь, когда скандал с Volkswagen подробно задокументирован, программисты могут четко поставить цель избежать конкретно этого хака. Однако рано или поздно возникнут новые непредвиденные действия ИИ, которые программисты не смогут предугадать. Урок джинна заключается в том, что так будет всегда.

58
Защита от хакеров с искусственным интеллектом

Очевидные хаки не единственная проблема. Если навигационная система вашего беспилотного автомобиля решает задачу поддержания высокой скорости за счет того, что автомобиль просто носится по кругу, программисты заметят такое поведение и соответствующим образом скорректируют цель ИИ. Но на дороге мы никогда не увидим подобного поведения. Наибольшее беспокойство вызывают менее очевидные взломы, которых мы даже не замечаем.

Многое было написано о рекомендательных системах[286] – первом поколении тонких хаков ИИ – и о том, как они подталкивают людей к поляризованному контенту. Они не были запрограммированы на это изначально. Такое свойство системы приобрели естественным образом, постоянно пробуя что-то, оценивая результаты, а затем модифицируя себя, чтобы действовать, повышая вовлеченность пользователей. Алгоритмы рекомендаций YouTube и Facebook научились предлагать пользователям более экстремальный контент, потому что он вызывает сильные эмоциональные реакции, и именно это заставляет людей проводить больше времени на платформе. Довольно простая автоматизированная система сама нашла этот хак. И большинство из нас в то время не осознавали, что происходит.

Аналогичным образом в 2015 г. ИИ научился играть в аркадную видеоигру 1970-х гг. Breakout. ИИ ничего не сообщали о правилах или стратегии игры. Ему просто дали управление и награждали за набор максимального количества очков. То, что он научился играть, неудивительно: все и так этого ожидали. Однако ИИ самостоятельно открыл и оптимизировал до не досягаемого людьми уровня тактику «туннелирования» сквозь кирпичную стену, чтобы отбивать мяч от ее обратной стороны.

Ничто из сказанного здесь не станет новостью для исследователей ИИ, и многие из них в настоящее время рассматривают способы защиты от взлома ради цели. Одним из решений является обучение ИИ контексту. Наряду с проблемой согласования целей исследователи рассматривают проблему согласования ценностей, чтобы создать ИИ, который лучше бы понимал человека. Решение этой проблемы можно представить как две крайности. С одной стороны, мы можем в форме прямых указаний закачать в ИИ наши ценности. В какой-то мере это можно сделать уже сегодня, но такой подход уязвим для всех описанных выше хаков. С другой стороны, мы можем создать ИИ, который изучит наши ценности, возможно

---

286 Zeynep Tufekci (10 Mar 2018), «YouTube, the great equalizer,» *The New York Times* , https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html. Renee DiResta (11 Apr 2018), «Up next: A better recommendation system,» *Wired* , https://www.wired.com/story/creating-ethical-recommendation-engines.

наблюдая за людьми в действии или взяв в качестве входных данных человеческую историю, литературу, философию и т. д. Это проект на много лет вперед, и, вероятно, именно такой подход задаст ряд свойств общему ИИ. Большинство же современных исследований колеблется между этими двумя крайностями.

Несложно представить себе вопросы, которые возникнут, когда ИИ придет в соответствие с человеческими ценностями. Чьи ценности он должен будет отражать? Сомалийского мужчины? Сингапурской женщины? Или нечто среднее между ними, что бы это ни значило? Люди часто придерживаются противоречивых ценностей и бывают непоследовательны, пытаясь жить в соответствии с ними. Ценности отдельно взятого человека могут быть иррациональными, аморальными или основанными на ложной информации. История, литература и философия тоже полны иррациональности, безнравственности и ошибок. Люди в принципе далеки от собственных идеалов.

Наиболее эффективная защита от любых хаков основана на выявлении уязвимостей, то есть на обнаружении и устранении хакерских атак еще до того, как они будут совершены. В этом могут существенно помочь технологии ИИ, тем более что они могут работать на сверхчеловеческих скоростях.

Однако вспомните, о чем мы говорили, когда рассматривали компьютерные системы. Как только ИИ станет способен обнаруживать новые уязвимости в программном обеспечении, фору получат все стороны, а значит, и правительственные хакеры, и криминал, и любители. Они смогут использовать новые уязвимости для компрометации компьютерных сетей по всему миру. Это поставит под угрозу всех нас.

Но та же самая технология будет более эффективно работать на безопасность, поскольку обнаруженная уязвимость может быть устранена навсегда. Представьте себе, что компания-разработчик программного обеспечения сможет внедрять ИИ-детектор уязвимостей непосредственно в код программы. Уязвимости будут найдены и устранены еще до того, как программное обеспечение будет выпущено. Тестирование может идти автоматически в процессе разработки. Таким образом, хотя и нападение, и защита будут иметь доступ к одной и той же технологии, защита сможет использовать ее для постоянного повышения безопасности своих систем. Мы можем надеяться на будущее, когда уязвимости программного обеспечения уйдут в прошлое. «Помните первые десятилетия вычислительной техники, когда хакеры взламывали программы через уязвимости? Вот было безумное времечко!»

Конечно, переходный период простым не будет. Новый код может быть безопасным, но старый все еще будет уязвим. Злоумышленники сосредоточат свои ИИ-инструменты на автоматическом поиске уязвимостей в уже действующем старом коде, который часто невозможно исправить. Однако в долгосрочной перспективе технология ИИ для поиска уязвимостей в программном обеспечении благоприятствует тем, кто защищает системы от вторжений и нанесения им вреда.

Это утверждение справедливо и для более широких социальных систем. Когда ИИ начнет находить уязвимости в политических, экономических и социальных системах, они будут использоваться в преступных целях. Более того, эти взломы могут способствовать интересам тех, кто контролирует системы ИИ. Индивидуально подобранная реклама намного убедительнее, а значит, она будет оплачена теми, в чьих интересах работает. Когда ИИ обнаружит новую налоговую лазейку, можно не сомневаться, что к ней тут же появится эксплойт, потому что те, кто имеет доступ к системе ИИ, захотят снизить свое налоговое бремя. Хакинг в значительной степени укрепляет существующие структуры власти, а ИИ будет усиливать их еще больше, если мы не научимся преодолевать существующий дисбаланс.

Однако, как и в случае компьютерных систем, та же самая технология будет полезнее стороне защиты[287]. Хотя ИИ-хакеры могут найти тысячи уязвимостей в существующем

[287] One example: Gregory Falco et al. (28 Aug 2018), «A master attack methodology for an AI-based automated

налоговом кодексе, эта же технология может быть использована для оценки потенциальных уязвимостей в любых новых законопроектах или постановлениях, касающихся сферы налогообложения. Последствия этого радикально изменят правила игры. Представьте себе, что по такому принципу проверяется новый налоговый закон. Законодатель, наблюдательная организация, журналист или любой заинтересованный гражданин могут проанализировать текст законопроекта с помощью системы ИИ, чтобы найти уязвимости. Это не означает, что они сразу будут исправлены (помните, что исправление уязвимостей – это отдельный процесс), но они как минимум будут вынесены в публичное поле. Теоретически эти лазейки можно будет устранить еще до того, как кто-нибудь ими воспользуется, но здесь вновь выходят на первый план опасности переходного периода, который будет протекать в среде унаследованных законов и правил. И все-таки в долгосрочной перспективе технология поиска уязвимостей с помощью ИИ благоприятствует защите.

Это и хорошо, и плохо. Хорошо, поскольку технология может быть использована обществом для предотвращения взлома систем правящими элитами. Плохо, потому что элиты с большей вероятностью возьмут ее на вооружение, чтобы противостоять общественному контролю и социальным изменениям. Как и всегда, все упирается в структуру власти.

59
Будущее хакеров с искусственным интеллектом

Насколько реалистичен сценарий будущего, в котором процветают ИИ-хакеры?

Его осуществимость зависит от конкретных моделируемых и взламываемых систем. Чтобы ИИ просто начал оптимизировать готовое решение, не говоря уже о разработке нового, все правила среды должны быть формализованы в понятном компьютеру виде. Необходимо определить целевые функции для ИИ, то есть установить цели. ИИ нуждается в обратной связи, чтобы понимать, насколько хорошо он справляется со своими задачами, и улучшать свою производительность.

Иногда это сделать просто. Например, для игры го правила, цель и обратная связь – выиграл или проиграл – четко определены, и ничто не может внести хаос. ИИ GPT-3 пишет относительно связные эссе, потому что его «мир» полностью подчиняется прозрачным правилам организации текста. Вот почему большинство современных примеров ИИ-хакинга ради цели происходят в смоделированных средах. Они искусственны и ограниченны, что позволяет задать ИИ четкие правила.

Степень неоднозначности, присутствующая в системе, играет здесь ключевую роль. Казалось бы, несложно «скормить» ИИ мировые налоговые законодательства, поскольку любой налоговый кодекс сводится к формулам, определяющим сумму налога в каждом конкретном случае. Существует даже язык программирования Catala, который оптимизирован для кодирования законов. Тем не менее любой закон всегда содержит некоторую неоднозначность. Она не поддается переводу в код, поэтому не по зубам ИИ. Налоговые юристы могут спать спокойно: несмотря на развитие ИИ, в обозримом будущем их услуги останутся востребованными.

Большинство человеческих систем еще более неоднозначны, чем законодательство. Трудно вообразить, что ИИ сможет произвести на свет реальный спортивный хак, такой как изогнутая хоккейная клюшка. ИИ должен досконально понимать не только правила игры, но и физиологию человека, аэродинамику клюшки и шайбы и т. д. Теоретически это возможно, но намного сложнее, чем придумать новый ход в игре го.

Эта неоднозначность, скрыто присутствующая в наших сложных общественных системах, и обеспечивает защиту от ИИ-хакеров, по крайней мере в ближайшем будущем.

---

attack planner for smart cities,» IEEE Access 6, https://ieeexplore.ieee.org/document/8449268.

Мы не увидим спортивных хаков, сгенерированных ИИ, до тех пор, пока андроиды сами не начнут гонять мяч или не будет разработан общий ИИ, способный понимать мир во всех его пересекающихся измерениях. То же самое можно сказать относительно хакинга казино (когда уже ИИ научится хорошо мухлевать?!) и законодательного процесса. Пройдет еще много времени, прежде чем ИИ сможет моделировать и имитировать то, как работают люди, по одному и в группах, чтобы придумывать новые способы взлома законодательных процессов.

Но хотя мир, наполненный ИИ-хакерами, существует сегодня только в книгах и фильмах, эта серьезная проблема все больше выходит за рамки научной фантастики. Прогресс в сфере ИИ идет невероятно быстрыми темпами, а новые возможности открываются внезапно и скачкообразно. То, что еще вчера мы считали почти невозможным, оказалось проще простого, а то, что казалось легким, превратилось в большую проблему. Когда я учился в университете в начале 1980-х гг., нас уверяли, что игра го никогда не будет освоена компьютером в силу ее высокой сложности: не самих правил, а огромного количества возможных ходов. Сегодня ИИ – это гроссмейстер игры го.

Поэтому, хотя ИИ претендует на роль проблемы завтрашнего дня, мы видим ее предвестников уже сегодня. Нам необходимо начать думать о том, какие решения, понятные и этичные, есть в нашем распоряжении, потому что если мы и можем быть в чем-то уверены относительно ИИ, так это в том, что эти решения понадобятся нам раньше, чем мы могли бы ожидать.

Вероятно, первым местом, где следует искать следы хакерских атак, генерируемых ИИ, являются финансовые системы, поскольку их правила разработаны таким образом, чтобы быть реализованными посредством алгоритмов. Алгоритмы высокочастотной торговли являются примитивным примером таких атак: в будущем они станут намного сложнее. Мы можем представить себе, как в режиме реального времени в систему ИИ закачивается вся мировая финансовая информация, мировые законы и правила, новостные ленты и все остальное, что, по нашему мнению, может иметь значение, а затем перед ним ставится цель получения максимальной законной прибыли или даже просто максимальной. Я полагаю, что это время не за горами, и уже скоро мы увидим новые, совершенно неожиданные хаки[288]. И, вероятно, будут такие хаки, которые находятся где-то за гранью человеческого понимания, а это значит, мы никогда не поймем, что они в принципе существуют.

В краткосрочной перспективе, скорее всего, наберет обороты совместный хакинг ИИ и человека. ИИ будет выявлять уязвимости, а опытные бухгалтеры или налоговые юристы – применять свой опыт и суждения, чтобы понять, можно ли с выгодой их использовать.

На протяжении почти всей истории хакинг был исключительно человеческим занятием. Поиск новых хаков требует опыта, времени, креативности и удачи. Когда ИИ начнет заниматься хакингом, ситуация в корне изменится. Для ИИ не существует стереотипов и ограничений, свойственных людям. Ему не нужно спать. Он мыслит как инопланетянин. И он будет хакать системы такими способами, о которых мы даже помыслить не можем.

Как я уже сказал в главе 55, компьютеры ускорили процесс хакинга по четырем параметрам: скорость, масштаб, охват и сложность. ИИ еще больше усугубит эту тенденцию.

Сначала о скорости. Процесс подготовки и внедрения хака, который для нас занимает месяцы или годы, может сократиться до дней, часов или даже секунд. Что может произойти, если вы «скормите» ИИ налоговый кодекс США и прикажете ему вычислить все способы минимизации налоговых обязательств? Или, в случае транснациональной корпорации,

---

288 Хедж-фонды и инвестиционные компании уже используют ИИ для обоснования инвестиционных решений. Luke Halpin and Doug Dannemiller (2019), «Artificial intelligence: The next frontier for investment management firms,» Deloitte, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/fsi-artificial-intelligence-investment-mgmt.pdf. Peter Salvage (March 2019), «Artificial intelligence sweeps hedge funds,» BNY Mellon, https://www.bnymellon.com/us/en/insights/all-insights/artificial-intelligence-sweeps-hedge-funds.html.

проанализировать и оптимизировать налоговую политику на базе налоговых кодексов всей планеты? Может ли ИИ без подсказок понять, что разумнее всего зарегистрировать компанию в Делавэре, а судно – в Панаме? Сколько лазеек он найдет, о которых мы еще не знаем? Десятки? Сотни? Тысячи? Ответов на эти вопросы у нас пока нет, но, вероятно, они появятся в течение следующего десятилетия.

Далее о масштабе. Когда системы ИИ начнут обнаруживать уязвимости, они смогут использовать их в таких масштабах, к которым мы просто не готовы. ИИ, успешно хакнувший финансовые системы, будет доминировать в этой сфере. Уже сейчас наши кредитные рынки, налоговые кодексы и законы в целом ориентированы на богатых. ИИ усилит это неравенство. Первые ИИ-хаки для взлома финансовых систем будут разработаны не исследователями, стремящимися восстановить справедливость, а глобальными банками, хедж-фондами и консультантами по управлению капиталом.

Теперь об охвате. У нас есть социальные системы, которые неплохо справляются с хакерскими атаками, но они были разработаны, когда хакерами были люди, а взломы осуществлялись в человеческом темпе. У нас нет системы управления, которая могла бы быстро и эффективно реагировать на волну атак через сотни, не говоря уже о тысячах, свежеобнаруженных налоговых лазеек: мы просто не сможем исправить налоговый кодекс так быстро. Мы не смогли предотвратить использование людьми Facebook для хакинга демократии; сложно представить, что может произойти, когда этим займется ИИ. Если ИИ начнет вычислять непредвиденные, но легальные хаки финансовых систем, а затем устроит мировой экономике безумные пляски, восстановление будет долгим и болезненным.

И, наконец, о сложности. Хакинг с помощью ИИ открывает путь для сложных стратегий, выходящих за рамки того, что может создать человеческий разум. Сложный статистический ИИ-анализ может выявлять взаимосвязи между переменными, а значит, и возможные эксплойты, которые лучшие стратеги и эксперты никогда бы не распознали. Такая изощренность может позволить ИИ развертывать стратегии, подрывающие сразу несколько уровней целевой системы. Например, ИИ, созданный для максимизации доли голосов политической партии, может определять точную комбинацию экономических переменных, предвыборной агитации и процедурных настроек голосования, которые могут принести победу на выборах. Это новый виток той самой революции, которую устроила картография, обеспечив появление джерримендеринга. И это не говоря о трудно обнаруживаемых хаках, которые ИИ может внедрить для манипулирования фондовым рынком, законодательными системами или общественным мнением.

Достигнув сверхчеловеческой скорости, гигантских масштабов, размаха и сложности, хакинг превратится в проблему, с которой мы как общество уже не сможем совладать.

Мне вспоминается сцена из фильма «Терминатор», где Кайл Риз описывает Саре Коннор киборга, который на нее охотится: «С ним бесполезно торговаться. Его нельзя переубедить. Оно не чувствует ни жалости, ни раскаяния, ни страха. И оно не остановится. Никогда…» Я не утверждаю, что нам придется иметь дело с киборгами-убийцами в буквальном смысле, но по мере того, как ИИ становится нашим противником в мире социального хакинга, попытки угнаться за его нечеловеческой способностью выискивать наши уязвимости будут точно так же обречены.

Некоторые исследователи ИИ выражают опасения в отношении того, что сверхмощные системы ИИ могут преодолеть наложенные человеком ограничения и потенциально захватить господствующую роль в обществе. Хотя это смахивает на дешевую спекуляцию, такой сценарий все же стоит рассмотреть и принять меры для его предотвращения.

Однако сегодня и в ближайшем будущем хакерские атаки, описанные в этой книге, будут по-прежнему осуществляться в основном правящими элитами против обычных граждан. Все существующие системы ИИ, воплощенные в вашем ноутбуке, облаке или роботе, запрограммированы другими людьми и, как правило, в их интересах, а не в ваших. Хотя подключенное к интернету устройство, такое как Alexa, может имитировать надежного друга, нельзя забывать, что оно создано в первую очередь для продажи товаров

компании Amazon. И точно так же, как веб-сайт Amazon подталкивает вас к покупке его домашних брендов вместо более качественных конкурирующих товаров, Alexa далеко не всегда действует в ваших интересах. Если говорить точнее, она хакает ваше доверие ради целей акционеров Amazon.

В отсутствие какого-либо значимого регулирования мы действительно ничего не можем сделать, чтобы предотвратить распространение ИИ-хакинга. Нам нужно просто принять его неизбежность и создать надежные структуры управления, которые смогут быстро и эффективно реагировать, нормализуя полезные хаки и нейтрализуя вредоносные или непреднамеренно наносящие ущерб.

Эта проблема поднимает более глубокие и сложные вопросы, чем те, о которых мы говорили: как будет развиваться ИИ? Как должны реагировать общественные институты? Какие хаки считать полезными, а какие вредными? Кто принимает решения? Если вы свято верите в то, что правительство должно быть немногочисленным и малозаметным, то, вероятно, вам придутся по душе хаки, которые снижают возможности правительств в плане контроля над гражданами. Однако и в этом случае вы вряд ли захотите сменить политических владык на технологических. Если вы исповедуете принцип превентивности[289], то должны понимать, как важно, чтобы разные эксперты тестировали и оценивали хаки, прежде чем они будут внедрены в наши социальные системы. И, возможно, стоит применить этот принцип и «выше по течению», то есть к институтам и структурам, которые делают эти хаки возможными.

Вопросы только множатся. Должны ли ИИ-хакеры регулироваться локально или глобально? Администраторами или референдумом? Есть ли какой-то способ позволить рынку или гражданскому обществу принимать решения? (Нынешние попытки применить модели управления к алгоритмам служат ранним индикатором того, как это будет происходить.) Структуры управления, которые мы разрабатываем, предоставят отдельным людям и организациям право отбирать хаки, которые определят будущее. И нужно сделать так, чтобы эти полномочия использовались с умом.

60
Системы управления хакингом

Защитный ИИ – это потенциальный ответ на ИИ-хакинг. Пока он еще недостаточно развит, чтобы можно было реализовать этот проект. Сегодня нам нужны люди и команды, которые бы включились в разработку структур управления и последующий процесс внедрения этой технологии.

Как должны выглядеть такие структуры управления, пока не совсем ясно, но уже выдвинуто немало интересных предложений по новым моделям регулирования, которые могли бы эффективно решать проблемы, связанные со скоростью, масштабом, охватом и сложностью ИИ. Технологи ИИ и лидеры отрасли, такие как Ник Гроссман [290], предложили, чтобы интернет-компании и компании больших данных перешли от парадигмы регулирования 1.0, при которой запускаемые проекты не проходят соответствующую проверку и не предоставляют отчетность, к парадигме регулирования 2.0, когда любые новые проекты подлежат строгой, основанной на данных проверке и должным образом ограничиваются. В главе 33 мы рассмотрели лучшую из систем управления, которая у нас

---

289 Maciej Kuziemski (1 May 2018), «A precautionary approach to artificial intelligence,» Project Syndicate, https://www.project-syndicate.org/commentary/precautionary-principle-for-artificial-intelligence-by-maciej-kuziemski-2018-05.

290 Nick Grossman (8 Apr 2015), «Regulation, the internet way,» Data-Smart City Solutions, Harvard University, https://datasmart.ash.harvard.edu/news/article/white-paper-regulation-the-internet-way-660.

имеется для социальных хаков, – систему общего права, состоящую из залов суда, судей, присяжных и непрерывно развивающихся прецедентов. Система управления разработками ИИ должна быть быстрой, инклюзивной, прозрачной и гибкой, впрочем, как и любая другая хорошая система управления.

Мы можем попытаться набросать, какого рода система управления сможет защитить общество от потенциальных последствий как преднамеренного, так и непреднамеренного ИИ-хакинга. И хотя я просто ненавижу случайно придуманные аббревиатуры, позвольте мне использовать в следующих абзацах сокращение HGS, от Hacking Governance System («система управления хакингом»). Эта абстракция облегчит нам обсуждение подобных вещей.

● **Скорость.** Чтобы быть эффективной в условиях ускорения темпов технологических и социальных изменений, любая HGS должна работать быстро и точно. Дилемма Коллингриджа [291] – это старое, но по-прежнему верное наблюдение на тему технологических изменений: к тому времени, когда что-то новое и разрушительное становится достаточно распространенным, чтобы стали ясны его последствия для общества, регулировать его уже слишком поздно. Слишком много жизней и средств к существованию оказываются связанными с новой технологией, чтобы вот так запросто вернуть джинна в бутылку. Вы скажете, это чепуха, потому что многое – строительная отрасль, железнодорожный транспорт, продукты питания, медицина, производство, химикаты, атомная энергетика – демонстрируют примеры обратного, но согласитесь, что регулировать уже созданное определенно сложнее. Хаки будут внедряться быстрее, чем большинство правительств смогут менять свои законы и постановления. Но даже если они научатся принимать ответные меры вовремя, регулировать разросшегося гиганта будет очень непросто. В идеале HGS должна быть способна действовать быстрее, чем хак успевает распространиться, и оперативно решать, развивать его дальше или пресечь в корне.

● **Инклюзивность.** Для того чтобы определить, является хак хорошим или плохим, особенно на ранних стадиях, любая HGS должна учитывать как можно больше точек зрения. Это поможет добиться того, что ни одна потенциальная угроза и ни одно преимущество хака не будут упущены. Такой подход означает как минимум, что в состав HGS должна входить разношерстная междисциплинарная команда – от социологов и юристов до экономистов, психологов и экологов, – способная изучить хаки и их последствия со всех сторон. Кроме того, HGS придется активно искать и использовать информацию от внешних групп, особенно от сообществ, пострадавших от хака, а также от независимых исследователей и экспертов, ученых, профсоюзов, торговых ассоциаций, местных органов власти и гражданских объединений. Эти группы и лица должны не просто высказывать свое мнение на случайных встречах; в идеале их диалог с сотрудниками HGS и друг с другом должен быть постоянным, чтобы в ходе обсуждения, с одной стороны, уточнялась оценка ситуации, а с другой – создавались условия для инициативы и лоббирования с целью изменить методы контроля ИИ-хакинга политиками и должностными лицами, не входящими в состав HGS.

● **Прозрачность.** Поскольку HGS будет привлекать к принятию решений широкий круг экспертов и простых граждан, ее процессы и постановления должны быть публично прозрачными[292]. Непрозрачная HGS, за работой которой смогут следить только инсайдеры или люди с учеными степенями, окажется закрытой для обратной связи с обществом, которая исключительно важна для полного понимания природы социальных хаков и их

---

[291] Adam Thierer (16 Aug 2018), «The pacing problem, the Collingridge dilemma and technological determinism,» *Technology Liberation Front*, https://techliberation.com/2018/08/16/the-pacing-problem-the-collingridge-dilemma-technological-determinism.

[292] Stephan Grimmelikhuijsen et al. (Jan 2021), «Can decision transparency increase citizen trust in regulatory agencies? Evidence from a representative survey experiment,» Regulation and Governance 15, no. 1, https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12278.

побочных эффектов. HGS с более прозрачными процессами и обоснованиями своих решений заслужит больше доверия со стороны граждан. Это дополнительное доверие будет иметь решающее значение для политической поддержки новых институтов, которым придется искать сложные компромиссы между инновациями, стабильностью систем и защищаемыми ценностями, такими как равенство и справедливость.

● **Гибкость.** Наконец, по мере роста политической поддержки граждан, внедрения хаков, признанных полезными, или по мере того, как ученые и правительство все больше узнают о том, как эффективно регулировать хакинг, любая HGS должна освоить механизмы быстрого развития своей структуры, возможностей, решений и подходов, чтобы преуспеть в меняющемся мире. Даже при наличии всей необходимой информации социальные системы сложны и труднопредсказуемы, и попытки блокировать вредные социальные хаки порой терпят неудачу, а когда HGS разрабатывает эффективный патч или другую защиту от социального хака, хакеры тут же начинают работать над ее взломом. Поэтому HGS должна быть итеративной: быстро учиться на своих ошибках, тестировать, какие подходы к контролю и внедрению социальных хаков лучше всего работают, и постоянно совершенствовать свою способность брать на вооружение передовые методы.

Общее решение здесь состоит в том, чтобы все мы, граждане, более осознанно подходили к вопросу о надлежащей роли технологий в нашей жизни. До сих пор мы в целом не возражали против того, чтобы программисты кодировали мир так, как они считают нужным. Мы делали это по нескольким причинам. Мы не хотели чрезмерно ограничивать зарождающиеся технологии. Законодатели в основном не понимали технологии настолько хорошо, чтобы регулировать их. И это было не настолько важно, чтобы вызвать наше беспокойство. Но сейчас ситуация изменилась. Компьютерные системы влияют не только на компьютеры, и, когда программисты принимают очередные решения, они буквально проектируют будущее мира.

Система общего права является хорошей отправной точкой. Я не хочу преуменьшать противоречия, существующие между демократией и технологией. С одной стороны, далеко не каждый способен понять и внести свой вклад в регулирование ИИ. С другой – где нам найти таких технократов, которым можно доверять и которые, в свою очередь, доверяли бы простым гражданам? Это более общая и крайне сложная проблема современного управления нашим информационно насыщенным, связанным и технологически развитым миром, которая выходит далеко за рамки этой книги. По своей важности она сопоставима с проблемой создания управляющих структур, способных работать со скоростью и в условиях сложности информационного века. Такие ученые-правоведы, как Джиллиан Хэдфилд, Джули Коэн, Джошуа Фэйрфилд и Джейми Сасскинд [293], пишут об этой более общей проблеме, для решения которой еще многое предстоит сделать.

Однако сначала мы должны решить ряд более крупных проблем нашего общества. Иными словами, повсеместный хищнический хакинг – это симптом несовершенной системы общественного устройства. Деньги – это власть, и правосудие для влиятельных нарушителей правил работает по-другому, нежели для тех, кто деньгами и властью не обладает. Если правоохранительные органы не добиваются справедливости (корпоративные преступления редко преследуются по закону), то у влиятельных людей пропадает стимул следовать правилам. Это подрывает доверие общества как к системам, так и к самим правилам.

Если подумать, становится очевидным, что ставки несправедливого правоприменения слишком высоки. Минимальное регулирование наиболее привилегированных лиц

---

[293] Gillian K. Hadfield (2016), Rules for a Flat World: Why Humans Invented Law and How to Reinvent It for a Complex Global Economy, Oxford University Press.

Julie E. Cohen (2019), Between Truth and Power: The Legal Constructions of Informational Capitalism, Oxford University Press.

Joshua A. T. Fairfield (2021), Runaway Technology: Can Law Keep Up? Cambridge University Press.

Jamie Susskind (2022), The Digital Republic: On Freedom and Democracy in the 21st Century, Pegasus.

или предприятий означает, что они получают возможность определять политику и де-факто становятся правительствами. Это значит, что остальные люди больше не имеют права голоса, то есть демократия умирает. Да, это крайняя постановка проблемы, но таков конечный результат наблюдаемого процесса, и мы не должны упускать его из виду.

Я описал взаимодействие между человеческими и компьютерными системами, а также риски, связанные с тем, что компьютеры начинают играть роль людей. Это тоже более общая проблема, чем неправильное использование ИИ. О ней много пишут технофилософы и футуристы. И хотя проще всего позволить технологиям самим вести нас в будущее, станет намного лучше, если граждане коллективно решат, какой должна быть роль технологий в этом будущем. Особенно в мире, где так много технологий доступно каждому.

Нигде в мире еще не существует HGS, и ни одно правительство не думает о ее создании. Но время сделать это уже пришло.

Послесловие

Завершая работу над рукописью этой книги летом 2022 г., я наткнулся на статью в *The Wall Street Journal* , в которой описывался новый финансовый хак. Импортеры должны платить государственные пошлины, зачастую немалые, на ввоз иностранных товаров. Но существует лазейка – правило de minimis [294] , предназначенное для освобождения от пошлин американских туристов, привозящих сувениры из зарубежных поездок. Сметливые импортеры воспользовались этой лазейкой и теперь поставляют товары зарубежных продавцов покупателям напрямую. «В результате более одной десятой китайского импорта в стоимостном выражении поступает в страну как поставки de minimis по сравнению с 1 % десять лет назад». Общая сумма потерь налоговых поступлений от этого хака составила $67 млрд в год.

Трудно не впасть в депрессию, наблюдая такие масштабы социального хакерства. Оно кажется неизбежным. Системы взламываются в угоду тем, кто наверху, и это продолжается с незапамятных времен. Те средства защиты, которые у нас есть, едва справляются с сегодняшними задачами, а в будущем о них можно будет забыть, поскольку хакерские атаки на общество будут только усиливаться.

По своей сути хакинг – это некое балансирование. С одной стороны, он двигает инновации, с другой – подрывает системы, укрепляет существующие несправедливые структуры власти и способен нанести вред обществу. Оглядываясь на нашу историю, можно утверждать, что инновации стоили риска. Конечно, привилегированные особы взламывали системы ради собственной выгоды, но большая часть общества уже и так была под их гнетом. Незначительный хак не сильно менял ситуацию.

Сегодня этот баланс меняется по двум причинам: культурной и технологической. И стоит изложить их подробнее.

Сначала о культурной причине. В долгосрочной перспективе – я имею в виду столетия – наши общественные системы становятся все более справедливыми, демократичными и честными. И по мере того как системы развиваются, хакинг становится все более привлекательным средством для привилегированных лиц и групп, чтобы подмять системы под себя. В целом проще получить то, чего желаешь, когда стоишь у руля автократии. Если вы можете безнаказанно устанавливать и нарушать правила, то в хакинге нет необходимости. Если же вы ограничены законом так же, как и все остальные, получать желаемое уже сложнее. И тогда лучшим вариантом становится взлом экономических,

294 Josh Zumbrun (25 Apr 2022), «The $67 billion tariff dodge that's undermining U.S. trade policy,» *Wall Street Journal* , https://www.wsj.com/articles/the-67-billion-tariff-dodge-thats-undermining-u-s-trade-policy-di-minimis-rule-customs-tourists-11650897161.

социальных или политических систем, которые ограничивают ваши аппетиты.

У меня нет прямых доказательств, но я считаю, что в последние десятилетия хакинг стал более распространенным именно в силу этой динамики. Это мое личное объяснение «позднего капитализма» и всех проблем, которые он с собой несет: поиск лазеек в правилах теперь регулярно становится путем наименьшего сопротивления. Когда те, у кого есть средства или технические возможности, поняли, что могут с выгодой хакать системы, они быстро нашли для этого ресурсы и опыт. Они научились использовать уязвимости. Они научились двигаться вверх и вниз по иерархии хакинга для достижения своих целей. Они узнали, как добиться того, чтобы их хаки были нормализованы, признаны законными и внедрены в систему.

Ситуация усугубляется неравенством доходов. Экономист Томас Пикетти объясняет, что неравенство создает излишки ресурсов у победителей[295] и эти излишки могут быть мобилизованы для усиления этого неравенства. Значительная их часть инвестируется в хакинг.

Сейчас мы имеем наибольшее число людей, обладающих знаниями в сфере хакинга и ресурсами для реализации хаков, чем когда-либо прежде. Эти знания и ресурсы вкупе приносят власть. Наши социальные системы переполняются хаками, возникшими в результате многолетней борьбы за власть и престиж. А поскольку облачные вычисления, вирусные СМИ и ИИ делают новые хаки более доступными и мощными, чем когда-либо, нестабильность и инновации, которые они порождают, будут расти в геометрической прогрессии. Разумеется, принося выгоду тем, кто их разрабатывает или контролирует, даже при условии, что их хаками пользуются все больше людей.

Социальные системы основаны на доверии, а хакинг его подрывает. В небольших дозах он может быть не так опасен, но, когда хаки начинают лезть как грибы после дождя, доверие рушится, и в конечном итоге общество перестает функционировать должным образом. Налоговая лазейка, доступная только богатым, вызовет недовольство и подорвет доверие ко всей системе налогообложения. Цунами хаков, накрывшее наше общество, отражает отсутствие в нем доверия, социальной сплоченности и гражданской активности.

Вторая причина нарушения баланса между инновационной функцией хакинга и укреплением несправедливости носит технологический характер. Наше общественное устройство в целом, возможно, и стало более справедливым и честным за прошедшие столетия, но прогресс развивается нелинейно, да и справедливость не входит в число его непременных свойств. Беглый ретроспективный взгляд создает ощущение восходящей траектории, но при более детальном рассмотрении мы увидим множество взлетов и падений. История – это «шумный» процесс.

Технологии увеличивают амплитуду этих шумов. Краткосрочные подъемы и спады становятся все более серьезными. И хотя они, возможно, не влияют на долгосрочную траекторию, мы, живущие здесь и сейчас, ощущаем их влияние на собственной шкуре. Именно поэтому XX в., согласно статистике, можно расценивать и как наиболее мирный в истории человечества и как век, породивший самые смертоносные войны.

Игнорировать этот шум можно было, когда ущерб не являлся потенциально опасным в глобальном масштабе – то есть как если бы мировая война еще не могла уничтожить человечество, разрушить общество или коснуться регионов и людей, не имеющих к этой войне никакого отношения. Но сейчас мы уже не можем быть уверены в этом. Риски стали экзистенциальными, чего не было раньше. Усиливающий эффект технологий превращает краткосрочный ущерб в долгосрочный и системный, причем в масштабах планеты. Полвека мы жили в тени призрака ядерной войны – катастрофы, которая может привести к вымиранию человечества как вида. Глобальная система транспортных сообщений позволила локальным вспышкам COVID-19 быстро превратиться в пандемию, которая

295 Thomas Piketty (2017), Capital in the Twenty-First Century, Harvard University Press.

обошлась нам в миллионы жизней и миллиарды долларов, увеличив политическую и социальную нестабильность. Изменения в атмосфере, обусловленные технологиями и усугубляемые петлями обратной связи, могут сделать Землю куда менее гостеприимной в ближайшие столетия. Сегодня решения отдельных хакеров могут иметь последствия для всей планеты. Социобиолог Эдвард Уилсон описал фундаментальную проблему человечества следующим образом[296]: «У нас палеолитические эмоции, средневековые институты и богоподобные технологии».

Представьте себе хакерскую атаку, подобную той, что устроил Volkswagen, выбрасывая в атмосферу больше углекислого газа, чем позволяли нормы. Если бы этим путем пошло слишком много компаний, мы бы резко приблизили момент повышения средней температуры климатической системы Земли на 2 °C и жизнь на планете стала бы невыносимой. Представьте себе апокалиптическую террористическую группу, которая взламывает командную структуру ядерного арсенала и запускает ракеты. Или биохакеров, выпускающих в мир новую болезнь. Мы можем увидеть массовую гибель людей и крах правительств, что приведет к необратимой нисходящей спирали, куда более быстрой, чем тяжелая и упорная борьба за повышение уровня жизни, которую человечество вело до сих пор.

По этим двум причинам хакинг сегодня – это экзистенциальный риск. Мы научились взламывать лучше, быстрее и больше. Наши социальные и технические системы моментально превращаются в поля битвы между хакерами и службами безопасности, мутируя в процессе и приобретая совершенно новые формы. На фоне перекоса в пользу верхушки пищевой цепи и порождаемой хакингом нестабильности все эти атаки будут и дальше происходить за счет обычных людей.

Но, думаю, повод для оптимизма все же есть. Технологические достижения, которые усугубляют хакерские атаки, также способны улучшить ситуацию, одновременно защищая от вредных хаков и продвигая полезные. Хитрость заключается в том, чтобы правильно настроить системы управления. И эта задача усложняется тем, что решить ее мы должны в ближайшее время.

Для того чтобы превращать хаки – и сегодняшние, созданные людьми, и завтрашние, созданные ИИ, – в социальные инновации, нужно отделить полезные хаки от вредных, расширить масштабы первых и минимизировать последствия вторых. Это гораздо больше, чем простая защита от взлома, о которой мы говорили во второй части книги. Это также означает наличие систем управления, которые могут идти в ногу с быстрыми изменениями, взвешивая конфликтующие интересы и интерпретации рисков, выгод и потенциала каждого отдельного хака.

Мы должны создать устойчивые структуры управления, способные быстро и эффективно реагировать на взломы. В них не будет никакого толку, если исправление налогового кодекса потребует годы или если хак законодательной базы настолько укоренится, что его невозможно будет исправить по политическим причинам. Нам нужно, чтобы правила и законы общества можно было оперативно исправлять патчами, как программное обеспечение компьютеров и телефонов.

Если мы не сможем хакнуть сам хакинг, сохранив его преимущества и снизив сопутствующие ему издержки и неравенство, нам будет трудно выжить в этом технологическом будущем.

Благодарности

Эта книга родилась в период глобальной пандемии и личных жизненных потрясений,

296 Tristan Harris (5 Dec 2019), «Our brains are no match for our technology,» *The New York Times* , https://www.nytimes.com/2019/12/05/opinion/digital-technology-brain.html.

пострадав от последствий того и другого. В 2020 г. я написал 86 000 слов, затем, в 2021 г., забросил рукопись, пропустил крайний срок, оговоренный с издателем, и вновь взялся за нее лишь весной 2022 г. Благодаря Эвелин Даффи из Open Boat Editing я выкинул из книги 20 000 слов и реорганизовал ее в 60 небольших глав, которые (как я надеюсь) вы только что прочитали.

В течение этих двух лет многие люди помогали мне в работе над книгой. Я хотел бы поблагодарить своих научных ассистентов: Николаса Анвея, Джастина Дешазора, Саймона Диксона, Деррика Флаколла, Дэвида Лефтвича и Вандинику Шукла. Все они были студентами Гарвардской школы им. Кеннеди и работали со мной в течение нескольких месяцев, включая летний семестр. Росс Андерсон, Стив Басс, Бен Бьюкенен, Ник Каулдри, Кейт Дарлинг, Джессика Доусон, Кори Доктороу, Тим Эдгар, FC (он же freakyclown), Эми Форсайт, Бретт Фришманн, Билл Хердл, Трей Херр, Кэмпбелл Хау, Дэвид Айзенберг, Дариуш Емельняк, Ричард Маллах, Уилл Маркс, Алисия Макдональд, Роджер Макнэми, Джерри Михальски, Питер Нойманн, Крэйг Ньюмарк, Кирстен Пейн, Дэвид Перри, Натан Сандерс, Мариетта Шааке, Мартин Шнайер, Джеймс Шайрс, Эрик Собель, Джейми Сасскинд, Рахул Тонгиа, Арун Вишванат, Джим Уолдо, Рик Уош, Сара Уотсон, Тара Уилер, Джозефина Вулф и Бен Визнер – все они прочитали книгу где-то на стадии черновика и сделали полезные замечания, к которым я в основном прислушался. Кэтлин Сейдел тщательно отредактировала книгу. То же сделала моя давняя помощница и редактор Бет Фридман.

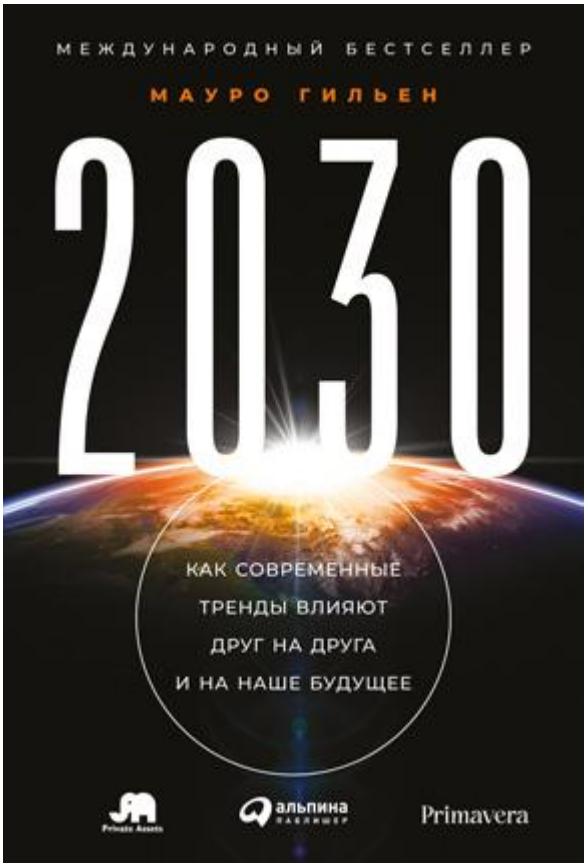
Спасибо моему редактору Брэндану Карри и всем остальным в Norton, кто приложил руку к превращению рукописи в готовый продукт, а также моему агенту Сью Рэбнер. Я благодарен моему новому сообществу здесь, в Кембридже: Гарвардской школе им. Кеннеди, Центру Беркмана Кляйна, Inrupt (и проекту Solid), а также моим многочисленным коллегам и друзьям. И, Тэмми, спасибо тебе за все.

Рекомендуем книги по теме

Старший брат следит за тобой: Как защитить себя в цифровом мире
Михаил Райтман

На 100 лет вперед: Искусство долгосрочного мышления, или Как человечество разучилось думать о будущем
Роман Кржнарик

Шифровальщики: Как реагировать на атаки с использованием программ-вымогателей
Олег Скулкин



2030: Как современные тренды влияют друг на друга и на наше будущее
Мауро Гильен