Содержание

От автора 7

Введение 9

Глава 1 Знакомство с хакерами 13

Глава 2 Падение берлинского брандмауэра 41

Глава 3 “Одиннадцать онлайн-друзей Оушена” 84

Глава 4 Цифровое вымогательство 126

Глава 5 Ваши данные на продажу 167

Глава 6 Даркнет и не только 199

Глава 7 Онлайн-машина ненависти 240

Глава 8 Тушите свет 282

Глава 9 Данные как оружие 316

Глава 10 Взлом выборов 347

Эпилог 393

Дополнительная литература 401

Благодарности 405

Предметно-алфавитный указатель 407

Глава 1
Знакомство с хакерами

На улице тридцать градусов в тени, и я стою, обливаясь потом, у входа в огромный рынок в районе Киапо в Маниле, столице Филиппин.

В руках я держу бумажку с именем человека, которого ищу: филиппинца Онеля де Гусмана. Я слышал, что он, кажется, работал где-то среди множества палаток, которые стоят передо мной… возможно… несколько лет назад.

Я начинаю показывать бумажку людям, которых встречаю на рынке. Задача кажется невыполнимой. Я ищу микроскопическую иголку в гигантском стоге сена.

Я не знаю, как де Гусман выглядит сейчас, поскольку у меня есть лишь одна его фотография, сделанная почти двадцать лет назад. Хуже того, это размытый снимок с суматошной пресс-конференции, а де Гусман запечатлен на нем в темных очках, да еще и прикрывает лицо носовым платком.

У юного студента была веская причина прятаться. Его обвиняли в рассылке наделавшего шума и чрезвычайно успешного вируса *Love Bug*, который заразил около сорока пяти миллионов компьютеров по всему миру и нанес урон на много миллиардов долларов[1].

Этот вирус стал настоящим прорывом. И дело было не в его технической сложности и не в ущербе, который он причинил,

1 *Love Bug May Have Been Accident // www.news.bbc.co.uk,* 11.05.2000. *(Здесь и далее примеч. авт., если не указано иное.)*

но в том, что он показал, как использовать кое-что гораздо более действенное, чем код. Он был ориентирован не столько на компьютерную уязвимость, сколько на человеческую, и эта тактика впоследствии стала применяться в бесчисленном множестве киберпреступлений. Но де Гусман ни в чем не признался. Он отделался уклончивыми ответами на пресс-конференции, дал несколько невнятных интервью СМИ и ушел от ответственности. Затем он залег на дно и двадцать лет не давал о себе знать. У него не было ни страниц в социальных сетях, ни онлайн-профиля. Он стал призраком в цифровом мире, в терроризировании которого его однажды обвиняли.

У меня ушел целый год, чтобы найти хоть какую-то зацепку и предположить, где он скрывается. Ходили слухи, что он в Германии, что он работает на ООН в Австрии, что он переехал в США и что даже устроился на работу в *Microsoft*. Теперь же я шел по манильскому рынку и показывал торговцам его имя, надеясь, что кто-нибудь его узнает.

Если бы я сумел его разыскать, возможно, я смог бы расспросить его о вирусе и узнать, понимает ли сам де Гусман степень его влияния. Возможно, по прошествии двадцати лет я убедил бы его сказать мне, правда ли этот вирус был его рук делом.

Однако сколько бы я ни показывал бумажку с его именем, я лишь встречал непонимающие взгляды и слышал настороженные вопросы. Но в конце концов один из палаточников мне улыбнулся.

— Тот парень с вирусом? Да, я его знаю.

Прежде чем продолжать историю Онеля де Гусмана, важно немного изучить технологические и, что важнее, социальные тектонические плиты, которые сдвинулись за несколько лет до того, как *Love Bug* оказался у всех на устах в 2000 году.

Такие вирусы — относительно новое явление, но у них тоже есть своя история. Современный хакер формировался не один десяток лет и впитал в себя знания нескольких отдель-

ных групп. Чтобы разобраться в киберпреступности, нужно понять, как появились эти группы, а для этого — вернуться к началу начал.

В конце 1969 года, через несколько месяцев после высадки человека на Луне, американские ученые совершили открытие, которое, пожалуй, повлияло на цивилизацию сильнее, чем лунный рывок, предпринятый NASA.

Министерство обороны США искало надежный способ передавать сообщения в своей распределенной компьютерной сети. Специалисты придумали разбивать сообщения на одинаковые по размеру фрагменты и посылать их с одного компьютера на другой по серии транзитных участков, задействуя для этого телефонную систему. Идея связать компьютеры друг с другом с помощью телефонных линий была не нова: вопрос всегда состоял в том, как создать достаточно масштабную систему, которую можно будет легко расширить, включив в нее новых участников. Разработанный для этого метод позволял любому компьютеру, зарегистрированному в общей системе, присоединяться к группе, а следовательно, отправлять и получать фрагменты данных. Таким образом была проложена дорога к беспрепятственному и быстрому развитию системы, которая стала применяться не только в военной сфере. В результате появилась взаимосвязанная сеть компьютеров, или интернет, и система для передачи сообщений от одного компьютера к другому, называемая интернет-протоколом (IP). Каждая машина, зарегистрированная в системе, получала уникальный адрес (IP-адрес), и, чтобы передать данные с одного компьютера на другой, нужно было просто прикрепить правильный адрес, тем самым показав всем остальным компьютерам в сети, куда их следует направить[1].

1 Leiner B. M., Cerf V. G., Clark D. D.,. Kahn R. E., Kleinrock L., Lynch D. C., Postel J., Larry G. Roberts, Wolff S. *Brief History of the Internet* // Internet Society. 1997. P. 2–4.

Интернет часто отождествляют со Всемирной паутиной, или вебом. На самом деле последняя появилась существенно позже, в 1989 году. До этого документ, которым делились в интернете, мог выглядеть по-разному на разных компьютерах. Всемирная паутина, по сути, дала способ публиковать данные в интернете и стандартизировать внешний вид материалов, доступных для разных машин[1].

В сочетании с интернетом всемирная паутина привела обе технологии к глобальному доминированию с начала 1990-х годов. Но почти за двадцать лет до этого интернет прекрасно существовал и без веба. Именно в тот период появились первые компьютерные хакеры, и их развитие и становление подпитывала система, которая фактически представляла собой винтажную версию фейсбука[2].

Как вы узнаете из этой книги, представление о том, что хакеры — сплошь необщительные одиночки, как правило, ошибочно. Порой их поведение действительно асоциально, но в большинстве своем они, как и другие люди, стремятся найти единомышленников. Многие первые пользователи компьютеров обрели приятелей через электронные доски объявлений (*bulletin board system*, BBS) — почти забытую ныне технологию, около двадцати лет существовавшую параллельно с интернетом. Эти доски были предельно простыми общедоступными службами обмена сообщениями, где пользователи проводили время и общались друг с другом. Они читали посты и отвечали на них — и иногда этот процесс растягивался на несколько дней. Как отметил один пользователь BBS, “это было похоже на разговор, только очень, очень медленный”[3].

Непосвященным, которые наблюдали за происходящим со стороны, это часто казалось не технологической

1 *History of the Web* // *www.webfoundation.org.*
2 Деятельность компании MetaInc (Facebook, Instagram) запрещена на территории РФ решением суда.
3 Scott J. *The BBS Documentary* //Режим доступа: bbsdocumentary.com.

революцией, а бессмысленной тратой времени. Но из бесед с первыми пользователями BBS становится очевидно, что именно их привлекало в досках объявлений. В тот период мало кто разбирался в компьютерах, и любовь к технологиям превращала их в аутсайдеров. И вдруг появилась непонятная система, которая связывала людей с общими интересами.

В культурном отношении электронные доски объявлений сыграли ключевую роль в технологической эволюции. На заре своего существования интернет в основном контролировался исследователями, сидящими в хорошо финансируемых лабораториях. Но дух этого нового мира, его обычаи и нравы все больше прорабатывались на BBS. В итоге именно там и нашли друг друга первые хакеры. Несколько сил слились воедино на просторах свободных чатов BBS в зарождающемся киберпространстве, и так возникла хакерская культура. Первая из этих сил зародилась благодаря группе психоделических скитальцев, бегущих от коллапса движения хиппи.

На исходе эпохи “силы цветов”, когда рассвет Вудстока сменился мрачными сумерками бунтов на Альтамонтском фестивале, в США появился журнал *Whole Earth Catalog*. Он продвигал идеи самодостаточности и жизни вне привычных рамок.

Вполне естественно, что следующим шагом стало создание его компьютеризированной версии. Его необходимо было постоянно обновлять, а электронный формат упрощал эту задачу. Кроме того, некоторые из людей, занимавшихся развитием журнала, в 1970-х годах принимали участие в американских экспериментах по строительству коммунальной жизни и хотели создать такую же атмосферу на цифровых форумах каталога. Его онлайн-версия под названием *Whole Earth ‘Lectronic Link* (WELL) была запущена в 1985 году и бы-

стро стала излюбленной доской объявлений контркультурного сообщества Западного побережья[1].

Связи сообщества с хиппи значительно укрепились в 1986 году, когда на форуме появился человек, глубоко проникшийся хакерской культурой: Джон Перри Барлоу, автор текстов легендарной рок-группы *Grateful Dead*.

Судя по всему, увлечение Барлоу интернетом и BBS подпитывалось не столько технологическими знаниями, сколько антропологической любознательностью. Он наблюдал за происходящим в зарождающемся сообществе как поэт и сохранял свой непритязательный марктвеновский голос в странном новом пространстве высоких технологий: “В этом молчаливом мире все разговоры печатаются. Чтобы войти в него, человек отказывается от тела и места и превращается просто в слова”[2]. Вскоре доска объявлений WELL стала местом притяжения технологически подкованных фанатов *Grateful Dead*, за которыми закрепилось прозвище “дэдхеды”.

“В первые годы на базе WELL сформировались два основных сообщества, — вспоминает один из пользователей. — В одно из них входили дэдхеды, которые использовали [платформу], чтобы оставаться на связи друг с другом в этой кочевой манере, а во второе… технари-экспериментаторы. В итоге получилось весьма любопытное сочетание технарства и контркультуры”.

Непонятно, то ли это Барлоу пришел на WELL за дэдхедами, то ли дэдхеды потянулись за Барлоу, но его присутствие закрепило за этой доской объявлений репутацию преимущественно постхиппарского комьюнити. К тому же Барлоу оказался в самой гуще первой потасовки в растянувшейся на долгие годы битве правоохранительных органов и всех, кто стоял на периферии компьютерной культуры.

Подобно тому как иногда копы брали в кольцо концерты *Grateful Dead*, не без причины полагая, что на них не обой-

1 *What Is the Well?* // Режим доступа: well.com, 24.06.2019.
2 Barlow J. P. Crime and Puzzlement // Режим доступа: eff.org, 08.06.1990.

дется без нарушений, представители власти принялись следить и за первыми онлайн-сообществами. Когда пошли слухи, что в интернет просочился конфиденциальный файл недавно образованной компании *Apple*, полиция устроила облаву. Среди прочих мест обыски прошли и дома у Джона Перри Барлоу, чего, вероятно, было не избежать.

С поэтическим остроумием Барлоу описывает, как летом 1990 года к нему со странным визитом явился агент ФБР, который расследовал это преступление. Произошло классическое столкновение старорежимной полицейской системы с технологиями нового мира. Барлоу пишет, что порой ему приходилось объяснять агенту, как работает электронная почта и как выглядит программный код:

> Он стал то и дело тереть лицо руками, смотреть на меня сквозь пальцы и приговаривать: “Вот дела!” Или: “Ох-х-х-х-х”. Сразу ясно, что прогресс ушел вперед, если потенциальным подозреваемым приходится объяснять полицейским, в чем суть их предполагаемых преступлений[1].

Рассказ Барлоу привлек внимание Митча Капора, одного из первых предпринимателей технологической сферы, сколотившего состояние на *Lotus Development Corporation*. Эта компания разработала чрезвычайно популярную программу для работы с таблицами, когда *Microsoft Excel* еще не было. Оказалось, что в связи с тем же делом *Apple* агент ФБР нанес визит и Капору.

“Больше всего меня поразило то, что было очевидно, как плохо они понимают все, что связано с этой сферой, — сказал Капор. — Они не были знакомы ни с кодом, ни с дискетами, ни с интеллектуальной собственностью — они не знали ничего, и меня это встревожило, ведь эти парни носили при себе оружие”.

1 Ibid.

Капор захотел встретиться с Барлоу и вдруг понял, что во время своего ближайшего путешествия должен будет пролетать на собственном самолете недалеко от его дома, а потому сделал остановку и навестил музыканта на его ранчо.

Оказалось, что их обоих проверяли в связи с попыткой вывести на чистую воду "хакеров", совершивших преступление, хотя в ФБР, похоже, не очень понимали, в чем оно заключается, и уж тем более не знали, как осуществлять преследование в его отношении. Барлоу и Капор были не единственными: на пользователей компьютеров по всей территории США совершили несколько облав, порой неоправданно жестоких, хотя юридически такие действия вряд ли были правомерны.

Однако за обескураженными агентами ФБР и периодическими неуклюжими обвинениями Барлоу разглядел нечто более глубокое: он почувствовал, что старые и заскорузлые институты пошли в наступление на зарождающееся в таких местах, как WELL, постхиппарское сообщество.

Вместе с Джоном Гилмором, еще одним пионером интернет-предпринимательства, который работал в компании *Sun Microsystems*, Барлоу и Капор основали организацию "Фонд электронных рубежей", призванную защищать гражданские свободы в интернете[1]. С тех пор этот фонд стал бельмом на глазу правительств разных стран (а также отметился в создании "дарквеба", о чем речь пойдет позже). Пока общество пыталось понять, что значит "хакер" — как юридически, так и культурно, — фонд выступал движущей силой при разметке этой территории. Барлоу (который умер в феврале 2018 года) сыграл в этом огромную роль, олицетворяя стремление раннего компьютерного сообщества к контркультурному антиавторитаризму.

В 1996 году Барлоу написал "Декларацию независимости киберпространства", которая начинается так:

1 *A History of Protecting Freedom Where Law and Technology Collide* // Режим доступа: *www.eff.org*.

> Правительства Индустриального Мира, вы — утомленные гиганты из плоти и стали; моя же родина — Киберпространство, новый дом Сознания. От имени будущего я прошу вас, у которых все в прошлом, оставьте нас в покое. Вы лишние среди нас. Вы не обладаете верховной властью там, где мы собрались[1].

Может показаться, что сегодня, когда четырьмя самыми дорогими компаниями в мире стали *Apple*, *Alphabet* (которой принадлежит *Google*), *Amazon* и *Microsoft*, слова Барлоу звучат несколько анахронично. Но его антиавторитарная позиция — средний палец в адрес тех организаций, которые не понимают онлайн-мир и пытаются его заблокировать, — остается глубоко укорененной в хакерском мировоззрении.

Идея, что онлайн-пространство лежит вне сферы полномочий традиционной власти, что это мир, созданный из грез и кошмаров его пользователей, своего рода игровая зона, где люди могут заново изобрести себя, освободившись от устаревших старорежимных приказаний, проникла в сердца тех, кто входил в авангард раннего цифрового общества. Но одного иконоборчества было недостаточно. Подъем хакерской культуры подпитывали и две другие зоны влияния, появившиеся в США с началом технологического бума.

Город Бостон в штате Массачусетс, возможно, не имеет в мире такой же репутации, как калифорнийская Кремниевая долина, но в 1990-е годы он славился другим: там были классные мусорные баки.

Пока Джон Перри Барлоу оборонял виртуальные баррикады, выстроенные для защиты киберпространства, некоторые бостонские технари кормились объедками растущей в городе технологической отрасли. Начинающие хакеры ко-

1 Barlow J. P. *A Declaration of the Independence of Cyberspace* // Режим доступа: eff.org.

пались на помойках, разбирая промышленный мусор компьютерных компаний, вытаскивали из баков все ценное, реанимировали технику, приспосабливая ее под свои нужды, и таким образом оснащали свои как попало оборудованные лаборатории.

“Там можно было найти что угодно: старые компьютеры, жесткие диски, дискеты — что только попадалось под руку”, — вспоминает Кристиан Риу.

Риу ворвался в мир бостонских технарей в 1994 году. Он переехал из Мэна — настоящего компьютерного захолустья по меркам мальчишки, который с пяти лет начал изучать, как программировать компьютеры *Apple II*. Естественно, он принялся искать единомышленников в чатах BBS. Теперь он изучал информатику в Массачусетском технологическом институте (MIT) и находился в одном из эпицентров зарождающейся технологической сферы. По его словам, в то время в университетских компьютерных системах содержались миллионы IP-адресов — значительная часть всех интернет-ссылок, благодаря чему университет выступал одним из узлов развития онлайн-пространства.

Приехав в Бостон, Риу узнал и другую причину, по которой MIT стал одной из движущих сил ранней хакерской культуры: в университете был популярен особый вид городских исследований, который назывался диггерством.

Риу вспоминает:

> Можно было залезать на крыши, а можно — спускаться в странные пропарочные тоннели под зданиями и все такое. Эта страсть к исследованиям показывала людям, что можно делать неожиданные вещи и попадать в неожиданные места и получать от этого огромное удовлетворение.
> [Суть была в том], чтобы оказаться в недоступном месте. Вы стоите на рассвете на крыше, от вида захватывает дух, и при этом вы единственные, кто проник туда за целый год, потому что вы поняли, как пролезть внутрь через странное

> окошко и взломать замок, которым пользуются только подсобные рабочие.
>
> Эти вещи позволяли людям познакомиться с концепцией хакинга задолго до появления компьютерного хакинга как такового. Так и зародилась эта культура[1].

На руку диггерам играло и то, что взлом замков, по словам Риу, был чрезвычайно популярным хобби у студентов-технарей из MIT: "На первом курсе MIT все студенты учатся вскрывать замки — так уж повелось".

Когда компьютеров стало больше, они стали для диггеров новым испытанием: в них стояли не физические замки, а цифровые. Вскоре Риу увлекся периферийным в те годы миром компьютерной безопасности и взял себе хакерский псевдоним *Dil Dog*, переиначив кличку собаки из комиксов о Дилберте. (Многие из этих никнеймов похожи на татуировки, которые люди набивают себе в юности: чем старше становятся их обладатели, тем глупее им кажутся принятые в молодости решения.) Для начала он выявил несколько уязвимостей в операционной системе *Windows*, разработанной в компании *Microsoft*: как выражается он сам, он "спустил с них штаны". Риу вспоминает, как однажды пришел на семинар, где преподаватель рассказал о некоторых его взломах, не догадываясь, что хакер, попавший в газетные заголовки, на самом деле сидит в его аудитории.

Риу чувствовал, что университет негласно одобряет его деятельность, хотя и не заявляет об этом во всеуслышание: "Терпимость администрации, которая в некотором роде даже поощряла [мои занятия], была мне на руку. Это не было табу. Ходило немало слухов о знаменитых хакерах из MIT, и их ценили по достоинству".

1 Это практиковалось не только в американских академических кругах, о чем свидетельствуют такие книги, как The Night Climbers of Cambridge, впервые опубликованная в 1930-х годах под псевдонимом Уипплснэйс (Cambridge, 2007), и Hartley A. *LA Climbs: Alternative Uses for Architecture*. London and New York, 2003.

Риу присоединился к хакерской группе *Lopht Heavy Industries*, которая получила свое название, поскольку обосновалась в лофте, где прежде находилась шляпная фабрика[1]. Эта группа прославилась после того, как в мае 1998 года ее члены выступили на заседании Сената США, посвященном обеспечению компьютерной безопасности правительственных систем. В этот невероятный момент контркультура встретилась с мейнстримом. На фотографии с того заседания запечатлен знакомый зал, обитый деревянными панелями, а члены группы *Lopht* сидят за длинным столом, и дают свои показания. Все выглядит вполне обычно, пока взгляд не падает на таблички с именами. Хакеры не хотели раскрывать свои личности, поэтому организаторы встречи использовали их никнеймы. В результате с сенаторами беседовали *Space Rogue*, *Brian Oblivion*, *Kingpin* и другие.

Имена у них были странные, а волосы — длинные, но говорили они о чрезвычайно серьезных вещах: об уязвимости интернета. Хакеры из группы *Lopht* предупредили сенаторов, что на систему ложится небывалая нагрузка и она берет на себя все больше ответственности, не обеспечивая безопасность своего функционирования, — об этом говорят и сегодня. Далее хакеры заявили, что всемером могут менее чем за полчаса вывести из строя интернет на всей территории Соединенных Штатов[2].

Такой и стала тактика *Lopht*: хакеры из группы взламывали системы, находили в них уязвимости, а затем сообщали об этом и заставляли своих сконфуженных жертв исправлять обнаруженные проблемы. Так же действовал и Риу: он извещал *Microsoft* о найденных ошибках, давал компании время их устранить и лишь затем предавал результаты своих действий огласке.

1 Fisher D, *We Got to Be Cool About This: An Oral History of the Lopht*// Режим доступа:.duo.com, 06.03.2018.

2 'Weak Computer Security in Government: Is the Public at Risk? Hearing Before the Committee on Governmental Affairs, United States Senate', U.S. Government Printing Office, 19.05.1998.

Это не приносило Риу денег, и хакеры *L0pht* в тот период тоже не получали финансовых стимулов. Их мотивация, по крайней мере в первые дни, носила некоммерческий характер. Они взламывали системы из интереса, чтобы потренироваться в хакинге и понять, насколько далеко в цифровые дебри они в состоянии залезть. Для таких людей, как Риу и члены группы *L0pht*, проникновение в запретную зону само по себе было наградой. Такие цели неодолимо влекли их, и радость обнаружить уязвимости в безопасности становилась бесконечно увлекательным занятием. Один специалист в области технологий, который работал с молодыми хакерами, сказал: "Покажи этим ребятам закрытую дверь — и следующую неделю они не поднимут головы, пока не откроют ее, даже получив из инструментов только столовую ложку".

По мере того как хакеры занимали все более видное положение, это стремление во что бы то ни стало преодолевать любые преграды на пути к цели все сильнее вписывалось в их создание. Оно прекрасно сочеталось с антиавторитаризмом хиппи-хакеров вроде Джона Перри Барлоу: в конце концов, закрытая дверь становилась лишь более манящей целью, если кто-то из власть имущих говорил, что открыть ее невозможно.

Но чтобы вывести хакеров на первый план во всем мире, потребовался третий ингредиент: озорной и издевательский характер их деятельности, благодаря которому о них писали во всех газетах. В колоде карт не обойтись без джокера, и главным претендентом на это амплуа в истории хакинга была группа "Культ мертвой коровы".