

{18+}

Даниил
Туровский

Вторжение

Краткая
история
русских
хакеров

19 • 20 • 21

Даниил Туровский

**Вторжение. Краткая
история русских хакеров**

«Individuum»

2019

УДК 004.491
ББК 60.54

Туровский Д.

Вторжение. Краткая история русских хакеров / Д. Туровский — «Individuum», 2019

ISBN 978-5-6042627-3-3

Летом 2016 года неизвестные выложили в интернет переписку высших чинов Демократической партии США – и российские хакеры, предположительно работающие на Кремль, моментально превратились в один из главных сюжетов мировой политики. Спецкор «Медузы», обладатель премии GQ в номинации «Журналист года» и четырех премий «Редколлегия» Даниил Туровский к тому времени писал об этих людях уже несколько лет: одни из них публиковали архивы почты российских чиновников, другие взламывали госсайты сопредельных стран по просьбе спецслужб, третьи просто зарабатывали миллионы, воруя их по всему миру. «Вторжение» – самая полная история российских хакеров: от советских матшкол и постсоветской нищеты к мировой кибервойне и транснациональным преступным группировкам. Книга описывает новый тип власти – но, как показывает Туровский, люди, которые обладают этой властью, сталкиваются все с теми же моральными дилеммами, выбирая между тюрьмой и сумой, чувством и долгом, добром и злом.

УДК 004.491

ББК 60.54

ISBN 978-5-6042627-3-3

© Туровский Д., 2019

© Individuum, 2019

Содержание

Предисловие	7
Пролог	9
Часть I	18
Глава 1	18
Глава 2	21
Глава 3	24
Глава 4	27
Глава 5	30
Глава 6	33
Часть II	35
Глава 7	35
Глава 8	40
Глава 9	42
Глава 10	44
Глава 11	46
Конец ознакомительного фрагмента.	50

Даниил Туровский

Вторжение. Краткая история русских хакеров

© Туровский, Д., 2019

© ООО «Индивидуум Принт», 2019

* * *

Моим родителям – за то, что научили любопытству

Предисловие

История русских хакеров – это история подростков всего бывшего СССР. Они росли в семьях советских инженеров, в юности читали киберпанк и научную фантастику, покупали на рынках клоны компьютеров IBM – и вдруг оказывались на хакерских форумах, которые часто заменяли им тоскливую русскую жизнь за окном: грязные улицы, бедность, пустое и пугающее в своей неопределенности будущее.

Пока в США рос экономический пузырь доткомов, хакеры запустили в России свою золотую лихорадку: воровство американских кредиток, взлом счетов банков и интернет-магазинов приносили многим миллионы долларов. Кто-то, боясь бандитов или государства, тщательно прятал их – вкладывая в цветочные магазины или пункты шиномонтажа; другие покупали особняки и дорогие спортивные машины; третьи обзаводились домами за границей и уезжали туда, где краски ярче, чем те, что они привыкли видеть за окном, – на Мальдивы, Кипр, в Израиль.

Биографии этих людей часто похожи на остросюжетные боевики. Когда я разговаривал с ними о прошлом, мне часто казалось, что все их проделки были не только ради денег – они как будто хотели стать героями книг и фильмов вроде тех, которые они так любили в детстве.

В юности я много читал журнал «Хакер», который то и дело советовал, как что-нибудь взломать, – все это напоминало обновленную для нового времени «Поваренную книгу анархиста». Я рос в семье, где у каждого был компьютер, а программирование приветствовалось; вечерами изучал коды сайтов – и пробовал их взламывать. В пятнадцать я раздумывал о том, чтобы пойти после школы учиться на факультет информационной безопасности – а потом, возможно, работать в ФСБ. К счастью, эти раздумья продлились недолго: вскоре я всерьез увлекся текстами, историями, журналистикой.

Тем не менее полутайное хакерское сообщество, попасть в которое мне так и не удалось, время от времени напоминало о себе. Сначала у знакомых взламывали соцсети и просили денег. Позже уже мои собственные аккаунты из-за работы репортером в России атаковали прогосударственные хакеры.

Эта книга про выбор – и про те пути, которые выбирали люди, которые стали частью хакерской субкультуры. Пока одни оставались романтиками и не думали о деньгах (часть I), другие богатели (часть II); когда пришло время обустраивать отношения с государством, кто-то начал работать на него, а кто-то – против (части III и IV).

Книга основана на текстах, которые я в течение последних лет писал для «Медузы» (meduza.io), одного из немногих независимых российских изданий, но не ограничивается ими. Большую часть материалов я собирал в свободное от работы время, изучая форумы, интернет-архивы, книги, встречаясь с хакерами или – чаще – разговаривая с ними в зашифрованных чатах. Я называю этих людей «русскими хакерами», потому что русскоязычное хакерское сообщество осталось единым: россияне, украинцы, белорусы и выходцы из других стран бывшего СССР росли на одних форумах, создавали совместные группировки и продолжали взламывать свои цели вместе, даже когда их государства вели друг с другом войну.

В чем-то эта книга – путеводитель по миру русскоязычных хакеров с последних лет СССР до нынешних времен; в чем-то – энциклопедия главных лиц; в чем-то – расследование о том, как российские власти построили одни из самых боеспособных кибервойск в мире. В книге много отдельных человеческих историй – по ним можно представить себе, в какой обстановке росли хакеры и что определило их дальнейшую судьбу.

В конце концов, это рассказ о том, как незнакомцы, сидящие за компьютерами, могут сосорить между собой страны, разрушать критическую инфраструктуру (например, отключать

электричество в целых регионах) и убивать, не ведя при этом никаких боевых действий и не зная своих жертв.

Пролог

Первый беженец кибервойны

22 августа 2015 года бородатый мужчина в очках зашел с двумя рюкзаками в здание Ленинградского вокзала в Москве. Он прошел к кассам, где купил билет на ближайший «Сапсан» – поезд-экспресс, за 4 часа доезжающий до Санкт-Петербурга.

По прибытии мужчина поспешил к стоящим неподалеку от вокзала маршруткам. Он вырос в Петербурге и знал: микроавтобус до Хельсинки – самый дешевый и незаметный способ попасть из России в Европу. Билет стоит 800 рублей; путь занимает 8 часов, которые путешественник проводит в окружении бедных студентов и спекулянтов, везущих из России в Финляндию сигареты, а обратно – бытовую химию.

Через несколько часов мужчина перешел финскую границу и наконец немного выдохнул. Пока его план удавался: он наверняка сбросил хвост. Он все хорошо продумал: не полетел на самолете, потому что его бы задержали на паспортном контроле; билет на поезд покупал не в интернете, а прямо в кассе на вокзале. Мужчина вспомнил свой предыдущий побег из привычной жизни: десять лет назад он проезжал на троллейбусе мимо вокзала в Петербурге и спонтанно решил переехать в Москву к своей девушке. Вышел на следующей остановке, купил билет на поезд – и уехал на нем навсегда. С девушкой они потом поженились.

В Хельсинки мужчина сел на паром до Стокгольма, а в Швеции обратился к местным правозащитникам, попросив помочь с политическим убежищем. Те отправили его обратно в Финляндию: по европейскому законодательству просить убежище можно только в той стране, через которую человек въехал в Евросоюз.

Вернувшись в Хельсинки, бородатый мужчина нашел помещение с вай-фаем и написал письмо на общую редакционную почту «Медузы», где я работал специальным корреспондентом. Его почтовый адрес по-русски выглядел бы как «Мертваярука1984» – это отсылало одновременно и к антиутопии Джорджа Оруэлла, и к системе «Периметр», комплексу автоматического управления ответным ядерным ударом, созданному в СССР в разгар холодной войны. В Америке «Периметр» называли «Мертвой рукой»: система была придумана так, чтобы запустить ядерные бомбы, даже если все, кто мог это сделать вручную, к тому времени были бы убиты.

В письме мужчина представился Александром Вярей, одним из руководителей *Qrator Labs* – российской компании, занимающейся защитой от DDoS-атак [1]. Он рассказал, что российские чиновники и спецслужбы интересуются кибероружием, а он сам был свидетелем того, как оно применялось по распоряжению государства.

«Сейчас, когда в РФ обстановка накаляется, я опасаясь, что меня могут „припахать“ заниматься организацией атак, так как я уже „в теме“, и я принял решение поставить общественность в известность, – писал Вряя (здесь и далее в цитатах героев сохранены авторские особенности орфографии и пунктуации). – Я считаю, что граждане должны знать, на что тратятся деньги в условиях кризиса. И КТО занимается этими грязными делами. Это не какие-то мелкие жулики. Если раньше все только догадывались, то теперь у вас есть доказательства:) Чтобы меня внезапно не переехала машина, например, мне пришлось покинуть страну. Это решение мне далось очень нелегко, я, считай, потерял хорошую работу, уезжаю от семьи просто в никуда. Плюс сейчас всякие шлюхи вроде *Lifenews* будут меня „мочить“».

¹ DDoS-атака – способ вывести из строя сайт или сервер, перегрузив их. Как правило, во время атаки очень много устройств, зараженных вирусом, одновременно начинают заходить на один и тот же сайт; он не успевает обработать нагрузку и перестает открываться или работает очень медленно.

Я ответил, что хотел бы подробнее узнать его историю и встретиться лично. Наш разговор сразу же перешел в секретный чат в Telegram – в России 2015 года уже массово начали пользоваться защищенными чатами, понимая, что российские спецслужбы могут слушать и читать открытые каналы, хотя по закону и должны сначала получить на это разрешение суда.

– Как быстро вы сможете приехать? Собираюсь идти сдаваться и просить защиты, – написал Вяря.

– Послезавтра?

– Оу.

– Долго?

– Нужно остановиться где-то сначала.

– Могу и завтра попробовать.

– Ох, я постараюсь найти какой-нибудь отель, у меня всего 4к на карте осталось.

Вяря остановился в общей комнате одного из городских хостелов. Хельсинки – дорогой город, но ему повезло и он нашел ночлег за 20 евро в сутки. На следующее утро, когда я сидел в самолет, я получил от него сообщение: «Непередаваемый экспириенс с хостелом, я впервые. Храпят, говорят во сне, ворочаются всю ночь».

Вскоре мы встретились у торгового центра неподалеку от набережной. Вяря стоял около дверей, нервно оборачиваясь и выглядывая меня среди переходящих через трамвайные пути. Все вещи – два рюкзака – были у него с собой. Мы зашли в ближайшее кафе, заказали кофе, и он начал рассказывать о том, что с ним произошло.

* * *

Александр Вяря родился в середине 1980-х в ленинградской коммуналке и рос без отца. Когда ему было двенадцать, он увлекся компьютерами – сначала видеоиграми, потом программированием и «железом». Первой его работой была должность системного администратора в компании его двоюродного дяди. Социальные сети тогда только начинали появляться, но аккаунты в них Вяря не заводил принципиально: не хотел оставлять никаких следов в интернете.

Переехав в Москву, он поработал сетевым инженером в нескольких хостинг-компаниях [2]. В 2012 году он обнаружил на одном из профильных форумов интересную вакансию – и после пары тестовых заданий его взяли в компанию *Qrator*, специализирующуюся на защите от DDoS-атак.

К тому времени она уже лидировала на рынке: среди ее клиентов были и многие независимые СМИ (телеканал «Дождь», «Новая газета», «Ведомости»), и банки («Альфа», «Тинькофф»), и интернет-магазины («Юлмарт», *Lamoda*). По словам Вяри, их услугами даже однажды воспользовался интернет-магазин по продаже кедровых бочек; что удивительно – именно на него была совершена самая серьезная атака за все время его работы в компании. «В России популярно сводить счета с конкурентами с помощью DDoS-атак, некоторым магазинам один день простоя стоит закрытия», – объяснял он. Такие атаки стоят очень дешево (около 3 тысяч рублей в сутки) и могут при этом вывести незащищенный сайт из строя, что приведет к серьезным убыткам.

Вяря работал в техподдержке и постоянно отвечал на звонки клиентов. Нередко в *Qrator* обращались те, кто недоволен тем, что она защищает в том числе оппозиционные сайты. Весной 2012-го – накануне инаугурации президента Владимира Путина – прогосударственные хакеры-патриоты атаковали сайты «Эха Москвы», «Коммерсанта» и «Дождя» – все они были клиентами *Qrator*. «Зачем же вы защищаете евреев?» – сказал Вяре один из позвонивших в тот день.

² Хостинг – место хранения данных для сайта в интернете.

Во время выборов мэра Москвы в 2013 году *Qrator* защищал сайт Алексея Навального: оппозиционный политик выдвинул свою кандидатуру и вел успешную кампанию. В какой-то момент Вяря заметил возле офиса компании фургон с тонированными стеклами и антеннами на крыше. В следующие дни он появлялся там почти каждый день. Выходя на обед, сотрудники *Qrator* пытались заглянуть в фургон и шутили, что тем, кто их прослушивает, надо бы принести пончики.

«Саша – талантливый человек, но очень впечатлительный и с тараканами в голове, – сказал мне его бывший начальник Александр Лямин. – Когда слишком долго работаешь в информационной безопасности, начинаешь меняться, начинаешь во всем видеть угрозу себе».

Так или иначе, к 2015 году Вярю повысили до руководителя службы эксплуатации. Он начал часто ездить за границу: приходилось посещать дата-центры, расположенные в европейских странах, чтобы устанавливать программное обеспечение, способное работать при больших нагрузках – во время атак. В *Qrator* такие серверы с фирменным ПО называют «центрами очистки трафика». Они помогают окружать сайты клиентов виртуальным «забором» с «пограничными пунктами», которые отфильтровывают здоровый трафик от паразитного.

Тогда же компания начала подготовку к открытию первого зарубежного отделения в Праге. Всем сотрудникам делали рабочие визы. Возглавить филиал должен был Вяря.

3 февраля 2015 года генеральному директору *Qrator* Александру Лямину позвонил Вартан Хачатуров, заместитель главы департамента инфраструктурных проектов Минкомсвязи. Хачатуров попросил кого-то из сотрудников компании помочь чиновникам с одним «щекотливым вопросом». Кроме Вяри помогать было некому: все разъехались по конференциям.

Хачатуров связался с Вярей и оставил номер телефона, на который тот отправил сообщение. Ближе к вечеру раздался звонок: звонил некий Василий Бровко. Вяря понятия не имел, кто это. Бровко сказал ему, что через пару дней им вместе необходимо слетать в столицу Болгарии, Софию; все необходимые документы оформит его помощница.

Вяря поискал в интернете информацию о Бровко и схватился за голову. Больше всего ему запомнилось, что тот основал компанию «Апостол», которую Алексей Навальный весной 2013 года обвинял в том, что она с помощью ботов [3] раскручивала соцсети «Аэрофлота». В последнее время Бровко работал начальником департамента коммуникаций в «Ростехе» – госкорпорации, созданной для производства высокотехнологичной продукции гражданского и военного назначения. Руководил ею Сергей Чемезов, близкий знакомый Владимира Путина.

Вяря предположил, что от него хотят помощи по его профилю – выбрать новую систему защиты от DDoS. Но удивился, что позвали в Болгарию: известные производители соответствующего программного обеспечения находятся в Израиле и Штатах.

5 февраля 2015 года он прилетел в Софию. Отправил сообщение Бровко; тот ответил, что встреча состоится во второй половине дня. Вяря погулял по центру, потом подошел к назначенному месту – помпезному стеклянному зданию *Grand Hotel Sofia*.

Вскоре появился Бровко. В одной руке у него был смартфон российского производства, а в другой айфон; он постоянно что-то на них набирал. Вяря поприветствовал Бровко и сказал, что София – удивительно небольшой город. «Помойка», – бросил Бровко в ответ.

Следом появились двое мужчин. Они оказались сотрудниками местной компании *Packets Technologies* (сайт⁴ компании скромно сообщает, что организация специализируется на «разработке передовых сетевых технологий»). Бровко сказал Вяре, что нужно сходить в офис компании: «посмотреть продукт» и высказать свое мнение.

³ Бот – программа, которая по расписанию выполняет определенные задачи. В последние годы так называют и живых людей – например, сотрудников «фабрики троллей».

⁴ Примечания и ссылки, собраны на странице <https://individuumbooks.com/vtorzhenie/notes/>...сайт компании скромно сообщает, что организация специализируется на «разработке передовых сетевых технологий»: <https://packetstechnologies.bg/bg/> (сейчас сайт недоступен)

Офис располагался неподалеку. В переговорной один из сотрудников *Packets Technologies* включил презентацию, а заодно рассказал о себе: работал в израильской армии, консультировал по сетевой безопасности крупнейшие интернет-компании, участвовал в *Black Hat* (главная мировая конференция по информационной безопасности, на которую приезжают и представители IT-корпораций, и хакеры).

После этого сотрудник болгарской компании, как утверждает Вря, заявил: «Сейчас я вам представлю продукт для организации DDoS-атак». Названия у программного обеспечения не было. Сотрудник добавил, что «продукт» умеет организовывать DDoS-атаки на сетевом уровне. Такие атаки «забивают» ресурсы сервера паразитными пакетами, из-за чего система перестает принимать полезные пакеты трафика.

Система представляла собой небольшое устройство – «коробку» с программным обеспечением, установленную на одном из трафикообменников [5]. Для «продукта» была выделена специальная полоса с максимальной мощностью в 10 Гбит / с. Специалисты *Packets Technologies* добавили: система позволяет совершать «коктейльные» – то есть смешанные по типам – атаки, которые труднее всего отражать; кроме того, можно легко увеличить трафик, установив еще одну «коробку». В 2010 году атака силой 10 Гбит / секунду была совершена на серверы *Wikileaks*; мощность крупнейшей DDoS-атаки⁶ в истории интернета – голландский хостер *Cyberbunker* против компании *Spamhaus* – достигала 300 Гбит / секунду: как писали в *The New York Times*, она «замедлила интернет».

Закончив с теоретической частью, сотрудник компании запустил VPN-соединение [7] и Тор-браузер [8], обеспечив себе анонимность (начало такой атаки отследить практически невозможно). Набрал в браузере IP-адрес [9] – открылась страница с крайне простым интерфейсом. Наверху размещалась адресная строка, ниже – около десятка названий подвидов DDoS-атак, рядом с каждой – пустая ячейка, которую можно отметить галочкой. Внизу – кнопка для выбора мощности атаки: от 100 мегабит до 10 гигабит в секунду. «Можно не на всю катушку, если жертве достаточно поменьше», – поясняет Вря.

Сотрудники компании ввели в строке интерфейса адрес сайта министерства обороны Украины. В соседнем окне открыли страницу сервиса, по которому можно определять работоспособность сайтов. Затем включили программу в полную силу. Возник график, показывающий мощность атаки – вскоре она достигла 10 Гбит / с. Сервис работоспособности показал, что сайт недоступен. Его попробовали открыть в браузере, но он не загрузился. Через пару минут атаку остановили и сайт снова стал открываться.

Потом они попробовали атаковать сайт украинского министерства обороны на мощности в 100 Мбит / с – он снова перестал работать.

«Давайте проверим на slon.ru», – предложил Бровко, до этого молчавший (я воспроизвожу его реплику со слов Вря). «Слон» (сейчас называется *Republic*), одно из самых популярных независимых новостных СМИ в России, атаковали на мощности 10 Гбит / с. Сайт перестал открываться и лежал несколько минут. Позже тогдашний главный редактор «Слона» Максим Кашулинский подтвердил мне, что 5 февраля 2015 года они зафиксировали атаку, которая на две минуты обрушила сайт.

⁵ Трафикообменник – точка обмена трафиком между провайдерами; их создают и для оптимизации скорости соединений.

⁶ ...мощность крупнейшей DDoS-атаки в истории интернета: «DDoS-атака 300 Гбит/с замедлила весь интернет», доступно на <https://xakep.ru/2013/03/27/60346/>

⁷ VPN – самый простой способ скрыть свое реальное местонахождение и адрес в интернете. Виртуальная частная сеть, которая по зашифрованному каналу может соединять компьютеры в разных городах и странах, делая вид, будто они находятся в одной локальной сети.

⁸ Тор – браузер, который скрывает данные пользователя и позволяет заходить на сайты, не индексирующиеся обычными поисковиками.

⁹ IP-адрес – уникальный адрес компьютера, подсоединенного к интернету.

«А что, если сайты пользуются защитой? Пробьете?» – спросил Вря. Ему ответили, что в этом случае придется узнавать реальный адрес сервера (все сервисы защиты пропускают атаку через себя, а реальный адрес сервера маскируют), но у *Packet Technologies* есть соответствующая методика. Вря уточнил, сколько стоит система; по его словам, Бровко ответил: «Около миллиона долларов».

После встречи Вря и Бровко отправились в *Grand Hotel Sofia*. Сели в лобби, взяли кофе. Вря вспоминает, что Бровко больше всего интересовало, как найти реальный адрес сайта и на каких трафикообменниках лучше всего ставить такую систему. Через некоторое время сотрудник «Ростеха» якобы сказал: «Ну что, нам нужен кто-то, кто будет этим управлять». Вря поперхнулся и сказал: «Нет, извините. Я не хакер. Это против моих принципов, и это противозаконно». Бровко, по словам Вря, спросил: «Ты знаешь, какая организация тебя сюда пригласила?» Вря предположил, что он намекает на ФСБ, но вслух сказал, что впредь готов только отвечать на вопросы по технической части. Они добавили друг друга в *Telegram* и разошлись.

Вря, по его словам, был шокирован произошедшим. Он сразу написал обо всем своему начальнику Лямину – тот рекомендовал «остаться максимально в стороне». На следующий день, 6 февраля, Вря вернулся в Москву.

Вря предоставил мне скриншоты дальнейших переписок с Бровко и свои с начальством. Сотруднику «Ростеха» он написал несколько сообщений с советами по технической части. В частности, порекомендовал использовать для системы голландские трафикообменники, где «проходят терабиты трафика – и на десяток гигабит не обратят внимания». Бровко ответил коротко: «Спасибо. Изучаю».

5 марта 2015 года Вря написала помощница Бровко, сообщила, что тот просит о встрече: «На Патриарших прудах. Это не конкретное заведение, просто прогулка». Через несколько часов Вря ответил, что этот вопрос нужно решать с его руководством. Тогда ему написал уже сам Бровко.

Привет. Мы же вроде договаривались иногда общаться без вовлечения твоего руководства.
Сможем сег повидаться?

Вря:

Привет
шеф просит через него решить
как он скажет

Бровко:

Нууу
Зачем?

Вря:

он очень недоволен что через голову прыгают, обычно Варган [Хачатуров] ему звонит и с ним обсуждает
а я человек подневольный и без одобрения шефа не могу

Бровко:

Ну ты скажи, что кофе выпить выйдешь

Вря:

к сожалению, не могу: (

Бровко:

Не прав, но ладно

Дай номер шефа своего

Лямину все это не понравилось. Он завел в *Telegram* чат под названием «WTF», куда пригласил Вярю, Бровко и Хачатурова.

Лямин:

Коллеги.
День добрый.
Сказать что я взбешен – это ничего не сказать.

Хачатуров:

Привет

Лямин:

Вартан, я всегда рад помочь тебе. Ты знаешь. Но когда к моим сотрудникам начинают лезть через мою голову – Я ПРОТИВ

Хачатуров:

Я честно говоря думал, что это разовая история:)

Лямин:

Я согласился помочь с Софией. Ни больше, ни меньше. Весь остальной «креатив» мной санкционирован не был. <...>. Ждем комментариев и объяснений Василия Бровко.

Хачатуров:

Коллеги, давайте только спокойно:)

Лямин:

я спокойно в бешенстве
джентльмены так не поступают.

Бровко:

Не понимаю о чем речь в целом. Мне Денис [Вяря не знает, кто это такой. – *Прим. Авт.*] сказал, что вы мой консалтинг в очень щекотливом вопросе. Нет, так нет

Хачатуров:

Василий, просто Денис не сказал, что это длящаяся работа, а не разовая помощь:)

Бровко:

Разовая помощь
15 мин хотел

Хачатуров:

Мне кажется, это тогда не проблема, Саш

Лямин:

Я не знал что это 15 минут и зачем эти 15 минут

Хачатуров:

Просто нужно с тобой согласовать

Лямин:

В любом случае это мой сотрудник рабочее время которого оплачиваю я.
о чем вообще речь?
есть мой контакт – со мной и работайте.
дело не в том что 15 минут. дело в том что с людьми на моей зарплате
общаются через мою голову. это недопустимо.

Хачатуров:

Ладно, Саш, успокойся, пожалуйста. Это недоразумение, и мы его уже
урегулировали:)

Лямин:

Надеюсь меня услышали и поняли.

По словам Вяри, после этого Бровко и его сотрудники больше к нему не обращались.

* * *

Я написал Василию Бровко на номер в *Telegram*, с которого тот предлагал Вяре встретиться для обсуждения кибератак. Он почти сразу же ответил, что «был в Болгарии для анализа системы защиты от киберугроз, а не для совершения таковых». «Не буду комментировать обвинения за рамками здравого смысла и не имеющие связи с реальностью, – добавил Бровко. – „Ростех“ постоянно подвергается кибератакам – с начала года на предприятия корпорации их было совершено свыше 11 тысяч».

Начальник Вяри Александр Лямин пригласил меня поговорить в офис *Qrator Labs*. Он оказался веселым разговорчивым бородачом в кедах и разноцветной футболке – и подтвердил, что Вяря ездил на встречу с Василием Бровко по просьбе Хачатурова из Минкомсвязи. «Речь шла вовсе не о системе для DDoS-атак, а о трафикогенераторе – системе, необходимой для проверки устойчивости сайтов к нагрузке, – сказал Лямин. – Да, скорее всего, был залп по „Слону“. Экспериментальный, на проверку. Нелегально? Это серая зона».

Лямин предположил, что Вяря чем-то обижен на его компанию и, возможно, рассказывая о заказе «Ростеха», выполнял заказ «Лаборатории Касперского», их главного конкурента. «В Финляндии доллары пригодятся», – сказал Лямин и отправил мне ссылку¹⁰ на расследование *Reuters* о том, что Евгений Касперский призывал «мочить конкурентов». Он добавил, что не уверен, что Вяря «здоров».

Весной 2015 года сотрудников *Qrator* всюю оформляли в Чехию. Вяря с семьей переехали из съемной квартиры в Чертанове в Бирюлево, чтобы немного сэкономить денег перед границей.

В конце мая Вяря обнаружил возле офиса знакомую машину – тот самый тонированный фургон с антеннами, который приезжал к зданию компании, когда *Qrator* обслуживал сайт Навального. Через несколько дней он увидел такой же автомобиль возле своего дома. Вяря говорит, что «начал параноить»: ему казалось, что он встречал одних и тех же людей в разных частях города. Он решил ездить из дома на работу разными маршрутами.

В последних числах июля Вяря сказал начальству, что не сможет ехать в Чехию, якобы потому что жена против. Тем не менее Лямин хотел, чтобы у сотрудников его компании были европейские документы: он посоветовал Вяре получить вид на жительство в Финляндии, где у сотрудника были родственники по отцовской линии. Для ВНЖ требовалось сдать экзамен на знание финского языка. Вяря взял отпуск, чтобы его подучить.

¹⁰ ...ссылку на расследование *Reuters*: «СМИ узнали об угрозах Касперского „мочить“ конкурентов», доступно на <http://top.rbc.ru/business/29/08/2015/55e0ed279a794742b6f4add8>

Параллельно, по словам Вяри, его знакомые рассказывали, что им продолжают интересоваться сотрудники «Ростеха» и спецслужбы, чтобы в конце концов привлечь к работе над кибероружием, раз он уже видел его в действии. Вярю и сам был уверен, что так и произойдет – или его «ударят по башке».

В августе 2015 года друзья со связями в спецслужбах посоветовали ему покинуть Россию. На следующий день он собрал вещи в два рюкзака и уехал в Хельсинки.

* * *

Ранним утром 25 августа 2015 года мы с Вярёй пришли к полицейскому участку в Хельсинки, в котором он должен был заявить о том, что просит политическое убежище. Участок был еще закрыт; рядом ожидали несколько беженцев из Ирака. После короткого интервью и снятия отпечатков пальцев Вярёю отправили в один из миграционных лагерей – трехэтажное здание недалеко от центра Хельсинки с бесплатной столовой. Внутри и вокруг дома ходили десятки иракцев и сирийцев, без остановки разговаривавших по телефону.

После заселения Вярёя встретил беженца из Чечни. Тот рекомендовал ему беречь постиранные вещи: в лагере воруют. На следующий день он познакомился с парой из Сибири, скрывающейся от уголовного преследования, и интеллигентным сыном какого-то египетского министра. На третий день из лагеря увезли мужчину с подозрением на малярию. На четвертый день Вярёе сказали, что после большого интервью с сотрудниками миграционной службы его, скорее всего, переведут в миграционный лагерь в 600 километрах к северу от Хельсинки – ждать решения по его делу.

Так и произошло. После этого в течение полутора лет Вярёю переводили из одного лагеря в другой, периодически вызывая на дополнительные интервью. Его не сильно ограничивали в передвижениях; ему выплачивали пособие, на которое с трудом, но можно было жить.

Его историей заинтересовались в посольстве Украины в Финляндии – на встрече с украинцами Вярёя рассказал, как проходила атака на сайт министерства обороны. «Ростех» и российские следственные органы на заявления Вяри никак официально не отреагировали.

* * *

В конце декабря 2016 года на первой полосе *The New York Times* вышла заметка о Вярёе, основанная на материалах, которые я делал для «Медузы» (позже газета получит Пулитцеровскую премию за серию материалов о России, включая этот). В тексте его назвали «элитным хакером». Вярёя удивился и написал мне: «Илитный хакир, блядь, что они несут?» После выхода статьи его в очередной раз вызвали на разговор финские спецслужбы – спросили, что он знает о российских хакерах и недавнем взломе энергетической системы Финляндии.

Летом 2017 года Вярёя наконец получил политическое убежище в Финляндии. В начале сентября – через два года после его бегства из России – мы решили встретиться. Я его не узнал. Он похудел на 20 килограмм и выглядел как человек, сбросивший груз, который его долго мучал.

Как рассказывал Вярёя, полтора года в финской миграционной системе дались ему непросто. Он даже пытался покончить с собой, но друзья вовремя вмешались и отвезли его в больницу, где он провел следующие несколько недель. Денег было мало, воссоединиться с семьей не получалось, допросы отнимали очень много времени; единственной отрадой была рыбалка, на которую он часто выезжал на велосипеде на целый день. Соседями Вяри по миграционным центрам в основном были иракцы и сирийцы, бежавшие от «Исламского государства» (запрещено на территории РФ. – Прим. ред.). Большинство сидели на антидепрессантах, у многих были ранения. Они часто принимали Вярёю за сотрудника центра.

Купив пиво и травяную настойку, мы с Вярей дошли до одного из озер на окраине города: он где-то вычитал, что там хороший клев. «Я теперь уже как дома тут. Меня все устраивает, климат мой, – сказал программист. – Я будто и не в эмиграции уже, это моя новая жизнь». Открыв металлическую коробку и немного покопавшись в снастях, он закинул спиннинг в воду.

* * *

Несколько недель спустя встречи с Вярей в одном из московских кафе я услышал знакомый голос. Обернувшись, я увидел бывшего начальника Вяри, Александра Лямина. Он давал кому-то интервью и сначала меня не узнал, а когда я поздоровался с ним, отвел глаза. Когда он уходил, я поздоровался с ним еще раз – оказалось, что, когда я поздоровался в первый раз, он подумал, что разговаривает слишком громко и мешает мне работать.

Лямин сказал, что рад, что Вяре удалось наконец получить документы. По его словам, большая часть сотрудников компании уже переехала в Прагу: оттуда удобнее предоставлять услуги по защите от кибератак. В конце разговора он спросил: «Что ты думаешь про историю с Михайловым, ФСБ, госизменой?» (незадолго до того высокопоставленный сотрудник ФСБ, занимавшийся киберпреступностью, был арестован по обвинению в государственной измене). Оказалось, Лямин в последнее время много об этом размышлял.

История Вяри – редкий случай, когда человек открыто рассказал об интересе российского государства и спецслужб к кибероружию. Возможно, Вяря единственный, кто отказался работать над таким оружием – и смог исчезнуть без серьезных последствий (если, конечно, не считать таковыми полный отказ от прежней жизни, в том числе семьи).

К осени 2017 года Вяря сменил имя и фамилию на финские; переехал, поменял телефон, почту и *Telegram*. Сейчас он мечтает купить большую лодку, с которой можно ловить лосося, ходящего на большой глубине. Похожими вещами он занимается и на работе: он устроился в неправительственную организацию, которая следит за тем, как одни государства совершают кибератаки на другие.

Часть I

Корни

Глава 1

Территория свободы

В 1992 году молодой житель Санкт-Петербурга Кирилл впервые попал¹¹ на рынок «Юнона» на юго-западной окраине города. Сформировалась толкучка еще в предыдущем десятилетии: вокруг магазина «Юный техник» собирались люди, которые продавали радиодетали, разложив их на тротуарах. С наступлением рыночной эпохи рядом отгородили территорию и поставили прилавки – при этом рынок сохранил свою специализацию: в основном там торговали электроникой и запчастями к ней. Одними из популярных предложений были 15-минутные сеансы игры на приставке *Atari*.

Как и многие петербуржцы, Кирилл купил на этом рынке свой первый компьютер – и сразу начал проводить за ним много времени. Через пару лет юноша ненадолго уехал в США, где как раз начал приобретать популярность интернет; в Калифорнии Кирилл открыл свой первый браузер. Вернувшись на родину, он заметил, что свой цифровой андеграунд постепенно зарождается и в России, и решил делиться с людьми полученными в США знаниями про то, что такое WWW, FTP [12] и IRC [13].

Вскоре Кирилл познакомился с другими первыми российскими любителями компьютеров и интернета. Себя они называли «сценой», их было около 30 человек, большинство жили в Москве и Петербурге. В 1995 году они впервые собрались на *Enlight*, фестивале любителей компьютеров; среди прочего там, например, проводился конкурс по метанию винчестера на дальность. Впрочем, в основном они встречали друг друга в IRC-чатах – и это общение многим заменяло обычное.

«Улицы России тогда были куда менее приветливыми, чем сегодня. Самой популярной темой для разговоров всегда была сама жизнь. Всё – от баб до космоса», – рассказывал один из представителей «сцены». – «Конкретных тем не было, фан заключался в том, что мы стали первыми в мире, кто использовал преимущества интернета для общения. Когда [в 1997 году] принцесса Диана разбилась – это произошло ночью, – на канале были люди отовсюду. И один из них жил в квартале от происшествия. Он сходил, посмотрел и, вернувшись, стал рассказывать о своих впечатлениях. А весь мир начал это обсуждать только через 8 часов, просмотрев выпуски новостей».

Одной из главных проблем в те годы было получить доступ к компьютеру: иногда это было непросто даже для тех, у кого они были дома. Программист Антон Мельников подробно вспоминал¹⁴, на какие ухищрения ему и его другу Мише приходилось идти, чтобы играть в компьютерные игры, – например, прогуливать школу. Вначале они симулировали болезни и печатали справки на струйном принтере. «„Болезнь“ дома я не мог, так как у нас жила бабушка, поэтому каждое утро приходилось мучительно вставать и переться как будто бы в школу. Ино-

¹¹ ...молодой житель Санкт-Петербурга Кирилл впервые попал на рынок «Юнона»: «Сценерский лайфстайл: часть 1», доступно на <http://xakep-archive.ru/xa/090/088/1.htm>

¹² FTP – протокол передачи файлов между компьютерами.

¹³ IRC – протокол обмена сообщениями.

¹⁴ ...Программист Антон Мельников подробно вспоминал, на какие ухищрения ему и его другу Мише приходилось идти: <https://twitter.com/proxiper/status/1045631964244578304>

гда врал, что нужно ко второму-третьему уроку, но часто так делать было нельзя – палево, – рассказывал Мельников. – Вместо школы я шел к Мише, но была проблема: его дом был ровно напротив школы. Так как в этот момент все одноклассники и учителя тоже шли в школу, приходилось играть в шпиона: идти аккуратно, нарезать круги, прятаться за сугробами etc. Потом пасти, когда отец Миши свалит на работу».

Были и другие трудности. «Отец Миши увидел появляющуюся у него зависимость [от игр и интернета] и собрал чудо-девайс, который подавал электричество на комп только при наличии ключа, – вспоминает Мельников. – Миша ключ, конечно, спиздил и сделал копию». Когда отец друга, как-то вернувшись домой, обнаружил, что монитор горячий, он начал прятать провод питания – и тогда подростки купили замену. Потом отец Миши стал убирать монитор в кладовку. «Но и тут решение было найдено. У двери были большие зазоры, и мы просто научились снимать ее с петель, – продолжает Мельников. – Самая жесь случалась, когда кто-то звонил в дверь. Нужно было оперативно отключить монитор, оттащить его в кладовку и поставить дверь на место».

В итоге друзья прогуляли почти целую школьную четверть. «Разоблачение закончилось одним из самых стыдных моментов в моей жизни, – говорит Мельников. – Нас шеймили перед всем классом. И каждый следующий учитель делал это заново. Особенно их тронула подделка справок. Нам пророчили карьеру фальшивомонетчиков». Теперь он играл у себя дома по ночам, разработав сложную систему, которая отключала систему охлаждения компьютера, чтобы он не шумел и не вызывал подозрения у родителей. Недостаток у нее был один: техника перегревалась – и однажды Мельников проснулся от того, что в комнате стоял запах гари.

Только через некоторое время после этого у подростков появился доступ в сеть. «Платить за интернет на фоне моей опустившейся школьной успеваемости никто не хотел, но выход нашелся, – говорит Мельников. – У провайдера „Метаком“ появился „гостевой доступ“. Халявный пул, где можно было посидеть в местном IRC и поюзать фтп. Время не было ограничено, но было очень сложно дозвониться. Хочется сказать спасибо людям, которые это сделали. Они во многом изменили мою судьбу и помогли найти себя на долгие годы. В общем, сидел я там безвылазно. Обзаводился друзьями и развивался как айтишник».

Похожим образом были устроены жизни и других молодых россиян, открывших для себя компьютеры. Некоторые из них быстро поняли, что на этом можно еще и зарабатывать: тем более что, как вспоминает Кирилл, большинство первых хакеров увлекались вошедшими тогда в моду рейвами и наркотиками, на которые нужны были деньги.

По словам хакера, сначала «сценеры» занимались «варезом» – компьютерным пиратством. Другие тратили дни (с медленным интернетом того времени), чтобы скачать популярные программы, записывали на CD-диски и перепродавали на рынках.

Следующим этапом стало воровство кредиток и взломы закрытых сетей – это приносило куда больше денег, чем пиратство. Участники группировки STEALTH рассказывали¹⁵, что еще в 1994 году внедрились в американское посольство и называли себя «создателями боевых роботов-убийц на просторах киберпространства». Их коллеги вспоминали¹⁶, как взламывали сайт Новороссийска и получали доступ к компьютерам Верховной Рады Украины. Сам Кирилл в какой-то момент основал хакерскую группировку *Sodom*. Ее лозунг гласил: «*Russian Mafia – we'll take care of you*».

«В девяностых Россия и Украина зажигали по полной. Можно было делать все что угодно, так как не было никакой законодательной базы, – вспоминал участник хакерского андерграунда начала 1990-х. – Нашей свободе завидовали все. В России не было ограниче-

¹⁵ ... Участники группировки STEALTH рассказывали, что еще в 1994 году внедрились в американское посольство: «Я – создатель боевых машин-убийц!», доступно на <http://xakep-archive.ru/xa/003/036/1.asp.htm>

¹⁶ ... Их коллеги вспоминали, как взламывали сайт Новороссийска: «Российские хак-группы: кто они?», доступно на <http://xakep-archive.ru/xa/026/044/3.asp.htm>

ний, как у ребят в Европе и Штатах. На мировой сцене нас всегда уважали и боялись, так как подрастающему поколению парни из России внушали животный страх рассказами о пушках, водке, мрачных улицах и других вещах».

Глава 2

Как обидеть тетю Асю

Это наш мир, мир кодов и электронных импульсов, наполненный красотой модемных звуков. Мы бесплатно пользуемся услугами, которые могли бы стоить копейки, если бы вы не спекулировали на наших потребностях и не были так жадны, – вы называете нас преступниками. Мы стремимся к знаниям – вы называете нас преступниками. Мы существуем без цвета кожи, без национальности и религиозных предубеждений – вы называете нас преступниками. Вы производите атомные бомбы, разжигаете войны, убиваете, обворовываете и врете нам, пытаясь убедить в своей правоте, – а мы все так же остаемся преступниками. Да, я преступник. Мое преступление – любопытство. Мое преступление – в том, что я сужу о людях по их знаниям, мыслям и поступкам, а не по тому, как они выглядят. Мое преступление в том, что я умнее вас, за что вы не можете меня простить. Я хакер, и это мой манифест. Вы можете остановить кого-то из нас, но вы не можете остановить нас всех.

В 2003 году в российском издании «Хакер» был опубликован¹⁷ фрагмент манифеста хакеров, который впервые появился за 17 лет до того в американском сетевом издании PHRACK. Для читателей русского перевода все сказанное в нем уже было прописными истинами: к тому моменту издание для «компьютерных хулиганов» пять лет весело и доступно рассказывало всем желающим, как взламывать электронную почту, организовывать DDoS-атаки и воровать данные кредитных карт.

«Хакер», запущенный в 1998 году издательским домом *Gameland* (в основном там выходили журналы о видеоиграх), быстро стал для многих российских школьников и студентов предметом своего рода культа. Этот ежемесячный журнал чем-то напоминал «Поваренную книгу анархиста» Уильяма Пауэлла. В начале 1970-х молодой и злой Пауэлл, считавший, что знания должны быть доступны всем, а люди способны сами принять разумные решения, написал и издал пособие, в котором рассказывалось, как делать взрывчатку из общедоступных ингредиентов, вести слежку и убивать людей. На протяжении следующих десятилетий книгу нередко находили в квартирах террористов и убийц – например, подростков, устроивших стрельбу в американской школе «Колумбайн» (сам Пауэлл в итоге стал учителем и многие годы пытался запретить переиздавать свой труд).

В первом же номере «Хакера» была опубликована инструкция о взломе кредитных карт; во втором – советы о том, как угнать аккаунт в мессенджере ICQ (заголовок: «Как обидеть или защитить тетю Асю»), а также материал с перечнем программ для взломов. «На самом деле существует два способа хакать, – писал автор материала. – Первый: ты покупаешь кучу книг по устройству и работе Интернета, языкам программирования, операционным системам, протоколам, работе процессора и т. д. Ты все это внимательно читаешь и через два года тренировок сможешь видеть все дырки и получать нужную тебе инфу без проблем. Но ведь ты лентяй! <...> И поэтому ты выбираешь второй способ: пусть другие парни книжки читают и программы пишут, а я уже воспользуюсь плодами их труда. Ну что ж, ладно, хорошо, не вопрос!»

В других материалах журнала рассказывалось про «самые урожайные хаки» и про места в интернете, где можно искать уязвимости нулевого дня [¹⁸]. Журнал публиковал мемуары чело-

¹⁷ ...в российском издании «Хакер» был опубликован фрагмент манифеста хакеров: «Манифест хакера», доступно на <http://xaker-archive.ru/spec/007/053/1.html>

¹⁸ Уязвимость нулевого дня – «дыра» в программном обеспечении, неизвестная производителю.

века, взломавшего банк; советы, как не попасться в лапы к спецслужбам; и интервью со знаменитостями – певец Дельфин, например, называл хакерство «экстремальным видом спорта» и признавался, что и сам хотел бы «что-нибудь взломать».

В шестом номере «Хакер», рассказывая об уязвимостях критической инфраструктуры, даже нечаянно предсказал будущее своих читателей. «Информационные войны в конце XX века стали настолько реальными, что в определенный момент можно будет развернуть третью мировую, не выходя из дома, сидя за клавишей своего компьютера, – писал автор материала. – И если раньше министерствам обороны различных стран приходилось уделять особое внимание защите своих наземных, воздушных и морских границ, то теперь появилась еще одна граница – виртуальная. Ну и кто же эти границы будет защищать? На мой взгляд, это будут выросшие хакеры, которым надоест заниматься всякой шнягой бесплатно, и они применят свои знания для работы на спецслужбы и Министерство обороны, становясь виртуальными пограничниками, отслеживающими каждый электрон, проходящий от континента к континенту».

Журнал фактически предлагал российским подросткам, жившим в бедных провинциальных городах, где нечем заняться, альтернативу. «Тебе катастрофически не дают. Обидно, но это легко исправить – стань хакером», – прямо говорилось в одном из номеров. Будущий хакер, который в 2000-х начал заниматься кардингом, в конце 1990-х рос в сибирском городе: в советское время он был организован вокруг большого промышленного предприятия, но после распада СССР завод закрылся и большинство жителей лишились работы. Раз в месяц после школы подросток ходил в единственную в городе палатку с прессой и покупал новый номер «Хакера» – продавщица в какой-то момент начала узнавать его в лицо и сразу протягивала ему журнал. «Возможно, к нам вообще только один номер и привозили, – вспоминал хакер в разговоре со мной. – Как бы тупо это ни звучало, „Хакер“ был как глоток свежего воздуха среди общей серости вокруг».

Впрочем, читали «Хакер» и в Москве. Илья Гофман родился в конце 1970-х в интеллигентной семье: его отец был композитором, мать занималась искусством. В детстве у него была сильная аллергия и астма, из-за чего он учился дома. У мальчика обнаружился талант и к музыке – он играл на скрипке и альте, – и к математике: он увлекался алгеброй и в подростковом возрасте опубликовал несколько научных работ в математических журналах. После школы Гофман поступил в Московскую консерваторию имени Чайковского – одним из его преподавателей стал Юрий Башмет. К концу 1990-х Гофман считался¹⁹ одним из самых перспективных и талантливых российских академических музыкантов.

Весной 1998 года он увлекся журналом «Хакер». Больше всего Гофману нравилась рубрика «Взлом», в которой рассказывалась, как воровать данные кредитных карт и преодолевать защиту банков; как он позже говорил, «все [было] доступно, как в сказке». Хакерство казалось юноше «удивительным явлением из области человеческого воображения», занятием романтического толка. «Одно дело – человек играет в компьютерную игру и не может из нее вылезти, – объяснял Гофман позже. – Но это понятно – потому что игра красивая, разработан интерфейс. А хакер живет в виртуальном мире, но имеется в виду не компьютерная реальность, а его внутренний мир. Это человек, который видит черный экран и мигающий курсор – и этого достаточно для него, чтобы он понимал, что он в этот момент действительно там. Это было как ребус, было довольно забавно изучать. Это была очередная математическая задача, да, на грани, но никто не ставил целью никакие финансовые операции. Мне казалось, что мораль не нарушается. Ведь у всего этого в банковской системе есть компенсационные механизмы – все восстановимо».

¹⁹ ...Гофман считался одним из самых перспективных и талантливых российских академических музыкантов: «Альт F4 Илья Гофмана», доступно на <https://www.kommersant.ru/doc/217749>

Он взял себе ник *NetSerpent* («Интернет-змея») и нашел компаньонов. Вместе они смогли перевести на свои счета около 97 тысяч долларов из 16 американских банков и нескольких российских: информацию о картах получили после взлома канадского интернет-магазина. Подозрительную активность заметили сотрудники отдела безопасности российского банка, в котором эти счета находились. Искать злоумышленников долго не пришлось: все счета они открывали под своими настоящими именами.

На украденные деньги хакеры покупали сотовые телефоны (тогда они были роскошью), а также вещи из бутиков *Versace* и *Calvin Klein*. Гофман свою долю потратить так и не успел: осенью 1998 года всех задержали и юного скрипача как предполагаемого организатора группировки отправили в СИЗО. В «Московском комсомольце» их назвали²⁰ «змеями из интернета».

В защиту Гофмана выступил Юрий Башмет, который назвал его «не только одним из лучших студентов моего класса, но и одним из лучших молодых альтистов Москвы». «Мне кажется, что необходимо сделать все возможное, чтобы сохранить его талант для нашей отечественной культуры», – говорил музыкант. Несмотря на это (и на астму), Гофман полгода просидел в «Матросской тишине» в камере на 70 заключенных – где продолжал писать музыку.

Суд приговорил юного москвича и его подельников к пяти годам условно. Выйдя на свободу, Гофман стал лауреатом IV Международного конкурса альтистов Юрия Башмета и продолжил музыкальную карьеру, выиграв еще несколько мировых соревнований альтистов. Сейчас он преподает в Гнесинке и часто выступает с концертами.

²⁰ ...их назвали «змеями из интернета»: «Змеи из интернета», доступно на <http://www.mk.ru/old/article/1999/11/14/133894-zmei-iz-interneta.html>

Глава 3

Сомнения стали страстью

На первых российских хакеров влияли не только форумы и профильная пресса, но и поп-культура. О людях, которые, сидя за компьютерами, управляют судьбами и государствами, писали фантасты и снимали фильмы в Голливуде. Первый из них появился еще в 1983 году – он назывался *Wargames*, и один из хакеров, взламывавший предприятия по всему миру в поисках секретных документов, рассказывал мне, что в детстве кино произвело на него большое впечатление. По сюжету хакер-подросток, проникнув в сеть американского военного ведомства, находит там файлы, которые принимает за видеоигры: «Воздушные бои», «Военные действия в городских условиях», «Война в пустыне», «Глобальная термоядерная война». В итоге дело чуть не заканчивается третьей мировой. Когда *Wargames* только вышел, он всерьез напугал²¹ тогдашнего президента США Рональда Рейгана – после этого Рейган поручил разработать стратегию национальной безопасности в области автоматических информационных систем; секретная директива об этом была подписана в 1984-м.

В середине 1990-х Голливуд снова обратился к теме хакеров. Один из фильмов, который так и назывался – «Хакеры», запустил карьеру Анджелины Джоли и рассказывал о том, как группа киберподпольщиков борется с алчным сотрудником транснациональной корпорации. Когда в 2004 году был проведен большой опрос²² среди посетителей русскоязычных хакерских форумов, выяснилось, что именно это кино повлияло на них сильнее всего, заставив задуматься о самоидентификации и «сопротивлении корпоративной глобализации».

До России видеокассеты с «Хакерами» добрались почти одновременно с тем, как фантаст Сергей Лукьяненко написал свой роман «Лабиринт отражений» о «дайверах», работающих в виртуальных мирах. При всем киберпанке во многом книга была реалистичной: в перерывах между рейдами в интернет герой ел бутерброды с колбасой. В романе даже был романтический гимн хакеров:

Наша работа во тьме –
Мы делаем, что умеем,
Мы отдаем, что имеем, –
Наша работа – во тьме.
Сомнения стали страстью,
А страсть стала судьбой.
Все остальное – искусство
В безумии быть собой.

Несколько моих собеседников рассказывали, что хорошо помнят этот диссонанс между повседневной российской реальностью 1990-х, когда даже на колбасу хватало не у всех, и безграничными возможностями интернета. К концу десятилетия на многочисленных хакерских форумах уже сложилось крепкое сообщество со своей атмосферой и даже своей культурой: кто-то сочинял стихи, кто-то – рассказы. Писали и «секретные инструкции для хакеров» о том, как выглядеть классно, если тебя снимают журналисты. Одна из них выглядела так:

- 1) Сесть за любое устройство, имеющее экран и клавиатуру

²¹ ... всерьез напугал тогдашнего президента США: *Dark Territory: The Secret History of Cyber War*, Fred Kaplan (Simon & Schuster, 2017)

²² ... большой опрос среди посетителей русскоязычных хакерских форумов: «Исследование компьютерного андеграунда на постсоветском пространстве», доступно на <https://bugtraq.ru/library/underground/research.html>

Центре „Выборы-99“, находящемся в Останкино, график предпочтений избирателей закономерно скачет – то на 5 % вырастает рейтинг у „Единства“, то у „Яблока“».

После этого по сюжету начинались беспорядки: «Народ уже всю бесновался. По многим каналам транслировали то, как уже в закрытых избирательных участках происходили драки, спровоцированные нервными сторонниками какой-то из политических сил, и народ в буквальном смысле разрывал бюллетени при вскрытии корзин с ними. В общем, началась повальная паника и беспредел».

Тогда такие сюжеты посетители хакерских форумов могли только выдумывать. Через двадцать лет – в 2016 году на президентских выборах в США – их мечты станут реальностью.

Глава 4

Школьники взламывают NASA

Большинство хакеров поначалу занимались взломами для развлечения: воровали пароли от родительских компьютеров, ломали соседский интернет, угоняли ICQ у друзей. Как сказал один из моих собеседников, «оказалось, что от воровства ICQ до участия в информационных войнах не так много шагов».

«[В середине 1990-х] интернет охватил все регионы России и принял глобальный характер. О проделках так называемых хакеров можно было услышать только из-за бугра или увидеть в кино, но наши люди не заставили долго ждать, – вспоминал²⁵ один из хакеров, начинавший в те годы. – Вскоре в России был организован отдел по борьбе с компьютерными преступлениями, в московских газетах появились статьи о „маленьких гениях-хакерах“, которые теперь отсидживают срок. На самом деле были пойманы бедные детки, студенты, которые просто хотели подзаработать немного денег через интернет, заказывая товар на дом по фальшивым кредиткам (к реальному хакерству это ну никак нельзя было отнести). А тем временем, пока люди из ФСБ гонялись за этими „хакерами“, другие спокойно себе сидели дома и получали новые знания, чувствуя себя в полной безопасности. Можно даже сказать, что хакерство в России развивалось с огромной скоростью и при этом не ощущало никаких преград со стороны органов правопорядка».

В 1998 году несколько приятелей создали группировку под названием «Камера предварительного заключения» – чаще они сами себя называли KPZ. «Как раз тогда тысячи подростков, посмотрев дошедший до России фильм „Хакеры“ и начитавшись статей в журналах, ринулись в интернет, возомнив себя профессиональными взломщиками», – вспоминал²⁶ участник группировки. В KPZ состояли от пяти до десяти участников. Первым делом они отомстили известному московскому компьютерному клубу «Орки», администрация которого «нанесла некоторый моральный ущерб» одному из друзей. Группировка взломала серверы заведения. После этого KPZ выполнила несколько взломов на заказ, а когда в российском интернете «ничего привлекательного не осталось», заинтересовалась интернет-ресурсами правительства США. Как утверждали²⁷ участники группы в одном из номеров «Хакера», они сумели взломать²⁸ 21 американский сайт – среди них были ресурсы университетов, военных ведомств и NASA.

Хакеры из KPZ довольно охотно рассказывали о себе – один из них признавался, что ему 15 лет и он учится в 10 классе. «Можно сказать, что я – хорошист:) Учусь на 3–4, – писал²⁹ он в материале, опубликованном в «Хакере» в 1999 году. – Кстати, в нашей школе даже нет предмета „Информатика“. Вот такая вот школа:) Приходиться все познавать самому: читать много книг на любые компьютерные темы, экспериментировать и делать многое другое без какой-либо помощи окружающих. В недалеком будущем собираюсь пойти работать в техподдержку к какому-нибудь провайдеру. Ну и было время, что мы нахацкали кучу военных хостов».

Как-то раз в квартире одного из участников KPZ выключилось электричество. В дверь постучали.

– Кто там? – спросил хакер.

²⁵ ...вспоминал один из хакеров, начинавший в те годы: «Хакерская группа KZP – изнутри», доступно на <http://xakep-archive.ru/xa/004/032/1.asp.htm>

²⁶ ...вспоминал участник группировки: там же

²⁷ ...Как утверждали участники группы в одном из номеров «Хакера»: «Хакерская группа KZP – изнутри», доступно на <http://xakep-archive.ru/xa/004/032/2.asp.htm>

²⁸ ...они сумели взломать 21 американский сайт: там же

²⁹ ...писал он в материале, опубликованном в «Хакере» в 1999 году: «Хакерская группа KZP – изнутри», доступно на <http://xakep-archive.ru/xa/004/032/3.asp.htm>

- Милиция! Откройте.
- По какому поводу?
- По компьютерному.

Войдя в квартиру, милиционеры забрали компьютер и повезли участника группировки в свой участок. Там они открыли на компьютере ICQ, изучили его, но «увидели только загадочные слова». Задав юноше несколько протокольных вопросов – «они даже и не знали, что спрашивать», – милиционеры отпустили его домой.

С развитием хакерского сообщества постепенно начал формироваться и рынок, на котором можно было купить их услуги. Дмитрий (имя изменено по его просьбе) заинтересовался взломами в начале 2000-х, когда ему было 13: для игр его компьютер был недостаточно мощным, а заняться чем-нибудь хотелось. Сначала они с одноклассником делали сайты: друг рисовал дизайн в тетради на уроках, а Дмитрий прямо на бумаге писал код. «Такие ограничения способствовали изобретательности, и у меня довольно быстро возник интерес к тому, как такие сайты ломать», – вспоминает хакер.

Первыми его жертвами стали сайты других школьников. Вскоре он открыл для себя хакерские форумы. Тогда их было много: *hackzone.ru*, из которого потом вырос закрытый *Underground Information Center* (старожилам *Hackzone* не нравилось, что сайт заполнили подростки, и они решили создать для себя отдельное пространство), *bugtraq.ru*, *void.ru*. Дмитрий стал завсегдатаем «Античата»³⁰, где обсуждались компьютерные уязвимости, взломы и новости информационной безопасности. Как и в случае других форумов, многие посетители «Античата» фактически жили на сайте – и даже посвящали ему песни³¹:

Просыпаясь рано утром, я включаю интернет
Захожу на Antichat.ru, в мире сайта лучше нет...
Античат.ру, Античат.ру,
За тебя я все сайты перетру!
Античат.ру, Античат.ру,
Потому что я тебя люблю

На форуме было несколько уровней доступа; попасть на следующий можно было, написав статью и доказав свои познания в программировании. Поднимаясь вверх в иерархии «Античата», Дмитрий познакомился с другими молодыми хакерами. Несколько лет спустя многие из них станут лучшими в России специалистами по кибербезопасности; другие начнут зарабатывать нелегальными взломами, а некоторые даже получают тюремные сроки в США. Сам он в итоге от идеи зарабатывать взломами отказался, потому что не мог «воспитать в себе параноика»: «Это ведь постоянный стресс, нужно всегда быть осторожным».

У его коллег по форуму таких проблем не было, и они открыто предлагали свои услуги всем желающим. Многие из подобных сайтов существуют и сейчас – и там по-прежнему можно найти коммерческие предложения: за деньги можно купить вирус, взломать соцсети или почти любой мессенджер (кроме *Telegram*), заказать слежку за своими близкими, организовать DDoS-атаку или накрутить себе рейтинг в игре GTA5. Объявления выглядят так³²:

Узнаем оригинальные логин и пароль ЖЕРТВА НЕ УЗНАЕТ О
ВЗЛОМЕ. Удаленно взломаем любой компьютер и получим доступ к любым
данным и информации на компьютере, работаем 24 часа в сутки.

³⁰ ...Дмитрий стал завсегдатаем «Античата»: <http://forum.antichat.ru/>

³¹ ...посетители «Античата» фактически жили на сайте – и даже посвящали ему песни: Antichat.ru – NoFear, доступно на https://www.youtube.com/watch?v=ZRiGv6Q3txA&list=PLT5tHbJPR2_opfQPmuy6pKd1C_qiWV0eD

³² ...Объявления выглядят примерно так: <https://blackbiz.club/threads/vzлом-whatsapp-viber-instagram-facebook-uznaem-vzlomaem.5098/>

Предоставляю услуги по устранению сайтов и серверов с помощью DDOS атак. Работаем с профессиональными приватными программами, которые устранят, положат, уронят, и приостановят работу сайта или сервера на заказанный вами ресурс. С нашей помощью вы устраните конкурента, или врага, который перешел вам дорогу, или помешал вам в бизнесе. У нас лучшее соотношение цены и качества на рынке ddos услуг, обращайтесь.

Как правило, хакеры обещают клиентам анонимность, скидки при длительном сотрудничестве и «индивидуальный подход». Один из людей, предлагающих такие услуги, рассказал мне, что одна из главных статей его дохода – взлом паролей по заказу. По его словам, денег такая работа приносит много, а делать ее, как правило, очень просто – большинство людей по-прежнему пользуются паролями вроде 124567 или *qwerty*.

Глава 5

Школа для взломщиков

Пока первые хакеры формировали собственные сообщества, на новый род занятий обратило внимание и государство. В конце 1990-х и начале 2000-х в большинстве российских технических вузов появились кафедры информационной безопасности. Самые сильные из них – в МГУ, МФТИ, университете имени Баумана, петербургских ЛЭТИ и университете информационных технологий, механики и оптики. Выпускники этих вузов к середине 2000-х стали пользоваться большим спросом на новом рынке труда: компании начали массово нанимать «пентестеров» (людей, проверяющих информационную безопасность бизнеса с помощью смоделированных кибератак).

Уже к середине 2010-х математики, программисты, специалисты по кибербезопасности захватили мир. Их влияние усиливается с каждым годом из-за постоянного роста количества средств слежения за гражданами, уязвимости личной информации, сбора больших данных – таких математиков исследователи, например, называют³³ создателями WMD (*weapons of math destruction*).

Впрочем, российское компьютерное образование создавалось вовсе не с нуля. Еще с 1960-х элитные советские математические школы и вузы, куда поступали их выпускники, готовили победителей международных олимпиад и будущих успешных ученых; постепенно эта система дополнилась разветвленной сетью выездных лагерей и сборов для юных математиков и компьютерщиков. Все эти институты сохранились и после распада СССР. Именно благодаря им российские подростки годами выигрывают мировые чемпионаты по программированию. Один из моих собеседников говорил, что российские хакеры стали лучшими в мире именно благодаря сильной системе образования: даже если конкретные взломщики сами не учились в матлицах или вузах, они все равно так или иначе представляют эту школу.

«Во всей этой истории очень важна математика, – объясняет Андрей Лопатин, сотрудник петербургского университета ИТМО и тренер юных российских программистов. – Все успехи можно напрямую связывать с сильной российской матшколой. Петербургская матшкола играет в этом большую роль, особенно 239-й лицей и кружки при Аничковом дворце. Я сначала там решал задачи по информатике на бумаге. Туда же ходил и Николай Дуров». (Николай – брат основателя «ВКонтакте» и *Telegram* Павла Дурова; именно он отвечал за программирование в обоих проектах.)

В Летнюю компьютерную школу – она проводится в июле-августе в одном из санаториев под Костромой – каждый год приезжают по 200 школьников со всей страны (есть у ЛКШ смена и в зимние каникулы). Нередко поездки оплачивают региональные власти или большие российские интернет-компании – «Яндекс» или «ВКонтакте»; туда же многие выпускники ЛКШ уходят работать, окончив университет. В школе изучают алгоритмы, структуры данных, теоретическую информатику. Каждый день подростки по 4 часа занимаются математикой; после обеда самостоятельно решают задачи.

«Советская и российская матшколы – это прежде всего очень сильные внеклассные занятия, – объясняет Лопатин. – На них рассказываются вещи за пределами школьной программы: они помогают быстро комбинировать идеи и для олимпиадного программирования, и для работы в корпорациях, и для чего-то другого».

То есть, например, для взломов. Российский хакер, ездивший в ЛКШ, вспоминает в разговоре со мной, что именно там научился быстро думать и изобретать оригинальные решения.

³³ ...называют создателями WMD: *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Cathy O'Neil (Broadway Books, 2016)

Сам он до шестого класса увлекался чистой математикой, но как только у него появился постоянный доступ к компьютеру, начал увлекаться информатикой. Пока на уроках компьютерной грамотности одноклассники играли в *Need for Speed*, он изучал языки программирования и писал свои первые программы. «Поиграть я всегда мог – меня с уроков математики отпускали в компьютерный класс, потому что на самих уроках мне делать было нечего, – вспоминает мой собеседник. – Для меня все задания там были – устный счет. Учительница знала, что я пойду не в игры играть, а делать что-то толковое». Потом он начал ездить в ЛКШ, потом – поступил в МГТУ имени Баумана на факультет информационной безопасности, но не доучился и вскоре стал зарабатывать на простых взломах, получая заказы через форумы.

ЛКШ – не единственное внеклассное мероприятие для талантливых подростков-программистов. Летом 2017 года я оказался в Петрозаводске – столице Карелии на берегу Онежского озера, где каждую зиму проходит самый престижный слет такого рода: в течение недели около полусотни школьников соревнуются друг с другом, решая задачи и готовясь к международным чемпионатам по программированию. «Петрозаводские сборы – самые древние, – рассказывает один из их организаторов Андрей Станкевич. – Почему наши ребята такие крутые? В том числе из-за того, что в СССР была построена сеть матшкол – мероприятия по программированию потом делали по их образцу».

Станкевич, выигравший несколько олимпиад по информатике в юности, в середине 2000-х стал курировать сборы программистов и возглавил команду петербургского ИТМО, которая побеждала на российских соревнованиях больше других. По его словам, после нескольких побед на олимпиадах и чемпионатах молодыми программистами начало интересоваться государство. Станкевич даже участвовал во встрече с Владимиром Путиным: как он объясняет, такие мероприятия хорошо подходят для поисков дополнительного финансирования спортивного программирования. После той беседы программирование внесли³⁴ в перечень дисциплин, которые преподают в лагере для одаренных детей «Сириус» в Сочи, созданном по инициативе Путина.

В 2013 году, продолжает Станкевич, подростками-компьютерщиками «очень заинтересовались» военные из Министерства обороны. Поначалу им было непросто. «Им тяжело заинтересовать наших, потому что у них там много ограничений. По передвижению, всему прочему. А у нас тут ребята космополитичные, хотят быть мобильными, – объясняет Станкевич. – Но я знаю, что некоторые ребята, которые учились у нас в летних школах, теперь учатся в академии ФСБ».

Со временем Минобороны и связанные с ним структуры (например, Ассоциация руководителей служб информационной безопасности, которую возглавляет бывший сотрудник КГБ и ФСО Виктор Минин) начали организовывать и собственные хакерские конкурсы: на них нужно, уложившись в определенное время, взломать какую-нибудь систему. В паузах участники конкурсов слушают выступления сотрудников министерств обороны и связи – те рассказывают³⁵ о подготовке «будущих защитников информационного пространства», о структуре ЦРУ и о хакерских группировках.

Борис Мирошников, много лет возглавлявший отдел по расследованию киберпреступлений в МВД, еще в 2005 году заявлял³⁶ на конференции о киберпреступности, что «российские хакеры – лучшие в мире». «Вчерашние подростки, бессистемно промышлявшие хакерством,

³⁴ ...После той беседы программирование внесли в перечень дисциплин: «Андрей Станкевич стал медиаперсоной года по версии „Комсомольской правды в Санкт-Петербурге“», доступно на http://news.ifmo.ru/ru/university_live/achievements/news/6802/

³⁵ ...они рассказывают о подготовке «будущих защитников информационного пространства»: https://vk.com/video-129090933_456239022?api_access_key=585f3ac8e3e68c4647

³⁶ ...заявлял на конференции о киберпреступности, что «российские хакеры – лучшие в мире»: «Российские хакеры – „лучшие в мире“», доступно на <https://www.securitylab.ru/news/215244.php>

выросли и усовершенствовали свои методы. Раньше этим занимались озорные мальчишки. Теперь они выросли, – говорил полицейский. – Они осознали, что если ты в чем-то хорошо разбираешься, ты должен использовать это, чтобы заработать на жизнь. Они стали хакерами и объединяются через сети, чтобы разбогатеть. Всем известно, что русские сильны в математике. Наши программисты лучшие в мире, поэтому и наши хакеры лучшие в мире».

Глава 6

Выпускник

Большинство выпускников технических университетов не становятся хакерами в полном смысле слова. Они уходят в профильные НИИ, связанные с Минобороны (подробнее о таких учреждениях – в главе 27), или начинают работать в частных IT-компаниях, которые с середины 2000-х начали активно возникать в России. Впрочем, некоторые из них легально предлагают примерно те же услуги, которые киберпреступники продают за деньги на своих форумах. Например, слежку за людьми.

В середине 2000-х в одной из сильнейших математических школ Москвы – № 1543 на юго-западе – учился высокий и улыбчивый школьник Артем Кухаренко. До школы он добирался на междугороднем автобусе из подмосковного Троицка; дорога обычно занимала около полутора часов в одну сторону – мимо Внуково, завода «Мосрентген», через МКАД.

Кухаренко с пятого класса ходил в кружки по информатике, летом ездил в компьютерные школы, где учили алгоритмическому программированию, структурам данных, методам их анализа; в 2006 году он победил на всероссийской заочной олимпиаде по информатике. После школы Кухаренко поступил в МГУ на факультет вычислительной математики и кибернетики, даже не думая про другие варианты. На втором курсе он ходил на спецкурс «Введение в компьютерное зрение», а в конце того года после собеседования попал в лабораторию компьютерной графики и мультимедиа при факультете. В лаборатории проводились эксперименты по машинному обучению и нейронным сетям [37]. Ближе к четвертому курсу по совету заведующего лабораторией Кухаренко обратил внимание на новую и неизученную область – распознавание лиц.

После выпуска из университета Кухаренко сменил несколько работ и часто путешествовал. В 2015 году на новогодних каникулах у него оказалось много свободного времени, и он от скуки написал приложение, определяющее породу собаки по фотографии, – для этого они с девушкой вручную разметили на 150 фотографиях собак их породы и загрузили их в самообучаемую нейронную сеть. Приложение не стало популярным, но следующей весной Кухаренко отправился с ним по возможным инвесторам. Им он рассказывал, что нейросети с распознаванием лиц – это будущее, и к 2020 году этот рынок вырастет до 6 миллиардов долларов. Некоторые поверили – так появилась компания *N-Tech. Lab*.

Один из инвесторов и кураторов проекта – Александр Кабаков. Он друг Василия Бровко, сотрудника «Ростеха», который, по словам Александра Вяри, испытывал программы для DDoS-атак на сайте slon.ru. Кабаков и Бровко вместе отдыхают и путешествуют – судя по фейсбуку, в 2016 году они делали это почти каждый месяц. Еще один инвестор – Максим Перлин, связанный с прокремлевскими молодежными движениями; его самый известный проект – эротический календарь со студентками МГУ, выпущенный в 2010 году ко дню рождения Владимира Путина.

Весной 2015 года компания Кухаренко въехала в небольшой офис в незаметном бизнес-центре недалеко от Тишинской площади в Москве. *N-Tech. Lab* занимали целый этаж, но в офисе было пусто и почти отсутствовала мебель. На первые инвестиции компания приобрела четыре сервера за несколько миллионов рублей каждый – три поставили под столы программистов, еще один установили в отдельном охлаждаемом помещении. Показывая свои владения,

³⁷ Нейронная сеть – систему соединенных между собой простых процессоров, которую можно обучить решать задачи. В нейронных сетях может быть несколько уровней, каждый уровень комбинирует признаки предыдущих уровней – то есть создаются все более сложные комбинации, о которых могут даже не знать сами ее создатели.

Кухаренко, внешне похожий на Эдварда Сноудена, улыбался и хвастался: «*Google* для этих целей использует тысячу серверов, а у нас их всего четыре».

Они написали алгоритм, который назвали *FaceN*, – нейросеть, которая сама обучалась и находила отличительные признаки лиц для опознания людей: величину глаз, фактуру бровей, форму губ и другие. Обучали сеть на миллионах фотографий; уже осенью 2015 года их алгоритм показал результаты лучше, чем у *Google*, – 73,3 % точных распознаваний лиц против 70,5 %. После победы на одном из программистских конкурсов компанию засыпали предложениями о продаже алгоритма, в том числе его хотела купить пограничная служба Турции, чтобы определять, кто переходит границу с Сирией. Были предложения и от российских спецслужб: московские власти решили подключить алгоритм к городской системе из более чем 100 тысяч видеокamer. «[Лица] людей, которые проходят мимо камер, [с помощью алгоритма] сверяются с загруженной в систему базой преступников или пропавших людей, – объяснял мне Кухаренко. – Если показывается высокая степень сходства, то предупреждение об этом отсылается сотруднику полиции, который находится рядом». Этот же алгоритм начали использовать для распознавания участников оппозиционных акций в Москве.

Параллельно Перлин предложил Кухаренко попытаться вывести его алгоритм на массовый рынок. Вместе они придумали *Findface* – приложение, которое позволяло бы по фотографии человека находить его аккаунт во «ВКонтакте». «Это стирает на хрен любую анонимность, – писал³⁸ Перлин, представляя приложение в своем фейсбуке. – Увидев симпатичную девушку в клубе, вы можете сфотографировать ее на телефон и моментально найти ее профиль во «ВКонтакте», узнать имя, интересы и отправить ей сообщение». Почти сразу же приложение начали использовать для другого: на анонимном форуме *2ch*, например, появился тред, в котором призывали искать «шкур, которые снимались в порно и работали проститутками». Приложение начали использовать полицейские: они поднимали старые дела, загружали в *Findface* фотографии подозреваемых, находили их во «ВКонтакте», а затем запрашивали у сети все данные пользователей.

Кухаренко все это не смущало: он считал, что безопасность важнее приватности. Я спросил его про пакет Яровой – как раз летом 2016 года Госдума приняла набор законопроектов, значительно облегчивший силовикам доступ к личным данным в интернете. «Мне вообще плевать, – ответил программист. – Я все обсуждаю в социальных сетях. Пусть ФСБ читает, с кем я спал, какие девушки у меня были. Деловая переписка? Ну узнают, сколько я зарабатываю и какие у меня клиенты. Я искренне считаю, что это никому не интересно. Проблема приватности преувеличена. Доступ к любому телефону получить элементарно, пусть спецслужбы меня читают».

В 2018 году система распознавания лиц, разработанная *N. Tech Lab*, начала работать в Москве. Как заявлял мэр города Сергей Собянин, уже к лету с помощью нее в метро задержали больше 10 человек, находившихся в розыске. Один из них, активист оппозиционной «Другой России», рассказывал, что у полицейских, которые его задержали, было специальное устройство, на котором была его фотография, сделанная камерой наблюдения, а также имя, дата рождения, адрес регистрации. Анкета светила красным и «пиликала»: оказалось, что в базу розыска его внес сотрудник центра по противодействию экстремизму. Мужчина спросил у полицейского, как он может исключить себя из этой базы. Полицейский ответил: «Никак».

³⁸ ...писал Перлин: <https://www.facebook.com/maxim.perlin/posts/745204182281015>

Часть II Деньги

Глава 7 Планета хакеров

Пока в США шла золотая лихорадка доткомов, российские хакеры – чаще всего еще подростки – запустили свою собственную: воровство кредиток американских торговых сетей и данных банков и интернет-магазинов многим из них начало приносить миллионы долларов. Если в США человек с хорошими программистскими навыками мог и без хакинга пойти получать десятки тысяч долларов, то в бывшем СССР, где люди зачастую зарабатывали несколько сотен долларов в год, искушение было слишком велико.

Первым среди российских хакеров получил международную славу петербуржец Владимир Левин, который в середине 1990-х украл из американского банка десятки миллионов долларов. Его довольно быстро вычислили, а курьеров, которые обналичивали деньги, арестовали. Левина экстрадировали в США, где он провел 36 месяцев в тюрьме – смешной срок по сравнению с теми, что хакеры получают сейчас. Вскоре по мотивам истории Левина сняли несколько эпизодов для российских сериалов про бандитов, а сам хакер, вернувшись в Россию, исчез – уже 20 лет никто не знает, где он и чем занимается.

В индустрию взломы начали превращаться в начале 2000-х – с появлением специализированных форумов, которые постепенно эволюционировали фактически в организованные группировки. «Раньше хакерские группы организовывались скорее как клубы по интересам. Люди занимались примерно одним и тем же и просто обменивались опытом, объединяли усилия в решении каких-либо задач, – рассказывал³⁹ в те годы Андрей Споров, он же хакер *Sp0Raw*. – Сейчас же организация групп часто строится для работы по конкретным делам. Если после выполнения нескольких совместных дел группа оказывается состоявшейся, она может существовать достаточно долго и заниматься своей деятельностью безнаказанно, потому что внешние контакты по делам ограничены: все специалисты есть внутри группы. Остались и группы, построенные по старым принципам, но там „воспитываются“ новички, которые, набравшись опыта на работе из интереса, начинают задумываться о превращении своих способностей в материальные блага».

Споров говорил, что российский интернет начала 2000-х чем-то напоминает российские улицы 1990-х. «Сейчас идет первичное накопление капиталов у людей, которые, вероятно, никогда не имели бы такой возможности, работая легально, – объяснял он. – Интеллектуальная преступность гораздо неуловимее ее обыденного собрата. В дальнейшем накопленные средства будут инвестированы во вполне обычные коммерческие проекты, некоторые из них существуют уже сейчас».

Главным сообществом киберпреступников в мире в начале 2000-х был российский форум *Carderplanet* – его еще называли «Планетой»: как объяснял мне один из хакеров, многим сайт и правда заменял реальный мир.

Начиналось все с сайта *carder.ru*, который в начале 2000 года создал человек, называвший себя *Script*. Из-за нескольких публикаций в журнале «Хакер» посещаемость вскоре выросла до 600 посетителей в день – тогда это было много. Вскоре *Script* закрыл форум и создал

³⁹ ...рассказывал в те годы Андрей Споров, он же хакер *Sp0Raw*: «Лицом к лицу с хакером», доступно на <https://www.vedomosti.ru/newspaper/articles/2004/11/02/licom-k-licu-s-hakerom>

Carderplanet, но задачи двух ресурсов совпадали: там торговали украденными кредитками – «картоном», как их называли на форуме. На сайте зарегистрировались около 1000 человек. В 2001 году *Script* сам присвоил себе на форуме статус «Вора в законе»: его кумиром был Саша Белов из недавно вышедшего сериала «Бригада», вымышленный криминальный авторитет, которого играл Сергей Безруков.

Вскоре «Планета» стала основным местом общения всего русскоязычного киберандеграунда: кроме кардеров там общались спамеры, создатели троянов [40], исследователи эксплойтов [41], взломщики аккаунтов на *PayPal* и люди, специализировавшиеся на подделке документов. Хакеры обменивались новостями, инструкциями по взломам, объясняли друг другу, как обезопасить себя от слежки. Многим новичкам, оказавшимся на форуме, казалось, что у них появилась возможность быстро начать зарабатывать большие деньги.

Подражая мафии, участники форума называли друг друга «семьей» и строили внутреннюю иерархию по принципам клана; у *Script* было звание не только «вора в законе», но и «крестного отца». Один из руководителей форума описывал⁴² эту иерархию так:

Sgarrista – зарегистрированный пользователь.

Dop – член семьи.

Caro Bastone – друг семьи и «правая рука» Крестного отца.

Gabellotto – верховный судья. Глава службы безопасности.

Consigliere – советник семьи по различным важным вопросам.

Caro di Caro – мемберы, на которых возложена миссия защиты и помощи семье.

Caro – надежные люди, к которым присматривается администрация, либо люди, не участвующие в жизни форума.

Giovane d'Onore – модератор форума.

Ripper – кидала.

Scum of Society – отброс общества. Чаще всего этот статус присваивался за оскорбления в адрес модераторов или мемберов.

Дятел – человек, постящий одинаковые объявления в разные разделы, задающий тупые вопросы, мешающий общению остальных мемберов.

«Хакеры взламывали защиту американских шопов и систем электронных переводов и собирали данные о кредитках их клиентов, – рассказывал⁴³ участник *Carderplanet*. – Все это добро передавалось кардерам, которые по своим каналам обналичивали деньги. После того как информация просочилась в прессу и журналисты рассказали миру о новом явлении, возможность быстро обогатиться привлекла толпы студентов. Большинство американских магазинов еще не имели опыта общения с кардерами, поэтому развести их не представляло большого труда даже для новичков. Падкий до халявы, народ заказывал часто, много и все подряд».

Большинство постоянных жителей «Планеты» зарабатывали⁴⁴ около 5000 долларов в месяц; доход основателя и других ветеранов сайта мог достигать до 100 тысяч. Эти деньги вкладывали в недвижимость, на них открывали шиномонтажи, цветочные магазины.

Script объяснял⁴⁵, что занимается кардингом в том числе для развлечения: «У человека, идущего на риск, выделяется так называемый гормон счастья. И вот этот гормон, помножен-

⁴⁰ Троян – вирус, выдающий себя за обычную программу или документ.

⁴¹ Эксплойт – программа, использующая уязвимость в безопасности другой программы.

⁴² ...Один из руководителей форума описывал эту иерархию так: «Планета СС. Золотое время *Carderplanet*», доступно на <https://bugtraq.ru/library/underground/planetacc.html>

⁴³ ...рассказывал участник *Carderplanet*: там же

⁴⁴ ...Большинство постоянных жителей «Планеты» зарабатывали около 5000 долларов в месяц: «Планета хакеров: как создавался крупнейший в мире форум киберпреступников», доступно на <http://www.forbes.ru/tekhnologii/tekhnika-i-biznes/332679-planeta-khakerov-kak-sozdavalsya-krupneishii-v-mire-forum-kiber>

⁴⁵ ...*Script* объяснял, что занимается кардингом в том числе для развлечения: «Кардинг. Интервью со *Script'ом*», доступно

ный на количество шелестящих бумажек, и играет основную решающую роль, заставляющую человека продолжать заниматься этим не совсем честным промыслом. Заниматься этим не стыдно. Стыдно пусть будет нашему правительству, что подростки уже в столь раннем возрасте превращаются в расхитителей». При этом *Script*, видимо, уже тогда сотрудничал с украинскими спецслужбами. Участники форума вспоминали, что он упоминал о том, что «СБУ (Служба безопасности Украины, украинский аналог ФСБ. – Прим. Авт.) его любит».

В 2002 году *Carderplanet* провел в Одессе кардерскую конференцию. На нее приехали около 20 человек. Они гуляли по городу, ходили в сауну, ели в ресторанах и обсуждали организационные вопросы. Домой большинство участников конференции вернулись в полном восторге: они впервые познакомились с теми, с кем годами общались только онлайн.

Тогда же на форуме появился пользователь под именем *Boa* («Удав» по-английски). Он быстро стал звездой: его статьи про хакинг и кардинг в то же время как будто рассказывали вообще о жизни. Главным хитом стала статья про этикет: ее Удав написал после того, как на форуме начали сотнями регистрироваться подростки, прочитавшие про «Планету» в журнале «Хакер» (некоторые ветераны *Carderplanet* просили *Script* поменьше его рекламировать, но тот отвечал, что «денег в интернете хватит на всех», а «органам мы не нужны»). Новички писали личные сообщения завсегдатаям форума и просили научить их взломам. Удав решил сначала научить их культуре общения.

Он писал так:

я хочу работать в спокойной обстановке, не отвлекаясь на разную ерунду, особенно на откровенный, уникальный дебилизм. Итак: Мне очень нравится приветствие *здравствуй* или *привет*. *Дарова* и подобное я воспринимаю нормально, если это исходит от тех, с кем я давно и плодотворно сотрудничаю. Всех остальных прошу воздержаться от такой фамильярности. Я не терплю обращение *братэло*, *перец*, *кардерюга*.

Четыре утра, Вы дома за компом или за бабой. Или перечитываете «Войну и мир» Толстого – Вам это в кайф в 4 утра. Заняты, в общем. Настойчивый звонок в дверь. Вопрос: Вы сразу распахиваете дверь нараспашку, не смотря в глазок или на монитор камеры, и с улыбкой приглашаете незнакомого бомжа зайти? Наливаете ему пива, расспрашиваете за жизнь, выслушиваете его просьбы, идиллия, в общем? Или все же спросите (хотя бы): Кто там? Спросите, видимо, для начала культурно какая это сука в 4 утра, бля, звонит в дверь, когда Вы никого, его мать, не ждете, и вам и так заебись? Ну дак какого же хера пачками идут запросы на авторизацию на Асю [ICQ] без ответа и приветов. Там рамочка есть – «reason of authorization request», или что-то в этом роде. Совсем не трудно наклацать строчку, типа, я такой-то, по такому то вопросу. Скажи в глазок имя свое и чего пришел, другими словами.

Впрочем, по основному профилю форума Удав тоже кое-что понимал. «Схемы воровства из американских банков начались с Удава, – рассказывал⁴⁶ позже один из кардеров. – Этот мужик-энтузиаст устраивал целые симпозиумы в отелях – учил всех воровать с американских кредиток. На *Carderplanet* многие делились такими секретами. Русский хакер – человек не жадный, это ведь не какой-нибудь кибергопник, а интеллигент с духовными скрепами. Из России можно грабить Америку почти в открытую, продолжая традиции холодной войны

на <http://xakep-archive.ru/xa/039/048/3.html>

⁴⁶ ...рассказывал позже один из кардеров: «„Если бы не стукач, нас бы не нашли“. История белорусского киберпреступника, живущего в США», доступно на <http://belgid.by/news/it/31784>

и подкармливая ФСБ. В 2002 году было столько дыр в онлайн-платежах, что через них можно было выносить вагонами».

Были у Удава проекты и за пределами *Carderplanet*. Сайт его «Фабрики», *boafactory.net*, предлагал всем желающим сделать за три дня российское гражданство, получить диплом об окончании престижного вуза, визу или водительские права. Здесь подделывали практически любые документы так, чтобы их почти невозможно было отличить от настоящих. На новых загранпаспортах даже проставлялись штампы о въезде и выезде из нейтральных стран, чтобы паспорт не выглядел новым. Кроме того, *Boafactory* помогала сделать фальшивые кредитки. Говорили⁴⁷, что к услугам «конторы» прибежали тысячи людей.

К 2004 году кардинг в исполнении русскоязычных пользователей стал настолько массовым, что англоязычные медиа заговорили о «холодной кибервойне». Тем летом *Script* заявил, что уходит из *Carderplanet*, а вскоре один из администраторов форума опубликовал пост, в котором сообщил, что «Планету» «пора закрывать», поскольку она находится «под колпаком всевозможных спецслужб – как русских, так и зарубежных»:

Работники ФБР ходят в компанию AOL, как к себе домой, беря оттуда логи от *icq* и распечатку из истории. Сотрудники ФСБ предлагают деньги хостинг-компаниям за логи этого форума. Какими бы мы все умными ни были, сколько прокси мы бы ни юзали, в каком бы темном уголке земли ни располагался ВПН, через который мы ходим – все мы люди и всем нам присущ человеческий фактор. Мы прекрасно понимаем, что многие потеряют работу, многие просто не смогут больше зайти и пообщаться с единомышленниками, но, к сожалению, мы не собираемся подставлять свой зад для чьих-то заработков.

На сбор вещей и обмен контактами пользователям дали две недели. Один из участников *Carderplanet* на прощание написал стихотворение по мотивам песни рэп-группы «Много-точие»: «Щемит в душе тоска, и темный конопляный дым въедается в глаза, как будто слезы пытаюсь выжать. Я помню, как всегда, заходя сюда и видя черно-синий цвет, я заново будто рождался».

Несмотря на закрытие форума, вскоре его участников начали задерживать. Через год очередь дошла и до *Script* – им оказался 22-летний Дмитрий Голубов. В момент задержания он скрывался в доме своей бабушки в Одессе. Голубова обвинили в создании международной организованной преступной группы, которая похитила более 11 миллионов долларов. Ему грозило до 12 лет лишения свободы, но в итоге его освободили⁴⁸ из-под ареста еще до суда – после того как за него лично поручились двое народных депутатов. «Парня просто угробят, – заявил один из них. – А ведь он молодой талантливый человек. Такие ребята – это сливки нашей молодежи». На одном из хакерских форумов освобождение Голубова прокомментировали так: «Как по мне так он красавец! Спи...ить столько лаве и выйти сухим из воды такое не каждый может!»

Голубов так и не предстал перед судом. Вскоре он и сам стал политиком – и даже создал «Интернет-партию Украины». На последних президентских выборах его партия пыталась выставить своего кандидата – Дарта Алексеевича Вейдера, использовавшего образ злодея из «Звездных войн». В 2018 году Голубов стал биткоиновым миллионером.

Судьбы его товарищей по *Carderplanet* сложились по-разному. Кое-кто, решив, что денег уже хватит, просто перестал воровать и уехал из России. Один из таких людей рассказывал

⁴⁷ ...его освободили из-под ареста еще до суда: «Банковские карты легли удачно», доступно на <https://www.kommersant.ru/doc/639299>

⁴⁸ ...его освободили из-под ареста еще до суда: «Банковские карты легли удачно», доступно на <https://www.kommersant.ru/doc/639299>

мне, что в лучшие времена получал от кардерской деятельности по 50 тысяч долларов в месяц, но, заработав на квартиры, дома и спорткары, решил успокоиться и осесть в одной из азиатских стран. Другие кардеры создавали новые площадки, следить за которыми было уже сложнее; по уровню влияния на киберподполье с *Carderplanet* можно сравнить разве что *Russian Business Network*, расцвет которой пришелся⁴⁹ на 2006–2007 годы. Некоторые бывшие участники *Carderplanet* продолжают заниматься тем же промыслом и сейчас – и как будто совсем не скрываются, например, создают открытые сообщества в социальных сетях, где ищут себе подручных и выкладывают видео о том, как снимают украденные деньги в банкоматах.

Хуже всего пришлось самым успешным соратникам *Script*. Мировые спецслужбы фактически объявили на них охоту – и начали отлавливать по одному.

⁴⁹ ...*Russian Business Network*, расцвет которой пришелся на 2006–2007 годы: Shadowy Russian Firm Seen as Conduit for Cybercrime, доступно на http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html?noredirect=on

Глава 8

Диссидент из Крыма

Кусок сала. Две банки соленых огурцов. Буханка черного хлеба. Чемодан с парой кроссовок и джинсами. Сборник рассказов Хулио Кортасара. Кассета с альбомом группы «Мышеловка».

Все это нашли и изъяли⁵⁰ при аресте у уроженца Крыма Романа Веги – он же Степаненко, он же *Boa*, он же Удав. Его арестовали в феврале 2003 года на Кипре. По словам⁵¹ другого бывшего участника «Планеты», у Веги нашли еще и около 200 фотографий основателей и участников *Carderplanet*: он постоянно делал им поддельные паспорта.

Роман Вега окончил математический факультет Симферопольского госуниверситета, после чего работал специалистом по системам комплексной безопасности и связи. Увлекался альпинизмом, спелеологией, коротковолновыми радиостанциями, а также противозаконными авантюрами, о которых до сих пор известно не так много (и в основном – с его слов). Хакер якобы продавал не только документы, но и оружие. В 1993 году его арестовывали в Египте, а в 1999-м – в Майами. «ФБР пыталась состряпать дело, что якобы одна из моих тогдашних майамских компаний была намерена поставлять оружие и спецтехнику баскским боевикам в испанский Сан-Себастьян, – писал⁵² Вега в своем блоге. – Кроме того, находившаяся в Кронштадте старая дизельная подлодка, которую хотели продать на металлолом, в бумагах превратилась в чуть ли не ядерную подводную лодку ВМФ России для перевозки кокаина в индустриальных масштабах из Колумбии в Штаты». Далее Вега утверждал, что дело против него развалилось, «что не помешало Вашингтону навесить на меня 250 миллионов долларов и указать в обвинении, что я якобы был организатором и руководителем нескольких хакерски-кардерских международных группировок».

В кипрской тюрьме Вега просидел полтора года, после чего его экстрадировали в США, где около десяти лет перебрасывали из одного города в другой, не предъявляя обвинений, – он побывал в Сан-Франциско, Оклахоме, Атланте, Нью-Йорке и Санта-Барбаре. Приговор – 18 лет тюрьмы за массовые взломы и объединение сотен хакеров – он получил только в 2013 году, спустя десять лет после ареста.

В США Вега начал вести подробный дневник. Он пишет от руки и передает записи друзьям, которые публикуют их на сайте romanvega.ru; как и когда-то на *Carderplanet*, он пишет много – и довольно талантливо. Из дневников можно выяснить, что в американских тюрьмах он успел поработать плотником и столяром в мебельном цехе, а также закончил заочно техникум в Миннесоте. Час в неделю Вега проводит уроки японского; играет на ударных и два раза в неделю ходит на уроки фортепиано; учит французский и испанский; раз в несколько дней бегает босиком во внутреннем дворе и в это время считает бабочек – как-то за 21 километр пробега насчитал их семь. В камере разрешают держать не больше пяти книг, а у него их около полутора сотен, поэтому над ним всегда висит угроза попасть в карцер. Последние несколько лет Вега пытается подготовить документы, чтобы его перевели досиживать срок в Россию, частью которой теперь является его родной Крым.

Некоторые свои заметки Вега называет «хроникой текущих событий», видимо, имея в виду диссидентский правозащитный бюллетень, выходивший в СССР с 1968 по 1984 годы.

⁵⁰ ...Все это нашли и изъяли при аресте у уроженца Крыма Романа Веги: «Система координат», доступно на <https://www.romanvega.ru/p/intro.html>

⁵¹ ...По словам другого бывшего участника «Планеты»: «Эксклюзивное интервью бывшего хакера, отсидевшего за киберворовство в США», доступно на <https://www.youtube.com/watch?v=3VIbPSPN8jE>

⁵² ...писал Вега в своем блоге: «Система координат», доступно на <https://www.romanvega.ru/p/intro.html>

Иногда он отвечает на вопросы посетителей сайта. Например, когда его спросили, изменил ли бы он что-то в своей жизни, если б знал, что попадет на 20 лет в тюрьму, он написал, что «страшнее тюрьмы физической – тюрьма внутренняя, тюрьма души». «Что лучше: жить в полную силу, пробуя себя в том и этом, смело идя навстречу новому опыту, навстречу опасностям и приключениям, не боясь трудностей, преодолевая их на грани своих возможностей, проходя через испытания, через дела, города и страны, через победы и поражения, через горести и радости; или же, таскаясь всю жизнь на какую-то опостылевшую работу, влачить убогое существование, с единственной мыслью „как бы чего не случилось?“, как бы не рухнул жалкий мирок боящейся жить души? Что лучше? Каждому свое, – писал Вега. – Помните у О’Генри? „Дело не в дорогах, которые мы выбираем, а в том, что внутри нас заставляет выбирать наши дороги“».

В феврале 2016 года в его тюрьме появился новый заключенный по имени Михаил Горбачев. Вега заинтересовался – выяснилось, что так зовут одного из афроамериканцев: тот рассказал, что мама придумала ему имя, когда, сидя с косяком перед телевизором в 1989 году, увидела на экране советского генсека, рассказывающего про перестройку. Чернокожих, сидящих в тюрьмах, Вега вообще недолюбливает: «Если их всех таких здесь выпустить на свободу, то в стране неизбежно и быстро наступит полный и уже окончательный хаос, резня и разруха, а нормальным людям (кто выживет) придется валить со всех ног». Бывший хакер Дмитрий Насковец рассказывал⁵³, что Вега – патриот России и всегда считал США врагами, которых «надо душить».

Американская тюремная система – любимая тема Веги: он знает, что в США больше заключенных, чем в любой другой стране мира, и охотно цитирует статьи Адама Гопника из журнала *The New Yorker*, написанные по этому поводу. Когда в 2011 году в тюрьме Вега получил письмо от избирательного штаба Барака Обамы с просьбой поддержать его кампанию по перевыборам (это обычная фандрайзинговая практика в США), хакер ответил гневным письмом⁵⁴ на шести страницах – о рабском труде и несправедливости:

Соединенные Штаты Америки отобрали у меня свободу, солнце (только и видим его раз в несколько месяцев из окна тюремного автобуса по дороге на суд) <...> правосудие; отобрали и возможность видеться с матерью – ей все время отказывает в визе ваше доблестное американское посольство. Граница на замке. 70-летняя мать ну никак не может встретиться с сыном, которого десятилетие держат без приговора. Твоя страна забрала мое здоровье и даже мои зубы.

Еще Вега часто упоминает «Архипелаг ГУЛАГ» Солженицына, особенно когда рассказывает о бездоказательных, по его мнению, процессах против американских русских. О своем хакерском прошлом человек, когда-то называвший себя Удав, в дневниках почти не вспоминает.

⁵³ ...Бывший хакер Дмитрий Насковец рассказывал: «Как кардер вышел из тюрьмы и делает бизнес на кибербезопасности», доступно на <https://secretmag.ru/trends/players/naskovets-hacker.htm>

⁵⁴ ...хакер ответил гневным письмом: <https://docs.google.com/file/d/0ByQf4BUGl49wSVV0Uk45U3doS1U/edit>

Глава 9

Белорусский Али-Баба

В 2004 году белорус Сергей Павлович, бывший завсегдатай сайта *Carderplanet*, купил себе новый «мерседес» и повесил на него номер 999. Потом он отпраздновал день рождения *DumpsMarket* – своего кардерского сайта. Вечеринка на даче длилась четыре дня, и на нее приехали большинство хакеров СНГ. «Алкоголь лился рекой, на столах танцевали шлюхи, пацаны нюхали кокаин», – вспоминал Павлович. Гости развлекались, стреляя из пистолетов по банкам; повара вылавливали прямо из озера карпов и осетров и жарили их на гриле.

Вскоре после этого Павлович отправился в гости к подруге. Вслед за ним туда приехали полицейские.

Пока они обыскивали дом, подруга сказала ему: «Зайчик, ты слышишь меня? Слушай. Что с тобой будет – неизвестно. Сейчас ты можешь сделать только одно: поесть. Потому что когда еще в следующий раз будет такая возможность». Она положила ему плов, шашлык, в карман куртки спрятала кусок хлеба. Его увезли в полицию, а через некоторое время белорусский суд приговорил Павловича к шести годам заключения за кардинг.

В тюрьме он написал мемуары «Как я украл миллион. Исповедь раскаявшегося кардера», в которых подробно вспоминал, почему и как стал хакером. В них много печали и много поэзии. «Моя жена, скорее всего, бросит меня. Дед, который меня воспитал, умрет [к тому времени, как я выйду из тюрьмы], – писал Павлович. – Мать состарится – больше от горя, чем от возраста. Для друзей стану призраком, с которым не о чем говорить».

Павлович уверен, что стал хакером из-за бедности и проблем в семье: «Больше всего киберпреступников [на территории бывшего СССР] – от безденежья. Мозгов у людей хватает, а реализовать себя смогли только в криминале». Компьютер у Павловича появился, когда ему было всего 12 лет, – большинство его друзей тогда еще играли в приставки вроде «Денди». Несмотря на это, большую часть свободного времени мальчик проводил в компьютерных клубах: домой ему не хотелось, потому что мать устраивала пьянки с незнакомыми мужчинами. Он играл в *Counter-Strike* и *Heroes of Might and Magic 3* – и как-то раз в перерыве между битвами наткнулся на *Carderplanet*.

Оказавшись на сайте впервые, он почувствовал себя, как «Али-Баба, который наткнулся на пещеру доверху наполненную сокровищами». Подросток понял: он нашел легкий способ разбогатеть, не отходя от компьютера. Если за обычную работу он мог получить около 200 долларов в месяц, то выполнение инструкций кардеров сулило ему миллионы. Он зарегистрировался на форуме, а через некоторое время создал свой: *DumpsMarket*, рынок для перепродажи украденных кредитных карт, фальшивых документов. «Дампы»⁵⁵ он получал от других хакеров – или продавал то, что украл сам.

И Павлович, и другие хакеры с «Планеты» предпочитали воровать только у иностранцев. «Жалко было [атаковать цели на территории бывшего СССР], – объяснял он. – В Америке все банковские счета застрахованы, а у нас владельца карты по милициям затаскают, все будут подозревать, что он сам у себя украл, а теперь еще и вернуть хочет. На наш век и буржуев хватит. Проявление патриотизма, что ли. Холодная война продолжается, сейчас ее новый виток, только в киберпространстве». Павлович признавался⁵⁶, что «никогда не смог бы украсть кошелек в общественном транспорте», но в интернете «не чувствуешь той грани, после которой начинается преступление». Еще он говорил, что «намного проще взломать выборную систему,

⁵⁵ Дамп – база украденных копий дебетовых и кредитных карт.

⁵⁶ ...Павлович признавался, что «никогда не смог бы украсть кошелек в общественном транспорте»: <https://tgraph.io/Interview-s-izvestnym-kardrom-08-10>

чем банки». Деньги Павлович хранил наличными в чемодане, который он закопал в огороде у деда.

«Я полностью посвящал себя работе, выкуривал по две пачки крепких *Marlboro*, набрал десять лишних килограммов, а специфический характер моих занятий не предполагал активного поиска новых друзей, – рассказывал Павлович. – Неудивительно, что в ту пору я спал в основном с дорогими шлюхами – высокие доходы позволяли мне иметь лучших из них. С миллионами жизнь особеннее, ярче, счастливее. Я тратил деньги иногда бездарно, иногда очень умело. Самый красивый способ расстаться с деньгами – это, конечно, женщины. Но самый приятный и, наверное, правильный – стать Санта-Клаусом, спасти жизнь тяжело больному человеку, оплатив ему операцию. Маме – новую машину, племяннику – компьютер и скутер, маме герлфренд – оплатить путешествие к океану, туда же – маму своей бывшей герлфренд». Когда Павлович однажды решил лично познакомиться с другим хакером, они заодно пригласили на встречу двух порноактрис.

Однажды у него украли со счета в *Webmoney* около 10 тысяч долларов. Когда он узнал IP-адрес вора, он заплатил знакомым сотрудникам ФСБ около 300 долларов, чтобы узнать его домашний адрес. Оказалось, что там был прописан пенсионер с 12-летним внуком. Он оставил их в покое.

Из тюрьмы Павлович вышел досрочно – в 2007 году. Почти сразу же он вернулся к кардингу, продаже оружия и созданию порносайтов, а параллельно консультировал местные спецслужбы: те подозревали заместителя начальника отдела по борьбе с киберпреступлениями в том, что он сам стал кардером. После тюрьмы начал активно заниматься спортом и сидеть на сайте знакомств «Мамба», а также думал о том, чтобы начать выпускать собственную водку под брендами *Hacker* и *Carder*, решив, что водка – «идеальный маркетинговый продукт». Проект в итоге не состоялся: «Большая часть времени проходила в погоне за женщинами».

В 2009 году Павловича вновь задержали. На этот раз суд приговорил его к 10 годам тюрьмы за воровство данных и сбыт поддельных банковских карточек. В это же время его разыскивали американские спецслужбы: Павловича считали участником группировки, совершившей⁵⁷ «крупнейшее хищение в истории США» – около 100 миллионов кредитных и дебетовых карт.

Америке Павловича не выдали. «Если бы его судили там, то ему вполне могло светить пожизненное заключение. Так что ему еще повезло, что арестовали его мы, а не они», – говорил в 2009 году начальник управления «К» КГБ Белоруссии Игорь Черненко. Во второй раз Павлович вышел из тюрьмы в 2015 году и запустил сайт *Carding Pro*, на котором выкладывает инструкции о взломах и другие статьи. Среди прочего Павлович опубликовал материал⁵⁸ о своих бизнес-планах – он собирается производить водку под брендами «Кардер» и «Хакер».

⁵⁷ ...Павловича считали участником группировки, совершившей «крупнейшее хищение в истории США»: Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U. S. Retailers, доступно на <https://www.justice.gov/archive/opa/pr/2008/August/08-ag-689.html>

⁵⁸ ...Среди прочего Павлович опубликовал материал о своих бизнес-планах: <https://carding.pro/ru/vodka-carder-i-hacker-byt/>

Глава 10

Авантюрист с Tesla

В начале августа 2010 года Владислав Хорохорин сидел⁵⁹ с коктейлем в зале ожидания аэропорта Ниццы. Он возвращался домой после отпуска в Монако. В этот момент в помещение забежали спецназовцы в масках и с автоматами.

Полиция в разных странах искала его еще с 2003 года, когда он называл себя *BadB* и был последним из руководителей форума *Carderplanet*, остававшимся на свободе.

Родители Хорохорина развелись, когда он был ребенком; детство он провел с матерью. Денег не хватало – в том числе на хороший интернет. Тогда Хорохорин взломал систему безопасности провайдера. Когда его вычислили, владельцы провайдера обратились не в полицию, а к бандитам, как это водилось в девяностых. Подросток отделался испугом, а вскоре они с матерью переехали в Израиль. Там он пошел служить в армию – и теперь взломал ее базу данных, чтобы чаще ходить в увольнение. Его снова вычислили – и снова без серьезных последствий. В те же годы Хорохорин познакомился с основателем *Carderplanet*, хакером *Script*, – попросил у того украденную карточку, чтобы заплатить за доступ к порносайту. Вскоре они оба были одними из самых успешных кардеров мира.

Знакомый Хорохорина называл его «беспринципным и азартным». «Он был авантюристом мирового масштаба. Его любимым выражением было „Красть – так миллион. Спать – так с королевой“, – рассказывал⁶⁰ его соратник по *Carderplanet*. – У него периодически совсем не было денег, потому что он постоянно их тратил на рулетку, выпивку, шлюх».

Он любил широкие жесты. Однажды Хорохорин и Павлович отправились в ночной клуб и «сняли» там всех стриптизерш. Хакер увлекался яхтами, дорогими автомобилями – незадолго до ареста он купил себе одну из первых *Tesla*. Деньги на это были: только взломав *Royal Bank of Scotland*, они с сообщниками заработали почти 10 миллионов долларов.

После того как *Carderplanet* закрыли, Хорохорин не прекратил заниматься кардингом, а вскоре начал использовать для продвижения своего бизнеса патриотические символы и образы Владимира Путина. В 2007 году на одном из хакерских форумов он разместил рекламное объявление, в котором рассказывал, что торгует базами украденных карт уже около восьми лет. Проиллюстрировано оно было рисунком, на котором Владимир Путин вручает медали хакерам; надпись гласила: «Мы ждем вас, чтобы бороться с империализмом США. Таким образом мы инвестируем средства США в российскую экономику и способствуем ее росту».

В 2007 году Хорохорин выпустил мультфильм в двух частях⁶¹, призывавший хакеров атаковать США. В них хакер в ушанке и тельняшке передает данные другому киберпреступнику, а тот обналчивает кредитные карты. После этого у бывшего госсекретаря США Кондолизы Райс выпадают глаза, а Джордж Буш-младший стреляет себе в голову, поскольку из Белого дома исчезли все деньги. В конце ролика нарисованный Путин награждает хакеров медалями в Кремле.

После задержания в аэропорту Ниццы Хорохорин провел два года во французском СИЗО, ожидая экстрадиции в США. Параллельно он распродал свои активы: дом в Израиле, стоивший около миллиона долларов, виллу во Франции за 3 миллиона евро. В Америке он

⁵⁹ ...Владислав Хорохорин сидел с коктейлем в зале ожидания: «Планета хакеров: как создавался крупнейший в мире форум киберпреступников», доступно на <https://www.forbes.ru/tekhnologii/tekhnika-i-biznes/332679-planeta-khakerov-kak-sozdavalsya-krupneishii-v-mire-forum-kiber>

⁶⁰ ...рассказывал его соратник по *Carderplanet*: «Как я украл миллион. Исповедь раскаявшегося кардера», Сергей Павлович (Питер, 2014)

⁶¹ ...В 2007 году Хорохорин выпустил мультфильм в двух частях: A BadB Welcome Cartoon, доступно на https://www.youtube.com/watch?v=O_hP-Mrhv7U, <https://www.youtube.com/watch?v=CEAMeVYqzSw>

заклучил сделку со следствием и выдал властям свою переписку с другими хакерами. Предлагали ему и дать показания против Романа Селезнева – он фигурировал на *Carderplanet* под ником *nСих*. Хорохорин утверждает, что отказался, заявив агентам ФБР: «Парни, мы в бане вместе гуляли. Какие показания? Идите на хуй».

Он получил 7 лет тюрьмы, а когда его досрочно освободили, то экстрадировали в Израиль. Российскому госканалу, приехавшему на интервью, хакер рассказал⁶², что, находясь в заключении, он нашел дыры в безопасности американских военных организаций. После чего заявил, что мечтает работать на российские спецслужбы. «Русских хакеров преследуют, это охота на ведьм, они создают врага себе, – заявил Хорохорин. – Я воровал, но не у людей, а у американского государства. У них надо воровать. Они воруют у всего мира». Через пару месяцев после выхода этого сюжета хакер начал путешествовать по России.

Сейчас Хорохорин выкладывает в своем фейсбуке ностальгические фотографии, сделанные до ареста, и философские размышления о жизни. «Мне 35 лет, – пишет он. – Я феерически талантливый идиот, говорящий на 8 языках и посмотревший мир. Иногда я хочу изменить мир. Но как я могу изменить мир, если я не могу изменить себя? Недавно, на другом конце света, я встретил людей, которых не видел очень давно. У этих людей красивые и умные жены, а у одного из них двое прекрасных детей, эти люди изменились, любят и любимы, и тех людей, которых помнил я – уже не узнать. Я же не изменился ничуть. Поэтому сегодня я повторяю, как мантру: „Господи, дай мне спокойствие принять то, чего я не могу изменить, дай мне мужество изменить то, что я могу изменить. И дай мне мудрость отличить одно от другого“».

А еще, как и многие российские хакеры, Хорохорин пишет стихи:

Но кто же Вы теперь?
Вы поколение Facebook и Lady Gaga,
Где исчисляя по количеству «лайков»
Оцениваете качества «френдов»
Или сливая злость на всё и вся вокруг, ты остаешься виртуальной, –
И рада;
За «авой» лишь следы ночей без снов,
Глаза опухшие от грустных мыслей и от слез,
За «ником» комплексов покров,
И что скрываешь ты в душе, моя отрада?
Что ищешь ты – там не найдешь ответа,
Ни помощи, ни дельного совета
И уж тем более того, о чем действительно мечтаешь:
Лишь мегабайты бреда и вопросы без ответа

⁶² ...хакер рассказал, что, находясь в заключении, он нашел «дыры» в безопасности американских военных организаций: «Эксклюзивное интервью бывшего хакера, отсидевшего за киберворовство в США», доступно на <https://www.youtube.com/watch?v=3V1bPSPN8jE>

Глава 11

Псих

Перед тем как американский суд вынес ему приговор, хакер Роман Селезнев написал от руки 11 страниц текста на английском языке. Вот⁶³ что он рассказал:

Я родился во Владивостоке 23 июля 1984 года. Мне было два года, когда родители развелись. Мы с мамой стали жить в комнате общей площадью 10 квадратных метров. Мы жили вместе с другими 4 семьями в эти трудные времена. Когда мне было 7 лет, моя мама купила квартиру у своего брата. Она не заплатила полную стоимость и должна была выплачивать деньги в течение года. Мы жили бедно, мне было больно смотреть, как маме приходится каждый день страдать. Она работала кассиром в одном из районных магазинов, и большую часть времени я был дома один. Так – самостоятельно – я начал изучать компьютерные технологии. У меня появились хорошие навыки. Когда я учился в школе, понял, что надо как-то помогать матери. В 16 лет я пошел в колледж, где изучал математику и информатику. Я хотел сделать жизнь матери лучше и хотел, чтобы у меня был отец, который бы мной гордился.

Я стал замечать, что мама часто выпивает. Иногда она делала это 7 дней подряд. Когда мне было 17, мама умерла. Я вернулся из школы и увидел, что она утонула в ванной. Она умерла из-за алкогольного отравления. На следующий день брат матери забрал из квартиры все ее украшения и хорошие вещи, а мне сказал уходить. Он сказал, что мама так и не заплатила ему за квартиру, хотя она платила.

После похорон я больше не появлялся в школе. Начал искать работу. Иногда мне помогала бабушка.

Я нашел работу в местном компьютерном клубе. Они предложили работать 24 часа каждый день. Платили примерно 5 долларов за день. Скоро я понял, что они просто используют меня. Я попытался найти работу в интернете. Это привело к тому, что все пошло под откос. Я занялся криминалом. Выбрал не тот путь – стал хакером, стал взламывать компьютеры, воровать кредитные карты и другую информацию, которую можно продать. Этих денег хватало. В 2007 году я нашел большую базу кредиток и продал ее за большие деньги. Я становился жадным.

В 2008 году я женился на Светлане. В следующем году у нас родилась прекрасная Ева. Они уехали в отпуск. Я остался дома. Тогда внезапно в квартиру ворвались грабители. Они избили меня, узнали мои пароли, забрали мои компьютеры. Они знали, чем я занимаюсь, и понимали, что их не будут ловить. Я не переживал из-за материальных потерь, но снова остался без денег. Но я знал, где их достать. Я боялся, что грабители могут вернуться, поэтому мы уехали для безопасности на Бали.

В середине 2010 года у меня были проблемы с работой, я не мог ничего найти. Поэтому снова занялся тем, что умел. В то же время у меня умерла бабушка – она была для меня настоящим родителем. Она не знала меня с плохой стороны – думала, я просто компьютерный специалист.

⁶³ ...Вот что он рассказал: https://www.nytimes.com/interactive/2017/04/21/technology/document-Seleznov-Letter.html?_r=0

(Следующие несколько предложений вымараны цензурой. Очевидно, речь идет про отца Селезнева Валерия – депутата Госдумы от ЛДПР. – *Прим. Авт.*) Он пригласил меня с семьей в Марокко. Мы приехали туда за день до того, как приедет отец. Мы решили позавтракать в отеле, но там сказали, что пустят, только если я надену пиджак. У меня пиджака не было, поэтому мы отправились в ближайшее кафе. Официант сказал, что нам придется подождать около получаса. Он добавил: «Это плохая идея». Но я не понял, что он имеет в виду.

Официант принес нам апельсиновый сок, в этот же момент шахид подорвал себя. Все кафе взорвалось⁶⁴, везде были мертвые люди и кровь. Взрывом повредило половину моей головы. Слава богу, моя жена не пострадала. (Как выяснится позже, 29 апреля 2011 года террористы оставили в кафе в Марракеше два портфеля со взрывчаткой и подорвали их с помощью мобильного телефона. Погибли 17 человек. Марокканские власти обвинили в теракте «Аль-Каиду», но организация брать на себя ответственность за взрыв отказалась. – *Прим. Авт.*)

У меня было плохое состояние, я думал, что умру прямо там. Я впал в кому. Моей жене врачи сказали, что не смогут ничего сделать для спасения моей жизни. Мне требовалась сложная операция на мозге, которую не умели делать.

Мой отец как-то смог организовать мою перевозку на самолете в Москву. Врачи сказали отцу и жене, что я скоро умру, а если произойдет чудо, я останусь «овощем на всю жизнь». Моя жена бросила меня и улетела в свой родной город – думала, я умру.

Я не был крещен. В России люди перед смертью должны креститься – иначе попадешь в ад. К больнице был приставлен священник, он быстро по просьбе моего отца крестил меня. Но чудо случилось. После двух недель я вышел из комы. Я не мог говорить и ходить, но понимал речь и мог взаимодействовать. Через 3 месяца я смог ходить, через год восстановил речь и понимание. С мая 2011 года по конец 2012 года я провел в различных больницах. У меня были операция за операцией – на мозге, на шее. В середине 2012 года мы с женой развелись. Она сказала, что оставила меня, потому что не хотела заботиться об «овоще». Она улетела в США с нашей дочерью, забрав все деньги.

В 2013 году я снова стал взламывать компьютеры и продавать кредитки. Моя жизнь была ужасной. Я ненавидел мужчину, которого видел в зеркале. Я спрашивал Бога: «Зачем ты спас меня?» Вскоре я встретил Анну, она стала моей невестой. Она ждет меня в России. Она любит меня и поддерживает уже три года. У нее есть дочь, которую я хочу удочерить.

В 2014 году я был арестован американскими властями. Когда я попал в тюрьму, у меня был плохой английский. Я был напуган, дезориентирован, не понимал и половины того, что происходит и что мне говорят люди. Мой адвокат дал мне ужасный совет бороться, потому что иначе я получу пожизненное. Сейчас мне понятно, что всем адвокатам, которые у меня были, нужна была только публичность.

⁶⁴ ...Все кафе взорвалось: «Раненного в Марокко сына депутата везут в Москву для срочной операции», <https://ria.ru/20110429/369552620.html>

Думаю, все это цена за то, что я делал всю жизнь. Я совершил много дурных поступков и беру на себя ответственность за них. Я не идеален. Теперь я отвечаю за это, как мужчина.

Я выслушал тех, кого ограбил. Мне хотелось плакать. Некоторые из них из-за меня потеряли бизнес.

Я боюсь наказания. Но понимаю, что я причинял не только финансовые проблемы. Из-за меня люди теряли ощущение безопасности – своей, своих денег, своей информации.

Я, Роман Селезнев, хочу сказать: «Я был неправ, я сожалею».

Надеюсь, что однажды выйду из тюрьмы. Я буду работать, чтобы выплатить деньги, потерянные моими жертвам. Буду работать честно. За годы в тюрьме я получил несколько образовательных дипломов, например по «ресторанному и отельному менеджменту».

До своего ареста я катился вниз по смертельно опасной дороге.

Спасибо большое.

Как указано в материалах⁶⁵ уголовного дела Селезнева, когда ему было 18 лет, он перешел от увлечения программированием к первым взломам. Их он совершал под именем *nСих* – «псих», если прочитать латинские буквы по-русски; этим именем он пользовался и при регистрации на кардерских форумах вроде *Carderplanet*. Поначалу он взламывал базы данных, чтобы воровать документы (имена, даты рождения, данные паспорта, номера соцобеспечения), потом стал красть номера кредитных карт и продавать базы данных другим кардерам.

Селезнев взламывал не отдельные счета, а процессинговые системы небольших предприятий в США, через которые проходили все финансовые операции этих бизнесов. Чаще других его целями становились небольшие закусочные в Вашингтоне и других городах США. В материалах уголовного дела упоминаются несколько пиццерий и булочных (всего около 3700 предприятий за все годы). Малый бизнес Селезнев выбирал из-за плохой защищенности: у таких предприятий не бывает своих департаментов киберзащиты, обычно они используют плохие пароли. Благодаря такому подходу к концу 2000-х Селезнев стал одним из самых успешных кардеров мира.

Спецслужбы США начали отслеживать деятельность Селезнева еще в 2005 году. В мае 2009 года агенты ФБР встретились в Москве с представителями ФСБ. Россияне представили американцам доказательства того, что за ником *nСих* скрывается житель Владивостока Роман Селезнев. Спустя месяц, в июне 2009 года, *nСих* сообщил на форуме, что уходит из бизнеса, после чего его профили на форумах были уничтожены. В США считают, что именно ФСБ передала Селезневу информацию, что им интересуются американские власти. Переписка хакера подтверждает, что он поддерживал связь с ФСБ. Одному из своих сообщников Селезнев объяснял, что у него есть защита от центра информационной безопасности ФСБ. Также он говорил, что ФСБ знает, кто он такой и чем занимается.

Мой источник, работа которого связана с кибербезопасностью, утверждает, что российских хакеров, взламывающих зарубежные системы, почти никогда не наказывают – чаще привлекают для работы на государство. Все российские хакеры знают присказку «Не работай по ги»; иными словами – нельзя, находясь в России, атаковать российские банки и компании.

Уничтожив свой прежний псевдоним, Селезнев скоро начал действовать как *Track2* и *Bulba*. Вскоре он вывел свой бизнес на новый уровень. В сентябре 2009 года он открыл интернет-магазин украденных карт. Выглядело это почти как *Amazon*: там можно было искать по категориям, выбирая между брендами карт или разными финансовыми организациями. Вла-

⁶⁵ ...Как указано в материалах уголовного дела Селезнева: <https://krebsonsecurity.com/wp-content/uploads/2014/07/Seleznnev-Indictment-CR11-0070RAJ-1.pdf>

сти США считают, что Селезнев пере придумал кардерский рынок: раньше украденные карты появлялись на отдельных ветках форумов, теперь процесс обмена ворованными данными был оптимизирован и автоматизирован. В апреле 2011 года в магазине Селезнева появилось около миллиона новых карт. Через пару недель после этого он улетел в Марокко и чуть не погиб при взрыве. Пока россиянин лечился, его сообщники продолжали работать над проектом, но в январе 2012 года сайт закрыли.

Выйдя из больницы, Селезнев взял себе ник *2Pac*. Он создал еще один интернет-магазин и запустил сайт, на котором можно было найти базовые инструкции о том, как красть банковские данные и использовать их. В верхней части сайта висело объявление на английском: «Тут я вам объясню, Как Зарабатывать Деньги. От \$ 500 до 5 000 и даже 50 000. Помните, это нелегальный путь! Весь процесс от начала до конца». В первый месяц работы сайта в июне 2014 года его посетили 3,5 тысячи человек.

Селезнев заработал очень много. Известно⁶⁶, что только через один из сервисов для переводов он получил около 18 миллионов долларов. Точный размер его состояния неизвестен: хакер получал деньги через биткойны, *WebMoney* и другие электронные кошельки. Он купил два дома на Бали, часто фотографировал пачки купюр и дорогие автомобили. У него есть фотография рядом со спортсменом на фоне собора Василия Блаженного – почти такая же, как у другого арестованного российского хакера Евгения Никулина⁶⁷ (его задержали в Праге в октябре 2016 года, обвинив во взломах *LinkedIn*, *Dropbox* и других сервисов; Никулин утверждал, что от него требовали признаться в том, что он взламывал почтовый ящик Хиллари Клинтон по приказу Владимира Путина).

Понимая, что его могут отслеживать агенты ФБР, Селезнев путешествовал аккуратно. Он выбирал страны, в которых нет экстрадиции в США, и покупал билеты в последний момент, чтобы мешать спецслужбам отслеживать свои перемещения.

В июле 2014 года он отправился на Мальдивские острова, где снял виллу за 1400 долларов в день. «Я взял себе самую дорогую виллу, у меня есть собственный слуга», – написал он одному из сообщников.

⁶⁶ ...Известно, что только через один из сервисов для переводов он получил около 18 миллионов долларов: там же

⁶⁷ ...как у другого арестованного российского хакера Евгения Никулина: <https://www.justice.gov/opa/press-release/file/904516/download>

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.