Станислав Макаров

Прекрасный, опасный, кибербезопасный мир

Всё, что важно знать детям и взрослым
о безопасности в интернете

Станислав Макаров

Прекрасный, опасный, кибербезопасный мир

Всё, что важно знать детям и взрослым
о безопасности в интернете

Москва
2022

Станислав Макаров
Прекрасный, опасный, кибербезопасный мир.
Всё, что важно знать детям и взрослым
о безопасности в интернете – М.: 2022. – 568 с.: ил.

Станислав Макаров родился в Волгограде, с 1983 года учился в МВТУ им. Баумана. С 2010 года занимается ИТ-журналистикой, автор множества публикаций и модератор конференций по широкому спектру тем из области цифровых технологий, в том числе по информационной безопасности. Зная о рисках информационной безопасности из реальной практики по внедрению ИТ-систем в крупных государственных и коммерческих организациях, решил написать об этом книгу для обычных людей – для детей и родителей, потому что технологии настолько проникли в нашу жизнь, что каждой семье впору об этом задумываться.

Содержание

Дорогие друзья,

Современный мир трудно представить без смартфонов, ноутбуков и интернета — мы живем в цифровом мире в той же мере, что и в реальном. Зарождавшийся как любопытная технологическая концепция, интернет постепенно стал полноценной вселенной, — и в ней, точно также, как в обычной жизни, можно найти друзей и единомышленников, а можно стать жертвой мошенников. Но это не значит, что нужно воспринимать интернет как угрозу. Как и в обычной жизни, достаточно просто знать базовые правила безопасного поведения.

Эта книга задумывалась как своего рода путеводитель, который даст конкретные практические советы о том, как избежать неприятностей в цифровом мире, распознать попытку обмана и выбрать правильную линию поведения. Интернет — это огромное пространство, которое может быть увлекательным, полезным и, главное, — безопасным. Только нужно помнить, что наша цифровая безопасность во многом зависит от нас самих.

Приятного чтения!

Игорь Ляпунов,
Генеральный директор компании «Ростелеком-Солар»
Вице-президент «Ростелеком» по информационной безопасности

Введение

Как бояться интернета правильно

На одной из площадей Берна уже почти пятьсот лет журчит фонтан с устрашающим названием «Киндлифресербрюнен» (Kindlifresserbrunnen), что означает «Пожиратель детей». Его вид полностью оправдывает название. На колонне в центре фонтана восседает ужасный великан-людоед, который засовывает в рот младенца, а еще несколько детишек в сумке, висящей у него на боку, ожидают своей незавидной участи.

Говорят, что статуя изображает Крампуса — злого персонажа альпийского фольклора, сопровождающего Святого Николая в ночь с 5 на 6 декабря[1]. В эту ночь Святой Николай раздает подарки послушным детям, а Крампус, со своей стороны, наказывает непослушных, причем самых отъявленных проказников он сажает в мешок и уносит в свою пещеру, чтобы съесть на рождественский ужин.

Не исключено, что детские экскурсии к этому фонтану имеют определенный педагогический эффект, но вряд ли существенный. Скорее всего, маленькие сорванцы пропускают назидательные страшилки мимо ушей.

В наши дни великаном, пожирающим детей, многие взрослые видят интернет. И так же, как экскурсоводы у фонтана пугают юных экскурсантов Крампусом, эти взрослые пытаются пугать своих детей опасностями, которые подкарауливают их в Сети. Но что может дать такое запугивание? Например, страх темноты, присущий человеку со времен палеолита, вполне рационален: наши далекие предки знали, что, если ночью выйдут в лес, их с высокой степенью вероятности съедят хищники. Но что случится, если выйти в интернет? Наши инстинкты в замешательстве — эволюция нас к такому не готовила.

---

1 *6 (19) декабря отмечается «Никола зимний» — день смерти Святого Николая Чудотворца, архиепископа Мир Ликийских.*

Нынешние дети с младенчества окружены различными гаджетами и абсолютно их не боятся, а вот многим взрослым современные технологии, наоборот, внушают мистический страх, отчего все их наставления в отношении интернета выглядят совершенно неубедительно.

Однако это ни в коем случае не означает, что ребенку не нужно рассказывать об угрозах в интернете, ведь число киберпреступлений, в том числе против детей, неуклонно растет год от года. Однако не стоит стращать детей неведомыми «неприятностями». Вы же понимаете, чем это может обернуться: отважный маленький исследователь тут же отправится их искать. И непременно найдет — на свою и вашу головы.

Чтобы этого не случилось, нам нужно научить детей «бояться интернета правильно» — то есть на основе знаний о том, как он работает и как могут действовать преступники, какие глупости можно натворить по собственному невежеству и как этого избежать. Придется стать в этом вопросе авторитетом для ребенка, иначе он вам не поверит. Или сделать так, чтобы рядом с ребенком был другой взрослый, сведущий в реалиях цифровой жизни. Но начальный уровень кибербезопасности вам придется освоить в любом случае — для вашего же блага.

Главное, что нужно понять и запомнить, — это то, что опасность представляют не технологии сами по себе, а люди, использующие их в нечистоплотных целях.

Главное, что нужно понять и запомнить, — это то, что опасность представляют не технологии сами по себе, а люди, использующие их в нечистоплотных целях.

В ходе технического прогресса меняются (совершенствуются) только инструменты преступников, тогда как их человеческая природа остается неизменной. Принято считать, что дети ориентируются в цифровом мире лучше большинства взрослых. И то, что дети тоже так считают, усугубляет проблему. На самом деле преимущества молодости в сфере кибербезопасности сводятся к нулю, потому что кибербезопасность — это больше про людей, чем про технологии. И жизненный опыт взрослого человека здесь придется как нельзя кстати.

Взрослому человеку лишь необходимо немного «подучить матчасть» — чтобы суметь обучить ребенка правилам безопасности в интернете также, как он его учил мыть руки перед едой или переходить дорогу на зеленый свет. Для этого придется вникнуть в вопросы кибербезопасности самому. Недаром же предупреждают в самолетах: «Сначала обеспечьте кислородной маской себя, потом — своего ребенка».

Наша книга поможет учителям и родителям повысить собственный уровень защищенности от киберугроз и сформировать у ребенка навыки безопасного поведения в интернете.

Важно! Эта книга — не пособие для учителей информатики. Эта книга вообще не про информатику как предмет. Эта книга — про жизнь и безопасность в цифровом мире для всех и каждого.

В следующих главах мы расскажем, какие меры стоит предпринять заранее, чтобы избежать этих ситуаций, и как действовать, когда инцидент уже произошел.

На вопрос «как правильно бояться интернета?» можно ответить так:

Не надо бояться самих технологий. Наоборот, нужно понимать принципы их действия и учиться грамотно ими пользоваться, чтобы уметь противостоять киберпреступникам. Тогда правила безопасности не будут казаться вам набором шаманских практик и приобретут вполне рациональный смысл.

Глава 1

Цифровые иммигранты и цифровые аборигены

В этой главе мы поговорим о том, чем отличается отношение к цифровым технологиям у взрослых и у молодого поколения, и о том, как учитывать эту разницу в восприятии, чтобы понимать друг друга. Также коротко перечислим возможные неприятности, случающиеся в цифровом мире, которые подробно рассмотрим в следующих главах.

Когда-то, давным-давно, когда нынешние учителя и родители школьников еще сами ходили в школу, никаких айфонов не было и в помине, и далеко не в каждом доме был интернет. Без повсеместного доступа к Всемирной паутине наше детство не слишком сильно отличалось от детства наших бабушек и дедушек, и даже пра-пра-бабушек и пра-пра-дедушек. За книгой нужно было идти в библиотеку, а за редкой книгой иной раз даже ездили в другой город. Чтобы пообщаться с друзьями, мы ходили в гости, а услышав что-то важное по радио, немедленно записывали это, чтобы не забыть. Расплачивались только наличными, а письма писали на бумаге, запечатывали в конверты и опускали их в почтовый ящик.

Мы застали уникальный период в истории цивилизации, когда за короткое время изменилось буквально все. Отсчет новой эры начался с появления айфона в 2007 году. Простота и естественность его интерфейса впервые позволили маленьким детям пользоваться компьютером самостоятельно — без помощи взрослых. А то, что со смартфона можно было еще и позвонить, стало рассматриваться подрастающим поколением лишь в качестве дополнительного бонуса. Телефонные звонки для молодежи — не самая главная функция.

Смартфон стал ключом ко всему, что можно найти в интернете, — а найти в нем можно все. Как явление интернет сравним разве что с изобретением книгопечатания в XV веке, когда каждому образованному человеку стали доступны почти все сокровища, ранее скрытые в монастырских библиотеках.

По средневековым меркам распространение печатных книг произошло практически мгновенно, хотя в действительно-

сти процесс занял довольно продолжительное время. Иоганн Гутенберг изобрел метод книгопечатания около 1450 года. Через 50 лет в Германии работало свыше 50 типографий, в которых трудились 200 печатников. А во всей Европе к тому моменту насчитывалось до 1000 печатников, которые до конца XV века в целом издали около 30 тысяч книг — так называемых инкунабул. Первая же газета в привычном для нас формате появилась лишь в XVII веке. Таким образом, технология книгопечатания достигла зрелости через 150 лет после своего изобретения (Википедия).

С момента изобретения телефона в 1876 году до массовой телефонизации в XX веке прошло почти сто лет, телевизоры пришли в наши дома в течение полувека. А затем все неимоверно ускорилось. Мобильные телефоны прошли путь от символа высокого статуса до ширпотреба лет за двадцать, доступ в интернет стал массовым явлением в течение десятка лет, iPhone завоевал сердце массового потребителя за год с небольшим, а iPad стал мегапопулярным всего за несколько месяцев. Теперь каждая новинка распространяется по планете со скоростью вируса гриппа, и есть все основания полагать, что так будет продолжаться и впредь.

У наших предков было время приспособиться к переменам, потому что изменения происходили медленно — на протяжении нескольких поколений. Нас же накрыло цифровой волной внезапно. Слова, которые еще совсем недавно могли вызвать, по меньшей мере, недоумение — например, «позвольте я вас сфотографирую на телефон», сегодня всеми воспринимаются как должное. Новые технологии распространяются настолько быстро, что никакие учебники и образовательные программы за ними не поспевают, и нам приходиться учиться на ходу.

«Нужно беспокоиться, когда что-то развивается слишком быстро. Не потому, что рост — это плохо, а потому, что прежние наработки не сохраняются. Если эволюция будет слишком быстрой, то некоторые виды вымрут». Эти слова принадлежат Нассиму Николасу Талебу, почетному профессору Нью-Йоркского университета в области управления рисками.

Да, мы более или менее приспособились к новому миру, но мы все равно в нем чужие. Мы — цифровые иммигранты[1], которые перебрались сюда из своего «теплого лампового» мира. Как известно, базовые навыки восприятия формируются в раннем возрасте, а в нашем детстве гаджетов не было и в помине. Поэтому, как бы мы ни старались стать «цифровыми», нам все равно не достичь такой легкости в пользовании гаджетами, какую мы наблюдаем у детей.

Современные дети — цифровые аборигены, родившиеся со смартфоном в руке. Они не представляют, зачем ехать в кассу, чтобы купить билет на поезд или самолет. Они не верят авторитетам и ставят под сомнение любые ваши слова. А пока вы напрягаете память, чтобы вспомнить дату Ледового побоища (1242 год, если кто забыл) или количество хромосом у морского ежа (на всякий случай, их 42), они успевают посмотреть все ответы в Сети и приготовиться поймать вас на любой неточности. Иногда это раздражает, иногда удивляет — но это совершенно другой способ познания мира, к которому нам трудно привыкнуть.

---

1 Термины «цифровые аборигены» и «цифровые иммигранты» были введены организацией Electronic Frontier Foundation в 1996 году в рамках Декларации независимости киберпространства (https://www.eff.org/cyberspace-independence) и популяризированы консультантом по образованию Марком Пренски в статье «Аборигены и иммигранты цифрового мира».
Digital Natives, Digital Immigrants. // On The Horizon (MCB University Press, Vol. 9 № 5, октябрь 2001 г.) © 2001 Marc Prensky.

В этом свете вечная проблема отцов и детей заиграла миллионами цифровых оттенков. Герои Тургенева спорили о путях развития страны, о материализме и идеализме, о знании науки, понимании искусства и отношении к народу. Но жизнь их от поколения к поколению мало менялась: они учились по одним и тем же учебникам, читали газеты, ездили на лошадях. К сегодняшнему же дню конфликт поколений изрядно помолодел, усложнился и сместился практически на уровень начальных классов. Несомненно, первоклашек еще не волнуют высокие материи, но зато у них уже есть собственное представление о том, как добывать информацию. А школа все еще пытается научить их методам, которые использовались в XIX веке.

> *«Школьники и студенты стали совсем другими, — писал Марк Пренски в 2001 году. — Сегодняшние учащиеся — больше не те люди, для которых была создана наша система образования. Мы родились до цифровой эпохи, но впоследствии были очарованы новым миром и многое в нем приняли. Тем не менее, по сравнению со школьниками мы навсегда останемся «цифровыми иммигрантами».*

Может быть, автор излишне драматизирует? Конечно, тонким перышком в тетрадь уже никто не пишет — мы давно перешли на авторучки, но все остальное-то не изменилось: про глагол и про тире, и про дождик на дворе, к четырем прибавить два — и так далее. Да, но где же про интернет и про смартфон, про YouTube и про Питон[1]? Сайты нужные любить, на плохие не ходить? Крепко-накрепко дружить, но внимательными быть — мало ли кто там? Школа считает цифровые

---

1 *Python — язык программирования, который одним из первых рекомендуют для изучения детям. Правильно произносится «пайтон», но в русском языке прижилось произношение «питон».*

технологии чем-то очень сложным, что следует изучать в рамках отдельного предмета, потому что для большинства учителей цифровые технологии действительно сложны. И вроде бы учителей они не касаются напрямую. Про острова и города мы говорим на географии, а в Google Earth ученики как-нибудь сами разберутся. В результате цифровая жизнь детей фактически изгоняется из школы, и они оказываются с ней один на один — вместе со всеми опасностями, которые существуют в интернете.

Марк Пренски обратил внимание на эту проблему еще двадцать лет назад. Но и сегодня нельзя сказать, что за прошедшие годы ситуация кардинально изменилась:

> *«Единственной проблемой становления нового формата образования является то, что наши преподаватели — цифровые иммигранты. Они говорят на архаичном языке доцифровой эпохи, изо всех сил старясь учить поколение, говорящее на совершенно новом языке. Цифровые аборигены часто воспринимают школу именно так: к местным жителям пришел невразумительный иностранец с сильным акцентом и собирается их чему-то научить. Вот аборигены часто и не понимают, что им говорит иммигрант».*

Наверное, можно было бы воспользоваться идеей Льва Толстого, который объединил в своей «Азбуке» все, что было нужно для обучения детей начальной грамотности — чтение, письмо и арифметику. Первое издание «Азбуки» вышло в 1872 году. А через три года доработанный вариант под названием «Новая Азбука» был рекомендован Министерством народного просве-

щения в качестве учебника для народных школ России. Еще при жизни автора пособие было переиздано 28 раз. Правда, под давлением критиков из новой редакции была исключена арифметика — во времена Толстого школа тоже была очень консервативной и отвергла его новаторскую идею.

Если бы Лев Николаевич писал «Азбуку» в наши дни, наверняка включил бы в нее и азы цифровой грамотности, ведь он задумывал свой учебник как минимальный набор знаний, необходимый человеку для нормального существования в современном ему обществе. И, наверное, точно также нашлись бы критики, требующие строго научного подхода в ущерб цельности. Что, в общем-то, мы и имеем.

Цифровизация школы, вне всякого сомнения, неизбежна. Но очевидно, что это случится еще нескоро. Поэтому пока в вопросах кибербезопасности нужно полагаться на свои силы и строить свою собственную цифровую крепость.

Родители и дети в цифровую эпоху

В начале нулевых годов на волне всеобщей эйфории от взрывного распространения интернета бытовало мнение, что дети — цифровые аборигены — обладают некими врожденными навыками и способны освоить цифровые технологии без помощи взрослых. Как и следовало ожидать, это была иллюзия. То, что дети безвылазно находятся в онлайне, еще не означает, что у них есть реальное представление о том, как применять цифровые инструменты наилучшим образом.

То, что дети безвылазно находятся в онлайне, еще не означает, что у них есть реальное представление о том, как применять цифровые инструменты наилучшим образом.

В большинстве своем они пользуются интернетом для решения самых примитивных задач — для общения в социальных сетях, просмотра видео и многого другого. Чуда не произошло. Одного только рождения в цифровую эпоху оказалось недостаточно для овладения ее технологиями, и мы встали перед фактом, что цифровых аборигенов тоже необходимо учить.

Строго говоря, цифровые аборигены и иммигранты — всего лишь красивая метафора, а не научная теория. К тому же, как нетрудно догадаться, в силу естественных причин существующее положение вещей не будет сохраняться вечно. После того, как первые цифровые аборигены повзрослеют и обзаведутся собственными детьми (что уже происходит), непонимание между поколениями уменьшится. А когда они станут бабушками и дедушками, то круг и вовсе замкнется — цифровых иммигрантов не останется.

Означает ли это, что проблема компьютерной грамотности и цифровой гигиены решится сама собой? Вовсе нет. Как и во всех других аспектах воспитания, в том, что касается «цифры», ключевую роль играет семья. Какой пример показывают родители, такую модель и воспроизводят дети, — яблоко от яблони недалеко падает.

Какой пример показывают родители, такую модель и воспроизводят дети, — яблоко от яблони недалеко падает.

Взрослые — цифровые иммигранты — адаптировались к внезапным изменениям очень по-разному. Одни были творцами и активными участниками цифровой революции. Другие отнеслись к происходящему с пассивным принятием, без глубокого интереса, и стали простыми потребителями. Нашлись и неолуддиты, которые отвергают технические новинки и видят в распространении цифровых технологий только зло. Все они транслировали свои воззрения детям, а их дети — своим детям и так далее.

По данным исследования Александры Самюэль, проведенного в 2015 году среди десяти тысяч американских семей[1], три указанные выше категории родителей оказались примерно равными по численности. И важно отметить, что они отличаются не только в вопросе отношения к технологиям, но также и в вопросах ограничения детей в пользовании этими технологиями или, наоборот, помощи в их освоении.

Первую категорию можно назвать **наставники (digital mentors)**. Они активно помогают отпрыскам осваивать компьютер и смартфон, записывают их на занятия по программированию и робототехнике, беседуют о правилах ответственного и безопасного поведения в киберпространстве. В результате их дети, которых Александра Самюэль называет **цифровыми наследниками (digital heirs)**, со школьной скамьи умеют создавать сайты, мон-

---

1 *Александра Самуэль — технический стратег (tech strategist), исследователь, писатель и докладчик. Автор книги «Работай умнее с социальными сетями» («Work Smarter with Social Media», Harvard Business Review Press, 2015), регулярно пишет для The Wall Street Journal и The Harvard Business Review, а также выступает в качестве обозревателя по цифровым технологиям для JSTOR Daily.*
Alexandra Samuel. Parents: Reject Technology Shame. // The Atlantic, 4 ноября 2105.

тировать видео, писать программы, быстро находить нужный контент и адекватно вести себя в социальных сетях. Иными словами, эти детишки оказываются вполне подготовленными, чтобы в будущем занять хорошие рабочие места в цифровой экономике.

Вторую категорию составляют **потакающие родители (digital enablers)**. Эти папы и мамы пускают цифровое воспитание своих детей на самотек. Они позволяют детишкам сколько угодно времени проводить за экранами гаджетов, но при этом нисколько им не помогают в освоении этих устройств, поскольку сами не слишком в них разбираются. Поэтому их детей называют **цифровыми сиротами (digital orphans)**. Несмотря на отсутствие контакта с родителями, они могут вырасти достаточно подкованными в техническом плане, но, скорее всего, будут лишены коммуникативных навыков и знаний, необходимых для того, чтобы использовать онлайн-инструменты для решения реальных жизненных проблем.

Третья категория — **запрещающие родители (digital limiters)**. А их дети — **цифровые изгнанники (digital exiles)**. Из опасения, что цифровые устройства могут причинить ребенку вред, запрещающие родители жестко ограничивают детей в пользовании гаджетами, а некоторые сторонники ограничений доходят до крайности — вообще не позволяют детям пользоваться гаджетами до достижения подросткового возраста. И это чревато, ведь подростки в гораздо меньшей степени склонны слушать советы старших, и как только им представится возможность, они могут уйти в онлайн-жизнь с головой, пренебрегая опасностями этой жизни. Возможен и такой вариант, что они по примеру родителей станут добровольными изгоями в цифровом мире — и он тоже

грозит неприятностями. Современное общество еще может понять, если люди старшего возраста не разбираются в компьютерах, но когда в них не разбирается молодой человек, он рискует элементарно остаться без работы.

Исследование, которое в 2015 году провели EU Kids Online и Лондонская школа экономики (LSE)[1], выявило пять основных видов взаимодействия родителей с детьми в возрасте от 9 до 16 лет:

- *активное посредничество: обмен и обсуждение онлайн-деятельности;*
- *обеспечение безопасности: консультирование и руководство по управлению рисками;*
- *ограничения: правила и запреты;*
- *технический подход: использование фильтров, родительский контроль;*
- *мониторинг: проверка компьютера, социальных сетей, телефонов и прочего после использования.*

Также исследование обнаружило зависимость между моделью поведения родителей и их социально-экономическим статусом. Например, в семьях с низким доходом и низ-

1 *Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S. and Lagae, K. (2015) How parents of young children manage digital devices at home: The role of income, education and parental style. London: EU Kids Online, LSE.*

ким образовательным уровнем дети сравнительно хорошо разбираются в цифровых устройствах. Но очень заметно, что они гораздо лучше владеют технологиями, чем родители. Особенно отчетливо поколенческий разрыв проявляется в семьях иммигрантов (обычных — нецифровых). Как правило, главы этих семейств ограничивают детей в пользовании гаджетами, хотя среди них встречаются и те, кто достаточно амбивалентен в этом вопросе.

В более образованных семьях, но также имеющих низкий доход (часто это неполные семьи), родители в вопросах цифровых технологий скорее взаимодействуют с детьми, нежели что-то им запрещают. Но все же и они нередко прибегают к ограничениям.

Что же касается семей, где высоки и доходы, и образовательный уровень, то в них принято рассматривать права и возможности ребенка с позиций этики. Родители, само собой, используют различные способы контроля за цифровой жизнью своих чад. Но, как правило, стараются обходиться без строгих запретов. А чтобы отвлечь детей от гаджетов, для них, например, организовывают различные офлайн-активности.

Суммируя, можно сделать вывод, что уровень образования родителей — определяющий фактор в выборе ими модели регулирования интернет-активности своих детей.

Вместе с тем стоит обратить внимание, что низкий уровень доходов не является барьером для вхождения в цифровой мир. Это значит, что дети из небогатых семей потенциально имеют шансы стать

цифровыми профессионалами. Они вполне могут построить карьеру, если школа даст им недостающие навыки рационального и ответственного использования технологий, которые они не смогли перенять от родителей. В противном случае они рискуют остаться всего лишь потребителями примитивного контента или перейдут на темную сторону: пополнят ряды киберпреступников, если «прокачают» свой технический уровень.

Необязательно быть мишенью, чтобы стать жертвой

«У меня нет миллионов в швейцарском банке, заводов и яхт, в политику я не лезу. Разве я интересен киберпреступникам?»

На первый взгляд может показаться, что среднестатистическому гражданину действительно не о чем беспокоиться, ведь преступная деятельность требует организованных усилий, вовлечения большого числа высококвалифицированных специалистов, а все это обходится весьма дорого. Вспомните любой добротный фильм про ограбление — хотя бы историю про друзей Оушена. Сколько сил и энергии тратят герои, чтобы завладеть сокровищами! Никто же специально не планирует ограбление квартиры простого служащего, живущего на скромную зарплату.

Персонально вы, скорее всего, неинтересны жуликам, и в аналоговом мире крайне маловероятно, что именно вас выберут мишенью. Но цифровой мир устроен не так. Здесь можно автоматизировать не только полезные процессы — скажем, запись

ребенка в школу или на прием к врачу. Ограбление тоже можно автоматизировать. Ваши деньги и персональные данные украдут вместе с деньгами и данными миллионов других пользователей, «за компанию».

Способов почти незаметного воровства денег, а также причинения другого вреда, существует довольно много, и мы в этой книге о них еще поговорим. Но сначала вам стоит уяснить одну вещь: сегодня скромные доходы не спасают от внимания криминальных структур. Поэтому о своей безопасности, равно как и о безопасности своих близких, нужно заботиться вне зависимости от уровня ваших доходов.

Пожалуй, наибольшее число неприятностей, в которые попадают обычные граждане, включая детей, связаны с неперсонализированными атаками, когда кибержулики ловят широким неводом, загребая любую мелкую рыбешку, какая встречается им на пути. Чтобы миновать их сети, необходимо стать чуть более умной рыбой. И это вполне возможно — просто нужно научиться соблюдать хотя бы элементарные правила цифровой гигиены.

Под прицелом

Совершенно иная ситуация, когда именно вы — или, того хуже, ваш ребенок — по каким-то причинам становитесь чьей-то мишенью. Чем скорее вы поймете, что находитесь под прицелом, тем лучше.

Чем скорее вы поймете, что находитесь под прицелом, тем лучше.

Ведь полагаться на пассивные методы защиты из области цифровой гигиены в этом случае уже бесполезно — нужно переходить к активным действиям, потому что вам грозят серьезные опасности. Например, это могут быть:

- травля в соцсетях;
- попытки вербовки в преступные организации;
- вовлечение в деструктивные сообщества;
- вымогательство, шантаж или преступления на сексуальной почве.

Экономические мотивы тоже могут присутствовать, но по сравнению с вышеперечисленным попытка обчистить ваши карманы выглядит сравнительно мелкой проблемой. А вот если ваш ребенок ввязался в переписку с маньяком (они, к сожалению, существуют не только в кино), то вы рискуете узнать об этом, когда будет уже поздно.

Вашим противником может оказаться как профессионал, который специально подготовлен к ведению преступной деятельности в киберпространстве, так и обычный преступник, который выискивает свои жертвы через интернет. В обоих случаях вам неизвестна его личность и истинное местонахождение. При этом первый умеет ловко заметать цифровые следы, что затрудняет его поиск и поимку, а второй бывает достаточно наивен в способах цифровой маскировки, вследствие чего с большей вероятностью может быть обнаружен и задержан. Тем не менее, уровень опасности в обоих случаях очень высок.

Рассказывает Константин Игнатьев, Лаборатория Касперского:

«Пятнадцатилетняя старшеклассница из Барнаула познакомилась в соцсети с мужчиной 30 с лишним лет. У них завязался диалог. Потом они встретились в реальности, он за ней ухаживал и, в конце концов, уговорил вступить с ним в половую связь. Более того, снял этот процесс на видео, сделал множество фотоснимков девочки в обнаженном виде, а затем начал ее шантажировать. Две недели она скрывала произошедшее от родителей, но потом все-таки призналась. Родители обратились в полицию, преступника нашли и осудили. Правда, срок он получил условный — 5 лет. Через какое-то время семья девочки переехала в Москву — они это давно планировали, а происшествие только ускорило переезд.

Но на этом история не закончилась. Мужчина снова попытался выйти с девочкой на связь и для этого создал в соцсети ВКонтакте ее фейковый аккаунт с фотографиями. Староста класса, в котором училась девочка, нашел этот якобы ее аккаунт и добавил его в группу класса. В результате злоумышленник узнал, где она учится, и снова начал ей угрожать. Но, к счастью, у него ничего не получилось.

Благодаря тому, что героиня этой истории тесно и доверительно общалась с родителями, которые ее всячески поддерживали, она прошла это испытание, хотя и не без травм, но все же сохранив здравый рассудок. Я общался с ней и вполне могу это засвидетельствовать.

Но бывают и трагедии. Встречаются авторитарные родители, особенно отцы, которые говорят: «Интернет — это помойка, я это запрещаю — и все!» В итоге они теряют контакт с ребенком. А если ребенок перестает доверительно общаться с родителями, это всегда не к добру.

Так случилось с девочкой, которой отец строго-настрого запрещал пользоваться социальными сетями. Но какой же подросток сегодня не «зависает» в соцсетях! Поскольку девочке приходилось скрывать это от родителей, она завела несколько аккаунтов со смартфонов друзей и через один из них познакомилась с мужчиной. Как потом оказалось, он планировал не просто шантаж, а изнасилование и убийство. Трагедии можно было бы избежать, расскажи она все родителям. Но несчастный ребенок боялся признаться самым близким людям, что тайком пользуется соцсетями...

В жизни случается, что угроза исходит от известных вам людей, действующих из мстительных побуждений или по каким-то другим личным мотивам. По личным мотивам, как правило, организовывается и травля в интернете (кибербуллинг). Чаще всего агрессоры — это кто-то из ближайшего окружения, например, одноклассники. Как от них скроешься? Они же все равно достанут в реальной жизни. Выход один: организовывать поддержку со стороны родителей и друзей, объяснять, что не нужно реагировать на агрессивные выпады. Делать это необходимо: кибертравля часто приводит к самоповреждениям и суицидам, потому что дети еще не способны выходить из сложных ситуаций самостоятельно, а рассказывать о них родителям стесняются или боятся».

Примечательно, кстати, что кибербуллинг в наибольшей степени распространен в детской и подростковой среде, а к старшим классам практически сходит на нет. Причина проста: когда дети становятся старше, они начинают понимать, что за свои действия им придется отвечать.

Когда некого винить, кроме себя

Третья группа киберпреступлений — те, которые становятся возможны вследствие неразумных или неосторожных действий пользователей. То есть когда жертва сама преподносит злоумышленникам свои данные, ключи и пароли. Типичный пример — школьные компьютеры, на которых дети регулярно оставляют открытые сессии в соцсетях или электронной почте, а в браузере — логины и пароли. Стоит ли потом удивляться, что кто-то украл их данные?

Можно вспомнить и неразумные посты в соцсетях, которые оборачиваются условными, а иногда и реальными сроками — просто потому, что ребенку не рассказали об ответственности за его публикации и о том, как работает правоохранительная система.

Если родители старательно внушали юному пользователю мысль, что честному человеку нечего скрывать, и не научили его заботиться о своих секретах, тогда этот пользователь, выйдя на работу, будет так же беззаботно относиться и к секретам своей компании, из-за чего может нажить себе крупные неприятности.

Короче говоря, цифровой мир дает множество возможностей, чтобы наделать глупостей.

Цифровой мир дает множество возможностей, чтобы наделать глупостей.

И если каждую минуту не отдавать себе отчет в том, что и зачем ты делаешь, то неприятные последствия фактически гарантированы. Зашел в интернет через публичный wi-fi, ввел логин и пароль от почты, на которую завязаны регистрации на всех сервисах, — и только успевай расхлебывать. Поленился сменить пароль по умолчанию на роутере — под твоим IP-адресом кто-то ограбил банк.

Понятное дело, стопроцентной защиты от всех рисков не существует, но можно хотя бы свести их к минимуму. И для этого даже не нужны какие-то специальные средства. Нужно лишь приучить себя соблюдать простые правила, и, разумеется, приучить к этому детей — чем раньше, тем лучше.

Ребенок как угроза

Обычно родители озабочены тем, как защитить ребенка от нехороших людей и недетского контента в Сети, но редко думают, как обезопасить самих себя от своего дитяти. Помните эту песенку?

В каждом маленьком ребенке,
И мальчишке, и девчонке,
Есть по двести грамм взрывчатки
Или даже полкило!

Должен он бежать и прыгать,
Все хватать, ногами дрыгать,

А иначе он взорвется, трах-бабах!
И нет его!

Каждый новенький ребенок
Вылезает из пеленок
И теряется повсюду,
И находится везде!

Он всегда куда-то мчится,
Он ужасно огорчится,
Если что-нибудь на свете
Вдруг случится без него![1]

Все именно так! А еще дети страшно любят хватать разные гаджеты, нажимать на все кнопки, удалять фотографии, отправлять странные сообщения вашим знакомым, устанавливать приложения-игрушки в промышленных количествах, находить и открывать сайты 18+++ (которые останутся в вашей истории просмотров), кликать на рекламные ссылки, цепляя кучу вирусов, и вообще творить бог знает что.

Ребенок — пользователь, который очень высоко мотивирован на достижение своих личных целей (играть или смотреть мультики), и ради этого готов пренебречь любыми правилами. С точки зрения специалиста по информационной безопасности, это — портрет типичного нарушителя. Поэтому следует предпринять меры, чтобы активность ребенка не привела к ущербу.

О чем нам говорят сказки? О том, что дети постоянно нарушают правила и попадают в разные нехорошие ситуации. Козлята

1 *Песня на стихи Григория Остера из мультфильма «Осторожно, обезьянки!» (1987 год).*

забыли все, что им говорила мама-коза, и открыли дверь волку. Красная Шапочка не послушалась маму и тоже угодила в лапы к волку, да еще вместе с бабушкой. Старшая сестра заигралась, и гуси-лебеди утащили ее братика. Буратино разговорился с незнакомцами и выдал им все персональные данные. В общем, полагаться на разумное поведение маленького пользователя не стоит.

В 2018 году организация EU Kids Online[1] при поддержке Министерства юстиции и общественной безопасности Норвегии провела исследование среди детей и подростков в возрасте 9-15 лет, которое показало, что существует большой разрыв между тем, что они знают об основных концепциях интернета, и их способностью применять эти знания на практике. Также исследователи отмечают, что детям не хватает целостного понимания рисков и возможностей, которые могут быть связаны с их действиями.

То есть детишки кое-что знают, но далеко не все умеют. По-хорошему, таким неопытным путешественникам по цифровому миру стоило бы давать специальный значок, наподобие знака «У» для водителей-новичков, чтобы другие участники движения были с ними поосторожнее. Но таких знаков не существует. Поэтому, прежде чем подпустить ребенка к своим цифровым устройствам, необходимо обезопасить свои цифровые активы.

Прежде чем подпустить ребенка к своим цифровым устройствам, обезопасьте свои цифровые активы.

1 *Ní Bhroin, N. and Rehder, M. M. (2018). Digital Natives or Naïve Experts? Exploring how Norwegian children (aged 9-15) understand the Internet. EU Kids Online.*

Понятно, что лучший выход из этой ситуации — покупка ребенку собственного гаджета. Но не всякий семейный бюджет это выдержит, особенно если семья — многодетная. С другой стороны, даже если у детки будет свой телефон, это еще не гарантия того, что он не заинтересуется вашим. Вдруг у вашего экран побольше и поярче. Так что расслабляться нельзя. Ни в коем случае не привязывайте к детскому телефону ни свою банковскую карту, ни даже карту ребенка, если таковая у него уже имеется, и настройте резервное копирование в облако: если юный исследователь цифровых миров все-таки угробит ваш девайс, вам будет проще восстановить данные.

Как обезопасить свои гаджеты от любимых детишек

- *Установите на телефон и компьютер пароль или пин-код. Не стоит считать это признаком недоверия к ребенку. Это самая обычная мера безопасности — как мы ставим заглушки на розетки и блокираторы на ящики и дверцы шкафов, когда в доме есть маленькие дети. Теоретически можно попытаться договориться с детьми, чтобы они не брали без спроса ваш телефон, но искушение бывает столь велико, что лучше подстраховаться.*

- *Не привязывайте к телефону (точнее, к учетной записи Apple ID или Google для обладателей Android-телефонов) свою основную банковскую карту. Это в принципе полезно, вне зависимости от наличия детей. Если у детей есть свои телефоны, то тем более. Лучше всего будет выпустить виртуальную карту (обычно это бесплатно) и положить на нее небольшую сумму — тогда ваш основной счет будет в большей безопасности. Если вы привыкли платить с помощью телефона, то есть пользуетесь сервисами Apple Pay*

или Google Pay, то к ним придется привязать настоящую карту для покупок.

- *Настройте копирование в облако фотографий, контактов, заметок и другой ценной информации. Помните: телефон, попавший в детские ручки, может вернуться к вам совсем не таким, каким вы его знали раньше.*

- *Установите приложение-контейнер. Это специальное приложение, которое из одного телефона «делает» два — как на компьютере могут быть отдельные профили для разных пользователей. Обычно это применяется для разделения рабочего и личного пространств, но для разделения взрослого и детского тоже подойдет. На телефонах Samsung это приложение называется Secure Folder (раньше это был Knox), есть аналоги и у других производителей. Secure Folder позволяет быстро и легко защищать любые папки на смартфонах Android. С этим приложением вы сможете создать пин-код или пароль, чтобы защитить файлы от любопытных глаз, перемещать их в защищенную папку и из нее. В эту папку можно поместить и приложения — например, для социальных сетей, сайтов знакомств и другие, доступ к которым вы хотите оградить от посторонних.*

Почему детей так тянет к смартфонам? Цифровой мир дает ребенку неограниченный простор для исследования — гораздо больший, чем мир реальный, который для него на самом деле ограничен пределами квартиры, двора, школы и нескольких других мест, куда его водят на занятия. Попасть в какие-то действительно новые места ребенку удается редко — только во время семейных походов в развлекательный центр по выходным, поез-

док в отпуск или к бабушке на дачу. Большую же часть времени перед глазами ребенка проплывают одни и те же, уже знакомые картины. Поэтому неудивительно, что виртуальные миры обладают для него притягательной силой, — там в полной мере реализуется его природная функция все изучать и пробовать, причем при почти полном отсутствии риска.

Само собой разумеется, ребенок не думает об угрозах, его ведут азарт и любопытство. И, увидев кнопку с призывной надписью или картинкой, он непременно на нее нажмет, сколько бы ему не рассказывали об опасных ссылках, вирусах, хакерах и мнимых виртуальных друзьях.

Случаи из жизни

— Хватило всего нескольких секунд в детских руках, чтобы айфон моего знакомого намертво завис. В итоге знакомому пришлось дожидаться, когда сядет аккумулятор, чтобы затем попытаться оживить смартфон.

— Раньше у меня на телефоне было приложение «Сити-Мобил». С его помощью ребенок несколько раз вызвал такси. Для этого всего-то и нужно — два нажатия. И всякий раз такси приезжало. В конце концов приложение пришлось удалить.

— Когда моему сыну было пять лет, он однажды накупил кучу платных игр в AppStore — за один вечер потратил около тысячи долларов. Действовал он следующим образом. Покупал сразу несколько игр, но если какие-то из них казались ему неинтересными, тут же удалял, а вместо них заказывал новые. Я обратился в Apple, описал ситуацию, и они вернули мне деньги.

Жизненные ситуации

«Если раз за разом пытаться потрогать раскаленную докрасна кочергу, то, в конце концов, обожжешься; если посильнее полоснуть по пальцу ножом, из пальца обычно идет кровь; если разом осушить пузырек с наклейкой «Яд!», рано или поздно почти наверняка почувствуешь недомогание», — рассудительно говорила Алиса. В наши дни она наверняка продолжила бы список: если заходить на все сайты подряд, непременно подцепишь вирус; если установить слишком простой пароль, его, весьма вероятно, взломают; если твой друг в соцсети просит у тебя фото кредитной карточки твоей мамы, это на 100% мошенник.

Давайте рассмотрим наиболее часто встречающиеся ситуации, связанные с нарушением кибербезопасности.

Что может случиться:

- Потерялся пароль;
- Взломали аккаунт;
- Пропали файлы или фотографии;
- Подцепил вирус;
- Украли (потерял) телефон;
- Нашел флешку;
- Надоела навязчивая реклама;

- Ребенок смотрит взрослый контент;
- Украли деньги с карты;
- Появились лишние подписки на сервисы;
- Утекли персональные данные;
- Кто-то угрожает ребенку или вам;
- Ребенок решил стать хакером;
- Похоже, у ребенка развилась зависимость от интернета;
- В Сеть попали фотографии, которые вы не хотели бы публиковать.

Наверное, список можно дополнить. Часть этих неприятностей будет связана с угрозами непосредственно вашему ребенку или вам, другая может нанести урон вашим цифровым ценностям. Об этом — в нашей следующей главе.

Контрольные вопросы

1. Кто такие цифровые аборигены и цифровые иммигранты?
2. К какой категории вы себя относите?
3. Может ли ребенок освоить цифровую грамотность только интуитивно?

4. Кого называют цифровыми сиротами, изгнанниками и наследниками?

5. К какой категории родителей вы себя относите — наставники, потакающие или запрещающие? Устраивает ли вас эта роль?

6. Почему преступники решают кого-то взломать или ограбить?

7. Что такое кибербуллинг?

8. Какие правила кибербезопасности вы нарушали?

9. На какие три группы можно разделить опасные ситуации?

10. Как защитить свои данные от нечаянных действий ребенка?

11. В каких жизненных ситуациях, перечисленных в этой главе, вы оказывались?

12. Можете ли добавить к этому списку что-то еще?

13. Что значит «бояться интернета правильно»?

Глава 2

Наши цифровые ценности

В этой главе мы рассмотрим виды цифровых активов, которые уже есть (или скоро будут) почти у всех,и увидим, что они обладают реальной ценностью, а потому их надо беречь также, как и привычные вещи — деньги, имущество и другое.

Многие считают себя «цифровыми бедняками» — мол, красть у нас нечего, потому и замки не нужны. Когда человек не осознает, что у него есть что-то ценное, любые меры предосторожности кажутся ему избыточными.

Когда человек не осознает, что у него есть что-то ценное, любые меры предосторожности кажутся ему избыточными.

Скорее всего, в ответ на ваши советы он покрутит пальцем у виска и назовет вас параноиком. В реальной жизни ведь никто не будет ставить мегазащищенную железную дверь, если в доме шаром покати — вот когда привалит богатство, тогда и подумаем об этом.

Такую точку зрения можно признать вполне рациональной, поскольку стоимость и сложность системы защиты должна быть адекватна ценности того, что мы пытаемся с ее помощью защитить. Однако в том, что касается цифровых ценностей, наш житейский опыт не всегда выступает хорошим советчиком: слишком внезапно произошли изменения, и у нас еще не выработались привычки, позволяющие действовать правильно «на автомате», не задумываясь. Поэтому даже многие взрослые, опытные во всех отношениях люди часто попадают впросак, когда сталкиваются с киберпреступниками или сами случайно уничтожают что-то для себя ценное.

Прежде всего, давайте проведем инвентаризацию наших цифровых активов, чтобы понять их истинную ценность, а уже потом подумаем, как их защитить от возможных посягательств преступников и от собственной глупости.

Итак, что у нас сегодня в «цифре»? Да почти все! Информационные технологии просочились всюду, и, помимо того, что дали нам кучу

новых возможностей, везде добавили новых рисков, которые теперь надо учитывать.

Условно наши цифровые богатства можно разделить на три категории:

- «**Измененные цифрой**» — то, что существовало и раньше, но под воздействием новых технологий претерпело значительные трансформации. Например, деньги. В этой сфере безопасность наших данных и ресурсов во многом зависит от действий других людей, на которых мы повлиять не можем. А между тем сами институты, поддерживающие эти ценности, тоже не до конца понимают масштабы новых угроз.

- «**Рожденные в цифре**» — это различные цифровые объекты, которые мы создаем сами, покупаем или которыми пользуемся. Все они, по сути, представляют собой лишь информацию, записанную в компьютерных системах, а у нас могут быть различные права на них. Например, виртуальный танк или персональная страница в соцсети. Их сохранность во многом зависит от того, насколько хорошо мы соблюдаем правила безопасности, и, конечно же, от квалификации разработчика.

- «**Кибервещи**» — сейчас каждая кофеварка норовит выйти в интернет. То есть обычные физические вещи становятся цифровыми, а значит, об их безопасности тоже надо позаботиться — это относительно новое явление, с которым еще предстоит разобраться.

Теперь давайте перечислим, что́ это могут быть за «богатства» (хотя, почему в кавычках?):

- **Деньги**. Кроме наличных в кошельке, они все электронные;
- **Бонусы**. «Как бы деньги» — мили, баллы лояльности и прочее;
- **Персональные данные, включая медицинские**. Пока это просто информация — до тех пор, пока кто-то не решит украсть и продать вашу цифровую личность;
- **Аккаунты в соцсетях, страницы и каналы**. Иногда это очень дорогой актив;
- **Цифровые авторские права на сайты, блоги, фото, видео и другой контент**;
- **Тайна частной жизни.** Когда вокруг камеры и микрофоны, это становится не просто богатством, а роскошью;
- **Репутация.** Все, что написано о вас, и все, что вы написали сами, сохраняется в интернете навечно. А ведь репутация — один из самых дорогих активов;
- **Переписка**, деловая и личная, в электронной почте и мессенджерах;
- **Цифровые коллекции. Музыка, кино, файлы, фотографии** (разумеется, без пиратских копий);
- **Виртуальные вещи.** Пока в играх, дальше будет больше;
- **Контакты и заметки**. Ведь никто уже не держит записных книжек, не так ли?;

- **Домены (сайты)**. В наше время уже бывает, что даже имя ребенку выбирают такое, чтобы домен был свободен;

- **Цифровые ресурсы.** Домашний wi-fi, место в облачном хранилище, виртуальные машины и тому подобное;

- **Цифровая техника.** Телефон, компьютер и прочая умная электроника;

- **Автомобиль**, который все больше превращается в компьютер на колесах со всеми вытекающими отсюда рисками;

- **Умный дом.** Эта тема только набирает популярность и пока не слишком волнует киберпреступников, но угрозы будут расти.

Ого, сколько, оказывается, всего у нас есть ценного! Естественно, найдутся люди, которые могут захотеть это украсть или уничтожить.

Теперь давайте посмотрим на наше «цифровое богатство» более подробно.

Деньги в эпоху цифры

Кроме наличных, которые лежат у вас в кармане, все остальные ваши деньги существуют в цифровом виде. Зарплата на карточке, депозит в банке, баланс на счете мобильного телефона, небольшой резерв в электронном кошельке Киви или Яндекс — это ведь

не более чем цифры в какой-то базе данных. Но это такие же настоящие деньги, как и наличные. И их точно также можно потерять. Или стать жертвой грабителей.

Ясно, что финансовые системы — одни из наиболее защищенных, но они же являются и самым лакомым куском для киберпреступников.

Это есть в главе про социнженеров. Как же они это делают? В основном — благодаря невнимательности граждан. Чаще всего жулики используют поддельные сайты (фишинг) и методы социальной инженерии, когда человек фактически сам отдает им деньги. Особенно активизировались в последнее время телефонные мошенники, вооруженные вашими персональными данными. Обычно они представляются службой безопасности банка и в разговоре выманивают у вас недостающую информацию, чтобы совершить перевод с вашего счета себе.

> *Центральный банк РФ (ЦБ РФ) подчеркивает, что социальная инженерия — это главная угроза информационной безопасности. «Более 97% хищений со счетов физических лиц и 39% хищений со счетов юридических лиц были совершены с использованием приемов социальной инженерии», — рассказал на форуме «Финополис» первый замглавы департамента информационной безопасности ЦБ РФ Артем Сычев*[1].

Увы, надежного метода защиты от социальной инженерии не существует. На удочку таких жуликов попадаются даже специалисты по информационной безопасности — потому что все мы живые люди и у нас есть эмоции, которые могут отключить наше критическое мышление.

---

1 *«Вам звонят из банка»: как воруют наши деньги. // Газета.ru, 10 октября 2019.*

Тем не менее, стоит еще раз повторить:

- Сотрудники банка никогда не спрашивают у клиентов проверочный код карты[1], ПИН-код и SMS-пароли. Но будьте осторожны: преступники тоже знают, что вы это знаете, и научились изображать переключение на якобы информационную систему банка, куда просят ввести ваш код;

- Железное правило: получив звонок о подозрительной операции по вашему счету, положите трубку и сами перезвоните в банк. Помните, что у вас нет никакой возможности проверить подлинность входящего звонка. Преступники умеют подменять свой номер на номер банка;

- Будьте крайне внимательны с SMS. Мошенники легко имитируют названия банков в качестве отправителей, но их сообщение упадет в новую переписку, и это должно вас насторожить. А если SMS, полученное как будто бы от банка, предлагает перейти по какой-то ссылке, то это почти наверняка жулики. Не поленитесь перезвонить в банк и узнать, действительно ли вам отправляли такое сообщение и зачем.

Главное — не поддаваться во время звонка панике, когда вам сказали, что ваши деньги вот-вот украдут, или, наоборот, эйфории, если вам позвонили, чтобы поздравить с небывалым выигрышем. Спокойно проанализируйте ситуацию и возьмите инициативу в свои руки, не поддавайтесь на разводку мошенников — хотя это проще сказать, чем

1 *У каждой платежной системы свое наименование секретного кода безопасности: у VISA — это код CVV2 (Card Verification Value 2); у MasterCard — CVC2 (Card Verification Code 2); у American Express — CID (Card Identification); у НПСК МИР — CVP2 (Card Verification Parameter 2).*

сделать. И на всякий случай будьте вежливы: иногда звонят настоящие сотрудники банков, которые действительно заботятся о сохранности ваших средств.

Безопасность ваших цифровых финансов далеко не всегда зависит от вас. Преступники, как и во времена Бонни и Клайда, все также любят грабить банки, а не отдельных клиентов. Только вместо шумных нападений со стрельбой и погонями теперь они действуют тихо: максимум, что можно услышать, это клацанье клавиш компьютера. И, надо сказать, действуют они гораздо эффективнее, чем грабители прошлого века.

В 2015 году прогремело известие о масштабном ограблении банков по всему миру. Более 30 компаний понесли ущерб на общую сумму порядка 1 миллиарда долларов. Это была умело проведенная хакерская атака. Мошенники заразили вирусами банки Украины, России, Европы, Китая, Юго-Восточной Азии, Ближнего Востока и Африки. И в течение двух лет незаметно крали у них деньги.

Схема внедрения вируса была проста: на электронную почту работнику банка приходило письмо, содержащее вложение с вредоносной программой. После проникновения вируса на компьютер мошенники начинали отслеживать принципы работы каждой конкретной банковской системы. Все действия, которые позже производили хакеры, — перевод денежных средств, управление банкоматами — совершались якобы от имени банковских служащих. А до этого кибермошенники серьезно изучали схему работы сотрудников, в том числе через камеры[1].

1 *Самое крупное киберограбление банков в истории на 1 миллиард долларов. // Яндекс.Дзен, 6 декабря 2018.*

Не наше дело указывать банкам, что и как им следует делать для повышения безопасности наших средств. Прежде всего, нужно уделить внимание безопасности собственных цифровых финансов, — тем более, что оборот наличных в мире неуклонно сокращается, а доля электронных платежей растет. Сейчас стало модно, особенно среди молодежи, не иметь при себе наличных и везде расплачиваться карточкой, а еще лучше — телефоном. Удобно? Несомненно. Рискованно? Не без этого. Но при соблюдении простых правил эти риски можно снизить до приемлемого уровня.

Бонусы. «Как бы деньги»

Кроме банковских карт у вас в кошельке наверняка есть еще куча разнообразного пластика — бонусные и скидочные карты, карты лояльности от авиакомпаний и тому подобное. Некоторые из них не жалко и выбросить, другие же имеют высокую ценность.

Но и этот пластик чаще всего есть всего лишь физическое воплощение неких цифр. Если вы потеряете саму карточку — это не страшно: попросите новую. А вот если кто-то получит доступ к вашему аккаунту, то он, скорее всего, найдет способ, как употребить ваши бонусные баллы. Формально, с точки зрения Центрального Банка, все эти баллы и бонусы деньгами не являются, но с практической точки зрения они равнозначны настоящим деньгам. Будет обидно, если вы целый год, летая по командировкам, копили мили, чтобы взять бесплатный билет и отправиться в отпуск, а кто-то их возьмет и украдет. Ваш кошелек испытает такую же боль, как если бы из него внезапно вытащили несколько крупных купюр.

Такой случай произошел в 2015 году, когда хакерской атаке подверглись аккаунты участников программы «Аэрофлот Бонус». Злоумышленники пытались украсть у клиентов авиакомпании бонусные мили, и чтобы остановить атаку, «Аэрофлоту» пришлось временно заблокировать у ряда пользователей мили на списание. Получить доступ к аккаунтам клиентов хакеры могли через почтовые ящики. В связи с этим «Аэрофлот» рекомендовал пользователям устанавливать разные логины и пароли на почту и личный кабинет в программе «Аэрофлот Бонус»[1].

Но не всем клиентам «Аэрофлота» так повезло. У жительницы Хабаровска накопленные за несколько лет заветные мили для перелетов со скидками таинственно исчезли из личного кабинета. Вот что она рассказала (стиль, орфография и пунктуация сохранены):

> *«В августе 2015 года я обнаружила значительное уменьшение накопленных мною за четыре года миль, а именно исчезло 97,5 тысячи. Зайдя в личный кабинет, увидела то, что три человека с конкретными Ф.И.О. и номерами документов в разные дни августа совершили перелет бизнес-классом по направлению Москва-Адлер. При этом оплатили они их милями с моего счета. ... В ответ на мои неоднократные устные и письменные заявления в компанию «Аэрофлот» я получала ответы будто моим вопросом занимаются, а такая ситуация впервые случилась и так далее»[2].*

---

1 *Хакеры попытались украсть бонусные мили у клиентов «Аэрофлота» // РБК, 12 августа 2015.*

2 *Кража по-русски: Участие в программе «Аэрофлот Бонус» хабаровчанка запомнит надолго // AmurMedia.ru, 18 ноября 2015*

Авиакомпания выразила сожаление, но помочь клиенту не смогла, ссылаясь на то, что услуга по перевозке была оказана в полном объеме, и посоветовала обратиться в правоохранительные органы.

Аналогичный случай был и в 2018 году. Клиент получил сообщение, что кто-то зашел в его личный кабинет и сменил телефон для SMS-информирования. Злоумышленник также поменял пароль, и теперь законный пользователь не мог получать уведомления о списании миль и контролировать свой счет. Он сразу же обратился в авиакомпанию, и после некоторых волнений ситуация все же разрешилась благополучно (стиль, орфография и пунктуация сохранены):

> *«По Вашему обращению в контакт-центр авиакомпании оператором, а затем службой экономической безопасности были предприняты необходимые действия по отмене несанкционированно оформленной перевозки. Мили возвращены на Ваш счет. Соответствующими подразделениями авиакомпании проводится работа по расследованию и упреждению подобных случаев. Выражаем надежду, что меры по защите счетов участников, предпринимаемые как со стороны авиакомпании, так с Вашей стороны, как владельца Личного кабинета, позволят не допустить подобных ситуаций в дальнейшем»*[1].

Подобные хищения — дело рук не каких-то хакеров-одиночек, а результат работы организованного киберпреступного сообщества в составе примерно двадцати человек. Мошенники получали доступ к аккаунтам участников программы «Аэрофлот Бонус», а потом продавали мили желающим приобрести билеты подешевле. Это слож-

1 *Кражи в Аэрофлоте // ЖивойЖурнал, блогер «nemihail», 13 сентября 2018.*

ное уголовное дело вела следователь управления на транспорте МВД по ЦФО Евгения Шишкина, которая была убита в ноябре 2018 года. Как писала газета «Коммерсантъ», начатое Шишкиной расследование, по данным близкого к нему источника «Ъ», продвигалось с большим трудом. Участники, например, постоянно спорили, можно ли считать похищенными мили, строго говоря, не имеющие материальной ценности, и кто в таком случае является потерпевшим — обворованный фактически клиент или авиакомпания — юридический владелец миль. Споры, по данным того же источника, приводили и к конфликтам, вышедшим в итоге за стены следственного кабинета[1].

Преступников юридические тонкости не волнуют — считать ли мили и прочие бонусы настоящими деньгами или нет. Зато они четко видят возможность заработать на их краже и могут пойти на любые действия, чтобы сохранить свой нелегальный бизнес. История трагическая, но весьма показательная.

Персональные данные

1984 год, Лос-Анджелес. Из уже недалекого от нас 2029 года, где идет война людей с машинами, в прошлое заброшен робот Терминатор, который должен найти и убить Сару Коннор, мать будущего предводителя Сопротивления. Чтобы его остановить, следом прибывает сержант элитного подразделения Кайл Риз. И что они оба делают? Идут к ближайшей телефонной будке, где лежит справоч-

1 *Полицейский следователь не поверила в госзащиту // Газета «Коммерсантъ», 11 октября 2018.*

ник, в котором они находят ее телефон и домашний адрес. Дальше вы знаете.

Для современного зрителя это выглядит шокирующим. Неужели персональные данные всех граждан вот так спокойно лежат в каждой телефонной будке, и кто угодно может их прочитать? Сегодня это бы назвали крупной утечкой и обсуждали бы во всех новостях, а на виновника наложили бы крупный штраф. За подобную промашку Facebook предстоит выложить кругленькую сумму в 5 миллиардов долларов[1] — и это на сегодня самое крупное взыскание с технологической компании. Ранее Google в подобной ситуации был оштрафован на 22,5 миллиона долларов.

> *По сравнению с США, в России штрафы пока выглядят символическими, даже с учетом их повышения в ноябре 2019 года. Теперь за допущенную утечку персональных данных юридическое лицо может заплатить от 1 до 6 миллионов рублей и от 6 до 18 миллионов рублей за повторное нарушение. Но для многих организаций и это может оказаться непосильным бременем.*

Что же заставило законодателей принять такие драконовские меры? Может быть, нашествие терминаторов, которого мы не заметили?

По правде говоря, какой-то одной причины нет. Скорее, это результат признания той огромной роли, которую стали играть в жизни общества информационные технологии, ведь благодаря им стала

---

1 *FTC slaps Facebook with record $5 billion fine, orders privacy oversight// CNBC, 24 июля 2019.*

возможной массовая обработка персональных данных, и принесла она с собой не только ощутимые удобства и блага, но и серьезные угрозы — поставленные на поток мошеннические схемы по краже денег с банковских карт, незаконные рекламные кампании и даже попытки влиять на исход выборов. То есть речь сегодня идет не о спасении какой-то конкретной Сары Коннор, а о противостоянии угрозам для общества в целом. С этих позиций жесткость властей выглядит объяснимой.

В России закон о защите персональных данных[1] был принят в 2006 году; с этого же момента развернулась и пиар-кампания по просвещению пользователей, местами переходящая в форменную истерию. Судите сами: во всех статьях и роликах про защиту персональных данных нам рассказывают, как опасно оставлять в интернете домашний адрес и телефон и называть свое имя, однако при этом все мы спокойно сообщаем эти данные первому попавшемуся водителю такси или курьеру по доставке пиццы. Логично ли это?

Наши паспорта копируют и сканируют в десятках учреждений, нас фотографируют, снимают отпечатки наших пальцев, просят заполнить кучу бланков с разнообразными сведениями. Если посмотреть на вещи реально, то у человека, в общем-то, нет возможности управлять данными о себе. Безусловно, следует проявлять разумную осторожность и не оставлять лишней информации на совсем уж левых сайтах. Но не впадать же при этом в паранойю! Достаточно будет задать себе вопрос: для чего кому-то нужны ваши дан-

1 *Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, ст. 3 п.1: Персональные данные—любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).*

ные? Например, если вы не скажете адрес таксисту, он вас не довезет до дома. Однако совершенно необязательно рассказывать ему, с кем вы живете и сколько денег у вас на счете.

Вообще говоря, вся эта история с персональными данными больше касается бизнеса и государственных организаций, которые занимаются их обработкой. Кроме того, что на них лежит ответственность за утечки, они еще обязаны обеспечивать хранение и обработку наших данных в соответствии с требованиями регулятора, а это достигается путем покупки разнообразных сертифицированных средств; иначе нельзя.

> *Главная причина утечек данных российских пользователей — большое количество организаций, в которые они предоставляют информацию о себе, а также низкая зарплата сотрудников таких организаций*[1].

То есть мы, граждане, должны понимать, что изрядная доля шумихи вокруг защиты персональных данных связана с желанием поставщиков продать свои решения заказчикам, а отнюдь не с реальными угрозами. Понимая это, мы должны трезво взвесить свои риски при возможной утечке.

Первое, чем нас пугают профессиональные «защитники» наших данных — реклама. Дескать, узнав ваши контакты и предпочтения, вам все наперебой начнут делать предложения, от которых вы не сможете отказаться. Но в чем же здесь риск? Если реклама окажется действительно полезной, это будет даже хорошо.

---

1 *Результаты исследования, проведенного специалистами компании Ernst & Young, и опубликованного в TAdviser.*

Правда, некоторые рекламодатели бывают слишком назойливы и достают нас звонками по телефону, — так на это у нас есть черный список. Поэтому, положа руку на сердце, скажем: да, избыток рекламы — это некоторое неудобство, но никак не угроза безопасности.

Избыток рекламы — это некоторое неудобство, но никак не угроза безопасности.

Еще говорят, что, добыв копию вашего паспорта, кто-нибудь сможет оформить на него кредит. Да, такое случается, и полностью уберечься от этого риска невозможно, — даже если вы не будете пользоваться интернетом вовсе. Достаточно потерять паспорт или лишиться его вследствие кражи. Кроме того, копии паспортов требуются и хранятся в самых разных учреждениях, сотрудники которых не всегда могут быть в ладах с законом. Это обычное уголовное преступление, которое, к сожалению, не всегда легко расследуется. Зачастую человек узнает о висящем на нем долге, когда возникает серьезная просрочка, или даже на этапе исполнительного производства. В такой ситуации трудно дать какой-либо другой совет, кроме самого очевидного: обратиться в полицию.

> *Если вы потеряли паспорт или у вас возникли подозрения об утечке персональных данных, необходимо отправить запрос в Бюро кредитных историй — один раз в год это можно сделать бесплатно. Согласно закону «О кредитных историях», Бюро обязано выдать исчерпывающую информацию обо всех кредитах, взятых на ваше имя, и кредиторах.*

Бывает, что мошенники оформляют на один добытый паспорт сразу несколько кредитов, поэтому лучше не ждать, когда к вам

постучатся приставы. Считайте ежегодный запрос в БКИ одним из элементов цифровой гигиены, даже если вы не теряли паспорт.

А стоит ли паниковать, когда произошла утечка паспортных данных? Если вы подозреваете, что в руки мошенников мог попасть не сам паспорт, а только паспортные данные, то не стоит.

> *Александр Баранов, заведующий кафедрой информационной безопасности НИУ ВШЭ*
>
> *«Наши паспортные данные растекаются направо и налево. Многие организации (например, гостиницы) требуют их предоставить, сканы документа остаются в салонах, где делают копии. Паспортные данные очень часто оказываются в открытом доступе, случается, что их продают или передают нечистые на руку банковские работники или сотрудники медицинских организаций. Если вы нашли свои паспортные данные в открытом доступе, можно написать жалобу в Роскомнадзор: этот орган занимается в России контролем за зашитой персональных данных и правильностью их передачи. Но это не повод, чтобы менять паспорт. Тем более что такое условие (утечка паспортных данных — прим. АиФ.ru) не является основанием для замены документа, в МВД вам откажут»*[1].

1 *В каких случаях стоит поменять паспорт? // Аргументы и Факты, 1 июля 2019.*

Медицинские данные

Среди персональных данных особо выделяют данные о состоянии здоровья — к их защите предъявляют повышенные требования. К таким данным относится информация о перенесенных заболеваниях, диагнозах, обследованиях, результаты анализов и даже сам факт обращения к врачу.

Почему люди так обеспокоены риском разглашения их истории болезни? В основном, из-за возможных социальных последствий. Увы, уровень образованности и толерантности в обществе не слишком высок, и поэтому некоторая информация, став публично известной, способна больно ударить по репутации и карьере. Например, факт обращения к психиатру может быть весьма негативно истолкован при приеме на работу — такому кандидату запросто откажут под каким-то надуманным предлогом. Но помилуйте, как человеку справляться, скажем, с депрессией? Лекарства в таких случаях может назначить только врач-психиатр. Есть, кроме того, «стыдные» болезни, которые никому не хочется афишировать.

Бывают ситуации, когда человек скрывает, что он действительно серьезно болен, хотя разглашение этой информации непосредственно его здоровью угрозы не несет. Некоторые же, наоборот, совершают «каминг-аут» и публично рассказывают о своем недуге. Иногда, кстати, это лучший способ пресечь слухи и даже помочь другим товарищам по несчастью, обратив таким образом, внимание общества на проблему.

> *О том, что Фредди Меркьюри болен СПИДом, подозревали давно, — он изменился внешне, перестал бывать на вечеринках, быстро утомлялся во время работы. Шила в мешке*

не утаишь, симптомы были слишком очевидны. Но публично Меркьюри заявил об этом только 23 ноября 1991 года, за день до смерти:

«Я заметил, что последнее время все говорят о том, что я болен СПИДом. Это правда. У меня СПИД. Я долго скрывал эту информацию, чтобы мои друзья и родственники не беспокоились, но теперь в этом не вижу смысла. Я надеюсь, что многие из вас поймут, что со СПИДом нужно бороться. Только вместе мы сможем остановить эту страшную болезнь».

Он мог бы этого и не делать — посмертный диагноз легко можно было заменить на пневмонию — но Фредди все-таки принял решение сказать о своей болезни. В то время люди, больные СПИДом, подвергались стигматизации: их публично всячески порицали; не то чтобы излечивающих препаратов, но даже средств поддерживающей терапии еще не было. Сейчас мы понимаем, что ВИЧ может инфицироваться абсолютно любой человек, но в те годы эта была «болезнь геев».

На этом фоне поступок Фредди был не просто смелым: он сыграл важную роль в осведомленности о СПИДе и заставил миллионы людей задуматься об этом. Музыканты Queen приняли решение направить все деньги от переиздания самой знаменитой своей песни «Богемская рапсодия» на борьбу со СПИДом.

Пожалуй, едва ли кто-то будет озабочен тем, чтобы скрыть, что он переболел гриппом или повредил ногу, катаясь на горных лыжах. Но закон един: все это — персональные данные особой категории, которые должны охраняться. С другой стороны, строгость закона часто становится препятствием для развития медицинских

сервисов, потому что трудно создать даже обезличенные базы медицинских данных, не нарушив при этом требований закона 152-ФЗ о персональных данных.

Возможно, страхи насчет утечек медицинских данных изрядно преувеличены. Интуитивно люди это, пожалуй, чувствуют — недаром же в поезде часто рассказывают случайным попутчикам про все свои болезни. Но нужно признать, что существует риск, связанный с рекламой или попытками мошенничества: узнав ваши медицинские данные, некто может попытаться продать вам лекарственные препараты или медицинские услуги, в том числе и сомнительного качества. Больной человек не всегда поступает разумно и может попасться на удочку мошенников.

Больной человек не всегда поступает разумно и может попасться на удочку мошенников.

Также нужно помнить и о случаях, когда медработники «сливают» данные об умерших в ритуальные агентства, вследствие чего их родственники подвергаются агрессивной коммерческой атаке.

Аккаунты в социальных сетях

Миллиарды людей имеют аккаунты в соцсетях. С одной стороны, это окно в мир, возможность общаться и получать информацию. Взрослых, по понятным причинам, беспокоит наличие в сетях нежелательного контента, от которого они пытаются оградить детей. Это тема отдельной главы. Сейчас же хочется обратить внимание на то, что сетевой аккаунт сам по себе представляет ценность, и его

утрата может быть очень болезненна психологически, а иногда и финансово.

Сетевой аккаунт сам по себе представляет ценность, и его утрата может быть очень болезненна психологически, а иногда и финансово.

Всякому человеку жалко терять плоды своих трудов, даже если это всего лишь мемы и фотографии, собранные на его странице. Но главное даже не в этом — еще печальнее потерять те знаки внимания, которые вы получали от реальных и виртуальных друзей.

Во времена Пушкина социальных сетей не было, зато были альбомы, куда друзья и знакомые писали (то есть, выражаясь современным языком, «постили») шутки, мадригалы, признания в любви, запрещенные цензурой стихи, эпиграммы, шаржи, романтические рисунки и прочий, как бы мы сейчас сказали, «контент». И точно также «репостили» понравившееся из альбома в альбом, как мы это делаем сегодня. Причем альбомы были не только у чувствительных барышень или поэтов — их имели даже гусары и кавалергарды, как, например, граф Николай Толстой, отец знаменитого русского писателя. Расцвет «альбомной» культуры в России пришелся на 1820-е годы, потом мода постепенно прошла, оставив нам множество изящных и любопытных свидетельств той замечательной эпохи.

«Конечно, вы не раз видали
Уездной барышни альбом
Что все подружки измарали
С конца, с начала и кругом.

Сюда, назло правописанью,
Стихи без меры, по преданью

В знак дружбы верной внесены,
Уменьшены, продолжены...
...

...Тут непременно вы найдете
Два сердца, факел и цветки;
Тут верно клятвы вы прочтете
В любви до гробовой доски;

Какой-нибудь пиит армейской
Тут подмахнул стишок злодейской.
В такой альбом, мои друзья,
Признаться, рад писать и я...»[1]

Ну, скажите: чем это отличается от девчачьих страниц во ВКонтакте?

Может быть, мода на соцсети тоже пройдет, а цифровые археологи, изучая наше время, будут удивляться тому, как мы были наивны. Так что не спешите ругать своих отпрысков за увлечение этим, в общем-то, невинным занятием; за минувшие двести лет люди нисколько не изменились, только перешли с бумаги на цифровые носители. Один из творцов альбомной культуры, Василий Львович Пушкин, очень точно сказал, что «альбом есть памятник души» — в наши дни это определение с полным правом можно отнести к персональным страницам в соцсетях. Вот именно поэтому потеря контроля над своим аккаунтом может вызвать психологическую травму у подростка или даже у взрослого.

В то время, как большинство пользователей соцсетей ведет свои страницы исключительно в личных целях, некоторые умудряются на этом

1 *А.С. Пушкин «Евгений Онегин», глава 4.*

неплохо зарабатывать. Причем, среди ударников креативного труда в YouTube и Instagram есть немало юных дарований, которые смогли монетизировать свою страсть к созданию публикаций и занимаются этим делом вполне профессионально. Разброс доходов в этой сфере значителен: одним едва хватает на мороженое, а другие оказываются главными добытчиками в семье и даже содержат своих родителей. Понятное дело, что о безопасности такой курочки, несущей золотые яйца, стоит позаботиться как следует, ибо охотников до чужого добра предостаточно.

> *Популярность в интернете может прийти внезапно: какой-то ролик вдруг набирает миллионы просмотров, и его автор однажды утром просыпается знаменитым. В тот же самый момент его аккаунт становится мишенью для атаки, и с очень высокой вероятностью будет взломан.*

Поэтому, начиная карьеру блогера, нужно сразу хорошенько подумать о безопасности своего аккаунта.

Авторские права на цифровые произведения

Обычные пользователи интернета редко задумываются об авторских правах на свои произведения, а зря. Ведь может так случиться, что у вас во дворе высадятся инопланетяне, и вы успеете их сфотографировать. Или ваш домашний питомец вдруг наберет толпу поклонников, как кошка из Аризоны по кличке Соус Тардар, которую весь мир знает как Grumpy cat («Угрюмая кошка»). Она стала знаменитостью и начала приносить своим владельцам ощутимый доход, набрав в итоге более 8 миллионов подписчиков на Facebook и 2,4 миллиона в Instagram — такая слава вполне конвертируется в деньги.

В цифровом мире каждый сам себе автор и сам себе издатель — даже маленькие дети делают контент. А каждый разумный автор должен позаботиться о защите своих прав. Пусть даже вы не зарабатываете миллионы — обидно, если кто-то сворует ваши произведения.

Не отстают в производстве интернет-контента и учителя.

64-летний преподаватель физики из Одессы Павел Андреевич Виктор по использованию современных технологий опережает многих молодых коллег. Уже пять лет он снимает на видео свои уроки для учеников 7-11-х классов и выкладывает их на YouTube. Сейчас их смотрят русскоязычные зрители со всего мира: у канала учителя более 80 тысяч подписчиков, а общее число просмотров перевалило за 8 миллионов.

Павел Андреевич вспоминает, что все началось со скайп-конференций, которые ему пришлось проводить для заболевших учеников в лицее, где он преподает. Затем он решил расширить аудиторию своих уроков и самостоятельно освоил для этого новые технологии.

К Виктору часто обращаются с предложениями монетизировать его канал, но преподаватель от них отказывается. «Мне кажется, что две вещи должны быть бесплатными в этой жизни — лечение и обучение», — говорит он[1].

1 *Посмотреть уроки П. Виктора можно здесь:* ***https://www.youtube.com/user/pvictor54/videos***

Такая позиция, безусловно, вызывает уважение. Если вы тоже решите сделать свой контент всеобщим достоянием, то это нужно специальным образом обозначить, потому что могут найтись люди, желающие заработать на ваших произведениях вместо вас.

Например, вы можете публиковать свои произведения под лицензией Creative Commons, которая используется, когда автор хочет дать другим людям право делиться и использовать созданное им произведение. Лицензии Creative Commons применяются ко всем работам, на которые распространяется авторское право, включая книги, пьесы, фильмы, музыку, статьи, фотографии, блоги и веб-сайты.

Программисты, в том числе и юные, тоже могут публиковать свои разработки под так называемыми открытыми лицензиями, которых существует несколько видов. Вообще говоря, в индустрии программного обеспечения движение в сторону открытого исходного кода (open source) становится мейнстримом; даже гиганты отрасли, такие как Microsoft и IBM, многие из своих продуктов выпускают под открытыми лицензиями.

Однако следует помнить, что свободная или открытая лицензия не означает, что «все вокруг колхозное, все вокруг мое» — есть правила, которые надо соблюдать. Уже упомянутая лицензия Creative Commons имеет шесть типов, отличающихся набором требований и ограничений.

Заботясь о своих авторских правах, нужно уважительно относиться и к чужим. И помнить, что пиратский контент — это еще и источник вирусов, троянов и прочей заразы.

Заботясь о своих авторских правах, нужно уважительно относиться и к чужим. И помнить, что пиратский контент — часто источник вирусов, троянов и прочей заразы.

Тайна частной жизни

Представьте, что все стены вдруг стали прозрачными, все сказанное по секрету слышно всем, все, сделанное когда-то давно, помнится, как будто это было вчера. Представили? Это может показаться шокирующим, но мир сегодня действительно таков. Мы ежедневно попадаем в поле зрения сотен видеокамер, наши разговоры записываются, перемещения фиксируются. Мы добровольно променяли наши маленькие секреты на удобства, которые дают цифровые технологии. Ведь достаточно просто сказать: «О'кей, Гугл...», — и нужная информация тут как тут. Голосовые интерфейсы, такие как Алиса от Яндекс или Siri от Apple, становятся все популярнее, а это значит, что нас, вполне возможно, слышат 24 часа в сутки, запоминают и анализируют каждое наше слово.

В русском языке нет аналога слову «privacy», которое обычно используется в этом контексте в англоязычных странах. Прямой перевод дает варианты «конфиденциальность», «секретность», «уединение», «частная жизнь», но все они не совсем точно передают тот смысл, который мы находим в английском толковом словаре Merriam-Webster: «свойство или состояние быть вне компании или наблюдения» или «свобода от несанкционированного вторжения» И только потом — как архаическое значение! — идут «уединение» и «секретность».

privacy noun

pri·va·cy | \ ˈprī-və-sē, *especially British* ˈpri-\

plural **privacies**

Definition of *privacy*

1 **a** : the quality or state of being apart from company or observation : SECLUSION

b : freedom from unauthorized intrusion
// one's right to *privacy*

2 *archaic* : a place of seclusion

3 **a** : SECRECY

b : a private matter : SECRET

Privacy вполне можно себе обеспечить и в цифровую эпоху, если относиться к вопросу технически грамотно. Оставьте дома свой мобильный телефон и пойдите погулять в лес — в нашем мире еще есть места, где вы не будете под присмотром Большого Брата и прочих любопытных глаз. А если вы находитесь в Сети, то будьте уверены — за вашими действиями наблюдают.

Если вы находитесь в Сети, то будьте уверены — за вашими действиями наблюдают.

Михаил Косински, в прошлом заместитель директора Центра психометрии Кембриджского университета, а в настоящее время доцент Стэнфордского университета США, говорит: «вместо того, чтобы ввязываться в очередную битву за приватность, стоит признать, что война уже проиграна, и лучше озаботиться тем, чтобы мир стал благоприятной средой для человека, лишенного приватности».

В течение нескольких лет Косински с коллегами по Кембриджу разрабатывал систему, которая на основе активности пользователя в социальной сети составляет подробный психологический профиль человека. Система способна не только описывать особенности характера, но и предсказывать, среди прочего, пол, сексуальную ориентацию, цвет кожи и даже политические предпочтения пользователя. (Наработки Косински использовались фирмой Cambridge Analytica, якобы помогавшей Трампу победить на выборах. Правда это или нет, доподлинно неизвестно, но то, что попытки манипуляции мнением и даже поведением людей на основе сведений о них, полученных из интернета, делаются и будут делаться — это факт).

Короче говоря, тайны частной жизни в том виде, как это было раньше, теперь не существует. Стоит ли этого опасаться? Вот, например, во многих европейских странах не принято иметь шторы на окнах — люди так и живут у всех на виду. О причинах возникновения этой традиции ходят разные легенды, но суть их одна: честному человеку нечего скрывать. Пожалуй, в нашем прозрачном мире это будет самое благоразумное решение: поменьше беспокоиться о том, что за вами наблюдают, и вести себя так, чтобы не было причин чего-то стыдиться.

- *В середине XVI века наместником Испанских Нидерландов был назначен жестокий Фернандо Альварес де Толедо, 3-й герцог Альба. За четыре года его наместничества было казнено более 18 тысяч мирных жителей. Среди многочисленных тиранических приказов герцога был запрет на закрытые шторами окна, поскольку голландцы часто устраивали домашние цеха по производству оружия и проводили революционные собрания. Спустя некоторое время король Испании отозвал Альбу из Нидерландов, революция победила, но традиция осталась в новом прочтении:*

теперь голландцы гордились, что им нечего скрывать, и их образ жизни соответствует христианским представлениям о морали.

- *В XVII столетии в Швеции был принят закон, запрещающий гражданам завешивать окна (кстати, документально он действует и по сей день, но является необязательным к исполнению). Закон был введен для того, чтобы каждый лично мог убедиться в том, что его сосед живет по средствам. Кроме того, во время обходов королевская стража имела право заглянуть в окна горожан, чтобы проверить, не нарушается ли порядок.*

- *Во Франции в период немецкой оккупации граждане, которые не сотрудничали с фашистами и не получали тем самым дополнительные пайки, держали окна открытыми, чтобы показать, что у них нет провианта от врага.*

Автор обескураживающей книги «Прозрачное общество» («The Transparent Society») Дэвид Брин приводит убедительные аргументы против тайны частной жизни.

Брин полагает, что чем упорнее мы пытаемся защитить нашу приватность, тем с большей долей вероятности ее потеряем. Он не предлагает, чтобы наши спальни стали открытой кормушкой для вуайеристов, но считает, что прозрачность дает нам возможность и право привлекать к ответственности тех, кто будет нарушать наши границы.

«Прозрачность — это не устранение частной жизни, — подчеркивает Брин. — Приватность подразумевает спокойствие дома и право быть в одиночестве», — пишет он[1].

1 *Is privacy possible in the digital age? // NBCNEWS.com, 7 декабря 2000.*

Но не надо путать приватность (конфиденциальность) и анонимность. Анонимность — это совсем другое дело, это желание скрыть свою личность при контактах с другими людьми или находясь на публике. Анонимность и раньше была проблемой: чтобы остаться неузнанными, люди переодевались в чужую одежду, носили маски, приклеивали бороды и усы — в общем, проявляли чудеса изобретательности, но весь этот карнавал отнюдь не гарантировал, что вас никто не узнает. А вдруг маска случайно спадет?

Также не стоит смешивать конфиденциальность с секретностью. Профессор Даниэль Вайцнер, директор Инициативы по исследованию политики интернета Массачусетского технологического института (MIT Internet Policy Research Initiative) и главный научный сотрудник Лаборатории информатики и искусственного интеллекта CSAIL объясняет разницу между ними так:

> *«Существует мнение, что конфиденциальность и секретность — синонимы. И если вы можете хранить личную информацию в секрете, то это и есть конфиденциальность. Если же вашу личную информацию хранят третьи лица, то вы утратили всю свою конфиденциальность».*

Вайцнер отвергает такой подход. Он считает, что защита конфиденциальности в эпоху цифровых технологий означает создание правил, которые требуют от правительств и предприятий прозрачности в отношении того, как они используют нашу информацию[1].

---

1 *If There's Privacy In The Digital Age, It Has A New Definition // NPR.org, 3 марта 2014.*

Репутация в цифровом мире

Репутация — или, на французский манер, реноме — это «закрепившееся определенное мнение о человеке или группе людей», сообщает нам Википедия. Как и в прежние времена, заработать хорошую репутацию все так же трудно, а испортить ее все так же легко — в этом смысле с приходом цифры ничего не изменилось.

Заработать хорошую репутацию все так же трудно, а испортить ее все так же легко.

Но есть одна важная деталь: люди по своей природе забывчивы, поэтому в прежние времена «все наши глупости и мелкие злодейства» могли сойти нам с рук. Теперь даже сущая ерунда, одно неудачное фото или резкая фраза могут если и не сломать жизнь, то хорошенько потрепать нервы, — люди очень по-разному понимают правила приличия и готовы затравить тех, кто, по их мнению, в эти правила не вписывается.

В фильме Алана Рене «Хиросима, любовь моя!» французская актриса приезжает в Японию на съемки и там знакомится с мужчиной-японцем. У них начинается роман, но суть не в этом: она впервые решается рассказать свою историю о том, как во время войны, будучи совсем молоденькой девочкой, влюбилась в немецкого солдата. Кончилось все печально: солдата убили, а ей не осталось другого выхода, кроме как бежать из своего родного городка в Париж, ибо репутация ее в глазах сограждан была загублена навечно. Хотя в чем она виновата? Судьба девушки и солдата почти в точности повторяет судьбу Ромео и Джульетты, с той только разницей, что на месте враждующих семей оказались враждующие страны, а «Джульетта» осталась жива. Что ждало ее, не решись она на побег? Ночной

разговор вдали от родины, на другом конце света, помог ей наконец-то пережить этот эпизод и найти силы жить дальше.

Если бы в 1945 году был интернет, то и в Париже героине не удалось бы скрыться. Обязательно нашелся бы какой-нибудь дотошный гражданин, который докопался бы до ее прошлого и окончательно поломал бы девушке жизнь. А уж в наше время то и дело встречаются бдительные товарищи, которые, как им кажется, стоят на страже общественной морали, хотя их никто на это место не назначал.

В январе 2019 года учительница из Барнаула разместила у себя в соцсети фото в купальнике. Сделала она это после заплыва в честь Универсиады в Красноярске, продемонстрировав свои медали и грамоту за участие в соревнованиях. Практически сразу вслед за этим учительница получила от директора школы настойчивое предложение уволиться: на нее пожаловалась мать одного из учеников, которой это фотография показалась вызывающей. История завершилась в целом благополучно: учителя по всей стране устроили флешмоб в поддержку коллеги и выложили фото в купальниках с хештегом #УчителяТожеЛюди; министр образования Алтайского края лично вступился за нее и предложил подыскать достойное место. Но учительница предпочла в школу не возвращаться.

Репутация — это не только сумма наших заслуг и проступков. Это еще продукт общественного мнения по их поводу, а нетерпимости и предрассудков и в наше время немногим меньше, чем в Средневековье. Что и говорить, мы не можем вести себя так, чтобы угодить всем тараканам в головах у разных людей, однако прежде, чем публиковать какие-то фото или что-то писать, стоит подумать о том, как это скажется на вашей репутации в будущем, ведь интернет

не только помнит все, он еще и сделал информацию доступной для всех и везде. И если раньше после какой-нибудь неприятной истории можно было переехать в другой город, где вас никто не знает, и начать жизнь с чистого листа, то теперь мы все живем в одной большой деревне под названием Земля, и деться с нее пока некуда.

Наверное, вы слышали про китайские эксперименты с социальным рейтингом, когда человеку за определенные проступки снижают баллы и, наоборот, поощряют за социально одобряемое поведение. Перевел бабушку через дорогу — заработал очко, не оплатил вовремя счета за коммунальные услуги — ушел в минус. А после некоторого порога начинают действовать ограничения: например, вам не продадут билет на самолет и придется добираться поездом в плацкарте. Можно по-разному относиться к этому эксперименту, но тенденцию он отражает точно.

> *Когда вся информация прозрачна, человеку надо осознанно относиться к управлению своей репутацией, и неважно, следит за ним какая-то государственная система или пока нет.*

Некоторые старшеклассники сами задумываются (и правильно делают) о том, что будущие работодатели обязательно посмотрят их страницы в соцсетях, и начинают более взвешенно принимать решения о том, что стоит публиковать, а что нет. Причем, нужно понимать, что полное отсутствие в Сети информации о человеке воспринимается как тревожный сигнал. Поэтому не стоит кидаться удалять свои страницы, если вам показалось, что они не соответствуют идеальному образу строителя цифрового будущего.

Так или иначе, не стоит забывать, что репутация — как осетрина: второй свежести у нее быть не может. А интернет только усиливает это свойство.

Переписка: почта и мессенджеры

Из тридцати томов полного собрания сочинений и писем А. П. Чехова письма составляют двенадцать томов — немногим менее половины всего им написанного.

> *Вступительный текст от редакции сообщает нам: письма Чехова представляют собой одно из самых значительных эпистолярных собраний в литературном наследии русских классиков. Всего сохранилось около 4400 писем, написанных в течение 29 лет — с 1875 по 1904 год.*
>
> *Эти двенадцать томов — своеобразное документальное повествование Чехова о своей жизни и творчестве. Но познавательное значение его писем шире их биографической ценности: в них бьется пульс всей культурной и общественной жизни России конца XIX — первых лет XX века.*
>
> *Тематика эпистолярного наследия Чехова многообразна: от дневников путешествий и календарей работы над произведениями до событий личной жизни, литературных связей, от заметок об общении с театральными деятелями и отзывов на критику до советов начинающим авторам.*

В наше время бумажных писем практически никто не пишет, кроме как в официальные инстанции, да и те активно переходят на цифровые форматы. Но и в электронных письмах точно так же бьется пульс эпохи и живут наши личные истории — любови, ссоры, обиды, бытовые дела, забавные глупости, просьбы, напоминания о встречах, планы, отчеты, претензии, благодарности, поздравления, офисные интриги и много-много рабочей рутины.

По объему переписки мы сегодня, пожалуй, превосходим Антона Павловича. Вот у меня, например, в почтовом ящике Gmail хранится более 8 тысяч отправленных писем, начиная с 2007 года. Я отнюдь не претендую на то, что мое эпистолярное наследие будет достойно изучения, однако потерять в одночасье весь этот накопленный багаж мне было бы жаль.

> *В письмах закопано много ценной информации — имена, адреса, телефоны, документы, интересные ссылки, важные договоренности, да и просто разные памятные моменты.*

Электронная почта сегодня не в чести, ее место заняли чаты и мессенджеры, но суть от этого не меняется: история общения с другими людьми все так же представляет для нас ценность. Пусть даже почта как формат общения считается устаревшей, но адрес почтового ящика часто используется в качестве логина и для подтверждения различных действий. Например, если вы забыли пароль к какому-то сервису, то, скорее всего, для его восстановления вам на email придет специальная ссылка. Так что отправлять электронную почту на покой было бы преждевременно.

Это так же хорошо понимают и хакеры, поэтому мы регулярно видим новости о массивных утечках паролей к электронной почте, а черный рынок услуг по взлому почтовых ящиков на заказ процветает. Если вы не какая-то знаменитость, то едва ли хакерам интересны ваши письма сами по себе. Но покопавшись хорошенько в чьей-нибудь почте, можно выудить оттуда «явки и адреса» — параметры доступа к различным ресурсам, которыми человек пользуется. Поэтому к защите почтовых ящиков — как своих, так и детских — надо отнестись со всей серьезностью.

К защите почтовых ящиков — как своих, так и детских — надо отнестись со всей серьезностью.

Кроме того, рекламщики охотятся за «чистыми» почтовыми адресами, которые еще не засветились в спам-рассылках. Если им удастся заполучить ваш пароль, они с удовольствием будут рассылать от вашего имени свой мусор на адреса ваших друзей, да и просто случайным людям. Потом кто-нибудь пожалуется на спам и ваш ящик заблокируют.

С мессенджерами история аналогичная: формат изменился, но суть осталась прежней. То есть все, сказанное выше про электронную почту, применимо и к более современным каналам коммуникаций — Skype, WhatsApp, Viber, Facebook Messenger, Telegram и др. Причем, благодаря большей интерактивности мессенджеров и эмоциональной вовлеченности, здесь чаще срабатывают банальные «разводки» — вроде такой, когда со взломанного аккаунта вашего знакомого просят срочно перевести деньги на какое-то важное дело. Увы, многие попадаются на эту удочку. Некоторые хозяева таких взломанных аккаунтов переживают подобные казусы настолько сильно, что готовы даже вернуть друзьям деньги, которые у них выманили злоумышленники, хотя их вины в этом нет. В любом случае, ситуация неприятная и лучше подумать о защите, чтобы в нее не попадать.

Персональные цифровые коллекции

Еще совсем недавно по обычным меркам времени, то есть лет десять назад, мы старательно собирали свои цифровые коллекции музыки, фильмов, книг и программ, гордились ими, делились этими сокрови-

щами с друзьями и тщательно берегли. Причем делиться тогда значило не просто нажать кнопку «Поделиться», а взять с собой пустых болванок CD или DVD и поехать к другу домой, чтобы переписать себе что-нибудь интересное.

Сегодня интернет практически обнулил ценность таких персональных коллекций, если они только не содержат уж совсем эксклюзивные материалы. Нам стало проще погуглить, чем искать вдруг понадобившийся файл в своих закромах.

Кстати, в отношении к персональным цифровым коллекциям четко прослеживается граница поколений: «игреки» еще помнят, что это имело ценность, и по привычке держат подборки любимых фильмов и музыки на собственных носителях, а «зеты» твердо уверены, что в любой момент найдут все, что нужно, на каком-нибудь ресурсе в интернете. Поэтому вместо коллекции файлов теперь держат коллекции ссылок — это еще и более экологично: вместо сотен миллионов копий популярных видеоклипов на жестком диске или флешке, на YouTube есть всего одна копия, которую все могут посмотреть. (Технически копий исходного ролика больше, но по суммарному объему это все равно на много порядков меньше, чем было бы в личных хранилищах).

> *Единственный вид коллекций, который с приходом тотальной цифровизации и вездесущего интернета не только не увял, а, наоборот, расцвел — это коллекции фотографий.*

Фотографируют теперь все, от мала до велика, и надо что-то с этим богатством делать, чтобы не потерять. О тех, для кого фотография стала серьезным хобби, можно не беспокоиться: они-то знают, как уберечь свои снимки от любых катастроф. А вот всем остальным не так оче-

видно, каким образом лучше организовать свой фотоархив. Память телефона забивается быстро, и, хочешь не хочешь, а придется учиться копировать фотографии в облако — на сегодня это самое адекватное решение для обычных пользователей. Как ни странно, для многих это все еще представляет сложность, причем даже для юного поколения, которое с гаджетами на «ты».

Виртуальные вещи

Звонок в полицию: «Помогите! У меня украли танк!» — «Какой танк?!» — «ИС-4!»[1]

Вы, конечно же, догадались, что это был не настоящий танк, а виртуальный. Кто-то взломал аккаунт игрока в игре World of Tanks и угнал боевую машину. Несмотря на то, что танк виртуальный, потеря человека вполне реальна: игровое оборудование стоит немалых денег, и чужой танк можно продать, выручив за него кругленькую сумму.

> *По данным исследования Newzoo, российские геймеры за 2019 год потратили более 2 миллиардов долларов[2], а согласно прогнозу аналитического центра по игровой индустрии Superdata, Россия в 2020 году выйдет на третье место в Европе, потеснив Францию[3].*

---

1 *Похитители танков. // Российская газета, 16 сентября 2019.*

2 *The russian game market. // Allcorrect Group, 22 мая 2020.*

3 *Russia to Become the Third Biggest European Market for Video Games // Superdata, 22 ноября 2020.*

Пока с точки зрения российского законодательства виртуальные вещи, используемые в игровых мирах, имуществом не считаются, а это значит, что их присвоение не квалифицируется как кража. Тем не менее, иногда пострадавшие все-таки обращаются в полицию; бывает даже такое, что виртуальных воров находят и возвращают украденное хозяину. Для нарушителя наступает ответственность по ст. 272 УК РФ за неправомерный доступ к компьютерной информации как за деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности. Светит ему за это крупный штраф или даже реальный срок.

Очевидно, что в дальнейшем количество виртуального имущества будет только расти, и придется учиться принимать меры по его охране от всевозможных посягательств: будут развиваться способы безопасной продажи и обмена виртуальных вещей и так далее.

> *Масштабы некоторых сделок уже сейчас поражают воображение. Так, например, планета Calypso в игровой вселенной Entropia Universe была продана за 6 миллионов долларов. В той же вселенной космический курорт Club Neverdie нашел нового владельца за 635 тысяч долларов, а в игре Second Life за 50 тысяч долларов продали город Амстердам (точнее, его виртуальную копию). Еще одной из громких сделок стала продажа «эфирной розовой боевой собаки» (Ethereal Flames Pink War Dog) в игре Dota 2 (кстати, сейчас собачка подешевела и оценивается всего в 4 тысячи баксов).*

Потерять свои виртуальные богатства можно по двум причинам: либо кто-то взломал ваш аккаунт, либо вы захотели купить, продать или обменять какой-то предмет, а вам попался жулик. Чтобы уберечь аккаунт, следуйте стандартным советам: используйте

сложные пароли, никому их не передавайте, не используйте один и тот же пароль для почты и аккаунта Steam, включите дополнительную защиту Steam Guard, остерегайтесь фишинга, не забывайте про антивирус. Особенно будьте осмотрительны в контактах с незнакомцами — бывает, что кто-то предлагает вам поиграть за их команду на турнире и кидает ссылку на якобы голосовой чат, чтобы вы могли общаться, — а там оказывается стилер — программа, ворующая пароли.

Необязательно быть обладателем уникального артефакта. Злоумышленников интересуют аккаунты, стоимость инвентаря на которых составляет всего 5-10 тысяч рублей. Получив ваш пароль, они перехватывают управление, привязывают аккаунт к своей почте, а затем распродают ценный инвентарь или ищут покупателя на аккаунт целиком, если у вас достаточно «прокачанный» персонаж.

Кстати, по этой причине следует крайне осмотрительно относиться к покупке готового аккаунта — он вполне может оказаться краденым, и если через некоторое время его найдут, то вернут законному владельцу, а вас забанят. Несомненно, есть и добросовестные продавцы, но будьте бдительны.

Следует крайне осмотрительно относиться к покупке готового аккаунта — он вполне может оказаться краденым.

Вторая ситуация связана с риском мошенничества при сделках с игровым инвентарем. Для каждого из виртуальных миров существуют свои торговые площадки, где игроки обмениваются оружием, магическими предметами, украшениями и прочими вещами. Как и в реальном мире, например, на Avito, здесь можно нарваться

на жуликов — как на стороне продавцов, так и на стороне покупателей. И точно также есть риск, что вам «впарят» какую-нибудь бесполезную ерунду по цене самолета — сделка пройдет без нарушений, но все равно вы останетесь обманутым.

К сожалению, эти виртуальные рынки еще слабо регулируются законодательством, так что надеяться здесь можно только на себя. Юристы работают над тем, чтобы ввести понятие виртуального актива, что повысило бы правовую защищенность игроков, но что и когда им удастся сделать — неизвестно.

Контакты и заметки

В магазине канцтоваров все еще можно купить телефонные записные книжки, хотя это, скорее, дань традиции, чем товар повседневного спроса. Большинство таких книжек них имеют формат А4 или А5, то есть представляют собой эдакий настольный вариант, а отнюдь не карманный. Карманные телефонные книжки тоже еще можно найти в продаже — некоторые в обложке из натуральной кожи, на хорошей бумаге и с золотым обрезом — отличный сувенир, ничуть не хуже берестяных грамот.

Реальной записной книжкой стал мобильный телефон, и сдавать позиции он не собирается.

А реальной записной книжкой стал мобильный телефон, и сдавать позиции он не собирается. Именно в телефоне у большинства людей хранятся все списки контактов и адреса, туда же заносятся важные заметки. К счастью, наши электронные записные книжки

в мобильных устройствах практически по умолчанию синхронизируются с облачными хранилищами Apple или Google (а может, и обоих сразу), так что потерять эти данные стало почти невозможно — если только вы специально не отключите опции резервного копирования.

Но при этом появляется другой риск — можно потерять контроль над своим аккаунтом, и тогда это будет большой проблемой, потому что все контакты тоже будут утеряны. (Есть еще соцсети, но пока еще это не 100-процентное перекрытие — не все наши контакты имеют профиль в соцсети). Дублирующих записей на бумаге уже никто не ведет, наизусть телефоны не помнит (иногда даже свой собственный). То есть можно констатировать, что в части хранения контактов произошла полная цифровизация. Даже бабушки и дедушки, все еще опасающиеся смартфонов, держат личный телефонный справочник в своем старомодном мобильнике с кнопками.

Список контактов в телефоне — лакомая цель для хакеров. Заполучив его, они могут делать рассылки вашим знакомым от вашего имени.

Список контактов в телефоне — лакомая цель для хакеров. Заполучив его, они могут делать рассылки вашим знакомым от вашего имени, что сразу повышает уровень доверия к полученной информации (на самом деле — дезинформации) — и человек кликает на присланную ссылку или открывает вредоносный файл. Или того хуже: мошенники начинают просить помощи от вашего имени, а ваши доверчивые друзья переводят им деньги. Чаще всего это срабатывает с самыми близкими людьми, особенно с нашими пожилыми родственниками.

Домены (имена сайтов)

Регистрация доменного имени (то есть названия сайта) в среднем стоит около 500 рублей в год. Но это имя может стать очень дорогим активом и яблоком раздора, если оно прибрело в интернете популярность. Как вы думаете, сколько стоит домен apple.com? Даже предположить трудно. Короткий или запоминающийся интернет-адрес может стоить тысячи или даже миллионы долларов.

Короткий или запоминающийся интернет-адрес может стоить тысячи или даже миллионы долларов.

Говорят, Facebook заплатил 8,5 миллионов долларов за покупку домена Fb.com в 2010 году, а сколько он стоит сейчас, можно только гадать. Впрочем, такое уже не продается, как и «Мона Лиза» Леонардо да Винчи. Название сайта становится важной частью идентичности компании, и его утрата может иметь катастрофические последствия для бизнеса. Из-за доменов порой разгораются настоящие баталии.

Так случилось в штате Айова в 2017 году[1]. Вооруженный пистолетом мужчина по имени Шерман Хопкинс ворвался в дом 26-летнего веб-предпринимателя Итана Дейо и потребовал перенести домен doitforstate.com на другой аккаунт. Завязалась борьба, Дейо был ранен в ногу, но в итоге получил

---

1 *Сейчас сайт doitforstate.com закрыт. Его имя «Do it for state» — сделай это для штата (или страны) — популярный мем, появившийся в Университете штата Айова. Возможно, у преступника были на него свои планы, но органы следствия не дали об этом информации.*

The Guy Who Robbed Someone at Gunpoint for a Domain Name Is Getting 20Years in Jail. // Vice.com, 15 июня 2018.

контроль над огнестрельным оружием и несколько раз выстрелил Хопкинсу в грудь. Нападавшего удалось спасти, он в итоге предстал перед судом и получил 20 лет тюрьмы.

До стрельбы в Айове дело дошло впервые, но кража (или как говорят «угон» домена) — дело вполне обычное. Кража доменного имени происходит, когда злоумышленник подделывает регистрационные данные жертвы и передает домен другому человеку, отнимая его, таким образом, у законного владельца и приобретая над ним полный административный и операционный контроль.

Причины, по которым это становится возможным, все те же: слабые пароли, шпионское ПО и социальная инженерия. Если вы были слишком беспечны, и преступнику в результате удалось действовать от вашего имени, то доказать, что это были не вы, будет трудно. Краденые домены часто «отмывают», устраивая серию передач между новыми владельцами и запутывая следы. К сожалению, регистраторы и полиция редко помогают в таких ситуациях, потому что доменные имена не рассматриваются как физическая собственность.

Впрочем, случаются редкие исключения. Альберт Ангел купил сайт P2P.com за 160 тысяч долларов в июле 2005 года в качестве инвестиций, но год спустя сайт был украден. Альберт сообщил о краже в полицию Майами-Дейд, и к нему отправили офицера. В результате следствие вышло на Дэниела Гонсалвеса, 25-летнего компьютерного специалиста из Нью-Джерси, и обвинило того в краже P2P.com путем взлома почтового аккаунта Ангела. В 2011 году Гонсалвес признал себя виновным и был приговорен к пяти

годам тюремного заключения. Этот случай считается единственным уголовным приговором за кражу домена[1].

Но чаще всего и красть ничего не нужно. Владельцы просто забывают продлить регистрацию, и домен становится бесхозным. В такой момент его могут легко у вас перехватить, чтобы потом потребовать выкуп. Или просто ваш раскрученный домен купит кто-то другой и будет использовать для своего сайта.

Цифровые ресурсы

В больших городах почти у каждого в квартире есть wi-fi. Сегодня мы пользуемся безлимитным высокоскоростным интернетом, а еще не так давно трафик был достаточно дорогим, и каждый мегабайт был на счету. В то время процветал вид мошенничества, связанный с воровством трафика, — кто-то из технически продвинутых соседей взламывал ваш роутер и за ваш счет пользовался интернетом. Сейчас едва ли будет актуально ломать чужую сеть, чтобы сэкономить 300-500 рублей в месяц, но у хакера могут быть и другие мотивы: например, если он совершит какие-то противоправные действия через ваш роутер, то полиция и ФСБ, разыскивая его, придут к вам. Так что позиция по отношению к wi-fi «пусть пользуются все, мне не жалко» весьма уязвима — свои цифровые ресурсы нужно защищать.

Кроме канала доступа в интернет к цифровым ресурсам можно отнести место на дисках в облачных хранилищах, пакеты минут

1 *When Hackers Steal A Web Address, Few Owners Ever Get It Back // Huffington Post, 29 сентября 2014.*

и SMS на телефоне, подписки на кино и ТВ и так далее. В результате взлома ваших аккаунтов вы рискуете все это потерять. Скажем, некто может получить доступ к вашему личному кабинету мобильного телефона и продать ваши накопленные гигабайты интернета на бирже, как это позволяет делать Tele2.

Автомобиль

Про автомобиль Tesla говорят, что это компьютер на колесах. Так оно и есть. И весь мировой автопром уверенно катится в том же направлении — ко все большей компьютеризации транспортных средств. Бортовой компьютер есть во всех современных машинах, а пройдет немного времени — и все автомобили, едущие по дорогам, окажутся подключенными к интернету. Зачем это нужно? Вовсе не ради того, чтобы передать картинку на экран навигатора, — с этим справляется и обычный смартфон. Прежде всего, подключенность нужна для повышения безопасности движения. Подключенный автомобиль будет оперативно обновлять свои управляющие программы и сообщать производителю технические параметры систем и агрегатов, а тот, в свою очередь, на основе статистических данных, собираемых со всех машин, сможет прогнозировать возникновение отказов и рекомендовать ремонт. В авиации это делается уже повсеместно, теперь очередь за автотранспортом.

У любой — даже золотой — медали есть обратная сторона.

Но у любой — даже золотой — медали есть обратная сторона. Наличие в автомобиле компьютера, который управляет всеми системами, да еще подключенного к сети, делает такой автомобиль

приманкой для хакеров. «Взлом машины — это прямая угроза для жизни ее владельца. Если злоумышленник получил удаленный доступ к автомобилю, это значит, что он может включить или выключить любую систему в любое время: повернуть руль, нажать на газ или тормоза, выключить фары», — говорит эксперт Лаборатории Касперского Денис Легезо, и в качестве примера приводит эксперимент американских исследователей со взломом Jeep Cherokee.

> *На момент начала атаки жертва хакеров ехала со скоростью 110 км/ч по автостраде в центре города Сент-Луис. «Пока два взломщика удаленно играли с кондиционером, радио и стеклоочистителями, я гордился своим самообладанием. И в этот момент они добрались до коробки передач», — пишет журналист Wired, который находился за рулем взломанной машины.*
>
> *Злоумышленники в результате получили контроль над акселератором и тормозной системой машины, а также стеклоочистителями и клаксоном. Для того чтобы удаленно управлять автомобилем, им понадобилось всего-то взломать мультимедийную систему Uconnect через сотовое соединение.*
>
> *«Таким образом можно добраться до машины, несущейся по шоссе где-то по стране, далеко от взломщика. Вот она, поворотная точка, после которой удаленный взлом автомобиля становится реальностью», — отмечает обозреватель издания.*

Этот эксперимент получил широкую огласку, и владельцы таких машин сильно обеспокоились. Автопроизводитель Fiat Chrysler оперативно исправил программное обеспечение, чтобы обезопасить

своих клиентов, и предложил им посетить дилеров для апгрейда ПО, либо скачать его с официального сайта компании. Но сколько еще уязвимостей наверняка прячутся в автомобильных системах?

Короче говоря, автомобили дружной толпой вошли в семью кибервещей, со всеми вытекающими отсюда плюсами и минусами.

Умный дом

Фантастика тихой сапой проникает в жизнь: наши дома все больше наполняются разнообразными умными устройствами, призванными сделать их уютнее, избавить нас от бытовых хлопот, волнений о том, выключен ли утюг, достаточно ли продуктов в холодильнике и какой фильм посмотреть сегодня вечером. Умная дверь откроется сама, узнав вас по лицу или по голосу, термостат настроит комфортную температуру вашего жилища, подумав также и об экономии ваших финансов, а ваш ужин будет автоматически приготовлен и подан к столу роботом-поваром.

Система безопасности, позволяющая отслеживать появление посторонних людей и предметов, обеспечит ваше спокойствие, а также позволит вести удаленный видеоконтроль за маленькими детьми и пожилыми людьми. На случай длительного отъезда может включаться режим симуляции присутствия хозяина, чтобы не давать ворам повода нанести вам визит.

> *Пока настоящий умный дом — это дорогая игрушка для обеспеченных людей, но будьте уверены: революция в домашнем хозяйстве пройдет незаметно и быстро. Роботом-пылесосом*

и сейчас уже никого не удивишь, а скоро все новые модели бытовых приборов начнут выпускать со встроенными «мозгами».

Все эти устройства будут автоматически подключаться к домашнему центру управления. Инженерные системы зданий тоже стремительно умнеют, и неизбежно с какого-то момента в новых домах начнут устанавливать все необходимые датчики сразу при постройке.

В принципе, ничего особо фантастического в этом нет: концепция «умного дома» была впервые сформулирована в 1984 году Американской Ассоциацией Домостроителей, и, по сути, является развитием тенденции улучшения условий жизни при помощи техники, возникшей с появлением электрических приборов в начале 1900-х годов. С приходом в дом компьютеров появилась возможность наладить согласованное управление устройствами и системами, а интернет добавил к этому связь с внешним миром — и теперь у каждой кофеварки есть шанс заявить этому миру о себе.

Теперь у каждой кофеварки есть шанс заявить этому миру о себе.

Кстати, именно с кофеварок все и началось. В 1991 году появился первый веб-сайт, и тогда же в Кембриджском университете в Соединенном Королевстве впервые применили веб-камеру, чтобы наблюдать за работой кофеварки, которая находилась в одной из компьютерных лабораторий. Теперь ученые точно знали, когда подойти за свежесваренным кофе.

Рэй Брэдбери превосходно описал умный дом в коротком и жестком рассказе «Будет ласковый дождь...», опубликованном еще в 1950 году.

«В гостиной говорящие часы настойчиво пели: тик-так, семь часов, семь утра, вставать пора! — словно боясь, что их никто не послушает. Объятый утренней тишиной, дом был пуст. Часы продолжали тикать и твердили, твердили свое в пустоту: девять минут восьмого, к завтраку все готово, девять минут восьмого!

На кухне печь сипло вздохнула и исторгла из своего жаркого чрева восемь безупречно поджаренных тостов, четыре глазуньи, шестнадцать ломтиков бекона, две чашки кофе и два стакана холодного молока.

— Сегодня в городе Эллендейле, штат Калифорния, четвертое августа две тысячи двадцать шестого года, — произнес другой голос, с потолка кухни. Он повторил число трижды, чтобы получше запомнили. — Сегодня день рождения мистера Фезерстоуна. Годовщина свадьбы Тилиты. Подошел срок страхового взноса, пора платить за воду, газ, свет».

В рассказе все закончилось для людей плохо: случилась атомная война и никто не выжил, а умный дом случайно уцелел и продолжал функционировать, как ни в чем ни бывало. (Похоже только, что у дома вышли из строя датчики присутствия хозяев — иначе зачем бы готовить завтрак, если никого нет?)

Однако совсем необязательно нужна глобальная катастрофа, чтобы внести разлад в слаженную работу маленьких автоматических помощников. Это могут сделать хакеры, и сценарий может оказаться хоть и не столь трагичным, как у Бредбери, но весьма и весьма неприятным.

Вы подходите к двери, а она не открывается: система «забыла» ваше лицо и рисунок сетчатки. Конечно, вы понимали, что такое может случиться, поэтому у вас с собой всегда есть обычный ключ. Открыв дверь, вы неожиданно оказываетесь в темном помещении. Внутри холодно, потому что отопление не включилось за два часа до вашего прихода, как вы его запрограммировали.

Через несколько секунд начинает трезвонить умная сигнализация, считая, что в дом проник посторонний, хотя она должна была определить присутствие смартфона и отключиться. Наконец вы замечаете, что хоть что-то работает: телевизор включен. Но только показывает он странное: на экран выведено видео в реальном времени с умной камеры на потолке, следящей за вами. А за окном слышны сирены мчащихся к дому пожарных и полиции. Да что же такое стряслось? Ничего особенного, все просто: ваш умный дом кто-то взломал.

Подобного развития событий можно ожидать, если кто-то получит доступ к контроллеру, который управляет всеми приборами и устройствами вашего умного дома. Эксперт «Лаборатории Касперского» Владимир Дащенко показал на выставке Mobile World Congress 2018, что сделать это довольно просто[1], и такой сценарий вполне вероятен. Дело в том, что при разработке систем умного дома их авторы много думали о комфорте и почти совсем не думали о безопасности, поэтому взламываются они относительно легко (по сравнению, например, с банковскими системами).

1 *Апокалипсис в умном доме // Блог Kaspersky Daily, 28 февраля 2018.*

При разработке систем умного дома их авторы много думали о комфорте и почти совсем не думали о безопасности.

Тем не менее, оснований для паники нет (ну, или пока нет): умные дома еще не стали мишенью для массовых атак злоумышленников, потому что не очень понятно, какую выгоду из такой операции можно извлечь. Допустим, кто-то получил контроль над вашей умной лампочкой и теперь балуется, включая и выключая свет, когда ему вздумается. Чтобы прекратить атаку, вам достаточно вывернуть эту лампочку и вкрутить обычную. Аналогичным образом можно поступить и с остальными приборами — просто перейти на ручной режим, пока проблема не будет устранена. Все же, обычный дом — не атомная станция, в нем нет таких систем, вмешательство в работу которых может иметь серьезные последствия. Максимум, чего добьются хакеры своими действиями, — вашего раздражения временными неудобствами.

Поэтому они предпочитают действовать другим образом: получив контроль над устройствами умного дома, формируют из них ботнет[1], с помощью которого могут в любой момент организовать DDoS-атаку.

Именно так и случилось в октябре 2016 года, когда без доступа в интернет осталась большая часть пользо-

1 *Ботнет — это набор компьютеров или умных устройств, подключенных к интернету, — «ботов», которые находятся под удаленным управлением какой-либо внешней стороны. Обычно эти компьютеры скомпрометированы злоумышленником, который управляет их функционированием без ведома владельцев.*

вателей на Восточном побережье США. В атаке участвовали миллионы устройств, она была столь масштабной, что власти готовы были заподозрить действия враждебного государства, но, как потом выяснилось, на самом деле это была работа гигантского ботнета Mirai (по-японски — «будущее»). В отличие от других ботнетов, которые обычно состоят из компьютеров, Mirai включал в себя множество устройств так называемого «интернета вещей» (IoT) — цифровых камер и видеопроигрывателей. Потом появились ботнеты, в состав которых входят роутеры, «умные» лампочки, розетки, датчики движения, выключатели, камеры наблюдения и другие гаджеты — настоящие пехотинцы DDoS-атак, которые просто-таки бомбардируют веб-трафиком целевой сервер до тех пор, пока он не будет перегружен и автоматически отключен. По состоянию на август 2019 года в интернете насчитывалось почти 27 миллиардов таких «вещей», и большинство из них может стать легкой добычей хакеров[1].

Персонально для владельца умного дома это опасности не представляет: ну, подумаешь, — ваша лампочка посылает запросы на какой-то сервер! Хозяин лампочки за ее действия ответственности не несет (правда, если сумеет доказать, что это не он ее так запрограммировал). И уж коль скоро уязвимость домашних умных устройств (не только лампочек, естественно) попала в фокус внимания, то какое-то решение проблемы будет найдено, и производители начнут выпускать более защи-

1 *Number of Internet of Things (IoT) Connected Devices Worldwide 2020: Breakdowns, Growth & Predictions // Finances Online, 2019.*

щенные модели. В общем, нет серьезных причин отказываться от благ цивилизации из-за наличия подобных угроз.

Но одно исключение, пожалуй, есть: камеры видеонаблюдения.

> *Шалости хакеров могут быть отнюдь небезобидны, если они получат доступ к видеопотоку из вашего дома. В лучшем случае они выложат ролики со взломанных камер на YouTube, чтобы получить свою минуту славы. Но если взломщик узнает ваши персональные данные, то у него может появиться желание шантажировать вас под угрозой публикации видео.*

Этому риску чаще подвергаются известные люди, хотя и обычные граждане от него не застрахованы.

Иногда ситуация принимает более угрожающий характер. Однажды хакеры взломали видеокамеру на ноутбуке, который стоял в комнате маленького ребенка. Родители ставили ему на ночь мультики, ребенок засыпал, а компьютер потом сам переходил в спящий режим. Все было хорошо, пока мальчик не стал жаловаться, что в его комнате кто-то есть и разговаривает с ним. Родители сначала не поверили: ну да, все дети боятся темноты и воображают невесть что! Но ребенок плакал и ни за что не хотел оставаться в своей комнате. Хорошо, что взрослые все-таки поняли, что происходит нечто ненормальное, и отнеслись к словам малыша внимательно. Оказалось, действительно кто-то развлекался тем, что пугал ребенка по ночам: видя через камеру, что мальчик уснул, включал зловещие звуки и показывал на экране страшные картинки. А ког-

да малыш бежал звать взрослых, тут же все гасил, — и ребенку, естественно, не верили. Такое «баловство» может довести и до серьезного невроза.

Современные IP-камеры, используемые в системах домашнего видеонаблюдения, оснащены также микрофоном и динамиком, поэтому они вполне могут быть использованы в подобных сценариях — совсем необязательно, чтобы в детской комнате стоял настоящий компьютер.

К сожалению, на текущий момент риск взлома видеокамер остается высоким. Чтобы его свести к минимуму, нужно следовать довольно простым правилам:

- Во-первых, всегда обновлять прошивки камер и ставить сложные пароли для доступа к ним, а заодно почаще эти пароли менять. Как это сделать, обычно описано в руководстве пользователя каждой такой камеры. Это минимальные необходимые меры защиты;

- Во-вторых, всегда отключать неиспользуемые функции. В первую очередь это касается разнообразных «облачных» сервисов, которыми оснащается все большее число камер;

- В-третьих, если вы достаточно хорошо подкованы в техническом плане, можно сделать еще кое-что. Например, включить HTTPS-доступ к камере[1].

1 *Веб-камера против человека. // Блог Kaspersky Daily, 20 февраля 2017.*

Контрольные вопросы

1. Назовите, что ценного есть у вас в цифровом виде.
2. Какими способами преступники крадут цифровые деньги?
3. Зачем воровать мили и бонусы?
4. Чем опасны утечки персональных данных?
5. Почему нам так дороги наши аккаунты в соцсетях?
6. Как защитить свои авторские права в интернете?
7. В чем разница между конфиденциальностью и анонимностью?
8. Как заботиться о своей цифровой репутации?
9. Храните ли вы старые электронные письма и сообщения? Почему?
10. Какие у вас есть цифровые коллекции?
11. Есть ли у вас виртуальные вещи? Как их могут украсть?
12. Почему списки контактов для нас ценны? Зачем они хакерам?
13. Что такое доменное имя? Почему оно имеет ценность?

14. Почему надо защищать свой wi-fi?

15. Что хакеры могут сделать с компьютеризированным автомобилем?

16. Чем хакеры могут угрожать умному дому?

Глава 3

Пароли, пароли, пароли...

В этой главе мы поговорим о паролях — как правильно с ними обращаться, где хранить и зачем их нужно регулярно менять. Узнаем, какие пароли надежны, а какие нет и почему. Научимся придумывать и запоминать надежные пароли.

Театр начинается с вешалки, а безопасность в компьютерных системах — с пароля[1]. Приходя в театр, вы сдаете в гардероб только одно пальто и получаете один номерок, за утерю которого администрация вам грозит штрафом. А современному пользователю компьютерными системами приходится хранить как минимум несколько десятков паролей, и потерять их проще простого. Если каждый пароль представить театральным номерком, их наберется целая куча — ни в карман положить, ни в руках удержать. Осталось только нанизать их на веревочку и повесить на шею.

Хотя пароли — это всего лишь набор символов, и они не будут брящать у вас на шее или оттопыривать карман, с ними придет другая проблема — их необходимо помнить. Поэтому многие люди, чтобы не напрягать память, выбирают очень простые комбинации в качестве секретного ключа, и начинают применять один и тот же пароль во всех используемых системах.

> *Корпорация SplashData регулярно публикует список 100 самых ненадежных паролей года, и уже несколько лет подряд первое место занимает пароль «123456». Его используют около 17 % пользователей. На втором месте — пароль «password», да и другие популярные пароли ненамного сложнее.*

Для защиты телефона часто используется ПИН-код[2], состоящий из четырех цифр, — это тоже пароль. Увы, и здесь пользователи

---

1 *Пароль (фр. parole — слово) — условное слово или набор символов, предназначенный для подтверждения личности или полномочий. Для входа в разные компьютерные системы используется комбинация — имя пользователя (логин) и пароль.*

2 *ПИН — персональный идентификационный номер (PIN — Personal Identification Number). Чаще всего это — комбинация из четырех цифр, которая представляет собой пароль для доступа к устройству или банковской карте.*

не блещут фантазией, склоняясь в пользу примитивных вариантов. Недавно отдел исследований киберугроз и уязвимостей компании Splunk опубликовал список наиболее часто используемых ПИН-кодов, который выглядит следующим образом: 1234, 1111, 0000, 1212, 7777, 1004, 2000, 4444, 2222, 6969, 9999, 3333, 5555, 6666, 1122, 1313, 8888, 4321, 2001, 1010.

С его помощью можно взломать 26% всех смартфонов.

Не лучше обстоит дело и с графическими ключами Android Lock Pattern (ALP). ALP может содержать от четырех до девяти узлов, что суммарно дает 389,112 возможных комбинаций. Также как в случае с обычными паролями, число комбинаций возрастает экспоненциально вместе с длиной графического ключа. И точно так же люди чаще всего выбирают самые примитивные варианты, которые им проще запомнить, а хакерам — проще подобрать.

Норвежская исследовательница Марте Лёге (Marte Løge) проанализировала относительно небольшую базу из 4000 ключей ALP и получила весьма интересные результаты:

- *44% ALP начинаются из верхнего левого узла;*
- *77% начинаются в одном из четырех углов экрана;*
- *5 — среднее число задействованных в графическом пароле узлов, то есть взломщику придется перебрать менее 8000 комбинаций;*
- *во многих случаях графический пароль состоит из 4 узлов, а это уже менее 1624 комбинаций;*

- *чаще всего ALP вводят слева направо и сверху вниз, что тоже значительно облегчает подбор.*

  Более 10% полученных Лёге паролей оказались обычным буквами, которые пользователи чертили на экране. Хуже того, почти всегда выяснялось, что это не просто буква, но первая буква имени опрошенного, его супруга или супруги, ребенка и так далее.

  Как сделать графический пароль более сложным? Во-первых, в графическом ключе стоит использовать большее количество узлов. Во-вторых, стоит добавить пересечений. Они усложняют хакерам подбор комбинации и могут запутать злоумышленника, если тот решит подсмотреть пароль через плечо жертвы. В-третьих, стоит отключить опцию «показывать паттерн» в настройках безопасности Android: если линии между точками не будут отображаться на экране, подсмотреть ваш пароль станет еще сложнее[1].

Если ваш графический пароль подсмотрит случайный попутчик в метро, это, по большому счету, не страшно. Ведь чтобы воспользоваться увиденным, наблюдательному попутчику еще нужно украсть у вас телефон. Другое дело, когда секретным «узором» завладевает человек, потенциально имеющий доступ к телефону жертвы, — например, кто-то из одноклассников вашего ребенка. Узнав пароль, он может от имени владельца телефона написать что-то в соцсети — оскорбить, поссорить, выставить в неприятном свете или даже опубликовать нечто противозаконное. Потом будет крайне трудно доказать, что это сделал не ваш ребенок.

---

1 *Графические ключи так же предсказуемы, как пароли «123456» и «password» // Журнал «Хакер», 21 августа 2015.*

То, с чем не справится человек, легко сделает искусственный интеллект: он проанализирует ваши движения и распознает пароль.

К сожалению, даже сложный графический пароль не всегда способен остановить злоумышленника. То, с чем не справится человек, легко сделает искусственный интеллект: он проанализирует ваши движения и распознает пароль. Пока такие исследования проводятся только в лабораториях университетов, но завтра хакерские инструменты могут появиться в открытом доступе.

> *Группа исследователей из Университета Ланкастера, Университета Бата и Северо-Западного университета Китая разработала программное обеспечение, способное расшифровать ваши движения пальцем по экрану с потрясающей точностью. В ходе тестирования исследователи смогли взломать 95% графических паролей Android за пять попыток — до того, как операционная система заблокировала дальнейшие действия.*
>
> *Все, что нужно было сделать команде исследователей, это снять «скрытой камерой», как пользователь разблокировал свой телефон. Причем для этого экспериментаторам не понадобилась какая-то спецтехника — стандартной камеры смартфона оказалось более чем достаточно.*
>
> *Как заявили в Google, визуальное хакерство стало одной из причин, согласно которой в Android была добавлена функция SmartLock, «снижающая частоту, с которой пользователям необходимо вводить свой ПИН-код / пароль / графический шаблон, и поэтому затрудняющая проведение подобных атак»[1].*

1 *Your Android Pattern Lock Could Be Incredibly Easy To Crack // Forbes, 23 января 2017.*

Эти и другие исследования показывают, что пользователи крайне беспечно относятся к защите своей информации, даже зная, что она представляет значительную ценность. А беспечность, вошедшая в привычку, многократно повышает ваши риски. Именно поэтому важно с детства воспитывать серьезное отношение к паролям. Это — один из важнейших элементов цифровой гигиены.

Как работает пароль?

Древние римляне изобрели бетон, водопровод, канализацию, центральное отопление, газеты, римское право и много других полезных для цивилизации вещей. Пароли — тоже их изобретение. Историк Полибий, живший во II веке до нашей эры, так описывает применение паролей:

> *«Вот каким образом они обеспечивают безопасное прохождение ночью. Из десяти манипул, расположенных в нижней части улицы, командир выбирает одного солдата, который освобождается от несения караульной службы. Этот солдат каждую ночь приходит к трибуну и получает от него пароль — деревянную табличку со словом. Сначала солдат показывает пароль своему командиру, а потом идет с табличкой к следующему, который, в свою очередь, передает табличку другому».*

Принцип действия пароля не изменился до наших дней. Нужно выбирать кодовое слово и по секрету передать тому, кто охраняет доступ к ресурсу, будь то крепостные ворота, облачное хранилище фотографий, социальная сеть или что-то еще. Потом часовой

(или программа) спрашивает всякого вновь пришедшего, знает ли он пароль. Если ответ правильный, то пропускает его, если нет, то возможны варианты. Вражеского лазутчика попытаются поймать или застрелить, обычному же пользователю просто покажут на экране окно с надписью «Доступ запрещен», а после нескольких неудачных попыток заблокируют вход в систему. Это не смертельно, но обидно и зачастую хлопотно. Если речь идет, например, об интернет-банке, то вам, вероятно, придется идти с паспортом в офис и доказывать, что именно вы владелец денежных средств, просто забыли пароль.

> *«Железным» аналогом пароля можно считать кодовые замки, которые используются в самых разных устройствах — от банковских сейфов до вокзальных камер хранения и противоугонных тросов для велосипедов.*

До широкого распространения компьютеров большинство секретов, в том числе государственной важности, охранялось при помощи хитроумных механических устройств, потому что все документы были бумажными, и скрыть их от посторонних глаз можно было, лишь положив в сейф. Но даже зная, насколько опасной может быть утечка информации, люди порой проявляли удивительную беспечность в отношении кодов своих замков — тех же паролей. В этом смысле весьма показательна история, рассказанная одним из самых известных физиков XX века, лауреатом Нобелевской премии Ричардом Фейнманом.

Помимо прочего, он любил, как бы сейчас сказали, троллить своих коллег и начальников, в том числе и по вопросам безопасности. Во время работы на Манхэттенском проекте в Лос-Аламосе у Фейнмана появилось два увлечения: игра на барабанах

и вскрытие замков. Для начала он научился открывать обычные висячие замки с трехцилиндровыми механизмами, которые использовались в шкафах с секретными документами. Вот как он это описывал в своей книге «Вы, конечно, шутите, мистер Фейнман»:

> *«Чтобы продемонстрировать никчемность этих замков, всякий раз, когда мне нужен был чей-нибудь отчет, а хозяина отчета не оказывалось на месте, я просто заходил в его кабинет, открывал шкаф и брал нужную бумагу. Закончив с ней работать, я отдавал ее хозяину со словами: «Спасибо за твой отчет». В ответ я слышал:*
> *— А где ты его взял?*
> *— У тебя в шкафу.*
> *—Но я его запер!*
> *— Знаю, что ты его запер. Но замки — барахло!»*
> *Потом в Лос-Аламосе появились шкафы с кодовыми замками: чтобы открыть такой замок, необходимо было знать комбинацию цифр. Эти шкафы стали вызовом для любознательности Фейнмана. Чтобы изучить, как работает кодовый замок, он разобрал один из них в своем кабинете. Но это не помогло. Тогда он купил несколько книжек известных взломщиков, чтобы ознакомиться с «лучшими практиками». Но и там не нашел ответа. В итоге Фейнман разработал собственный метод. Однажды, стоя возле шкафа с открытым замком, он заметил: если аккуратно поворачивать лимб, пока запирающий стержень не перестанет возвращаться в исходное положение, то можно узнать последнее число в комбинации. Этот же прием в чуть усложненном виде позволил ему узнать и второе число. А первое оставалось подобрать простым перебором при закрытом замке.*

Затем Фейнман использовал сочетание методов социальной инженерии со своими техническими навыками (именно так и делают современные хакеры):

«Я практиковался и практиковался до тех пор, пока не достиг той степени совершенства, при которой мог подобрать последние два числа на открытом замке, почти не глядя на лимб. И тогда я стал проделывать такую штуку: зайдя к коллеге в кабинет для обсуждения какой-нибудь физической задачи, я прислонялся к открытому шкафу и как бы в забывчивости крутил его лимб туда-сюда, как это делает человек, рассеянно играющий ключами во время разговора. Иногда я не смотрел на стержень, а просто клал на него палец — чтобы знать, когда он пойдет вверх. Таким способом я выяснил последние два числа на нескольких сейфах. Вернувшись в свой кабинет, я записывал пары последних чисел на бумажке, которую хранил в замке своего сейфа. Чтобы достать бумажку, я каждый раз разбирал свой замок — это место я считал самым надежным».

Фейнман пару раз продемонстрировал свои удивительные способности по открыванию секретных замков, но, как настоящий фокусник, хранил свой метод в секрете. После этого его стали звать на помощь, когда срочно требовалось открыть шкаф, хозяин которого был в отъезде. Если это был «неизученный» шкаф, Фейнман отказывался. А если из числа попавших в «разработку», то шел в свой кабинет якобы за инструментами, смотрел в шпаргалку, а дальше оставалось только перебрать двадцать первых чисел — и вуаля, дело сделано! Люди думали, что он открывает хитрые замки без всякой предварительной информации, и Фейнман старался поддерживать эту легенду.

Многие мамы нередко удивляются, как их дети умудряются подобрать пароль к телефону или компьютеру. Точно также, как мистер Фейнман, они очень наблюдательны, очень мотивированы и у них есть куча времени, чтобы заниматься перебором вариантов. Вот один из детских лайфхаков (рассказ мамы):

> *«Мои сыновья начисто вытирали экран айпада. Потом подходили ко мне и говорили, что им срочно нужно что-то сделать — и для этого я должна разблокировать айпад. А после того, как я его разблокирую, они смотрели на оставленные мною отпечатки пальцев и быстро вычисляли простой пароль, составленный из цифр. С более сложным паролем им пришлось повозиться, ведь по отпечаткам пальцев на экране нельзя определить порядок символов. Но они стали подбирать пароль по смыслу, и у них снова получилось».*

Что тут скажешь? Молодцы! Кстати, таким же образом по отпечаткам на клавиатуре Николас Кейдж добыл пароль к секретному компьютеру в «Сокровищах нации».

Зная о склонности пользователей к беспечности, разработчики стали устанавливать более высокие требования к паролям, чтобы заставить людей заботиться о безопасности. Сегодня стандартом де-факто стало требование, чтобы длина пароля была не менее восьми символов, и чтобы пароль обязательно включал заглавные и строчные буквы, цифры и специальные символы (#, $, %, @, &, ! и другие). Чуть позже мы узнаем, чем это обусловлено.

Человек не в состоянии запомнить сложные комбинации и вынужден свои пароли где-то хранить.

Но тут другая беда — человек не в состоянии запомнить такие сложные комбинации и вынужден свои пароли где-то хранить. Чаще всего пароли оставляют в текстовом файле на рабочем столе компьютера или в заметках в телефоне, откуда их и похищают злоумышленники. Некоторые выбирают варианты еще легче: например, используют один и тот же пароль ко всем сервисам, записывают его на бумажке и прикрепляют на видном месте возле компьютера. А потом делают селфи и выкладывают фото в Инстаграм. Нужно ли удивляться, что через некоторое время их данные оказываются похищенными?

Нолан Сорренто, главный злодей в фильме Стивена Спилберга «Первому игроку приготовиться», тоже хранил свой пароль записанным на бумажке, которая была приклеена к боковой панели его крутейшей игровой системы. И когда он вызвал к себе в кабинет Уэйда Уоттса в образе его аватара Парсифаля, чтобы попытаться его уговорить работать на корпорацию IOI, тот, естественно, увидел и запомнил этот пароль, благодаря чему Уэйд и его друзья смогли проникнуть в систему Нолана и заставить освободить Саманту.

«— Вы дистанционно взломали его машину?
— У него стационарная точка. Найти просто, хакнуть тяжело.
— Правда, этот тупица хранил там же записку с паролем.»

Никогда не делайте так, как Нолан Сорренто! Если бы не эта его оплошность, пасхантерам[1] было бы гораздо труднее победить.

---

1 *Пасхантер (англ. Gunter) — охотник за «пасхалками», пользователь игры «ОАЗИС», который ищет Пасхальное яйцо Холлидея, создателя игры. Нашедший его получит полный контроль над виртуальной реальностью. («Первому игроку приготовиться»).*

Два ключа лучше, чем один, или Двухфакторная аутентификация

Наверное, у многих на двери в квартиру стоят два замка — для большей надежности. Точно также и в компьютерных системах, чтобы впустить пользователя, часто кроме пароля используется еще и второй параметр.

Второй пароль? Ни в коем случае. Нужен другой, независимый канал, по которому можно подтвердить, что вы это вы.

Второй пароль? Нет, ни в коем случае. Если злоумышленники как-то узнали один пароль, возможно, они заполучили всю базу или смогли внедриться в систему и перехватывают информацию. Или кто-то украл ваш ноутбук вместе со всеми паролями. В таких случаях специалисты говорят, что канал скомпрометирован.

Поэтому нужен другой, независимый канал, по которому можно подтвердить, что вы это вы. Эти каналы должны быть принципиально разными. Парольная защита основывается на знании ключа. В принципе, знанием может обладать кто угодно — тот, кто украл или получил пароль. Тогда в игру вступает второй фактор, который основан на владении чем-либо — чаще всего телефоном или USB-ключом. Конечно, эту вещь тоже можно украсть, но маловероятно, что одновременно с паролем.

Обычно в роли второго канала используется SMS — вам на телефон приходит код, который надо ввести в специальное поле для подтверждения входа в систему или совершения каких-то действий. Обычно, подтверждение нужно чтобы перевести деньги или изменить какие-то важные данные.

Увы, и SMS могут перехватить. Шпионские приложения на Android умеют принимать SMS-сообщения незаметно для владельца телефона, так, что на экране не появится никаких уведомлений и не будет звукового сигнала, а потом быстренько передают полученный код жулику, который уже ввел ваш пароль на своем компьютере. Технически возможен перехват SMS и без установки шпионских программ. Это могут делать спецслужбы или коррумпированные сотрудники оператора сотовой связи — подробнее мы поговорим об этом в главе, посвященной мобильным телефонам. А пока можно остановиться на том, что в целом SMS-канал считается достаточно надежным, если вы не устанавливаете разные «левые» программы из непроверенных источников и не даете свой телефон в руки посторонним.

Непосредственно для входа в систему два ключа используют редко — мы ведь и квартиру не каждый раз закрываем на оба замка, это было бы неудобно. Но не помешает удостовериться, что входит настоящий пользователь, а не жулик, когда система замечает попытку входа с нового компьютера или телефона, — в этом случае задействуется двойная проверка.

Дополнительно вам на почту придет сообщение о входе с неизвестного устройства. Если вам подарили новый телефон, и вы с него зашли в свой аккаунт, то это сообщение можно просто принять к сведению. А если действительно кто-то другой пытался вас взломать, то вы узнаете об этом и сможете быстро поменять пароль. Так что не забывайте проверять вашу электронную почту, даже если не пользуетесь ею регулярно.

Кстати, поскольку пока большинство сервисов для подтверждения входа или важных действий полагается именно на SMS, не держи-

те телефон в одной сумке с ноутбуком — это будет слишком щедрым подарком ворам.

Не держите телефон в одной сумке с ноутбуком — это будет слишком щедрым подарком ворам.

Главный плюс подтверждения входа при помощи SMS — простота. Каждый, у кого есть мобильный телефон, с этим справится. И при этом код подтверждения всегда будет разный, а это безопаснее, чем постоянный пароль. Однако, есть и минусы — ваш телефон всегда должен быть заряжен, оплачен и находиться в зоне действия сети, иначе SMS-ка к вам не придет. К тому же, для многих смартфон стал сегодня основным или даже единственным средством доступа в интернет, поэтому фактически происходит слияние двух факторов в один — если кто-то завладел вашим телефоном, он с него войдет в ваш аккаунт и на него же получит код. Так что плюс оборачивается минусом.

Чем мы располагаем, кроме SMS, в качестве второго фактора? Еще можно использовать электронную почту — это следующий по популярности канал. Вам точно так же приходит на почту код, который надо ввести для подтверждения ваших прав. Более редко встречается использование телефонного звонка, когда код сообщают вам голосом. Почти совсем ушло из практики использование заранее напечатанных резервных кодов и специальных генераторов ключей. USB-ключи все еще используются банками, особенно как носитель электронной подписи, но это не массовое явление.

В дополнение к паролю часто используется капча (CAPTCHA, Completely Automatic Public Turing Test to Tell Computers and Humans Apart) — механизм, с помощью которого веб-сайт отличает людей от ботов (программ-роботов), заставляя их проходить обратный

тест Тьюринга. Обычно пользователю предлагается ввести в поле формы выражение из цифр и букв разного регистра, изображенное на автоматически сгенерированной картинке или определить, где на показанной картинке находятся автомобили, мосты, дорожные знаки или еще что-нибудь. Предполагается, что тупая программа с такой задачей не справится, а человек — запросто.

Капча не только не допускает массовой регистрации ботов в соцсетях или на других сервисах, но еще препятствует автоматизированным попыткам взломать пароль путем перебора вариантов — ведь в таком случае программа-взломщик должна еще распознать изображение и правильно ответить на вопрос. Теоретически это возможно, однако всегда нужно взвешивать, стоит ли овчинка выделки. Чаще всего нет, поэтому механизм капчи действительно помогает повысить уровень защищенности системы.

Усы, лапы и хвост — вот мои документы!

Кот Матроскин заявлял совершено справедливо про усы, лапы и хвост, потому что для идентификации пользователя можно использовать какое-либо из присущих ему свойств: отпечатки пальцев, лицо, рисунок радужной оболочки или сетчатки глаза, снимок кровеносных сосудов в руке, голос, походку, сердечный ритм, ДНК, в конце концов. То есть биометрические данные, которые по своей природе уникальны и однозначно связаны с человеком.

> *Казалось бы, вот оно, решение! Наукой доказано, что у людей не бывает одинаковых отпечатков пальцев — даже у близнецов. Вот вам и универсальный пароль!*

Любители детективов и фантастики на это лишь усмехнутся и расскажут кучу историй, как преступникам, или, наоборот, хорошим парням удавалось использовать чужие отпечатки, чтобы проникнуть на секретный объект или взломать систему. В кино такие вещи часто излишне драматизируют — на самом деле необязательно воображать всякие ужасы вроде отрубания пальцев или вырывания глаз — в реальной жизни есть способы более гуманные и не менее эффективные, хотя и такой риск исключать нельзя, поскольку бандиты могут оказаться технически неграмотными и поступить, как им кажется, проще.

На что годится мертвый палец?

Вопрос далеко не праздный, им интересуются как преступники, так и полицейские. Ответ зависит от типа биометрического датчика и конкретного устройства. Хотя многие устройства анализируют биологическое состояние пальца (например, при помощи инфракрасного датчика), следует признать, что такая возможность все-таки существует. Бывало, когда полицейские пользовались этим свойством для разблокировки айфонов погибших террористов или людей, умерших от передозировки наркотиков, чтобы выйти на след дилера, но с переменным успехом. А в 2005 году был случай, когда малазийские угонщики автомобилей отрезали палец владельца Mercedes-Benz, чтобы обойти высокотехнологичную систему безопасности.

Если производителям биометрических устройств не удастся исключить такую возможность, это может стать источником серьезной опасности получения увечий для владельцев потенциально привлекательных активов,

использование или доступ к которым заблокированы биометрической защитой[1].

Однако чаще пальцы все-таки подделывают: изготовление желатиновых или силиконовых слепков не является особенно сложной задачей для специалиста. А добыть оригинальный отпечаток даже очень высокопоставленного лица не составляет большого труда, что продемонстрировали активисты из Chaos Computer Club, опубликовавшие в своем журнале «пальчики» министра внутренних дел Германии Вольфганга Шойбле, которые они сняли со стакана, использованного им во время публичного мероприятия. Фокус был проделан в 2008 году, чтобы продемонстрировать фундаментальные риски биометрических систем, но тем не менее технология получила широкое распространение. Более того, обязательное применение дактилоскопии в государственных системах, планируемое сегодня во многих странах, может привести к дискриминации некоторых людей, и это тоже надо учитывать.

Люди без отпечатков пальцев

Существуют редкие генетические мутации, при которых у человека может не быть отпечатков пальцев вообще. Люди с синдромом Негели или дерматопатией пигментной ретикулярной формы, например, могут не иметь отпечатков пальцев. Оба заболевания являются формами эктодермальной дисплазии, и отсутствие отпечатков в этом случае — всего лишь самый безобидный из симптомов.

---

1 *Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации. // Блог компании «ИНТЕМС»*

Отпечатки пальцев могут также исчезнуть в результате побочных эффектов от приема некоторых лекарственных препаратов, например — капецитабина (выпускается под брендом Кселода), противоракового препарата, применение которого задокументировано, приводило к исчезновению отпечатков пальцев.

Еще более интересным случаем является адерматоглифия. Единственным проявлением этой генетической мутации является отсутствие папиллярного рисунка на всех пальцах, ладонях рук и подошвах ног. У этой мутации нет никаких сопутствующих проявлений, выраженных в нарушении нормальной жизнедеятельности или снижении продолжительности жизни. То есть адерматоглифия не является заболеванием. Люди, обладающие это особенностью, могут иметь сложности в общении с силовыми структурами и получении виз. Но если они встанут на преступный путь, то смогут обходиться без перчаток.

А в общем и нечаянный порез может на некоторое время лишить вас возможности разблокировать свой телефон. Так что слишком полагаться на эту технологию не стоит — хотя после заживления раны папиллярный рисунок обычно восстанавливается[1].

Никто не спорит, что очень удобно разблокировать пальцем телефон или ноутбук, открыть дверь в квартиру, получить деньги в банкомате, расплатиться за покупку в магазине или завести дви-

1 *Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации. // Блог компании «ИНТЕМС»*

гатель машины. Но всегда, когда вы слышите об удобстве в связи с безопасностью, стоит насторожиться. Действительно ли метод идентификации человека по отпечатку пальца безопасен? Что будет, если кто-то украдет эту информацию?

Действительно ли метод идентификации человека по отпечатку пальца безопасен? Что будет, если кто-то украдет эту информацию?

Чтобы разобраться, давайте заглянем на технический уровень и посмотрим, как это работает. На самом деле телефон не может «видеть» ваш палец — с датчика он получает не снимок всего отпечатка, а некий соответствующий ему цифровой код, который сравнивает с хранящимся в памяти. Если коды совпадают, значит, доступ разрешен. То есть достаточно украсть эту информацию, чтобы попытаться войти в систему под вашим именем.

В этом смысле пароли имеют преимущество перед биометрией, потому что могут быть заменены на новые даже при подозрении на утечку, а палец или глаз так легко не поменяешь. Помните, чего это стоило герою Тома Круза в фильме «Особое мнение»? Собственно, здесь и пересекаются основное преимущество и главный недостаток всех биометрических систем — высокая точность идентификации человека вызывает большие сложности при компрометации системы.

Поэтому защите биометрических систем приходится уделять повышенное внимание. Во-первых, практически в обязательном порядке применять шифрование данных. Во-вторых, использовать так называемый метод «отменяемой биометрии», суть которого состоит в том, что в биометрический признак (отпечаток пальца, например) вносится повторяемое искажение — как будто в системе хранится ваше изображение, полученное при помощи кривого зеркала. В слу-

чае утечки данных вам достаточно изменить кривизну зеркала, чтобы сгенерировать новый ключ вместо скомпрометированного.

Есть и еще одна проблема: при использовании биометрии всегда существует вероятность ложного пропуска и ложного отказа. В первом случае это значит, что доступ будет открыт случайному человеку, чьи биометрические данные просто очень похожи на ваши; во втором законный владелец данных не сможет войти в систему, потому что она его не узнала.

Качественные характеристики биометрических систем[1]

Метод биометрической идентификации	Коэффициент пропуска	Коэффициент ложного отказа
Отпечаток пальца	0,001%	0,6%
Распознавание лица 2D	0,1%	2,5%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Дело в том, что сканеры отпечатков пальцев и другие биометрические датчики, особенно встроенные в потребительские приборы,

1 *Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации. // Блог компании «ИНТЕМС»*

несовершенны — это и является источником ошибок. Кроме случайной ошибки существует и вероятность срабатывания системы на «муляж». Но по мере развития технологий качество датчиков повышается, и примитивные методы обмана, такие как «желатиновые пальцы», перестают работать. В свою очередь, исследователи обнаруживают все новые уязвимости таких систем.

Группа исследователей из университета Нью-Йорка и Мичиганского университета разработала способ взломать практически любой гаджет, защищенный технологией сканирования отпечатков пальцев. При этом отпечатки владельца для этого не нужны вовсе! Специалисты создали, если можно так выразиться, изображение «универсального отпечатка пальца». В этом рисунке присутствуют отличительные признаки огромного количества разных отпечатков абсолютно разных людей. Как показали опыты, этого достаточно для того, чтобы обмануть большинство недорогих сканеров, устанавливаемых в мобильных телефонах, планшетах, ноутбуках и другой электронике.

Для того чтобы сделать «ключ от всех биометрических замков», ученые взяли за основу базу данных, состоящую из более чем 800 реальных отпечатков. При помощи специального компьютерного алгоритма они были совмещены таким образом, что в итоге получившийся «ключ» имеет схожесть на 26–65% с любым отпечатком, взятым у случайного человека, не находившегося в исходной базе.

Высокотехнологичные сканеры обмануть таким образом вряд ли получится, но вот устройства повседневного пользования — вполне. Дело в том, что сканеры наподобие Touch ID

имеют малую площадь, что не дает им возможности считать весь отпечаток пальца, и сенсор «ориентируется» лишь по фрагменту. Эта уязвимость как раз и была использована учеными. Как говорят сами исследователи, существует очень высокая вероятность того, что за несколько попыток авторизации, которые предоставляет система мобильного телефона, сканер может попасть на похожий участок «универсального отпечатка». Если системе авторизации удастся определить несколько признаков соответствия, она посчитает «универсальный отпечаток» за отпечаток владельца и разблокирует электронное устройство. Во время испытаний удалось успешно обмануть сканер в 15% случаев, что указывает на весьма большую «дыру» в этой системе авторизации[1].

То есть надо признать, что биометрия не обеспечивает 100% защиты от действий злоумышленников. Однако она может существенно снизить риски несанкционированного доступа. Поэтому эксперты советуют защищать одной лишь биометрией только данные, не имеющие особой ценности.

Например, когда нужно сделать так, чтобы ребенок, который взял поиграть родительский гаджет, не мог случайно разослать неуместные фотографии по вашим контактам, совершить покупку в интернет-магазине или перевести средства с банковского счета. Таких неприятностей можно избежать, если установить запуск важных приложений и подтверждение финансовых операций по отпечатку пальца.

---

1 *Создано изображение «универсального отпечатка пальца», способное обмануть большинство сенсоров // Hi-News.ru, 18 апреля 2017.*

Кроме того, биометрия — защита на случай экстренных ситуаций. В Японии после разрушительного землетрясения и цунами в марте 2011 года множество людей лишись не только своих банковских карт, но и документов. Они вынуждены были проходить через долгие и утомительные процедуры идентификации личности, чтобы снять деньги со своих счетов. После этого в стране создали единую биометрическую систему, которая исключает такую проблему в будущем.

Датчик распознавания отпечатка пальца на телефонах компании Apple впервые появился в модели iPhone 5S, представленной в 2013 году, и стал обязательным элементом всех новых устройств. Он позволяет их владельцам производить разблокировку, а также подтверждать покупки в App Store, iTunes и iBooks. Компании Apple удалось не только сделать одно из самых точных биометрических устройств для массового пользователя, но и разработать действительно надежное решение для безопасного хранения идентификационных данных.

Здесь важно сказать, что некой централизованной базы отпечатков не существует в принципе, поэтому никто не может ее взломать и украсть. Все отпечатки хранятся только на самом устройстве в специальной защищенной области Secure Enclave, расположенной непосредственно на процессоре. Точнее говоря, хранятся не сами снимки отпечатков, а их цифровые образы, дополнительно зашифрованные. Эта информация не записывается в резервные копии iTunes и iCloud, серверы компании или любой другой источник.

Прежде чем начать использовать Touch ID нужно создать резервный пароль в качестве дополнительной защиты. Он понадобится для разблокировки телефона в случаях, когда:

- *устройство было выключено или перезагружено;*
- *был добавлен отпечаток еще одного пальца;*
- *устройство получило команду удаленной блокировки через Find My iPhone;*
- *произошло пять безуспешных попыток разблокирования с помощью отпечатка подряд;*
- *устройство ни разу не было разблокировано в течение двух суток;*
- *прошло более шести суток с момента последнего ввода кода блокировки, а само устройство не было разблокировано датчиком Touch ID в течение восьми часов.*

Слив ключа, впрочем, не означает, что теперь смартфон не может обеспечивать безопасность: важные данные, хранящиеся в Secure Enclave, защищены другими ключами, которые все еще не найдены и, скорее всего, не будут. Все, что можно сделать, это расшифровать и изучить секретную систему Apple, которая работает на криптографическом процессоре. Получить доступ к данным, которые там хранятся таким образом, нельзя.

Иначе говоря, технология Touch ID пока остается устойчивой к взлому. Другое дело, что ее можно обмануть, используя разные приемы.

Осторожно, мошенники!

В 2018 году появились сообщения о мошеннических приложениях в AppStore, которые использовали технологию Touch ID. Они маскировались под приложения якобы для отслеживания здоровья, которые назывались Heart Rate Monitor, Fitness Balanceapp и Calories Trackerapp (Сейчас эти приложения уже удалены).

Их работа была основана не на вредоносном ПО, а на хорошем понимании человеческого поведения. Люди привыкли использовать Touch ID не только для разблокировки телефона, поэтому часто даже не задумываются о том, когда приложение просит их приложить палец к датчику. После того, как вы отсканируете отпечаток пальца, такое мошенническое приложение быстро показывает всплывающее окно с внутренней покупкой и списывает со счета от $90 до $120, одновременно уменьшая яркость экрана, чтобы это окно было сложно увидеть[1].

Лицо вместо пальца

С выходом смартфона iPhone X в 2017 году Apple заменила дактилоскопический датчик Touch ID на систему идентификации пользователей по лицам Face ID, которая использует набор камер True Depth. По сути, это комплекс из двух датчиков — 7-мегапиксельной фронтальной камеры и инфракрасной камеры, и двух инфра-

1 *Берегитесь хитроумного мошенничества с Touch ID, проникшего в App Store // Habr.com, 8 декабря 2018.*

красных осветителей — «проектора точек» (всего точек 30 тысяч) и «заполняющего» излучателя (свет от обоих невидим).

С помощью этой системы iPhone сканирует лицо владельца в формате 3D, затем обрабатывает изображение специальной нейросетью и создает цифровой отпечаток, который используется для разблокировки. Точно так же, как было и с Touch ID, биометрические данные хранятся в специальной защищенной области на самом телефоне в зашифрованном виде и никуда не передаются.

Хакеры всех мастей тут же бросились ломать новую игрушку и кое-каких успехов достигли. Буквально через несколько дней после начала продаж телефонов с Face ID, в ноябре 2017 года вьетнамская компания Bkav сообщила, что им удалось обмануть систему с помощью сложной маски, сделанной из комбинации 2D и 3D деталей, но повозиться им пришлось изрядно, и повторить такой трюк будет чрезвычайно сложно[1].

В августе 2019 года на конференции хакеров Black Hat в Лас-Вегасе показали еще один изощренный способ «ломануть» Face ID и получить доступ к iPhone спящего или мертвого человека. Как оказалось, если пользователь носит очки, то система игнорирует область вокруг глаз, воспринимая ее как пустое пространство с белой точкой блика от подсветки посередине черного зрачка,

1 *Vietnamese Firm Bkav Claims to Have Beaten Apple Face ID With an Elaborate Mask // GIZMODO.com, 11 декабря 2017.*

считая это достаточным, чтобы определить, что человек жив и бодрствует. Специалисты из Tencent Security Xuanwu Lab взяли обычные очки, наклеили на них по куску черной ленты с небольшой белой точкой в центре, надели их на «спящего» пользователя и успешно разблокировали его телефон[1].

Однако оснований для паники пока нет. Все эти сценарии трудно воспроизвести в жизни. Сама Apple заявляет, что ее система распознавания лиц предназначена для удобства, а не абсолютной безопасности. Она менее уязвима, чем Touch ID, и в целом работает. Говорят, что Touch ID может вернуться в усовершенствованном виде полноэкранного датчика, Apple уже оформила соответствующий патент. Но подтверждения этой информации до сих пор нет.

- *Использовать вместо пароля лицо или отпечаток пальца вполне можно.*

В общем, использовать вместо пароля лицо или отпечаток пальца вполне можно. Кое-какие способы их обхода существуют, но реальной опасности для обычных пользователей они не представляют. Остальные биометрические технологии еще не созрели для массового применения, и в жизни вы можете встретиться с ними реже, чем в кино. Однако пройдет совсем немного времени, и то, что вчера было фантастикой, станет нашим повседневным опытом, как стала им, например, идентификация человека по ДНК.

---

1 *Biometric Authentication Under Threat: Liveness Detection Hacking // Конференция «Black Hat USA», 3-8 августа 2019.*

«Мой пылесос шпионит за мной» — о паролях по умолчанию на разных устройствах

Нет, это не исповедь параноика на приеме у психиатра. Это вполне реалистичный сценарий, который реализуется, если вы станете без должного внимания впускать в свой дом разнообразные умные устройства, в том числе и бытовые приборы, у которых становится все больше «мозгов».

Сегодня микрокомпьютер может быть встроен во что угодно, хоть в лампочку.

Сегодня микрокомпьютер может быть встроен во что угодно, хоть в лампочку. А если там есть компьютер, значит, на нем есть операционная система, в которой есть администратор, у которого есть пароль на доступ ко всему. Как правило, эти пароли устанавливаются еще на фабрике и потом не меняются, чем часто и пользуются злоумышленники. Как правило, это пользователь «admin» с паролем «admin» — иными словами, кто угодно может зайти в систему и сделать любую пакость.

Итак, давайте проведем небольшую ревизию умных устройств в вашем доме, которые могут иметь пароль по умолчанию.

Прежде всего, это роутер, который обеспечивает подключение к интернету и раздает wi-fi по квартире. Большинство из них так и используется с заводскими настройками. Обычно провайдеры рекомендуют их сменить, но кто читает их рекомендации? Известны и такие случаи, когда производитель, наоборот, рекомендовал

«сохранить установки и настройки по умолчанию». Интернет работает — и отлично! Между тем, это очень серьезная брешь в вашей цифровой крепости, фактически — незапертые входные ворота. Естественно, сначала хакерам придется взломать ваш wi-fi, ведь вы же не настолько наивны, чтобы открыть доступ к своей беспроводной сети без пароля, да?

> *Запаролить роутер, не обладая техническими навыками, непросто. Но это важно сделать. Поспособствует вам в этом множество инструкций, которые легко найти в интернете, указав модель вашего роутера. Или кто-то из знающих людей, которым вы доверяете.*

Если ваш телевизор достаточно новый, то он, скорее всего, тоже оснащен встроенным компьютером, пароль которого также нужно сменить с заводского на собственный. Вы спросите: где тут риск? Зачем злоумышленнику ваш телевизор? Если в телевизоре есть встроенная камера и микрофон, то он может превратиться в шпионское устройство. Кроме того, в памяти телевизора может оказаться много конфиденциальной информации — например, вам же надо оплачивать подписки, а это значит, что в телевизоре могут быть ваши платежные данные, вот уже и улов для хакеров. Посмотрели на большом экране фотографии из отпуска — а среди них оказались и фото паспортов. В общем, к телевизору надо относиться как к настоящему компьютеру и принимать такие же меры безопасности.

К телевизору надо относиться как к настоящему компьютеру и принимать такие же меры безопасности.

Более того, появились умные пылесосы с видеокамерами, которые также подключаются к домашнему wi-fi. Имея возможность

перемещаться по дому, они способны превратиться в настоящих соглядатаев и начать шпионить за вами. Не забудьте и про холодильники, которые сами заказывают продукты, про кондиционеры, отопительные системы, умные розетки, умные лампочки и так далее.

Приборы, которыми можно управлять удаленно, как правило, имеют коды доступа. Заводские настройки всем известны, и если их не поменять перед началом использования, то этим вы очень сильно облегчите задачу взломщикам.

Вот еще одна история про Ричарда Фейнмана, на этот раз о паролях по умолчанию.

> *В послевоенное лето хозяйственники Лос-Аламоса[1] вывозили кое-что из списанного имущества. Среди этих вещей был сейф одного из высокопоставленных сотрудников. Прибыв сюда во время войны, он решил, что шкафы недостаточно надежны для его секретов и заказал специальный сейф, который с трудом втащили в его кабинет. Все в Лос-Аламосе знали об этом сейфе. Но прежде, чем отправить сейф на распродажу, его надо было опорожнить, а сам сотрудник был на Бикини[2]. Кроме него шифра никто не знал.*

---

1 *Лос-Аламосская национальная лаборатория (ЛАНЛ, англ. Los Alamos National Laboratory, LANL, ранее — Site Y, LASL) — одна из шестнадцати национальных лабораторий Министерства энергетики США и одна из двух лабораторий, ведущих в США секретные работы по ядерному оружию. Находится в городе Лос-Аламос, штат Нью-Мексико, США. Управляется службой Triad National Security, LLC. Основана в 1943 году.*

2 *Бикини — атолл в Тихом океане, где проводились испытания ядерного оружия.*

Разумеется, первым делом позвали Фейнмана как известного взломщика. Но кодов от этого сейфа у него не было, к тому же ему было некогда, поэтому он попробовал уговорить секретаршу все-таки позвонить на Бикини и узнать комбинацию чисел. И вот, пока Фейнман ее уговаривал, пришел местный слесарь и запросто открыл знаменитый сейф.

«Этот слесарь гораздо лучший взломщик, чем я», — подумал мистер Фейнман. Он потратил несколько недель, чтобы подружиться со слесарем и расспросить того, как ему удалось открыть сейф.

Ответ оказался ошеломляюще простым:

— Я знаю, что замки приходят с завода установленными на 25-0-25 или на 50-25-50, — сказал слесарь. — И я подумал: «Чем черт не шутит? Может, этот олух не потрудился сменить комбинацию». Вторая комбинация открыла замок.

Узнав это, Фейнман прошелся по кабинетам своего здания, пробуя две заводские комбинации, и открыл каждый пятый сейф.

Бывает и хуже: в 2004 году из воспоминаний Брюса Блэйра стало известно, что в течение почти двадцати лет коды запуска ядерных ракет США были «00000000» — да-да, восемь нулей! По правде сказать, сначала вообще никаких кодов не было, только в 1962 году президенту Кеннеди пришла в голову мысль, что ядерную войну может начать кто угодно — террористы, захватившие ракетную шахту, диверсанты или просто какой-нибудь полковник по собственной инициативе. Поэтому он приказал оборудовать

все ракеты специальным устройством контроля Permissive Action Link (PAL), которое блокировало систему запуска до введения правильного кода. Система считалась абсолютно надежной, и, наверное, так оно и было, только военные, чтобы не «заморачиваться» на всех пусковых установках, сбросили коды в ноль.

Купив или получив в подарок новую вещь, никогда не оставляйте заводские пароли по умолчанию.

Мораль этой истории такова: купив или получив в подарок новую вещь, никогда — слышите, никогда! — не оставляйте заводские пароли по умолчанию. Точно так же поступайте и с прежними паролями, если вещь пришла к вам от другого владельца.

Украсть оптом, ломать поодиночке

Чтобы заполучить пароль, у злоумышленников есть два основных способа: взлом или кража. Например, можно попытаться перехватить легионера, несущего табличку с паролем, и отнять ее — это будет грубый взлом. А можно заслать шпиона, чтобы он втерся к вам доверие, и вы бы сами ему все рассказали — это уже будет кража с помощью социально-психологической инженерии.

Чтобы заполучить пароль, у злоумышленников есть два основных способа: взлом или кража.

Трудно сказать, какой метод эффективнее, ведь чтобы воспользоваться отнятой у легионера табличкой, враг должен был уметь читать по-латыни, а среди варваров этот навык едва ли был широ-

ко распространен. Но уж читать-то современные хакеры умеют, и если ваш пароль попал к ним в руки, они не преминут пустить его в дело. (Поэтому разработчики стараются их запутать, но об этом чуть ниже). К тому же взлом всегда оставляет следы, и жертва постарается восстановить защиту. А кража может долгое время оставаться незамеченной.

Взлом всегда оставляет следы. А кража может долгое время оставаться незамеченной.

Надо сказать, что у самого метода защиты при помощи пароля есть две слабые точки. Во-первых, пользователь должен назвать свой пароль при входе в систему, и в этот момент кто-то может попытаться его похитить. Самое простое — подсмотреть из-за вашего плеча, так работают визуальные хакеры. Например, когда вы пользуетесь телефоном в метро. Или это сделает программа-вирус, проникшая в ваш компьютер.

Во-вторых, провайдер должен хранить у себя пароли всех пользователей, а много секретов в одном месте — это настоящее пиршество для хакеров. Поэтому жулики обычно не охотятся за паролями отдельных пользователей, а стараются украсть всю базу целиком. Образно говоря, они предпочитают сначала вынести сейф, чтобы потом спокойно его распилить. Делать это надо предельно тихо и незаметно, иначе операция теряет смысл. Естественно, здесь на первый план выходит человеческий фактор: в любой компании всегда найдется сотрудник, который не откажется подзаработать на сливе информации, и задача преступников состоит только в том, чтобы выйти на него и договориться о цене.

Зная об этом риске, разработчики предпринимают встречные меры, которые призваны если и не остановить преступников, то осложнить

им задачу и дать атакованной структуре время, чтобы восстановить защиту — в том случае, если утечка была обнаружена.

Утечки паролей

В прессе регулярно появляются шокирующие заголовки об утечках миллионов паролей. Просто погуглите, чтобы ощутить масштаб бедствия. О крупнейшей базе украденных е-мейл адресов и паролей сообщил в начале 2019 года известный специалист по безопасности Трой Хант. Он следит за хакерскими форумами и покупает базы данных, выставленные на продажу (иногда эти базы ему присылают бесплатно). Но Хант никогда не видел, чтобы на продажу выставляли такую огромную базу, как нынешняя Коллекция № 1 (Collection #1). Гигантский архив содержит 2 692 818 238 записей с адресами электронной почты и паролями.

Кстати, вы можете проверить, есть ли ваш е-мейл и пароль среди украденных хакерами. Для этого зайдите на сайт **https://haveibeenpwned.com/**, который уже несколько лет ведет Трой Хант[1].

Брутфорс — против лома нет приема

Чтобы взломать систему, когда нет никаких догадок насчет пароля, используют метод брутфорс (по-английски brute force — бук-

1 *Крупнейший дамп в истории: 2,7 млрд аккаунтов, из них 773 млн уникальных. // Habr.com, 17 января 2019.*

вально «грубая сила»), основанный на переборе всех возможных значений. Например, если у вас есть чемодан с кодовым замком, имеющим три лимба с цифрами от 0 до 9, то, чтобы его открыть, вам нужно перебрать всего тысячу комбинаций — с этим справится даже ребенок. Для четырех цифр уже потребуется перебрать 10 тысяч комбинаций, для пяти — 100 тысяч и так далее. Или можно увеличить число значений на лимбе, допустим до 100, и тогда на трех лимбах мы уже имеем 100 * 100 * 100 = 1 000 000 — один миллион комбинаций.

Теперь вы понимаете, почему Фейнман так стремился выведать два числа из трех на замках шкафов с секретными документами. Перебирать вручную миллион комбинаций на механическом замке — задача нереальная, проще такой сейф просверлить. Но если замок электронный и перебор производит компьютер, то миллион вариантов — это пустяк.

> *Чтобы усложнить задачу взломщику, в паролях не только наращивают количество символов в длину, но также используют помимо цифр буквы, что значительно увеличивает число вариантов.*

Судите сами: если бы у нас был такой же трехлимбовый кодовый замок, но вместо цифр на его лимбах были бы буквы латинского алфавита, то число комбинаций было бы 26 * 26 * 26 = 17576. Это гораздо больше, чем в случае с одними цифрами.

Допустим, что в пароле используются 36 различных символов (латинские буквы одного регистра + цифры), а скорость перебора составляет 100 тысяч паролей в секунду.

Кол-во знаков	Кол-во вариантов	Стойкость	Время перебора
1	36	5 бит	менее секунды
2	1296	10 бит	менее секунды
3	46 656	15 бит	менее секунды
4	1 679 616	21 бит	17 секунд
5	60 466 176	26 бит	10 минут
6	2 176 782 336	31 бит	6 часов
7	78 364 164 096	36 бит	9 дней
8	2,821 109 9x10^{12}	41 бит	11 месяцев
9	1,015 599 5x10^{14}	46 бит	32 года
10	3,656 158 4x10^{15}	52 бита	1 162 года
11	1,316 217 0x10^{17}	58 бит	41 823 года
12	4,738 381 3x10^{18}	62 бита	1 505 615 лет

Мы видим, что пароли длиной до 8 символов включительно, в общем случае, не являются надежными. Для современных компьютеров порог надежности гораздо выше. Так, 64-битный ключ (пароль) перебирается на современном компьютере примерно за два года, но перебор легко может быть распределен между множеством компьютеров, что существенно сократит сроки взлома.

Для повышения стойкости пароля важна даже не столько его длина, сколько разнообразие используемых символов.

Для повышения стойкости пароля важна даже не столько его длина, сколько разнообразие используемых символов. Именно поэтому сервисы, которые действительно заботятся о безопасности своих пользователей, требуют, чтобы пароль обязательно содержал буквы верхнего и нижнего регистра, цифры и специальные знаки.

Интересно, что длинные пароли, состоящие из 12 символов и более, ломаются ничуть не хуже, чем короткие. Дело в том, что для их составления люди используют фразы, состоящие из 3-4 обычных слов — такая задача легко решается с помощью перебора по словарю.

Также наивно будет использовать в качестве пароля русские слова, набранные латиницей. Например, конструкция «**JxtymCkj;ysqGfhjkm**» на самом деле в русской раскладке клавиатуры будет «**ОченьСложныйПароль**», что вскрывается программными средствами в два счета.

В реальных условиях брутфорс-атаке можно противостоять ограничением числа неправильных попыток ввода пароля и последующей блокировкой аккаунта. Например, если вы три раза неправильно ввели пин-код своей кредитной карты, банкомат ее «проглотит» и заблокирует. Точно так же может быть заблокирован доступ к соцсети или электронной почте, если кто-то будет пытаться тупо угадать пароль методом перебора. Тем не менее такие атаки имеют место, особенно когда взламывается конкретно чей-то аккаунт.

> *Эффективность брутфорс-атаки прямо пропорциональна уровню беспечности пользователя. Чем надежнее ваш пароль, тем меньше шансов его взломать в лоб.*

Потому что хакер не сидит и не вводит данные вручную, для этого есть специальные утилиты, к которым подключаются словари известных паролей и настраиваются алгоритмы их перебора.

Шифр и хеш — в чем разница?

Сегодня только совсем безалаберные разработчики хранят пароли в открытом виде в базе данных. (Но такие еще встречаются). И какой бы сложный пароль вы ни придумали, это ничем вам не поможет, если администратор базы данных управляет ей под логином «admin» с паролем «password». Такая база будет взломана с вероятностью 100% и пароли будут похищены.

Ответственные программисты никогда не хранят пароли в открытом виде. Чтобы защитить своих пользователей, они применяют два метода: шифрование и хеширование. С точки зрения обывателя, разница почти незаметна — вместо вашего любимого пароля «vasya2006» в базе данных окажется какая-то абракадабра, и злоумышленник не сможет вместо вас получить доступ в систему. Но разница есть, и довольно существенная.

Все, что было зашифровано, можно расшифровать, зная секретный ключ.

Все, что было зашифровано, можно расшифровать, зная секретный ключ. И если кто-то добудет этот ключ, ему станут известны все пароли, хранящиеся в базе. А вопрос «Почему бы не купить этот ключ вместе с ворованной базой?» — риторический, как вы понимаете. Если бы можно было обезопасить систему от рисков, связанных с недобросовестным поведением сотрудников, то этот метод считался бы надежным, потому что взломать шифрованный пароль при текущем уровне развития компьютеров практически невозможно — для перебора вариантов потребуется много времени даже по астрономическим масштабам. (Именно по этой причине шла такая битва за передачу ключей шифрования мессенджера

Telegram спецслужбам — если у вас нет секретной лазейки, шифрование обеспечивает очень высокую надежность).

Алгоритмов шифрования существует множество, и у нас нет цели познакомиться со всеми ними подробно. Одним из наиболее популярных является алгоритм AES — Advanced Encryption Standard, который, в частности, используется для шифрования паролей wi-fi. Этот алгоритм в настоящее время считается достаточно стойким.

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Даже суперкомпьютеру понадобилось бы неисчислимо огромное количество времени, чтобы получить доступ к информации под защитой AES посредством лобовой атаки. Для сравнения: возраст Вселенной — где-то между 13 и 14 миллиардами лет. Даже если предположить, что некий супер-суперкомпьютер мог быть справляться с более старым алгоритмом DES за одну секунду, то на взлом AES у него ушло бы около 149 триллионов лет. Как видите, размера ключа в 128 бит вполне достаточно, хотя совершенно секретная информация все равно шифруется с размером в 256 бит[1].

Однако все имеет обратную сторону. Алгоритмы шифрования математически очень сложны и потому работают медленно, что неудобно при повседневной работе: системе пришлось бы расшиф-

1 *Алгоритм шифрования AES. // Блог* ***OpenGsm.com***

ровывать пароль при каждом входе пользователя, а это вызывало бы заметную задержку. К тому же возникает тема с хранением ключей шифрования, а это отдельная и непростая история.

Поэтому сейчас для хранения паролей почти повсеместно используют хеширование[1]. Если не вдаваться в математические дебри, то хеширование — это алгоритм, который преобразует строку символов любой длины (ваш пароль) в другую строку фиксированной длины, называемую хешем.

> *Хеш обладает двумя свойствами. Во-первых, из него невозможно восстановить исходные данные, иначе говоря, расшифровать хеш нельзя, ключа в принципе не существует. Во-вторых, с очень высокой вероятностью каждому уникальному паролю соответствует уникальный хеш, что и позволяет использовать его вместо самого пароля.*

Тут нужно сделать оговорку — теоретически возможна коллизия, когда для двух разных паролей получится одинаковый хеш, но подбором параметров функции и длины самого хеша можно свести вероятность этого события почти к нулю. И, наконец, главное отличие от шифрования: хеш-функция работает очень быстро.

Как же преступники взламывают хешированные пароли, если ключа вообще нет? Да очень просто: они перебирают всевозможные комбинации символов, генерируют для них хеши и сравнивают

---

1 Hash (англ.) — мешанина, мусор, ненужная информация. В русском языке возможны два варианта транслитерации: хеш или хэш. Смысл термина можно трактовать так: зная только хеш, мы не получим никакой полезной информации, сам по себе хеш выглядит бессмысленным набором байтов.

с имеющимися в базе. Если совпали хеши, то и сами пароли совпадают. Например, хеш самого популярного пароля 123456 по алгоритму SHA-1 выглядит вот так: 7c4a8d09ca3762af61e59520943dc26494f8941b.

Само собой, жулики даром время не теряли и провели большую работу, чтобы составить так называемые радужные таблицы, которые позволяют не тратить время на вычисление хешей популярных паролей — подобно тому, как раньше были таблицы Брадиса для квадратных корней, синусов, косинусов и других функций.

И как же быть? Ведь если по таблице запросто можно найти исходный пароль, значит, хеши бесполезны?

Не совсем так. Во-первых, полная таблица для всех возможных паролей получилась бы такого гигантского объема, что поиск по ней занял бы слишком много времени. Во-вторых, есть множество разных функций хеширования, и под каждую из них нужна своя радужная таблица.

Зачем пароли солят?

Чтобы они были вкуснее. Шутка! На самом деле, чтобы осложнить жизнь хешкрекерам (это хакеры, которые специализируются на подборе хешей), разработчики придумали перед вычислением хеша добавлять к исходному паролю некую случайную последовательность символов — на их жаргоне это называется «соль». Причем «соль» может динамически меняться, чтобы еще больше запутать взломщика.

«Соление» паролей полезно еще и потому, что, если два пользователя имеют один и тот же пароль, у них будет совпадать и хеш-код пароля.

> *Люди не склонны слишком напрягать фантазию, изобретая пароли. Например, в 2018 году на 23 месте в списке 100 худших паролей оказалось имя президента США Трампа — «Donald». Также часто используются имена других знаменитостей и популярных персонажей, названия культовых кинофильмов и музыкальных групп.*

Можете быть уверены, что хакеры провели предварительную работу и посчитали для них хеши, так что на сегодняшний день добавление «соли» является абсолютно необходимым элементом защиты паролей — и пока достаточно надежным.

Зачем это пользователю? Чтобы понимать, откуда взялось требование сложных и длинных паролей, и не ворчать по этому поводу. И еще: чтобы относиться с недоверием к ресурсам, допускающим короткие и простые пароли.

> *Но откуда нам знать, насколько ответственно разработчики относятся к защите паролей? Увы, на этот вопрос ответа нет. Именно поэтому важно использовать разные пароли к разным сервисам.*

Вполне вероятно, что ваши любимые пароли уже утекли, и продолжать ими пользоваться небезопасно. Национальный центр кибербезопасности Великобритании в мае 2019 года опубликовал список из 100 тысяч паролей, известных хакерам, и это лишь малая часть того, что можно найти в интернете. «Соль»

задержит злоумышленников на какое-то время, но не остановит совсем, так что к составлению паролей лучше подойти креативно.

Как придумать хороший пароль?

Итак, насчет плохих паролей все понятно — не использовать дни рождения, номера телефонов, вообще любые комбинации только из цифр; не годятся простые слова — все, которые есть в словаре; ни в коем случае пароль не должен совпадать с логином (именем пользователя) и его электронной почтой, не быть его вариацией типа логин «user123», пароль — «user321». Не годятся в качестве пароля и «прогулки по клавиатуре» — так называемые keyboard-walks пароли — например, «qwerty», «qazwsx», даже с добавлением цифр типа qwerty123456 и тому подобное. Не остановят хакеров и такие банальные хитрости, как заменить букву «o» на ноль, «s» на $, «i» на 1 и так далее.

Может быть, взять строку из песни или из стихотворения? Вот, например, «Tobeornottobe» или «Strawberryfieldsforever» или уж «BewaretheJabberwockmyson!» — уберемпробелыиготово! Хакеры тоже не дураки, эти варианты они учли. К тому же, выбранная вами фраза может оказаться очень длинной, а у многих сервисов есть ограничение на количество символов в пароле. Да и намучаетесь вводить его. Разумная длина пароля должна быть порядка десяти знаков, больше не имеет смысла.

Разумная длина пароля должна быть порядка десяти знаков, больше не имеет смысла.

И как же быть? Придется проявить фантазию.

> *Нужно придумать алгоритм, который лично вам будет понятен и логичен, чтобы по нему можно было не только составить надежный пароль, но и вспомнить его, когда понадобится.*

И еще одно важное замечание: многие сервисы устанавливают политики, требующие регулярной смены паролей. То есть ваш алгоритм должен позволять генерировать новые пароли, которые можно будет легко запомнить.

Можно призвать на помощь приемы мнемотехники. Вкратце суть мнемотехники можно передать следующим образом: нам сложно запомнить абстрактные и/или разрозненные данные (в нашем случае это пароли, удовлетворяющие требованиям безопасности) и легче запомнить связи между объектами, между новой информацией и уже имеющейся, ассоциации, наши эмоции по отношению к чему-либо. Иными словами, намного проще запомнить логические, ассоциативные, образные и другие связи между объектами, а не сами объекты. В случае с паролями нам потребуется провести обратное действие — из чего-то хорошо знакомого сделать абстрактный набор символов.

Намного проще запомнить логические, ассоциативные, образные и другие связи между объектами, а не сами объекты.

Вы же помните, как заучивали последовательность цветов спектра? «Каждый охотник желает знать, где сидит фазан» — вот вам и пароль: «kozzgsf». Семь букв маловато, но это не беда, можно взять по две буквы от каждого слова и чередовать заглавные и строчные: «KaOhZhZnGdSiFa».

О, теперь это похоже на перечисление химических элементов! А почему бы не попробовать таблицу Менделеева как генератор паролей? Там и цифры есть. Возьмем, к примеру, инертные газы: «He2Ne10Ar18» — осталось добавить специальные символы, и дело в шляпе. Пусть будет так: «He2!Ne10@Ar18#» — немного банально — символы «!», «@» и «#» идут подряд на клавиатуре, но это не страшно. Теперь проверим его в анализаторе паролей **https://howsecureismypassword.net/** — и увидим, что стойкость этого пароля 204 миллиона лет! А когда понадобится обновить пароль, в следующий раз возьмем, допустим, щелочные или щелочноземельные металлы, галогены, драгоценные металлы, редкоземельные элементы — да что угодно! Можете ходить по периодической таблице хоть по диагонали или даже буквой «Г», как конь в шахматах — каждый ход будет давать вам прекрасные пароли. Органическая химия тоже может послужить источником вдохновения для придумывания хитрых паролей, если вдруг это ваше хобби.

Если вы не в ладах с химией, можете придумать себе другой способ генерации паролей, главное, чтобы предметная область была вам хорошо знакома и ассоциации рождались легко. Но будьте осторожны с историей!

— Не понимаю, как они смогли взломать пароль у меня на ноуте?
— А что у тебя за пароль был?
— Год канонизации святого Доминика папой Григорием IX.
— А это какой год?
— 1234

Не хотите попробовать придумать свой алгоритм составления надежных паролей, чтобы они содержали не менее 8 символов — буквы верхнего и нижнего регистра, цифры и специальные символы? Поле широчайшее: можно использовать мелодии, запись шахматных партий, географические координаты, стихи (не слишком известные), физические формулы, счет в теннисном матче и вообще что угодно.

Бывает так, что фантазия нас покинула, а новый пароль придумать надо. Чтобы не ломать голову, можно воспользоваться генераторами паролей, коих в интернете есть великое множество. Один клик — и готово. Например, «w0v2X4%(dA», еще клик — «Yw4ite#3(&7h%9Ms» и так далее. Можно задавать длину пароля, наличие цифр и спецсимволов, гласные или согласные буквы, верхний или нижний регистр, в общем, любой каприз.

> *Человеку психологически трудно самому сгенерировать случайный набор символов, причем удовлетворяющий критериям надежности пароля, если просто наобум тыкать по клавиатуре. Лучше поручить это программе.*

Понятное дело, что запомнить такой пароль нет никаких шансов. Но зато надежно.

Должны ли все пароли быть уникальными?

Согласитесь, если бы ключ от квартиры подходил к машине, банковскому сейфу и шкафчику в раздевалке фитнес-клуба, то это было бы слишком рискованно, не правда ли? Однако люди часто

используют одинаковые пароли к разным сервисам — к электронной почте, социальной сети, интернет-банку и случайному сайту, где вдруг потребовалась регистрация, чтобы скачать какой-то файл.

> *В идеальном мире у пользователя должны быть уникальные сложные пароли для каждого сервиса, но мы живем в реальном мире и понимаем, что так делать никто не станет, даже обладая удобной схемой генерации.*

Пожалуй, разумным компромиссом будет использование какого-то одного пароля, который легко запомнить, для регистрации на разных случайных сайтах, когда нужно прочитать какую-то статью или скачать документ, и где не требуется вводить персональные данные. Придумывать и хранить уникальные надежные пароли для каждого из таких сайтов было бы слишком утомительно.

В обязательном порядке вам нужны разные пароли для наиболее важных сервисов: основной электронной почты, социальной сети и банковских приложений. Электронная почта используется как универсальный логин, и на нее же завязана функция восстановления забытых паролей. Получив доступ к вашей почте, злоумышленник может завладеть почти всем вашим цифровым достоянием, поменяв пароли учетных записей.

Обязательно нужны разные пароли для наиболее важных сервисов: основной электронной почты, социальной сети и банковских приложений.

То же самое справедливо и относительно социальных сетей — кроме ущерба для репутации и выпрашивания денег у ваших друзей, преступник может получить доступ ко многим сайтам и приложени-

ям, в которых вы зарегистрированы через ваш аккаунт в соцсети. Это действительно очень удобно, когда можно нажать всего одну кнопку и сразу начать пользоваться новым сервисом вместо того, чтобы каждый раз заполнять анкету. У этого удобства есть и обратная сторона — более высокий риск при потере контроля над своим аккаунтом.

Про банковские приложения, наверное, понятно и без комментариев. Деньги — это главное, что интересует всех преступников и в интернете, и в обычной жизни. Если у вас несколько банковских приложений, то придется придумать уникальные пароли к каждому из них.

> *В июле 2019 года интернет-магазин Ozon сообщил об утечке логинов и паролей 450 тысяч пользователей. Все скомпрометированные пароли были сброшены сразу после обнаружения утечки, о чем компания уведомила пользователей. «Судя по всему, эти данные попали в сеть потому, что пользователи из списка использовали одинаковые пароли для разных сервисов. Мошенники также могли получить их в разное время при помощи вирусной атаки на компьютеры пользователей», — добавили в Ozon.*

Вот вам и цена беспечности — взломают что-то одно, а под угрозой окажутся многие ваши аккаунты. Так что думайте сами, решайте сами. Но лучше все-таки не рисковать.

Пароли и дети

Если взрослые испытывают трудности с запоминанием и использованием сложных паролей, то что уж говорить о детях! Было бы наивно полагать, что дети справятся с такой задачей.

В школах Норвегии, где у детей были iPad'ы, они использовали для доступа к своим устройствам как отпечатки пальцев, так и индивидуальные пароли. У них также были пароли для подключения к образовательным платформам и к различным приложениям. Министерство образования Норвегии выдало школьникам индивидуальные пароли, позволяющие им безопасно получить доступ к некоторым учебным платформам. Однако другие платформы и приложения требуют использования дополнительных паролей. В общем, дети изо всех сил пытались запомнить эти различные пароли. В одной из школ однажды утром потребовалось 45 минут, чтобы начать урок, потому что дети забыли свои пароли. В другой школе пароли детей были автоматически обновлены в ночь перед тем, как они должны были пройти тест по математике. Это изменение вызвало проблемы и задержки, когда некоторые из детей пытались получить доступ к тестовым заданиям[1].

Увы, простого ответа на этот вопрос нет. Чтобы безопасно пользоваться интернетом, нужно помнить свои пароли, и при этом они должны быть надежными. Киберпреступники не делают скидок на возраст. Но и требовать от детей, чтобы они всегда помнили все свои пароли — просто глупо, ибо это требование невыполнимо. Наверное, разумным выходом будет записывать детские пароли и хранить их дома в надежном месте.

Требовать от детей, чтобы они всегда помнили все свои пароли — глупо, ибо это требование невыполнимо.

Дети не всегда понимают важность паролей и последствия их компрометации (то есть ситуации, когда пароль становится известен

1 *Digital Natives or Naïve Experts? Exploring how Norwegian children (aged 9-15) understand the Internet. // EU Kids Online 2018.*

кому-то еще). Согласно данным исследования Teen Angels из организации Wired Safety, 75 процентов детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам: в этом же признались 66 процентов девочек в возрасте 7-12 лет[1].

> *Задача взрослых — научить детей хранить свои пароли также бережно, как ключи от квартиры, и никогда не сообщать их даже друзьям. А если такое все же случилось, то немедленно менять пароль.*

Нельзя отправлять пароли по электронной почте или в SMS, если кто-то попросил, потому что настоящие владельцы веб-сайтов никогда не спрашивают пароли у своих пользователей — так делают только мошенники.

Не вводите пароли на компьютерах, которые вы не контролируете. Не пользуйтесь для входа в соцсети, мессенджеры, электронную почту и другие сервисы, защищенные паролем, общедоступными компьютерами в школе, библиотеке, в интернет-кафе или компьютерных лабораториях. На таких компьютерах можно только посмотреть открытые сайты или поиграть.

- *Не вводите пароли на компьютерах, которые вы не контролируете*

Имеют ли родители право знать пароли детей? Если спросить психологов и юристов, их мнения разойдутся. Ребенок до 14 лет с юридической точки зрения вообще не может иметь мобильного телефона. А психолог скажет, что у ребенка должно быть личное пространство и его нельзя нарушать. При этом оба они будут правы[2].

---

1 *Памятка по безопасности детей в сети Интернет // Сайт* ***Docplayer.ru.***

2 *Немецкие родители знают пароли своих детей. // RusVerlag.de, 25 ноября 2014.*

Менеджеры паролей

Итак, коль уж мы договорились, что пароли ко всем аккаунтам должны быть разные, но при этом сложные и длинные, и что хранить их где попало небезопасно, самое время задать вопрос — а где и как?

Ричард Фейнман хранил свою шпаргалку с кодами ко всем шкафам в лаборатории Лос-Аламос в замке своего шкафа — он вполне разумно предполагал, что если кто-то вскроет сам шкаф, то вряд ли будет разбирать замок на части. Но чтобы добраться до этих кодов, ему приходилось каждый раз разбирать и собирать замок, что было не очень удобно.

> *С точки зрения безопасности самый надежный вариант хранения пароля — записать его на бумаге и положить в сейф. С особо ценными паролями — например, от криптокошелька, где лежат биткоины на сотни миллионов долларов — именно так и поступают.*

Первые биткоин-миллиардеры братья-близнецы Уинклвоссы (те самые, что судились с Марком Цукербергом из-за Facebook)[1], разработали сложную систему хранения и защиты своих персональных ключей. Они разрезали распечатки ключей на части и поместили фрагменты в конверты, хранящиеся в надежных депозитных боксах по всей Америке. Таким образом, если вор и похитит один из конвертов, то не получит весь ключ.

---

1 *Кэмерон Ховард Уинклвосс и Тайлер Ховард Уинклвосс (англ. Cameron Howard Winklevoss, Tyler Howard Winklevoss; род. 21 августа 1981, Саутгемптон, Нью-Йорк) — близнецы, американские гребцы и предприниматели. Братья являются основателями социальной сети ConnectU и долгое время судились с Марком Цукербергом, настаивая на том, что он украл идею их сайта для своей сети Facebook.*

Если у вас нет сейфа — не беда. Запишите свой пароль на бумаге и уберите дома в надежное место.

Если у вас нет сейфа — не беда. Запишите свой пароль на бумаге и уберите дома в надежное место. Киберпреступник до ваших записей не доберется, а обычному вору нужны деньги и ценные вещи, а не какие-то бумажки, пусть это и идет вразрез с большинством советов про хранение паролей, которые вы можете найти в интернете. Дело не в том, что пароль записан на бумаге, а в возможности доступа к нему посторонних. Если вы приклеите бумажку с паролем на монитор или положите в открытый ящик письменного стола на работе, это одно. А если уберете в папку с документами дома — то совсем другое.

Однако для повседневного пользования этот способ вряд ли подойдет, ведь пароли для входа в социальные сети или игры нужны каждый день и не только дома. Записывать все пароли в текстовый файл и держать их на рабочем столе или в заметках на телефоне — так себе идея. Их может похитить не то что неведомый хакер, а просто не в меру любопытный друг, которого пустили поиграть на компьютере. Ему достаточно просто вставить флешку или перекинуть ваш файл с паролями себе на почту.

Лучше всего использовать специальную программу — менеджер паролей. Это будет ваш цифровой сейф. Как и все цифровые вещи, в отличие от своего железного собрата он обладает новыми полезными свойствами. Пароли в нем можно не только безопасно хранить, но и использовать. Менеджер паролей работает и как заполнитель форм, и сам подставит нужный пароль, когда вы зайдете на соответствующий сайт.

Дополнительно менеджеры паролей могут работать как защита от фишинга. В отличие от людей, программа не ведется на визуальные имитации, которые похожи на настоящие веб-сайты. То есть после перехода по сомнительной ссылке на фишинговый сайт менеджер паролей не подставит ваши данные в форму ввода, а сообщит, что сайт является подделкой. Это весьма ценное свойство, особенно с учетом того, что человек не может быть постоянно бдительным, и вероятность попасться на удочку мошенников достаточно велика. С таким бонусом использование специальной программы становится выгодным, даже если у вас имеется всего несколько паролей, которые можно было бы и так запомнить.

Человек не может быть постоянно бдительным, и вероятность попасться на удочку мошенников достаточно велика.

Практически все современные браузеры имеют встроенный менеджер паролей. Почему бы не воспользоваться этой их функцией? Профессионалы в области информационной безопасности непременно скажут, что это дурной тон и небезопасно, что такие менеджеры не могут заменить полноценных приложений для управления паролями, но... тем не менее согласятся, что менеджеры паролей на основе браузера лучше, чем ничего. Для не слишком искушенного в технологиях пользователя это в целом приемлемый вариант. Ибо, во-первых, это удобно — благодаря функции синхронизации в браузере, ваши пароли будут с вами на любом устройстве, как только вы войдете в свой аккаунт.

Во-вторых, они активно совершенствуются. Еще недавно браузерным менеджерам паролей ставили в упрек неумение автоматически генерировать сложные пароли, состоящие из букв, цифр и специальных символов, но это уже в прошлом. Chrome и Firefox уже умеют создавать пароли, отвечающие требованиям безопасности.

Что касается возможностей взлома, этот риск существует для всех систем. Но чаще всего для реализации такой атаки все-таки сначала нужно установить на компьютер или телефон жертвы шпионское ПО. Чтобы этого избежать, не давайте свои устройства посторонним, используйте антивирусы и другие средства защиты — будьте начеку.

Не давайте свои устройства посторонним, используйте антивирусы и другие средства защиты — будьте начеку.

В качестве аргумента против использования Chrome для хранения паролей упоминают еще и то, что Google следит за пользователями в попытке показывать им более точно таргетированную рекламу. Да, это факт, но безопасности ваших паролей это не угрожает. (Подробнее о механизмах слежки и способах противодействия мы поговорим в главе об анонимности в интернете). То есть если вы так или иначе пользуетесь продуктами «корпорации добра», как иронически называют Google, то в целом нет особых причин отказываться и от их менеджера паролей.

> *В браузере Chrome от Google появилось расширение под названием PasswordCheckup, которое автоматически проверит, были ли пароли раскрыты в результате взлома данных. После установки расширение проверяет все используемые данные для входа в систему Google по базе данных, насчитывающей около четырех миллиардов имен пользователей и паролей, и предупреждает вас, если найдет совпадение*[1].

1 *Google's new Chrome Extension automatically checks your passwords are still secure // The Verge, 5 февраля 2019.*

Кроме встроенных в браузеры программ есть еще множество специального ПО для управления паролями — платного и бесплатного, от известных производителей и не очень. Все они очень разные, ситуация на рынке постоянно меняется, поэтому нужно следить за обзорами, чтобы выбрать тот продукт, который вам подойдет больше.

Опасайтесь стилеров и кейлоггеров

А не слишком ли опасно хранить все пароли в одном месте? Если основной пароль будет похищен или взломан, это поставит под угрозу все хранимые пароли.

Да, такая опасность существует, и разработчики менеджеров паролей об этом знают. Поэтому они настоятельно рекомендуют соблюдать следующие правила:

- Основной пароль должен быть сложным, и его надо запомнить. Ни в коем случае не держите его записанным на компьютере или на бумажке рядом с ним;

- Используйте двухфакторную аутентификацию для входа в аккаунт браузера, если вы пользуетесь встроенным менеджером паролей;

- Настройте безопасный вход в менеджер паролей в соответствии с инструкциями производителя, если вы используете специальное ПО;

- Используйте антивирус, он может заметить подозрительную активность и пресечь атаку на вас;

- Не давайте свои устройства посторонним и всегда блокируйте, если вам нужно отойти.

> *Что такое стилер? Это шпионская программа, предназначенная для того, чтобы находить и воровать с устройства жертвы ценные данные — пароли, номера банковских карт и тому подобное.*

Название происходит от английского слова «steal» — воровать. Обычно эти данные хранятся в определенных местах на диске, и стилер просто пытается скопировать нужные файлы и отправить их своему хозяину. Простейший стилер может написать даже школьник, но чтобы его внедрить на чей-то компьютер, нужен физический доступ. Более сложные программы-шпионы могут проникнуть к вам по сети. Однако на диске пароли, как правило, хранятся в зашифрованном виде, и далеко не факт, что вору удастся их расшифровать.

Даже если все ваши данные надежно зашифрованы и лежат в секретном месте, есть один момент, когда система очень уязвима — это момент ввода пароля. Вот здесь-то и вступают в игру кейлоггеры.

> *Кейлоггер — другая разновидность шпионского ПО, также нацеленная в основном на кражу паролей. Этот шпион после внедрения на компьютер записывает нажатия клавиш на клавиатуре и передает их преступникам.*

Потому он так и называется — от английского «keylogging», что значит «вести журнал нажатий клавиш». Разумеется, кейлоггер записывает не все подряд, иначе объем передаваемых данных

был бы слишком заметным. Он умеет определять, что́ в данный момент показывается на экране, и ждет, когда появится окно ввода пароля. Этот вид шпионов широко распространен, у них даже есть свои рейтинги. В их функции входит получение случайных снимков экрана, запись звука, отправка записанных нажатий клавиш на указанный адрес электронной почты, мониторинг других активных приложений и посещенных веб-сайтов. Многие программные кейлоггеры работают незаметно, никогда не появляясь в диспетчере задач как работающие приложения.

Существуют также и аппаратные кейлоггеры — их можно вполне открыто приобрести на Amazon примерно за 50 долларов. Однако, чтобы их использовать, нужно каким-то образом получить доступ к компьютеру жертвы.

Есть кейлоггеры и для телефонов с ОС Android. Их кто-то может скрытно установить на ваш телефон и следить за вами.

Акустический криптоанализ: немного из настоящей шпионской жизни

Как можно догадаться из названия, это метод получения секретных данных на основе изучения шумов, издаваемых при печати текста. Его использовали еще с 1950-х годов, когда все печатающие механизмы сильно шумели. Например, в ходе операции в 1956 году в Лондонском посольстве Египта были размещены прослушивающие устройства, которые перехватывали шумы, издаваемые шифромашинами. Это позволило британским разведчикам получить секретную информацию, что повлияло на позицию Великобритании в Суэцком кризисе.

И сейчас этот метод стоит на вооружении хакеров и спецслужб, потому что мы все еще используем механические клавиатуры, и они издают шумы. (В этом месте начинающий параноик должен подумать хотя бы о том, чтобы отключить звук тональных сигналов при наборе телефонного номера). Несмотря на прогресс шпионских технологий, атака подобным методом все-таки довольно сложна и ее еще надо «заслужить» — против обычных пользователей вряд ли кто-то станет ее использовать.

Снизить риск от такого рода угрозы можно путем использования экранной клавиатуры — эта функция обычно есть в продвинутых менеджерах паролей. Можно воспользоваться и стандартной экранной клавиатурой Windows.

Что надо запомнить про пароли

Итак, подведем итоги. Что грамотный пользователь должен знать про пароли?

Длинный и сложный пароль — это не каприз разработчиков, а реальная необходимость. Чтобы пароль мог считаться безопасным, его длина должна составлять не менее 8 символов и включать буквы верхнего и нижнего регистров, цифры и специальне символы.

Для придумывания и запоминания сложных паролей можно использовать различные мнемотехники, это не так трудно, как кажется.

Графический пароль на Android должен включать не менее 8 узлов, не начинаться из угла и иметь пересечения, чтобы считаться надежным.

Иметь одинаковые пароли для всего слишком рискованно. По крайней мере, для всех важных сервисов пароли должны быть уникальными.

Пароли надо регулярно менять, потому что происходят утечки данных, возможно и ваших тоже.

Использовать отпечаток пальца или снимок лица можно, но не в качестве основного пароля.

Двухфакторная аутентификация, то есть подтверждение входа в систему или важных действий по SMS или другому каналу, обязательна для всех важных сервисов.

Менеджер паролей — полезная вещь, нужно выбрать и научиться им пользоваться, если вы еще этого не сделали.

В общем, к своим паролям нужно относиться максимально трепетно, заботиться об их сохранности, и тогда у вас будет меньше поводов волноваться о сохранности своих данных, денег и репутации.

Контрольные вопросы

1. Что такое пароль?
2. Как паролем пользовались древние римляне?
3. Что такое ПИН-код?
4. Что такое двухфакторная аутентификация?
5. Что такое биометрия?
6. Какие виды биометрических показателей вы знаете?
7. Можно ли защищать ценные данные только отпечатком пальца?
8. Почему обязательно нужно менять пароли по умолчанию?
9. Какой пароль считается надежным?
10. Что нельзя использовать как пароль?
11. Зачем надо регулярно менять пароли?
12. На каких домашних устройствах могут быть пароли?
13. Почему нельзя использовать один пароль на все?
14. Как можно хранить свои пароли?

15. Что такое брутфорс?

16. Что такое капча и зачем она нужна?

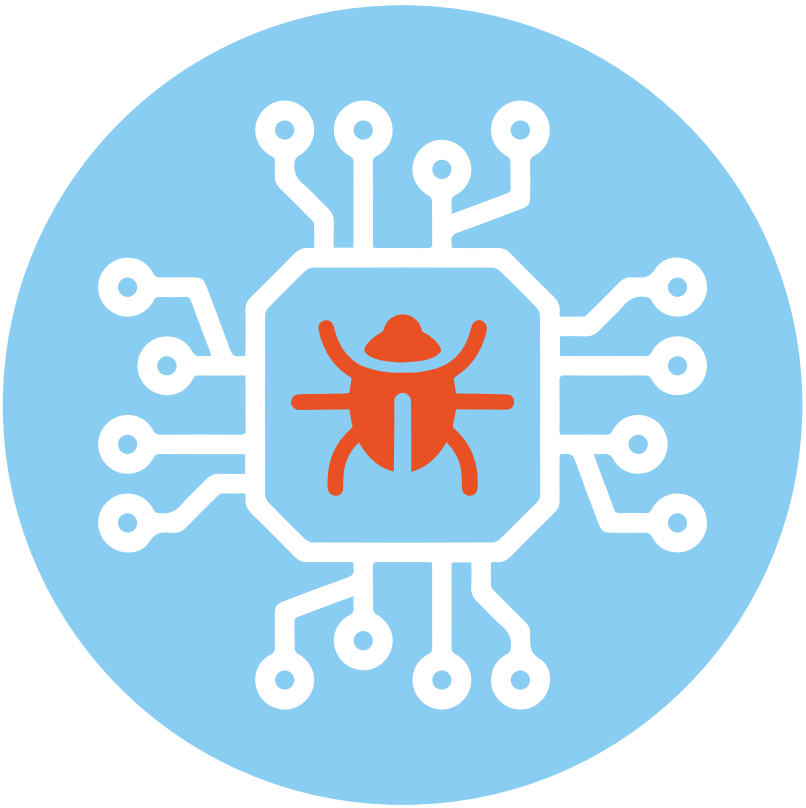
17. Сколько комбинаций на кодовом замке с тремя лимбами по 20 чисел?

18. Что такое хеш пароля?

19. Для чего нужны менеджеры паролей?

20. Что такое стилеры паролей?

21. Что такое кейлоггеры?



Глава 4

Арсенал киберпреступников

В главе 2 мы провели инвентаризацию нашего цифрового хозяйства и увидели, что нам есть, что терять. А сейчас поговорим об инструментах, с помощью которых киберпреступники творят свои темные дела.

Чтобы успешно противостоять преступникам, необходимо понимать, как они нас атакуют, в какие наши слабые места бьют, и, исходя из этого, выстраивать линию обороны.

Можно во все это не вникать? Есть же специально обученные люди: вот пусть они все как следует настроят, а мы будем просто пользоваться.

Увы, так не получится. В сфере цифровых технологий к сегодняшнему дню сложилась примерно такая же ситуация, какая наблюдалась в среде автолюбителей лет пятьдесят назад: чтобы «железный конь» исправно бегал, каждый водитель должен был стать немножко автомехаником. Помните, как было в старых фильмах? Машина внезапно останавливается, из нее, чертыхаясь, выходит водитель, и только поковырявшись какое-то время под капотом, едет дальше.

Знаете, почему таких сцен нет в современном кино? Потому что техника существенно изменилась. Если на приборной панели замигала лампочка, это означает, что нужно не лезть под капот, а ехать в сервис.

Если на приборной панели замигала лампочка, это означает, что нужно не лезть под капот, а ехать в сервис.

Но в том, что касается обеспечения кибербезопасности компьютеров и смартфонов, ситуация с сервисом на сегодняшний день еще далека от идеала. Например, просто за установку антивируса (пиратской копии или бесплатного) в Москве попросят от 500 до 2000 рублей, а настройка wi-fi-роутера обойдется в 300-1500 рублей. При этом комплексной услуги по обеспечению безопасности всей цифровой жизни человека никто не предлагает, так что спасение утопающих продолжает оставаться делом рук самих утопающих: пользователям волей-неволей придется беспокоиться о своей кибербезопасности самостоятельно.

Темпы роста киберпреступности в нашей стране значительно опережают все другие виды криминальной деятельности. Так, по данным Генпрокуратуры, за первые восемь месяцев 2019 года количество зарегистрированных преступлений в России выросло почти на 67%. А в 2018 году киберпреступность показала двукратный рост.

Краткая история вирусов: начало

Давным-давно, когда компьютеры были большими, а данные — маленькими, никаких вирусов не существовало вовсе. Писать программы тогда было делом трудным и хлопотным, поэтому программисты по большей части занимались чем-то важным и полезным, а не созданием вредоносного ПО.

Но в один прекрасный день каким-то умникам пришла в голову мысль, что можно написать программу, которая будет самовоспроизводиться до тех пор, пока не займет всю свободную память. Сказано — сделано! В 1961 году математики фирмы Bell Labs изобрели необычную игру «Дарвин», в которой несколько программ, названных «организмами», сражались за память компьютера. Это были еще не вирусы, но их предвестники — киберобъекты, наделенные свойством размножения по подобию живых организмов. И до начала эпохи персональных компьютеров эти протовирусы служили лишь забавой программистам, не представляя никакой опасности.

В сегодняшнем виде компьютерные вирусы появились в начале 1980-х, когда «персоналки» попали в руки школьников и студентов.

В том виде, в каком мы их знаем сегодня, компьютерные вирусы появились в начале 1980-х, когда «персоналки» попали в руки школьников и студентов. Поначалу вирусы были вполне безобидны, ведь их создавали не для того, чтобы кому или чему-либо причинить вред, а из пустого тщеславия. Первым получил распространение вирус ElkCloner, написанный пятнадцатилетним школьником из Питтсбурга по имени Ричард Скрента.

Возможно, это несколько удивит молодых поклонников Стива Джобса, но «Лось-клонировщик» (так можно перевести название вируса), передаваясь через дискеты, заражал операционную систему компьютеров Apple II. Это сейчас продукты компании из Купертино считаются эталоном безопасности, а в то время они работали под управлением одной из версий DOS — со всеми вытекающими для безопасности последствиями. Вирус питтсбургского школьника не вредил преднамеренно — лишь иногда случайно ломал систему, а в «нормальном режиме» после каждой 50-й загрузки выводил на экран стишок.

Elk Cloner:	«Лось-клонировщик»:
The program with a personality It will get on all your disks It will infiltrate your chips Yes it's Cloner! It will stick to you like glue It will modify RAM too Send in the Cloner!	Программа с индивидуальностью. Он проникнет во все ваши диски, Он внедрится в ваши чипы. Да, это — Клонировщик! Он прилипнет к вам, как клей, Он даже изменит оперативную память. Отправь Клонировщика!

Появление ElkCloner прошло практически незамеченным, поскольку владельцев техники Apple тогда было немного. Зато вирус Brain («Мозг»), который инфицировал компьютеры IBM PC, наделал много шума и вошел в историю как вызвавший первую эпидемию (или даже пандемию).

Brain («Мозг») инфицировал компьютеры IBM PC и вошел в историю как вирус, вызвавший первую эпидемию (или даже пандемию).

Его создали в 1986 году братья-студенты Базит и Амджад Фарух Алви из Пакистана. По своей природе Brain тоже был достаточно мирным — он всего-навсего замедлял работу флоппи-дисков. Более того, братья даже оставили свой адрес и телефоны, чтобы пользователи зараженных компьютеров могли с ними связаться:

> *WelcometotheDungeon © 1986 Basit&Amjads (pvt). BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS.... Contact us for vaccination...*

«Зачем вы это сделали?» — спросил их Микко Хиппонен (Mikko Hyponen), эксперт по кибербезопасности компании F-Secure. В 2011 году, спустя четверть века после эпидемии Brain, он специально приехал в Лахор по указанному адресу, где и нашел авторов «Мозга». Для Хиппонена эта поездка была сродни паломничеству. Ведь он, потративший большую часть своей жизни на борьбу с вредоносными программами, встретился с авторами первого вируса, с которым ему пришлось столкнуться.

В интервью Хиппонену братья рассказали, что были молоды, горячи и очень хотели наказать пиратов, которые нелегально копировали их

медицинскую программу для мониторинга работы сердца. Но что-то пошло не так — и вирус начал бесконтрольно распространяться, в результате чего добрался до Великобритании, США и ряда других стран. Первый звонок от инфицированного поступил из Университета Майами, а вслед за ним на братьев обрушился целый шквал звонков, так что телефоны им пришлось отключить. Но в целом история с Brain закончилась если и не удачно, то без особых потерь: зараженные компьютеры вылечили, а законов, предусматривающих наказание за создание вирусов, в Пакистане не существовало. И сейчас братья Фарух Алви руководят одной из крупнейших в стране телекоммуникационных компаний — Brain Telecommunications, расположенной все по тому же адресу. Вирусов они больше не писали.

А вот создателю первого компьютерного червя (программы, которая самостоятельно распространяется по сети) — Роберту Моррису (Robert Morris), аспиранту Корнеллского университета — повезло меньше. Он стал первым осужденным по закону о компьютерном мошенничестве и злоупотреблениях (Computer Fraud and Abuse Act), принятому в США в 1986 году.

> *Червь Морриса, или «Великий червь» (Great Worm), запущенный 2 ноября 1988 года, парализовал весь тогдашний интернет, заразив около 6000 серверов — 10% от общего количества (по другим данным — 2000 серверов). И снова эпидемия возникла из-за ошибки в механизме распространения!*

По задумке Морриса, его программа должна была записать себя на каждый доступный компьютер в сети, что могло произойти практически незаметно. Но так уж случилось, что вирус начал заражать каждую систему многократно и в итоге съедать все вычислительные мощности. Естественно, на это обратили внимание.

В результате из безвредного, как считал автор, интеллектуального упражнения червь превратился в опасную атаку типа «отказ в обслуживании» (DoS)[1]. В принципе, Роберта Морриса могли и не найти — он достаточно хорошо замаскировался. Однако его отец, работавший в АНБ, убедил сына сдаться добровольно. И, судя по всему, правильно сделал. Моррис-младший отделался условным сроком и штрафом в 10 тысяч долларов — притом, что ущерб от его «эксперимента» оценивался в 96,5 миллиона. Правда, согласно распространенному мнению, оценка ущерба была сильно завышена.

Моррис отделался условным сроком и штрафом в 10 тысяч долларов, хотя ущерб от «эксперимента» оценивался в 96,5 миллиона.

Чего только не вытворяли вирусы 1980-1990-х годов рождения! На мониторах зараженных ими компьютеров возникали самые разные и не всегда приличные надписи и расхаживавшие взад-вперед мультяшные персонажи; демонстрировались чудные визуальные и звуковые эффекты и др. Иногда вирусы даже играли с пользователями, как, например, вирус Casino. При инфицировании компьютера он предлагал пять раз сделать ставку на примитивной слот-машине. Если вам выпадал выигрыш, вирус честно оставлял ваши файлы в покое, если нет — безжалостно удалял.

---

1 *DoS (Denial of Service, «отказ в обслуживании») — хакерская атака на вычислительную систему с целью доведения ее до отказа. В результате атаки пользователи системы могут лишиться доступа к предоставляемым системным ресурсам (серверам) или этот доступ будет затруднен.*

Чаще употребляется термин DDoS (от англ. Distributed Denial of Service, распределенный отказ в обслуживании), означающий, что запросы на атакуемый сервер поступают с множества адресов.

Еще один вирус-пакостник — Laroux, один из первых вирусов для Excel. Он не только заражал все электронные таблицы, но при каждом открытии файла случайным образом округлял числовые значения в ячейках на 0,001% вверх или вниз. Постепенно ошибка накапливалась, что могло привести к неприятным последствиям.

> *А 2 июня 1997 года студент Датунского университета (Тайбэй, Тайвань; КНР) Чэнь Инхао (Chen Yinghao) создал первую версию вируса Chernobyl («Чернобыль» или CIH — по первым слогам имени автора). Вирус заражал компьютеры с операционными системами Windows 95 и ежегодно срабатывал 26 апреля — в годовщину катастрофы на Чернобыльской АЭС. CIH стирал загрузочную область жесткого диска, реже — данные BIOS. В последнем случае требовалось менять чип на материнской плате или даже приобретать новый компьютер, поскольку старый полностью выходил из строя. По оценкам, CIH заразил более 60 миллионов ПК по всему миру и причинил ущерб в размере свыше 1 миллиарда долларов. Но, что примечательно, непосредственно к Чэнь Инхао не было подано ни одного иска и к ответственности его никто не привлек.*

Такого рода «вирусотворчество» можно считать проявлением обычного вандализма — наряду с битьем окон, порчей общественного транспорта или созданием граффити, ведь финансовых интересов авторы вирусов прошлого века не преследовали. И не потому, что были бескорыстными. Дело в том, что получить деньги с жертвы и при этом остаться незамеченным, было сложно, а получить срок в цивилизованной стране — легко.

В наши дни вирусы ведут себя тихо. Они больше не показывают нам забавные картинки, не проигрывают мелодии и даже не пишут

никаких сообщений, кроме требований выкупа. Они максимально скрытно проникают в компьютер или телефон, маскируют свое присутствие и ждут подходящего момента, чтобы ограбить владельца. Теперь главная цель вирусописателей — не потешить свое самолюбие, а получить деньги.

Теперь главная цель вирусописателей — не потешить свое самолюбие, а получить деньги.

От интеллектуальных забав к извлечению денег

Преступный мир не сразу распознал, какие возможности открывает наступление компьютерной эры. Вероятно, для обычных бандитов это было слишком сложно, поэтому пальма первенства в сомнительном, с точки зрения этики, соревновании по монетизации компьютерных угроз принадлежит ученым. Но если ученые могут выдвигать блестящие идеи, это еще не означает, что они способны блестяще воплощать их в жизнь. Нередко и незаурядные умы допускают нелепые ошибки, оборачивающиеся крахом.

Весьма поучительный пример, а вместе с тем и сюжет для комедии — история первого вируса-вымогателя AIDS («СПИД»), известного также как Aids Info Disk и PC Cyborg Trojan[1].

В 1989 году д-р Джозеф Л. Попп (Dr. Joseph L. Popp), эволюционный биолог из Гарварда, разослал почтой (обычной, а не элек-

1 *Virus Bulletin, January 1992.*

тронной!) 20 тысяч дискет по обширному списку адресатов, включая подписчиков журнала PC Business World и делегатов конференции по СПИДу, проходившей под эгидой Всемирной организации здравоохранения. Где он взял эти списки? Купил под вымышленным именем у некоего кенийского бизнесмена.

Письма адресатам поступили от компании PC Cyborg Corporation, зарегистрированной в Панаме (ох уж эти панамские оффшоры!), а в приложенной к дискете лицензии на использование ПО значилось, что дискета содержит интерактивную анкету для оценки риска заражения СПИДом.

Однако кроме анкеты на дискете был еще записан и вирус-шифровальщик, который активировался после 90-й загрузки компьютера и зашифровывал все имена файлов на жестком диске, а после шифровки на экране появлялся текст с требованием заплатить от 189 до 378 долларов якобы за «аренду программного обеспечения». Таким нехитрым образом вымогатель пытался придать своим действиям законный вид. Забавно, но все это было изложено и на бумаге — в приложенном лицензионном соглашении. Но кто их читает! Отправить деньги нужно было на анонимный счет в Панаме. Взамен же вымогатель обещал прислать пароль для расшифровки файлов.

Впервые вирус AIDS проявил себя в Англии, причем под удар попали именно медицинские учреждения. Скотланд-Ярд немедленно начал расследование.

В канун Рождества главный герой этой истории возвращался с семинара ВОЗ из Найроби через Амстердам в США. Внимание со-

трудников аэропорта Схипхол привлекла тревожная надпись на его чемодане: "DR. POPP HAS BEEN POISONED", что можно было перевести как «Д-р Попп отравлен» или, если учесть, что рейс прибыл из Африки, подумать, что доктор инфицирован ВИЧ. Разумеется, нидерландские полицейские решили его досмотреть, а во время досмотра обнаружили среди вещей печать PC Cyborg Corp, о чем и сообщили своим британским коллегам. Доктору позволили добраться до Огайо, а там арестовали и экстрадировали в Великобританию, где он должен был предстать перед судом по обвинению в 11 эпизодах вымогательства. Очевидно, что пострадавших было больше, просто далеко не все обратились в полицию. Но и выявленных эпизодов оказалось вполне достаточно для возбуждения дела.

Никогда не используйте в качестве пароля свое имя! Не будьте как д-р Попп!

Среди изъятых у подозреваемого дискет был найден его дневник, в котором обнаружили ключ шифра от вируса: «Dr. Joseph Lewis Andrew Popp Jr». Банально, не правда ли? Никогда не используйте в качестве пароля свое имя! Не будьте как д-р Попп! Также среди его файлов нашли и полный исходный код программы-вымогателя. В общем, доказательств для суда набралось предостаточно.

> *Как установило следствие, стоимость дупликации носителей и почтовые расходы доктора превысили 10 тысяч фунтов. К этому сыщики прибавили затраты на регистрацию компании в Панаме, аренду помещения в Лондоне и в итоге обнаружили, что у этой авантюрной затеи складывается вполне внушительный бюджет. Это дало повод усомниться в рациональности действий Поппа. Однако, как вскоре было подсчитано, заплати все получатели дискет полную стоимость «лицензии» — 378*

долларов, доктор собрал бы в сумме 7,5 миллионов. И даже если бы его шантажу поддался всего один процент получателей дискет, и все они заплатили бы минимальный выкуп — 189 долларов, итоговые 38 тысяч покрывали все издержки. К тому же американский поверенный Поппа подтвердил, что доктор собирался вести бизнес с размахом и в дальнейшем планировал разослать не менее двух миллионов дискет.

К чести адресатов Поппа, только 5% из них вставили инфицированные дискеты в свои компьютеры. Люди оказались не такими беспечными, какими, видимо, их считал доктор.

Во время суда Попп вел себя странно: надевал на голову картонную коробку, накручивал на бороду бигуди, а на нос надевал презерватив, который, по его словам, защищал «от радиации и микробов». Адвокаты настаивали, что их подзащитный планировал жертвовать полученные от аферы деньги на альтернативные образовательные программы по СПИДу. И это, по данным следствия, было чистой правдой. В итоге многие пришли к выводу, что доктор на самом деле никто иной, как криптоанархист, своего рода Робин Гуд, который пытается инициировать реформы в просвещении по вопросам СПИДа. Хотя, согласно The Guardian, Поппом могли двигать и куда менее благородные мотивы — например, месть за то, что ему было отказано в работе в ВОЗ. Но, в конце концов, суд, невзирая на многочисленные сомнения и подозрения, решил, что доктор все-таки сошел с ума, и отправил его домой.

Забавный факт: после высылки из Англии крестный отец кибервымогателей Джозеф Попп основал в городе Онионта на севере штата Нью-Йорк оранжерею бабочек, назвав ее своим именем. Эта оранжерея существует по сей день.

Эксперты, изучавшие вирус AIDS, признали концепцию Поппа гениальной, а ее техническую реализацию — весьма слабой, ведь доктор использовал симметричное шифрование, а это довольно ненадежный метод. Он предусматривает, что для шифровки и расшифровки применяется один и тот же ключ, который хранится в теле вируса. То есть жертва, имея определенную квалификацию, может сама обнаружить этот ключ и спасти свои данные без какого-либо выкупа. Тем не менее, AIDS впервые показал действенную схему монетизации вирусов, которую в дальнейшем многократно использовали преступники. Особую популярность эта схема приобрела с появлением биткоина.

Однако эпизод непосредственно с вирусом AIDS остался в памяти лишь как экстравагантная выходка чудака-ученого. Последователей у него не нашлось, что, в общем-то, понятно — кто возьмет на себя труд по рассылке тысяч дискет? А вот когда все компьютеры подключились к электронной почте, и доставка вирусов значительно упростилась, преступники оценили его изобретение по достоинству.

> *По мнению упоминавшегося выше Микко Хиппонена[1], рубежом, когда создание вирусов окончательно превратилось в преступную деятельность с целью извлечения выгоды, стал 2003 год. Тогда появился вирус Fizzer — сложный почтовый червь, созданный исключительно в коммерческих целях. Его авторы открыли еще один способ монетизации. Их червь заражал компьютеры, из которых был сформирован ботнет — сеть компьютеров-зомби, тайно управляемых злоумышленниками.*

---

1 *Mikko Hypponen. The History and the Evolution of Computer Viruses. // Privacy-pc.com, 19 марта 2012.*

Затем создатели Fizzer стали продавать услуги по рассылке спама с зараженных машин другим злоумышленникам.

Если вы станете рассылать спам со своего адреса, провайдер его быстро заблокирует. Поэтому организаторы рассылок постоянно нуждаются в новых, еще не скомпрометированных адресах. Новые почтовые ящики теоретически можно регистрировать вручную, но это слишком неэффективный процесс, и активность такого рода тоже легко пресекается. А вот запустить рассылку с тысячью случайных адресов реальных пользователей — это эффективно!

Очень быстро многие любители вирусов поняли, что могут использовать свои навыки для заработка, если будут сотрудничать со спамерами, красть пароли и данные кредитных карт, когда люди совершают онлайн-покупки.

Вскоре очаги вирусных инфекций сменили локацию. В старые добрые времена — до того, как вирусы превратились в «машины по производству денег» — они создавались главным образом в странах Западной Европы, США, Канаде, Японии, Австралии. Но самые горячие точки сегодняшнего дня — это Россия, Украина, Казахстан, Румыния, Молдова, Китай, Бразилия и Иран.

Киберпреступность сегодня выгоднее торговли наркотиками. По данным Cybersecurity Ventures, ежегодная прибыль от наркобизнеса составляет около 400 миллиардов долларов, а киберпреступники в 2018 году заработали в общей сложности около 600 миллиардов.

За время, прошедшее с появления первых вирусов, мир коренным образом изменился. Эпоха хакеров-одиночек давно канула

в Лету, и теперь нам приходится иметь дело с организованной преступностью. Хуже того, образовалась целая преступная индустрия: одни злоумышленники разрабатывают вредоносное ПО и продают его, другие организуют атаки, третьи обналичивают добытые деньги.

Цифровой бестиарий: знай своего врага

Существует широкое разнообразие видов вредоносных программ, в том числе вирусов, червей, троянов, вымогателей, шпионских программ и прочее, объединяемых термином malicious software — вредоносная программа. Собирательно их еще называют malware (по-русски — вредоносные программы, а на сленге — «зловреды»).

> *Зловреды тайно действуют против интересов пользователя, в чем бы это ни выражалось. Это может быть кража паролей и учетных данных, личной информации, номеров банковских карт, кодов доступа и денежных средств, шантаж и вымогательство, навязчивая реклама, звонки и SMS на платные номера, уничтожение данных, захват аккаунтов и тому подобное.*

При всем разнообразии методов киберпреступники действуют примерно по одной и той же схеме. Сначала необходимо незаметно проникнуть в устройство пользователя и замаскироваться. Затем нужно доставить и распаковать «полезную нагрузку» — собственно, инструмент для совершения диверсии — и в подходящий момент нанести удар. Поэтому названия типов зловредов

чаще всего происходят либо от способа проникновения, либо от вида совершаемого действия.

Вообще говоря, деление зловредов на типы весьма условно. Это не систематика млекопитающих, когда только на основе строения зубов вы можете отнести животное к отряду грызунов и предположить, как оно выглядит. Зловредов же практически невозможно четко структурировать по типам, ведь здесь возможны любые химеры, обладающие качествами разных типов. Это в живой природе невозможно скрестить ужа и ежа, а в киберпространстве — запросто! Но пусть нам и трудно точно классифицировать всех наших врагов, с основными категориями вредоносного ПО все-таки стоит познакомиться.

Вирусы
Viruses

В обыденной жизни и в СМИ вирусом называют любую вредоносную программу — все, чем «болеет» компьютер. Технически это не вполне корректно.

Вирус отличает от других зловредов его способность к самораспространению и свойство внедряться в код других программ или системные области на устройстве. То есть он ведет себя подобно биологическому вирусу, который проникает в живые клетки и там размножается, а затем передается дальше. (Кстати, честь открытия вирусов принадлежит русскому ученому Дмитрию Ивановскому).

Эпидемии компьютерных вирусов вспыхивают подобно эпидемиям гриппа и также лечатся «противовирусными препаратами» — специальными программами, иногда уникальными для каждого вируса.

Ваш антивирус может оказаться неэффективен против нового вируса — как прошлогодняя вакцина не может справиться с новым вирусом гриппа. Поэтому нужно регулярно обновлять базы вирусных сигнатур, но и это не гарантия. Всегда есть временной промежуток между появлением яда и противоядия. Так что антивирус — не панацея, а лишь средство гигиены. С его помощью перекрываются известные каналы заражения и определяется набор «таблеток» от известных вирусов, если ваш компьютер или телефон подцепили кого-то из них.

То есть у каждого есть риск оказаться «нулевым пациентом» — быть первым, у кого обнаружат неведомый ранее вирус. Поэтому не стоит слишком расслабляться, даже если у вас стоит самый новый и навороченный антивирус. Враг не дремлет!

Черви
Worms

Червь — совершенно другой зверь. Если вирусу нужен переносчик в виде дискеты (в старое время), флешки или зараженного файла, то червь

распространяет себя сам. Существует несколько разновидностей червей.

Интернет-червь — первый червь в истории. Будучи однажды запущенным, он стремится заполонить собой всю сеть. Ему вообще не нужен никакой «транспорт». Этот червь сканирует подряд IP-адреса, и, если находит незащищенное подключенное устройство, проникает в него. Теоретически червь такого типа может заразить весь интернет менее чем за 15 минут. Его назвали «червь Уорхола» — в честь Энди Уорхола, автора изречения «В будущем каждый получит шанс на 15 минут славы». Эпидемия червя SQL Slammer, заразившего в 2003 году более 75 тысяч серверов за 10 минут, была близка к этой модели распространения.

Обычно скорость распространения червей меньше, так как они используют более сложные техники. Например, находят в компьютере список пользователей и пытаются взломать их пароли, чтобы атаковать и эти системы. В 2001 году во время эпидемии червя CodeRed II за 28 часов заразились около 350 тысяч узлов сети.

Почтовый червь действует несколько иначе. Попав в компьютер, он начинает рассылать сообщения всем контактам из адресной книги пользователя якобы от его имени. При этом червь для убедительности прикрепляет к сообщению

какой-либо файл с диска, предварительно заразив его. В результате адресат получит зловреда, а файлом-переносчиком может послужить любой документ: любовное письмо, конфиденциальный контракт, очень личная фотография или копия паспорта. Здесь мы уже видим и черты вируса: есть переносчик «болезни», а для заражения требуется опрометчивое действие человека. Хотя некоторые почтовые черви — например, Nimda — могут активироваться даже в режиме предварительного просмотра сообщений. Вы еще ни разу не кликнули на опасное письмо, а уже заразились.

Встречаются и другие типы червей, использующие уязвимости разных протоколов. Мы не собираемся изучать их во всех подробностях, но у нас есть вопрос: зачем их создатели это делают? Вариантов множество: от банального вредительства до скрытного майнинга криптовалют. Главное, что червь дает преступнику контроль над вашим устройством, и тот в результате может делать что угодно. Допустим, рассылать детскую порнографию. И когда в вашу дверь постучат сотрудники правоохранительных органов, вам придется доказывать, что вы были не в курсе, что конкретно делает ваш компьютер.

Трояны
Trojans

Это старый добрый троянский конь в декорациях компьютерной эры. Доверчивый пользователь

видит что-то полезное, загружает себе, открывает — а оттуда толпа разных зловредов.

Подобно древнегреческим воинам, вышедшим из деревянного коня, программа-троян открывает ворота вашей крепости, а дальше все происходит по уже известному сценарию: вредительство, кража данных, незаконное использование техники и прочее.

Например, получаете письмо от своего знакомого с приложенной картинкой — а это почтовый червь сам себя рассылает. Или скачиваете полезную программу с какого-то сайта, установили — и заразились. В отличие от обычных вирусов и червей, трояны не обладают механизмом репликации, но поскольку они хорошо замаскированы — спрятаны внутри «коня» — люди загружают их себе сами, часто — с удовольствием.

Специально для поклонников фирмы Apple: трояны уже стали обычным делом для маков и айфонов, тогда как обычные вирусы на этих устройствах встречаются редко. Все дело в том, что вы сами открываете дверь этому зловреду, и хваленая безопасность вендора здесь не имеет значения.

Вымогатели
Ransomware

Самый популярный на сегодняшний день тип зловреда — вымогатели. И своей популярностью вымогате-

ли обязаны предельно простой схеме монетизации: проникаешь в компьютер, шифруешь файлы (что чаще) или блокируешь систему — и вперед, требуешь выкуп. Обычно указываются сравнительно небольшие суммы — порядка 500 долларов. Поэтому многие пострадавшие предпочитают заплатить. Иногда преступники выполняют свое обещание — присылают ключи дешифровки. Иногда — нет.

Вымогателем может оказаться и вирус, и червь, и троян. Название происходит от слова 'ransom' — 'выкуп'. Оно отражает не механизм заражения, а суть действия зловреда. Этот способ криминального заработка зацвел буйным цветом с появлением криптовалют, когда стало практически невозможно отследить получателя выкупа.

Если вы стали жертвой вымогателей, не спешите им платить — сначала разберитесь, что за «зверь» на вас напал. Есть простые зловреды, которые только блокируют доступ к функциям системы, и от них, как правило, можно избавиться без выкупа.

С шифровальщиками дело обстоит хуже. Если зловред написан грамотно, то шансов взломать его шифр практически не существует. Тогда жертва встает перед выбором: платить или не платить. Отказ означает утерю всех своих данных. Но перед таким выбором может встать лишь тот пользователь, который не делает резервное копирование важ-

ных файлов. А кто регулярно их копирует, может с легким сердцем послать преступников в любом удобном направлении и восстановить данные.

Показательный случай произошел в ноябре 2016 года, когда троян HDDCryptor, известный также под именем Mamba, зашифровал более двух тысяч серверов Агентства муниципального транспорта Сан-Франциско (SFMTA) и потребовал выкуп в размере 100 биткоинов (на тот момент — 73 тысячи долларов). Система управления транспортом поездов от этой атаки не пострадала, но билетные автоматы и многие внутренние системы были выведены из строя.

Агентство блестяще справилось с ситуацией — просто выключило турникеты и открыло метро для бесплатного проезда. Горожане даже подумали, что это рекламная акция. Тем временем инженеры агентства восстановили данные из резервных копий, и уже на следующий день городской транспорт заработал в обычном режиме. Злоумышленник остался с носом[1].

Вы еще не озаботились резервным копированием ваших файлов? Это самый простой и надежный способ защиты от кибервымогателей, а заодно и от таких несчастий, как кража ноутбука или неожиданный потоп, устроенный соседями сверху.

1 *San Francisco Rail System Hacker Hacked. // Krebsonsecurity.com, 16 ноября 2016.*

Шпионы
Spyware

В отличие от вымогателей, программа-шпион ничем себя не выдает. Сидит себе тихо, собирает ваши данные и передает своему хозяину. Зачем? Как правило, жуликов интересуют только деньги. И чтобы украсть их у пользователя ПК, шпион охотится за номерами его счетов и банковских карт, логинами и паролями к интернет-банкам или даже к криптокошельку.

Но случается, что шпионским софтом пользуются правоохранительные органы или спецслужбы. Во многих странах это разрешено законодательством. К сожалению, трудно провести четкую грань, когда эти средства применяются для поимки настоящих преступников, а когда — для слежки за гражданами.

Что может делать шпион? Грубо говоря, все: подслушивать, подглядывать, читать вашу переписку, фиксировать местонахождение. Ну а дальше все зависит от планов владельца шпионской программы. Например, шпион может не размениваться по мелочам, а долго и упорно ждать поступления крупной суммы на счет — и как только она поступит, в один момент ее похитить.

Наверное, вам уже захотелось установить защиту от программ-шпионов, правда? Но не спешите. Здесь, как и в шпионских фильмах, полно двойных агентов.

Интернет кишит поддельными антишпионскими программами, разумеется, бесплатными. Но вместо того, чтобы защитить вас, они запустят в ваш компьютер стаю новых зловредов. Чтобы не попасться на эту удочку, предварительно изучите «досье» защитника, посмотрите отзывы об этом ПО в авторитетных источниках.

Рекламное ПО
Adware

Adware — зверек назойливый, но не слишком опасный. Как можно догадаться, его название происходит от слова 'advertisement' — 'реклама'. Его миссия состоит в том, чтобы показывать вам рекламные объявления, когда вы этого не хотите. Его излюбленное место обитания — браузер, ведь именно через браузер вы «смотрите» на мир.

Разработчики этого ПО получают доход от показов рекламы и кликов. Но если бы они показывали что-то стоящее! Чаще всего с помощью adware рекламируют такую ерунду, что кликнуть можно только случайно. И вы обязательно кликните, если весь экран будет завален всплывающими окнами, которые никак не получается закрыть! В этот момент автор зловреда и получит свою трудовую копеечку. Стоит ли объяснять, что он заинтересован, чтобы вы как можно дольше терпели все это рекламное безобразие на своем компьютере.

Поэтому создатели рекламного ПО стараются делать свои продукты приставучими, как репей. И преуспевают в этом. Чаще всего пользователю не удается самостоятельно удалить adware, и приходится прибегать к помощи антивирусов с соответствующим функционалом.

Но и рекламщики не дремлют. В 2015 году выяснилось, что рекламное ПО Vonteera отключает многие антивирусы, чтобы те его не удалили. А это уже за гранью. Если раньше еще можно было относиться к adware снисходительно, поскольку серьезной угрозы для пользователя это ПО не представляло, то теперь — нет. Отключение антивируса означает, что ваш компьютер остается беззащитным перед другими атаками, чего нельзя допускать ни в коем случае.

Таким образом, можно констатировать, что рекламное ПО окончательно перешло на темную сторону и является полноценным зловредом.

Фейковое ПО
Scareware

Строго говоря, scarware — не вполне зловред. Скорее это — безобидная бабочка стеклянница, притворяющаяся грозной осой. Scarware пытается напугать пользователя, чтобы тот сделал необдуманную покупку. Например,

фейковое ПО может сообщить, что ваш ПК вдруг заразился страшным вирусом, и если вы прямо сейчас не купите «противоядие», то рискуете остаться без компьютера.

Происходит имитация угрозы и навязывание покупки совершенно бесполезного товара. И хорошо, если просто бесполезного, а не зловредного. Правда, тогда это не scarware, а троян.

Казалось бы, банальный «развод», но это работает. Многие покупают навязываемые пустышки. Чтобы не оказаться в их числе, выберите доверенного поставщика средств антивирусной защиты, установите их и пользуйтесь. Как увидите всплывающее окно с информацией об инфекции, проверьте с помощью антивируса, насколько эта информация правдива. Если новоявленный спаситель предлагает отключить установленные средства защиты, это — стопроцентный зловред.

Различные «чистильщики реестра», «оптимизаторы Windows», «ускорители» и тому подобное часто оказываются фейками, имитирующими бурную деятельность. Они пытаются заманить пользователей яркими картинками, щедрыми скидками (до 90%!) и фантастическими обещаниями. Безусловно, среди них есть и полезные программы. И уход за ком-

пьютером действительно необходим. Но будьте бдительны, проверяйте репутацию продуктов и поставщиков.

К настоящему моменту проблема фейкового ПО достигла такого масштаба, что Microsoft объявил ему войну. С 1 марта 2018 года Windows Defender и другие продукты Microsoft начали классифицировать программы, отображающие принудительные сообщения как нежелательные и подлежащие удалению при обнаружении.

Руткиты
Rootkits

Руткит представляет собой набор программ, предназначенных для доступа к компьютеру в обход стандартных путей. Кроме того, он часто маскирует другое ПО, чтобы его не обнаружили ни пользователь, ни антивирус.

Название происходит от слова «root» — так во многих системах называлась учетная запись самого привилегированного пользователя. То есть руткит дает злоумышленнику администраторские полномочия, и тот может делать с вашим компьютером все, что ему заблагорассудится.

Классно, не правда ли? Одна проблема: как руткит незаметно установить на вашем ПК? Здесь

на помощь преступникам приходят наши старые знакомцы — трояны и социальная инженерия. Обнаружить руткит сложно, а удалить, случается, и вовсе невозможно. Иногда для этого требуется переустановка операционной системы или даже замена оборудования.

Известность руткиты получили после скандала с защитой от копирования компакт-дисков компании Sony BMG. Если бы в 2005 году вы купили один из 22 миллионов CD с записями поп-музыки и прослушали его на своем плеере, никаких проблем не случилось бы. А вот если бы вы решили прослушать этот диск на компьютере, то на нем без вашего согласия и без каких-либо предупреждений автоматически установилась бы DRM-система (Digital Rights Management — управление цифровыми правами).

Чтобы скрыть следы своей диверсии, Sony BMG добавила в пакет установки руткит, который изменял поведение Windows. В результате операционная система переставала видеть все файлы и папки с названиями, начинавшимися с символов «sys». Именно в такой папке и пряталась DRM-система звукозаписывающей компании.

Скандал разразился 31 октября 2005 года, когда исследователь компьютерных угроз Марк Руссинович (ныне технический директор Microsoft Azure) опубликовал в своем блоге подробный анализ программного обеспечения, установлен-

ного на его компьютер при проигрывании музыкального диска. Кроме блокировки копирования, этот секретный софт еще шпионил за пользователями, отправляя отчеты об их музыкальных привычках производителю.

В ответ на упреки в нарушении прав граждан один из руководителей Sony BMG Томас Хессе раздраженно заявил в интервью: «Большинство людей даже не знают, что такое руткит, так почему они должны волноваться об этом?» Да потому, что этот руткит, делая файлы и папки невидимыми для системы, включая антивирус, тем самым пробивал огромную брешь в безопасности компьютеров. И этим молниеносно воспользовались хакеры. Прошло всего девять дней, и появился вариант зловреда Breplibot, который использовал этот «подарок» от борцов с пиратством.

Бэкдоры
Backdoors

Буквально "backdoor" — «задняя дверь», или, как мы чаще называем, «черный ход». Это специально или случайно оставленная разработчиками лазейка, позволяющая получить доступ к данным или к удаленному управлению всей операционной системой в обход стандартных мер безопасности.

Зачем оставляются такие лазейки? Например, чтобы восстановить забытый вами пароль

и спасти ваши данные. Но некоторые вендоры утверждают, что никаких бэкдоров у них нет в принципе, и помочь они не в состоянии. В частности, Apple по этой причине отказалась вскрывать айфон террориста, несмотря на давление полиции.

Бэкдор — любой метод, с помощью которого авторизованные и неавторизованные пользователи могут обойти обычные меры безопасности и получить высокий уровень доступа пользователя (он же root-доступ) в компьютерной системе, сети или программном приложении.

Снифферы
Sniffers

Сниффер, или анализатор пакетов — программа для перехвата сетевого трафика. Полезная вещь, которую администраторы используют для диагностики сети, в том числе, для выявления вирусной активности, а хакеры применяют этот инструмент, чтобы украсть логины и пароли пользователей, особенно бесплатных wi-fi сетей.

Сам по себе сниффер — вполне легальная и нужная в хозяйстве штука, примерно как отвертка в доме. Представляете, сколько на свете продается разных отверток? Вот и снифферы предлагаются в избытке. А это означает высокую вероятность того, что кто-то может использовать их в корыстных целях.

Известны случаи установки сниффера на компьютер жертвы при помощи трояна, а, установив сниффер, преступник может удаленно анализировать ваш сетевой трафик — со всеми вытекающими неприятными последствиями.

Ботнет
Botnet

Ботнеты — сети из зараженных компьютеров «зомби», которые могут использоваться для DDoS-атак, рассылки спама, распространения вирусов и других деструктивных действий. На каждом из «зомби» установлен специальный агент — бот, находящийся в «спячке», пока не поступит команда от хозяина сети.

Некоторые ботнеты достигают огромных размеров. Например, Necrus, появившийся в 2012 году и здравствующий до сих пор, содержит шесть миллионов зараженных устройств. В ноябре 2017 года с его помощью преступники осуществили рассылку нового штамма вируса-шифровальщика Scarab. В результате массовой компании было отправлено около 12,5 миллионов инфицированных электронных писем. Скорость рассылки превысила 2 миллиона писем в час.

В «зомби» могут превратиться не только компьютеры, но и любые умные устройства, подключенные к сети: веб-камеры, телевизоры,

пылесосы, кофеварки и даже лампочки. Ведь для участия в DDoS-атаке много ума не требуется, достаточно постоянно посылать один и тот же запрос на указанный адрес.

Например, летом 2016 года — во время Олимпийских игр в Рио-де-Жанейро — один из ботнетов, основу которого составляли около 10 тысяч зараженных веб-камер, проводил многочисленные и продолжительные DDoS-атаки. Но, несмотря на участившиеся подобные случаи, производители IoT-устройств пока не слишком задумываются об их безопасности.

Майнеры
Miners

Когда стоимость биткоина резко взлетела вверх, киберперступники тут же придумали новый способ заработка: на компьютер жертвы тайно устанавливается майнер криптовалюты, который работает на благо своего владельца, но за счет хозяина оборудования. Таким образом, преступник получает свои монеты практически задаром, а вы платите за электричество и недоумеваете, почему ваш ПК так медленно работает.

Майнер не крадет ваши деньги и данные, он просто использует ваши ресурсы. По сравнению с прочими видами угроз эта, надо признать, не самая страшная. Но все равно обидно!

Мобильные зловреды
Mobile malware

Смартфон, младший брат компьютера, болеет теми же болезнями, что и старший братишка. Есть мобильные вирусы, трояны, кейлоггеры, шпионы, вымогатели, ботнеты и даже майнеры криптовалют. Предсказуемо, что, на Android их больше, но и на iOS зловреды тоже достаточно частые гости. Считать, что устройства Apple на 100% безопасны, было бы весьма наивно.

Встречаются на мобильных устройствах и специфические вредоносы. Например, одним из первых способов заработка, придуманных мошенниками, была отправка SMS на платные короткие номера.

Также весьма востребован в преступном мире перехват звонков и особенно SMS. Это не только позволяет ревнивым мужьям и женам удовлетворить свое любопытство (к слову, с нарушением Уголовного кодекса РФ), но еще и помогает воровать деньги со счетов.

Даже если вы устанавливаете приложения только из официальных магазинов, это еще не гарантия от рисков. Зловреды проникают и в продукты из официальных магазинов — под видом нормальных приложений. Еще одна уловка жуликов — chargeware. Это ПО совершает покупки через приложения без вашего ведома. Никаких оповещений на экране вы не увидите, а деньги уплывут в неизвестном направлении.

Разумеется, это не исчерпывающий перечень угроз, к тому же их число постоянно растет. Чтобы оценить, какое вредоносное ПО наиболее популярно на подпольных форумах, исследователи Insikt Group проанализировали около четырех миллионов сообщений на русском, английском, китайском и других языках. В период с мая 2018 по май 2019 года они выявили более 100 тысяч вариантов вредоносных программ в 61 категории[1].

Перед любым продавцом вредоносного ПО стоит серьезная проблема: как бороться с конкуренцией, особенно с альтернативными продуктами? В ход идут известные маркетинговые приемы. Продавцы троянов и спам-сервисов предоставляют праздничные скидки, а надежные анонимные хостеры выплачивают реферальные бонусы существующим клиентам, отправляющим к ним новых заказчиков — прямо как в акциях «приведи друга».

Но преступник и честность — понятия несовместимые. На этом подпольном рынке процветает обман и надувательство. Например, был случай, когда продавец программы-вымогателя встроил в свой продукт еще и майнер биткоинов, который работал на компьютере покупателя. Но покупатели не остаются в долгу — malware взламывают так же, как и обычный коммерческий софт, а разработчики жалуются на пиратов, использующих их продукты без лицензии. Вот уж воистину «вор у вора дубинку украл».

---

1 *Bestsellers in the Underground Economy: Measuring Malware Popularity by Forum, 2019.*

Кибероружие

Правительства многих стран берут на вооружение хакерские методы и разрабатывают кибероружие. Перед этим оружием ставятся самые разные задачи: от обычного шпионажа до выведения из строя промышленных объектов или даже провоцирования катастроф.

Впервые о кибероружии заговорили в 2010 году, когда был обнаружен червь Stuxnet. Существует предположение, что этот червь — специализированная разработка спецслужб Израиля и США, направленная против завода по обогащению урана в Иране. Естественно, этого никто не признал.

> *Stuxnet — непростой червь. Он поражал не все компьютеры, а только определенной модели Siemens S7-417, применяемой на химических заводах. И не все подряд, а лишь те, которые использовались для настройки программируемых логических контроллеров — устройств, непосредственно управляющих работой оборудования. Для этого червь проверял наличие в компьютере специального софта Step 7. Но это еще не все. Червь активировался только в тот момент, когда к зараженному компьютеру подключали для настройки высокочастотные преобразователи энергии. И, опять же, не абы какие преобразователи, а произведенные компанией VaCom. Как раз такие использовались на иранском заводе.*

В итоге Stuxnet нарушил работу почти 1000 центрифуг для обогащения урана. При этом авторы червя сумели настолько ловко замести следы, что иранские специалисты списали инцидент на ме-

ханические проблемы с оборудованием. Очень может быть, что этот эпизод стал первым случаем успешного применения кибероружия.

Наши домашние устройства вряд ли станут целями столь мощных и изощренных атак. Но эта история интересна нам тем, что червя Stuxnet не заметил ни один антивирус. Его обнаружили лишь годом позже, когда он уже успел выполнить свою задачу. Отсюда неутешительный вывод: в киберпространстве нападающая сторона имеет преимущество, а, следовательно, наши средства защиты, увы, не всегда смогут защитить наши ПК.

В киберпространстве нападающая сторона имеет преимущество, а, следовательно, значит, наши средства защиты не всегда смогут защитить наши ПК.

Так что же делать? Неужели сдаваться?

Нет. Просто нужно научиться осмотрительности, ведь основная причина подавляющего большинства случаев заражения и других неприятных инцидентов — человеческий фактор, то есть мы с вами. Беспечные пользователи.

Берегите свои данные!

Контрольные вопросы

1. Что такое вирусы? Когда они появились?

2. Какие разновидности зловредов вы знаете?

3. Как трояны попадают в компьютер?
4. Что значит DDoS?
5. Что такое ботнеты и зачем они нужны?
6. Что такое вирус-шифровальщик и в чем его опасность?
7. Какой лучший способ защиты от вируса-вымогателя?
8. Чем плохо рекламное ПО (adware)?
9. Зачем создается фейковое ПО?
10. Что такое руткит и в чем его опасность?
11. Как избежать заражения своего компьютера?
12. Насколько безопасны айфоны?
13. Какие особые типы вирусов поражают смартфоны?

Глава 5

Остапы Бендеры наших дней

Киберпреступники прекрасно знают, что самым слабым звеном любой системы остается человек: «взломать» его проще, чем обойти технические средства защиты. Социальная инженерия — это психологическая атака, с помощью которой злоумышленник заставляет вас делать то, чего вы делать не должны.
В этой главе мы рассмотрим различные сценарии использования социальной инженерии и способы противодействия им.

Великому Комбинатору наше время наверняка бы понравилось. Его род занятий в современных терминах можно определить именно как социальную инженерию — метод психологического воздействия на человека с целью вынудить его совершить то, что выгодно злоумышленнику. Остап Ибрагимович оценил бы достоинства цифровых технологий: когда нет прямого контакта с потенциальной жертвой, то нет и риска получить шахматным конем по голове, если обман раскроется.

И последователи Остапа Бендера весьма преуспевают на этом поприще, ибо люди все так же доверчивы и готовы отдать «ключ от квартиры, где деньги лежат» первому встречному, который пообщается с ними дружелюбно и авторитетно.

> *Увы, стопроцентной защиты от профессиональных обманщиков нет — даже специалисты по информационной безопасности иногда попадаются на их уловки, не говоря уже об обычных пользователях.*

Секрет успеха социальных инженеров в том, что они ловко используют против нас наши же чувства и эмоции: жадность, страх, любопытство, сострадание, альтруизм, и даже любовь. Моральных барьеров для них не существует; нет такой подлости, на которую они не пойдут ради наживы. Они могут выманивать последние деньги у стариков, вовлекать подростков в торговлю наркотиками и сдавать их после этого полиции, или давить на жалость, собирая пожертвования якобы на операцию тяжелобольному ребенку.

Чаще всего интерес преступников носит чисто коммерческий характер. Их цель, выражаясь их же языком, — «развести» человека на деньги, поэтому дети обычно представляют для этой

публики меньший интерес, чем взрослые. Но успокаиваться было бы ошибкой. Во-первых, дети вырастут, заведут собственные счета в банках и тоже станут объектом охоты, а, значит, они должны быть подготовлены к взрослой жизни. Во-вторых, монетизация социальной инженерии может быть и не столь прямой, но куда более циничной и опасной. Например, некто может уговорить девочку-подростка всего на одну фотографию в обнаженном виде — и эта фотография сломает ей жизнь, как это случилось с Амандой Тодд[1].

Некто может уговорить девочку-подростка всего на одну фотографию в обнаженном виде — и эта фотография сломает ей жизнь.

Увы, несмотря на все усилия полиции в разных странах, рынок детской порнографии существует, и кто-то зарабатывает на этом. Целью может быть и вербовка в экстремистские организации и деструктивные сообщества, что тоже хорошо оплачивается заинтересованными политическими структурами.

Тем не менее, руки опускать не стоит. Соблюдая ряд простых правил, можно значительно снизить риск пополнить статистику жертв компьютерных преступлений, совершаемых при помощи социальной инженерии. Для этого следует познакомиться с их основными приемами и научиться постоянной бдительности. Главное — не стать при этом законченным параноиком. Сложно? Да! Мир чрезвычайно усложнился. Но надо учиться в нем жить.

«Доверяй, но проверяй» — советует эксперт по информационной безопасности Алексей Лукацкий:

1 *См. главу про кибербуллинг.*

«В сфере безопасности доверие — именно та точка, с которой начинается провал. Сейчас среди специалистов в этой области широко распространена концепция Zero Trust Security — «безопасность с нулевым доверием». Мы изначально исходим из того, что никакого доверия быть не должно, и рассматриваем протоколы и программы, исходя из того, что против нас действует враг, который может подменить кого-то, выдать себя за кого-то и т.п. Подобную стратегию я рекомендую и обычным пользователям. Конечно, это работает далеко не всегда: ведь человеку присуще испытывать доверие, и именно этим пользуются киберпреступники. А если не доверять никому, то жить становится неинтересно, грустно и тяжело»[1].

На жадину не нужен нож

В 1990-х годах, когда все пользовались в основном наличными деньгами, а не карточками, уличные мошенники широко практиковали такой сценарий: вы идете по оживленной улице, и вдруг неожиданно вам под ноги падает тугая пачка долларов. В ту же секунду появляется случайный прохожий, который восклицает: «Вот нам повезло!», — и предлагает поделить деньги. Даже если у вас и были моральные терзания из серии «А может, отдать хозяину?», ваш новый знакомец быстро их гасит и настойчиво предлагает отойти в укромное место, чтобы пересчитать добычу. В этот момент появляется «потерпевший»

1 *Алексей Лукацкий. «Не заклеивайте камеру!» 8 правил кибербезопасности для всех. // Идеономика (**ideanomics.ru**), 23 января 2018.*

(как правило, не один), и, даже если вы готовы с радостью вернуть пропажу, вы все равно «попали» на деньги, потому что мошенник утверждает, что в пачке было больше, чем вы отдали, а поскольку перевес в физической силе на его стороне, то спорить бесполезно — приходится выворачивать карманы якобы для более точного пересчета. Тут-то вас и обчистят.

> *Встречалось множество вариаций этой схемы, но итог был один — вы в минусе, преступники в плюсе. Нехитрый спектакль разыгрывали на улицах до тех пор, пока большинство людей не узнали о ловушке и не перестали в нее попадаться. Доходность промысла упала, и жулики переключились на другие способы обмана граждан.*

Помню, как-то раз и мне выпала такая «удача» на Манежной площади, но я проигнорировал свой шанс немного разбогатеть, несмотря на уговоры внезапно материализовавшегося возле меня товарища, чем его очень расстроил. Не то чтобы я был такой умный и проницательный, просто несколькими днями раньше мне попалась статья о таком способе обмана, и вовремя полученное знание уберегло меня от неприятностей.

Даже когда здравый смысл кричит «Это ловушка!», жадность шепчет «Все получится!» — и человек отдает деньги.

Тогда основным источником информации были газеты и «сарафанное радио», теперь — интернет и социальные сети. Казалось бы, все фокусы жуликов давно описаны и разобраны по шагам, но люди все равно продолжают попадаться на самые примитивные «разводки». Причина, по-видимому, заключается в том, что почти все мы в какой-то мере инфицированы вирусом

жадности, вакцину от которого так и не изобрели. Даже когда здравый смысл кричит «Это ловушка!», жадность шепчет «Все получится!» — и человек отдает деньги, порой весьма немалые, ловким пройдохам просто потому, что они сочинили красивую сказку, в которую так и хочется поверить.

> *Иначе как объяснить недавний случай, когда женщина из Камбоджи отдала 75 тысяч долларов выпускнику средней школы в Нигерии, который создал в Instagram фальшивый аккаунт и прикинулся американским пилотом[1]? Все было как обычно: они познакомились в сети, и он, что называется, напел ей про красивую жизнь летчика и большие заработки, а потом предложил вместе провернуть одно дельце: дескать, он пришлет ей дорогих вещей на 500 тысяч долларов, чтобы продать их и вложить деньги в камбоджийскую недвижимость. Но... прежде ей нужно будет оплатить пошлину. (Как можно поверить в такую чушь? Не спрашивайте!). Для вящей убедительности «летчик» подключил к афере друга из Индонезии, изображавшего сотрудника курьерской почты. За первую посылку сообщники попросили 800 долларов; потом якобы возникли трудности, и нужно было доплатить еще (как всегда), и так далее — камбоджийка все платила и платила, втянувшись в эту игру, и даже взяла кредит в банке.*

Жадность — болезнь почти неизлечимая, она поражает мозг, блокируя критическое мышление, причем не только жертвы, но и преступников. Ведь они сорвали весьма солидный

---

1 *19-year-old impersonates American pilot, defrauds woman of N27m. // PUNCH, 29.02.2020.*

куш, на который и рассчитывать не могли! Пора было бы и остановиться — но нет. А зря!

> *В минуту просветления несчастная жертва заметила, что «американский пилот» звонит ей с нигерийского номера, и обратилась в полицию. Дальнейшее было делом техники — начинающего социального инженера отследили по SIM-карте и арестовали.*

Этого лжепилота по имени Чигемезу Арикибе можно признать достойным продолжателем национальных традиций. Его старшие товарищи рассылали знаменитые «нигерийские письма» по всему миру, начиная с 1980-х годов (в бумажном виде, разумеется). С появлением электронной почты дело поставили на поток, и вряд ли можно найти человека, ни разу не получавшего подобный спам. Обычно в таком письме рассказывается душещипательная история про принца или принцессу, томящегося в лагере беженцев, бывшего министра, убитого повстанцами, внезапно умершего богатого бизнесмена, не оставившего наследников, и тому подобное. Суть всегда одна: якобы в некоем банке зависли огромные деньги, и с вашей помощью их можно вытащить — за что вам обещают щедрое вознаграждение. То есть вам предлагают соучастие в преступлении, если называть вещи своими именами, и, как ни странно, многие соглашаются.

Сюжеты «нигерийских писем» настолько фантастичны и абсурдны, что поверить в этот бред может только абсолютно неадекватный человек, неспособный усомниться и просто погуглить, проверить: есть ли хоть крупица правды в полученном письме. За творческий подход к сочинительству авторам

«нигерийских писем» в 2005 году даже коллективно присудили Шнобелевскую премию[1] по литературе. Однако на церемонию награждения никто не явился — лауреаты предпочли остаться анонимными.

Пожалуй, наиболее блестящим образцом этого жанра можно считать историю нигерийского космонавта, застрявшего на орбите:

> *«Меня зовут Бакаре Тунде, я брат первого нигерийского космонавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским космонавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-163» к секретной советской космической станции «Салют-8Т». В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли «Прогресс» снабжают его необходимым. Несмотря ни на что, мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата*

1 *Шнобелевская (Игнобелевская, Антинобелевская) премия (англ. Ig Nobel Prize, от игры слов: англ. ignoble — «постыдный») — пародия на престижную международную награду — Нобелевскую премию. Десять Шнобелевских премий вручаются в начале октября, то есть в то время, когда называются лауреаты настоящей Нобелевской премии, — «за достижения, которые заставляют сначала засмеяться, а потом — задуматься» (first make people laugh, and then make them think) (Википедия).*

составила 15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем оплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами.

Вечно ваш, доктор Бакаре Тунде, ведущий специалист по астронавтике».

Нормальный человек посмеется над этим и пройдет мимо. Однако в столь несуразном на первый взгляд подходе есть свой смысл: люди даже с минимальными зачатками рационального мышления отсекаются сразу, что экономит ресурсы мошенников. Ведь если «клиент» «заглотил наживку», приходится вступать с ним в личный контакт, отвечать на его вопросы, разговаривать по телефону, а это требует времени и дополнительных расходов.

Схема стала настолько популярной, что у нее появилось собственное название — «Разводка 419» («Scam 419»), по номеру соответствующей статьи в уголовном кодексе Нигерии. Поскольку криминальное сообщество не уважает авторские права, эту схему стали использовать мошенники всех стран — разумеется, без каких-либо отчислений ее изобретателям, так что «нигерийской» считать ее можно весьма условно. Отправитель письма может находиться где угодно — в Латвии, Египте, США, Мексике, Украине, Венгрии, Малайзии, Колумбии и, само собой, в России. Нигерия больше не удерживает пальму первенства

в этом виде жульничества, но из-за общей бедности и высокого уровня коррупции для многих молодых нигерийцев такой способ заработка остается едва ли не единственно возможным и, кстати, весьма доходным — некоторым из них удается получить до 60 тысяч долларов в год. С такими деньгами в Африке действительно можно жить как принц или космонавт. И даже лучше.

Конечно же, вы не настолько наивны, чтобы принять участие в спасении Абака Тунде с борта станции «Салют», которая, как выясняется, не затонула в Тихом океане, а все летает и летает вокруг Земли с несчастным нигерийцем на борту. Означает ли это, что вас нельзя поймать на крючок жадности? Едва ли. Пусть отечественные коллеги нигерийских мошенников и не прославились литературными шедеврами, но действуют они не менее изобретательно.

> *Например, вам приходит SMS, в котором говорится о выигрыше в лотерее с новенькой Audi в качестве приза. (Мне приходило). Но сначала вам нужно перечислить небольшую сумму, чтобы подтвердить свое участие, или просто послать ответное SMS на указанный номер, который… оказывается платным. И сколько б не твердили миру про бесплатный сыр, который бывает только в мышеловке, азарт и жадность снова выигрывают у логики.*
>
> *Бывает и проще: вам говорят (или пишут), что вы выиграли небольшой денежный приз, и просят сообщить данные банковской карты. Правда, чуть больше данных, чем нужно для перевода, зато вполне достаточно для снятия. Что удивительно, попадаются на эту разводку преимущественно мужчины среднего возраста с опытом работы в силовых*

структурах. Может быть потому, что рисковать — дело для них привычное?

Таких сценариев множество, рассказать про все нереально. Помните, Остап Бендер говорил, что знает четыреста относительно честных способов отъема денег у населения? Он не преувеличивал. Главное, что следует уяснить: не будьте самонадеянны! Мошенники постоянно оттачивают свои приемы и изобретают новые. Не считайте себя умнее их, потому что вас могут подловить как раз на знании общеизвестных схем.

Не будьте самонадеянны! Мошенники постоянно оттачивают свои приемы и изобретают новые.

Например, в письме будет сказано, что отдел борьбы с компьютерными преступлениями полиции Нигерии арестовал шайку спамеров; в их списке рассылки обнаружен ваш адрес, поэтому вам, как пострадавшему, причитается компенсация; сообщите, пожалуйста, данные вашей карты. К гадалке не ходи: жадность снова уговорит кого-то сделать очередную глупость.

Или вот еще относительно новый прием[1], специально для технически подкованных жадин. На ваш телефон несколько раз звонят с какого-то неизвестного номера и сразу сбрасывают. Что делает заботящийся о своей безопасности человек? Правильно: он гуглит подозрительный номер и — о, чудо! — видит ссылку на страницу, где владелец номера, похоже, пытался сделать перевод в криптовалюте, но у него чуть-чуть не хватило средств для завершения транзакции — система сообщает, что на счету

1 *Высокотехнологичные нигерийские письма. // **Habr.com**, 14 июля 2019.*

должно быть минимум 2,5 биткоина. Сессия осталась открытой (вот же он лох!), нужно всего-то кинуть на этот кошелек 0,01 битка, указать свой адрес в качестве получателя и вуаля — тысяч 15–20 долларов у вас в кармане!

А на самом деле? На самом деле, сто наивных любителей халявы вроде вас — и целый биткоин в кошельке криптожуликов, причем никто не побежит жаловаться. Гениально!

«Это звонок из службы безопасности банка...»

Кроме жадности, социальные инженеры активно эксплуатируют наше чувство страха. Нет, им для этого не надо внезапно выскакивать из монитора или рассказывать на ночь леденящие душу истории типа «черной-черной ночью в черной-черной комнате...» Все куда прозаичнее: они играют на страхе человека потерять деньги.

Звонящий представляется сотрудником службы безопасности банка и говорит, что с вашего счета вот-вот уйдет крупная сумма, и если прямо сию минуту ничего не предпринять, то будет поздно. В такой ситуации человек может запаниковать и, не успев ничего сообразить, выдать мошенникам нужную им информацию. И вот тогда действительно его счет выпотрошат в ноль.

Добавит печали осознание факта, что денег вам никто не вернет. Закон в этом случае будет на стороне банка: если клиент в результате обмана или злоупотребления доверием сам нарушил условия

договора, обязывающие сохранять конфиденциальность платежной информации, и сообщил ворам номер карты, пароль, присланный в SMS, CVV-код и другие сведения, то компенсации ему не положено.

> *В 2019 г. мошенники провели около 577 000 операций с использованием электронных средств платежа без согласия клиентов банков — физических и юридических лиц. Сумма таких операций превысила 6,4 млрд руб., подсчитал ФинЦЕРТ (Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России). Средняя сумма похищенного со счетов физлиц составила 10 000 руб., юрлиц — 152 000 руб. Банки возместили клиентам 935 млн. руб., — говорится в отчете, то есть примерно один рубль из семи похищенных (15%). Статистику возвратов ЦБ публикует впервые*[1].

Телефонные мошенники нашли «золотую жилу» и будут ее разрабатывать, пока денежный поток не иссякнет. Число пользователей банковских услуг растет, увеличивается и число потенциальных мишеней преступников. Остановить эту волну может только осведомленность людей о таком способе обмана.

К сожалению, пресечь на корню саму возможность телефонного мошенничества силами правоохранителей едва ли получится, ведь преступники могут находиться где угодно, необязательно в России, а телефонная сеть в принципе устроена так, что можно позвонить

---

1 *Мошенники в прошлом году украли у клиентов банков 6,4 млрд рублей. // Ведомости, 19 февраля 2020.*

с любого номера на любой другой. Блокировать телефоны мошенников в такой ситуации технически и юридически очень сложно.

На первых порах подпольные колл-центры организовывали в местах лишения свободы, сейчас — в обычных офисах или квартирах. Полиция может поймать одну шайку, но ей на смену придет новая. Порог входа в этот «бизнес» низкий, доходность высокая, риски небольшие. Нужно лишь найти несколько молодых людей с хорошо подвешенным языком, базу номеров для обзвона, и можно начинать. Кстати, совершенно необязательно красть базу данных из банка.

> *«По сути, для завязки разговора всего-то нужно знать номер телефона, фамилию, имя и отчество. Основной сценарий, который используют злоумышленники, кстати, не предполагает знания, в каком банке у клиента открыт счет, — говорит Артем Сычев[1], замдиректора департамента Банка России по информационной безопасности. — Человека «раскручивают» на то, чтобы он сам рассказал, в каком банке обслуживается, какие у него счета, какие операции он совершает; чтобы назвал злоумышленнику номер карты, подтвердил, что ему пришла эсэмэска с паролем. На данный момент нам известны 15 различных мошеннических сценариев. Утечки баз данных, к сожалению, действительно есть. Но информация о клиентах, утекшая из банков, — это капля в море по сравнению с тем количеством людей, которых обзванивают мошенники».*

Но есть и хорошие новости. По сравнению с 2018 годом клиенты банков стали осторожнее: тогда на социальную инженерию прихо-

1 *Телефон недоверия. // Российская газета, 16 февраля 2020.*

дилось 97% мошеннических операций, а в 2019 — только 69%. Прогресс налицо, и если так пойдет дальше, то через год-другой эта схема станет нерентабельной.

Пока же интересно и неожиданно то, что жертвами обмана чаще всего становятся не пенсионеры, как можно было бы подумать, а экономически активные граждане в возрасте от 28 до 55 лет. Но и это вполне объяснимо: во-первых, у них есть деньги; во-вторых, они активно пользуются технологиями и в целом доверяют им, ведь если жулики позвонят какой-нибудь бабушке и даже уговорят ее сказать им пароль от интернет-банка, она все равно едва ли сможет его найти. А вот продвинутый пользователь это сделает запросто. Для особо бдительных, которые помнят, что никому нельзя сообщать пароли и пин-коды (в том числе и сотрудникам банка), предусмотрена еще одна ловушка: их переключают на «автоматизированную систему», которая, как нетрудно догадаться, есть лишь имитация настоящей.

Поэтому, хотя об этом много раз говорили, не лишним будет напомнить:

> *Если вам позвонили из банка, не пытайтесь угадать, настоящий это звонок или разводка. Уточните причину и сами перезвоните в банк по заранее сохраненному номеру на своем телефоне. Или зайдите в мобильное приложение и задайте вопрос в чате. Оба эти способа вполне надежны.*

И еще раз: все входящие телефонные звонки — какой бы номер на экране ни высвечивался — по определению считаются подозрительными. Финансовые вопросы по таким каналам обсуждать категорически нельзя!

Если друг оказался вдруг... взломан

«Не имей сто рублей, а имей сто друзей» — гласит пословица, известная всем со школы. В трудную минуту мы обращаемся к друзьям за помощью и готовы ответить им тем же.

А где сейчас все наши друзья? Правильно, в мессенджерах и соцсетях. Этим и пользуются мошенники: взломав чей-либо аккаунт, они начинают рассылать просьбы перечислить денег по всему списку контактов. А нас же учили, что «друг в беде не бросит, лишнего не спросит», правда? 500 рублей на телефон? Надо так надо, не приставать же с расспросами, когда у человека и так проблемы. И сумма эта вовсе не предел — иногда люди отдают злоумышленникам куда больше, поверив в легенду, которую им подсунули.

Казалось бы, все знают и про этот прием социальной инженерии, и про то, что лучше позвонить и удостовериться: друг ли это обращается к вам или мошенник. Но мы настолько привыкли к общению в текстовом формате, что этот нехитрый трюк часто срабатывает. Задним умом крепки все, но прежде, чем упрекать кого-то в излишней доверчивости, вспомните: социнженеры — хорошие психологи, они прекрасно понимают, что один-единственный звонок раскроет их обман, и придумают дюжину убедительных причин, почему пообщаться голосом никак невозможно, а дело срочное.

Например, человек находится в другой стране, телефон украли, пишет он вам с чужого компьютера, и единственный пароль, который смог вспомнить, это пароль от Skype. Ваши действия? Здравый смысл подсказывает, что все выглядит подозрительно,

и что именно Skype чаще всего и взламывают. Но что, если ваш приятель действительно попал в беду?

Прежде чем расстаться с деньгами, постарайтесь проверить, кто же на самом деле с вами общается.

Прежде чем расстаться с деньгами, постарайтесь проверить, кто же на самом деле с вами общается. Первое, что приходит на ум, — задать вопрос, ответ на который знает только ваш друг. Так в фильме «Гостья из будущего» Коля Герасимов проверял, точно ли перед ним его друг Фима, а не космический пират:

— Как прозвище нашего физкультурника?
— Илья Муромец.
— А, это ты, Королёв.
— Честное пионерское.

Хороший способ, но есть одна проблема: если вы закончили школу лет 10–20 назад, то можете и не вспомнить прозвище вашего физкультурника. А как быть, если ваш друг тоже его забыл? Да и вообще, трудно сходу придумать уникальный вопрос для каждого — нас ведь связывают с разными друзьями очень разные вещи.

Поэтому лучше обратиться к опыту капитана Алехина из романа Владимира Богомолова «В августе 44-го».

> *В кульминационный момент его группа встречает в лесу опаснейшего немецкого агента в сопровождении двух пособников. Все трое — в советской форме, документы у всех в порядке, отвечают уверенно, держатся естественно. Мо-*

жет, и вправду свои? Чтобы вывести врага на чистую воду, Алехин как бы невзначай задает вопрос о несуществующем персонаже — некоей поварихе, якобы служившей в том госпитале, где он якобы лежал, и где, судя по документам, лечился подозреваемый.

«Нет, не знаю, — после некоторой, пожалуй, излишне затянутой паузы угрюмо сказал старший лейтенант. — Я поварихами не интересовался!»

А что тут ответишь с ходу? Сказать: «Знаю», — а вдруг это вопрос-ловушка, и никакой такой поварихи там нет? Сказать: «Не знаю», — а если это опять же ловушка, и она там — местная знаменитость, которую не знать просто невозможно?

Алехин же, провоцируя «лейтенанта», просто внимательно следил за его реакцией. И того выдала излишняя напряженность в ответе на второстепенный, казалось бы, вопрос. Потому пользуйтесь приемом особистов СМЕРШа, если у вас возникли даже малейшие сомнения в вашем собеседнике. «Бдительностью дело не испортишь!» — говорил капитан Алехин, и, безусловно, был прав.

Бывает и так, что взломали ваш аккаунт, а ваши друзья оказались не столь бдительны и откликнулись на ложный призыв о помощи. Ситуация неловкая: с одной стороны, они сами виноваты; с другой — вы пусть и невольная, но причина их финансовых потерь. Возмещать им понесенный урон или нет? Формально вы не обязаны, не поддавайтесь первому порыву, обдумайте случившееся спокойно. А потом уже решайте.

Ловись, рыбка, большая и маленькая

Любопытство и невнимательность — еще два свойства человеческой натуры, тянущие нас в западни, расставленные социальными инженерами. Принцип действия таких ловушек чрезвычайно прост: пользователь получает письмо или сообщение с интригующим содержанием, открывает вложенный файл или кликает по ссылке — и он попался! Его данные утекают к злоумышленникам, которые даже не потрудились взломать систему или расшифровать пароль.

Такой способ кражи логинов и паролей, телефонов, номеров кредитных карт и других конфиденциальных данных называется **фишинг** и считается одним из методов социальной инженерии, требующим также и технических навыков.

> *Английский термин "phishing" — это неологизм, образованный как омофон (то есть звучит одинаково, а пишется по-разному) от слова "fishing" (по-русски — «рыбалка»), что довольно точно передает суть явления: хакер забрасывает наживку и ждет, пока пользователь «клюнет», то есть откроет зараженный файл или перейдет по ссылке.*
>
> *Происходит этот термин от сочетания слов "phreak" и "fishing". В свою очередь, "phreak" родилось из "phone" и "freak". В 1970-х так называли технически продвинутых фриков, которые взламывали телефонные сети ради бесплатных звонков или других фокусов.*
>
> *Само же исходное слово "freak" имеет богатую и запутанную историю, уходящую корнями в XVI век. По-русски можно сказать «чудак», но это не передаст всех смыслов оригинала.*

Есть три варианта фишинга. В первом происходит заражение вирусом-троянцем, который спрятан во вложенном файле или на сайте, куда ведет ссылка. Этот троянец установит на ваше устройство бэкдор[1], который превратит компьютер в узел ботнет-сети, и кейлоггер[2], который украдет ваши логины и пароли, и майнер криптовалют[3] — все, чего пожелает взломщик.

Во втором варианте ссылка ведет на поддельный сайт — например, государственного органа, где вас попросят ввести свои данные. Визуально подделка выглядит точь-в-точь как настоящий сайт, и едва ли вы что-то заподозрите. Например, в почту вам пришло уведомление о штрафе от ГИБДД. Если у вас есть машина, то вы захотите узнать, где именно вы нарушили правила, а если нет — возмутиться и сообщить об ошибке. Но сначала вас попросят авторизоваться — как на настоящем сайте Госуслуг. Чаще всего подделывают сайты банков, авиакомпаний, государственных учреждений, интернет-магазинов и так далее — то есть те, где ввод платежных и персональных данных выглядит естественно.

---

1 *Бэкдор (от англ. back door — «черный ход», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.*

2 *Кейлоггер (англ. keylogger) — программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.*

3 *Под скрытым майнером подразумевается программа-вирус, которая использует ресурсы вашего компьютера для добычи криптовалют. Делается это в автоматическом режиме без ведома пользователя и каких-либо предупреждений.*

При появлении фишинговой страницы счет идет на часы, иногда — на минуты, поскольку пользователи несут серьезный финансовый, а если это компания, то еще и репутационный ущерб. Некоторые фишинговые страницы менее чем за сутки нанесли ущерб на суммы от миллиона рублей[1].

Есть еще и третий вариант, когда фишинговый сайт или приложение создаются под видом полезного ресурса. Особенно фишеры любят маскироваться под бесплатный антивирус — программу для оптимизации работы компьютера и тому подобное. Более того, иногда они даже работают. Самый анекдотичный, но вполне реальный случай — сайт, предлагающий проверить, есть ли ваша кредитная карта в базе данных хакеров. Вы вводите номер и другие реквизиты — и теперь ваша карта точно у них есть. Как это ни смешно, находятся те, кто им верит.

Можно ли защититься от фишинга техническими средствами? От первого варианта — практически нет. Человек сам принимает решение открыть файл или перейти по ссылке, то есть открывает дверь злоумышленникам. Можно только уповать на то, что антивирус отследит подозрительную активность троянца, или что браузер предупредит о небезопасном сайте, но это уже вторая линия обороны, и она тоже может пропустить атаку.

Популярный совет «Не открывать подозрительные файлы и ссылки» в реальной жизни помогает мало.

1 *Деньги на ветер: почему ваш антифишинг не детектирует фишинговые сайты и как Data Science заставит его работать? // **Habr.com**, блог Group IB, 31 августа 2018.*

Популярный совет «Не открывать подозрительные файлы и ссылки» в реальной жизни помогает мало. Потому что никто вам не скажет, чем (в общем случае) подозрительная ссылка отличается от неподозрительной. Правильным будет считать подозрительными все спам-рассылки и сообщения от незнакомцев, но письмо может прийти от кого угодно — в том числе от вашего друга, почту которого взломали. И текст будет абсолютно правдоподобным, разве что вас немного удивит фраза «Вот фотки с корпоратива, которые я обещал», а вы ничего такого не припоминаете. Но любопытство вполне может пересилить чувство осторожности... Так что нам остается полагаться только на интуицию и здравый смысл. И — что ж поделать — быть немного параноиками.

Чтобы снять опасения, разумнее всего переспросить отправителя, что именно он вам послал и с какой целью. Причем сделать это желательно по другому каналу связи (и держа при этом в уме, что, возможно, вам отвечает злоумышленник — вспомним предыдущий раздел). Если ответ вас удовлетворит, открывайте послание.

> *Кстати, когда вам нужно переслать кому-то файл или ссылку, не поленитесь написать несколько слов о том, что это и зачем, чтобы ваш адресат тоже не терзался сомнениями. Считайте это обязательным правилом цифрового этикета.*

Со вторым вариантом, когда мы потенциально сталкиваемся с сайтом-подделкой, немного проще: тут можно подстраховаться техническими средствами. Понятно, что человеческий глаз не обратит внимания на небольшое отличие в веб-адресе: допустим, вместо **moi-lyubimyi-bank.ru** будет **moi-lyubimyi-bank.su**. Но менеджер

паролей[1] обнаружит эту разницу и не подставит автоматически ваши данные в форму авторизации, даже если внешнее сходство подделки с оригиналом будет идеальным.

> *Полезный совет: если вместо интернет-банка пользоваться мобильным приложением, то на удочку фишеров вы не можете попасться в принципе, потому что приложение само помнит правильный адрес.*

Это касается и всех других сервисов, где надо осуществлять платежи или передавать персональные данные. Но используйте только официальные приложения!

Что касается третьего варианта с мнимо полезными сайтами, то здесь нам отчасти приходят на помощь разработчики браузеров — встроенные средства антифишинговой защиты есть в Chrome, Firefox, Opera, Microsoft Edge, Internet Explorer и других приложениях для веб-серфинга. Когда вы пытаетесь перейти по какому-либо адресу, браузер проверяет, нет ли его в списке фишинговых. Если проверка проходит успешно, открывает его. Внимательный читатель сразу заметит брешь: такая защита эффективна только против известных угроз. А как быть с новыми, если адрес еще не успели внести в базу? Ответ донельзя прост: соблюдать осторожность и не ходить куда попало.

Чтобы оценить масштаб проблемы, обратимся к цифрам. По данным Anti-Phishing Working Group, за 4-й квартал 2019 года было выявлено 162 тысячи уникальных фишинговых сайтов, причем каждый такой сайт может использовать

---

1 См. главу о паролях.

тысячи веб-адресов, ведущих в итоге на один источник угроз. Для сравнения — в мире регистрируется порядка 20 миллионов доменных имен в квартал[1]. То есть 1-2% всех веб-адресов принадлежат фишерам. И протокол **https** больше не является гарантией безопасности.

> *Среди советов по цифровой гигиене можно встретить и такой: лучше посещать только сайты, работающие по протоколу* ***https****, где буква «s» значит «secured» («безопасный»). То есть те, у которых адресная строка начинается с https:// (или видна иконка закрытого замка), например* ***https://google.com****. А если адрес начинается просто с* **http://** *без буквы «s» (или на иконке замок разомкнут), то это может быть фишинговый сайт.*
>
> *В наши дни этот совет устарел. По данным на конец 2019 года три из четырех фишинговых сайтов использовали защищенный протокол* ***https***[2]*. Несмотря на то, что это дополнительные расходы — сертификат безопасности стоит до нескольких сотен долларов, киберпреступники идут на это, чтобы вводить пользователей в заблуждение. Так что наличие буковки «s» больше не говорит о безопасности.*

Фишеры очень оперативно реагируют на актуальную повестку. Как только весь мир заговорил о коронавирусе, тут же, как грибы, стали вырастать мошеннические сайты. Ки-

---

1 *По данным за 3-й квартал 2019 г. 100+ Internet Statistics And Facts For 2020. //* ***websitehostingrating.com****, 17 июня 2020.*

2 *Phishing Activity Trends Report 1th Quarter 2020. // APWG.org, 11 мая 2020.*

берпреступники используют интерес к глобальной эпидемии для распространения своей злонамеренной активности. По данным Check Point Software Technologies[1], вероятность того, что домены, связанные с коронавирусом, представляют киберугрозу, на 50% выше, чем опасность любых других доменов, зарегистрированных в течение того же периода. Это, кстати, относится к любым другим доменам, связанным с «сезонными» темами, которые хакеры обычно используют для кибератак.

> *Эксперты по информационной безопасности советуют пользователям быть внимательными при работе с веб-площадками, в URL-адресе которых фигурируют такие ключевые слова как «coronavirus», «covid», «vaccine», «корона», «ковид», «вирус».*

Аналогичным образом злоумышленники эксплуатируют и другие сезонные темы. Так, в преддверии Дня святого Валентина отмечается 200% рост вредоносных веб-сайтов, посвященных этому празднику. Только за первую неделю февраля 2020 года мы увидели более 10 тысяч доменов со словом «Valentine», к которым обращались пользователи по всему миру. Угрозы на таких веб-сайтах могут различаться, и включают в себя онлайн-мошенничество, кражу учетных или платежных данных, а также заражение вредоносным ПО[2].

---

1 *Update: Coronavirus-themed domains 50% more likely to be malicious than other domains. // Check Point Software, 5 марта 2020.*

2 *Valentine's & Chocolate Don't Always Equal Love. // Check Point Software, 12 февраля 2020.* ***https://novayagazeta.ru/articles/2016/05/16/68604-gruppy-smerti-18***

«Синий кит», «красная сова» и все-все-все

В мае 2016 года в «Новой газете» вышла статья[1] Галины Мурсалиевой о существовании в сети ВКонтакте некой игры, финальной целью которой является совершение самоубийства, и что, по информации редакции, жертвами организаторов этого сообщества стали 130 подростков в разных городах России. Чтобы попасть в игру, нужно было вступить в одну из так называемых «групп смерти» и выполнять все более и более разрушительные для психического и физического здоровья задания «кураторов», в итоге приводящие игрока к гибели.

> *Символом одной из таких групп был синий кит — этот образ, растиражированный СМИ, мгновенно приобрел вирусную популярность. Почему кит? Потому что киты выбрасываются на берег, совершая самоубийство. Иногда массово. Почему синий? Потому что синий — цвет грусти. Какие-либо конкретные биологические особенности голубого полосатика (по-латыни Balaenóptera músculus) значения для игры не имеют.*
>
> *Статья о «группах смерти» набрала более 1,5 миллиона просмотров за два дня, информация разлетелась по родительским чатам, и встревоженные мамочки донесли ее до каждого ребенка — даже до того, кто ни о чем таком не то что не помышлял, а и слыхом не слыхивал. В результате паника взрослых оказалась настолько заразительной, что возымела обратный эффект. Дошло до того, что в Екатеринбурге девочка пыталась покончить с собой*

1 *Галина Мурсалиева, Группы смерти (18+) // Новая газета, 16 мая 2016.*

после школьной лекции о «Синемките»[1] — ее буквально сняли с крыши.

После публикации статьи Следственный Комитет начал проверку по изложенным фактам и возбудил уголовное дело. Спустя несколько месяцев в подмосковном Солнечногорске арестовали 21-летнего безработного Филиппа Будейкина, известного в интернете под ником «Филипп Лис», предполагаемого администратора «Группы смерти». Собственно, он и не прятался — все лето и осень Лис раздавал интервью и хвастался своими «успехами», пожиная плоды хайпа, к которому так стремился.

Всего Будейкину хотели инкриминировать 15 эпизодов доведения подростков до самоубийства — об этом сообщил в интервью[2] «Новой газете» руководитель первого следственного отдела первого управления по расследованию особо важных дел ГСУ СК по Санкт-Петербургу Антон Брейдо. Однако ни по одному из них связь с обвиняемым доказана не была.

Кроме того, в деле была одна попытка совершения суицида, в которой фигурировала единственная конкретная потерпевшая — ее удалось спасти. Но и тут все оказалось неоднозначно: девочка с 12 лет «слышала голоса», была подписана на несколько сотен групп суицидальной тематики и уже пыталась совершить самоубийство годом ранее.

---

1 *В Екатеринбурге девочка пыталась покончить с собой после школьной лекции о «Синем ките». // Росбалт, 22 марта 2017.*

2 *Галина Мурсалиева. Биомусор // Новая газета, 12 декабря 2016.*

Мнения экспертов-лингвистов и психиатров по поводу того, насколько повлияло на ее поступок участие в «Группе смерти», разошлись. Психолого-лингвистическая экспертиза показала разрушительное воздействие постов и сообщений Лиса на психику девушки. Психиатры же на вопрос о способах психологического манипулирования, которому подвергался ребенок, ответили, что не существует общепризнанных каким-либо сообществом теорий и тем более методик психологического давления и манипулирования.

Следовали допросили и других участников игры, не пытавшихся совершить суицид. Одни говорили, что всем была понятна ее шуточная природа, другие признавались, что воспринимали пропаганду суицида серьезно, она вызывала у них мысли о самоубийстве и подавленное состояние.

Тем не менее, в июне 2017 года суд приговорил Будейкина к 3 годам и 4 месяцам колонии-поселения. Он освободился в марте 2019-го. Сегодня Филипп работает администратором в тренажерном зале и уверяет, что в интернете почти не сидит: времени нет[1].

Тогда же, в июне 2017-го, был принят закон[2] об ужесточении уголовной ответственности за побуждение детей к суициду,

---

1 *Сергей Хазов-Кассиа. «Че, малыши, когда суицидимся?» За что Филипп Лис сел в тюрьму // Сайт Радио Свобода, 15 июня 2019.*

2 *Федеральный закон от 7 июня 2017 г. № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению».*

чтобы исправить несовершенство статьи 110 УК РФ «Доведение до самоубийства», по которой организаторам «синих китов» и других подобных игр было трудно предъявить обвинения.

Понятно, что нам хочется оградить детей от контента, который им не по возрасту, и закон здесь на нашей стороне: согласно Федеральному закону 436[1], запрещается распространять среди детей информацию, побуждающую к причинению вреда своему здоровью, самоубийству; способную развить порочные наклонности (алкоголизм, наркоманию, занятие проституцией, бродяжничеством или попрошайничеством). Распространяемые среди детей сведения не должны оправдывать насилие и жестокость, противоправное поведение; отрицать семейные ценности; содержать нецензурную брань и порнографию.

Роскомнадзор начал действовать, и за один только 2017 год заблокировал 14 тысяч страниц и сообществ, имевших хотя бы намек на отношение к зловещей игре. Мониторинг ведется постоянно, и теперь новые «группы смерти» блокируются сразу, не успев набрать популярность. Казалось бы, можно праздновать победу, отныне дети защищены.

Или нет?

Одни лишь запретительные меры никогда не помогают, а молодежь всегда придумает обходные пути.

---

1 *Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».*

«Киты, единороги, бабочки, крокодилы, тараканы и орангутанги? — Завтра будут другие символы, вы их не успеете и заметить. Раннее утро, 4.20? — будет другое время икс. Вы не успеете за нами, если зациклитесь на конкретных деталях», — так написала на своей странице в Фейсбуке одна школьница[1], обращаясь к взрослым, и была совершенно права.

«Это не решение проблемы, а лишь возможность сделать ее невидимой для старшего поколения и надзорных институтов. Решение проблемы — в офлайне, в семейном воспитании, в умении работать с новым типом сознания, навыке понимания», — объясняет руководитель социологического центра «Платформа» Алексей Фирсов[2].

Действительно, тотальная зачистка информационного поля не помогла. Не прошло и года, как «синий кит» вернулся — на этот раз в образе «красной совы». Теперь ВКонтакте блокируют страницы, если написать «Сова никогда не спит» — это новый код-заявка на участие в игре. Снова таинственные кураторы, опасные задания и новая фишка — не спать несколько суток, постоянно быть онлайн и смотреть шокирующие видео.

Ночные бдения были частью ритуала и у «синих китов». Фраза «разбуди меня в 4:20», замеченная у ребенка на его странице, явно указывала на то, что он в игре. «Эксперты» уверяли, что именно в это время мозг ребенка наиболее беззащитен, и таким образом его можно подчинить воле кураторов. Это, разумеется, чушь.

---

1 *Страница Facebook Елизаветы Скульской* ***https://www.facebook.com/ElizavetaSkulskaia/posts/851766544967641***

2 *«Синий кит» вернулся в новом обличье. // Известия, 25 января 2018.*

Но то, что ребенок перестает высыпаться и от этого становится раздражительным, невнимательным и у него падает успеваемость — это факт.

Безотносительно всяких «китов» и» сов», все гаджеты на время сна должны находиться подальше от кровати ребенка.

Поэтому безотносительно всяких «китов» и «сов», все гаджеты на время сна должны находиться подальше от кровати ребенка. А чтобы просыпаться вовремя, заведите обычный будильник — смартфон для этого совершенно не обязателен. И помните, что без вашего личного примера это не работает — с привычкой держать свой телефон под подушкой придется расстаться и вам.

«Мода» на «красных сов» сегодня уже прошла. Что будет дальше? Малиновый медведь? Фиолетовый ястреб? Фантазия детей не знает границ, обязательно появится что-то еще. Как же быть? Опять массово блокировать новые сообщества и сайты, всегда отставая от их выдумок?

В этой ситуации Следственный комитет демонстрирует весьма взвешенную позицию по вопросу о влиянии Сети на подростков и об истинных причинах детских суицидов.

> *«Не надо демонизировать интернет», — считает старший помощник председателя СКР Игорь Комиссаров, — по нашей статистике, больше всего несовершеннолетних — 800 человек — в России погибло в результате самоубийств в 2014 году. В 2017 году — 692, за девять месяцев этого года (2018) погибло 583 несовершеннолетних. Значительного роста числа самоубийств, совершенных несовершеннолетними, за последние*

годы нет и не было, несмотря на громкие заявления отдельных представителей власти, общественников и журналистов.

Мы тщательно разбирались в рамках обязательно возбуждаемого уголовного дела по каждому случаю суицида или попытки суицида у детей. И пришли к выводу, основанному, в том числе, на результатах проведенных экспертиз, что каждый раз это было обусловлено комплексом причин. И ни в одном случае нет определяющего влияния только интернета на последующие действия несовершеннолетних.

Никогда те или иные группы, содержащие деструктивный контент, не становились главной причиной детских суицидов. И не только суицидов, но и основной причиной противоправного или опасного поведения несовершеннолетних.

Нельзя убить или заставить совершить преступление по интернету. В большинстве случаев ребенок принимает решение о лишении себя жизни под воздействием сразу нескольких факторов в условиях длительной психотравмирующей ситуации и отсутствия понимания и поддержки со стороны окружающих. Проблемы в семье, часто внешне благополучной, в школе, ориентированной на показатели ЕГЭ, затруднение в общении со сверстниками, увеличение потребления школьниками наркотических и психотропных препаратов, незанятость несовершеннолетних позитивной деятельностью и так далее. А сам интернет никогда не играл в этом главную роль. Это только средство коммуникации. Не надо демонизировать его влияние»[1].

1 *Следственный комитет России: «Не надо демонизировать интернет» // Известия, 29 ноября 2018.*

Среди части взрослых весьма популярна конспирологическая версия, что все эти «группы смерти» созданы и управляются врагами нашей страны с какими-то далеко идущими политическим целями — чтобы подчинить себе молодых людей и использовать их для дестабилизации обстановки, когда это потребуется, и что «кураторы» обладают прямо-таки сверхъестественными способностями в области манипуляции сознанием подростков: вот так запросто прикажут человеку прыгнуть с крыши — и он прыгнет.

При сколь-нибудь критическом размышлении эта версия рассыпается — достаточно взглянуть на Филиппа Лиса и других горе-кураторов, чтобы понять, что социальные инженеры из них так себе, и что никакая вражеская спецслужба не даст им ни цента за их «подрывную работу».

Нормального подростка нельзя склонить к суициду, просто показывая ему какие-то картинки в интернете и отдавая приказы.

Нормального подростка нельзя склонить к суициду, просто показывая ему какие-то картинки в интернете и отдавая приказы. К сожалению, иногда обстоятельства складываются так, что юноша или девушка уже имеют психологические проблемы, и мысль об уходе из жизни засела у них в голове. Тогда любое слово может подтолкнуть к фатальному решению — будь то диалог с «куратором» или статья в газете. Это так называемый «эффект Вертера», известный еще с XVIII века, когда по Европе прокатилась волна самоубийств, вызванная публикацией романа Гёте «Страдания молодого Вертера».

Но раз эти группы существуют и создаются все новые, значит, это кому-то выгодно? Совершенно правильный вопрос!

Но он, как ни удивительно, в большинстве публикаций про «группы смерти», начиная со статьи Галины Мурсалиевой, даже не поднимается. Или того хуже, обсуждение уходит в мистическую плоскость: самодеятельные расследователи на полном серьезе демонстрируют публике договор купли-продажи души, который владелец группы якобы заключает с куратором.

Когда группа становится достаточно многочисленной, ее владелец начинает зарабатывать на рекламе.

На самом деле все гораздо проще: когда группа становится достаточно многочисленной, ее владелец, как это обычно происходит в соцсетях, начинает зарабатывать на рекламе. Именно на это рассчитывал Будейкин и его коллеги по цеху. Кроме того, практикуются в таких группах и банальные «разводки» на деньги: по словам одного участника, он трижды натыкался на кураторов, которые вторым заданием просили прислать им 200 рублей на телефон или Киви-кошелек.

Не гнушаются такие «предприниматели» зарабатывать и на чужой крови — почти в буквальном смысле этого слова. Например, сайт памяти Рины Паленковой[1] представляет собой, по сути, интернет-магазин, где можно купить вещи «как у Рины» — тетради, барабанные палочки, одежду и прочее. Ничего личного — только бизнес.

---

1 *Рина Паленкова (настоящее имя Рената Камболина, 18 декабря 1998 – 23 ноября 2015) — студентка из Уссурийска, прославившаяся после своего самоубийства. Также с ней связан мем «Ня.Пока» из ее последней записи, ставшей своего рода предсмертной запиской. Этот пост получил более 400 тысяч лайков, а в «группах смерти» ее образ стали использовать как пример для подражания.*

Воронка вовлечения

«Синих китов» и «красных сов» можно, пожалуй, считать городской легендой: их опасность была сильно преувеличена в результате массовой паники родителей, возникшей после ряда нашумевших публикаций. Следствие не выявило никаких тайных организаторов, стоящих за созданием подобных игр, и единого центра координации.

> *В Сети встречаются куда более реальные угрозы, реализуемые методами социальной инженерии. Речь идет о вовлечении подростков в различные деструктивные сообщества, связанные с наркотиками, радикальными движениями, экстремизмом и терроризмом.*

Вся эта «темная сторона» обладает особым ореолом притягательности для неокрепших умов, хотя в подавляющем большинстве случаев дело, к счастью, ограничивается банальным любопытством, позерством и пустой болтовней. В общем, как у взрослых: вряд ли кто-то из них из-за прослушивания «Владимирского централа» по радио «Шансон» реально решится избрать преступный путь.

Тем не менее, нельзя сбрасывать со счетов тот факт, что криминальный мир постоянно нуждается в притоке новых «бойцов», которые становятся пушечным мясом в его войне с правоохранительными органами. Например, есть постоянный спрос на наркокурьеров-закладчиков, и молодежь идеально подходит на эту роль.

Криминальный мир постоянно нуждается в притоке новых «бойцов».

Понятно, что рекрутировать на такую «работу» в открытую сложно — страницы с наркоконтентом будут быстро заблокированы, а их владельцами заинтересуются оперативники. Поэтому преступники поступают иначе: сначала формируется максимально широкое сообщество вокруг какой-то темы, не запрещенной, но близкой по смыслу к истинной цели — например, психоделические мультики. Затем некоторым участникам высылают приглашение в закрытую группу, где намерения организаторов выражаются более явно; на следующем этапе «когорту избранных» могут пригласить в секретный чат, в котором ведутся совсем откровенные разговоры — это уже не считается публикацией контента и под действие закона не попадает. И наконец, с наиболее «перспективными» кандидатами начинают персонально общаться в мессенджере — чтобы завершить вербовку и дать новичку конкретное задание.

> *Судьба закладчика, как правило, незавидна: обычно они попадаются на третьей-четвертой попытке, или их сдают сами дилеры, которым дешевле набрать новых курьеров, чем платить тем, кто уже отработал какое-то время.*

За такую «работу» по статье 228 УК РФ[1] молодым людям, если им уже исполнилось 18, грозит лишение свободы на срок от 10 до 15 лет в колонии строгого режима, а несовершеннолетним — от 5 до 10.

---

1 *УК РФ Статья 228. Незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов, а также незаконные приобретение, хранение, перевозка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества.*

При этом дети, которые устраиваются работать «закладчиками» (или, как их чаще называют, «кладменами»), порой даже не осознают, что это противозаконно. Они считают всякие «смеси» и «соли» вполне легальным товаром, а их родители ничего не замечают. Ну, зарабатывает ребенок через интернет, но ведь и учится при этом хорошо, и ведет себя адекватно, и выглядит нормально, то есть сам — явно не наркоман[1].

Механика вовлечения в другие преступные сообщества и группировки примерно такая же. Но вербовка далеко не всегда является целью администраторов сообществ, публикующих у себя деструктивный контент. В подавляющем большинстве случаев они хотят просто, как серферы на волне, прокатиться на модной теме, хайпануть и на этом заработать — так же, как и в случае с «группами смерти».

> *Например, есть еще одна «страшилка» для взрослых — А.У.Е. Аббревиатура расшифровывается как «арестантский уклад един» (или «арестантское уркаганское единство») и представляет собой одновременно название и девиз предположительно существующего российского неформального объединения банд, состоящих из несовершеннолетних. Тренд опять задала «Новая газета»[2], резко подняв градус обеспокоенности общества процессами криминализации подростков.*

---

1 *14-летние наркоторговцы: как дети попадают за решетку. // Сайт* ***Ok-inform.ru****, 15 октября 2017.*

2 *Алексей Тарасов. Страна из трех букв // Новая газета, 16 июня 2017.*

При том, что детские банды действительно существуют, и с этим надо что-то делать, есть еще и гипертрофированное отражение реальности в интернете, которое возникает тогда, когда что-либо становится модным. Из того, что количество групп ВКонтакте, посвященных АУЕ или похожей тематике, зашкаливает, вовсе не следует, что все дети вырастут уголовниками. Подавляющее большинство этих групп носит чисто коммерческий характер — их участникам предлагают купить футболки, банданы и другие предметы с соответствующей символикой. Но число их участников исчисляется сотнями тысяч, и это не может не настораживать.

Давайте сопоставим факты. По словам все той же «Новой газеты», эта молодежная субкультура наиболее распространена в Забайкальском крае и соседних регионах, которые едва ли можно назвать экономически благополучными. Напрашивается вывод: отнюдь не интернет является главным виновником распространения тюремных обычаев среди подростков, а сама среда, в которой они живут. Что же касается их более обеспеченных сверстников, то для них это просто очередная игра. Хотя, разумеется, сказанное ничуть не умаляет опасности самого явления — вне зависимости от того, насколько влияет на его распространение интернет.

По данным компании «Крибрум», на март 2019 года в деструктивные течения в Рунете были вовлечены порядка 5 миллионов аккаунтов российских подростков (35% от их общего числа в России), и количество таких аккаунтов продолжает расти.

Период с января 2018 г. по март 2019 г. характеризуется стабильно высоким, растущим деструктивным фоном. Особую опасность представляют следующие темы: наркомания, ультра-движение, анархия.

В подростковой среде в социальных медиа фиксируется стремление подростков к группам, продвигающим разрушающее поведение через темы социопатии, массовых и серийных убийств, обесценивания собственной жизни и стремления к смерти, сатанизма и псевдомистических культов, наркомании, ритуальных убийств и самоубийств, нацизма и национализма, экстремизма и радикализма[1].

Как относиться к этим пугающим цифрам и фактам? Прежде всего, уточнить, что имеют в виду под вовлеченностью аналитики «Крибрум»: участие в группе, репост или лайк, поставленный материалу деструктивной тематики. Как вы понимаете, между лайком и реальным действием — дистанция огромного размера. Разумеется, мониторинг интересов подростков может дать много полезной информации для размышления взрослым и помочь сделать так, чтобы эта дистанция не была преодолена. Но и излишне драматизировать ситуацию не стоит. Доверие — один из важнейших инструментов воспитания, а большинство детей вполне четко разграничивают игру и настоящую жизнь.

---

1 *Форум «Цифровая гигиена. Молодежь в сети», 28 марта 2019.* ***http://digital-gigiena.ru/***

Контрольные вопросы

1. Что такое социальная инженерия?
2. Какие эмоции и чувства преступники используют наиболее часто?
3. Что значит «нулевое доверие»?
4. Как работают «нигерийские письма»?
5. Как телефонные мошенники обманывают клиентов банков?
6. Почему банк не компенсирует потери в результате применения социальной инженерии?
7. Как проверить, просит помощи друг или мошенник от его имени?
8. Что такое фишинг?
9. Какие варианты фишинга вы знаете?
10. С помощью чего можно защититься от фишинга?
11. Как вы отличаете подозрительные ссылки от неподозрительных?
12. Почему надежнее пользоваться мобильными приложениями?

13. Что такое «группы смерти»? Что вы об этом думаете?

14. Что такое воронка вовлечения?

Глава 6

У нас все ходы записаны

Эта глава посвящена цифровым следам,
которые мы вольно или невольно оставляем
своим присутствием в интернете.
Мы узнаем, где и как это происходит, от каких следов
можно избавиться, а какие остаются навсегда.
И еще: нужно ли об этом беспокоиться или нет.

Во все века люди стремились оставить о себе память, след в истории. Одни творили и строили, другие, как Герострат, — наоборот, разрушали. Но в любом случае самого факта действия было мало — нужно, чтобы он был задокументирован и сохранен в анналах истории, иначе даже современники быстро забудут о ваших подвигах. Да и собственная память может подвести, поэтому лучше все записывать сразу, а не фантазировать потом, когда придет охота писать мемуары.

> *Писатель, поэт, журналист и общественный деятель Константин Симонов вел подробный архив, который он сам называл «Все сделанное» — сейчас это звучит как название папки в компьютере.*
>
> *«Архив Константина Михайловича огромен и по-своему сложен…. Мало ему было собственных трудов. При его разнообразной и активной деятельности на его голову буквально сыпались в невероятном количестве письма, материалы, деловые бумаги, рукописи всех жанров… Представьте себе, он ведь с шестнадцати лет хранил все присылаемые ему письма и снимал для себя копии со своих», — рассказывала Нина Павловна Гордон, бывшая в течение многих лет секретарем писателя*[1].

Чтобы вести такой архив, надо быть очень организованным человеком, и далеко не каждый на это способен. В наши дни задача сильно упростилась: интернет помнит все, хотим мы того или нет.

---

1 *Из книги Бориса Панкина «Четыре Я Константина Симонова»*

Интернет помнит все, хотим мы того или нет.

Каждое отправленное письмо или сообщение, каждый клик по ссылке, открытие сайта, каждый пост, лайк или комментарий в соцсети, фотография или видео, телефонный звонок или SMS, покупка в магазине (онлайн или офлайн, если по банковской карте), любая поездка (самолетом и поездом, само собой, в том числе и городским транспортом — во время самоизоляции в Москве проехать в метро по карте «Тройка» можно было, только если она привязана к цифровому пропуску), все ваши маршруты пешком и на велосипеде или самокате — это цифровые следы, остающиеся в памяти разных компьютерных систем. Причем эти данные сохраняются практически навечно и, откровенно говоря, у вас нет возможности полностью удалить свой цифровой след, несмотря даже на последние инициативы законодателей (об этом чуть ниже).

> ***Цифровой след*** *(или цифровой отпечаток; англ. digital footprint) — совокупность информации о посещениях и действиях пользователя во время пребывания в цифровом пространстве. Может включать в себя информацию, полученную из интернета, мобильного интернета, веб-пространства и телевидения.*

Принято разделять цифровые следы на активные и пассивные. Активные — это то, что люди делают сами, включая публикации в соцсетях, комментарии, фотографии и так далее. Своей активностью пользователь может управлять — например, выбирать, на какие темы писать, какие делать репосты, как себя вести в комментариях. То есть осознано формировать свой цифровой образ. А пассивные — это то, что компьютерные системы записывают автоматически: IP-адрес, с которого вы выходите в ин-

тернет, история посещений сайтов, данные геолокации и прочее. Большинство людей и не подозревают о том, как много следов они оставляют в цифровом пространстве, даже если помалкивают и не ввязываются ни в какие холивары. Некоторые называют цифровые следы «цифровой тенью» — будем считать, что это одно и то же.

Большинство людей и не подозревают о том, как много следов они оставляют в цифровом пространстве.

Контролировать свои пассивные следы практически невозможно. Чтобы от них полностью избавиться, нужно совсем перестать пользоваться телефоном и компьютером, и то не факт, что это поможет. Во-первых, все важные вехи вашей жизни, от рождения до смерти, фиксируются в государственных информационных системах — учеба в школе и в институте, служба в армии, работа, свадьба, развод, участие в выборах, получение водительских прав, покупка квартиры, выезд за границу, обращение в поликлинику — буквально каждый ваш чих оставляет цифровой след. (Это в полной мере ощутили москвичи, которых обязали пользоваться приложением «Социальный мониторинг» во время пандемии коронавируса).

Если вы живете в большом городе, то вы каждый день попадаете в поле зрения камер видеонаблюдения. Например, в Москве в 2019 году их насчитывалось больше 170 тысяч, и мэрия планировала установить еще, обещая даже запустить систему распознавания лиц. Так что в скором времени все наши перемещения по городу будут известны, как минимум, властям, а возможно и хакерам, потому что абсолютно надежных систем не бывает.

Скоро все наши перемещения по городу будут известны, как минимум, властям, а возможно и хакерам.

Кто этому точно порадуется, так это будущие историки, которым больше не придется по крупицам собирать информацию, рассеянную в письмах и книгах, а можно будет написать один запрос к базе данных и получить исчерпывающую фактографическую информацию о перемещениях и активности своего героя. Дальше им останется только придумать, каким образом лучше ее визуализировать и каким комментарием снабдить.

> *Поэтесса Анна Ахматова не вела блог и не отмечалась в Фейсбуке, но тем не менее мы сейчас имеем возможность просмотреть ее цифровые следы. Хотите совершить виртуальную прогулку по ахматовским местам в Москве? Пожалуйста! Необходимые геоданные в машиночитаемом виде уже лежат на Портале открытых данных РФ.*
>
> *Загружаете эти данные в Google My Maps — сервис внутри Google Maps, позволяющий создавать свои собственные карты, и вуаля — ваша карта готова! Можно отправляться по цифровым следам любимой многими поэтессы — просто кликайте по меткам на карте. Вот здесь, во флигеле сталинской высотки на Котельнической набережной, Ахматова гостила у Фаины Раневской в 1950-е; в районе Остоженки жила в 1917-1918 со своим вторым мужем, ассириологом и поэтом Владимиром Шилейко; на Никитский бульвар ходила в гости к Михаилу Булгакову и его жене, которая была подругой Ахматовой, а на Поварской общалась с писателями Борисом Пильняком и Корнеем Чуковским*[1].

1 *Электронный след Анны Ахматовой. // Системный Блок{ъ}, 23 июня 2019.*

Если даже прошлое может быть оцифровано, что уж говорить о настоящем! Очевидно, что дальнейшая история человечества будет записана в цифровом формате и со все большими подробностями — вплоть до создания полной цифровой копии всей жизни каждого человека.

Риск и польза геоданных

«— Киса, — продолжал Остап, — давайте и мы увековечимся. ... У меня, кстати, и мел есть! Ей-богу, полезу сейчас и напишу: „Киса и Ося здесь были"».

Говоря современным языком, Остап Бендер таким образом решил «зачекиниться».

Когда интернета еще не было, люди оставляли информацию о посещении каких-то мест более прямолинейным способом — в виде надписи на камне, на заборе или стене. Сейчас эту функцию взяли на себя наши цифровые компаньоны, и делают это автоматически, днем и ночью, вне зависимости от того, просим мы их об этом или нет. Ведь вы же не выходите из дома без мобильного телефона, да? Он фиксирует ваше местонахождение даже без подключения к интернету. Ваш смартфон — фактически GPS-устройство. Если функция геолокации включена, его встроенный приемник получает сигналы со спутников и с высокой точностью определяет ваши координаты.

Распространено заблуждение, что спутники GPS каким-то образом следят за пользователями и знают, где те находятся. На самом деле спутники только передают сигналы. Ни спутники, ни операторы GPS-оборудования не знают, где вы находитесь, и сколько

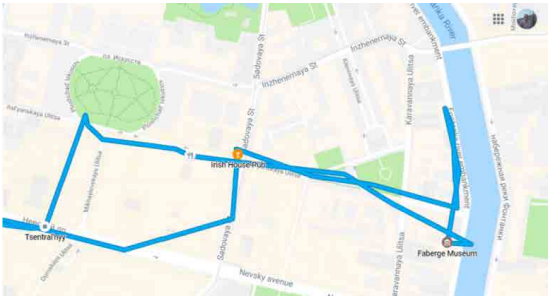
людей использует систему. Спутники — это просто маячки, по которым GPS-навигатор определяет свое местоположение.

Ни спутники, ни операторы GPS-оборудования не знают, где вы находитесь, и сколько людей использует систему.

А кто же тогда следит? Это делают приложения, установленные на телефоне. Зайдите в свой Google-аккаунт и откройте страницу **https://www.google.com/maps/timeline** — если вы никогда раньше сюда не заходили, то вас ожидает сюрприз.

> *Google помнит все ваши перемещения, все адреса и явки будут как на ладони. Можно даже посмотреть, где вы были в конкретный день.*

Теперь не скажешь «ой, где был я вчера, не найду, хоть убей, только помню, что стены с обоями». Гугл все помнит, и даже покажет фото, которые вы сделали в каждом месте. Допустим, вы гуляли по Невскому проспекту, заходили в музеи и кафе, прошлись по набережной — спроси вас через год про точный маршрут, так вы и не скажете. А на карте все видно!



Хотя с позиционированием он иногда ошибается — может быть, просто «глючит», а может быть — не по своей вине. Например, довольно часто бывает, что люди гуляют около Кремля, а GPS показывает, что они во Внуково — спецслужбы устраивают такие фокусы, чтобы запутать шпионов. То есть на точность записей Google на 100% полагаться нельзя. Разработчики это тоже знают, поэтому в приложении есть функция подтвердить место, где вы были, или удалить его из маршрута. Вы можете отключить функцию слежения и даже стереть всю историю или подчистить отдельные места, пребывание в которых вам не хочется афишировать. Не ходи к гадалке, параноики скажут, что это ничего не значит, и что на серверах Google все равно вся информация сохранится — и возможно, они будут правы. Но если вы не делали ничего противозаконного, беды в этом большой нет.

Можно отключить функцию слежения, стереть всю историю или подчистить места, пребывание в которых вам не хочется афишировать.

Ну, ладно Гугл. Ему мы все-таки доверяем. Однако на вашем телефоне могут быть шпионские приложения, которые отправляют информацию о ваших перемещениях неизвестно кому и неизвестно с какой целью. Поэтому не стоит скачивать приложения из непроверенных источников и давать им доступ к геолокации. Если это приложение для ловли покемонов, то о'кей, доступ к геоданным ему действительно нужен, иначе не поиграешь. А если это очередная модификация Тетрис, то зачем ему знать, где именно вы решили убить немного времени, укладывая падающие фигуры?

Не стоит скачивать приложения из непроверенных источников и давать им доступ к геолокации.

Вы можете подумать, что, отключив GPS на телефоне, избавитесь от отслеживания ваших перемещений. Увы! При включенном wi-fi все будет прекрасно работать, может быть, даже еще точнее. Ведь вы, скорее всего, включаете wi-fi на телефоне, когда находитесь дома или на работе, и вряд ли сразу выключаете его, выйдя за дверь. (Особо продвинутые могут настроить так, чтобы это делалось автоматически, но это требует специальных усилий). А в городе полным-полно точек доступа, и ваш телефон будет все время пытаться подключиться к ближайшей из них, раскрывая, таким образом, ваше местоположение.

Каким же образом эта коробочка, раздающая беспроводной интернет, узнает, где она сама находится? Ведь в wi-fi-роутере нет GPS-приемника: принесли из магазина, включили и все. А происходит вот что: когда в зоне сигнала роутера появляется телефон с включенным GPS, информация об обнаруженных wi-fi сетях передается поставщику его операционной системы (например, Apple или Google для телефонов на Android). Таким образом, геопозиция нового роутера фиксируется и заносится в базу. Потом, когда кто-то заходит в кафе или магазин, где стоит этот роутер, и подключается к wi-fi со своего телефона (пусть и с выключенным GPS), его координаты мгновенно определяются. И вовсе не обязательно логиниться в эту wi-fi-сеть — достаточно того, что ваш телефон ее увидел. Аналогичным образом работает геопозиционирование по вышкам сотовой связи — их точное местоположение хорошо известно, а точка, где вы сейчас находитесь со своим телефоном, вычисляется методом триангуляции (эти данные доступны только оператору).

Точность позиционирования по wi-fi и станциям мобильных операторов может достигать 5-15 метров, что даже выше, чем по сигналу со спутника GPS — если вы находитесь в районе с очень плотной инфраструктурой связи. Например, в Москве одно лишь количество публичных точек доступа превышает 60 тысяч, не считая wi-fi-роутеров, установленных в квартирах. А в самой большой базе данных точек wi-fi, принадлежащей компании Combain Positioning Solutions, хранятся координаты почти 2,7 миллиардов устройств. Естественно, все они находятся в населенных пунктах или вдоль дорог — в тундре или тайге обнаружение с помощью такого метода вам не грозит.

> *В Google есть способ, позволяющий администраторам точек доступа (включая вас, если вы управляете домашним или офисным wi-fi), отказаться от внесения координат вашего роутера в глобальную базу данных. Добавьте «_nomap» в конец имени сети (например, mynetwork_nomap), и Google больше не будет отслеживать его.*

Однако Google не единственная компания, собирающая такие данные, и не все компании предоставляют столь простые способы отказаться от отслеживания. Поэтому, скорее всего, ваш wi-fi-роутер все-таки окажется в какой-то глобальной базе данных. Стоит ли по этому поводу волноваться? Пожалуй, нет. В базу попадает только уникальный номер вашего устройства (MAC-адрес), который никак не связан с вашими персональными данными. Пускай ваш роутер тоже будет одним из маячков в цифровом океане. Вдруг он однажды поможет заблудившемуся путнику найти дорогу.

Что делать, если вам все-таки хочется «пропасть с радаров»? Манипуляции с настройками телефона, скорее всего, не помогут. Рас-

следование Associated Press, проведенное в 2018 году, показало, что многие службы Google на устройствах Android и iPhone хранят данные о вашем местоположении, даже если вы явно указали в настройках конфиденциальности, что запрещаете это делать[1].

Что делать, если хочется «пропасть с радаров»? Лучше всего просто выключить телефон.

Поэтому лучше всего будет выключить телефон. Но даже это не гарантирует, что он не отслеживает свои (то есть, ваши) координаты, уверены параноики, и советуют для большей надежности вынуть из него батарею. Возможно, они правы, но не со всеми моделями это получится. Сначала лучше задать себе вопрос: с какой целью вы хотите стать невидимым? Ведь геотрекинг работает, скорее, на благо вашей безопасности, нежели против нее. Полиция, например, активно использует цифровые следы при раскрытии преступлений.

> *Летом 2019 года в Солт-Лейк-Сити пропала девушка, студентка местного университета. Ее тело нашли три недели спустя в 90 милях от города. В доцифровую эпоху это преступление имело бы высокие шансы остаться нераскрытым, но в наши дни все оставляют цифровые следы — и жертва, и преступник, что помогает работе полиции. Следователи проанализировали геоданные с телефона девушки (по записям оператора мобильной связи) и выяснили, что человек, подозреваемый в ее похищении и убийстве, находился неподалеку от нее в тот момент, когда ее телефон прекратил работу. Сначала подозреваемый отрицал, что знаком с потерпевшей,*

1 *AP Exclusive: Google tracks your movements, like it or not. // AP News, 14 августа 2018.*

однако на его телефоне обнаружили несколько ее фотографий, и он, кроме того, оказался подписан на ее Инстаграм. Конечно, одних только цифровых следов было бы недостаточно, чтобы предъявить обвинение, но они очень помогли в поиске преступника. Позже полицейские обнаружили и более серьезные улики[1].

Преступник оказался бывшим специалистом по ИТ, но это ему не помогло. «Хороший айтишник может пойти и сделать отличную работу, чтобы подчистить свои следы, но я гарантирую вам, что он не сможет сделать эту работу исчерпывающе. В продуктах и системах, которыми мы пользуемся, встроены некоторые вещи, практически исключающие полное блокирование работы полиции», — прокомментировал ситуацию частный детектив с 25-летним стажем, занимающийся расследованием подобных случаев[2].

Тем не менее, постоянный мониторинг ваших перемещений вполне обоснованно может вызвать раздражение и ощущение вмешательства в частную жизнь. С одной стороны, это так. Но с другой — вы же не думаете, что все это результат всемирного заговора, и что технологические мегакорпорации вместе со спецслужбами озабочены тем, чтобы вызнать про вас все подробности? Все гораздо проще: компании хотят вам что-то продать, и для этого они хотят знать ваши маршруты и любимые места — чтобы показывать вам более точную рекламу, а взамен они предоставляют вам множество по-

1 *Body of Utah student Mackenzie Lueck recovered, identified. // FOX8 Digital Desk, 5 июля 2019.*

2 *How an alleged killer's digital footprint led to his capture. // ABC4.com, 29 июня 2019.*

лезных сервисов, таких как карты, такси, поиск друзей поблизости, ресторанов, магазинов, игры вроде покемонов, фитнес-трекеры для учета своих ЗОЖ-достижений и многое другое. Большинство из этих приложений бесплатны.

По-моему, это честная сделка. И потом: вы же хотите знать, где находится ваш ребенок и куда он вообще ходит, да? Если технологии в этом помогают, то это хорошо — для его безопасности и вашего спокойствия. Любые инсинуации про постоянную слежку и Большого Брата в данном случае будут неуместны — это ваше право и обязанность как родителя. И закон, и здравый смысл в этом вопросе на вашей стороне.

> *В июле 2019 года Госдума окончательно одобрила законопроект об упрощении поиска пропавших детей с помощью геолокации. В случае пропажи ребенка его родители (или один из них, или законные представители) смогут обратиться в органы полиции с письменным заявлением, и те в течение 24 часов должны начать поиски, в том числе с возможностью получить доступ к данным геолокации мобильных устройств ребенка — например, его телефона или планшета. При этом о начале проведения таких оперативно-розыскных мероприятий правоохранительные органы должны будут также уведомить суд, и в течение 48 часов с момента их начала получить судебное решение о проведении такого оперативно-розыскного мероприятия, либо прекратить его проведение, — говорится на сайте Думы*[1].

1 *Принят закон об упрощении поиска пропавших детей. // Государственная Дума, официальный сайт, 24 июля 2019.*

Председатель Государственной Думы Вячеслав Володин подчеркнул, что возможность правоохранительных органов оперативно получить доступ к данным геолокации ребенка позволит значительно ускорить его розыск. «Это время может оказаться бесценным, если, например, ребенок заблудился, потерялся или с ним случилась беда», — отметил он.

По словам председателя профильного Комитета по безопасности и противодействию коррупции Василия Пискарева, «в случае пропажи ребенка быстрое определение его местонахождения также поможет пресечь совершение в отношении него противоправных действий и не допустить наступления общественно опасных последствий, сохранить его жизнь и здоровье».

Безусловно, это здравое решение, и его можно только приветствовать — технологии могут и должны использоваться во благо. Однако на этом примере снова видно, насколько те, кто пишет законы, далеки от понимания того, как работает интернет.

В переводе с бюрократического языка на человеческий это означает: «данные о геолокации мобильных устройств ребенка» — это данные оператора связи, который вычисляет местоположение устройства относительно вышек сотовой связи. Их действительно надо запрашивать у компании, онлайн они недоступны. Преимущество этого метода только в том, что таким образом можно получить координаты даже самого примитивного кнопочного мобильника, с которого нет доступа в интернет. Но какой подросток согласится ходить с таким гаджетом? Ведь засмеют. Да и как на нем играть? А даже самый дешевый китайский смартфон умеет выходить в Сеть и позволяет устанавливать приложения — значит, на него можно установить и приложение для обеспечения безопасности.

Даже самый дешевый смартфон выходит в Сеть и работает с приложениями — значит, на него можно установить и приложение для обеспечения безопасности.

Например, Kaspersky Safe Kids позволяет видеть на карте местоположение ребенка (точнее говоря, его телефона). При этом можно заранее задать безопасный периметр и получать уведомления о выходе ребенка за его пределы. А чтобы не впадать в панику почем зря, приложение еще сообщит вам о низком уровне заряда батареи на его устройстве и заодно не даст соврать «ой, у меня телефон разрядился», когда ребенок не хочет отвечать на ваши звонки.

На случай, когда ребенок намеренно не выходит на связь, а в это время у бабушки давление уже скакнуло под 200, тоже есть решение. Хорошо, что некоторые отцы умеют программировать. Одному из них, англичанину Нику Герберту надоело, что сын может игнорировать его сообщения и звонки, поэтому он придумал приложение Respond ASAP, которое блокирует телефон ребенка до тех пор, пока он не перезвонит родителям. Если телефон ребенка вдруг стоит на беззвучном режиме, приложение может запустить специальную сирену, чтобы звонок не остался незамеченным. Пока есть только версия для Android, над версией для iOS Ник еще работает.

Вот что он сам написал об этой истории на своем сайте **http://respondasap.co.uk/**:

> *«...У меня есть сын Бен. Когда он пошел в среднюю школу, я купил ему смартфон, чтобы иметь возможность связаться с ним, а он мог бы связаться со мной (разумеется, не во время занятий).*

Однако то, что я считал решением, превратилось в другую проблему. Поскольку телефон «умный», Бен может на нем играть в игры и смотреть видео. Поэтому он всегда держит телефон в беззвучном режиме, чтобы я об этом не знал. Когда я пытаюсь связаться с ним, он редко отвечает — либо потому, что не слышит сигнала, либо потому, что (и мне наконец-то пришлось признаться в этом самому себе) смущается говорить с отцом в присутствии друзей.

Иногда мне нужно передать ему сообщение, но он не может знать, насколько важен звонок или текст, который он игнорирует или не видит, а у меня нет возможности узнать, видел ли он его (я имею в виду именно видел, а не просто смахнул сообщение, чтобы продолжить игру). Существуют приложения-мессенджеры, которые сообщают вам, когда сообщение доставлено и просмотрено, но ведь оно может быть проигнорировано просто потому, что сигнал о его поучении никто не слышал.

RespondASAP ® — мое решение этой проблемы.

В процессе разработки я поговорил с Беном, показал ему дизайн и концепцию приложения; идея ему понравилась, потому что, получив такое сообщение, он обязательно услышит его и поймет, что это нечто важное. Более того, у него будет возможность отправлять такие же сообщения мне. Так у нас возникает взаимопонимание, что RespondASAP ® предназначено только для важных случаев, а то, что Бену нужны новые батарейки для контроллера Xbox, к таковым не относится.

Мои друзья увидели и другие, «взрослые» применения этого приложения, потому что большинство из них большую часть

времени тоже держат свои телефоны в беззвучном режиме. Предложения варьировались от изменения заказа, когда друг берет вам напитки в баре, или поиска телефона, потерянного где-то дома, до рабочих ситуаций, когда нужно быстро связаться с коллегами...»

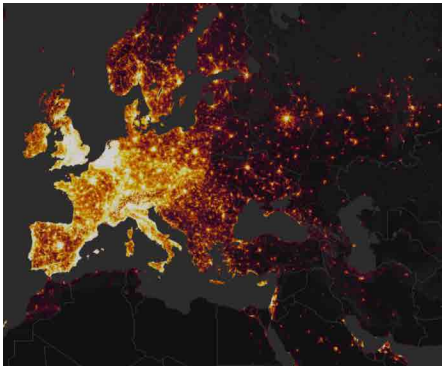
Конечно, существует риск, что злоумышленники получат контроль над вашим телефоном или доступ к вашему аккаунту с историей перемещений. Да, всякое вторжение в частную жизнь неприятно, поэтому надо предпринимать превентивные меры, чтобы такого не произошло, защищать свою информацию и не пренебрегать правилами цифровой гигиены. А еще рекомендуем иметь поменьше тайн, раскрытие которых может вам навредить.

Мы живем в прозрачном мире, где ничего нельзя абсолютно надежно спрятать.

Помните, что мы живем в прозрачном мире, где ничего нельзя абсолютно надежно спрятать. Например, не надо выкладывать маршрут своей пробежки в интернет, если вы служите на секретном объекте — такая курьезная история действительно произошла. Хакерам даже не потребовалось ничего ломать, достаточно было проанализировать открытые данные.

Бегают сегодня все — студенты и бизнесмены, домохозяйки и кинозвезды, пенсионеры и топ-менеджеры, любители собак (вместе с ними) и любители кошек (без них), спецагенты, солдаты и дипломаты. Поскольку все сегодня стало социальным, для бегунов есть специальные приложения, в которых они отмечают достижения, соревнуются заочно друг с другом, находят партнеров по тренировкам в реале — в общем, типичный клуб по интересам.

Вполне логично, что такие приложения записывают маршруты пробежек, чтобы вести статистику и точно подсчитывать сожженные калории, контролировать кардионагрузки и другие показатели физической активности. Разработчикам одного такого популярного приложения Strava пришла в голову мысль отобразить все пробежки своих пользователей по всему миру на тепловой карте. Надо признать, поучилось красиво!



Карту опубликовали в ноябре 2017-го, а спустя два месяца неожиданно случился конфуз. 20-летний австралийский студент Натан Русер, изучающий международные конфликты, обнаружил, что на этой карте можно увидеть и фитнес-маршруты солдат и агентов в чувствительных местах, включая американские базы в Афганистане и Сирии, авиабазу Великобритании на Фолклендских островах Маунт-Плезант, предполагаемую базу ЦРУ в Сомали и даже Район 51 (где, как говорят, американское правительство скрывает доказательства существования НЛО). Главным образом, в поле зрения

попали американские и британские войска, но также на этой карте засветились и российские базы — в том числе беговые дорожки наших дипломатов в Дамаске. В государствах, где не ведутся войны, карта окрашена примерно одинаково по всей площади, а в горячих точках она темная, за исключением мест дислокации военных.

Формально никакой утечки не произошло — данные на карте Strava обезличены, из них нельзя выяснить, кто именно бегает в этих отдаленных местах. Но сам факт повышенной физической активности в определенных районах уже позволяет делать выводы о присутствии там воинских формирований. Ну, не инопланетяне же бегают по секретной базе! Хотя кто знает...

Пентагон отреагировал быстро и объявил о новой политике, вступившей в силу немедленно: всем действующим сотрудникам Министерства обороны США запрещено использовать функции слежения на своих телефонах и устройствах в оперативных районах (в любом месте, где военные выполняют определенную миссию). Командиры могут разрешить использование в каждом конкретном случае только после проведения проверки безопасности. Обязательное обучение кибербезопасности теперь будет включать информацию о фитнес-трекерах и других технологиях, способных к геолокации.

Министерство обороны России запретило военнослужащим включать на смартфонах геолокацию вскоре после публикации об открытии австралийского студента.

Учитывая сказанное выше про возможности геолокации, эти меры нельзя признать достаточными. На самом деле у военных есть только один выход: полностью отказаться от использования потребительских

смартфонов, если они хотят сохранить режим секретности. Обычным же законопослушным гражданам не о чем беспокоиться: им можно бегать по утрам и вечерам там, где заблагорассудится, и спокойно делиться своими маршрутами с товарищами по этому увлечению.

Стоит ли бояться своей цифровой тени?

«Человек без тени — ведь это одна из самых печальных сказок на свете», — писал Евгений Шварц в одной из своих самых известных пьес (по мотивам сказки Г. Х. Андерсена). Мы добавим, что в наше время человек, не имеющей цифровой тени — то есть тот, о ком в Сети нет никакой информации или она крайне скудная, не выглядит реально существующим. Он становится призраком, если не оставляет цифровых следов. Получается как в сказке Шварца: когда Ученый опрометчиво отправил свою тень к принцессе, он сразу упал в обморок и все всполошились: «Беги за доктором! Доктор уложит дурака в кровать недели на две, а тем временем у него вырастет новая тень», — говорит один из персонажей.

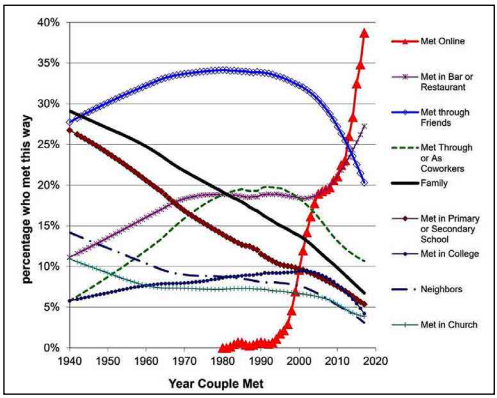
Не теряйте свою цифровую тень и следите за ее здоровьем: кормите хорошей информацией и водите гулять в интересные места.

Так что, не теряйте свою цифровую тень и следите за ее здоровьем: кормите хорошей информацией, водите гулять в интересные места — когда ваш принц или принцесса захотят с вами познакомиться, им будет легче понять, что вы за человек.

Опросы показывают, что 7 из 10 молодых людей в Великобритании проверяют интернет-профили человека перед тем, как отправить-

ся на свидание со своим визави, и 40% из них с подозрением относятся к людям, о которых сложно найти информацию в интернете. Только один из двадцати (5%) юношей и девушек в возрасте от 18 до 24 лет говорят, что они никогда этого не делают[1].

Интернет сегодня становится основным местом, где люди находят себе пару. Все остальные способы знакомства остались в прошлом веке. Просто примите это как факт. Встречают теперь не по одежке, а по аватарке и цифровому следу.



Michael Rosenfeld et al., Stanford University, Reuben J. Thomas, University of New Mexico, Sonia Hausen, Stanford University. Disintermediating your friends: How Online Dating in the United States displaces other ways of meeting. // Published in 2019 in the Proceedings of the National Academy of Sciences, Volume 116, issue 36, **https://doi.org/10.1073/pnas.1908630116**

---

1 *Would you go on a date with someone who didn't have a digital footprint? // YouGov, 2018.*

Выращивать правильную цифровую тень полезно не только из романтических соображений. Это влияет и на такие более прозаические и насущные стороны нашей жизни, как, например, поиск работы или обращение за кредитом в банк. Современный человек без адекватной цифровой тени вызовет много вопросов у любой службы безопасности. Поэтому не торопитесь уходить в полный цифровой детокс на веки вечные. Будет лучше, если вы научитесь с этим жить.

Воздействие цифрового следа на жизнь пользователей возрастает с каждым годом: к примеру, опросы показывают, что если в 2006 году только 11% работодателей проверяли социальные сети соискателя на работу, то в 2017-м это делали уже 70% компаний (по данным Career Builder, США, 2017). Едва ли в России ситуация принципиально отличается[1].

Но удивительное дело: насколько же много в интернете публикаций на тему того, как удалить свои цифровые следы! Почему-то людей это очень беспокоит. Авторы советов по «выпиливанию» себя из интернета, как правило, не озабочены тем, зачем это делать и каковы будут последствия. Они одержимы лишь одной идеей — стать цифровыми невидимками, чтобы скрыться от всевидящего ока государства.

Авторы советов по «выпиливанию» себя из интернета, как правило, не озабочены тем, зачем это делать и каковы будут последствия.

В большинстве случаев их советы по меньшей мере наивны, потому что у правительств есть свои механизмы отслеживания граж-

1 *70% of employers are snooping candidates' social media profiles. // Career Builder, 15 июня 2017.*

дан. Кроме того, цифровых следов сегодня так много и системы стали настолько сложными, что никакие рекомендации не будут исчерпывающими и надежными. И если уж вы что-то такое натворили, то цифровой след где-то все равно останется — там, где вам и в голову не придет искать.

В Мидлтауне, штат Огайо, в сентябре 2016 года сгорел дом 58-летнего Росса Комптона. К счастью, хозяин успел выбраться через окно, но его кошка погибла в огне. Сгорело все: дом площадью 2000 квадратных футов с четырьмя спальнями и тремя ванными комнатами стоимостью 179 тысяч долларов вместе со всем имуществом. Страховая компания оценила общий урон в 400 тысяч долларов.

Вроде бы обычное дело — пожар: загорелась электропроводка или коротнуло что-нибудь. Тем не менее, департамент пожарной охраны начал расследование — порядок есть порядок. Об умышленном поджоге сначала никто не думал: трудно поверить, что человек подожжет дом и оставит своего питомца умирать в огне. Но эксперты обнаружили, что очагов возгорания было несколько, да и сам погорелец путался в показаниях. Однако всего этого было недостаточно, чтобы сделать вывод о мошенничестве. Понятно же: у человека стресс, а ко всему прочему оказалось, что у него «искусственное сердце» — то есть он пользуется кардиостимулятором.

«Ага!» — сказали следователи и запросили ордер на получение медицинских данных с кардиостимулятора Комптона. Они хотели знать, каков был его пульс до, во время и после пожара. В судебных документах говорится: «Кардиолог, проверивший данные, определил: очень маловероятно, что г-н

Комптон смог собрать, упаковать и вынести такое количество вещей из дома, выбраться через окно своей спальни и оттащить многочисленные большие и тяжелые предметы в сторону за столь короткий промежуток времени при наличии имеющихся у него заболеваний»[1].

То есть налицо было очевидное вранье. В этом деле полиция впервые использовала данные кардиостимулятора, которые оказались отличным средством расследования и помогли выдвинуть обвинение в поджоге с целью получения страховки.

Даже продвинутые хакеры оставляют следы, по которым их находят. Обычным же пользователям лучше учиться ответственному поведению в цифровой среде и не впадать в цифровой анархизм.

«Многие очень опасаются трансформации общества и тотального контроля за обществом, вроде того, что описаны в книгах Хаксли или Оруэлла, — пишет в своем Фейсбуке учитель истории Александр Гулин. — Я всегда парирую цитатой из Джона Леннона: "Каждому есть что скрывать, кроме меня и моей обезьянки"[2]*. До 30 лет я вообще ничего нигде не терял и не забывал, держал все на контроле. Но возраст берет свое: часто, решая рабочие вопросы, отключаешь блок, связанный с контролем себя самого. (Обычно все происходит из-за банальной спешки). В прошлом году я забыл на остановке сумку со всеми документами (добрые люди на следующий день меня нашли и вернули). Зимой*

---

1 *Cops use pacemaker data to charge homeowner with arson, insurance fraud. // CSO Online, 30 января 2017.*

2 *Everybody's Got Something to Hide Except Me and My Monkey — песня The Beatles из «Белого альбома», написанная Джоном Ленноном.*

оставил макбук в такси (благодаря приложению, водитель привез его мне на следующий день). В пятницу в каршеринге выпал чехол от AirPods (ну очень торопился подписать какие-то документы). «Делимобиль» пытался найти мои вещи, но безрезультатно. И тут в воскресенье вечером мне пришло письмо от Belka Car — отчет о поездке в пятницу (я дважды ездил на «Делимобиле» и один раз на «Белке»): по цифровым следам машины они нашли человека, который пользовался ею после меня. Естественно, он им сообщил, что нашел мои наушники, и завтра с утра я могу забрать их на пункте охраны. Технологии не хорошие и не плохие; они упрощают нашу жизнь — на моем примере видно, что из-за цифровых следов я вернул намного больше, чем мог потерять. И вообще, хороших людей больше, чем плохих, — Джон Леннон это знал...»

Каждый клик — в истории

История посещения веб-сайтов и отдельных страниц — один из богатейших и ценнейших источников цифрового следа, оставляемого человеком. Маленькие дети, «дорвавшись» до компьютера, совершенно не задумываются о том, что каждый их клик сохраняется в истории браузера, и что потом будет неудобно, когда мама увидит, какие «интересные» ролики смотрел ее сын на YouTube. Он-то на голубом глазу будет все отрицать, дескать, он только играл в игру, которую ему открыли. Но предатель-браузер быстро выведет врунишку на чистую воду.

(В принципе, ничего драматичного в этом нет. Ну, посмотрел и посмотрел. Тему про «недетский» контент и ограничение доступа

к нему мы разберем в другой главе; сейчас наше внимание сосредоточено на технике).

> *История браузера хороша тем, что наглядно показывает, насколько дотошно фиксируются в интернете все действия пользователей, и как легко попасть в неловкую ситуацию, когда вы думаете, что делаете что-то втайне, а на самом деле это видно всем.*

Хорошо будет выучить этот урок с детства, потому что во взрослой жизни все точно также: на работе ваш системный администратор видит, какие сайты вы открывали и сколько времени вы там сидели, и если дело дойдет до конфликта с руководством, то эти данные запросто лягут на стол вашему начальнику, и крыть будет нечем.

Более-менее продвинутый ребенок уже знает об этом коварстве со стороны браузера и умеет чистить историю, благо это совсем не сложно: достаточно нажать «Ctrl-H», и появится список посещенных веб-страниц с точным временем посещения. Если ваша рука сразу тянется к кнопке «Очистить историю», — не спешите. Вездесущий Гугл уже запомнил все ваши блуждания по сайтам и настроил свои алгоритмы показа рекламы, так что локальная чистка в браузере ничем не поможет. Зато если вы вдруг закрыли страницу с какой-то важной информацией и забыли название сайта, то можно будет его найти в истории — согласитесь, это весьма полезно.

> *Кроме истории, есть еще кэш браузера — место, где он хранит временные файлы. Когда вы в первый раз открываете веб-страницу, то сначала все картинки и тексты с нее скачиваются на ваш компьютер (или телефон), а потом уже показываются на экране.*

Причем когда вы закрываете страницу и даже удаляете из истории запись о том, что вы ее смотрели, в кэше все равно остается ее копия. Это делается для того, чтобы ускорить его работу, — когда вы в следующий раз зайдете на ту же страницу, картинки не будут скачиваться заново, и вы увидите ее быстрее. Удобно? Конечно! Как водится, за все удобства надо платить. В данном случае плата невысока, всего лишь место на диске и цифровой след, отображающий ваши интересы.

Пока вы пользуетесь интернетом с личных устройств, про кэш браузера можно не беспокоиться — разве что иногда почистить, если возникли какие-то сбои с отображением некоторых страниц, а вот когда приходится пользоваться публичными компьютерами, об этом следует помнить. Например, вам нужно зайти в почту и переслать письмо с копией паспорта и другим документами вашему турагенту, чтобы оформить поездку в отпуск. Вы открыли письмо — и сканы паспортов попали в кэш. Поэтому закончив свои дела, не забудьте очистить историю браузера и удалить сохраненные данные. В браузере Chrome для этого надо нажать Ctrl-Shift-Del, и откроется окно «Очистить историю», в других браузерах есть аналогичная команда.

Закончив работать на публичном компьютере, не забудьте очистить историю браузера и удалить сохраненные данные.

Простые методы, описанные выше, защитят вас от чьих-то слишком любопытных обычных глаз, но не от профессионалов. В большинстве случаев этого будет достаточно, и не стоит пренебрегать такими мерами предосторожности, но помните — есть и более продвинутые инструменты: такие, как, например, HstEx — утилита из арсенала компьютерной криминалистики, которая создана

и разработана для восстановления удаленной истории и кэша браузера. Предположим, человек захотел что-то утаить, удалив свои следы — в таком случае программа HstEx поможет их извлечь из недр жесткого диска[1].

> *Разумно не пользоваться публичными компьютерами и чужими устройствами для любых операций, требующих ввода личной информации: просмотра почты, платежей через интернет-банк, подключения или отключения услуг в личном кабинете мобильного оператора или чего-то подобного.*

Кстати, если вы используете домашний компьютер в коллективном режиме (один на всех), то будет лучше завести для каждого члена семьи отдельный аккаунт. В этом случае и история браузера тоже будет у каждого своя, и тогда среди недавно просмотренных роликов у вас не окажутся сплошь стримы «Майнкрафта» и популярные ютьюберы. Также верно и обратное: если вы сами решите вечером посмотреть какое-то кино для взрослых, ребенок не увидит эту ссылку на стартовой странице, когда ему будет позволено посмотреть мультики.

Но этого мало: еще нужно будет приучить всех заходить только под своим аккаунтом и обязательно выходить из него, закончив играть или работать. Эта полезная привычка не раз сослужит вам хорошую службу, когда придется пользоваться чужими компьютерами. Например, школьники после занятий очень часто оставляют свои сессии открытыми, и кто угодно может получить доступ к их данным.

---

1 HstEx: **http://www.spy-soft.net/hstex/**

Нужно приучить всех заходить только под своим аккаунтом и обязательно выходить из него, закончив играть или работать.

Если по каким-то причинам вам не хочется оставлять следов в браузере, то можно воспользоваться режимом, когда функция отслеживания выключена. В браузере Chrome это называется режим «инкогнито», в FireFox — приватное окно, в Microsoft Edge — режим InPrivate; аналогичные режимы есть и в других браузерах. В таком режиме не сохраняются файлы cookie, данные сайтов и история просмотров, а также информация, которую вы вводите в формы. Когда это может вам понадобиться? Например, когда нужно что-то быстро посмотреть с чужого компьютера или телефона.

Но не стоит обольщаться насчет секретности в этом режиме: ваши действия в приватном окне видны системному администратору и интернет-провайдеру, а также доступны веб-сайтам, которые вы посещаете. Использование режима «инкогнито» скорее можно отнести к правилам цифрового этикета, нежели к средствам обеспечения безопасности. Приличный человек не оставляет за собой мусор, в том числе и цифровой.

Приличный человек не оставляет за собой мусор, в том числе и цифровой.

Перечитайте предыдущий абзац внимательно: даже в приватном режиме действия пользователя в браузере видны внешнему наблюдателю. Теперь представьте ситуацию: какой-то не слишком знакомый вам человек, случайно оказавшийся в компании, просит вас одолжить телефон — дескать, ему надо срочно зайти в свою почту и ответить на письмо. Надеюсь, вы понимаете, что все его

действия для провайдера, а, следовательно, и для правоохранительных органов будут выглядеть как ваши?

> *Иногда лучше показаться невежливым, чем потом доказывать, что это были не вы. В Англии даже есть поговорка: «Не пиши в интернете то, чего не можешь сказать полицейскому».*

Право на забвение и эффект Стрейзанд

«Что написано пером, того не вырубишь топором». Европейские, а следом за ними и российские законодатели решили оспорить эту народную мудрость и приняли ряд актов, которые условно называют «законом о забвении». Причина его возникновения ясна: она в том, что возник конфликт между правом человека на тайну частной жизни и свойством интернета помнить все. Действительно, нельзя же всю жизнь тыкать человека носом в ошибки молодости или в какие-то другие факты его биографии, которые давно утратили актуальность, но неизбежно всплывут в поисковой выдаче, как только новый работодатель или деловой партнер захочет просмотреть его цифровые следы.

> *В мае 2014 года Европейский суд рассматривал дело испанского гражданина Марио Костеха Гонсалеса против корпорации Google. В 2010 году Гонсалес обратился в Национальное агентство по защите данных с требованием удалить электронную версию статьи 1998 года в архиве газеты La Vanguardia о продаже его дома на аукционе в счет уплаты долга, который был впоследствии им погашен, а также ссылки на эту статью.*

В итоге дело дошло до Европейского суда, который вынес решение, что ссылки на Гонсалеса надо удалить, но только с испанского сайта Google.es, а материалы газеты оставить как есть. В первый же день вступления этого решения в силу Google получил 12 тысяч запросов на удаление персональных данных из своей поисковой системы (Википедия).

Это решение было воспринято как крайне неоднозначное — особенно в США и Великобритании, где свобода слова имеет приоритет над правом на конфиденциальность. По мнению противников «закона о забвении», он может привести к цензуре и переписыванию истории. «Кто контролирует прошлое, контролирует будущее», — писал Оруэлл и, несомненно, был прав. К тому же вызывает вопросы техническая реализация закона. В частности, редактор британского журнала Index on Censorship заявил The Guardian, что право на забвение выглядит как «план людей, не знающих, как работает интернет»[1].

Похоже, что это действительно так. Формально поисковики подчинились и разместили на своих сайтах специальную форму, где нужно указать адреса страниц, которые вы требуете удалить из поисковой выдачи, и убедительно аргументировать, почему это нужно сделать. Все обращения рассматриваются вручную, и при наличии объективных причин вашу заявку удовлетворят (но это неточно).

Предположим, вам удалось реализовать свое право на забвение, и раздражающая вас статья исчезла из индекса поисковика. А как быть с тем, что она осталась на сайте издания, которое ее опубликовало?

---

1 *Google to fight Spanish privacy battle. // The Guardian, 16 января 2011.*

Законодателей это не волнует. Видимо, они считают, что люди не умеют пользоваться другими инструментами поиска, кроме Google, Bing или Yandex. На самом деле в мире существует большое количество поисковиков, далеко не все из которых подчиняются правилам конкретной юрисдикции. Как мы видели из дела Костеха, даже Google нашел паллиативное решение, удалив ссылку только с испаноязычного домена.

Достиг ли Марио Костеха Гонсалес своей цели? В интервью 2014 года он выражал полное удовлетворение решением Европейского суда. Действительно, ссылку на ту злополучную статью удалили из поиска. Зато его имя стало нарицательным, и теперь уж точно никто не забудет, что в 1998 году он испытывал финансовые трудности, а потом судился с Google. В его случае мы видим действие эффекта Стрейзанд[1] во всей красе — когда кто-то пытается изъять информацию из общественного доступа, это приводит к ее большему распространению. В общем, на чужой роток не накинешь платок. Странно, что люди этого не понимают.

Попытки изъять информацию из общественного доступа приводят к ее большему распространению.

В Англии сформировалась другая культура по отношению к информации. Если в вашей биографии был какой-то нели-

1 *Эффект Стрейзанд (англ. Streisand effect) — социальный феномен, выражающийся в том, что попытка изъять определенную информацию из публичного доступа (цензура) приводит лишь к ее более широкому распространению (обычно посредством интернета). Термин получил распространение в 2003 году, когда Барбра Стрейзанд обратилась в суд с требованием взыскать с фотографа Кеннета Адельмана и сайта Pictopia.com 50 миллионов долларов США, так как фотография ее дома была доступна среди более 12 200 других фотографий побережья Калифорнии.*

цеприятный факт, то надо быть готовым, что это в любой момент может быть опубликовано, а потому иметь заготовленный разумный ответ вместо того, чтобы пытаться заткнуть рот говорящему.

Лучше иметь заготовленный разумный ответ, чем пытаться заткнуть рот говорящему.

Вот, например, Ричард Брэнсон в автобиографии «К черту все! Берись и делай!» со всей откровенностью рассказывает, как в 1971 году он попал под арест по обвинению в продаже в магазинах Virgin пластинок, которые декларировались как экспортные товары. Тогда таможня согласилась отказаться от уголовного преследования и уладить дело без суда, но весь ущерб ему пришлось возместить. А ведь мог бы умолчать про эту историю и потребовать права на забвение, чтобы никто ее не раскопал.

Британский подход к проблеме в целом выглядит более здравым, особенно в контексте современных технологий, когда гарантировать полное удаление какой-то информации практически невозможно — для этого нужно также уничтожить все ее копии, которых может быть сколько угодно и в самых разных местах.

Но законодателям Италии, Германии, Франции, Аргентины и ряда других стран пример Испании понравился, невзирая на технические сложности и эфемерность результатов. В результате граждане, которые тоже не особо разбираются в том, как устроен интернет, завалили главный европейский поисковик заявлениями об удалении разной информации о себе. Возможно, европейцы просто не знают, что в Яндексе «найдется все» — в том числе все, что удалено из Гугла.

Европейцы просто не знают, что в Яндексе «найдется все» — в том числе все, что удалено из Гугла.

Все та же газета La Vanguardia, получившая мировую известность в связи с первым делом по закону о забвении, по прошествии пяти лет подвела итоги его применения. С 2014 года по начало мая 2019 года Google получила в Европе 802 259 запросов на удаление данных, затрагивающих 3 127 986 веб-страниц, из которых 1 199 955 было удалено — 44,5% запросов. Из них 88,6% были выдвинуты частными лицами, а остальные — несовершеннолетними, юридическими лицами, политиками и людьми, занимающими общественные или другие должности[1].

Получается, что законодатели, действуя из лучших побуждений, на самом деле только подняли волну достаточно бессмысленной активности, направленной почти исключительно против корпорации Google. Пользователи «вошли во вкус» и захотели добиться большего успеха, чем Марио Костеха Гонсалес, — чтобы о них забыли не только в родной стране, но и вообще везде.

Чтобы не доводить ситуацию до полного абсурда, Европейский суд в начале 2019 года вынес решение о том, что «право быть забытым» не должно иметь обязательной юридической силы во всем мире. Дело возникло после того, как Национальная комиссия Франции по информационным технологиям и гражданским свободам (CNIL) оштрафовала Google на 100 тысяч евро за неспособность удалить информацию о человеке из всех его

1 *Cinco años de una sentencia pionera "para olvidar". // La Vanguardia, 11 мая 2019.*

доменов в интернет. Google обратился в суд с просьбой аннулировать штраф и выиграл спор[1].

Но это все взрослые дела. А как насчет детей?

> *В январе 2015 года в штате Калифорния вступил в силу закон, который неофициально называют 'Online Eraser Law for Minors' — «закон об онлайн-ластике для несовершеннолетних», если перевести буквально. Согласно этому закону, вебсайты и другие операторы интернета обязаны удалять по требованию любой контент, опубликованный несовершеннолетними. Закон также запрещает передавать данные несовершеннолетних третьим лицам в целях маркетингового продвижения товаров и услуг. Но его действие не распространяется на контент, опубликованный третьими лицами, в котором присутствует информация о ребенке или подростке[2].*

В принципе, подход здравый: взрослый человек должен думать головой, прежде чем публиковать в интернете всякие глупости, и отвечать за возможные последствия. Например, если вы выкладываете свои фото с чумовой вечеринки с друзьями, а потом вас не приглашают на серьезную работу, то это целиком ваша проблема. Для несовершеннолетних же закон делает исключение: ну, пошалили — и хватит! Детские выходки стираем, и добро пожаловать во взрослую жизнь.

---

1 *'Right to be forgotten' by Google should apply only in EU, says court opinion. // The Guardian, 10 января 2019.*

2 *How does California's Erasure Law stack up against the EU's right to be forgotten. // IAPP.org, 17 апреля 2018.*

У нас в России детские неразумные публикации могут обернуться вполне взрослыми проблемами — ведь в интернете «все ходы записаны», это знают, в том числе, и сотрудники правоохранительных органов.

> *В июле 2019 года произошло два похожих случая: суд оштрафовал на две тысячи рублей молодых жителей Ульяновска и Владимира по статье 20.29 КоАП — производство и распространение экстремистских материалов — за посты во ВКонтакте, размещенные ими в 2010 году, когда одному из них было 12 лет, и другому примерно столько же. Оба они запостили какие-то песни, которые, наверное, тогда казались им крутыми, а потом были признаны экстремистскими, — вот вам и административное правонарушение. Не то, чтобы пятно на всю жизнь, но неприятно*[1].

Поэтому нелишним будет объяснить подростку, что надо бы произвести ревизию своих музыкальных пристрастий и генеральную уборку на своей странице во ВКонтакте. И не только музыкальных.

Но как это сделать? В Федеральном Перечне экстремистских материалов сегодня почти 5 тысяч позиций. Дать ребенку полный список — только возбудить лишнее любопытство. Да и как технически сопоставить содержимое его страницы с перечнем?

В России аналогичный «закон о забвении» появился в 2016 году[2]. Согласно ему, операторы поисковых систем должны по запро-

---

1 *Двух россиян оштрафовали по статье об экстремизме из-за постов во «ВКонтакте» девятилетней давности. // МБХ медиа, 18 июля 2019.*

2 *Федеральный закон от 13 июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации».*

су граждан изымать из выдачи ссылки на материалы, которые, по мнению заявителей, являются недостоверными или неактуальными. При этом закон во вступившей в силу редакции не распространяется на внутренний поиск по соцсетям.

Только за три первых месяца после вступления закона в силу Google, по ее данным, получила свыше 1,4 тысячи запросов на удаление ссылок, а Яндекс — более 3,5 тысяч. При этом обе компании удалили более четверти запрошенных ссылок[1].

Чтобы воспользоваться своим правом быть забытым, нужно заполнить специальную форму в каждом из популярных поисковиков:

- ***Google*** *(https://support.google.com/legal/troubleshooter/1114905)*

  https://support.google.com/legal/contact/lr_rudpa?product=websearch&uraw=

- ***Яндекс*** *(https://yandex.ru/support/abuse/troubleshooting/oblivion.html)*

- ***Mail.ru*** *(https://go.mail.ru/support/oblivion/)*

В форме понадобится указать адреса страниц, которые вы хотите изъять, и пояснить, какое отношение они имеют к вам, и почему не должны появляться в результатах поиска. Чем больше аргументов вы при этом приведете, тем больше шансов, что запрос удовлетворят: запросы рассматриваются вручную,

1 *Конституционный суд не усомнился в «праве на забвение» // Газета «Коммерсантъ», 20 апреля 2019.*

и решение по каждому случаю принимается индивидуально. К форме нужно будет приложить копию паспорта или другого документа, удостоверяющего личность: их сверят, чтобы избежать ошибок.

> *Решение принимает администрация сервиса, которая может и отказать. Не всякая информация подлежит удалению по желанию гражданина, а лишь признанная недостоверной или неактуальной.*

Если вы не согласны с решением, и хотите настоять на удалении каких-то сведений о себе, то можете обратиться в суд. Только помните об эффекте Стрейзанд: пока вы общаетесь с поисковиком, это ваше частное дело, поисковики не публикуют информацию о запросах на удаление данных. А вот идти в суд, чтобы отстоять свое право быть забытым, — лучший способ достичь обратного эффекта. Так случалось уже не раз, однако граждане этого упорно не понимают и продолжают наступать на одни и те же грабли, приобретая все более широкую известность. Эффект Стрейзанд работает в интернете неумолимо. Это испытал на себе, в частности, продюсер Евгений Пригожин, который в итоге отозвал свой иск к Яндекс, и авторитет Сергей Михайлов, известный как «Михась»: суд он, правда, выиграл, но тем самым напомнил о своих прошлых делах всем, кто давно уже о них забыл.

Право на забвение у вас есть, но пользоваться им нужно аккуратно.

Короче говоря, право на забвение у вас есть, но пользоваться им нужно аккуратно, с пониманием того, как работают технологии и как распространяется информация в сети.

Заметаем цифровые следы самостоятельно

Как мы с вами выяснили, иметь цифровые следы — нормально, даже для ребенка. В целом пользы от них больше, чем вреда. Однако бывают ситуации, когда свою цифровую историю нужно основательно почистить. При этом едва ли стоит впадать в крайность и пытаться удалить все следы своего присутствия онлайн — на самом деле, обычному человеку это не под силу, даже хакеры и спецслужбы не всегда справляются с такой задачей. Но кое-что можно сделать для уменьшения будущих рисков.

> *Прежде всего, стоит удалить все аккаунты, которыми вы не пользуетесь, а стало быть, не меняете пароли к ним и вообще не следите за их безопасностью. О'кей, хорошая мысль, но как их все найти?*

Довольно часто учетные записи привязываются к почте, и если у вас почтовый ящик на Gmail, то можно воспользоваться сервисом **deseat.me**, который найдет все ваши активные и давно забытые аккаунты в соцсетях и на других сайтах, чтобы провести ревизию и решить, что оставить, а от чего пора избавиться.

Если у вас другая почта, то придется удалять свои учетные записи вручную. Вспомнить, где вы регистрировались, поможет менеджер паролей — специальное приложение или сервис в браузере. Идем методично по списку и «пропалываем» наши цифровые грядки. Иногда бывает так, что владельцы интернет-ресурсов не хотят расставаться со своими пользователями и прячут функции удаления аккаунта поглубже. В этом случае воспользуйтесь советом сайта Justdelete.me (**https://backgroundchecks.org/justdeleteme/ru.html**), который сразу перенаправит вас на нужные страницы или объяснит, почему удаление невозможно.

Не рубите сгоряча, может быть, вам еще пригодится ваша история — вдруг надумаете мемуары писать?

Многие ресурсы — например, Фейсбук, ВКонтакте, почти все сервисы Google и другие — дают возможность выгрузить все свои посты, фотографии и документы в виде архива и сохранить у себя на компьютере. Не всегда эта функция на виду, но если поискать, то найдется. Не рубите сгоряча, может быть, вам еще пригодится ваша история — вдруг надумаете мемуары писать? Но помните, что если уж «рукописи не горят», то цифровая информация и подавно — где-то копия все равно останется.

Мы уже не раз говорили, что в интернете почти ничего не исчезает. Но где же это все лежит, если мы этого не видим? Вот, например, написал человек сгоряча какой-то твит, а потом подумал и удалил. Или компания решила полностью переделать веб-сайт, где были, в том числе, и ваши посты в форуме — а в новой версии его вообще не оказалось. Бывает, что издание опубликовало какую-то новость, а она оказалась недостоверной, и пришлось ее убрать. Неужели все это исчезло навсегда? Вовсе не обязательно. Есть множество вариантов для путешествия в цифровое прошлое.

Во-первых, есть Wayback Machine — всемирный архив интернета с поисковым сервисом, позволяющим увидеть нужный веб-сайт таким, каким он был на определенный момент в прошлом. Вводите адрес, выбираете время — и готово! Проект ведет некоммерческая организация Internet Archive, которая с 1996 года создает цифровую библиотеку интернет-сайтов и других культурных артефактов в цифровой форме. Там хранятся копии веб-страниц, книги, газеты и журналы, телепрограммы, аудио и видеозаписи.

Во-вторых, кэш Google — поисковик сохраняет тексты всех проиндексированных им страниц, чтобы люди могли их просмотреть в случае недоступности сайта. Для этого в результатах поиска после адреса страницы нажмите кнопку со стрелкой вниз и выберите Cached — вам откроется сохраненная копия искомой страницы. Обычно информация хранится в кэше несколько дней, в зависимости от частоты переиндексирования сайта. Или можно воспользоваться специальным сервисом ***http://cachedview.com/****, который ищет сразу по кэшу.*

Аналогичным образом работают кэш Яндекса и других поисковых машин. Имеют архивные копии своих ресурсов все социальные сети, интернет-магазины, онлайн-библиотеки и другие провайдеры. Если вам понадобилось сохранить какую-то страницу, то для этого есть специальный сервис Archive.is: просто вводите адрес — и все, вы приняли участие в сохранении цифрового наследия.

Теперь вы понимаете, насколько трудно полностью уничтожить информацию после того, как она попала в интернет? Здесь все многократно копируется и архивируется, плотность записи все время повышается, а стоимость носителей падает, так что в обозримой перспективе процесс будет продолжаться. Поэтому лучше хорошенько подумать, прежде чем выкладывать что-либо в Сеть.

Как случайно попасть в Википедию

Чтобы удостоиться персональной статьи во всемирной онлайн-энциклопедии, надо быть известным человеком. Таким, например,

как Олег Тиньков, про которого, естественно, есть статья. Из нее можно узнать, что кроме всего, прочего он увлекается велоспортом и создал команду «Тинькофф», которая участвует в престижных международных велогонках.

> *В 2015 году на Джиро д'Италия Олег Тиньков участвовал в тренировках наравне со своими спортсменами и проехал всю дистанцию — неофициально. Естественно, это привлекло внимание прессы, и фото известного банкира на велосипеде пополнило его досье в Википедии. Но, кроме самого Олега Юрьевича, в кадр попала пользовательница Фейсбука Юлия Барышева, которая просто приехала в Италию посмотреть велогонку. Позже фотографию увидели ее коллеги и рассказали ей. Юлия сама увлекается велосипедным спортом и работает в банковской сфере, так что история получилась сугубо позитивная. «За спиной сильного мужчины всегда должна стоять красивая женщина!» — пошутила она на своей странице в Фейсбуке, обнаружив себя в Википедии.*

Но давайте посмотрим шире: мы ежедневно попадаем в объективы чьих-то камер и не можем никак этого избежать. Это не только камеры наблюдения, про которые мы уже говорили.

> *Фотографируют сегодня все: наши друзья, туристы, случайные прохожие, блогеры и профессиональные журналисты. И все это с высокой степенью вероятности попадает в интернет, потому что все фото нынче цифровые.*

Это тоже часть цифрового следа, на которую очень трудно влиять. Поиск по изображениям и технология распознавания лиц скоро сделают такие фото источником информации о вас. Да и сейчас,

если вы публикуете фотографии в Фейсбуке, он сразу предлагает отметить на фото людей из числа ваших знакомых, но вы же понимаете, что распознал-то он всех, да?

Едва ли имеет смысл этого бояться — надо просто учитывать, что мир действительно прозрачен. Если вы куда-то направляетесь по секрету и даже оставили свой телефон, чтобы вас не отслеживал Google, вы можете просто встретить на пути группу китайских туристов, которые запечатлеют вас в летний день на фоне Эрмитажа — а вы на работе сказали, что страшно больны и не можете выйти из дома. Получится неудобно.

По крайней мере, попробуйте не усугублять ситуацию — когда фотографируете что-либо сами, старайтесь, чтобы в кадр не попадали случайные люди. Это тоже часть современного цифрового этикета.

Когда фотографируете что-либо сами, старайтесь, чтобы в кадр не попадали случайные люди.

К тому же изображение частного лица защищает закон. В России это статья 152.1 Гражданского кодекса, которая гласит, что обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. К счастью, для любителей фотографии есть ряд исключений: согласие не требуется, если съемка производится в общественных местах и на публичных мероприятиях, или если гражданин позировал за плату (чем промышляют «живые статуи» в туристических местах).

В Европе с 2018 года действует GDPR, в котором есть аналогичная статья, запрещающая публикацию изображений третьих лиц без их ведома, но с такими же оговорками насчет публичных мест. Так что не надо безуспешно ждать, пока толпа перед «Моной Лизой» рассосется, чтобы, не дай бог, не нарушить право на конфиденциальность какого-нибудь европейца. Если вы не занимаетесь коммерческой фотографией, то вам не стоит бояться баснословных штрафов за это. Максимум, что может произойти, если кто-то из жителей Евросоюза увидит себя на вашей странице в Фейсбуке, — он или она потребуют это фото удалить, и вам придется это сделать, потому что закон будет на их стороне.

- *Учитесь вести себя так, чтобы не было стыдно за свои цифровые следы.*

В общем, стоит помнить: любое наше действие в виртуальном мире и почти каждое в реальном оставляет цифровой след. И мы не всегда имеем возможность управлять этим. Учитесь вести себя так, чтобы не было стыдно за свои цифровые следы.

Контрольные вопросы

1. Что такое цифровой след?
2. Чем отличаются активные и пассивные цифровые следы?
3. Как местоположение отслеживается по wi-fi?
4. Почему не стоит удалять все свои цифровые следы?

5. Когда нужно использовать режим «инкогнито» в браузере?

6. Что такое кэш браузера? Как его очистить?

7. Что такое «право на забвение»? Как это работает?

8. Что такое кэш Google? Можно ли его очистить?

9. Как увидеть, как выглядел какой-то сайт в прошлом?

Глава 7

В интернете правда никто не знает, что ты собака?

В этой главе мы обсудим тему анонимности в интернете. Это важная тема: анонимность часто равна безопасности, но корпорации и госорганы борются с ней, чтобы эффективнее учитывать пользователей (и их интересы). В большинстве случаев это происходит по обоюдному согласию: люди жертвуют анонимностью ради удобства. Уровень анонимности может быть разным в зависимости от ситуации; грамотный пользователь должен знать о технических средствах ее защиты и понимать, когда их следует применять, а когда нет.

На рисунке Питера Штейнера, опубликованном 5 июля 1993 года в The New Yorker, изображены две собаки, и та, что сидит за компьютером, говорит: «В интернете никто не знает, что ты собака».

Эта фраза, ставшая впоследствии крылатой, абсолютно точно отражала состояние анонимности в сети в начале 90-х: действительно, каждая собака (если она была достаточно грамотна, чтобы работать на компьютере) могла зайти в интернет и свободно высказывать свое мнение по любому вопросу, вступать в дискуссии на любые темы, публиковать что угодно — и не раскрывать о себе никакой информации, кроме прозвища (nickname). То есть назваться президентом Соединенных Шатов мог кто угодно, и ему бы за это ничего не было. Впрочем, в то время не существовало и понятия «официальный аккаунт» — назваться-то президентом собака могла, но этому бы никто не поверил. В итоге была полная сетевая вольница.

"Remember when, on the Internet,

В наши дни эта поговорка утратила актуальность: анонимности в интернете больше нет. Поэтому вполне естественным стало появление 23 февраля 2015 года на страницах того же The New Yorker рисунка Каамрана Хафиза, на котором одна собака спрашивает другую (обе отчетливо напоминают псов с рисунка Штейнера): «А помнишь, когда в интернете никто не знал, кто ты?»

Вот так два рисунка, разделенные 22-мя годами, наглядно демонстрируют эволюцию анонимности в глобальной сети. Как видите, все изменилось.

> *Собак больше не пускают в интернет. Знаете, почему? У них нет удостоверения личности, телефонного номера и банковского счета. А чтобы пользоваться большинством сервисов, теперь нужно сначала подтвердить свою личность.*

По большому счету существуют две причины такой трансформации. Во-первых, интернет превратился в огромную базарную площадь, где каждый что-то покупает и продает. И, как на всяком базаре, в сети появились жулики и мошенники — как со стороны продавцов, так и со стороны покупателей. Но если все анонимы и никто никого не знает, то как найти обманщика, чтобы призвать к ответу? Такое положение вещей мешало развитию рынка, поэтому от анонимности стали отказываться в пользу прозрачности и репутации, ведь безупречная репутация — главное условие успеха в торговле.

Второй причиной стало то, что в интернет пришла политика — в самом широком смысле. Сначала появились новостные сайты, потом блоги, следом за ними социальные сети — и вдруг оказалось, что техническая система, созданная некогда учеными для собственных целей, формирует общественное мнение сильнее, чем телевизор. Плюс к тому сеть превратилась в среду коммуникации всех со всеми, что способствовало созданию сообществ самой разной направленности — от клубов любителей котиков до тоталитарных сект и террористических организаций. Естественно, что правительства всполошились и стали закручивать гайки. Котики их не пугали, чего никак нельзя было сказать о терроризме и манипуляции общественным мнением (и, более того, общественным сознанием) с помощью фейков. Анонимность означала безнаказанность, а это власти предержащие никак не устраивало.

Сегодня опубликовать что-либо в интернете — все равно, что написать это на заборе и приложить свои паспортные данные.

Сегодня опубликовать что-либо в интернете — все равно, что написать это на заборе и приложить свои паспортные

данные. Анонимности больше нет. Строго говоря, ее никогда и не было: технически всегда существовала возможность проследить действия пользователя и установить его личность, как бы он ни пытался замести следы. (Оговоримся: речь идет об обычных пользователях). Но до относительно недавнего времени киберполицейским и спецслужбам не хватало опыта в таких делах и законодательных рычагов для влияния на провайдеров интернет-сервисов.

Важная вещь, которую следует запомнить: интернет — это публичное пространство, и не существует абсолютно надежных способов сделать что-либо в Сети анонимно. Любая анонимность временна. Поэтому нужно вести себя так, чтобы быть готовым ответить за каждое высказывание и за каждое действие.

«Слепите мне маску от доносчивых глаз...»[1]

В реальном мире для анонимности издавна использовались маски. Их надевали для тайных встреч влюбленные, под ними скрывались знатные особы, когда не хотели привлекать к себе внимание. Не меньше любили маски и преступники, стремившиеся остаться неузнанными и избежать правосудия.

Наиболее известны в широких кругах венецианские маски: у нас они прочно ассоциируются с карнавалом, однако в Венеции было принято носить их и в повседневной жизни — город-то был небольшой, и практически все друг друга знали. Невозможно было выйти

1 *Егор Летов, строка из песни «Слепите мне маску».*

из дому, чтобы не встретить кого-то из знакомых, какая уж тут тайна частной жизни! Поэтому маски пришлись венецианцам настолько по вкусу, что в XVII веке их стали надевать везде и всюду, причем поступали так не только знатные особы, но и простолюдины. Обычай этот весьма удивил стольника Петра Толстого, посланного царем Петром Первым в заграничное учение в Италию в 1697 году:

> *«И приходит в оперы множество людей в машкарах, по-словенски в харях, чтоб никто никого не познавал, кто в тех операх бывает, для того что многие ходят з женами, также и приезжие иноземцы ходят з девицами; и для того надевают мущины и женщины машкары и платья странное, чтоб друг друга не познавали. Так и все время каранавала ходят все в машкарах: мущины, и жены, и девицы; и гуляют все невозбранно, кто где хочет; и никто никого не знает»*[1].

Властям республики повальное увлечение горожан анонимностью не понравилось. Были введены специальные законы: например, в маске нельзя было заходить в церковь и даже приближаться к ней; запрещено было ношение масок в казино, а также в ряде других случаев. В итоге маски остались разрешены только во время карнавала, и обычай этот сохранился до наших дней.

Сегодня маски раздражают правоохранителей ничуть не меньше, поэтому во многих странах запрещено скрывать лицо во время массовых мероприятий. Такие законы действуют в Канаде, Австрии, Дании, Германии, Испании, Швеции, Франции, Украине, в пятнадцати штатах США и в некоторых кантонах Швейцарии.

---

1 *Толстой Петр Андреевич. Путешествие стольника П. А. Толстого по Европе (1697-1699) // Библиотека Максима Мошкова Lib.ru/Классика.*

Закон Российской Федерации «О митингах»[1] также запрещает участникам митингов скрывать свое лицо, в том числе использовать маски, средства маскировки, иные предметы, специально предназначенные для затруднения установления личности.

Организатор митинга должен требовать от участников не скрывать свои лица. Лица, не подчинившиеся законным требованиям организатора публичного мероприятия, могут быть удалены с места проведения данного публичного мероприятия.

В общем, наивно было бы полагать, что правительства, столь нетерпимые к обычным маскам, спокойно отнесутся к анонимности в интернете. Разумеется, власти пойдут на любые шаги, чтобы исправить свое первоначальное упущение и добиться тотальной идентификации пользователей компьютерных сетей, что мы сейчас повсеместно и наблюдаем. Однако техническая сторона этого вопроса гораздо сложнее, и одними запретами тут не обойтись.

Власти пойдут на любые шаги, чтобы добиться тотальной идентификации пользователей компьютерных сетей.

С одной стороны, нельзя не признать, что анонимность мешает государственным органам выполнять свои прямые обязанности, то есть обеспечивать нашу с вами безопасность и ловить преступников. С другой — средства обеспечения анонимности помогают реализовать законное право граждан на тайну личной жизни и частной переписки, закрепленное в Конституции Российской

1 *Федеральный закон «О собраниях, митингах, демонстрациях, шествиях и пикетированиях» № 54-ФЗ от 19 июня 2004 года.*

Федерации (и других стран). Соблюсти в такой ситуации баланс интересов довольно трудно, поэтому каждое изменение границ анонимности вызывает в обществе горячие дебаты.

Зачем нам анонимность в интернете

Затем же, зачем она была нужна венецианцам в их маленьком городе. Интернет стал большой деревней, где все на виду. И вполне естественно, что людям не хочется выставлять напоказ всю свою жизнь, все свои маленькие слабости, привычки, интересы, друзей, врагов, покупки, перемещения, состояние здоровья и все прочее. Кому какое дело, что за фильмы я смотрю и какая пицца мне нравится? Если мне захочется, я сам об этом расскажу.

Сегодня мы опасаемся излишнего внимания не со стороны Большого Брата, а со стороны Большого Продавца.

Но нет. Мир сегодня устроен иначе. Сегодня мы больше опасаемся излишнего внимания к себе не со стороны Большого Брата (то есть спецслужб), а со стороны Большого Продавца — всех этих бесчисленных «корпораций добра»[1] — Google, Apple, Amazon, Facebook, Microsoft и других гигантов ИТ-индустрии, которые очень любят собирать данные о своих пользователях и не раз на этом попадались. Из российских компаний в этом ключе стоит упомянуть Ян-

1 *Фраза «Don't be evil» (рус. — «Не будь злом») уже давно известна как неофициальный девиз Google, благодаря которому компанию называют «Корпорацией добра». Впервые упоминание этого выражения появилось в 2000 году в корпоративном кодексе сотрудников Google. Спустя 18 лет, как заметило издание Gizmodo, фразу незаметно удалили.*

декс со всеми его многочисленными сервисами и Mail.ru, которой принадлежат популярные соцсети ВКонтакте и Одноклассники.

Зачем они шпионят за нами? Ответ прост: чтобы больше продавать нам. Сбором пользовательских данных занимаются сегодня все интернет-компании от мала до велика, ведь «люди — это новая нефть». Конечно, они хотят сделать нашу работу в интернете удобнее и приятнее, они рекомендуют нам фильмы и книги, отели и экскурсии, кредиты и страховки — и все на основе наших же «предпочтений». То есть на основе нашего цифрового следа, той информации, которую мы вольно или невольно оставляем, пользуясь различными сервисами.

> *Мегакорпорации типа Google обладают сегодня фантастическими ресурсами и могут консолидировать информацию о человеке, собранную из различных источников.*

Чтобы «засветиться», нам даже необязательно называть свое имя и показывать фотографию — достаточно входить в интернет со своего телефона или компьютера. С телефоном все просто — его номер указывает на вас однозначно. С компьютером, в принципе, тоже — открыли один раз свою почту или зашли в соцсеть — и это устройство будет привязано к вашему профайлу.

Так что забавная история, которая гуляет по Сети и которую я привел ниже, на самом деле отнюдь не выглядит фантастической. Можно только добавить, что отвечать вам будет не сотрудник «Корпорации добра», а голосовой ассистент — искусственный интеллект, знающий о вас абсолютно все.

— Пиццерия Google, добрый день, слушаю вас!
— Пиццерия чего?

— Пиццерия Google. Что будете заказывать?
— Но... Разве это не пиццерия «Синьор Помидор»?
— Да, была, но Google ее купил, и теперь объем наших услуг стал полным.
— Прекрасно. Примете заказ?
— Естественно! Хотите повторить ваш обычный заказ?
— Обычный заказ? Откуда вы знаете, какой?
— У нас установлен идентификатор заказчиков, и мы знаем, что последние 53 раза с этого номера заказывали пиццу «Везувий», с двойным сыром и ветчиной, плюс бутылка хорошо охлажденного пива «Лагер».
— Надо же, я и не думал... Хорошо, давайте.
— Простите, могу вам дать совет?
— Конечно.
— У вас есть наше полное меню?
— Нет.
— Это самое полное меню, и я хотела бы посоветовать вам пиццу с творогом и зеленью, и бутылку минеральной воды с малым содержанием солей.
— Творог? Зелень? Соли? Вы с ума сошли? Я все это ненавижу!
— Понимаю, но это только на пользу вашему здоровью. Кроме того, у вас очень высокий холестерин...
— Откуда вы это знаете?
— Наша фирма располагает самой большой базой данных на нашей планете. Через номер телефона мы знаем ваше имя, и поэтому имеем доступ к вашим анализам в поликлинике.
— Плевать на вашу базу данных! Я не хочу пиццу с творогом и зеленью! Я принимаю медикаменты, и поэтому могу есть все, что мне вздумается, понятно?
— Сожалею, но вы не принимали таблетки в последнее время.

— Откуда вы знаете? Шпионите за мной каждый день?
— Нет, нет! Просто мы располагаем базой данных всех аптек в городе, и последний раз вы там были 3 месяца тому назад. А в одной упаковке только 30 таблеток.
— Это правда. И откуда вам это известно?
— Из вашей кредитки...
— Чего?
— Да, вы, когда платите в своей аптеке картой своего банка, получаете скидку. В нашей базе данных все ваши расходы по карте. И за последние три месяца вы там ничего не покупали, но покупали в других магазинах, что означает, что вы карту не потеряли.
— А что, я не могу заплатить наличными? А? Что? Что теперь скажете?
— Это невозможно. Вы платите наличными только 100 долларов в неделю своей служанке, все остальное платите только кредиткой.
— Откуда вам известно, сколько я плачу служанке?
— Но она же платит соцстрах...
— Да пошли вы!
— Как хотите. Сожалею, но вся эта информация у меня на экране, и я хочу только помочь вам. Думаю, что вы должны зайти к своему врачу и взять анализы, которые вы сделали в прошлом месяце, чтобы уточнить дозировку медикаментов.
— Вы мне все осточертели — и ты, и компьютеры, и базы данных, и интернет, и Google, и Facebook, и отсутствие личной жизни в XXI веке, и это проклятое государство...
— Пожалуйста, не расстраивайтесь. Это не в ваших интересах...
— Заткнись! Завтра же уеду куда-нибудь дальше от всего этого дерьма. Поеду на острова Фиджи, или куда угодно, где нет интернета, компьютеров, телефона, ни людей, которые

будут за мной все время подглядывать...
— Я вас понимаю...
— В последний раз воспользуюсь кредиткой, чтобы купить билет на самолет и улететь на край света!
— Прекрасно...
— Снимите заказ на пиццу. Я ее не хочу.
— Хорошо, уже снят. Если вы позволите... одна маленькая деталь...
— ЧТО ЕЩЕ!?
— Хочу только напомнить, что ваш паспорт просрочен...

Ну, а что такого? Ведь они следят за нами для нашего же блага. А то купил бы человек билет на самолет, а улететь бы не смог. Все так, но кому-то такая забота может показаться чрезмерной. К тому же рекомендации, которые дает искусственный интеллект, запросто могут оказаться ошибочными. Когда это касается выбора пиццы, в том нет большой беды, а вот насчет здоровья совсем другое дело, тут ошибка ИИ может стоить кому-то жизни. Или банк откажет студенту в кредите на обучение, сочтя его IQ слишком низким на основе анализа просмотренного им контента — а он-то всего лишь дал побаловаться телефоном младшему брату. Иными словами, вся эта система рекомендаций и целевой рекламы, якобы максимально точно отражающей потребности человека, все еще очень несовершенна и при этом очень назойлива, поэтому желание от нее скрыться вполне понятно.

Система рекомендаций и целевой рекламы, якобы точно отражающая потребности человека, все еще очень несовершенна.

На самом деле мы хотим не так уж и много: анонимного серфинга и анонимных публикаций. То есть чтобы никто не подглядывал,

на какие сайты мы ходим и что там смотрим, и чтобы можно было высказать любое мнение или выложить фотографии, не подписывая их своим именем — анонимно. Заметьте: это не означает автоматически возможности публиковать преступные или запрещенные материалы, модератор сайта или провайдер их удалит, а ваш аккаунт заблокирует (как это сейчас и происходит на Фейсбуке, например).

Псевдоним — это почти как аноним, но не совсем

Кроме анонимности, есть такое понятие как псевдонимность. Оно обозначает действия от лица вымышленного персонажа, чье имя обычно напрямую не связанно с настоящей личностью человека.

Очень любят псевдонимы деятели искусства — писатели, художники, актеры, музыканты. У Чехова было более 50 псевдонимов — вот уж он бы разошелся в наше время! Создал бы полсотни разных профайлов и постил бы там свои рассказы. Псевдонимы заводят по разным причинам: например, когда собственное имя не слишком благозвучно — была Норма Джин Бейкер, а стала Мэрилин Монро. Или когда уважаемый в своей профессии человек вдруг решает написать детективный роман — так мы сначала познакомились с писателем Борисом Акуниным и только потом узнали, что есть известный ученый-японист и переводчик Григорий Чхартишвили, и что это один и тот же человек.

Если ваша цель — отделить часть интернет-активности от обычной сетевой жизни, то псевдонимность — вполне приемлемый вариант.

Короче говоря, если ваша цель состоит в том, чтобы отделить некоторую часть вашей интернет-активности от вашей же обычной сетевой жизни, то псевдонимность — вполне приемлемый вариант. Создаете несколько аккаунтов на разные случаи — и готово. Например, захотели попробовать себя в поэзии, но побаиваетесь критики друзей, да и вообще у вас серьезная работа — псевдоним как раз то, что нужно, или любите погонять танчики в свободное время — тоже лучше под псевдонимом. Главное — не запутаться самому в своих виртуальных личностях.

Профессор физики Ричард Фейнман очень любил играть на барабанах и достиг в этом деле такого мастерства, что его стали приглашать поиграть настоящие музыканты. Однажды их игру услышала жена одного из преподавателей Калтеха[1] *— она была хореографом и ей захотелось поставить балет, где в качестве музыкального сопровождения использовались бы ударные инструменты. Фейнман согласился сотрудничать, но настоял на том, чтобы никому не стало известно, что он — профессор физики, лауреат Нобелевской премии и тому подобное. Он хотел, чтобы зрители пришли посмотреть балет и послушать музыку, а не поглазеть на мировую знаменитость, играющую на барабанах.*

Балет имел успех. Хотя аудитория была не слишком большой, зрителям, которые пришли посмотреть представление, оно очень понравилось. Позже музыку записали

1 *Калифорнийский технологический институт (англ. California Institute of Technology; часто сокращается до Caltech) — частный исследовательский университет, расположенный в городе Пасадина в штате Калифорния, один из ведущих университетов в США и один из двух самых важных, наряду с Массачусетским технологическим институтом.*

на кассету, хореограф переехала на Восточное побережье и поставила там свой «Карибский балет» — так назывался ее спектакль на музыку Фейнмана. А потом он узнал, что она выдвинула балет на конкурс, собравший хореографов со всех Соединенных Штатов, и заняла призовое место[1].

Только не надо строить иллюзий, что стоит назваться другим именем — и вас никто не найдет. Возможно, обычному пользователю соцсети или форума, чувства которого вы ранили ехидным комментарием, найти вас окажется не по силам, и все его угрозы «вычислить вас по IP и ноги переломать» останутся пустыми словами. Но не пытайтесь играть в прятки с настоящим Большим Братом — с правоохранительными органами и спецслужбами, а также с мафией. Вас действительно вычислят, встретят возле дома и предложат поговорить так, что не будет возможности отказаться.

Да и для компаний типа Google раскрыть подобный уровень конспирации — детская задача. Зашли с одного компьютера в два аккаунта? ОК, вот вы и попались. Использовали один телефон для регистрации? Пополнили базу сведений о себе. Для начинающего поэта беды в этом никакой нет, пишите себе под псевдонимом. В случае успеха ваш псевдоним может оказаться известнее и популярнее, чем ваше настоящее имя. А нет — так и не страшно.

Но если у вас есть причины для более тщательной маскировки в Сети, то стоит подумать о более продвинутых методах анонимизации.

---

1 *Из книги «Вы, конечно, шутите, мистер Фейнман».*

> *Применительно к интернету под анонимностью понимают техническую невозможность связать действия, выполняемые на интернет-ресурсах, с человеком, выполняющим эти действия.*

IP-адрес вашего компьютера или телефона как раз и выполняет роль этого связующего звена между вами и вашим устройством — его вам выдает интернет-провайдер или оператор связи, с которым у вас есть договор.

Вычислить по IP — что это значит?

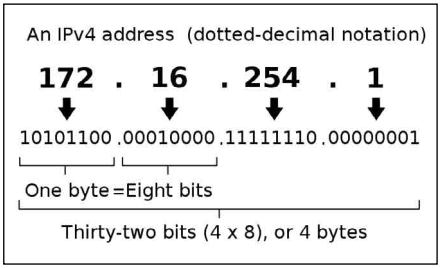
Что же такое этот IP-адрес, знание которого так важно для определения личности пользователя?

IP — это сокращение от Internet Protocol, дословно означающее «межсетевой протокол». Его придумали в середине 1970-х годов отцы-основатели интернета Винт Серф (Vint Cerf) и Боб Кан (Bob Kahn), когда решали задачу, как обеспечить передачу информации в Сети в условиях нестабильной работы каналов связи и отдельных узлов.

Есть легенда, что это делалось на случай ядерной войны, чтобы сохранить управление войсками, если какие-то из командных центров попадут под удар. На самом деле все гораздо прозаичнее: в то время для связи использовались обычные телефонные линии, имевшие свойство разрывать соединение в самый неподходящий момент. Люди в такой ситуации просто перезванивают, спрашивают друг друга, на чем оборвался разговор, и продолжают дальше, а компьютеры этому надо было научить.

IP-протокол вместе со своим «братом», протоколом TCP, позволяют компьютерам восстановить соединение и продолжить передачу данных с момента, когда связь нарушилась. IP-адрес — это аналог телефонного номера, он должен быть у каждого устройства, подключенного к Сети.

IP-адрес состоит из четырех чисел в диапазоне от 0 до 255 и выглядит так:



Максимальное число адресов в сети — 4 294 967 296, всего четыре с небольшим миллиарда, причем некоторые серии адресов зарезервированы для разных технических нужд и не используются, так что реально доступное число адресов еще меньше.

Значит, у интернета тоже есть номерная емкость и она может исчерпаться? Да, именно так и произошло. К настоящему времени свободные IP-адреса закончились, а нужно подключить еще пару миллиардов новых пользователей и десятки миллиардов всяких датчиков и умных устройств, поэтому все интернет-провайдеры постепенно переходят на новую версию IP-протокола, IPv6, где адресов хватит на всех. Похоже на то, как было в Москве, когда к семизначным городским номерам пришлось добавить код 495 или 499.

Как и телефонные номера, IP-адреса выдают блоками: сначала региональным интернет-регистраторам, которых всего пять: Америка, Европа (включая Ближний Восток), Азиатско-Тихоокеанский регион, Латинская Америка и Африка. Те, в свою очередь, делят свою квоту между странами, входящими в их регион; дальше блоки распределяются по провайдерам, которые и раздают их конкретным пользователям, но далеко не всем, а только тем, кто попросил выделить статический (то есть постоянный) адрес. Большинству же обычных пользователей дается динамический адрес из числа свободных в настоящий момент.

Статический адрес может вам понадобиться в случае, если вы решили завести собственный веб-сайт — чтобы посетители знали, куда приходить. Для того чтобы гулять по интернету, хватит и динамического. Да, он будет каждый раз разный, и узнать, кто под ним «сидит», не получится — если только не попросить провайдера показать свои записи, где зафиксировано, когда и какому клиенту данный IP-адрес был выдан. Такая информация может быть получена только по запросу правоохранительных органов, человеку с улицы провайдер ничего не скажет.

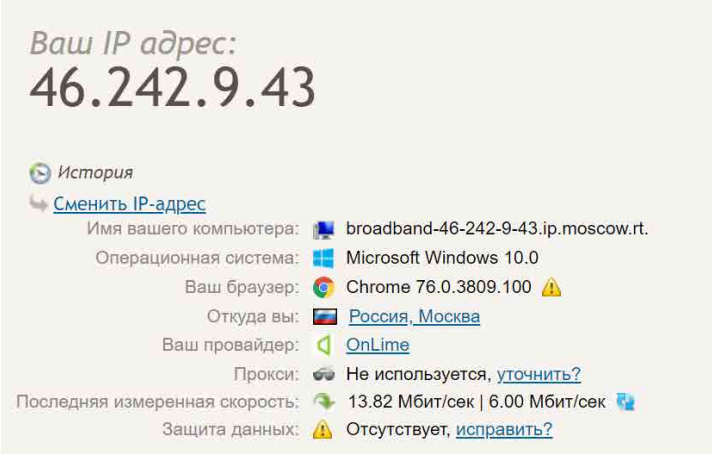
Важно: если вы хотите найти злоумышленника или хулигана по IP-адресу, обязательно фиксируйте время, в которое он предположительно выходил в интернет. Адрес-то у него, скорее всего, динамический.

А потом предстоит доказывать, что с этого устройства совершил противоправные действия именно тот человек, который официально числится его владельцем; что он его не потерял, не оставил без присмотра в общественном месте, где к нему мог иметь доступ

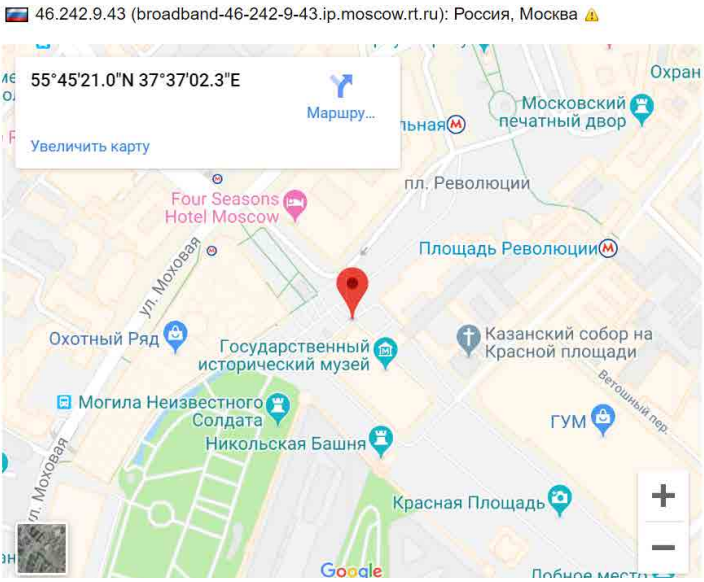
неограниченный круг неизвестных лиц, что wi-fi в его квартире не взломали хакеры и т.д. и т.п.

Кстати, для внешнего наблюдателя IP-адрес всех устройств, подключенных к вашему роутеру, — ноутбуков, планшетов, телефонов, своих и гостей, в том числе и непрошенных, будет один и тот же. Чтобы вычислить нарушителя, нужно будет провести более детальное расследование.

Как узнать свой IP-адрес, под которым вас видно в интернете? Очень просто. Напишите в окне поиска Google «ip», нажмите «Ввод» — и сразу увидите свой публичный адрес, выданный вам провайдером. Если вам хочется более подробной информации, то можно перейти на сайт ***2ip.ru****. Также здесь можно проверить и любой другой адрес — просто введите его в специальном окне.*



Здесь уже видно, откуда вы: Россия, Москва. Если кликнуть по этой ссылке, то сервис покажет более точно ваше местоположение. Но не спешите волноваться, что все видят, где вы сидите:



публично доступны только координаты города — для Москвы это будет нулевой километр: помните это место перед Иверскими воротами, где туристы бросают монетки?

И еще раз: без запроса из правоохранительных органов физический адрес пользователя по его IP-адресу узнать нельзя. Полиция, Следственный комитет или ФСБ направит провайдеру за-

прос только в рамках расследования какого-либо дела; просто так из любопытства никто работать не будет. Но даже это вовсе не означает, что злоумышленника мгновенно возьмут — если только он не круглый идиот, то он позаботился о том, чтобы скрыть свой настоящий IP-адрес.

Другое дело, если вас ищут за пост, например, во ВКонтакте, нарушающий законодательство РФ: тут данных, предоставленных провайдером и администрацией соцсети, будет достаточно для идентификации. Поэтому не мешает лишний раз подумать перед тем, как публиковать контент на потенциально опасную тему.

Что скрывать честному человеку?

Прежде чем продвинуться немного дальше к цели стать интернет-невидимкой, давайте еще раз поразмыслим, зачем это нужно. «Честному человеку скрывать нечего», — говорят противники анонимности, мотивируя свою позицию интересами общественной безопасности. Дескать, тотальная слежка нужна, чтобы ловить террористов. Обычно под такими лозунгами выступают представители власти, уговаривая общество согласиться с очередным ограничением свободы. Этот мотив тут же подхватывают и представители бизнеса, не менее госорганов заинтересованные в сборе данных на своих пользователей. Возьмем, к примеру, слова исполнительного директора Google Эрика Шмидта (Eric Schmidt), сказанные в интервью каналу CNBC в 2009 году:

> *«Если у вас есть то, о чем не должен знать никто, возможно, в первую очередь вам не стоило делать этого. Но если вам*

> *действительно нужна такого рода конфиденциальность, реальность заключается в том, что поисковые системы, включая Google, хранят подобную информацию в течение некоторого времени. И это важно, потому что, например, все мы в Соединенных Штатах должны соблюдать Патриотический акт. Вполне возможно, что эта информация может предоставляться органам власти»*[1].

С тех пор возможности Google по отслеживанию действий пользователей фантастически выросли, и это вызывает все большее беспокойство в обществе, в то время как политики и крупный бизнес продолжают изображать недоумение: «Разве вы делаете что-то незаконное? Что вы хотите скрыть?»[2]

На самом деле речь идет не о сокрытии, а о защите. Мы живем в мире, полном тайн. Есть тайна государственная, коммерческая, банковская, налоговая, адвокатская, врачебная, тайна завещания, тайна усыновления, тайна следствия (куда без нее), а у журналистов есть право не раскрывать источник информации. В конце концов, есть тайна связи, раз уж мы говорим про интернет.

> *Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (действующая редакция) гласит, что на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи.*

---

1 *Google CEO Eric Schmidt on privacy. // YouTube,* ***https://youtu.be/A6e7wfDHzew***

2 *Честному человеку нечего скрывать? // BitNovosti.com, 13 июля 2015.*

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

Операторы связи обязаны обеспечить соблюдение тайны связи.

Но, как говорится, на оператора надейся, а сам не плошай: граждане тоже имеют право позаботиться о сохранении своих тайн, если считают меры, предпринимаемые операторами, недостаточными. И анонимность может быть очень полезным инструментом в этом деле.

Вот несколько примеров.

Допустим, вы работаете над новым проектом и придумали гениальную идею, способную изменить мир. Всякой идее такого масштаба предшествует долгий и кропотливый поиск, изучение массы научных работ, просмотр тысяч статей и публикаций. Это значит, что вам непременно придется воспользоваться поисковиком в интернете — и если это будет наш любимый Google, то все ваши поисковые запросы будут сохранены, проанализированы и привязаны к вашему профайлу. А значит, есть риск, что эта информация куда-то утечет. Да, сама по себе она несекретна, но на ее основе можно сделать вывод о направлении работ вашей лаборатории, а это уже хлеб для шпионов.

Или, предположим, вы врач и ведете анонимный прием больных. При некоторых диагнозах, таких как алкогольная или наркотическая зависимость, психические или венерические болезни, это вполне распространенная практика. Не исключено, что с кем-то

из пациентов вам понадобится общаться через интернет, и в таком случае, разумеется, стоит позаботиться об анонимности и на техническом уровне, чтобы сохранить врачебную тайну. (Строго говоря, оказание телемедицинских услуг в анонимном порядке на данный момент в нашем законодательстве не предусмотрено, но и не запрещено)[1].

Работа адвокатов, следователей и журналистов тоже требует анонимных контактов со свидетелями и информаторами, и нужно понимать риски, которые при этом возникают, — в первую очередь, у людей, которые, возможно, рискуют жизнью, передавая вам какие-то сведения. В такой ситуации тезис, что «честному человеку нечего скрывать» выглядит особенно лицемерно — даже если идентификация пользователей производится суперзащищенной государственной системой, риск утечки этих данных все равно остается. Уж лучше оставаться анонимом.

Общепринято, что благотворительность должна быть анонимной. Благотворитель может иметь разные причины сохранять инкогнито: нежелание раскрывать свое финансовое состояние, стремление избежать персонифицированного чувства благодарности и так далее. (В связи с этим возникает вопрос об анонимных платежах, но это отдельная большая тема).

И, в конце концов, право на тайну частной жизни тоже еще никто не отменял. «Дело не в том, что у меня есть что скрывать, а в том, что мои дела не касаются всех остальных». Может быть, я хочу смотреть мультики про розовых пони, но не желаю, чтоб об этом

1 *Возможно ли анонимное обращение пациента за получением телемедицинской консультации? // ГАРАНТ.РУ, 21 мая 2018.*

знали все на свете. Это не бог весть какая тайна, просто мне так спокойнее.

Анонимность для «чайников»: начнем с прокси

Достичь базового уровня анонимности в ситуации, когда большинство людей не знают, кто вы — простая задача даже для «чайника».

> *«Все, что нужно — это VPN, блокировщик рекламы и инструмент конфиденциальности (privacy tool), например, Privacy Badger[1]. Этот уровень контроля поможет запутать ваши следы в интернете и сбить с толку тех, кто попытается собрать личные данные», — объясняет Бен Уильямс, операционный директор блокировщика рекламы Adblock Plus[2].*

Стоп-стоп, давайте по порядку, не так быстро.

Итак, чего, прежде всего, хочет путешественник по интернету? Посещать любые сайты, которые ему заблагорассудится, сообщая им

---

1 *Privacy Badger — это надстройка для браузера, которая запрещает рекламодателям и другим сторонним трекерам тайно отслеживать, куда вы переходите и какие страницы просматриваете в интернете. Если рекламодатель отслеживает вас на нескольких сайтах без вашего разрешения, Privacy Badger автоматически блокирует загрузку любого содержимого от него в вашем браузере. Для рекламодателя это выглядит так, как будто вы внезапно исчезли. Проект организации Electronic Frontier Foundation. Есть версии для Firefox и Chrome.*

2 *Возможна ли анонимность в интернете? // **GeekBrains.ru**, 15 мая 2018.*

о себе только те сведения, которые он сочтет нужным сообщить, а может и вовсе ничего, — ведь оказавшись где-то за рубежом, мы хотим бродить по городу, слившись с толпой туристов, а вовсе не расхаживать все время с российским флагом, тем более что неизвестно, как там относятся к русским. Но наш IP выдает нас с головой. По IP-адресу владелец каждого сайта сразу видит, откуда вы — с точностью до города.

По IP-адресу владелец каждого сайта сразу видит, откуда вы — с точностью до города.

Дальше возможны варианты. Например, в зависимости от страны, вам могут ограничить доступ к какому-либо контенту. Часто так бывает с онлайн-кинотеатрами, потому что правообладатели предоставляют им лицензию для показа фильмов на определенной территории. Для интернета, где нет физических границ, это звучит глупо, но тем не менее такие ограничения существуют со времен, когда фильмы продавали на кассетах и DVD, и, купив диск в Англии, дома вы с удивлением обнаруживали, что его нельзя посмотреть на вашем плеере.

Кстати, бывает и наоборот: если вы попробуете зайти в свой оплаченный аккаунт в легальном российском онлайн-кинотеатре из-за рубежа, то, скорее всего, вас не пустят — местный провайдер даст вам IP-адрес, с которым вы будете выглядеть для администрации как иностранец — и все, «кина не будет».

Чтобы избежать всех этих неприятностей, вам нужно скрыть свой IP-адрес. Но интернет так не работает: для установления сеанса связи с любым сайтом какой-то адрес обязательно нужен.

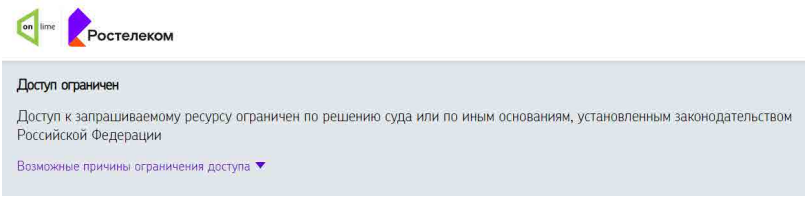
Эту задачу решают сервисы-анонимайзеры, которые подставляют вместо вашего настоящего IP-адреса IP-адрес любой страны по вашему выбору, устраивая эдакий бал-маскарад в интернете. Хотите нарядиться ковбоем с дикого Запада — пожалуйста! Предстать немцем в баварской шляпе с пером — не вопрос! Венецианцем в таинственной маске — тоже организуем!

Технически анонимайзеры, кроме самых примитивных, представляют собой прокси-сервер (от англ. **proxy** — «представитель», «уполномоченный»). Что это такое? На самом деле — очень полезная вещь, которая есть у каждого провайдера и в каждом крупном офисе. Причем сокрытие вашего IP-адреса — далеко не основная цель ее работы.

> *Представьте: в офисе работают сто человек, и все заходят с утра посмотреть новости в Яндексе. Это значит, что с сервера Яндекса нужно сто раз загрузить одну и ту же страницу — даже если трафик у вас безлимитный, скорость-то все равно ограничена, а всем хочется, чтобы интернет работал быстро. Поэтому и придумали сохранять на промежуточном сервере информацию, скачиваемую извне, чтобы экономить трафик. Еще прокси защищает компьютеры внутренней сети от внешних атак. Не то чтобы на сто процентов (это было бы слишком легко) — но, по крайней мере, от прямых посягательств. А в качестве бонуса как раз и прилагается анонимизация — для внешних наблюдателей все внутренние пользователи имеют один и тот же IP-адрес.*

Есть у прокси и неприятное для пользователей свойство: его можно настроить так, что он будет блокировать какие-то сайты. Для этого используют черные и белые списки: например, в офисе

могут закрыть доступ к соцсетям, занеся их в черный список, чтобы в рабочее время сотрудники не отвлекались; или закрыть доступ вообще ко всему интернету, кроме нескольких нужных для работы серверов, включенных в белый список. Кстати, примерно также работают блокировки Роскомнадзора: ведомство издает список запрещенных сайтов, а провайдеры его регулярно скачивают, чтобы настроить черные списки на своих серверах. И когда вы идете, куда не положено, вам показывают вот такую страницу:



Кроме провайдерских и офисных прокси есть и прокси-анонимайзеры, специально созданные для обеспечения анонимного доступа. Они-то и меняют ваш настоящий IP-адрес на случайный (обычно давая вам выбрать страну). Таким образом, прокси помогает обходить блокировки: провайдер видит, что вы заходите на разрешенный сайт, и спокойно вас пропускает, а дальше вы говорите прокси-серверу, куда вам на самом деле хочется попасть — и идете.

Благодаря активности Роскомнадзора, который в своих попытках закрыть доступ к мессенджеру «Телеграм» в 2018 году массово блокировал миллионы IP-адресов, на время переставали работать ни в чем не повинные сайты; «под раздачу» попали, в частности, ВКонтакте, Яндекс, Одноклассники, Yahoo, Twitter и многие другие. Ошибочные блокировки быстро исправили, но, как говорится, оса-

дочек остался[1]. Граждане занялись повышением компьютерной грамотности, и все от мала до велика узнали о существовании прокси (и VPN, но про них чуть позже) как средства доступа к заблокированным ресурсам. Впрочем, кибербезопасность — такая тема, где поверхностные знания могут оказаться хуже, чем полная неосведомленность.

Кибербезопасность — такая тема, где поверхностные знания могут оказаться хуже, чем полная неосведомленность.

«В интернете есть много открытых бесплатных прокси-серверов, и некоторые из них предоставляют разнообразные полезные услуги», — встретив такую фразу, стоит насторожиться. Как же они себе на жизнь зарабатывают, если не берут денег с пользователей? Вариантов всего два: либо это честный сервис, который сначала даст бесплатно какую-то ограниченную функциональность и будет потом очень настойчиво предлагать купить полный пакет (что в целом вызывает понимание); либо это чей-то очень «мутный» бизнес, который на самом деле собирает ваши данные с корыстными целями — например, чтобы продать их рекламодателям (в лучшем случае) или хакерам (что гораздо хуже). А может быть, такой «левый» прокси вообще работает под колпаком у спецслужб, чтобы учесть всех несознательных граждан.

Какой же прокси выбрать? Платный или бесплатный? Российский или обязательно зарубежный? Вообще говоря, никакой. Прокси в чистом виде сейчас уже почти не используются. Все разработчики предлагают более совершенное решение — VPN.

---

1 *После двух лет безуспешных попыток Роскомнадзор объявил о снятии требования по ограничению доступа к мессенджеру Телеграмм. О мессенджере Телеграмм. // Роскомнадзор, официальный сайт, 18 июня 2020.*

Сайт в конце туннеля, или Зачем нам VPN

Fig.1 VPN functional principles

Так что же это такое — VPN? Чем она лучше прокси? VPN расшифровывается как Virtual Private Network, а по-русски — виртуальная частная сеть. По правде говоря, название ничуть не проясняет того, как эта штука работает и как помогает нашей анонимности в интернете. Разгадка, как это часто бывает, лежит в истории.

> *Изначально VPN были созданы для того, чтобы позволить сотрудникам удаленно работать с корпоративными серверами не только находясь в офисе, но и дома или в командировке.*

Компании были очень озабочены конфиденциальностью своих данных и не доверяли публичным сетям. (Кстати говоря, правиль-

но делали — мы к этой теме еще вернемся). Начальник службы безопасности какого-нибудь условного банка или госкорпорации упал бы в обморок, если бы узнал, что сотрудники пересылают файлы, сидя со своим ноутбуками где-нибудь в Макдональдсе. А что делать? Пропустить день рождения ребенка и ехать в офис, чтобы пару раз кликнуть мышкой?

К счастью, программисты придумали решение. Чтобы исключить возможность кражи или подмены данных при их передаче по публичным сетям, они разработали технологию, которая позволяет установить защищенное соединение между компьютерами одной организации, даже если они находятся за пределами офиса. Это похоже на то, как члены тайного общества узнают друг друга по особым знакам на званом приеме, и среди общего шума находят минуту-другую, чтобы пошептаться о своих коварных планах по захвату мира.

> *Использовать VPN специально для того, чтобы анонимно ходить в интернет, никто не собирался. Она потому и частная, что была предназначена только для своих. А виртуальная — потому, что работает поверх обычной сети и каждый раз коммутируется по-новому.*

Как же это происходит? Вот, допустим, вы сидите в кафе и хотите подключиться по VPN к своей рабочей электронной почте. Если вы внимательно читали предыдущий раздел про IP-адреса, то, наверное, догадались, что сначала вам придется через местный (небезопасный) wi-fi подключиться к интернету, и тогда вашему компьютеру дадут IP-адрес. Так, а дальше? Дальше ваш компьютер видит в сети VPN-сервер и подает ему тайный знак. Сервер отвечает, и они прокладывают между собой туннель, то есть уста-

навливают логическое соединение, которое для внешнего наблюдателя выглядит как обычный обмен пакетами. А на самом деле они обмениваются зашифрованными сообщениями, которые даже если перехватить, то прочитать все равно не получится. На выходе из туннеля VPN-сервер расшифровывает ваш трафик и выпускает его в офисную сеть.

Вы входите где-нибудь в Польше, а выходите в Канаде — и ни один провайдер этого не видит.

Зачем все эти хитрости обычному пользователю? Представьте, что VPN-серверы стоят во всех (ну, хорошо, во многих) странах мира и между ними прорыты туннели, и это все единая сеть. Вы входите где-нибудь в Польше, а выходите в Канаде — и ни один провайдер этого не видит. Что значит «выходите в Канаде», спросите вы? Это значит, что VPN работает и как прокси — то есть выдает вам IP-адрес той страны, какой вы попросили, и дальше вы обращаетесь к любым сайтам так, как будто находитесь в Канаде.

Чем же это отличается от обычного прокси? Во-первых, прокси обычно не шифруют трафик, и он может быть перехвачен (встречаются и шифрованные прокси, но это уже почти VPN). Во-вторых, чтобы обходить блокировки, прокси-сервер должен стоять за границей, но тогда и он сам может быть заблокирован. А сервер VPN может стоять и дома — трафик-то передается по шифрованному туннелю! (Правда у провайдера остается возможность блокировать подозрительный трафик — все, что непонятно, то и подозрительно).

Современные VPN установить не сложнее, чем какой-нибудь антивирус, — просто скачиваете дистрибутив и ставите.

Первые VPN были очень дороги и сложны, установить и правильно их настроить могли только специально обученные люди, и потому технология оставалась недоступной обычным пользователям. Да и секретов у них особых не было, чтобы платить за такой сервис. Современные VPN установить не сложнее, чем какой-нибудь антивирус, — просто скачиваете дистрибутив и ставите. Или того проще: устанавливаете плагин в браузере, и — вуаля! Но у браузерных VPN есть ограничение: через них идет только веб-трафик, а ведь бывает, что некоторым приложениям тоже нужен защищенный канал — например, почтовому клиенту. Короче говоря, десктопные VPN более универсальны.

Остается вопрос: платить или не платить? Решайте сами, не давая, однако, жадности пересилить голос разума. Вот, например, что пишут в новостях:

> *Каждое пятое VPN-приложение в Google Play — потенциальный источник вредоносного ПО.*
>
> *22 января 2019 года стало известно, что наиболее популярные бесплатные VPN-приложения в Google Play Store содержат проблемы, которые могут угрожать безопасности пользователей. Согласно результатам исследования, проведенного специалистом Metric Labs Симоном Мильяно (Simon Migliano), каждое пятое приложение является потенциальным источником вредоносного ПО, а в четверти проанализированных программ содержатся уязвимости, связанные с утечками DNS-запросов пользователей*[1].

1 ***TAdviser.ru.***

Конечно, сам по себе факт оплаты не гарантирует, что продукт надежный, но риск нарваться на преднамеренное хищение ваших данных при использовании коммерческих продуктов все-таки значительно меньше.

Из минусов VPN обычно упоминают низкую скорость работы, однако чаще причина медленного интернета кроется в настройках wi-fi или ограничениях провайдера. На хорошем канале замедление из-за включенного VPN практически незаметно. К сожалению, факт использования VPN невозможно полностью скрыть: некоторые программы могут по этой причине работать некорректно. Сам провайдер тоже может счесть трафик VPN подозрительным и блокировать его, хотя расшифровать и прочесть — не сможет.

Можно сказать, что VPN — это основной инструмент защиты вашей анонимности в интернете.

Итак, можно сказать, что VPN — это основной инструмент защиты вашей анонимности в интернете. Фактически VPN включает в себя функции прокси, то есть позволяет скрывать ваш IP-адрес и шифрует данные при передаче, чтобы не допустить их утечки.

По статистике за 2018 год, сервисами VPN хотя бы однажды пользовались 19% российской аудитории. Согласно данным Brand Monitor, чаще всего VPN устанавливают молодые пользователи (18–24 лет) — 22% опрошенных. Вероятнее всего, число пользователей VPN продолжит расти вместе с ростом понимания, что анонимность в сети имеет большую ценность.

Ситуация на рынке VPN меняется динамично, поэтому трудно дать совет, какой именно продукт выбрать. Почитайте свежие обзоры

и выберите для себя VPN, платный или бесплатный — на ваше усмотрение. Не забудьте защитить все устройства, с которых вы выходите в интернет, включая смартфоны.

Интернет как госуслуга? Еще нет, но может быть

Государство (любое) выступает последовательным противником анонимности. С точки зрения властей идеальной была бы ситуация, когда все граждане заходят в интернет по предъявлению паспорта (например, через сайт Госуслуг) и все их шаги записываются в специальный журнал. Посетил такой-то сайт, прочитал новости, оставил комментарий. Написал письмо иностранцу, вот текст. В интернет-магазине заказал черную футболку, зонт и велосипедный шлем. Очень подозрительно!

Это не шутка, это правда жизни: летом 2019 года в Гонконге эти предметы входили в стандартную экипировку участников протестов, поэтому китайские интернет-магазины прекратили их продажу жителям города. Зачем протестующим зонты? Очень просто. Чтобы скрывать лица от камер видеонаблюдения[1].

---

1 *В связи с пандемией коронавируса во многих городах и странах ношение масок в общественных местах стало обязательным. И даже после снятия ограничительных мер едва ли власти станут заставлять граждан перестать носить маски. Интересно, как это отразится в законодательстве о митингах? Поставщики систем распознавания лиц заявляют, что могут узнать человека и в маске, но маска ведь может быть любой, не только стандартной медицинской.*

Зачем протестующим зонты? Очень просто. Чтобы скрывать лица от камер видеонаблюдения.

Если в целях борьбы с анонимностью власти готовы запретить обычные зонты, то что уж говорить о специализированных средствах сокрытия личности в цифровом пространстве. Естественно, они попали под огонь законодательной «артиллерии».

> *С 1 ноября 2018 года в России действует закон[1], который обязывает владельцев VPN-сервисов и анонимайзеров не предоставлять пользователям возможность обхода блокировок сайтов, внесенных в единый реестр Роскомнадзора.*

Технология VPN не создавалась специально для обхода блокировок. Так получилось. После введения упомянутого закона эта возможность, скорее всего, останется только в продуктах зарубежных поставщиков. Что касается российских разработчиков, то они, безусловно, вынуждены подчиниться, о чем, в частности, объявила Лаборатория Касперского. С июля 2019 года VPN-сервис Kaspersky Secure Connection выполняет требования Роскомнадзора и блокирует трафик, сообщая пользователям при попытке доступа к сайтам из реестра, что «данная страница недоступна в РФ».

Зарубежные VPN могут уйти из России, если на них будет оказываться давление: например, штрафы за неисполнение требований РКН. Об этом прямо сказал представитель Tor Guard:

---

1 *Федеральный закон от 29 июля 2017 года № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».*

«Удаление серверов в стране, в которой “правовой климат может представлять угрозу для онлайн-безопасности наших клиентов” — стандартная политика компании. По этой причине решено немедленно прекратить работу серверов в Санкт-Петербурге и Москве».

Анонимайзеров и служб VPN так много, что заблокировать их все нереально.

Такой поворот событий может создать сложности для пользователей — ведь IP-адреса VPN-сервера, находящегося за рубежом, тоже могут быть заблокированы, а пока ты не добрался до сервера, туннель не построишь. Успокаивает то, что анонимайзеров и служб VPN так много, что заблокировать их все нереально. Теоретически возможен и китайский сценарий, когда блокируется весь подозрительный трафик, который не поддается расшифровке спецслужбами, но это маловероятно.

Пока закон не запрещает частным лицам пользоваться анонимайзерами и VPN-сервисами, в том числе и зарубежными. Нет ответственности для граждан и за просмотр заблокированных страниц — ответственность наступает только за распространение запрещенного контента и за высказывания, нарушающие законодательство РФ. Для обычного пользователя это выглядит как запрет продажи сигарет несовершеннолетним: когда подросток покупает сигареты, наказывают не его, а продавца.

И еще раз: VPN — средство безопасного доступа к сетевым ресурсам, а не средство обхода блокировок. За заботу о собственной безопасности пользователя надо хвалить, а не наказывать.

Пространство для анонимности сокращается не только из-за гонений на анонимайзеры и VPN. 1 июля 2018 года в России вступил в действие так называемый «закон Яровой»[1]. Согласно этому закону, все провайдеры должны хранить на своих серверах переписку и звонки пользователей в течение полугода. Такие меры обосновывают борьбой с терроризмом. Но при этом они еще дают спецслужбам неограниченные возможности слежки за всеми гражданами без исключения.

О том, какие конкретно данные будут о нас собирать, было сказано позже в приказе Минкомсвязи. Согласно этому документу, интернет-компании и сервисы должны хранить и предоставлять спецслужбам: псевдоним, дату рождения, адрес, фамилию, имя, отчество, паспортные данные, языки, которыми владеет пользователь, список его родственников, текст сообщений, аудио- и видеозаписи, адрес электронной почты, дату и время авторизации и выхода из информационного сервиса, наименование программы-клиента.

«Закон Яровой» определяет, что сохраняемая информация должна предоставляться сотрудникам ФСБ по их запросу. В то же время, последующим постановлением Правительство прописало возможность круглосуточного доступа ФСБ к хранилищу и базе данных — между системой оператора и соответствующими структурами ФСБ должен быть налажен постоянный канал связи. Кроме того, не исключено, что ФСБ

1 *Постановление Правительства Российской Федерации от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи».*

сможет получить у владельцев некоторых соцсетей, почтовых служб и мессенджеров доступ к ключам шифрования.

К Яндексу с требованием предоставить ключи шифрования для сервисов «Яндекс.Диск» и «Яндекс.Почта» уже пришли. Пока непонятно, чем эта история закончится, но лучше исходить из предположения, что все российские интернет-сервисы будут полностью прозрачными для спецслужб[1].

Что нужно объяснить подростку: не надо изображать из себя крутого хакера; надо понимать, что все доступные пользователю средства анонимизации, скорее всего, будут неэффективны против государственных систем, поэтому надо учиться ответственному поведению в Сети.

Пользователь, иди сюда, у нас есть печеньки!

Анонимность всегда продается в обмен на удобство и маленькие радости жизни. Если вы регулярно ходите в одно и то же кафе, вас начинают там узнавать, здороваться при входе и спрашивать: «Вам как обычно?» И вы отвечаете «Да». Постепенно вы разговоритесь с официантом, расскажете, что живете здесь неподалеку, что ваш ребенок ходит в соседнюю школу, в пятый класс, ваша мама как раз приехала посидеть с внуком, и сегодня вы можете задержаться в кафе подольше. То есть сообщите о себе много личной инфор-

1 *За год применения закон Яровой угодил в патовую ситуацию. // **Telesputnik.ru**, 18 июля 2019.*

мации, которую официант запомнит и, возможно, даже передаст своему сменщику, чтобы тот позаботился о постоянном клиенте. Вы расслаблены и не думаете о безопасности. А вместе с чашкой кофе и счетом вам принесут печеньку — комплимент от заведения.

Веб-сайты тоже раздают посетителям печеньки-куки[1], только виртуальные. И не вам лично, а вашему браузеру, который хранит их в специально отведенном месте — как мы, бывает, кладем в карман фирменные леденцы, взятые на ресепшне какой-нибудь респектабельной фирмы, и забываем про них. Но если кто-то не в меру любопытный заглянет в ваш карман, он сразу поймет, где вы были. Куки — это отметка, свидетельствующая, что вы были на данном сайте.

Вот что про куки говорит Google:

> *Файл cookie — это небольшой фрагмент текста, передаваемый в браузер с сайта, который вы посетили. Он помогает сайту запомнить информацию о вас, например, то, на каком языке вы предпочитаете его просматривать. Это будет полезно при следующем посещении этого же сайта. Благодаря файлам cookie просмотр сайтов становится значительно более удобным.*
>
> *Файлы cookie применяются в различных целях. Например, они позволяют сохранять настройки рекламных предпочтений и безопасного поиска, подбирать интересующие пользователей объявления и подсчитывать количество посещений страницы. Также они необходимы при регистрации в сервисах Google и обеспечении безопасности личных данных.*

1 *Куки (англ. cookie, буквально — печенье).*

Почему же их так боятся? Вроде же отличная вещь, придуманная для нашей же безопасности!

Не совсем так. На заре интернета браузеры были программами для просмотра веб-сайтов и не умели ничего больше. У самого сайта технически не было возможности идентифицировать посетителя, если тот не представится, то есть не введет имя и пароль (а если сайт не подразумевал регистрацию, то вообще никак). Как если бы вы приходили в свое любимое кафе, а официант, с которым вы вчера мило болтали, смотрел бы на вас в полном изумлении, как будто у него отшибло память, пока вы не назовете свое имя. Вот тогда он сразу бы включался, вспоминал ваши привычки и предлагал вам ваш любимый столик.

Но это еще полбеды: стоило бы вам на минуту выйти, допустим, покурить (хотя в то время не возбранялось курить и в заведениях) — и по возвращении нужно было бы начинать диалог с официантом с начала, потому что добрый малый уже не помнил, за каким столиком вы сидели и что заказали. Не очень-то удобно, не правда ли?[1]

> *В общем, дело было так. Шел 1994 год. Программист компании Netscape Communications Лу Монтулли ломал голову над тем, как излечить интернет-браузер от амнезии. Его компания разрабатывала первую в мире систему электронной коммерции, и нужно было заставить браузер запоминать состояние виртуальной корзины клиента. Идея, пришедшая ему в голову, была гениально простой — пусть веб-сайт посылает на каждый клиентский компьютер небольшой файл,*

1 *Giving Web a Memory Cost Its Users Privacy. // The New York Times, 4 сентября 2001.*

в который мы запишем его уникальный номер и нужные параметры. Когда клиент вновь посетит наш сайт, мы тихонько считаем этот файл и сразу вспомним, кто он такой. Продолжая аналогию с кафе, это, как если бы забывчивый официант записывал имя гостя на карточке и незаметно подкидывал бы ему в карман, а при следующем визите так же незаметно бы доставал ее, чтобы вспомнить, как его зовут.

Но ведь шарить по чужим карманам нехорошо, скажете вы. Да, нехорошо. Однако разработчики именно так и сделали — втихаря стали записывать куки с важными данными на компьютеры клиентов. Естественно, когда после публикации в Financial Times, где говорилось об угрозах приватности, возникавшей из-за применения этой технологии, все выплыло наружу, общественность возмутилась. Вопрос даже был рассмотрен Федеральной комиссией по торговле США в двух слушаниях — в 1996 и 1997 годах. Но механизм оказался настолько удобным для рекламщиков и продавцов (и спецслужб), что дело в итоге замяли, а печеньки-куки распространились повсеместно. Сегодня их использует почти каждый из посещенных вами сайтов. Найдите в своем браузере список сохраненных куки и ужаснитесь, как их много — в том числе от сайтов, о существовании которых вы даже не знали.

Механизм оказался настолько удобным для рекламщиков, продавцов и спецслужб, что дело замяли, а печеньки-куки распространились повсеместно.

Нет, ну а что вы хотели от 24-летнего программиста? Ему сказали решить задачу, он решил. Ему же не поручали думать о безопасности и анонимности пользователей. «Это вроде работает, но определенно придумано за одну ночь», — так отзывались о первой

реализации cookie специалисты. Конечно, потом технологию доработали, самые острые проблемы с безопасностью удалось решить, но все равно «печеньки», на скорую руку придуманные Лу Монтулли, остаются одной из основных угроз анонимности пользователей интернета.

Чем же они так опасны?

> *Есть два связанных с куки неприятных момента. Во-первых, с их помощью можно отслеживать пользователей — этим пользуются как продавцы, так и спецслужбы. Во-вторых, куки можно похитить и добыть таким образом конфиденциальную информацию о вас — этим промышляют хакеры.*

Давайте сначала разберемся с хакерами: где и как они могут украсть наши печеньки? Вот вы сидите в своем любимом кафе (не в нашем гипотетическом кафе с беспамятными официантами, а в настоящем) и подключаетесь по wi-fi к интернету. О'кей, раз закон требует, то регистрируетесь — сообщаете свой телефон, вам приходит SMS, вы вводите код в нужное поле и выходите на цифровой простор. Вы замечали, что иногда сайт провайдера спрашивает, сколько вас помнить — неделю, месяц, квартал? Вот это как раз про куки.

Условно говоря, кафе выписывает вам читательский билет со сроком действия 7, 30 или 90 дней. Когда придете в следующий раз в течение этого периода, вас пустят без регистрации, а по истечении указанного времени куки автоматически удалится. А что будет, если ваши куки достанутся жулику? Правильно, он сможет подключаться к этому wi-fi вместо вас. (На самом деле все сложнее, но в общих чертах примерно так). Поэтому у жуликов есть мотивация охотиться за куки.

Способов украсть куки множество. Вот, например: берете wi-fi-роутер, называете свою сеть так, чтобы в имени были слова «WIFI_FREE», садитесь в людном месте и ловите «рыбку».

Все любят «халявный» wi-fi, поэтому люди сами принесут вам свои куки на блюдечке с голубой каемочкой, даже уговаривать никого не надо. А в них часто — логины и пароли. (Вы все еще пользуетесь публичными wi-fi без VPN? Ну-ну...). Есть и специальные программы-снифферы для перехвата куки — они могут встретиться не только в публичных wi-fi-сетях (так что VPN всегда полезен). И это далеко не все варианты.

К счастью, крупные интернет-сервисы — Google, Facebook, Яндекс, ВКонтакте, Mail.ru и другие — используют сегодня шифрованные куки. Но в мире по-прежнему полно программистов, которым нужно сделать что-то по-быстрому. Их подгоняют менеджеры проектов, на которых покрикивают основатели стартапов, опасающиеся гнева инвесторов за бездарно потраченные деньги... Скорость выхода на рынок все еще важнее безопасности. А сделанное однажды кое-как, но работающее решение, имеет все шансы просуществовать очень долго. За это время разработчики станут миллионерами, как мистер Монтулли, а проблемы безопасности будет решать кто-то другой, если, конечно, уязвимость будет обнаружена.

Сделанное кое-как, но работающее решение имеет все шансы просуществовать очень долго.

Зачем хакерам ваши куки? Чаще всего, чтобы угонять аккаунты соцсетей, мессенджеров, игровые аккаунты и другие цифровые активы. Или войти под вашими учетными данными в ту же wi-fi-сеть

и обстряпать свои черные делишки. А искать по IP потом будут вас. Натворить они могут что угодно, фантазия у них богатая. Ограбить банк или взломать государственный сайт, например. В общем, лучше не давать им такого шанса.

Для этого нужно усвоить следующие правила:

- При пользовании чужими компьютерами или телефонами всегда включайте в браузере режим «Инкогнито». По окончании работы обязательно закрывайте все сессии, все открытые вами окна и удаляйте куки;

- При пользовании публичными сетями обязательно включайте VPN. Если нет такой возможности, не посещайте сайты, требующие ввода конфиденциальных данных;

- Включите двухфакторную авторизацию на всех важных сервисах (соцсети, почта, мессенджеры, облачные хранилища, платежные системы и т.д.).

Спасет ли двухфакторная авторизация при краже куки? Абсолютной гарантии нет, потому что есть вероятность подделки вашей SIM-карты для перехвата SMS или хищения пароля от почты, но в целом эта мера значительно снижает риски. (Подробнее о двухфакторной авторизации см. главу про пароли).

Помните, что куки задумывалась как полезная технология, призванная сделать вашу жизнь более удобной. Поэтому не надо объявлять «печенькам» тотальную войну — многие из них честно несут свою службу. Без куки большинство сайтов не смогут функционировать нормально, а ваш браузер снова станет очень забы-

вчивым. Проблема не в технологии, а в том, что есть люди, скажем так, с очень размытыми этическими принципами, которые используют куки в своих целях.

«Он и меня посчитал!» Как за нами следят с помощью куки

Наиболее беспардонно используют куки для слежения за пользователями компании, занимающиеся интернет-рекламой. Это стало возможным благодаря так называемым «сторонним куки». Если вы уже посмотрели список куки в своем браузере, то наверняка заметили, что там полно «печенек» от сайтов, которые вы никогда не посещали и даже не знали об их существовании. Откуда они все взялись?

А это и есть сторонние куки — ваш браузер получает их, когда открывает страницу, где, кроме основного контента, показываются рекламные баннеры, блоки новостей, прикольные картинки и видео, прогноз погоды, курсы валют, турнирные таблицы, гороскопы, программы ТВ и тому подобное. Такая веб-страница представляет собой коллаж фрагментов с разных сайтов — вот они-то и присылают сторонние куки. Вам даже не надо кликать на баннер — достаточно того, что он отобразился на экране, это уже засчитывается за посещение его родного сайта, и его куки остаются на вашем устройстве.

> *Итак, если веб-сайт A содержит рекламное объявление, которое обслуживается веб-сайтом B, веб-сайт B может установить cookie в вашем браузере.*

Вообще-то изобретатель технологии такого не планировал, это получилось по недосмотру, и он потом это признал. В то время веб-страницы чаще всего были целыми, взятыми с одного сайта, поэтому никто и не думал, что сторонние куки могут превратиться в инструмент отслеживания пользователей. А когда заметили, то было уже поздно, — крупные рекламные сети начали активно эксплуатировать этот изъян конструкции. В первых рядах была компания Double Click, которая давно стала частью Google — куки с ее именем наверняка есть и на вашем компьютере.

Козленок из известного мультфильма тоже всех считал — как и продавцы интернет-рекламы.

> *Помните, гуляя по лесу, он начинает присваивать номера всем, кого встречает по пути: «...один — это я, два — это Теленок, три — это Корова. Один, два, три!», на что посчитанные неизменно обижаются, жалуются друг другу и хотят наказать Козленка за самоуправство. Обидно им просто потому, что какой-то Козленок без разрешения и объяснений произвел с ними непонятную процедуру, поставив их перед фактом.*
>
> *Компания недовольных растет, и вот уже все они дружно бегут за Козленком, чтобы его побить (или вразумить на тему недопустимости посягательств на персональные данные граждан).*

Кстати, если вы не знали: ситуация, показанная в мультфильме, совсем не про обучение устному счету. Она связана с психологическим феноменом оценивания, стрессом, который вызывает у индивида осознание ситуации, что он стал объектом чьей-то оценки. Ряд граждан, например, испытывают чувства, схожие с пережива-

ниями героев «Козленка...» во время переписи населения. Примерно также дело обстоит и с озабоченностью людей тем, что их действия в интернете отслеживаются, да еще неизвестно кем и с какой целью. Конечно, из-под такого контроля хочется выйти.

Чтобы уменьшить внимание к своей персоне, включите в браузере блокировку сторонних cookie, выполнив следующие действия:

- **в FireFox**
  Сервис> Параметры> Конфиденциальность. Снимите флажок «Принимать сторонние cookie»;

- **в Chrome**
  Настройки> Расширенные настройки> Конфиденциальность> Настройки контента. Установите флажок «Блокировать сторонние файлы cookie»;

- **в Internet Explorer 11**
  Сервис> Свойства браузера> Конфиденциальность> Дополнительно. Выберите «Блокировать» в разделе «Сторонние файлы cookie».

Вы спросите: а как именно с помощью куки за нами следят? Мы же не логинимся на этих рекламных сайтах, значит, наши имена им неизвестны. Но дело в том, что им и не нужно знать ваше имя, чтобы попытаться вам что-нибудь продать. Им достаточно однажды дать вашему браузеру уникальный номер, чтобы потом видеть, на сайты какой тематики вы ходите и какие страницы просматриваете. При этом рекламщики уверяют, что все это делается для вашего же блага — чтобы показывать вам только рекламу, отвечающую вашим интересам. Еще это помогает им контролировать показы рекламы — чтобы считать,

сколько и кому баннеров продемонстрировали, и как клиенты на это реагировали, с каких сайтов пришли реальные покупатели, и делать прочую аналитику.

> *Можно было бы предположить, что раз ваше имя им неизвестно, то и анонимность вашу куки не нарушают. Но это, увы, не так. Достаточно вам один раз зайти на сайт, где требуется регистрация, как по номеру браузера с вашим именем свяжут все посещенные вами страницы.*

То есть рекламная компания может собрать на пользователя практически полное досье, а уж что с ним потом делать, они решат. Например, продать банкам, которым очень пригодится информация о том, что потенциальный заемщик тщательно изучал сайты по теме «как взять кредит и не платить» — почти наверняка такому клиенту откажут. (Хотя вполне может быть, что это всего-навсего журналист отрабатывал задание редакции, вовсе не собираясь становиться злостным неплательщиком). Или наоборот: тому, кто активно смотрит сайты застройщиков, можно попробовать продать ипотеку. Вариантов использования информации о вас масса.

Спецслужбы тоже не гнушаются использовать куки как средство негласного наблюдения за пользователями — потому что это просто и удобно.

Спецслужбы тоже не гнушаются использовать куки как средство негласного наблюдения за пользователями — потому что это просто и удобно. Показал один раз человеку картинку и дальше можешь видеть все его шаги. Да, это незаконно, но когда и где это останавливало спецслужбы?

Правительство Соединенных Штатов приняло строгие законы в отношении куки в 2000 году после того, как выяснилось, что Агентство по борьбе с наркотиками США использовало куки для отслеживания пользователей, просмотревших их антинаркотическую рекламу в сети.

Тем не менее, в 2002 году стало известно, что ЦРУ устанавливает на компьютеры постоянные куки со сроком хранения до 2010 года. Когда ЦРУ было уведомлено о неправомерности подобного использования куки, Управление заявило, что это было непреднамеренно, и прекратило их установку.

А в 2005 году обнаружили, что Агентство национальной безопасности оставляло пару постоянных куки после обновления программного обеспечения. После этого сообщения Агентство немедленно отключило куки.

Полагать, что на этом история закончилась, и что спецслужбы других стран не занимаются тем же, было бы, пожалуй, наивно.

Когда вы удаляете куки, где-то плачет рекламщик

«У куки есть один большой недостаток — его можно очистить. Любой, даже технически неподкованный пользователь знает, как очищать куки. Он нажимает «Настройки», заходит и очищает. Все, пользователь опять становится для вас анонимным, вы не знаете, кто он такой», — жалуется на жизнь один из представителей рекламной индустрии.

Что произойдет при удалении куки из браузера? Да ничего страшного. Можно сказать, что у браузера просто будет стерта память, в которой он хранил ваши действия при посещении сайтов. (Обычно говорят, что браузер забудет все сохраненные пароли, и придется везде заново логиниться, но это не так. Пароли хранятся во встроенном менеджере паролей, а не в куки).

> *Совершенно точно нужно удалять куки, если вы работали за чужим компьютером, или если компьютером пользуются несколько человек под одной учетной записью. (Так часто бывает с домашними компьютерами).*

Если вы еще сомневаетесь, стоит ли это делать, то давайте взглянем на цифры. По данным сайта Cookiepedia (**https://cookiepedia.co.uk/**), в базе данных которого собрана информация более чем о 10 миллионах куки, по своему назначению они распределяются следующим образом:

- 1% — строго необходимые, без которых работа сайта будет невозможна;

- 5% — используемые для анализа производительности, который включает в себя подсчет посещений страниц и скорости их загрузки, времени задержки, показателей отказов, и технологий, используемых для доступа к сайту;

- 3% — функциональные, позволяющие веб-сайту запоминать ваш выбор (например, имя пользователя, язык или регион, в котором вы находитесь) и предоставлять расширенные, более персонализированные функции;

- 58% — рекламные (это почти всегда будут сторонние куки);
- 32% — неизвестного назначения.

Статистика недвусмысленно намекает, что на самом деле куки больше нужны рекламщикам, чем пользователям. Так что периодическая их чистка должна стать обязательным элементом вашей цифровой гигиены.

Если у вас установлено несколько браузеров, операцию придется повторить в каждом из них. Не забудьте и про телефон: там тоже есть браузер (возможно, и не один), значит, есть и куки. Разумеется, на детских устройствах чистка также обязательна.

Если у вас установлено несколько браузеров, операцию придется повторить в каждом из них.

Но не спешите радоваться, что вам удалось уйти из-под колпака мировой индустрии интернет-рекламы. Распробовав печеньки, они вошли во вкус и продолжают изобретать все новые методы трекинга пользователей. Они искренне не понимают, зачем людям анонимность, и досадуют, что пользователи становятся умнее и учатся использовать различные средства, препятствующие отслеживанию. Поэтому они постоянно совершенствуют куки.

> *Так появились evercookie — трудноудаляемые куки, которые прописывают информацию о себе в 13 различных местах системы, поэтому их очень трудно вычистить. Есть PNG Cookies, которые притворяются обычной картинкой и пытаются навечно закрепиться в кэше браузера. Есть Flash Cookies, бывшие до недавнего времени практически неудаляемыми.*

Наконец, это супер-куки, которые привязываются к домену верхнего уровня типа .com, а не к конкретному сайту; они являются потенциальной проблемой безопасности и поэтому часто блокируются веб-браузерами. Их иногда называют «зомби-куки», потому что они умеют «оживать» после того, как пользователь их «убил». Сколько бы вы их не удаляли, они появляются снова — поможет только осиновый кол.

Надо сказать, что разработчики браузеров всерьез озаботились этой проблемой и начали предпринимать активные шаги по наведению порядка. Осведомленные источники говорят, что в Google идут внутренние дебаты, которые могут привести к ограничениям использования технологий слежения и таргетинга (целевой рекламы). Поскольку Google владеет самой мощной рекламной и вездесущей платформой Google Marketing Platform и самым популярным браузером Chrome, занимающем 63% мирового рынка, то решение будет трудным.

Apple представила умную технологию защиты от отслеживания Intelligent Tracking Protection (ITP) в браузере Safari еще в 2017 году, а в начале 2019 выпустила обновление, устанавливающее весьма жесткие правила по использованию куки. Теперь «срок годности печенья» от основного сайта сокращен до 7 дней, а сторонние куки блокируются сразу. Стоит также отметить, что в ITP 2.1 удалена поддержка параметра «Не отслеживать» (DNT — Do Not Track), поскольку разработчики рекламных технологий все равно полностью игнорировали этот параметр, даже если пользователи включали его.

Но ведь это же фактически «пчелы против меда», скажете вы. Неужели у кого-то проснулась совесть?

Едва ли. Скорее дело в давлении общественности, выразившееся в принятии новых законов по защите прав пользователей. Люди возмутились тотальной слежкой со стороны интернет-гигантов, и теперь технологические компании вынуждены принимать меры, чтобы не попасть под нешуточные штрафы.

В мае 2018 года в Евросоюзе начал действовать Общий регламент по защите данных (GDPR[1]), обязательный для всех сайтов, посещаемых из Евросоюза, и приравнивающий большую часть куки к персональным данным. В изначальном проекте предполагалось, что настройки браузера могут признаваться достаточным выражением согласия пользователя на установку куки, а согласно окончательной версии, нужно было всего лишь уведомление об установке куки, чтобы получить «информированное согласие» пользователя.

Ассоциация потребителей Нидерландов решила проверить, как исполняется новый европейский закон. Оказалось, что 49% веб-сайтов (74 из 150 исследованных) размещают маркетинговые и/или рекламные файлы cookie непосредственно при открытии сайта, без вашего разрешения. Да, они обычно показывают посетителям окно куки с кнопкой OK для получения вашего согласия, но по факту они уже их разместили. Эта практика была незаконной в соответствии с предыдущим законом о cookie-файлах и остается таковой с GDPR.

Голландские исследователи рекомендуют пользователям не рассчитывать на соблюдение закона владельцами сайтов и позаботиться о конфиденциальности своих данных само-

1 *General Data Protection Regulation, подробнее см.* ***https://gdpr.eu/***

стоятельно. В частности, чтобы воспрепятствовать установке куки, они советуют устанавливать блокировщики рекламы.

В 2020 году вступил в силу Калифорнийский закон о защите персональных данных интернет-пользователей (California Consumer Privacy Act, CCPA), который называют самым жестким из всех подобных. Поскольку именно в Калифорнии расположены штаб-квартиры многих ведущих ИТ-компаний (Facebook, Google, Apple, Netflix и др.), закон может оказать очень сильное влияние на всю интернет-индустрию.

Внимание! Даже если вы будете использовать прокси-анонимайзер или VPN, через куки-файлы информация о вас может быть передана на сервер, к которому вы будете обращаться. Поэтому перед настройкой браузера на работу через прокси или до смены используемого прокси-сервера необходимо обязательно выполнить их очистку.

При посещении нового сайта, который следует политике GDPR и просит вашего информированного согласия на установку cookies, прежде чем согласиться, посмотрите список того, что они собираются установить. Обычно для этого есть специальная кнопка во всплывающем окне. Выбирайте только необходимые cookies, а от всех прочих можно отказаться.

С глаз долой, из браузера вон, или Блокировка рекламы

Обилие рекламы обычно раздражает людей. Она отвлекает внимание, занимает место на экране. Она маскируется под обычный

контент: броские заголовки якобы новостей на самом деле ведут на рекламные «помойки», где, кроме кричащих баннеров, ничего нет. Конечно, нормальному человеку хочется от всего этого избавиться, «развидеть», как говорят в интернете, и уж тем более убрать это подальше от детских глаз, ибо неизвестно, что в следующую секунду всплывет.

> *К сожалению, сегодня экономика мирового интернета устроена так, что провайдеры не могут отказаться от рекламы на сайтах или хотя бы существенно уменьшить ее объем. Просмотр рекламы — это часть сделки, которую мы заключаем.*

В обмен нам дают бесплатный поиск, почту, мессенджеры и соцсети, бездонное количество видео и музыки (это не про пиратов, это про легальный контент), облачные хранилища для наших фото и многое другое. Чтобы все это работало, кто-то должен заплатить. Весьма существенную часть бюджета провайдеров бесплатных сервисов, как ни крути, составляет реклама.

И это была бы честная сделка, если бы наше участие ограничивалось только просмотром. К тому же, иногда реклама и полезна. Но рекламщики сами первыми нарушили негласное соглашение, унаследованное от бумажной прессы и ТВ, когда они показывают, мы смотрим и ничего больше. Рекламные компании научились собирать данные пользователей с помощью куки и других методов, и стали торговать ими. А такого уговора не было. Поэтому пользователи стали защищаться от чрезмерного вторжения в свою частную жизнь.

Что есть лучшая защита от назойливого продавца? Полная анонимность.

Что есть лучшая защита от назойливого продавца? Полная анонимность. Если продавец не знает, сколько денег у вас в кармане, он и напрягаться не станет. Он лучше подождет более платежеспособного клиента, поэтому главная задача правильного блокировщика рекламы не в том, чтобы скрыть от ваших глаз раздражающие картинки, а в том, чтобы не допустить в ваш браузер куки от рекламных сайтов и препятствовать другим техникам сбора личных данных.

Самые первые блокировщики имели в основе другой принцип: они скрывали от глаз пользователя рекламные элементы, которые уже были загружены на страницу, современные же устроены гораздо сложнее. Например, они не блокируют все подряд всплывающие окна, а умеют определять, когда такое окно содержит рекламу, а когда оно необходимо для работы сайта. Как водится, если есть спрос, есть и предложение — существует большое количество блокировщиков рекламы, различающихся по возможностям настройки, платных и бесплатных, и у каждого есть свои плюсы и минусы, так что очень сложно дать на их счет однозначные рекомендации.

Современные блокировщики умеют определять, когда всплывающее окно содержит рекламу, а когда оно необходимо для работы сайта.

При поиске лучших бесплатных блокировщиков рекламы можно ориентироваться на следующие критерии:

- доступен бесплатно, без платного доступа к важным функциям;
- имеет хорошие пользовательские рейтинги;

- не требуется учетная запись для использования;
- недавно обновлен (за последние 12 месяцев);
- легко доступен в качестве плагина как минимум для одного браузера или операционной системы;
- блокирует «показы рекламы» (всплывающие окна, баннеры, видео, статические изображения, обои, текстовые объявления);
- блокирует потоковые видеообъявления (например, на YouTube).

Единого общепризнанного рейтинга блокировщиков рекламы нет, придется побыть немного самому себе аналитиком и выбрать подходящее решение, а может быть, и несколько — для разных браузеров и разных задач. Только обязательно загляните в настройки своего блокировщика, потому что далеко не всегда все нужное по умолчанию включено, придется поработать руками.

Относительно недавно в эту игру включились и сами разработчики популярных браузеров (Chrome, Firefox, Opera, Microsoft Edge) — сегодня их актуальные версии обзавелись встроенными функциями блокировки рекламы. Они тоже отличаются по своим качествам, и придется сравнивать их со специализированными решениями, которые пока сдаваться не планируют.

Эксперты высказывают сомнения, что встроенные блокировщики будут последовательно стоять на стороне пользователя. Например, говорят, что браузер Chrome, в котором эта функция

стала доступна во всех странах только с июля 2019 года, борется лишь с той рекламой, которая не соответствует стандартам, принятым Coalition for Better Ads. Фактически это означает, что встроенный блокировщик борется только с наиболее агрессивной и навязчивой рекламой, которая нарушает следующие правила:

- реклама со звуком и видеоролики, которые начинают проигрываться автоматически;
- всплывающие сообщения, закрывающие большую часть экрана;
- так называемая prestitial-реклама. Этим термином обозначают рекламу, которая имеет собственную страницу и загружается перед целевым URL, а затем пользователю демонстрируют таймер, отсчитывающий время до закрытия навязчивого объявления;
- крупные баннеры, «прилепленные» поверх окна и занимающие до 30% экрана;
- для мобильных версий сайтов не поощряется «мигающая» реклама, цвета или фон которой быстро и агрессивно меняются, пытаясь привлечь внимание и тем самым затрудняя чтение.

Тем не менее, базовый уровень защиты от рекламы и отслеживания браузеры сегодня обеспечивают. Не забудьте только их обновить и включить функцию блокировки.

«Тренд на анонимность — не новое явление для рынка, но в последнее время оно получило наибольший размах и рискует сохраниться», — печалятся мастера навязчивой онлайн-рекламы,

но сдаваться не собираются. Если нельзя будет использовать куки, то у них наготове уже есть технология следующего поколения, против которой известные технические способы защиты пока бессильны, а законодательные ограничения еще не придуманы.

Когда быть уникальным плохо: цифровой отпечаток браузера

Психологи любят говорить, что каждый человек — уникальная личность, и, как снежинки не похожи одна на другую, так и люди наделены уникальными внешними данными и обладают уникальным внутренним миром. Педагоги твердят, что каждый ребенок уникален, и к каждому нужен индивидуальный подход. Инвесторы ищут уникальные стартапы, способные изменить мир. Сколько раз я повторил слово «уникальный»? Все просто одержимы уникальностью!

Абсолютно одинаковых браузеров не существует. Точнее, они одинаковы, пока ими не начали пользоваться.

Оказалось, что браузеры тоже подвержены этому глобальному тренду — абсолютно одинаковых практически не существует. Точнее говоря, браузеры одинаковы, пока ими не начали пользоваться. Как только браузер устанавливается на конкретный компьютер, он тут же получает целый букет уникальных параметров — тип и версия операционной системы, модель устройства, язык, часовой пояс, характеристики экрана, комплект шрифтов, установленные расширения и разнообразные настройки, о которых вы, скорее всего, и не помните.

Это может показаться удивительным, но, тем не менее, факт: по комбинации нескольких параметров можно идентифицировать конкретный браузер с точностью, превышающей 99%.

На этом свойстве основана технология Browser Fingerprint[1] — «отпечатков пальцев» браузера, получившая широкое распространение после начала гонений на cookies.

Тем, кто не слишком любит математику, сейчас будет немного больно, но ничего не поделаешь — в основе метода браузерной дактилоскопии лежит математическая теория. Вы можете пропустить это объяснение и просто поверить на слово: очень вероятно, что ваш браузер уникален, что позволяет вас идентифицировать вне зависимости от наличия cookies и VPN.

Принцип метода браузерной дактилоскопии нам объяснит Питер Экерсли (Peter Eckersley), директор по исследованиям в Electronic Frontier Foundation (**eff.org**).

«Давайте начнем не с браузеров, а с людей, так будет понятнее. Представьте, что вам нужно установить личность человека, а единственное, что вы о нем знаете, это почтовый индекс, дата рождения или пол. Очевидно, что каждого из этих признаков, взятых по отдельности, будет недостаточно для идентификации.

---

1 *Фингерпринт или отпечаток компьютера (браузера) — информация, собранная об удаленном устройстве для дальнейшей идентификации. Отпечатки могут быть использованы полностью или частично для идентификации, даже когда cookie выключены (Википедия).*

Существует математическая величина, которая позволяет нам измерить, насколько данный критерий близок к полному раскрытию чьей-либо личности. Эта величина называется ***энтропией****, и ее часто измеряют в битах. Можно сказать, что энтропия — это обобщение числа различных возможностей для случайной величины: если есть две возможности, есть 1 бит энтропии; если есть четыре возможности, есть 2 бита энтропии и т.д. Добавление еще одного бита энтропии удваивает число возможностей.*

Поскольку на планете насчитывается около 7 миллиардов человек, личность случайного, неизвестного человека определяется чуть менее 33 битами энтропии (233 примерно равно 8 миллиардам). Когда мы узнаем новый факт о человеке, этот факт уменьшает энтропию его личности на определенную величину. Есть формула, чтобы сказать, на сколько:

$\Delta S = -\log_2 Pr(X = x)$,

где ΔS — уменьшение энтропии, измеренное в битах, а Pr (X = x) — вероятность того, что этот факт будет правдой для случайного человека. Легко догадаться, что знание пола сокращает энтропию на 1 бит, если считать, что мужчин и женщин на планете поровну. А день рождения? Применим нашу формулу и получим:

$\Delta S = -\log_2 Pr(\text{День рождения}) = -\log_2 (1/365) = 8{,}51$ *бит информации.*

То есть чем выше значение энтропии, тем более данный признак ценен для раскрытия личности. Для повышения точности при расчете вероятности надо учитывать реальную статистику.

Как известно, рождаемость неравномерна — заметно больше детей появляется на свет в сентябре, в аккурат через девять месяцев после новогодних праздников. И очень редко встречается день рождения 1 и 2 января — просто потому, что это выходной, и часто родившихся в праздники младенцев записывают следующим днем. Соответственно, сокращение энтропии нужно рассчитывать для каждой конкретной даты. Аналогично и с местом жительства: знание того, что человек живет в Москве, сокращает энтропию на 9,3 бита, а если он живет в Беверли Хиллз, то на 18,21 бита.

Таким образом, комбинация нескольких вполне обезличенных признаков может абсолютно точно указать на единственного человека. Например, если мы узнаем, что в небольшом поселке у кого-то день рождения 29 февраля (самая редкая дата), то, вполне возможно, он будет единственным. А если среди членов экипажа МКС есть только одна женщина, то этот признак становится на 100% идентифицирующим[1].

Теперь вернемся к нашим браузерам. Предположим, что есть один миллион пользователей. У 60% из них установлен Chrome, у 40% — Firefox. (Это теоретическое допущение довольно близко к правде, доля остальных браузеров невелика). То есть мы разделили нашу выборку на две группы. Затем давайте посмотрим, какая версия браузера стоит у каждого. Для простоты будем считать, что есть три версии Firefox — тогда вторая группа делится на три подгруппы по, скажем, 15%, 15% и 10%. Эти группы все еще слишком большие, чтобы идентифицировать конкретного пользователя. Дальше посмотрим, какой у них

1 *Peter Eckersley. A Primer on Information Theory and Privacy. // EFF.ogg, 26 января 2010.*

размер экрана, часовой пояс, язык и так далее — наша выборка будет дробиться на все более мелкие группы.

*В исследовании, организованном Electronic Frontier Foundation в 2010 году, на специально созданном сайте Panopticlick (**https://panopticlick.eff.org**) было собрано более 470 тысяч цифровых отпечатков браузеров. Когда их проанализировали, то обнаружили, что в распределении отпечатков содержится, по крайней мере, 18,1 бит энтропии, а это означает, что для любого взятого наугад браузера вероятность того, что он совпадет с каким-то другим, равна 1/286 777. То есть 83,6% имели уникальный отпечаток. Среди браузеров с поддержкой Flash или Java ситуация даже хуже: 94,2% были уникальными[1]. (Вы и сейчас можете зайти на этот сайт и проверить свой браузер на уникальность).*

Однако, 94,2% — это еще не 100%. Такая точность недостаточна, чтобы однозначно утверждать, что перед нами тот самый пользователь, который посещал сайт пару дней назад. Это как если бы вы пытались кому-то позвонить, зная только код оператора и пытаясь набрать остальные цифры наугад. Для целей рекламы такая погрешность в принципе приемлема — подумаешь, миллионом показов больше или меньше. Казалось бы, беспокоиться не о чем, и ваша анонимность будет сохранена.

Как бы не так! Беда пришла, откуда не ждали. Вы же хотели, чтобы картинки и трехмерные изображения в браузере отрисовывались быстро и в хорошем качестве? Хотели наслаждаться дизайнерской графикой, визуальными эффектами и играть в динамичные

1 *Peter Eckersley. «How Unique Is Your Web Browser?» // Panopticlick.eff.org 2010* ***https://panopticlick.eff.org/static/browser-uniqueness.pdf***

игры, да? Для этого программисты придумали технологии WebGL и Canvas. Но чтобы порадовать вас сочной картинкой и мгновенной сменой кадров, им пришлось обращаться к низкоуровневым функциям вашего ноутбука или телефона. И тут вскрылась любопытная вещь: из-за особенностей оборудования отрисовка одних и тех же элементов происходит на разных моделях чуть-чуть по-разному — на глаз незаметно, но если взять битовый образ, то отличия легко зафиксировать. Чем не преминули воспользоваться разработчики: они тут же добавили анализ Canvas и WebGL в отпечаток браузера, и точность сразу повысилась до 99%.

В 2013 году проект исследователей INRIA (Французский национальный исследовательский институт цифровых наук) получил в целом аналогичные результаты на еще большей выборке. Ознакомиться с результатами исследования и проверить свою уникальность можно на сайте с говорящим названием «Am I Unique?» — «Уникален ли я?» (**https://amiunique.org/**). В отличие от предыдущего исследования EFF, во французском проекте задействованы новейшие технологии определения отпечатка по особенностям графики, и данные постоянно обновляются.

В отличие от отпечатка пальца, который неизменен всю жизнь, отпечаток браузера есть вещь изменчивая.

Временной фактор вообще очень важен — выходят обновления браузеров и операционных систем, люди меняют телефоны на новые модели, изменяется начинка компьютеров и прочее. То есть в отличие от обычного нашего отпечатка пальца, который неизменен всю жизнь, отпечаток браузера есть вещь изменчивая по своей природе. Как же в таком случае с его помощью можно кого-то идентифицировать? Очень просто: вы же узнаете вашего приятеля, если он отпустил бороду, не так ли? Параме-

тры браузера не меняются все сразу, а к небольшим изменениям можно адаптироваться — разработчики научились их учитывать. Это значит, что если изменения будут происходить постепенно, как это бывает в реальной жизни, вас все равно отследят.

Вы, конечно, можете попытаться поставить новый браузер и работать через него. Но и на эту хитрость уже есть ответ. Программисты подумали хорошенько и решили, что собственно браузер не так уж и необходим для отслеживания вас в интернете. Для этого достаточно знания параметров операционной системы и оборудования — прежде всего процессора и графической карты. Так в 2017 году появилась кросс-браузерная дактилоскопия (Cross-Browser Fingerprinting — CBF), и техники CBF позволяют точно идентифицировать 99,24% всех компьютеров и смартфонов. Исследователи проводили тесты с использованием браузеров Chrome, Firefox, Edge, IE, Opera, Safari, Maxthon, UC Browser и Coconut[1].

Сам браузер не так уж необходим для отслеживания вас в интернете — достаточно знать параметры операционной системы и оборудования.

Наверное, здесь стоит остановиться и сказать о полезных применениях технологии браузерной дактилоскопии, прежде чем перейти к обсуждению методов защиты от нее. Ведь не только же ради показов рекламы все делается!

Действительно, отпечатки браузера широко используются в системах обнаружения мошенничества. Всякий раз, когда вы захо-

1 *(Cross-)Browser Fingerprinting via OS and Hardware Level Features. // Yinzhicao.org, 2017. В более простом изложении — «Фингерпринтинг конкретного ПК с точностью 99,24%: не спасает даже смена браузера» // **Habr.com**, 14 января 2017.*

дите в соцсеть с нового устройства, срабатывает двухфакторная аутентификация, а на почту приходит письмо с просьбой подтвердить, что это были именно вы. Это делается как раз на основе определения браузера. Аналогичным образом поступают банки и интернет-магазины (те, которые заботятся о безопасности). Еще эта технология применяется в игровой индустрии, чтобы обнаруживать попытки игроков «хакнуть» игру, в СМИ — чтобы контролировать пользование платными подписками, а также при продаже билетов, бронировании гостиниц и других операциях пользователя, требующих особого контроля.

> *Зачем все это сайту, который вы хотите просто посмотреть? Затем, чтобы сформировать страницу, которая будет правильно отображаться на вашем устройстве, будь то телефон или компьютер. То есть чтобы лучше вас обслужить.*

Конечно, у этой технологии есть и темная сторона. В течение нескольких лет цифровые отпечатки браузеров были подарком для поставщиков рекламы, которые отслеживали посетителей своих сайтов независимо от того, установлен следящий cookie-файл или нет. Пользуются браузерными отпечатками и вирусописатели. В 2016 году в ходе кампании по распространению вредоносного ПО для Mac OS у исследователей возникло подозрение, что злоумышленники идентифицируют цели с помощью цифровых отпечатков браузера[1].

Поэтому желание пользователей избежать слежки, осуществляемой с помощью этого механизма, вполне объяснимо. Но тут нас

---

1 *Firefox перестанет оставлять свои отпечатки на сайтах. // **TreatPost.ru**, 2 ноября 2017. Scareware Campaign Targets Mac OS X Machines. // **TreatPost.com**, 5 февраля 2016.*

поджидает парадокс, на который обратил внимание еще Петер Экерсли в статье 2010 года: чем больше вы стараетесь защититься от снятия отпечатков браузера, тем более уникальным вы становитесь, и тем легче вас обнаружить.

Чем больше вы стараетесь защититься от снятия отпечатков браузера, тем более уникальным вы становитесь, и тем легче вас обнаружить.

Профессиональные разведчики (как, впрочем, и преступники) знают, что уникальность — худший враг анонимности. Чтобы остаться неузнанным, нужно слиться с толпой, выглядеть самым средним и заурядным представителем народных масс. Одеваться неброско, вести себя как все, и тогда, может быть, удастся уйти от слежки. Но главное в стремлении стать незаметным — не переусердствовать.

> *Основной метод маскировки заключается в придании своему отпечатку максимально средних значений. Используйте популярные браузеры с настройками по умолчанию, не меняйте шрифты и язык, не ставьте разнообразных плагинов — в общем, будьте как все.*

Отдельно надо позаботиться о параметрах, снимаемых с помощью анализа вашей графической системы, поскольку настройками изменить вы их не можете. Сразу надо сказать, что идея поставить блокировщик отпечатков Canvas так себе — наличие блокировщика делает вас похожим на человека, стоящего среди толпы в маске. Никто точно не знает, кто вы, но вы единственный, кто носит маску, так что вас могут опознать. А если таких, как вы, несколько, вас немедленно сгруппируют как «людей в масках». Даже блокировщиками рекламы пользуются всего 5-10% пользователей — на их фоне ваш блокировщик отпечатков будет выглядеть вообще экзотикой.

Есть браузерные расширения, которые умеют подменять ваш истинный отпечаток на некий фиктивный. С этим тоже надо быть осторожным — нормальный человек не будет переодеваться на ходу, а частая смена отпечатка именно так и выглядит для наблюдателя. Если вы все-таки настроены заметать следы, то можно воспользоваться расширением для браузера Canvas Defender (или аналогичным), которое вы найдете в магазине приложений.

Нормальный человек не будет переодеваться на ходу, а частая смена отпечатка именно так и выглядит для наблюдателя.

Хотя сегодняшние методы не дают надежной защиты от снятия сайтами отпечатков вашего браузера, аргумент «защита от дактилоскопии бесполезна» — пример пораженческого поведения. Сталкиваясь с наплывом плохих новостей о возможностях слежки, мы проявляем склонность к выученной беспомощности и приходим к упрощенному выводу, что конфиденциальность умирает, и мы ничего не можем с этим поделать.

Однако такая позиция не подтверждается историческими свидетельствами: вместо этого мы видим постоянный пересмотр равновесия конфиденциальности и отслеживания. И хотя нарушения, затрагивающие право на тайну частной жизни, случаются постоянно, время от времени они компенсируются юридическими, технологическими и социальными механизмами.

Отпечатки браузера сегодня остаются на переднем крае битвы за конфиденциальность. GDPR усложняет их использование, приравнивая отпечаток к персональным данным. Поставщики браузеров также стали серьезно относиться к этой практике, и вводят ограничения на ее использование.

В обоих упомянутых нами исследованиях опубликованы замечательные научные данные. Но время не стоит на месте, технологии развиваются, и старые гипотезы нужно регулярно проверять, чтобы подтвердить их или опровергнуть. Поэтому в 2018 году выпускник университета Братиславы провел новое исследование реальных возможностей идентификации по отпечатку браузера. Было собрано более 500 тысяч отпечатков, но, в отличие от прошлых исследований, 65% устройств составляли смартфоны — примерно пополам iPhone и Android.

Согласно полученным данным:

- *74% настольных устройств могут быть однозначно идентифицированы, в то время как то же самое можно сказать только о 45% мобильных пользователей;*
- *Только 33% отпечатков браузера, собранных на iPhone, были уникальными;*
- *Остальные 33% айфонов вряд ли можно отследить вообще, потому что 20 или более айфонов показывают тот же отпечаток браузера.*

Новые результаты кардинально отличаются от известных ранее — о точности свыше 99% речь не идет. То есть для гарантированной идентификации пользователя технология отпечатков браузера пока не доросла. Особенно интересно, что смартфоны Apple гораздо сильнее похожи друг на друга, чем устройства остальных типов, что является следствием высокого уровня стандартизации устройств и ограниченности модельного ряда.

В итоге можно сказать, что отпечатки браузера идеально подходят для таких случаев использования, как персонализация рекламы (где точность не является особо важной) или предотвращение банковского мошенничества (где паранойя вполне уместна)[1].

Срывание всех и всяческих масок: деанонимизация

Говоря формальным языком, деанонимизацией называется лишение человека анонимности, то есть установление связи между действиями пользователя на интернет-ресурсах и конкретной личностью. Естественно, власть всеми ветвями за деанонимизацию и достаточно продвинулась на этом пути, принимая все новые законы.

Плохо ли это? Ведь в отсутствие анонимности любого обидчика будет легко найти и выяснить отношения в офлайне, а полиция быстро вычислит и поймает любого преступника. В идеальном мире, наверное, так и было бы, но в реальном все не столь однозначно, и анонимность часто является главным залогом безопасности.

В реальном мире анонимность часто является главным залогом безопасности.

Посмотрим, какие последствия имела или могла бы иметь деанонимизация на примере трех историй. В двух из них анонимность была раскрыта, в третьей — нет.

---

1 *Peter Hraška. We've analysed 500,000 browser fingerprints. Here is what we found. // **Medium.com**, блог Slido, 7 февраля 2019.*

История первая

WikiLeaks — созданная в 2006 году международная некоммерческая организация, которая публикует утечки документов из государственных и коммерческих организаций, предоставленные анонимными источниками. До сентября 2018 года ее возглавлял австралийский интернет-активист Джулиан Ассанж. На счету организации много громких публикаций, вызвавших международные скандалы. Среди них материалы о коррупции в Кении, о содержании заключенных на американской базе в Гуантанамо, о незаконной деятельности швейцарского банка Julius Baer, секретные «библии» саентологии, список членов ультраправой Британской национальной партии и другие. Но настоящей бомбой стала публикация секретных документов Пентагона, касающихся войн в Ираке и Афганистане — в частности, видео авиаудара по Багдаду, в результате которого погибли два журналиста Reuters (пилоты по ошибке приняли их видеокамеры за оружие).

WikiLeaks провозглашала в качестве одного из своих принципов обеспечение полной анонимности для информаторов и утверждала, что сайт организации обладает пуленепробиваемой защитой, однако утечка все же произошла. Чья-то глупая ошибка — список адресов всех доноров WikiLeaks в почтовой рассылке был случайно подставлен в поле CC (копия) вместо BCC (скрытая копия). Одним из якобы доноров был Адриан Ломо, хакер, работавший на правительство США, который тоже получил полный список. И он не упустил свой шанс — вычислил информатора, который слил секретные документы, вступил с ним в личную переписку в чате и спровоцировал назвать свое имя и рассказать о том, что тот сделал. Снова социальная инженерия, ничего больше!

Информатором оказался военнослужащий армии США Брэдли Мэннинг, которого осудили на 35 лет. (Позже президент Обама его помиловал, и он вышел на свободу после 7-летнего заключения, правда, уже как Челси Мэннинг — за время пребывания в тюрьме он сменил пол).

Объем материалов, добытых Мэннингом, был огромен. Только в «Афганском архиве» было 92 тысячи документов. Конечно, общественность должна была узнать правду о войне, но многие из этих документов содержали персональные данные агентов, и после публикации архива их жизнь оказалась бы под угрозой. Несмотря на мнение своих товарищей, считавших, что документы надо обезличить, Ассанж единолично решил обнародовать весь архив как есть. «Мы не редактируем документы», — заявил он. Этот поспешный жест привел к тому, что многие из афганцев, сотрудничавших с силами антитеррористической коалиции, были казнены талибами.

Мораль этой истории:

- Будьте осторожны с электронной почтой. Довольно частая ошибка, когда секретные списки адресов случайно улетают всем;

- Будьте осторожнее с чужими тайнами. Ваши действия могут деанонимизировать других людей. Пусть это не всегда вопрос жизни и смерти, но готовы ли вы взять на себя ответственность за возможные последствия?;

- Опасайтесь социальной инженерии. В интернете этот риск выше, чем в офлайне.

История вторая

В качестве еще одного яркого примера можно привести историю с нашумевшим стартапом Find Face. Эта компания прославилась тем, что без дополнительного уведомления скачала базу фотографий всех пользователей социальной сети «ВКонтакте», что позволило ей идентифицировать буквально любого человека на улице, если в его профиле ВК есть фото подходящего качества. Сервис приобрел вирусную популярность после того, как петербургский фотограф Егор Цветков запустил свой фотопроект, в рамках которого находил в соцсетях профили встреченных им в метро людей. «Таким образом, я узнавал многое о жизни человека, не вступая в личный контакт, и мог сопоставить реальный образ с интернет-репрезентацией», — говорил фотограф. В принципе, это был безобидный арт-проект, ничего более.

Затем пользователи имиджборда «Двач» стали использовать Find Face для деанонимизации порноактрис. Этот кейс оказался потенциально куда более опасным: он вылился в травлю и шантаж девушек, которые действительно снимались, или могли оказаться просто похожими на героинь фильмов для взрослых. Пока шантажисты и хипстеры развлекались как могли, сами владельцы проекта делали деньги, занимаясь фактически шантажом — требуя 459 рублей ежемесячно за возможность удалиться из поисковой выдачи сервиса.

В сентябре 2018 года общедоступный «бесплатный» сервис Find Face был закрыт, потому что компания-собственник переключилась на обслуживание заказов крупного бизнеса и государства. Но свято место пусто не бывает: в феврале 2019 года открылся Search Face —

новый сервис для поиска людей в ВК по фото, аналогичный закрытому Find Face и запущенный неизвестными разработчиками.

Мораль этой истории:

- Технология распознавания лиц — очень опасная штука в руках безответственных людей с размытыми этическими принципами. Семь раз подумайте, прежде чем оставить где-то свое фото, кроме своей страницы в соцсети;

- И еще более основательно подумайте, прежде чем постить фото других людей без их явного согласия. Эффекты могут быть самые неожиданные.

История третья

> *Наверное, нет человека, который бы не слышал про биткоин и его загадочного создателя Сатоши Накамото. Вот уже десять лет мир будоражит криптолихорадка, а ее «виновника» никто в глаза не видел. В октябре 2008 года Накамото опубликовал статью, описывающую протокол биткоина, а 3 января 2009 года начала работать сеть, и был сгенерирован первый блок и первые 50 биткоинов.*
>
> *Все это время изобретателю криптовалюты удается сохранить анонимность, несмотря на отчаянные попытки его найти. Его ищут криптоэнтузиасты, которые хотят не иначе как лично воздать ему хвалу. Наверное, не меньше почитателей заинтересованы в деанонимизации отца-основателя биткоина и спецслужбы — старый финансовый мир чувствует в криптовалюте угрозу доллару, а вызвать на ковер в Конгресс и пропесочить как следует некого — как прикажете сражаться с пустотой?*

Последнее сообщение от Сатоши датируется 23 апреля 2011 года, оно было адресовано разработчику Майку Херну: «Я сейчас занят другими проектами. Дело остается в надежных руках, есть Гэвин [Андресен] и все остальные». Сатоши всегда выходил в интернет, используя сеть Tor и прочие средства, которые обеспечивали анонимность. В своем профиле на сайте P2P Foundation он указал, что родился в 1975 году и живет в Японии, хотя, скорее всего, это легенда, и человек, пользующийся этим псевдонимом, не японец: он пишет на английском языке как на родном.

«Охота» на Сатоши идет давно, но безуспешно. Программист из Швейцарии Штефан Томас обнаружил, что между 05:00 и 11:00 (GMT) Накамото никогда ничего не публиковал. Это касалось, в том числе, и выходных. Так Томас предположил, что Накамото проживает в Великобритании. В пользу этой версии говорили и особенности почти идеального английского языка создателя биткоина — он часто использовал слова вроде «bloody», «optimise» или «colour», что свойственно именно британцам. Другие «охотники» уверены, что это лишь маскировка. Многие вообще считают, что это не один человек, а группа людей.

За это время кого только ни подозревали в том, что он и есть создатель «битка»! Однако все «кандидаты» категорически отвергли такие предположения. В 2014 году журналисты нашли американца японского происхождения по имени Дориан Сатоши Накамото, проживающего в Калифорнии. Уже тогда ему было 64 года, и он наотрез отказывался общаться с прессой, но это снова оказался не настоящий Сатоши. Были, наоборот, самозванцы, объявлявшие себя Сатоши Накамото, однако убедить сообщество в собственной подлинности они не смогли.

В каком-то смысле исчезновение Сатоши — лучшее, что произошло с первой криптовалютой за всю ее историю, поскольку оно автоматически решило проблему возникновения культа личности.

Мораль этой истории чрезвычайно проста:

- Если очень постараться, то свою анонимность можно сохранить, несмотря на активные действия людей, желающих вас найти. Будь как Сатоши!

Анонимность — не только ваше личное дело. От вашего умения соблюдать правила безопасного поведения в интернете может зависеть безопасность других людей. Иногда сохранение инкогнито становится жизненно важным. Об этом надо помнить также, как о правилах оказания первой медицинской помощи — может быть, вам никогда не придется делать кому-то искусственное дыхание и массаж сердца, но лучше на всякий случай это уметь. Также и с анонимностью в интернете: в повседневной жизни параноиком быть ни к чему, но владеть хотя бы базовыми приемами маскировки — полезно. Или по меньшей мере знать об их существовании.

«Луковый» браузер Tor для повышения анонимности

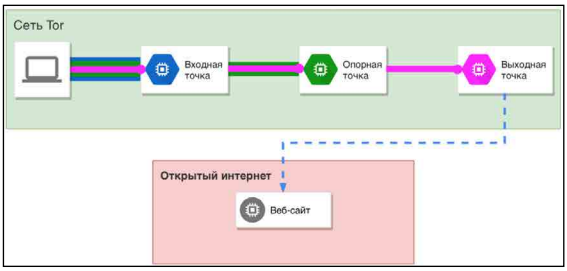
Когда речь заходит о действительно высоком уровне анонимности, то продвинутые в таких делах пользователи непременно вспоминают про браузер Tor. Его название никак не связано со скандинавским богом Тором и героем «Мстителей», не имеет оно ничего об-

щего и с геометрической фигурой в форме баранки. На самом деле это сокращение от «The Onion Router» — «луковый маршрутизатор».

Причем здесь лук, спросите вы? Притом, что кроме браузера, который видит пользователь, есть еще сеть Tor Network, состоящая из нескольких тысяч серверов, раскиданных по миру. Она, собственно, и обеспечивает анонимность — ваш Tor-браузер не напрямую выходит в интернет, а через несколько ее узлов. По умолчанию через три, но узлов может быть и больше, чтобы запутать следы.

> *Для каждой страницы, которую вы намерены посетить, случайным образом формируется своя цепь узлов, причем сами узлы об этом не знают, их адреса берутся из каталога сети. Затем клиент сети Tor (в составе вашего браузера) готовит «луковый» пакет, то есть многократно шифрует исходное сообщение таким образом, что первый узел в цепи может расшифровать только верхний слой, после чего он узнает адрес следующего узла и передает пакет ему. Тот расшифровывает второй слой, видит адрес очередного получателя и передает оставшийся пакет дальше. Каждый узел видит только своих соседей, но не знает ни исходного отправителя, ни конечного получателя, ни длины цепи. Последний узел также выполняет расшифровку и в итоге передает ваше сообщение по адресу назначения в обычный интернет.*

Если все это нарисовать, то получится похоже на луковицу: каждый узел как бы снимает один ее слой, пока последний не доберется до сердцевины. Отсюда и название. Сам же браузер Tor является просто защищенной версией Firefox. Он включает в себя многочисленные модификации конфиденциальности и безопасности, встроенные в версию по умолчанию.



Если вы сейчас подумали, не стоит ли использовать совместно VPN и Tor, то вы на правильном пути. Действительно, эти методы дополняют друг друга, и эксперты именно так рекомендуют поступать, ибо у обоих способов есть свои сильные и слабые стороны.

VPN прячет вас от местного интернет-провайдера и оберегает от хакеров, способных перехватить ваши данные при работе в публичной сети, — например, если вам пришлось воспользоваться wi-fi. Но при этом самому провайдеру VPN ваши данные могут быть доступны. Как кто-то сказал: «Ни один провайдер VPN не собирается отправляться в тюрьму, чтобы защитить подписчика, приносящего 20 долларов в месяц», — и это правда.

Tor хорош в обеспечении анонимности, но ваш локальный интернет-провайдер может счесть трафик подозрительным и блокировать его. К тому же, в Tor'е все-таки есть уязвимости: например, может быть скомпрометирован выходной узел. То есть кто-то может сидеть там и читать весь ваш трафик — пароли, явки, адреса, любовные послания, планы по захвату мира и все прочее. В основном Tor'ом управляют ответственные люди, но такие истории случались.

Если использовать VPN и Tor совместно, то эти риски можно снизить. Сначала запускаете VPN, потом через Tor обращаетесь к нужному сайту. Ваш локальный интернет-провайдер в этом случае видит только подключение к VPN, но не видит, что вы используете Tor. Затем сервер VPN на другом конце туннеля отправляет ваши зашифрованные данные первому узлу Tor, который, однако, не знает вашего настоящего местоположения и IP. А тот уже по цепочке передает запрос нужному сайту. То есть ваш провайдер VPN видит, что вы используете Tor, но не знает, куда и зачем вы обращаетесь по сети.

Из минусов этой схемы можно назвать только замедление работы, но с безопасностью всегда так[1].

Сложилось мнение, что Tor'ом пользуются в основном хакеры и преступные элементы, что там процветает торговля оружием и наркотиками, детская порнография и экстремизм, и что нормальному человеку там делать нечего. Это мнение подогревается не слишком компетентными публикациями в СМИ, в которых Tor прочно ассоциируется с даркнетом[2] — темной стороной интернета. В ответ на это можно только еще раз повторить: проблема не в технологиях, а в людях. Tor — это технология обеспечения анонимности, а уже люди ее используют в разных целях.

Tor — технология обеспечения анонимности, а уже люди используют ее в разных целях.

1 *Tor vs. VPN — A 2020 Comparison. // **Blokt.com**, 11 июня 2020.*

2 *Даркнет (англ. DarkNet) — это собирательное название компьютерных сетей, предназначенных для анонимной передачи информации. Там тоже есть сервисы для торговли, общения и обмена контентом, но их нельзя открыть через стандартный браузер или найти в обычном поисковике.*

Например, на основе Tor реализован проект Secure Drop — платформа для безопасной коммуникации журналистов с их информаторами, желающими сохранить анонимность. По сути, проект продолжает дело, начатое WikiLeaks. Этой платформой пользуются многие уважаемые издания — Forbes, The New Yorker, The Guardian, Associated Press, Bloomberg, The Wall Street Journal, Aftenposten и другие.

> *Неправительственные организации пользуются сетью Tor, чтобы их сотрудники могли посещать веб-сайт организации во время пребывания в чужой стране, не оповещая при этом всех вокруг о том, что они к ней принадлежат.*
>
> *Частные лица пользуются Tor'ом для того, чтобы сайты не отслеживали их активность в сети, или чтобы подсоединяться к новостным сайтам, сервисам мгновенных сообщений и прочим подобным услугам, заблокированным местными интернет-провайдерами. Скрытые сервисы Tor дают пользователям возможность публиковать информацию, не раскрывая своего местонахождения. Отдельные лица также пользуются сетью Tor для обсуждения конфиденциальных тем — например, на форумах поддержки жертв изнасилования или домашнего насилия, или людей с определенными болезнями.*
>
> *Подразделение ВМФ США использует Tor для передачи разведывательной информации, в том числе с Ближнего Востока. Правоохранительные органы пользуются сетью Tor, чтобы посещать или наблюдать за веб-сайтами, не оставляя в их логах запросов с правительственных IP-адресов, а также для безопасности операций внедрения и контрольных закупок*[1].

1 *Краткий обзор Tor. // Сайт* ***pf.team.***

Когда мы говорим, что Tor — защищенный браузер, это не значит, что можно расслабиться и гулять по всем сайтам, по которым вздумается. Tor оберегает только вашу анонимность, но не может защитить вас от собственной глупости: если вы зайдете на какой-то вредоносный сайт, то точно также можете подцепить вирус или шпионское ПО, которое будет использовано для деанонимизации. Или банально для того, чтобы просто украсть у вас деньги.

Злоумышленники знают, что среди пользователей Tor много новичков, которые прибегли к нему из-за роста ограничений в интернете, изобретаемых правительствами различных стран. Злоумышленникам грех этим не воспользоваться.

Заходя в Tor, надо удвоить осторожность. И также следует быть осторожным с настройками самого Tor'а.

Значит, заходя в Tor, надо, наоборот, удвоить осторожность. И также следует быть осторожным с настройками самого Tor'а, чтобы случайно не превратить свой компьютер в выходной узел сети. В таком случае запущенный Tor-браузером ретранслятор Tor-сети может трактоваться как программа, участвующая в предоставлении доступа к запрещенным в РФ ресурсам кому-то, кроме вас, а это уже влечет ответственность по закону.

13 августа 2014 года французский студент Жюльен Вуазен обнаружил поддельный ресурс, в точности имитирующий официальный сайт The Tor Project, Inc. Через него под видом пакета Tor Browser распространялось вредоносное программное обеспечение, и похищались пожертвования пользователей. Согласно информации, которую

удалось добыть Вуазену, за созданием фальшивого сайта стояла группа хакеров из Китая[1].

В апреле 2017 года в России был арестован математик Дмитрий Богатов. Его обвинили в призывах к терроризму и организации массовых беспорядков в сообщениях, размещенных на форуме sysadmins.ru. Единственной уликой против Богатова является то, что ему принадлежит IP-адрес, с которого было размещено сообщение. Богатов поддерживал на своем компьютере выходной узел сети Tor, которым мог воспользоваться любой. По словам защиты Богатова, его невиновность подтверждается записями камер наблюдения, которые доказывают, что в момент публикации он возвращался домой из магазина. Арест Богатова широко обозревался в российских СМИ и вызвал широкий интерес россиян к работе анонимайзера[2].

Бдительный читатель обязательно должен спросить: а как у Tor'а с отпечатками браузера? Мы тут усложняем себе жизнь, громоздя Tor поверх VPN, а нас, может быть, все равно идентифицируют в два счета. Или нет? Ситуацию разъясняет Пьер Лаперди (Pierre Laperdrix), один из ключевых участников проекта amiunique.org.

«Tor Browser был первым браузером, который решал проблемы, связанные с дактилоскопией, еще в 2007 году, до того, как появился термин «дактилоскопия в браузере» — в Tor была добавлена функция перехвата Javascript для маскировки часового пояса.

---

1 *Закон об анонимайзерах вступил в силу. Что о нем нужно знать? // Русская служба BBC, 1 ноября 2017.*

2 *Следствие по делу Дмитрия Богатова через год было прекращено, и он уехал в США.*

Подход, выбранный разработчиками Tor, прост: все его пользователи должны иметь одинаковые отпечатки браузера. Независимо от того, какое устройство или операционную систему вы используете, отпечаток вашего браузера должен совпадать с любым устройством, на котором запущен Tor.

Кроме того, вы, возможно, задавались вопросом, почему при развертывании окна браузера появляется следующее сообщение: "Максимизация Tor Browser позволяет веб-сайтам определять размер вашего монитора, это может быть использовано для отслеживания вас. Мы рекомендуем оставить окна браузера Tor в их исходном размере по умолчанию".

Это из-за дактилоскопии. Поскольку пользователи имеют разные размеры экрана, один из способов убедиться в том, что различий не наблюдается, состоит в том, чтобы все использовали один и тот же размер окна. Если вы развернете окно браузера до максимума, ваш браузер может оказаться единственным, использующим Tor с этим конкретным разрешением, — таким образом повышается риск вашей идентификации в интернете.

На самом деле, «под капотом» было сделано еще множество доработок, призванных уменьшить различия между пользователями. Были введены резервные шрифты по умолчанию для минимизации отпечатков шрифтов. WebGL и Canvas API по умолчанию заблокированы, чтобы предотвратить скрытый сбор параметров графики. Проделано было и много другой работы[1].

---

1 *Browser Fingerprinting: An Introduction and the Challenges Ahead. // Блог Tor Project, 4 сентября 2019.*

По состоянию на сегодняшний день можно сказать, что Tor довольно неплохо противостоит попыткам идентификации пользователей с помощью технологии снятия цифровых отпечатков браузера. Его разработчики считают эту задачу одной из приоритетных и намерены продолжить борьбу за анонимность.

Учтите, что сказанное выше о противодействии фингерпринтингу верно при условии, что в Tor выбран наивысший уровень безопасности (Safest).

Итак, подумайте еще раз хорошенько: вам действительно нужен Tor? Пользование им выделит вас из общей массы ежедневной аудитории интернета. В мире ежедневно Tor используют 2-3 миллиона человек, среди которых из России — порядка 500 тысяч. То есть порядка 0,7% от общего числа российских пользователей. Трафик Tor заметен, а это значит, что вы сразу привлечете к себе внимание. Ради того только, чтобы получить доступ к заблокированным ресурсам. Не избыточно ли это?

Трафик Tor заметен, а это значит, что вы сразу привлечете к себе внимание.

Тем не менее, если все же по каким-то причинам Tor вам нужен, соблюдайте следующие правила:

- Никогда не входите в свои обычные аккаунты почты и соцсетей через Tor;
- Не пользуйтесь онлайн-банкингом. (Тем более что банк, скорее всего, посчитает это подозрительным и заблокирует ваш счет);

- Используйте VPN. (Об этом уже говорили, но не лишне напомнить);
- Никому не сообщайте никаких личных сведений, остерегайтесь «социальных инженеров»;
- Не смешивайте анонимный режим с обычным. Лучше вообще иметь для Tor отдельный компьютер или хотя бы виртуальную машину.

Контрольные вопросы

1. Как обеспечивали анонимность в реальном мире?
2. Зачем нужна анонимность в интернете? Ваши версии.
3. Что понимается под анонимностью в интернете?
4. Что такое псевдоним (в обычной жизни и в интернете)?
5. Что такое IP-адрес? Опишите своими словами.
6. Как найти человека по IP-адресу?
7. Что такое прокси?
8. Почему могут быть опасны бесплатные анонимайзеры?
9. Что такое VPN? Опишите своими словами, как это работает.

10. Что на самом деле запрещает закон о запрете анонимайзеров?

11. Что значит «ответственное поведение в интернете» и почему это важно?

12. Что такое куки и где они хранятся?

13. Чем куки опасны? Назовите два основных риска.

14. В чем слабые места позиции «мне нечего скрывать»?

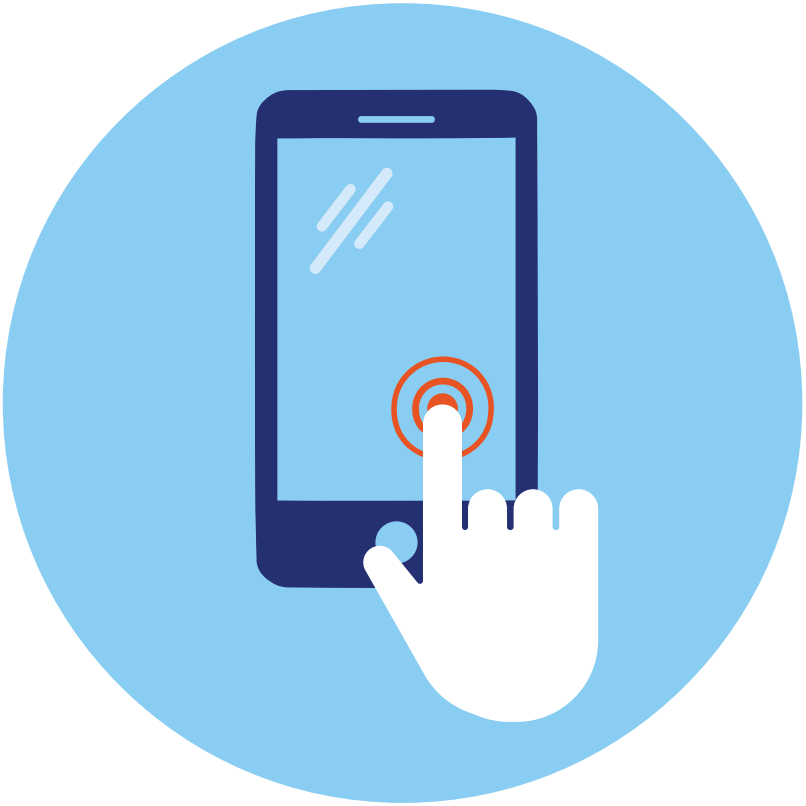
15. Для чего нужен блокировщик рекламы помимо блокировки рекламы?

16. Что такое отпечаток браузера?

17. Что такое Tor?

18. С какими целями люди используют Tor?

19. Зачем использовать VPN и Tor совместно?



Глава 8

Мой мобильный друг, моя прелесть

Эта глава о том, чем стал мобильный телефон для современного человека, и почему мы так к нему привязаны, особенно дети.
Мы обсудим, какое место должен занимать телефон в семье и школе, узнаем, как за нами могут с его помощью шпионить, и поговорим о том, что нужно сделать, чтобы минимизировать потери и риски, если с телефоном что-то случилось.

Вам знаком этот холодок в груди, когда шаришь по всем карманам, копаешься в сумке, рюкзаке или портфеле и никак не можешь найти свой телефон?

«Ну, где же он, моя прелесть? Неужели какой-то хоббит запустил свои ручонки в мой карман и похитил его? Как тогда жить дальше? Ведь там было все, что связывает меня с этим волшебным цифровым миром... Ах, вот он! Счастье! Ну-ка, посмотрим, что за последние три минуты произошло нового... Ой, батарея почти разрядилась... Ужас! Скорее, скорее дайте зарядку!»

> *Мы все стали немного похожи на Голлума, когда думаем о любимых мобильных устройствах, без которых нам сразу становится неуютно, не так ли?*

Если вы испытываете дискомфорт, беспокойство и чувство страха, разлучившись даже на короткое время со своим телефоном или оказавшись без связи, то, весьма вероятно, что у вас номофобия. Сам термин происходит от английской фразы «no mobile phone» и означает боязнь остаться без мобильного телефона. Это явление обнаружили в 2008 году, когда исследование[1] YouGov, проведенное по заказу UK Post Office, показало, что 66 человек из 100 испытывали панический страх, оставаясь без связи.

> *Номофобия официально не признана психическим заболеванием, хотя были призывы включить ее в перечень DSM-V (Diagnostic and Statistical Manual of Mental Disorders, 5th Edition). Часто ассоциируемая с тревогой разделения (separation anxiety), номофобия сопровожда-*

1 *Nomophobia // Википедия*

ется набором идентифицируемых симптомов: учащенное сердцебиение и артериальное давление, одышка, беспокойство, тошнота, дрожь, головокружение, депрессия, дискомфорт, страх и паника. Тем не менее, медицинское сообщество все еще спорит о его классификации — это фобия, тревожное расстройство, расстройство образа жизни или зависимость?[1]

Например, в Италии с номофобией пытаются бороться на законодательном уровне. Подготовленный в июле 2019 года законопроект предусматривает образовательные программы для родителей, чтобы обнаружить чрезмерное использование мобильного телефона детьми. Также в нем изложены планы «обучения добросовестному использованию интернета и социальных сетей» в школах и университетах[2]*. Подобную инициативу можно приветствовать, если только в руках государственных чиновников это не выродится в унылую обязаловку «для галочки».*

Сегодня 2008 год выглядит как доисторическая эпоха — тогда первый айфон только-только увидел свет, а мобильный интернет был медленным и неуклюжим. И, если в то время новой фобией уже страдала значительная часть населения, то теперь эти симптомы, наверное, есть у каждого.

Если в 2008 году номофобией уже страдала значительная часть населения, то теперь эти симптомы, наверное, есть у каждого.

1 *Nomophobia: The Modern-Day Pathology. // Psychiatry Advisor, 18 сентября 2018.*

2 *Italy drafts 'no-mobile-phone phobia' law. // RTL Today, 24 июля 2019.*

YouGov повторил свое исследование[1] в 2019 году: согласно свежим данным, девять из десяти британцев (88%) в настоящее время имеют смартфон, и значительная часть из них будет чувствовать нервозность или беспокойство по поводу того, что они расстались со своим устройством даже на один день. Предсказуемо, что более молодая часть опрошенных испытывает большую привязанность к своим гаджетам, чем старшее поколение. Нервничать из-за разлуки с телефоном будут 72% участников опроса в возрасте от 18 до 24 лет против 47% в возрасте старше 55 лет.

Хотите проверить себя? Попробуйте отключить телефон хотя бы на день. И, допустим, вам удалось пройти это испытание. А что, если не отвечает мобильный вашего ребенка? Как долго вы сможете сохранять спокойствие?

> *Одна девочка-третьеклассница потеряла свой мобильный. Мама, естественно, рассердилась и сказала: «Раз ты не можешь следить за своими вещами, походишь пока без телефона — у меня сейчас нет денег на новый». На следующий день девочка ушла в школу и в обычное время не вернулась домой. «Ничего страшного! Наверное, зашла к кому-то в гости», — успокаивала себя мама. Но вот дело к вечеру, а ребенка все нет. Мама уже в легкой истерике обегает окрестные дворы и обзванивает родителей одноклассников. Вскоре пропавшая нашлась: она, как и предполагала встревоженная мать, сидела дома у подружки. Диалог был следующий: «Но ты же могла позвонить! — А у меня нет телефона. — Но был же телефон в квартире твоей подруги! — Мы делали уроки, и я не заметила, что уже поздно». Понятно, что это была месть*

1 *Could you live without your smartphone? //YouGov, 8 марта 2019.*

за отказ купить новый телефон немедленно. Рассерженная мать пошла на принцип: «Вот тебе телефон, самый простой. Этого достаточно, чтобы позвонить». Не прошло и недели, как ни в чем не повинный кнопочный телефон «случайно» утонул в туалете.

В итоге новый смартфон был куплен. Конечно, такое поведение недопустимо, однако взрослым надо понимать, что для современного ребенка телефон — это не бубенчик на шее, чтобы мама всегда знала, где он есть, а ключ ко всем богатствам цифрового мира, который плюс к тому же умеет еще и звонить. Поэтому ребенок готов сражаться за свое право на доступ к информации всеми честными и нечестными способами.

Надо признать, что позиция взрослых по отношению к детским телефонам противоречива: с одной стороны, они хотят, чтобы дети всегда были на связи, и впадают в панику, когда ребенок не отвечает; с другой стороны, их раздражает, что дети постоянно сидят, уткнувшись в свои мобильники. Только попробуй оставить телефон дома, когда ушел погулять! Вернешься через час — а бабушку уже увезли на скорой. Так что еще неизвестно, у кого больше развита эта самая номофобия, — бабушка говорит, что легко может обойтись без мобильника, но сойдет с ума, если внук внезапно устроит себе цифровой детокс.

Попробуй оставить телефон дома, когда ушел погулять! Вернешься через час — а бабушку уже увезли на скорой.

Может быть, дело не в том, что молодое поколение поразила эпидемия новой болезни? Может быть, это часть процесса перехода к цифровому будущему, когда наш мозг будет напрямую подключен

к Матрице? (Шутка!). Пока футуристы спорят о возможных сценариях дальнейшей судьбы нашей цивилизации, смартфон уже сейчас выполняет роль связующего звена между человеком и его цифровой личностью — собственно, разрыв этой связи и ощущается так болезненно. Почти 50% участников вышеупомянутого опроса YouGov в возрасте от 18 до 24 лет ответили, что без мобильного телефона «чувствовали бы себя странно, потому что не знали бы, что делать». Не все могут сформулировать причину своего беспокойства, но показательно следующее: 11% обозначили, что будут нервничать, если окажутся отключенными от сетевой идентификации.

Половина пользователей смартфонов носят их за собой из комнаты в комнату, когда находятся дома. «У меня телефон подключен к часам, и когда они теряют связь, часы начинают вибрировать, — теперь я всегда физически чувствую, когда удаляюсь от телефона», — говорит Катерина, художник-иллюстратор.

В этом контексте медикализация проблемы избыточного увлечения молодежи мобильными телефонами и отнесение ее к ряду известных зависимостей — игровой, алкогольной, наркотической и других — может оказаться сильным упрощением.

> *Право на доступ к информации считается одним из фундаментальных прав человека, а сегодня оно технически реализуется в основном через мобильный телефон.*

Так что «лечить» это надо с большой осторожностью: поскольку надежных научных данных о явлении пока очень мало, важно не спутать реальные риски для здоровья с обычным конфликтом поколений, ведь большинство исследователей — люди старшего возраста, которые просто боятся новых технологий. Возможно,

у них самих технофобия[1], скажут молодые врачи, которые вскоре займут места в частных клиниках и государственных медучреждениях и будут сами дни напролет сидеть в телефоне, считая это нормой.

Чьи в семье симки

Телефон есть у каждого, даже у младших школьников. И тут возникает интересная коллизия: ребенок считает, что телефон — его сугубо личное пространство, и психолог будет на его стороне. А юрист нам скажет, что контракт на телефонный номер оформлен на родителя, и что именно на нем, как на владельце лежит ответственность за все, что делается с этого номера, в том числе и публикуется в интернете. И что по закону у вас, как у владельца номера и аппарата, есть полное право знать, что ваш ребенок читает и пишет.

По закону у вас, как у владельца номера и аппарата, есть полное право знать, что ваш ребенок читает и пишет.

Подспудно большинство детей понимают, что не они платят за телефон, и что им придется оставаться в зависимом положении до тех пор, пока они не вырастут, и что у взрослых действительно есть право проверять содержимое их телефонов. Это может быть неприятно, взрослый даже может быть неправ с точки зрения этики и психологии, но дети вынуждены подчиняться.

---

1 *Технофобия — страх или неприязнь к передовым технологиям или сложным электронным устройствам. Страх перед техническим прогрессом вообще. Не имеет отношения к фобиям в медицинском смысле (Википедия).*

Один из эпизодов в фильме «Отрочество»[1], который родителям подростков стоит посмотреть, как раз про это. Глава семейства собирает у всех детей телефоны, чтобы выяснить, куда скрылась его жена после очередной ссоры. Дети не смеют ему перечить. При этом никто не пытается спрятать телефон, поставить пароль или что-то в этом роде. Конечно, они опасаются физического насилия со стороны взрослого, находящегося далеко не в адекватном состоянии, но их покорность продиктована не только страхом — заметно, что они признают право взрослого это сделать, хотя им это неприятно. Несмотря на то, что все происходит без рукоприкладства и криков, впечатление все равно тяжелое: мы наблюдаем явное психологическое насилие.

Когда вам захочется проверить телефон своего ребенка, вспомните об этой сцене, потому что, какие бы ни были у вас мотивы, сколько бы вы с ним заранее ни обсуждали этот вопрос, как бы это ни казалось вам правильным и «для его же блага» — это все равно будет вторжение в его личное пространство. И вы будете выглядеть как тот — далеко не самый приятный — персонаж фильма. Не делайте этого без крайней необходимости!

---

1 *«Отрочество» — уникальный фильм Ричарда Линклейтера, съемки которого длились с 2002 г. по 2013 г. История охватывает двенадцать лет самой обычной жизни ребенка (от первого класса в школе до первого дня в колледже) и складывается из небольших эпизодов, показывающих взросление и отношения с родителями ребенка, подростка, юноши. Главную роль исполнил семилетний (на то время) мальчик Эллар Колтрейн, который, согласно заключенным договоренностям, не мог быть заменен никем другим до окончания съемок. Вместе с Элларом росла и снималась в роли его сестры дочь режиссера Лорелей Линклейтер. Четкого сценария не было, он из года в год переписывался от года к году.*

Сепарация от родителей — обязательная часть процесса взросления. Границы личного пространства вашего ребенка постепенно будут расширяться, в том числе и в отношении гаджетов.

Дошкольник и сам с радостью покажет маме, что ему пришло сообщение или письмо, — неважно от кого, потому что корреспонденции у него пока совсем немного. Другое дело подростки, у которых уже появляются свои секреты, пусть и безобидные, — вроде и прятать нечего, но и открывать не хочется. Тинейджеры и сами по большей части относятся к этому с юмором — в TikTok полно смешных микрокомедий на тему «Мама хочет проверить мой телефон. Ой, караул! Что делать?»

Ну, а чтобы требовать показать переписку от человека, которому скоро стукнет восемнадцать, нужно иметь совсем уж веские основания. Предположим, вам кажется, что они у вас есть. И что с того? Пароль-то он вам все равно не скажет. Если вас посетит мысль, что аккаунт ребенка не грех и взломать, лучше выкиньте ее из головы. (Не стоит, кстати, «ломать» телефон супруга или супруги, как бы вас ни разбирали любопытство и ревность, — это тоже уголовно наказуемое деяние).

Неудобно получилось в одной из деревень Чечерского района Гомельской области. Местная школьница заметила, что на ее странице в соцсети хозяйничает кто-то посторонний: заходит под ее данными, читает сообщения и даже вступает в переписку с парнями. Хозяйка аккаунта обратилась в милицию. Лазутчика удалось вычислить. Правда, заметая следы, он удалил всю страницу. О некоторых обстоятельствах этой высокотехнологичной истории рассказали в Гомельском областном управлении Следственного комитета.

События начали разворачиваться, когда девочке было 16 лет. Отец школьницы заходил на ее страницу, чтобы контролировать отношения дочери с парнями. Что он им писал — не сообщается. Когда школьница обратилась в правоохранительные органы, и запахло жареным — строгий папа на всякий случай удалил аккаунт.

Теперь у мужчины статус подозреваемого. СК информирует, что уголовное дело возбуждено по статье 351 «Компьютерный саботаж», — под нее подпадает уничтожение компьютерной информации. Позже в СК сообщили: уголовное дело прекращено ввиду незначительности деяния, а также с учетом личности подозреваемого[1].

По достижении ребенком совершеннолетия можно переоформить сим-карту на него — и обязательно стоит это сделать. Многие про это забывают, и выросшие дети продолжают пользоваться телефонами, зарегистрированными на родителей. Вопрос, конечно же, не в том, чтобы спихнуть ответственность; важно показать уважение к ребенку и подчеркнуть его самостоятельность. Дети обязательно это оценят. Во-вторых, есть и практическая сторона: если сломается или потеряется симка, или вашему чаду захочется сменить оператора — решать эту проблему вам не придется.

Все, что вам нужно сделать, — приехать в центр обслуживания абонентов сотового оператора, предъявить свои паспорта и написать соответствующие заявления. Перед визитом обязательно по-

1 *В Чечерском районе мужчина взломал аккаунт дочки-школьницы и переписывался от ее имени. Завели уголовное дело, но позже прекратили. //* ***Tech.Onliner.by****, 22 мая 2019.*

полните баланс телефона, поскольку передача другому владельцу номера с минусовым балансом невозможна. (Детали уточняйте у своего оператора, эта услуга может быть платной).

> *Учтите: для оператора ваш сын или дочь будут новым клиентом. Это значит, что историю лояльности ему или ей придется нарабатывать заново. Накопленные бонусы и привилегии не передаются.*

Как мы хорошо знаем, телефон теперь нужен по большей части не для того, чтобы звонить, а чтобы пользоваться разными приложениями — и полезными, и развлекательными. Пользователю нужно иметь аккаунт, чтобы загружать приложения из магазина (даже бесплатные) и пользоваться облачными сервисами (например, iTunes для владельцев айфонов). Политика владельцев платформ — Apple и Google — в принципе, одинакова, потому что обе компании подчиняются американскому законодательству.

Завести Apple ID ребенку младше 13 лет можно при помощи функции «Семейный доступ»[1], и это единственный легальный способ, к тому же самый удобный. Если вам пришла в голову мысль немного соврать насчет возраста ребенка при создании аккаунта, не надо этого делать. Конечно, американская полиция из-за этого не нагрянет к вам в дом, но, когда ребенок подрастет и станет распоряжаться своими iOS-устройствами самостоятельно, откатить возраст к реальному значению будет нельзя. Тогда придется создать новый Apple ID, но при этом все его достижения в играх, покупки и история «сгорят».

---

1 *Подробнее см.* ***https://www.apple.com/ru/family-sharing/***

> *«Семейный доступ» позволяет видеть статистику использования игр и соцсетей ребенком и ограничить ему время их использования и тип доступного контента, причем все можно сделать со своего телефона удаленно.*

Кроме того, вы можете согласовывать все покупки ребенка в iTunes Store, Apple Books, App Store, в том числе даже загрузку бесплатных приложений, — для этого надо лишь включить и настроить функцию «Попросить купить». Согласитесь, это проще, чем привязывать к аккаунту ребенка свою кредитную карту и потом ругать его за неразумные траты.

> *Для детского аккаунта есть и некоторые дополнительные ограничения. В частности, владельцы iPhone X в возрасте до 13 лет не смогут пользоваться распознаванием по лицу. Согласно новым правилам для разработчиков, опубликованным на официальном сайте Apple, компания будет принудительно отключать работу сканера Face ID в приложениях для детей. В первую очередь, возрастные ограничения, накладываемые компанией Apple на своих юных клиентов, связаны с особенностями американского законодательства. В США предусмотрена особая система непреложных правил, препятствующая повсеместному сбору данных о пользователях, не достигших 13 лет.*

Google придерживается, в целом, аналогичной политики. Создать аккаунт Google могут только пользователи старше 13 лет; более юным нужно участие родителей. Все управление ведется через приложение Family Link[1] и позволяет контролировать дей-

1 *Подробнее см.* ***https://families.google.com/familylink/***

ствия ребенка, включая текущее местоположение и используемые программы. По достижении 13 лет аккаунт может быть передан ребенку в самостоятельное использование.

Как «достать» ребенка из телефона?

Ребенок постоянно залипает в телефоне. Что делать?

Этот вопрос задают многие родители, отчаявшиеся справиться с ситуацией самостоятельно. Кстати, вопрос задан предельно точно, ребенок именно «в телефоне», а не с телефоном, — внешний мир для него почти перестает существовать, остается только магический экран. Даже когда дети приходят друг к другу в гости, они садятся на диван и уходят в свои виртуальные миры. Они не такие, как мы, — и взрослых эта картина пугает.

Родители пытаются решить эту проблему по-разному. Самые нетерпеливые и неадаптированные «цифровые иммигранты» идут путем запретов и объявляют тотальную войну гаджетам, что только усиливает отчуждение между детьми и родителями. Другие пробуют отвлечь детей от экранов прелестями «теплого лампового мира» — бумажными книгами, играми во дворе, разговорами на кухне — и терпят неудачу. Но мало кто из взрослых выбирает вариант, рекомендованный во всех учебниках по маркетингу, быть там, где находится ваш клиент. Если дети сидят в телефоне, то нужно проникнуть туда, чтобы говорить с ними.

Если дети сидят в телефоне, то нужно проникнуть туда, чтобы говорить с ними.

Именно так поступил отец пятерых детей Джастин «Джо» Смит — он создал в YouTube канал, чтобы с его помощью общаться со своими детьми. Менеджер по продажам продуктов питания Джо был уверен, что видеоблог станет хорошим способом для его детей увидеть, чем он занимается, путешествуя по Великобритании и за рубежом[1].

«Причина, по которой я это сделал, вот в чем: я до смерти устал от того, что постоянно вижу головы моих детей, опущенные к их телефонам. И если YouTube — единственный способ, которым я могу общаться с ними, то пусть так и будет.

У меня пятеро великолепных детей. Однако в то утро я был слегка расстроен, потому что, встав и спустившись вниз, хотел поговорить с дочками, но... их головы оказались склонены к телефонам, а на ушах были наушники. Дочери смотрели YouTube».

В тот момент мистер Смит решил, что с него довольно.

«Я просто хорошенько подумал. И вспомнил: „Если вы не можете победить их, присоединяйтесь к ним". А моя школьная подруга предложила действительно хорошую идею. Она сказала: „Почему бы тебе просто не завести канал на YouTube?". Так я и сделал».

Начинающий ютьюбер предложил и другим родителям последовать его примеру.

«Создайте свой собственный канал, как я. Продолжайте постить видео. Я тоже буду продолжать делать видео. Я за-

1 *См. YouTube-канал «Joe Daddyutube».*

ставлю своих дочерей и остальных моих детей подписаться на него».

«Итак, я просто собираюсь снимать случайные видео. Я надеюсь, что вам они понравятся… Это может происходить не каждый день, но я хочу, чтобы мои дети, как только у меня будет возможность, наблюдали за мной, а не смотрели бессмысленную чушь».

Эта история попала на страницы британских газет — как говорится, «тема вызвала широкий общественный резонанс». Наверное, это прибавило отцу авторитета в глазах детей. Однако Джо выпустил только десять роликов и забросил свой канал — хлеб видеоблогера отнюдь не легок, любое занятие требует труда. Но идея была классная! Надеюсь, у него получилось наладить контакт с детьми — ведь цель была именно в этом, а не в том, чтобы стяжать лавры на новом поприще.

Не телефон отнимает у вас ребенка, а ваше неумение общаться в привычном для него формате.

Так, может быть, не стоит торопиться спасать детей от гаджетов? Не телефон отнимает у вас ребенка, а ваше неумение общаться в привычном для него формате. В этом нет ничего противоестественного — слова любви и заботы одинаково воспринимаются сказанными вслух и написанными в мессенджере. Также, как обидные замечания и постоянные одергивания портят отношения вне зависимости от того, каким способом они попадают к адресату. Около 40% английских подростков признались, что время от времени общаются с родителями с помощью мессенджеров даже тогда, когда те находятся в соседней комнате, —

и не видят в этом ничего дурного. Важно то, что вы хотите сказать человеку, а не то, каким именно способом.

Вот как взаимопроникновение детской аудитории и Всемирной Сети выглядит в отраслевом докладе Института исследований интернета «Детский Рунет 2019[1]»:

- *Для выхода в интернет смартфон используют 67% детей в возрасте 5–11 лет и 74% детей в возрасте 8–11 лет.*

- *У 44% детей в возрасте 5–7 лет есть собственный смартфон, у детей в возрасте 8–11 лет этот показатель уже 74%.*

- *Наиболее популярные практики у детей в интернете, по мнению родителей: онлайн-игры — 59% детей, просмотр видео — 53% детей, потребление образовательного контента — 42%.*

- *Картина потребления контента детьми с возрастом меняется. Младшие (до 7 лет) преимущественно пассивны — смотрят кино, мультики и видео (76,6%), даже игры идут с сильным отставанием (44,1%). У детей постарше (8–10 лет) в приоритет выходят игры (69%) и также много времени занимает просмотр разнообразного видео (58,6%). Подростки (10–13 лет) начинают уделять больше внимания учебному контенту, который выходит у них на второе место (42,9%), а пальму первенства все также удерживают игрушки (67,3%). Старшеклассники (14–17 лет) практически поровну делят основное*

1 *Детский Рунет 2019. Отраслевой доклад. //Институт исследований интернета, 2020.*

время между играми и учебой (57,7% и 56,2%), а следующим по популярности занятием становятся у них социальные сети (49,2%).

Между тем, сам интернет полон устрашающих заголовков о «телефонной зависимости» подростков и советов по избавлению от нее. Подчас от них за версту несет глубоким непониманием того, как на самом деле работают технологии. Вот всего лишь несколько примеров из области тестов и анкет для диагностики компьютерной зависимости.

«Как часто ваш ребенок выглядит погруженным в мысли о возвращении в Сеть, когда он находится вне Сети?» *— ну, прямо Нео, размышляющий о возвращении в Матрицу.*

«Как часто вы заставали своего ребенка пробивающимся в сеть против вашей воли?» *— видимо, Сеть есть нечто магическое и непостижимое для автора вопроса, куда надо «пробиваться».*

«Как часто ваш ребенок выглядит более уставшим и утомленным, чем в то время, когда у вас не было интернета?» *— бабушкам и дедушкам такой вопрос задать еще можно, а родителям подростков — вряд ли. Интернет был всегда, а теперь есть и везде.*

«Вы не помните на память ни одного телефонного номера, полагаясь на телефонную книгу мобильника» *— ага, значит, у вас зависимость от телефона! А если вы не помните, как выполнить деление в столбик, то у вас зависимость от калькулятора, логично же!*

> ***«Вы используете мобильник даже тогда, когда у вас дома есть обычный телефон»*** *— подозрительно, не правда ли? Нормальный человек ведь не станет так делать, он лучше позвонит через телефонную барышню. Или напишет письмо на бумаге и отнесет на почту.*
>
> ***«На ночь вы кладете свой телефон под подушку или на прикроватный столик»*** *— разумеется, это признак зависимости! Только скажите честно, остался ли у кого-то всамделишный будильник?*

Создается впечатление, что авторы подобных тестов в силу собственной наивности представляют себе цифровой мир даже не по «Матрице», а скорее на уровне «Газонокосильщика»: для 1992 года это было круто, но фильм в прокате провалился, потому что публика не поверила в такой виртуальный мир — угрозы выглядели слишком надуманными. Над всем этим можно было бы посмеяться, однако, если таким тестом на самом деле воспользуется школьный психолог, то ничего хорошего из этого не выйдет. Будет только нагнетание тревоги у родителей, и невыполнимые на практике советы по изгнанию гаджетов из дома. Это все равно что призывать вместо электричества вернуться к керосиновым лампам — мило, но нереально. Однако, вывод делается непререкаемый: у детей поголовная зависимость от телефонов, и надо срочно их спасать.

> *Но позвольте: как эта маленькая вещица из стекла, кремния и алюминия может быть предметом зависимости? Говорить такое — все равно что рассуждать о том, что человек зависит от микроволновки или электродрели.*

На самом деле зависимость может быть от того, что человек делает при помощи телефона. Например, если он играет в азартные игры,

то у него лудомания (пристрастие к азартным играм). Если не вылезает с сайтов для взрослых, то это, вероятно, порнозависимость. Когда кто-то постоянно строчит сообщения в мессенджере одному адресату, не исключено, что он или она находятся в зависимых отношениях. Бесконечно смотрит видео — это обновленная версия ТВ-зависимости (а мусорного контента в интернете гораздо больше, чем в телевизоре). Безудержно заказывает бесполезные вещи в интернет-магазинах? Мы скажем: шопоголик. И так далее.

Большинство известных зависимостей успешно мигрировали в цифровой мир, где предаваться им стало даже удобнее.

То есть, нет зависимости «от телефона», «от компьютера» или «от интернета». Есть зависимости от конкретных паттернов поведения, которые реализуются при помощи этих технических средств. С ними-то и надо разбираться, а не винить во всем научный прогресс. Большинство известных зависимостей — например, та же лудомания, — успешно мигрировали в цифровой мир, где предаваться им стало даже удобнее. Одноруких бандитов с улиц убрали, а онлайн-казино процветают, несмотря на все старания их искоренить.

Технологии принесли и новые виды зависимостей, которых прежде не было.

Однако, справедливости ради, нужно сказать, что технологии принесли и новые виды зависимостей, которых прежде не было.

Во-первых, зависимость от компьютерных игр, которая иногда доводит и до смертельного исхода. Чаще всего это происходит от переутомления, когда геймеры не отрываются от компьютера по 70-80 часов подряд. Был случай и похуже: молодые родители

так заигрались, что забыли про ребенка на балконе, которого вынесли «погулять». Дело было зимой, малыш погиб. (Но это, скорее, про стационарные компьютеры, на мобильнике сутки напролет не поиграешь).

Второй вид зависимости, напрямую связанный компьютерными технологиями, — зависимость от социальных сетей. Здесь механизм действия другой: слишком долгое зависание в соцсетях повышает риск развития депрессии, что может довести и до суицида. И в соцсетях как раз зависают, в основном, с телефона, поэтому он и считается источником всех подобных бед. (Подробнее об этом поговорим в главе про социальные сети).

Но есть и хорошие новости! Российские ученые изучили влияние интернета на развитие умственных способностей у детей и пришли к выводу, что пребывание детей в Сети положительно сказывается на их развитии. Как пояснила в комментарии газете «Коммерсантъ» директор Фонда развития интернета, профессор факультета психологии МГУ Галина Солдатова: «Сейчас и российские, и зарубежные ученые стараются смотреть на интернет иначе, чем раньше: не говорят в ужасе, что все живут онлайн, а стараются оценить среднюю активность и эффективность использования. При этом авторы убеждены, что у детей, пользующихся интернетом, в целом выше успеваемость по сравнению с детьми, для которых пребывание онлайн сведено к минимуму»[1].

Ученые факультета психологии МГУ провели исследование с участием 200 детей, которые были разделены на четыре

1 *Доступ разрешен. Российские ученые определили оптимальное время, которое дети могут проводить онлайн. // Газета «Коммерсантъ», 7 октября 2020.*

возрастные группы. Внутри групп детей разбили по интенсивности пользования интернетом и определили оптимальное время времяпровождения в Сети:

- *5–6 лет. Для детей в этой группе оптимально использование интернета до одного часа в день. У них лучше развита слухоречевая память, чем у сверстников, которые проводили в Сети больше времени.*

- *7–10 лет. В этой категории детям рекомендуется проводить в Сети 1-3 часа в день. Они демонстрировали оптимальный уровень эрудиции и были лучше осведомлены, чем другие участники этой возрастной группы.*

- *11–13 лет. В группе младших подростков также можно предположить существование «оптимального» временного диапазона пользования цифровыми устройствами, который, в сравнении с младшими школьниками, уже существенно больше и может составить от 3 до 5 часов в день.*

- *14–16 лет. Оптимальное времяпровождение для этой группы не удалось определить. Были получены достаточно противоречивые данные. Подростки с низкой онлайн-активностью лучше строили рассказ и грамматически его оформляли. Они имели больший объем зрительной памяти, допускали меньше ошибок при воспроизведении зрительных фигур. Однако подростки из групп с высокой онлайн-активностью также демонстрировали достаточно высокие показатели в данных функциях, в то время как подростки со средней активностью, наоборот, в вербальных функциях*

и в зрительной памяти показывали низкие результаты. Это может быть связано как со спецификой ведущей деятельности в данном возрасте (профессионально ориентированная учебная деятельность), так и с тем, что познавательная сфера в данном возрасте уже достаточно сформирована и меньше зависит от цифровой активности подростка.

Помимо понимания некоторых тенденций формирования когнитивных функций у детей и подростков, в исследовании подтверждается предлагаемая зарубежными авторами «гипотеза Златовласки», согласно которой существует некоторая «золотая середина» — такой временной диапазон ежедневной онлайн-активности, который позволяет ребенку пользоваться достижениями научно-технического прогресса не во вред своему когнитивному развитию и психологическому благополучию[1].

Зависимость — это вопрос выбора объекта. Соответственно, диагностирование и лечение (или точнее будет сказать, помощь в избавлении от зависимостей) должны проводиться известными методами, без перекладывания всей вины на технологии. Помните, что главная причина детских зависимостей — это проблемы в общении с родителями. Не стоит во всех проблемах винить телефоны.

---

1 *Солдатова Г.У., Вишнева А.Е. Особенности развития когнитивной сферы у детей с разной онлайн-активностью: есть ли золотая середина? // Консультативная психология и психотерапия. 2019. Т. 27. № 3. С. 97–118. doi: 10.17759/cpp.2019270307.*

Я ль на свете всех милее? Феномен селфи

Основоположником жанра селфи можно считать Эдварда Мунка. Испытывая любопытство к современным технологиям, он приобрел свою первую камеру Kodak Bull's Eye №2 в Берлине, когда ему было 40 лет, и начал фотографировать не только то, что видел вокруг, но и себя. (На своих картинах он тоже появлялся часто — просто меняя камеру на кисть). Одна из наиболее известных его фоторабот в новой технике — автопортрет «а-ля Марат» рядом с ванной в психиатрической клинике доктора Якобсона в Копенгагене, где Мунк в 1909 году лечился от депрессии, сопровождавшейся параноидальными идеями и алкоголизмом. Это изображение может быть одним из самых ранних когда-либо сделанных селфи[1].

Гениальный норвежский художник не был психически здоровым человеком. Может быть, и его последователи, регулярно выкладывающие на всеобщее обозрение «себяшки», тоже больны?

> *В 2014 году появилось сообщение, что Американская психиатрическая ассоциация признала чрезмерное увлечение самофотографированием обсессивно-компульсивным расстройством и дала ему название «селфитис». В статье утверждалось, что существует три уровня расстройства: пограничный («фотографирование себя как минимум три раза в день, но без размещения в социальных сетях»), острый («фотографирование*

1 *Исторически первым селфи считается дагерротип, сделанный в 1839 году Робертом Корнелиусом, американским пионером в области фотографии. Он установил камеру, снял крышку с объектива, отбежал и сел на стул, потом встал и закрыл объектив — птичка тогда вылетала медленно, можно было все это успеть. Мунк же фотографировал себя, держа фотоаппарат на вытянутой руке, в той же манере, как мы это делаем сейчас. И по стилю его селфи очень близки к современным.*

себя как минимум три раза в день и размещение каждой фотографии в социальных сетях») и хронический («неконтролируемое желание круглосуточно фотографировать себя и публиковать фотографии в социальных сетях более шести раз в день»).

Новость тут же перепечатали многие уважаемые издания, не посмотрев на источник. Разумеется, сообщение оказалось уткой. Ее придумали журналисты веб-сайта Adobo Chronicles, базирующегося на Филиппинах и позиционирующего себя как источник актуальных невероятных новостей. «Все, что вы читаете на сайте, основано на фактах. За исключением лжи», — говорится в описании ресурса.

Удивительно, как легко люди ведутся на фейки, когда заходит речь о вреде от новых технологий!

Чтобы расставить точки над «i» в истории с публикацией Adobo Chronicles, ученые (разумеется, британские) провели настоящее исследование[1] по шкале «селфитис», опубликованное на сайте вымышленных новостей. Они опросили более 200 индийских студентов и выяснили, что две трети студентов соответствуют критериям «селфитиса». Конечно, заболеванием это не считается, но тенденция была отмечена верно. Вот что отвечали студенты:

Возможность зафиксировать окружение: *«Селфи в определенных условиях помогает мне надолго запомнить этот момент».*

---

1 *An Exploratory Study of "Selfitis" and the Development of the Selfitis Behavior Scale/ Balakrishnan, J. & Griffiths, M.D. International Journal of Mental Health and Addiction (2018) 16: 722.* ***https://doi.org/10.1007/s11469-017-9844-x***

Социальная конкуренция: *«Я чувствую себя потерянным, когда мои друзья получают больше лайков и комментариев для селфи, чем я».*

В поисках внимания: *«Для меня главная причина того, чтобы делать селфи или публиковать их в социальных сетях, — возможность привлечь внимание».*

Изменение настроения: *«Иногда селфи помогает мне выходить из депрессивных мыслей».*

Самоуверенность: *«Я восхищаюсь собой и обретаю необычайную уверенность, когда вижу себя в селфи».*

Субъективное соответствие: *«Я чувствую себя оторванным от своей группы, если не делаю частые селфи».*

Короче говоря, селфи — не болезнь. Не спешите верить всему, что пишут в интернете, — пусть это и созвучно вашим внутренним ощущениям. Даже с нарциссизмом селфи напрямую не связано: далеко не все, кто делает селфи — нарциссы (хотя именно так обществом воспринимаются любители этого способа запечатлеть себя, особенно те, кто пользуется селфи-палкой); обратное утверждение, что все нарциссы любят селфи — тоже не получило научного доказательства (есть множество исследований на эту тему, которые противоречат друг другу).

В 1914 году, будучи тринадцатилетней, Великая княжна Анастасия Николаевна стала одной из первых, кто сделал селфи, чтобы отправить другу. Для этого она использовала собственное изображение в зеркале — это и сегодня один

из популярных способов самофотографирования. В письме, которое сопровождало фотографию, она написала: «Я сделала эту фотографию себя, смотрящей в зеркало. Мне было очень тяжело, потому что мои руки дрожали».

То, что психиатры не признают страсть к селфи болезнью, требующей лечения, не делает это занятие абсолютно безопасным. Достаточно всего одной неудачной попытки сделать захватывающий кадр, чтобы расстаться с жизнью. Тем не менее, раз за разом люди такие попытки совершают, желая удивить друзей, а если повезет, то и весь мир. Некоторым это действительно удается — увы, посмертно.

По данным глобального исследования[1], предпринятого в 2018 году (на этот раз индийскими учеными) для оценки смертей, связанных с селфи во всем мире, за период с 2011 по 2017 год зарегистрировано 137 подобных инцидентов, в которых погибли 259 человек. Разумеется, эта цифра не показывает истинный масштаб бедствия — исследователи включили в обзор только случаи, попавшие в газеты на английском языке.

Достаточно всего одной неудачной попытки сделать захватывающий кадр, чтобы расстаться с жизнью.

Было обнаружено также, что смертельные случаи, связанные с селфи, наиболее распространены в Индии, России, США и Пакистане. Средний возраст «героев» этих эпизодов составил около 23 лет, большая часть из них оказалась мужчинами (72,5%). Главными

1 *Journal of Family Medicine and Primary Care. 2018 Jul-Aug; 7(4): 828–831. doi: 10.4103/jfmpc.jfmpc_109_18*

причинами смерти во время съемки селфи являются утопление, несчастные случаи на транспорте (часто удар током) и падение с высоты. При этом селфи никогда не упоминается как официальная причина смерти. Например, дорожно-транспортные происшествия во время позирования для селфи регистрируются как смерть в результате ДТП, — таким образом, реальная статистика искажается.

Мотивы всех этих претендентов на «Премию Дарвина»[1], в принципе, понятны: глупая бравада, желание показать свою крутость, «безбашенность» или мегаоригинальность. К этому можно добавить обычное хвастовство («Смотрите, где я был»). По сообщению информационного портала The Telegraph, за 2015 год селфи унесли больше жизней, чем нападения акул. (А если акула напала на человека, снимающего селфи, — как это учитывать?). В «Википедии» даже есть целая страница, посвященная смертям и травмам, связанным с селфи, — List of selfie-related injuries and deaths[2].

В России увлечение селфи приняло настолько распространенный характер, что этим озаботилось МВД.

В России увлечение селфи приняло настолько распространенный характер, что этим озаботилось МВД и даже выпустило в 2015 году специ-

1 *«Премия Дарвина» (англ. Darwin Awards) — виртуальная антипремия, ежегодно присуждаемая лицам, которые наиболее глупым способом умерли или потеряли способность иметь детей, и в результате лишили себя возможности внести вклад в генофонд человечества, тем самым потенциально улучшив его. Хотя премия присуждается за «защиту генофонда», фатальная глупость ее победителей была не врожденной, а социально обусловленной, поэтому говорить о прогрессе генофонда человечества в данном случае некорректно. Довольно часто упоминается в связи с гибелью в процессе съемки селфи.*

2 *List of selfie-related injuries and deaths (Википедия).*

альную памятку. Особенно впечатляет, что по общей селфи-активности Москва в то время занимала только 301 место среди городов мира[1]. Похоже, что у российских подростков (а именно они чаще всего попадают в такие истории) тяга к риску сильнее прочих.

Безопасное селфи. Памятка МВД России

Ваше здоровье и ваша жизнь дороже миллионов лайков в соцсетях!

МВД России обеспокоено участившимися случаями травматизации и даже летального исхода при попытке сделать уникальное селфи. Каждый из таких случаев можно было предотвратить. Для этого в МВД России создана памятка «Безопасное селфи», призванная обратить внимание — в первую очередь, молодежи — на данную проблему. Мы попытались наглядно, в виде пиктограмм, изобразить наиболее травмоопасные случаи создания селфи, тем самым предостеречь граждан от неоправданного риска ради запоминающегося кадра.

Когда человек пытается сфотографировать сам себя — у него рассеяно внимание, теряется равновесие, он не смотрит по сторонам и не чувствует опасности. Делайте селфи, убедившись, что Вы находитесь в безопасном месте и вашей жизни ничего не угрожает!

Надеемся, что наше начинание поддержат во всех регионах, поддержит молодежь, взрослые и дети[2].

---

1 *The Selfiest Cities in the World: TIME's Definitive Ranking, // **TIME.com**, 10 марта 2014.*

2 *Безопасное селфи. // МВД РФ, официальный сайт, 2015.*

Многие откликнулись на эту инициативу и прислали собственные рекомендации, чего следует избегать, делая селфи. Например, недопустимо использовать металлическую палку для селфи во время грозы. В МВД учли эти предложения и подготовили новую версию «Памятки». В мире нашу инструкцию по безопасному селфи тоже заметили — Би-Би-Си рассказала о ней в своем материале, а Райан Тернер (Ryan Turner), автор блога Connecticut.Marketing, даже перевел ее на английский язык[1].

Отдельно стоит сказать, что экстремальные селфи пользуются большой популярностью у посетителей веб-сайтов. Видео на YouTube, в котором собраны так называемые «25 самых опасных селфи за всю историю»[2], было просмотрено более 40 миллионов раз. Соответственно, на подобный контент есть спрос. А раз так, то появляется и мотив на этом заработать.

Самое отвратительное, что есть люди, которые сами не рискуют собственной жизнью, но склоняют к этому других.

Но что самое отвратительное — есть люди, которые вместо того, чтобы рисковать собственной жизнью, склоняют к этому других. Предложение о такой «работе» заметили иркутские правоохранители: за опасное фото на краю крыши молодым симпатичным девушкам обещали две тысячи рублей. Почему именно девушкам? Видимо, парней уговаривать не надо, они и бесплатно готовы рисковать.

---

1 *Russian Selfie Guide In English. // Connecticut.Marketing, 8 июля 2015.*

2 *25 Most Dangerous Selfies Ever! // YouTube, 12 февраля 2015. (Кстати, фото с акулами оказались фейками).*

Что делать, если ребенок увлекся опасными селфи? Увы, простого рецепта нет. Когда вопрос относится к области психологии — а это именно тот случай — все очень индивидуально.

Если родителям стало известно об опасном увлечении — уже хорошо, потому что обычно подобные вещи дети держат в секрете. Первой обычно приходит мысль рассказать о смертельных случаях из-за селфи. Но одного ребенка это и вправду заставит задуматься, а другому вы, таким образом, только подскажете несколько новых идей. Кстати, никакой разницы в том, делает ли экстремальный снимок ваш ребенок сам или камеру держит его товарищ, нет — речь ведь идет не об авторских правах и чистоте стиля, а о жизни и смерти.

Проблема не в телефонах с камерами. Риск — бессмысленный и беспощадный — существовал и до их появления, просто не осталось документальных свидетельств творимых людьми глупостей.

Вспомните, как начинается фильм Андрея Звягинцева «Возвращение»: компания мальчишек прыгает с вышки в воду. Среди них двое братьев — Андрей и Иван. Все, кроме Ивана, прыгают, а он, не решаясь ни уйти, ни прыгнуть, остается сидеть на вышке. За ним приходит мать и, взволнованная, уговаривает уйти. Если бы у тех мальчишек были телефоны, они бы делали селфи. И точно также Иван оказался бы изгоем в компании и потом попытался бы доказать, что он не трус, — что в финале картины и привело к трагедии.

Чтобы пресечь поведение подростков, публикующих опасные селфи на своих страницах в соцсетях, депутаты предлагают штрафовать их родителей. Едва ли можно согласиться с тем, что эта мера

разумна, но нельзя отрицать, что ответственность все-таки лежит на взрослых, окружающих ребенка.

Нельзя отрицать, что ответственность все-таки лежит на взрослых, окружающих ребенка.

Что же делать?

Думайте, анализируйте, проконсультируйтесь с психологом. Однако, относитесь с осторожностью к советам специалистов: многие из них еще верят в мифическое заболевание «селфитис» и готовы винить во всем технологии. С такими вам точно не по пути!

Самый большой в мире магазин игрушек

Что дети любят больше всего на свете? Правильно, играть. Мобильный телефон для них — это, прежде всего, самый большой в мире магазин игрушек, который всегда под рукой. Неважно, айфон у вас или андроид — все равно выбор игр во много раз больше, чем в «Детском мире»: в App Store — 292 тысячи, в Google Play — 367 тысяч (по данным Statista.com на 1 кв. 2019 г.). Где вы еще найдете такое изобилие?

Современные малыши начинают осваивать мобильные игры где-то с двух лет, в 3–4 года в них играют 49% детей, в 5–8 лет — 75–76%, в 9–10 лет — 84%[1]. То есть почти все. Не опасно ли это для детского здоровья?

---

1 *Мобильные игры для детей: психологи не возражают. // Сайт* ***7ya.ru****, 12 августа 2016.*

Российские медики и психологи рекомендуют начинать использовать гаджеты с 2-3 лет, их американские коллеги считают, что и с годовалого возраста уже можно. Так что при соблюдении разумных ограничений ничего страшного в мобильных играх нет. А мультики детвора пока предпочитает смотреть по телевизору.

При соблюдении разумных ограничений ничего страшного в мобильных играх нет.

Наверное, вы в курсе, что не все игры в телефонах детские. Есть игры вполне себе 18+, которые ребенку лучше не видеть. Дело не только во взрослом контенте — игра не по возрасту, скорее всего, покажется ребенку слишком сложной или скучной, поэтому нужно обращать внимание на возрастную маркировку. Пока у ребенка не появится собственный гаджет, с этим проблем, казалось бы, нет: дали свой телефон поиграть, потом забрали телефон.

Да? Вы уверены, что проблем действительно нет? В безобидной игрушке категории 3+ вполне может всплыть реклама онлайн-казино, ваш любознательный ребенок сделает несколько движений своим пальчиком и, может быть, сорвет для вас джекпот в миллион долларов. Или (что более вероятно) благополучно успеет проиграть немного денег с вашей привязанной карты, пока вы заметите, чем он там занимается. Или переключится на «очень взрослую игру», которую подсунула реклама, и вам придется значительно расширить свои познания о сексе, чтобы ответить на его вопросы.

Финансовых потерь можно избежать, если не привязывать к аккаунту телефона свою основную карту.

Можно ли этого избежать? Финансовых потерь — да, если не привязывать к аккаунту телефона свою основную карту. Нежелательного, с вашей точки зрения, расширения кругозора ребенка — едва ли, поэтому будьте готовы ответить на любые неудобные вопросы. Спокойно и без паники! (Подробнее — в главе о нежелательном контенте).

> *Безусловно, каждому хочется сэкономить, поэтому мы скачиваем бесплатные игры. Но в этом случае сами становимся товаром: разработчик зарабатывает на показах рекламы и на покупках внутри приложения. Он делает процесс покупки максимально гладким и удобным, чтобы не отрывать вас от игры. Тут и себя-то с трудом удается контролировать, что уж говорить о ребенке!*

Может быть, устанавливать только платные игры? Вряд ли этот совет выполним. По статистике, менее 10% пользователей готовы платить за игрушки на телефонах. К тому же, в платных приложениях тоже часто встречается реклама, если только не было прямо заявлено, что после оплаты она исчезнет, да и в этом случае — не факт.

Конечно, мы понимаем, что игровой индустрии надо как-то жить, и если никто не будет смотреть рекламу, то новых игр мы тоже не увидим. Но эта ситуация нуждается в регулировании, которого пока нет даже в США, где базируются Apple и Google — владельцы мобильных платформ, управляющие рекламой. Конкретный разработчик просто определяет место в игре, где будет показано объявление или ролик. Он не знает, что именно будет показано, однако, в его интересах, чтобы реклама работала. Например, чтобы как можно больше игроков нажали кнопку «Установить» после показа демо новой игрушки в перерыве между уровнями.

И здрасьте-пожалуйста: вы долго выбирали ребенку хорошую «развивалку», а он уже гоняет монстров по подземельям. Вполне возможно, что он и сам этому не рад, — исследования показывают, что дети до 8 лет не различают рекламный контент, считая его частью самой игры, поэтому они будут попадаться на удочку манипуляторов-рекламщиков.

Исследования показывают, что дети до 8 лет не различают рекламный контент, считая его частью самой игры.

К сожалению, такая практика чрезвычайно широко распространена. Результаты исследования[1], проведенного доктором Дженни Радецки с коллегами, показали, что 95% приложений для детей 5 лет и младше содержат хотя бы один вид рекламы. Реклама была значительно более распространена в бесплатных приложениях (100% против 88% в платных приложениях), но столь же часто встречается в приложениях, помеченных как «образовательные», как и в других категориях. Эта «бомбардировка» рекламой подрывает большую часть образовательного контента, содержащегося в приложении, — дети просто не могут сосредоточиться.

Похоже, рекламщики уверены, что дети — это «еще более новая нефть». И при этом чувствуют полную безнаказанность. В некоторых случаях показ рекламы даже превосходит время, которое ребенок проводит в игре. Персонажи в играх мягко давят на детей, чтобы они делали покупки, — между прочим, такая практика, известная как host-selling, была в 1974 году запрещена в детских телевизионных программах Федеральной торговой комиссией.

1 *Advertising in Young Children's Apps: A Content Analysis // Journal of Developmental & Behavioral Pediatrics: January 2019 — Volume 40 — Issue 1 — p 32–39 // doi: 10.1097/DBP.0000000000000622*

В исследовании доктора Радецки приводятся конкретные примеры манипуляций:

- *В игре Olaf's Adventures от студии Disney нажатие на светящийся торт, который не отмечен как реклама, переносит игрока в магазин;*

- *В приложении Doctor Kids от Bubadu игровой персонаж плачет, если игрок нажимает на кнопку «Выйти из магазина».*

В другой ситуации Радецки позволила сыну поиграть в одну из игр по мотивам популярного российского анимационного сериала «Маша и Медведь». И тут всплыло нечто странное: «Это была реально жуткая мультипликационная версия Дональда Трампа, пытающегося сопротивляться нажатию большой красной кнопки с ядерным оружием, — рассказала Радецки. — Мой сын расстроился из-за карикатуры: „Подожди, а у Трампа в офисе есть такая кнопка?" — и я сказала себе: „О, здорово, теперь мне нужно это объяснить!"».

«Наши результаты показывают, что рынок приложений для детей раннего возраста — это настоящий Дикий Запад, и многие приложения больше ориентированы на зарабатывание денег, чем на игровой опыт ребенка, — делает вывод доктор Радецки. — Это должно иметь серьезные последствия для регулирования рекламы, этики дизайна детских приложений, а также для того, как родителям определить те детские приложения, которые стоит загружать».

Иначе говоря, каждый ответственный родитель должен сам протестировать игру, прежде чем давать ее ребенку. Если ребенок уже

выбирает и устанавливает игры самостоятельно, поиграйте вместе с ним. Объясните и покажите на примерах, что реклама — это не часть игры, научите игнорировать ее и не отвлекаться. Технических средств, чтобы блокировать рекламу внутри приложений, к сожалению, нет.

> *Попытка встревоженных всеобщей цифровизацией родителей вовсе оградить детей от мобильных устройств будет иметь негативные последствия, потому что ребенок не получит тех навыков и знаний, которые есть у большинства сверстников.*

В некоторых школах планшеты используются в учебном процессе уже с первого класса, и воспитанный в аналоговом мире ребенок окажется к цифровой среде ничуть не более приспособленным, чем Маугли, выросший в джунглях. Хорошо, что дети быстро обучаются, — он, конечно, догонит одноклассников, но некоторые умения трудно приобрести в «зрелом» возрасте. Просто посмотрите, как подростки набирают текст на телефоне, и сравните с тем, как это делаете вы: такой скорости и легкости никогда не достичь тем, кто с раннего детства не «тыкал» пальчиками в экраны. Недаром будущих музыкантов и спортсменов начинают готовить с дошкольного возраста — потом уже поздно.

Полезно будет ознакомиться с докладом «Дети. Медиапотребление. 2017», основанного на данных уникального комплекса из 25 исследований, проведенных Институтом современных медиа (MOMRI)[1].

---

1 *Ежегодный доклад «Дети. Медиапотребление. 2017» // Сайт* ***momri.org****, март 2018. (К сожалению, доклад не стал ежегодным — как было заявлено авторами, это единственный выпуск).*

Половина детей довольна временем, которое дома отводится на мобильные и компьютерные игры (46%). Каждый третий ребенок жалуется, что ему такого времени не хватает, и он хотел бы играть больше.

Начиная с 10 лет некоторые дети ложатся спать около полуночи, потому что им нужно приготовить много уроков на следующий день. А им еще хочется поиграть, пообщаться онлайн. Есть подростки, которые играют по ночам, — если нет четкого запрета, который установлен с самого раннего возраста.

Чем старше ребенок, тем чаще он играет или один (их число растет с 53% до 71%), или с друзьями (с 5% до 27%). С родителями в младшем возрасте играют 43%, в возрасте 6–9 лет — 19% и в возрасте от 10 до 12 лет — лишь 8%.

Большинство детей в возрасте от 2 до 12 лет (64%) играют в несколько игр одновременно: чем меньше возраст детей, тем чаще они играют в несколько игр сразу. Чаще всего дети играют в 2–3 игры параллельно.

Компьютерные и мобильные игры — одна из тем, которая обсуждается в детской среде, начиная с детского сада (50%). Рост интереса к обсуждению игровых тем у девочек отмечается в младшем подростковом возрасте (+17%). Доля мальчиков, коммуникации которых строятся вокруг игровых историй, растет непрерывно: в 3–5 лет — 49%, в 6–9 лет — 65%, в 10–13 лет — 78%.

Девочки играют на смартфонах и планшетах больше, чем мальчики, а на компьютерах и ноутбуках — меньше. Мальчики, в це-

лом, чаще играют: среди девочек практически нет «игроманов», которые играют более 3 часов в день ежедневно. Девочки чаще всего играют несколько раз в неделю.

Если родители сами играют в компьютерные игры, то они чаще узнают информацию об играх из магазина приложений или видят рекламу в интернете; неиграющие родители чаще прислушиваются к мнению ребенка.

Чем старше ребенок, тем реже он прибегает к помощи старших для скачивания игр и чаще делает это сам: в возрасте от 2 до 5 лет мама скачивает игры в 33% случаев, сам ребенок — в 19%; в возрасте от 10 до 12 лет это соотношение уже 13% к 65%. Помощь отца практически одинаково востребована во всех возрастах.

Большинство родителей в России (72%) знают о развивающем потенциале мобильных игр; до половины детей (39%) используют развивающие приложения, но лишь небольшая часть родителей рассматривает мобильные игры как формат совместной деятельности с ребенком.

76% родителей играют в развивающие игры с детьми, но используют при этом планшет только 15%. Одной из существенных причин такой ситуации является отсутствие подобного опыта в собственном детстве и дефицит достоверной информации о том, как взаимодействовать с гаджетом, как правильно интегрировать его в жизнь ребенка.

Так что осваивайте игры вместе с детьми. Если вас смущает, что кто-то застанет вас за этим занятием, скажите, что проводите исследование.

Правда, есть риск, что вам тоже понравится.

«Ноль по поведению», или Телефон в школе

Школа — очень древний институт, который не претерпел существенных изменений со времен Аристотеля. Учитель говорит — ученики внемлют. Любое нарушение дисциплины нещадно карается. Понятно, что в такой обстановке смартфон в портфеле есть великий соблазн для ученика, ведь с его помощью можно ускользнуть со скучного урока в виртуальный мир, где он полностью свободен.

Ученик прекрасно знает, что это бунт, но удержаться не может, пусть бы ему за это и вкатили «Ноль по поведению».

Ученик прекрасно знает, что это бунт, но удержаться не может, пусть бы ему за это и вкатили «Ноль по поведению», как юным героям фильма Жана Виго[1], сотворившим вполне невинную шалость и получившим за это самое суровое наказание. «Ноль по поведению» во французской школе-пансионе означает, что учеников не отпустят на выходные домой, и эта явная несправедливость становится поводом для бунта. Если бы действие фильма происходило в наши дни, то, несомненно, причиной стал бы смартфон, а в конце фильма мальчишки не ушли бы вдаль по крышам, а нырнули бы в цифровое пространство.

1 *«Ноль по поведению» — фильм Жана Виго, снятый в 1933 году. Картина была запрещена во Франции до 1946 года из-за показа в невыгодном свете и высмеивания учителей, и государственной власти. Цензоры, как обычно, перестарались: по духу это примерно наша «Республика ШКИД» — никакой особой крамолы и подрыва устоев там нет, просто правда жизни подана в сюрреалистическом ключе.*

По меркам существования столь древнего образовательного института как школа, мобильники появились буквально мгновение назад, и школа просто не знает, как на них адекватно реагировать.

Современные технологии еще не интегрированы глубоко в образовательный процесс и часто мешают его плавному и неторопливому течению. Поэтому телефоны в школах пытаются запретить.

Выполняя свое предвыборное обещание, президент Эммануэль Макрон добился принятия закона, по которому с сентября 2018 года французским школьникам запрещено пользоваться мобильными телефонами где-либо на школьной территории. (Надо сказать, что, начиная с 2010 года, Французский кодекс образования уже и так запрещает мобильные телефоны «во время любой учебной деятельности»; новый же закон изгнал гаджеты не только с уроков, но и со школьного двора).

Макрон сделал запрет на использование телефонов в школах частью своего избирательного манифеста вскоре после того, как мэр Нью-Йорка Билл де Блазио сделал обратное: отменил запрет на телефоны в государственных школах в 2015 году, заявив, что родители хотят поддерживать связь со своими детьми.

Сопоставив эти факты, можно сделать вывод, что в мире нет единой научно обоснованной политики относительно присутствия телефонов в школьной жизни. Решения принимаются политиками, которые просто пытаются угодить своим избирателям, и это не может не настораживать — популизм плохой советчик для педагогики. Одно радует: дети очень адаптивны и легко приспосабливаются к самым нелепым правилам, которые изобретают взрослые.

Французские школьники после введения запрета на гаджеты стали приносить в школу пачки карточек, чтобы играть на перемене, а некоторые — даже книги! Кроме того, было замечено, что ученики разговаривали друг с другом больше, чем раньше. С одной стороны, можно праздновать победу над «цифрой», которая чуть не поработила детей, но с другой — они сами признаются, что компенсируют вынужденное воздержание после уроков.

Корреспондент Guardian спросила у школьных ворот 14-летнюю девочку, что она чувствует по этому поводу. «Существует мнение, что наше поколение не может сосредоточиться или утратило способность общаться. Это неправда, — ответила та. — Когда я нахожусь с друзьями, я показываю им фотографии на телефоне или что-то ищу, и это только добавляет интереса нашему разговору. Жаль, что я больше не могу делать этого в школе»[1].

«Запрет на то, что так важно в жизни учащегося, превращает это в подпольную деятельность».

Некоторые специалисты указывают на негативные последствия запретов. Антонио Вендрамин, директор школьного округа Суррей в Британской Колумбии говорит: «Запрет на то, что так важно в жизни учащегося, превращает это в подпольную деятельность». Он считает, что молодые студенты нуждаются в совете и руководстве при использовании новых технологий, и что образование и технологии не являются чем-то несовместимым.

Если удалось донести до студентов идею, что телефон может быть инструментом обучения, это работает гораздо эффективнее, чем запрет.

1 *'It's pretty easy to talk instead': pupils react to French phone ban. // The Guardian, 7 сентября 2018.*

В ходе исследования, касавшегося использования телефона в школе и охватившего 4000 участников, Вендрамин нашел ряд возможных решений этой проблемы. Например, один учитель просил учеников положить телефон на угол стола экраном вниз и выключить звук. Иногда во время урока он предлагал им воспользоваться телефонами для поиска информации в интернете. Таким образом, преподавателю удалось донести до студентов идею, что телефон может быть инструментом обучения, — и это работало гораздо эффективнее, чем запрет, поскольку способствовало возникновению уважения и доверия между учащимися и учителем.

Что касается России, то, по заявлению главы Рособрнадзора (ныне — Министра просвещения) Сергея Кравцова, введение в школах запрета на гаджеты не планируется. Однако проблема эта вызывает в ведомстве озабоченность. В августе 2019 года Роспотребнадзор, Минпросвещения, Рособрнадзор и Российская академия образования подготовили методические рекомендации[1], касающиеся порядка использования личных устройств мобильной связи в общеобразовательных организациях.

Как сообщается в пресс-релизе Рособрнадзора, в ходе опроса 61% обучающихся, 89% родителей и 90% педагогов поддержали ограничение использования мобильных телефонов школьниками во время уроков. Около трех четвертей опрошенных считают, что и педагоги, находясь в школе, должны ограничить использование сотового телефона в личных це-

1 *Роспотребнадзор, Минпросвещения и Рособрнадзор рекомендуют рассмотреть вопрос об ограничении использования мобильных телефонов в школах. // Рособрнадзор, официальный сайт, 19 августа 2019.*

лях в присутствии обучающихся. Более половины школьников согласны с тем, что неупорядоченное использование мобильных телефонов может нанести вред их здоровью и отвлекает от учебного процесса. Среди взрослых участников опроса (родителей и педагогов) с этими утверждениями согласны 83-90% опрошенных.

К сожалению, реальной пользы от этой «методички» мало. Пожалуй, единственный практический совет, который в ней содержится, гласит, что целесообразно переводить устройства мобильной связи в режим «без звука» при входе в образовательную организацию, а также ограничить их использование школьниками во время учебного процесса.

В некоторых школах перед началом первого урока у детей собирают все телефоны и уносят в учительскую до конца учебного дня. Уходя из школы, дети забирают свои телефоны. Никаких проблем родителям это не создает, а учителям так лучше работается. Родители при этом совершенно не против (не говоря о том, что их никто не спрашивает, если в школе приняты такие правила). Между тем, с юридической точки зрения, практика сбора телефонов у детей спорна, хотя распространена в школах достаточно широко. При этом часто игнорируются риски, связанные с возможной пропажей или поломкой телефона, пока он пребывает в «красивом ящичке».

С юридической точки зрения, практика сбора телефонов у детей спорна, хотя распространена в школах достаточно широко.

Давайте рассмотрим, какая сделка происходит между учителем учеником в момент, когда последний кладет мобильный в коробку. На ум приходит только один вид сделки, подходящий под эту ситуацию: хранение.

По договору хранения одна сторона (хранитель) обязуется хранить вещь, переданную ей другой стороной (поклажедателем), и возвратить эту вещь в сохранности (ст. 886 ГК РФ). Хотя договор хранения и предусматривает простую письменную форму, отсутствие таковой не означает ничтожности сделки (в конце статьи будет приведен в качестве примера судебный акт), и, в соответствии с п.3 ст.887 ГК РФ, несоблюдение простой письменной формы договора хранения не лишает стороны права ссылаться на свидетельские показания в случае спора о тождестве вещи, принятой на хранение, и вещи, возвращенной хранителем.

По окончанию срока хранения (урока) хранитель (учитель) обязан возвратить поклажедателю (ученику) ту самую вещь, которая была передана на хранение (п. 1 ст. 900 ГК РФ).

Хранитель отвечает за утрату, недостачу или повреждение вещей, принятых на хранение, по основаниям, предусмотренным ст. 401 ГК РФ (п.1 ст. 901 ГК РФ). Согласно п. 2 ст. 401 ГК РФ отсутствие вины доказывается лицом, нарушившим обязательство.

При безвозмездном хранении убытки, причиненные поклажедателю (ученику) повреждением вещей (утраты), возмещаются: за утрату и недостачу вещей — в размере стоимости утраченных или недостающих вещей; за повреждение вещей — в размере суммы, на которую понизилась их стоимость (п. 2 ст. 902 ГК РФ).

Пока неизвестно об инцидентах, связанных с пропажей детских телефонов во время хранения. Возможно, потому, что такая практика чаще встречается в частных школах, — когда в классе всего пять человек, это не выглядит проблемой. Если же решение будет растиражировано в масштабах страны, едва ли можно будет гарантировать

безопасность хранения всех устройств. Риск для педагогов и администрации школ станет вполне реальным.

Есть, однако, родители, которые считают, что быть на связи — это право любого человека, даже маленького. Если же кто-то злоупотребляет этим правом в ущерб остальным, то преподаватель должен, в свою очередь, иметь право воздействия: потребовать убрать телефон, поставить «Ноль по поведению», вызвать родителей и так далее — применить весь школьный арсенал дисциплинарных взысканий.

> *Просто взять и отнять телефон у ребенка нельзя. С точки зрения закона, в этом случае учитель ничем не лучше «гопника» в подворотне, — это будет изъятие чужой собственности со всеми вытекающими юридическими последствиями.*

Школа не тюрьма, чтобы ограничивать возможность коммуникации, — в частности, с родителями. Если ребенок не учится, а играет в телефоне, но при этом никому не мешает, он в своем праве: получит «неуд», но это его проблема. Вместо того, чтобы бороться с этим неприятным, но относительно безобидным явлением, учителям неплохо бы обращать больше внимания на тех, кто активно мешает учиться другим и проявляет агрессию.

Между тем, мобильный телефон сегодня стал инструментом разоблачения разных неприглядных историй, которые происходят в школе, в том числе и при участии учителей. И не только разоблачения, но и противодействия — такая точка зрения, кстати, распространена в США, где в школах с печальной регулярностью происходят вооруженные нападения, и мобильный телефон может оказаться единственным средством спасения и вызова полиции. Вы только представьте себе, что в школе — стрельба, а все телефоны заперты в учительской...

Представьте себе, что в школе — стрельба, а все телефоны заперты в учительской...

Если бы вместо чиновников от образования, активистов-общественников, юристов, встревоженных учителей и родителей вопрос доверили бы решать инженерам, то всех этих безрезультатных дискуссий и принятия неоднозначных законов можно было бы избежать. Достаточно вспомнить, что смартфон — это карманный компьютер, который может управляться, в том числе, и удаленно, внешним администратором. И что проблема школы не в наличии устройства у учеников, а в том, что они его используют неподобающим образом, мешая уроку.

> *«Мобильный телефон — это реальность наших детей, нравится нам это или нет. Мы можем сколько угодно возмущаться: мол, мы на переменах во дворе носились, воздухом дышали, а эти — в мобильниках сидят. От наших криков и запретов они из своих телефонов не вылезут. Мы хотим украсть у детей ту реальность, в которой они живут, которую любят, без которой будут страдать, и к которой нам, взрослым, все равно придется привыкнуть, потому что она возникла объективно», — считает журналист, писатель, драматург, радио- и телеведущий, сценарист и театральный режиссер Андрей Максимов*[1].

Между тем, уже существуют приложения, позволяющие автоматизировать школьные правила[2]. Нет никакой необходимости изымать гаджет у ребенка, когда можно просто запретить использование всех приложений во время урока, кроме тех, которые могут понадобиться (например, каль-

---

1 *«Наших детей обидят и в этот раз». Андрей Максимов — об идее отнять у школьников смартфоны. // Правмир, 27 августа 2019.*

2 *Например, сервис «яРядом»* ***https://www.imnear.ru/***

кулятор). Техническими средствами можно ограничить и использование приложений на определенной территории, в том числе — на школьном дворе. Если бы французский президент больше консультировался с айтишниками, а не с чиновниками и политтехнологами, то не было бы никакой нужды принимать обещанный им закон в форме тотального запрета, — достаточно было бы внедрить систему по управлению мобильными устройствами и установить ее на телефоны учащихся.

Нет никакой необходимости изымать гаджет у ребенка. Можно просто на программном уровне запретить использование всех приложений во время уроков.

При этом ребенок остается на связи с родителями — звонки возможны, но телефон автоматически переводится в беззвучный режим. Когда ребенок покидает школу, все его функции восстанавливаются в полном объеме.

У меня зазвонил телефон. Кто говорит?

Александр Белл, долгие годы считавшийся создателем телефона, пользоваться своим изобретением[1] не любил. Ученый утверждал, что телефонные звонки отвлекают его от работы и размышлений.

Наверное, ему бы пришлось по душе изобретение Стива Джобса, превратившее телефон из аппарата для совершения звонков

1 *11 июня 2002 года Конгресс США в резолюции №269 признал, что первенство в изобретении телефона принадлежит итальянцу Антонио Меуччи, который подал заявку на соответствующий патент в 1871 году, а также то, что Белл потенциально мог иметь доступ к материалам Меуччи (Википедия).*

в удивительный прибор, позволяющий заниматься разнообразными делами, в том числе общаться письменно и отвечать в удобное для себя время. В наши дни правилом хорошего тона стало сначала договориться о звонке в мессенджере, а потом уже звонить, — раньше для этого нужно было бы обменяться телеграммами; возможно, кто-то так и поступал. Надо сказать, что такой способ коммуникации будет уместен и в отношении ребенка, когда он находится в школе, особенно, если вы не знаете точно его расписание: неожиданный звонок от мамы в середине урока может поставить его в неловкое положение. Точно также и звонок ребенка в разгар важного совещания будет весьма некстати для любого из родителей. Разумеется, этим правилом можно пренебречь в экстренных ситуациях.

В наши дни правилом хорошего тона стало сначала договориться о звонке в мессенджере, а потом уже звонить.

К сожалению, всегда найдутся люди, готовые ворваться к вам своим телефонным звонком безо всякого предупреждения. Ладно бы, это были только близкие или друзья, которым мы готовы простить небольшое беспокойство и будем даже рады их слышать. Проблема в том, что на другом конце провода (хотя какие теперь провода?) может оказаться совсем незнакомый человек с отнюдь недобрыми намерениями. Конечно, непосредственно по телефону никто вам вреда причинить не может (вы же не верите в страшилки типа старого японского ужастика «Звонок», где все, услышавшие странный голос по телефону, через неделю умирали). Но ваш неожиданный собеседник может, в лучшем случае, отнять время на бесполезный разговор, а в худшем — задействует арсенал методов социальной инженерии и оставит вас в серьезном минусе.

Современные злоумышленники весьма искусны и способны «развести» на деньги практически любого, даже самого подготовленного специалиста по противодействию телефонному мошенничеству.

По статистике чаще всего жертвами телефонных мошенников становятся пожилые люди, но не только — дети тоже находятся в зоне риска. Например, во Владивостоке некоторое время назад в дежурную часть стали обращаться родители маленьких детей с заявлениями о том, что, пока их ребенок находился дома один, на домашний телефон позвонил «дядя» и попросил собрать все ценные вещи и скинуть их в окно. И ведь дети это делали![1]

Если у вас в квартире все еще есть стационарный телефон, объясните ребенку, что не следует отвечать на его звонки, а сами звоните своему чаду только на мобильный — ничего другого тут не посоветуешь. Что же касается звонков на мобильный, то давайте остановимся на технических средствах, которые могут снизить риск контакта с мошенником.

Кроме преступников, использующих телефон в уголовно наказуемых целях, есть огромная проблема телефонного спама.

Кроме явных преступников, использующих телефон в своих уголовно наказуемых целях, есть еще огромная проблема телефонного спама. Вам начинают названивать страховые агенты, сотрудники банков, брокеры, продавцы пластиковых окон, пылесосов и тысячи других вовсе не обязательно нужных вам вещей; вам надоедают разнообразными социологическими и маркетинговыми опросами.

---

1 *Телефонное мошенничество стало эпидемией. // **PrimaMedia.ru**, 17 февраля 2011.*

По данным «Лаборатории Касперского», спамерские звонки получают в России примерно три из четырех владельцев смартфонов (72%). Чаще всего спамеры звонят в четверг и пятницу, в интервале между 16 и 18 часами. С вероятностью 70% звонок человеку с неизвестного номера окажется спамом.

От всего этого хочется отгородиться самим и оградить детей. Ведь когда вы покупаете сим-карту для ребенка, то оформлять ее приходится на себя[1]. Соответственно, у спамеров, которые каким-то образом раздобудут базу телефонных номеров, нет возможности различить, где взрослый телефон, а где детский, и они будут названивать по всем подряд.

Особо назойливых абонентов можно занести в черный список — такая возможность появилась в телефонии уже очень давно. Когда не было смартфонов, эту услугу предоставлял оператор связи. Сейчас такая функция есть во всех современных аппаратах — обычно она называется «блокировка контактов» или близко к тому. В ответ на свой вызов звонящий услышит только короткие гудки — ваш номер для него всегда будет занят.

Однако количество спамеров настолько возросло, и они научились так часто менять свои номера, что черный список не решает проблему: вы устанете его пополнять. К счастью, разработчики уже проделали за вас эту работу и составили базу спам-номеров, которая постоянно пополняется,

1 *Если точнее, то это действует для детей младше 14 лет. С 14 лет можно оформить номер непосредственно на ребенка, но договор заключается только в присутствии одного из родителей или опекуна.*

в том числе самими пользователями. Установите на телефон себе и ребенку приложение Kaspersky Who Calls, включите в нем блокировку спам-звонков и ваша жизнь станет гораздо спокойнее[1]. Решайте, отвечать ли на звонок после того, как увидите название компании звонящего, адрес, категорию и сведения о ее репутации. (На телефонах iPhone будет отображаться только название компании). Однако, если звонящий скрывает свой номер телефона, Kaspersky Who Calls не сможет определить, кто это[2].

Кроме того, в телефоне есть возможность заблокировать все звонки с неизвестных номеров. В этом случае вы увидите вызовы только с тех с номеров, которые есть в вашем списке контактов. Можно также настроить черный и белый списки в личном кабинете вашего оператора связи.

В общем-то, все знают о черных и белых списках, но далеко не все этим пользуются. А зря! Это простое решение может избавить вашего ребенка от нежелательных звонков, и практически сведет к нулю риск, что он попадется на удочку телефонных мошенников. Не поленитесь, настройте на его телефоне белый список, включив туда близких родственников и друзей, с которыми ваш сын или дочь регулярно общаются.

Взрослые едва ли могут себе позволить ограничить круг общения только белым списком — им приходится отвечать на разные звонки, со знакомых и незнакомых номеров. Если спамеров можно

---

1 *В бесплатной версии Kaspersky Who Calls требуется доступ в интернет, а платная загружает базу номеров на ваш телефон и работает офлайн.*

2 *См.* ***https://www.kaspersky.ru/free-caller-id***

отсечь при помощи специальных приложений, то против мошенников, которые научились подменять свой номер на номер уважаемого учреждения, например, вашего банка, никакие списки и определители номеров не помогут. Так что не теряйте бдительности!

Против мошенников, подменяющих свой номер на номер, например, вашего банка, никакие списки и определители номеров не помогут.

Не меньше хлопот доставляет людям и SMS-спам. Раньше это вообще было стихийным бедствием — рекламные рассылки делали все, кому не лень. Проблема разрослась до такого масштаба, что в 2014 году Госдума приняла поправки в закон о связи, запрещающие рассылать SMS, на которые абонент не подписывался. А с 1 января 2018 года запрещены анонимные SMS и голосовые рассылки. Тем не менее, интернет пестрит предложениями об организации спам-рассылок на любые сотовые номера, причем технически это настолько просто, что с задачей справится кто угодно.

Если голосовой спам опасен тем, что вас могут уговорить на совершение невыгодных и опасных для себя действий, то главная опасность SMS — это ссылки в теле сообщения. Одно неловкое движение — и вирус или вредоносная программа у вас в телефоне. Думаете, ребенку будет легко устоять от искушения, когда ему предложат сотни бесплатных игр? Или когда придет MMS с текстом «Скорее открой прикольное фото»? После установки вируса могут произойти любые «чудеса», например, спишутся все деньги со счета телефона или с привязанной к нему банковской карты.

Как это делается? Например, вирус может заставить ваш телефон позвонить или отправить SMS на дорогой плат-

ный номер, причем без всяких видимых признаков. Вы это заметите, только когда получите счет от вашего мобильного оператора. Платные звонки и отправка текстовых сообщений с большого количества зараженных телефонов становятся для преступников неплохим источником дохода. А сам платный номер окажется в какой-то далекой стране: жуликов там наша полиция искать не будет, и деньги вам никто не вернет.

Главное правило, которое надо усвоить: никогда не открывайте ссылки из подозрительных сообщений! Вроде бы очень просто, да? Но как отличить подозрительные сообщения от нормальных?

Прежде всего, все сообщения с незнакомых или скрытых номеров — подозрительные. Удаляйте их сразу. А чтобы не искушать судьбу, все-таки настройте блокировку спама на своем телефоне и обязательно на телефоне ребенка.

Все сообщения с незнакомых или скрытых номеров — подозрительные. Удаляйте их сразу.

Хорошо, а если ссылку на фото прислал знакомый человек? И даже подписался своим смешным прозвищем. Стоп-стоп-стоп! Это может быть ловушка! Возможно, что ваш сын, дочь, папа, мама, бабушка, дедушка, начальник, лучший друг, заклятый враг, одноклассник, которого вы не видели лет двадцать, тренер по боксу или йоге — кто угодно из тех, у кого мог быть записан ваш телефон, — не был достаточно осторожен и таки словил себе вирус. Обустроившись на телефоне жертвы, вирус забирается в список контактов и начинает от имени ничего не подозревающего человека рассылать сообщения его знакомым.

Сами понимаете, что против такого приема блокировка по черным и белым спискам не поможет. Сообщение придет из доверенного источника — и почему бы сразу не открыть его? Не спешите. Перезвоните и спросите, что это за ссылку вам прислали и с какой целью. Письменно вам может ответить и злоумышленник, поэтому звонок будет надежнее. Или напишите по другому каналу связи, например, через мессенджер. Если вы услышите разумное объяснение от известного вам человека, то, скорее всего, эту ссылку можно открыть. Однако часто оказывается, что это активность вируса, и ваш знакомый будет вам благодарен за информацию.

Кстати, если вы не хотите понапрасну пугать своих друзей, не отправляйте им ссылки без внятного сопроводительного текста. Современный цифровой этикет предполагает, что сначала нужно немного пообщаться, прежде чем кидать человеку ссылку или какой-то файл.

По секрету всему свету

Анонимность и телефон — вещи взаимоисключающие. Интуитивно это все знали и до эпохи мобильников: коснувшись в беседе какой-нибудь деликатной темы, говорили «Это не телефонный разговор». Сегодня ситуация только усугубилась. Все, что вы делаете при помощи телефона, видно спецслужбам (причем разных стран, а не только нашим родным), владельцам платформ (Apple и Google), производителям разнообразных телефонов на Android, операторам связи, интернет-провайдерам, владельцам wi-fi и просто случайным людям, которые заглядывают вам через плечо. Подробно об этом уже сказано в главе, посвященной анонимности

в интернете. Но вот несколько важных вещей, которые стоит особо упомянуть применительно к мобильному телефону.

С мобильного телефона нельзя делать никаких анонимных звонков и SMS.

С мобильного телефона нельзя делать никаких анонимных звонков и SMS. Никаких обидных розыгрышей, угроз, дерзких постов в соцсетях. Никаких глупых выходок вроде звонка о том, что в школе заложена бомба, чтобы отменили контрольную. Даже с «левой» симки, купленной у вокзала. Вас все равно найдут и очень просто. У телефона есть уникальный номер IMEI[1]. Раньше в нем стояла ваша симка, привязанная к договору со всем вашими персональными данными, потом была другая, а теперь снова ваша. Думаете, трудно связать эти факты?

Нельзя давать свой мобильный телефон незнакомым людям.

Из этого вытекает важное следствие: не давайте свой телефон незнакомым людям. Мало того, что его могут просто не вернуть; все, что будет сделано с его помощью, припишут вам, и доказать обратное будет очень сложно. Да, но как же быть, если кому-то действительно нужна помощь? Очень просто: держите свой телефон в руках, попросите человека назвать номер и включите громкую

1 *IMEI (International Mobile Equipment Identity — международный идентификатор мобильного оборудования) — это уникальный 15-разрядный номер для идентификации телефонов. Как правило, IMEI указывается в четырех местах: в самом аппарате (в большинстве случаев его можно вывести на экран набором *#06# на клавиатуре), под аккумуляторной батареей, на упаковке и в гарантийном талоне. IMEI играет роль серийного номера аппарата при авторизации в Сети, передается в эфир при авторизации в Сети.*

связь. Лучше показаться невежливым, чем остаться без телефона и получить кучу проблем.

Для все большего числа людей телефон становится основным (а порой и единственным) каналом выхода в интернет. Это, несомненно, радует рекламодателей, потому что мобильных пользователей им отслеживать гораздо проще. Когда навязчивая реклама превратилась в настоящее бедствие, с ней стали бороться с помощью блокировщиков и анонимайзеров, и достаточно в этом преуспели — теперь технологии, препятствующие отслеживанию, встраиваются во все популярные браузеры, не говоря уже о том, что есть и специальные плагины, которые можно себе установить.

Каждый смартфон, благодаря наличию в нем кучи датчиков, еще более уникален, чем персональный компьютер.

Однако смартфоны в этом смысле по-прежнему уязвимы. Дело в том, что каждый смартфон, благодаря наличию в нем кучи датчиков, еще более уникален, чем персональный компьютер. Каждый датчик — это миниатюрный физический прибор, требующий калибровки, а набор калибровочных параметров формирует уникальный «отпечаток» конкретного аппарата, который не изменятся даже после переустановки операционной системы и сброса настроек к заводским параметрам.

> *Современные мобильные устройства поставляются с различными встроенными датчиками, такими как акселерометр, гироскоп и магнитометр. Мобильные приложения полагаются на эти датчики, чтобы обеспечить богатую функциональность: отслеживание тренировок, улучшение взаимодействия с пользовательским интерфейсом и повышение*

производительности игр. Естественная вариация при изготовлении встроенных датчиков означает, что выход каждого датчика уникален, и поэтому они могут быть использованы для создания «отпечатков пальцев» устройства.

Датчики движения, используемые в современных смартфонах (включая акселерометр, гироскоп и магнитометр), основаны на технологии MEMS (Micro-Electro-Mechanical Systems)[1]. Акселерометр и гироскоп измеряют ускорение и скорость вращения устройства по каждой из осей соответственно. Большинство смартфонов и смарт-часов оснащены одним трехосным акселерометром и одним трехосным гироскопом. Магнитометр измеряет магнитное поле Земли относительно устройства, он также есть в большинстве моделей.

Хотя технология MEMS значительно сократила размер и стоимость датчиков движения, датчики MEMS обычно менее точны, чем их полноразмерные аналоги, из-за различных типов ошибок. Многие коммерческие датчики откалиброваны на фабрике, а параметры калибровки хранятся в прошивке, обеспечивая точные измерения без предварительной калибровки. В отличие от этого, датчики, встроенные в недорогие смартфоны, как правило, плохо откалиброваны из-за высокой стоимости и сложности заводской калибровки.

---

1 *Микроэлектромеханические системы (МЭМС) — устройства, объединяющие в себе микроэлектронные и микромеханические компоненты. МЭМС-устройства обычно изготавливают на кремниевой подложке с помощью технологии микрообработки, аналогично технологии изготовления однокристальных интегральных микросхем. Типичные размеры микромеханических элементов лежат в диапазоне от 1 микрометра до 100 микрометров, тогда как размеры кристалла МЭМС-микросхемы имеют размеры от 20 микрометров до 1 миллиметра (Википедия).*

Авторы новой методики берут данные калибровки каждого устройства из таких датчиков, как гироскоп, акселерометр и магнитометр. Они выбрали эти датчики, потому что каких-либо специальных разрешений для доступа к ним не требуется: данные акселерометра и гироскопа могут быть доступны как через родное приложение, установленное на устройстве, так и через JavaScript, когда пользователь посещает веб-сайт. Пока исследователи сосредоточились на датчиках движения, но ожидается, что отпечаток на основе калибровки может быть создан для других датчиков на различных устройствах, включая камеру, сенсорный экран и батарею[1].

Среди широкой публики распространено мнение, что через телефоны нас постоянно подслушивают. В подтверждение этому обычно приводят истории, как кто-то произнес слово, а потом эта реклама появилась у него в ленте, хотя человек (как он сам клятвенно заявляет) поисков по этой теме не выполнял и в переписке ни с кем этого вопроса не касался — ни в почте, ни в мессенджерах. Нельзя отрицать, что телефон собирает множество данных о пользователе, и что эти данные любят анализировать как рекламные фирмы, так и спецслужбы — каждая в своих интересах. Но слишком демонизировать технологии все же не стоит.

Специалисты из компании Wandera решили проверить опасения пользователей[2]*. Взяли два телефона и поместили один в «аудиокомнату», где звучала реклама, а другой — в звуко-*

---

1 *SENSORID: Sensor Calibration Fingerprinting for Smartphones. Jiexin Zhang, Alastair R. Beresford (University of Cambridge), Ian Sheret (Polymath Insight Limited) // IEEE-Security.org, 5 мая 2019.*

2 *Вас подслушивает телефон: миф или реальность? // Русская служба BBC, 5 сентября 2019.*

изолированную комнату. На телефонах были запущены приложения соцсетей. Потом проверили наличие рекламы в обоих и проанализировали расход батарей и трафик. Активность телефонов в «аудиокомнате» и звукоизолированной комнате была идентичной. Это означает, что телефон не ведет аудиозапись и не передает данные на сервер, считают исследователи. Если бы это происходило, то нагрузка на телефон была бы такой же, как при использовании голосовых помощников.

То есть рассказы о тотальной прослушке (и тем более подглядывании) при помощи мобильных телефонов можно отнести к области мифов. Владельцы платформ просто не располагают достаточными техническими ресурсами, чтобы прослушивать миллиарды пользователей в режиме 24/7, это факт. А вот истории о выборочном прослушивании частных разговоров подтвердились.

В частности, компания Apple извинилась перед пользователями устройств после того, как выяснилось, что она нанимала субподрядчиков, которые имели возможность слушать записи разговоров, происходивших вблизи айфонов, — как утверждается, для контроля качества распознавания речи голосовым помощником. Теперь пользователи могут выбрать, соглашаться или нет на мониторинг качества распознавания их речи. Только у тех пользователей, кто прямо даст на это согласие, записи разговоров будут доступны для прослушивания человеком[1].

Пользователи могут выбрать, соглашаться или нет на мониторинг качества распознавания их речи.

1 *Siri слушала, записывала и расшифровывала разговоры окружающих. Apple обещает, что больше не будет. // Русская служба BBC, 28 августа 2019.*

Сотням людей платили за расшифровку голосовых сообщений из приложения Facebook Messenger. Как выяснило агентство Блумберг, социальная сеть отдавала голосовые сообщения на расшифровку компаниям-подрядчикам. В Facebook подтвердили эту информацию. Компания заявила, что обрабатывала сообщения только тех пользователей, которые в приложении выбрали опцию расшифровки голосовых сообщений[1].

Несмотря на поднятый вокруг этих разоблачений ажиотаж, тревожиться едва ли стоит: в упомянутых случаях речь шла действительно только о совершенствовании качества распознавания речи. Искусственному интеллекту нужна надежная обучающая выборка, основанная на реальных данных, поэтому компании и привлекали людей к расшифровке записей разговоров.

Плохо другое: во-первых, делалось это не вполне публично, а во-вторых, расслабляться по поводу слежения за мобильниками рано.

> *Есть масса способов прослушивать разговоры по мобильному — пусть и не в мировом масштабе. В пределах страны этим занимаются, выполняя свои задачи, правоохранительные органы, и операторы связи обязаны предоставлять им доступ к своему оборудованию.*

С позиций защиты гражданских свобод можно, конечно, выразить озабоченность слишком широкими полномочиями спецслужб. Однако, в целом, для законопослушных граждан риск от этого канала

1 *Facebook привлекал людей к расшифровке голосовых сообщений. Компания свернула проект. // Русская служба BBC, 14 августа 2019.*

невелик, зато преступников при помощи таких методов ловят, причем весьма эффективно.

Что же до мошенников и других заинтересованных лиц, действующих за рамками закона, то у них существует еще несколько способов перехвата телефонных разговоров. Например, установка фальшивой базовой станции, которая, правда, требует специального оборудования и технических знаний и применяется, в основном, разведчиками или шпионами — в зависимости от того, на чьей стороне они работают. В Китае, впрочем, коммерсанты часто применяют фальшивые базовые станции для массовой рассылки спама на мобильные телефоны, находящиеся в радиусе сотен метров.

Но оставим шпионские страсти и обратимся к более насущным проблемам.

> *Потенциально можно прослушать телефон любого пользователя: для этого надо всего лишь установить на него специальную программу-троян. Подвержены этому риску телефоны как с Android, так и с iOS.*

Каналы заражения могут быть разными. Например, преступник, получив доступ к вашему телефону, просто устанавливает нужное приложение. Даже если это делает близкий человек, он все равно остается преступником — об этом следует помнить ревнивым мужьям и женам. Советов по поводу организации такой прослушки в интернете полно, однако их авторы умалчивают об уголовной ответственности за подобное деяние — ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений».

> *Установить прослушку могут и во время ремонта телефона, поэтому не пользуйтесь услугами случайных мастерских.*

Пользователи могут выбрать, соглашаться или нет на мониторинг качества распознавания их речи.

Подростки могут захотеть сделать это из озорства — прикольно же подслушать, о чем говорят девочки, например, или еще лучше — учителя. Поговорите с ребенком о том, что прослушивание чужих телефонов — это не забава, а самое настоящее уголовное преступление.

Но бывает, что вы сами скачиваете софт, содержащий шпионские функции, причем необязательно ограничивающиеся только прослушкой. Если уж троян пробрался на ваш телефон, он не погнушается кражей личных данных, паролей и денег. Конечно, в официальных магазинах такого быть не должно, однако истории, подобные приведенной ниже, регулярно случаются.

> *MobonoGram 2019 — приложение, позиционирующееся как неофициальная версия Telegram с большим набором функций. Из официального магазина Google Play его скачали более 100 тысяч пользователей. На деле приложение не только не могло предложить расширенных функций мессенджера, но и продвигало вредоносные сайты. В MobonoGram 2019 использовался код легитимной версии Telegram, к которому были добавлены несколько скриптов, работающих незаметно для пользователя. Именно эти скрипты отвечали за загрузку вредоносного контента, получаемого от командного сервера*[1].

В целом, следует признать, что действия, совершенные в интернете с мобильного телефона, отслеживаются гораздо лучше, чем

1 *Неофициальную вредоносную версию Telegram установили 100 тыс. юзеров. // **Anti-Malware.ru**, 16 июля 2019.*

с обычного компьютера. Даже профессиональному хакеру трудно замести свои следы, работая с телефона. Лучше и не пытайтесь!

Цифровой швейцарский нож

«Я всегда с собой беру видеокамеру!» Помните этот припев из некогда популярной телепередачи «Сам себе режиссер»? Как ни странно, она продолжает выходить в эфир, хотя, казалось бы, кому это нужно, когда можно смотреть сколько угодно прикольных роликов на YouTube, TikTok или Likee (бывшем Like.Video).

В 1992 году, когда все только начиналось, первые материалы для программы были куплены у американского канала ABC, а последующие снимала творческая группа, потому что редко у кого была видеокамера, да и сюжеты любительских видео не блистали разнообразием. Потом публика постепенно втянулась, среди присланных материалов стали попадаться по-настоящему талантливые, но рейтинг передачи безнадежно упал и никогда больше не достигал былых высот.

Почему? Да потому, что в телефонах появились видеокамеры вполне приличного качества и открылось множество возможностей публиковать свой фото- и видеоконтент, не дожидаясь одобрения редактора. Каждый теперь действительно сам себе режиссер.

Видеокамера так и не успела стать массовым бытовым прибором, который имеется в каждом доме, — смартфон убил ее практически на взлете. Вы вообще когда-нибудь задумывались, сколько вещей

вытеснил из нашей жизни изящный гаджет, который мы по инерции все еще называем телефоном? Давайте вспомним их поименно, павших под натиском цифровизации:

- **Видеокамера** — раз уж мы с нее начали. Пожалуй, основное количество видео сегодня снимается именно на телефоны; этим пользуются даже известные телеведущие для своих личных проектов в интернете;

- **Фотоаппарат** — качество съемки стало чуть ли не главным критерием, по которому выбирают новый телефон;

- **Фотоальбом** — на телефон не только снимают, на нем же и просматривают фотографии;

- **Калькулятор**;

- **Фонарик**;

- **Будильник**;

- **Секундомер**;

- **Зеркало**;

- **Лупа**;

- **Ежедневник**;

- **Адресная и телефонная книжка** — уже и свой-то номер не все помнят, не говоря о чужих;

- **Календарь** — бумажный остался разве что в виде арт-объекта для украшения стен;

- **Диктофон**;

- **Радио** — хотя эта функция уже и в телефонах умирает при переходе к беспроводным наушникам; ранее провод использовался как антенна;

- **Плеер** — если помните, то первым успешным ходом Apple на потребительском рынке был именно выпуск MP3-плеера iPod с магазином iTunes, где была доступна любая музыка;

- **Портативный телевизор и видеоплеер**;

- **Шагомер** (его еще называют педометр) — все фитнес-трекеры используют эту возможность телефонов;

- **Тюнер для настройки гитары, укулеле или другого инструмента.** Теперь можно это делать, вообще не имея слуха.

Кроме того, смартфон может работать как множество физических приборов — нужно только установить специальные приложения:

- Измеритель уровня звука, или **шумомер** — может пригодиться, чтобы понять, нарушает ли уже сосед с перфоратором закон о тишине или еще нет;

- **Виброметр** — чтобы продиагностировать, нет ли где опасных вибраций, и не пора ли отдавать компьютер в ремонт, потому что подшипники вентилятора износились;

- **Люксметр** — для замера освещенности на рабочем месте. Вдруг не соответствует стандартам по охране труда;

- **Прибор для поиска скрытой проводки** — да-да, в телефоне есть датчик электромагнитного поля, он и это может;

- **Металлоискатель** — пригодится для поиска кладов или гантелей, закинутых под кровать;

- **Уровень** — для профессионального использования, может, и не подойдет, но зато всегда под рукой. По крайней мере, картину повесите прямо;

- **Линейка** — небольшая, в размер экрана, но иногда и этого хватит. Обладатели телефонов с большим экраном почувствуют свое превосходство;

- **Сканер штрих- и QR-кодов** — тоже полезная вещь. У нас пока оплата по QR-коду не очень распространена, а в Китае она уже на каждом шагу;

- **Тюнер для настройки гитары, укулеле, балалайки и вообще любого инструмента.** Если вы не обладаете идеальным слухом, а играть охота — незаменимая вещь;

- **Метроном** — крайне полезная штука для начинающих музыкантов;

- **GPS-датчик**, чтобы не спрашивать «Где я?». Увы, работает только на Земле, если вас похитят инопланетяне — не поможет;

- **Компас** — с телефоном вы всегда будете знать, где север, где юг; это надежнее, чем определять стороны света по мху на деревьях;

- **Спидометр** — можно поставить хоть на детский велосипед и устраивать гонки;

- **Акселерометр** — с его помощью можно проверить закон земного тяготения (только не бросайте телефон на асфальт с балкона);

- **Термометр** — в качестве медицинского едва ли сойдет, но насколько тепло или холодно в комнате, покажет. В некоторых моделях есть даже датчики влажности и давления, так что получается полноценный климат-контроль;

И это далеко не полный список того, что умеет ваш телефон. Пожалуй, единственное, чего в современных телефонах нет, так это отвертки и штопора, иначе он бы уже потеснил знаменитый швейцарский армейский нож.

Современный смартфон — настоящая маленькая физическая лаборатория у вас в кармане.

А теперь подумайте: если у ребенка изъять настоящий телефон (смартфон) и дать простую «звонилку» — сколько всего ему еще понадобится? Положим, без компаса он найдет дорогу в школу. Но калькулятор ему нужен, плеер и фотоаппарат он тоже попросит, будильник сами купите, чтобы не проспал школу. Да и остальные цифровые

вещи тоже полезны — надо только показать, что они есть в его телефоне, и научить ими пользоваться. Может быть, тогда он будет меньше смотреть YouTube и больше интересоваться окружающим миром, ведь современный смартфон — это настоящая маленькая физическая лаборатория у вас в кармане.

Работает? Не трогай! — Джейлбрейк и рутование

Компания Apple ограничивает доступ к некоторым функциям своих устройств. Например, на iPhone вы не можете увидеть файловую систему, хотя она там есть, как и на любом компьютере. Кроме того, стандартная версия iOS позволяет устанавливать приложения только из официального магазина App Store. Чтобы обойти эти и некоторые другие ограничения, установленные вендором, хакеры-энтузиасты научились делать **джейлбрейк** («jailbreak» дословно с английского — «побег из тюрьмы») — взламывать операционную систему, чтобы получить полный доступ ко всем функциям.

Поначалу это имело смысл, поскольку приложений в «родном» магазине Apple было мало, и попасть туда независимым разработчикам было сложно. Многие пользователи с нетерпением ждали джейлбрейка после выхода новой версии операционной системы, чтобы расширить возможности своих устройств.

Сейчас джейлбрейк практически потерял смысл, поскольку iOS ушла далеко вперед в своем развитии, да и приложений

в официальном магазине так много, что едва ли есть необходимость искать их на стороне.

В принципе, ничего противозаконного в джейлбрейке нет: ломайте свои айфоны на здоровье, но учтите, что после взлома вы лишаетесь права на техническую поддержку и гарантийное обслуживание. (Вы все еще уверены, что оно вам надо?). Правда, можно заново установить официальную версию iOS, и это устранит следы взлома. Но главное не в этом — приложения из непроверенных источников могут быть потенциально опасными. А, значит, обычным пользователям джейлбрек противопоказан.

Если вдруг ваш ребенок наслушался легенд о давних временах, когда, чтобы быть крутым, нужно было обязательно ставить джейлбрейк, объясните ему, что эти сведения устарели, и сегодня нужды в этом никакой нет.

Аналогичная процедура на андроид-телефонах называется рутование или **рутинг** (от английского «root» — «корень»). Цели аналогичные — получить полный контроль над своим устройством и выжать из него максимум. Например, на рутованном телефоне можно увеличить частоту процессора, чтобы заставить его работать быстрее, или установить приложения для взлома игр. Такие приложения получают доступ к памяти игр, чтобы изменять в них те или иные параметры или позволять играть бесплатно.

Но, как обычно, вместе с новыми возможностями вы получаете и новые риски.

Наличие у владельца устройства прав суперпользователя нарушает главные принципы безопасности Android. С та-

кими правами приложения получают возможность творить что угодно, в том числе удалять файлы, необходимые для работы операционной системы.

Это могут сделать и честные приложения — просто потому, что разработчики не тестировали их работу на взломанной системе. А уж для вредоносных приложений после получения прав суперпользователя наступает полное раздолье. Они могут воровать пароли из браузера, скрытно покупать приложения на Google Play, подменять адреса в браузере (фишинг), скрытно устанавливать приложения, в том числе в системные разделы, помогать закрепиться троянам.

Для вредоносных приложений после получения прав суперпользователя наступает полное раздолье.

В общем, не уверен — не рутуй. Гарантия на взломанный аппарат не действует. И, если взвесить трезво, проблем от джейлбрейка и рутинга можно «поиметь» много, а выгоды — практически никакой.

Предупредительные меры

Вообразите ситуацию, когда ваш телефон действительно исчез. То ли его вытащили у вас из кармана, то ли вы сами забыли его на скамейке, то ли выронили на переходе и прямо на ваших глазах по нему проехал грузовик. Увы, такое может произойти с каждым, и лучше быть заранее к этому готовым, чем в панике вспоминать все прочитанные когда-то советы, которые будут уже бесполезны.

Тогда ваша беда сократится до размера суммы, которую придется выложить за новенький аппарат.

К сожалению, большинство пользователей игнорируют даже самые простые рекомендации, а потом грустят об утраченных фотографиях с романтического свидания или с веселой вечеринки, переживают из-за записанных в заметках паролей ко всем счетам и аккаунтам (хотя этого как раз делать нельзя), думают, где заново найти все нужные контакты — поводов для печали у них предостаточно.

> *Всех бед, связанных с утратой смартфона, можно избежать, если настроить на нем копирование в облако. В наше время этот совет звучит банально, и, тем не менее, некоторые им пренебрегают — либо из легкомыслия, либо из принципа.*

У каждого телефона свои настройки, с которыми вам придется разобраться самостоятельно. В любом случае, ничего сложного в этом нет. В итоге вам предложат более-менее стандартный набор для резервного копирования: контакты, сообщения, заметки, приложения, настройки, фотографии, музыка, документы, настройки будильника, вид главного экрана и прочее.

> *Если по каким-то соображениям вы не хотите, чтобы ваши данные и фотографии хранились в облаке, то остается вариант регулярно делать резервное копирование с телефона на домашний компьютер.*

Имея такую копию, вы можете запросто восстановить свой телефон до рабочего состояния, если нечаянно «словили» вирус, доигрались с настройками так, что пришлось все обнулить до завод-

ских установок, или купили новый аппарат взамен утраченного. Это очень облегчает жизнь и бережет нервы.

> *Как водится, в каждом деле есть свои тонкости. Поставщики телефонов — Apple, Samsung, Xiaomi, Huawei и другие — дают в своем облаке бесплатно не очень много места. Например, владельцы айфонов получают только 5 ГБ, Samsung более щедр — выделят 15 ГБ. Для хранения резервной копии этого достаточно, однако, если вы станете регулярно сливать в облако свои фотографии, то быстро почувствуете, что вам тесновато.*
>
> *Поэтому копирование фотографий (и видео) лучше настроить отдельно. Для этого подойдет любое популярное облачное хранилище — Yandex.Диск, Облако.Mail.ru, OneDrive от Microsoft, DropBox или Google — причем у Google есть специальное приложение Photo, которое умеет не только копировать фотографии с телефона, но и сортировать их по разным признакам. Для большей надежности можно настроить копирование сразу в два облака, хуже не будет.*

Так, хорошо. О данных мы позаботились, теперь давайте позаботимся о самом аппарате, чтобы в случае, если вы с ним нечаянно расстанетесь, можно было его разыскать. Наверное, все об этом знают, но нелишним будет напомнить.

> *На айфоне нужно просто включить функцию поиска потерянного устройства в настройках; для телефонов на Android сначала придется установить специальное приложение от Google — Find My Device (оно видит и айфоны тоже).*

Сделав это, вы сможете в случае утери телефона, во-первых, увидеть, где он находится (если не отключена геолокация). Если вы обронили свой телефон в лесу, то этого будет достаточно для поиска. В городе ваш мобильник обязательно кто-то подберет и, возможно, захочет его вам вернуть. А может быть, и нет.

Есть и еще ряд действий, предпринять которые весьма желательно.

- *Заблокируйте вход в телефон. Это особенно важно сделать, если вы вдруг были настолько беспечны, что не поставили пин-код или пароль. Еще вы сможете выводить на экран блокировки сообщение, которое будет появляться при каждой попытке включения, чтобы объяснить нашедшему, как с вами связаться.*

- *Закройте все открытые на телефоне сессии и выйдите из всех приложений на случай, если кто-то все-таки сломает входной пароль. Для пущей верности можно вообще очистить устройство, удалив с него все данные без возможности восстановления. (У вас же есть резервная копия, не так ли?).*

- *Важно: после удаления данных с телефона отследить его с помощью функции поиска будет невозможно. Но если надежды на возвращение нет — это нужно сделать. Если устройство не в Сети, данные будут удалены при следующем подключении.*

Один нюанс относительно детского телефона. Если вы не настроили семейный доступ (как было сказано выше), то телефон ребенка,

скорее всего, привязан к аккаунту одного из родителей, а, значит, он сам заняться поиском не сможет, даже добравшись до компьютера. Положение детского телефона можно отслеживать и при помощи Kaspersky Safe Kids, если у вас это приложение установлено.

И еще из предупредительных мер: если ваш телефон найдется, то вам придется доказывать, что вы его владелец. Вы точно помните его приметы? Царапина на правом боку, трещина на стекле? Модель, серийный номер и IMEI, который понадобится при розыске? И знаете, где лежит коробочка с паспортом и чеком из магазина? Очень хорошо!

Совсем не лишним будет сохранить их копии в специальной папке в облаке, чтобы иметь возможность быстро предъявить. И еще: наберите *#06# на клавиатуре, чтобы увидеть IMEI и серийный номер, и сделайте скриншот — это проще, чем переписать множество цифр и не ошибиться.

Если это все-таки произошло...

Увы, никто не застрахован от таких неприятностей, как расставание с телефоном. На этот случай у вас должен быть план действий. Честно скажем: шансы вернуть свое устройство невелики, но они есть, и сразу отчаиваться не стоит. Вы ведь выполнили все, о чем мы говорили в предыдущем разделе: данные — в облаке, функция поиска включена, телефон заблокирован. Да?

Прежде всего, надо четко разграничить две ситуации — потеря и кража — и не смешивать одно с другим. А именно:

не надо пытаться выдать свое ротозейство за чей-то преступный умысел.

Потому что при обращении в полицию вас попросят максимально точно описать обстоятельства происшествия, время, место и приметы потенциального преступника. Если вы все это будете выдумывать, то обязательно запутаетесь, и в возбуждении дела вам откажут, а без открытого дела ваш телефон искать никто не будет. Также надо быть готовым подтвердить свои права на аппарат — на слово вам никто не поверит, понадобятся документы или хотя бы их копии.

Будьте готовы подтвердить свои права на аппарат — на слово вам никто не поверит, понадобятся документы.

Допустим, вам повезло убедить полицию открыть дело. Что произойдет дальше? Следователь направит запрос операторам мобильной связи, и, если повезет еще раз, то ваш телефон найдут. То есть технически можно найти любой телефон, но это довольно хлопотно и дорого, поэтому обычно такие методы задействуют только при расследовании тяжких преступлений, в которых засветился какой-то телефон, а на обычные кражи просто не хватает ресурсов. Короче говоря, если за пару месяцев чуда не произойдет, об украденном телефоне можно забыть. Все предложения «пробить» телефон в обход полиции — чистое мошенничество.

Искать ваш телефон полиция обязана следующим образом:

Заявление согласно ст. 141 УПК РФ и Инструкции, утвержденной приказом МВД РФ №736 от 2014 г., должно быть принято сразу же. Потерпевший может сделать его в письменном виде (в этом случае документ регистрируется в Книге учета

заявлений), либо в устном (в этом случае его слова заносятся в протокол).

В течение 3 дней полиция должна провести проверку заявленных сведений и возбудить дело, или дать мотивированный отказ, согласно ч. 1 ст. 144 УПК РФ. В некоторых случаях срок может быть продлен до 10 или 30 суток.

Если уголовное дело возбуждено, потерпевший об этом письменно информируется. Если же в возбуждении отказано, то ему направляется постановление об отказе, которое может быть обжаловано в суде либо районным прокурором в порядке ст. 124–125 УПК РФ.

Срок следствия (то есть реального поиска телефона) не может быть больше 2 месяцев согласно ст. 162 УПК РФ. По ходатайству следователя может быть продлен еще на 3 месяца. (Но вряд ли в случае обычной кражи).

На практике, если находят, то часто по горячим следам. Вора могут задержать и безо всяких технических хитростей — по приметам, как это делали в МУРе во времена Глеба Жеглова и Володи Шарапова.

Если вы просто потеряли телефон, то сразу отчаиваться не стоит. Мир не без добрых людей, и наверняка среди ваших знакомых найдутся несколько человек, которые поделятся историями о том, как им вернули телефон. Люди забывают мобильники в такси, кафе, магазине, аэропорте, в самолете в кармане впереди стоящего кресла (хотя стюардессы настойчиво напоминают, что класть их туда не стоит), в метро, на скамейке в парке —

да где угодно. Кто-то теряет, а кто-то находит — и даже отдает найденную вещь.

Можно повысить вероятность возврата, если внести IMEI пропавшего телефона в базу LoSToleN.

Можно немного повысить вероятность возврата, если внести IMEI пропавшего телефона в базу LoSToleN (**https://sndeep.info/en/lostolen**). Потому что скупщики б/у телефонов, не желая попасть под уголовную ответственность за сбыт краденного, часто проверяют принесенные им аппараты по этой базе. А если вы укажете размер вознаграждения, то ваши шансы еще немного подрастут. И проверяйте сами эту базу — бывает, что утерянный телефон обнаруживается там в разделе найденных, — если человек честно хочет вернуть его владельцу, но не знает, как с вами связаться.

Но когда вас накроет волна эйфории от радостного известия, не следует терять бдительность. Не ведитесь на уговоры назвать пароль, чтобы нашедший мог разблокировать телефон и убедиться, что он ваш. Не сообщайте никаких подробностей о телефоне — цвет, модель, особые приметы, пусть его описывает нашедший. И уж точно не ходите на встречу с незнакомцами в одиночку в непонятные места.

> *После того, как телефон побывал в чужих руках, разумно будет не только продезинфицировать его снаружи, но и сбросить до заводских настроек и восстановить из резервной копии. Ибо вы не знаете, через сколько рук прошел ваш телефон и что на него могли установить.*

Например, ребята с радиорынка перед тем, как получить с вас вознаграждение за находку, могли запросто внедрить туда шпионский софт, который потом сольет им все ваши пароли.

Полный сброс настроек не помешает сделать и когда вы приобрели поддержанный телефон в магазине или с рук. Обязательно, еще до покупки, проверьте его по базе украденных и потерянных, потому что, если объявится законный владелец, то крайним можете оказаться вы. В лучшем случае аппарат у вас просто конфискуют.

Несем мобильный в ремонт

Бывает, что телефон внезапно перестает подавать признаки жизни или совершает акробатический прыжок из наших рук прямо на бетонный пол. Тогда мы несем его в ремонт, надеясь, что мастер оживит верного друга и залечит все его раны.

Насколько это безопасно? Там же все ваши личные данные, явки-пароли-адреса, фотографии (в том числе и компрометирующие), банковские приложения, подключенный NFC[1] для удобства оплаты. И все это богатство люди готовы дове-

1 *NFC (Near Field Communication) — технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров. Применяется для того, чтобы «платить телефоном» — банковская карта привязывается к приложению Apple Pay или Google Pay, которые используют встроенный в телефон NFC-чип для взаимодействия с платежным терминалом.*

рить пареньку, сидящему в ларьке под вывеской «Ремонт телефонов» — то есть первому встречному. Странно, не правда ли? Стоит ли потом удивляться, что с вашего счета начинают утекать деньги, или что ваше видео с новогодней вечеринки стало хитом YouTube?

Как же правильно отдать телефон в ремонт? Давайте разберемся.

> *Де-факто ситуацию с ремонтом можно приравнять к потере или даже краже в плане грозящих вашим данным рисков, поэтому относиться к ней надо соответственно. Прежде всего, еще раз напомнить себе о предупредительных мерах (настройте, наконец, резервное копирование).*

Разумеется, не все мастера по ремонту киберпреступники, но все они обладают технической квалификацией и оборудованием, недоступным обычному пользователю. Кроме того, они получают физический доступ к вашему устройству, чего не имеют хакеры, действующие удаленно. Так что осторожность не помешает.

> *Перепишите свой IMEI, чтобы убедиться, что после ремонта вам вернули именно ваш аппарат. Внимательно смотрите все документы, которые вам выдают в сервисном центре, чтобы, если что-то пойдет не так, можно было обратиться в полицию.*
>
> *Разумеется, нужно вынуть из телефона сим-карту (и вторую тоже) и карту памяти, если она есть, — в любой мастерской должны быть тестовые симки. Помните, что к телефон-*

ному номеру привязано немыслимое количество сервисов, поэтому берегите ее также, как паспорт.

Если ваш аппарат, в принципе, работает (например, требуется только замена экрана), то лучше всего будет сделать свежую резервную копию и сбросить телефон к фабричным настройкам. Сделав это, можно смело отдавать телефон кудесникам, которые его починят.

Иногда поломки случаются внезапно, причем телефон просто перестает включаться. Если у вас (еще раз!) есть резервная копия, можете дать сервисному инженеру разрешение на обнуление аппарата и чувствовать себя куда спокойнее, нежели если бы раскрыли ему пароль и пин-код. Тем не менее, будет лучше поменять пароли всех критичных приложений и самого аккаунта (Apple ID или Google Account) — это можно сделать с компьютера. Не забудьте и те, которыми вы пользуетесь редко, например, Skype.

У вас вообще не стоял пароль на разблокировку экрана? Плохо. Ваши данные под угрозой! Остается только уповать на честность мастера.

Некоторые клиенты требуют, чтобы ремонт выполнялся только в их личном присутствии и под видеозапись, потому что они очень ценят свои данные и ясно представляют, что с ними может произойти. Например, при ремонте в ваш телефон будут установлены «жучки» или вредоносный софт. Сценарии голливудских боевиков с поразительной скоростью проникают в реальную жизнь, и с этим стоит считаться. Если у вас дорогая модель, то вполне вероятно, что вы работаете в компании, секреты которой можно

будет кому-то продать, а средства кибершпионажа становятся все доступнее и доступнее.

Относитесь к ремонту как к рискованному мероприятию и принимайте всевозможные меры предосторожности.

В общем, относитесь к ремонту как к весьма рискованному мероприятию и принимайте всевозможные меры предосторожности. Лучше показаться параноиком, чем потом жалеть о своей доверчивости.

Контрольные вопросы

1. Что такое номофобия?
2. Что для вас значит мобильный телефон?
3. С какого возраста в России человек может иметь мобильный телефон?
4. С какого возраста можно завести Apple ID? Google Account?
5. Зачем нужен «Семейный доступ»? А вы его используете?
6. Как вы считаете, есть ли у вас зависимость от телефона? В чем она выражается?
7. Как постоянное пользование смартфоном влияет на умственное развитие ребенка?

8. Существует ли заболевание «селфитис»?

9. Какие виды селфи вы знаете?

10. Когда делать селфи опасно?

11. Чем опасна реклама в мобильных играх?

12. Каков вред от телефона в школе?

13. Какова польза от телефона в школе?

14. Кто изобрел телефон?

15. Что такое черные и белые списки?

16. Какие способы борьбы с телефонным спамом вы знаете?

17. Почему нельзя делать «анонимные» звонки с мобильного телефона?

18. Как можно отследить мобильник по сенсорам?

19. Действительно ли телефоны постоянно нас подслушивают?

20. Почему нельзя ставить на чей-то телефон программы для прослушки?

21. Какие из обычных вещей заменил смартфон? Что из этого вам полезно и почему?

22. Почему не стоит делать джейлбрейк?

23. Что нужно сделать, чтобы не горевать о своих данных при утрате телефона?

24. Как правильно искать потерянный телефон?

25. Что делать, если телефон украли?

26. Что такое IMEI?

27. Что нужно сделать, отдавая телефон в ремонт?

Глава 9

Что в профиле тебе моем?..

Социальные сети.
Именно ради них многие пользователи выходят в интернет.
В этой главе мы вспомним, как они появились,
и узнаем, в чем секрет их популярности,
а также разберем правила безопасного поведения
в соцсетях — что в них можно делать и чего нельзя.

«Люди хотят зайти в интернет, чтобы узнать, как дела у друзей. Так почему бы не написать для этого вебсайт? Друзья, фотографии, профили — зайти можешь куда угодно, ходить по страницам. Может, там будет новый знакомый с вечеринки. Но я не о сайте знакомств говорю. Я говорю о переносе всей социальной жизни университета в онлайн, — так рассказывал о своей идее Марк Цукерберг. — И не надо ничего взламывать. Люди сами предоставят свои фотографии, свою информацию. Люди смогут приглашать — или не приглашать — своих друзей. Понимаете, в мире, где все завязано на социальную структуру, это стало бы прорывом».

«Я говорю о переносе всей социальной жизни университета в онлайн», — так рассказывал о своей идее Марк Цукерберг.

Происходил этот разговор в 2003 году в Гарварде, где тогда учился юный основатель Facebook, ставший вскоре самым молодым миллиардером в истории.

На самом деле, говорил не сам Марк, а Джесси Айзенберг, исполняющий его роль в фильме Дэвида Финчера «Социальная сеть», который вышел на экраны в 2010 году. К тому времени Facebook из сайта для студентов уже стал не просто глобальной компанией с количеством пользователей более 500 миллионов, а настоящим социальным феноменом, требовавшим осмысления. Поэтому фильм, изначально задуманный как обычная история успеха студента-ботаника, умудрившегося заработать кучу денег, вызвал широкий резонанс. Всем вдруг стало неважно, насколько точно киноверсия соответствует реальной истории — кто кого обманул, кто был прав, а кто нет, каковы были мотивы поступков героев, и кто какую долю в итоге получил.

На первый план вышли вопросы этики отношений в эпоху интернета и влияния социальных сетей на все стороны нашей жизни — именно это вызвало самые жаркие дебаты, которые не утихают и по сей день.

В том же 2010 году Марк Цукерберг был признан «Человеком года» по версии американского журнала Time. Главный редактор издания Ричард Стенджел считает, что Facebook как явление изменил представление об отношениях людей во всем мире[1].

1 *Интересно, что соперником Цукерберга был тоже человек из сферы ИТ, представитель ее теневой стороны — Джулиан Ассанж, основатель WikiLeaks, убежденный борец за раскрытие любых секретов в интернете. Его кандидатуру выдвинули читатели журнала, но по традиции «Человека года» выбирает главный редактор, и он предпочел Цукерберга.*

Источник: Отчет «Digital-2020», подготовленный We Are Social и Hootsuite.

По состоянию на первый квартал 2020 года ежемесячно активных пользователей Facebook было 2,6 миллиарда, а общее число пользователей соцсетей в 2019 году достигло примерно 3,484 миллиарда человек, что составляет 45% населения Земли. Если соотнести число пользователей соцсетей с общим числом тех, кто имеет доступ в интернет, мы получим 80%. То есть четверо из пяти человек, заходящих в интернет, делают это ради того, чтобы заглянуть в социальную сеть. (Хм, интересно: а что делают в интернете оставшиеся 20% ?) Благодаря Фейсбуку в наш обиход вошли слова «лайкнуть», «зафрендить», «отфрендить», «зашерить», и, наверное, этим дело не ограничится, потому что платформа продолжает развиваться, а значит, будут появляться и новые слова для обозначения новых действий.

Четверо из пяти человек, заходящих в интернет, делают это, чтобы заглянуть в социальную сеть.

Социальная сеть не была изобретением Марка Цукерберга. Начало «социализации» интернета было положено еще в 1995 году, когда открылся сайт **Classmates.com**[1]. Этот сайт по-прежнему работает и не сильно изменился за почти четверть века своего существования. Там американцы могут найти своих товарищей по школе или колледжу, пройдя довольно утомительным маршрутом, — нужно выбрать штат, город, школу, в которой они учились, и только после того увидеть друзей детства. Как это непохоже на современные соцсети!

> *«Посещая домашние странички, обнаруживаешь, что целью множества людей является обнародование своей малоинтересной нормальности или, хуже того, малоинтересной ненормальности. <...> цель их — обнародовать пред лицом всех окружающих факты своего частного существования», — писал Умберто Эко в книге «Полный назад»*[2].

В чем же секрет такой притягательности Фейсбука и его клонов (пример — Вконтакте)? Почему это так затягивает людей? Ведь общаться можно было и раньше — в Skype и ICQ. Для того чтобы постить короткие и длинные тексты, у нас был и есть ЖЖ (Живой журнал / Live Journal); были сайты для публикации фотографий, агрегаторы новостей и все прочее. Но, как это часто бывает, собранные вместе отдельные вещи вдруг дают мощный синергетический эффект.

Собранные вместе отдельные вещи вдруг дают мощный синергетический эффект.

1 *По-русски «Classmates» значит «одноклассники», но не путайте его с российской соцсетью «Одноклассники», которая появилась в 2010 году.*

2 *Эко У. Полный назад. М. : Эксмо, 2007.*

Объединив в себе возможности общения, развлечения, флирта, узнавания нового, самоутверждения, творческого самовыражения, нарциссического самолюбования, чувства принадлежности к группе, поиска друзей и деловых партнеров, баталий с врагами (не покидая дивана), просьб о помощи, пестования своего тщеславия, показа рекламы (хоть это нам и не нравится), — социальная сеть стала вселенной современного человека. Это уже гораздо больше, чем «книга лиц», какой она изначально задумывалась создателями. Фейсбук — это полная экосистема.

Здесь пора остановиться и сделать первый вывод.

> *Социальные сети — не очередное модное увлечение подростков, на которое можно не обращать внимания, а если будет мешать учебе — запретить. Социальные сети — реальность современного мира, они будут видоизменяться, эволюционировать, конкурировать друг с другом, но уже никуда от нас не уйдут.*

Быть вне соцсети теоретически можно, но это будет чем дальше, тем больше похоже на попытку ходить в лаптях вместо кроссовок.

Поэтому главная задача взрослых состоит не в том, чтобы оградить ребенка от попадания в соцсети, а в том, чтобы научить его адекватному, позитивному и безопасному пользованию ими. Увы, опасности в соцсетях тоже реально существуют, и мы о них обязательно поговорим позже. А начнем лучше все-таки с позитива.

Прежде всего, социальная сеть — отличный полигон для оттачивания навыков самопрезентации.

Прежде всего, социальная сеть — это отличный полигон для оттачивания навыков самопрезентации, умения выражать свои мысли, оформляя их в текст и визуальные образы, отличное упражнение в ведении дискуссий, тренажер для выработки стрессоустойчивости — то есть поле для развития эмоционального интеллекта. Ведь каждое удачное действие в сети тут же получает одобрение в виде лайка или позитивного комментария — и в мозг впрыскивается порция дофамина, навык подкрепляется. Каждая глупость мгновенно получает оценку, причем безо всяких сантиментов, порой очень жестко, — и с этим тоже надо уметь справляться.

Каждое удачное действие в сети тут же получает одобрение, каждая глупость — соответствующую оценку.

В обычной жизни круг людей, которые могут дать ребенку или подростку обратную связь, значительно уже, да к тому же эти взрослые вечно заняты и не понимают, что сейчас актуально, а что нет. Однако родителям все-таки придется включиться в «тренировочный процесс», если они хотят сохранить контакт со своим сыном или дочерью. Раньше про неблагополучного ребенка говорили, что его воспитала улица, сейчас место улицы могут занять социальные сети, и тогда эффект окажется даже более мощным в негативном плане.

О том, чему дети могут самостоятельно научиться в соцсетях, лучше всех знают их мамы. Вот их мнение.

> *Видео — самый подходящий формат для обучения новым навыкам, а главный его источник — YouTube. Популярные блогеры, вопреки стереотипам взрослых, не только бесконечно демонстрируют себя и свою красивую жизнь, но и учат своих зрителей разным полезным вещам.*

«Плетение фигур из резиночек, основы рисования на планшете с помощью разных программ, лепка, оригами и все, что касается поделок и творчества, дети освоили благодаря интернету», — говорит одна мама. Ее средний сын занимается спортом и, просматривая видео из соцсетей, научился стоять на руках.

Также видео можно использовать в просветительских целях. Чтобы уберечь детей от некоторых поступков — например, от занятий паркуром, — мама иногда показывает «страшилки» — неудачные падения, сломанные руки-ноги и т.д. Еще они вместе смотрят ролики про микробов, чтобы дети не забывали о гигиене.

Другая мама рассказала, что ее сыновья научились хорошо готовить. Они подписались на каналы топовых фуд-блогеров, смотрят мастер-классы и экспериментируют. Надо сказать, что у них получается все успешнее.

Кроме того, они сами пробуют снимать видео: купили камеру GoPro с функцией подводной съемки, монтируют и выкладывают ролики, учатся продвижению и анализу статистики. В соцсетях дети находят списки интересной литературы — потом заказывают и читают эти книги.

Само собой, что про уроки и расписание все теперь узнают ВКонтакте — это надежнее, чем бумажный дневник, и проще, чем специальное приложение.

Социальная сеть как наркотик

С вами случалось такое: присели на пять минут полистать ленту, глянуть, что есть новенького, а залипли часа на полтора? Ничего удивительного, интерфейсы приложений соцсетей специально разрабатываются так, чтобы удержать пользователя на сайте как можно дольше.

Интерфейсы соцсетей специально разрабатываются так, чтобы удержать пользователя на сайте как можно дольше.

Один американский сенатор даже разработал законопроект[1], запрещающий соцсетям использовать функции, вызывающие привыкание, требующий обеспечить свободу выбора и возможность контролировать свое время, проведенное в приложении. Сенатора волнует, что слишком много «инноваций» в этом пространстве предназначено не для создания более качественных продуктов, а для привлечения большего внимания с помощью психологических приемов, которые затрудняют отвод взгляда от страницы. В частности, он предлагает запретить бесконечную прокрутку ленты: прочитал все новости — и выходи.

> *По аналогии с известным пищевым расстройством, состояние, когда человек не в силах прекратить потребление контента, называют медиабулимией. (Научным сообществом этот термин пока не принят, но он достаточно образно описывает явление).*

1 *Josh Hawley, U.S. Senator for Missouri. The Social Media Addiction Reduction Technology (SMART) Act.*

Это не может не вызывать беспокойства, особенно, если в такую ситуацию, как вам кажется, попал ваш ребенок.

Поведение подростков часто не только беспокоит, но и раздражает взрослых. Например, сын или дочь могут демонстративно уткнуться в телефон, пока родители читают нудную нотацию о том, что «надо хорошо учиться... бла-бла-бла... — а то пойдешь работать дворником... бла-бла-бла...». Ты им важные вещи говоришь, а они в телефон пялятся! Естественно, весь гнев переносится на гаджет, который, по сути, ни в чем не провинился. И удивительное дело: работающий телевизор при этом взрослым не мешает!

> *Такое поведение — концентрацию на своем телефоне вместо того, чтобы разговаривать с другим человеком напрямую[1] — называют «фаббинг» ("phubbing"). Оно представляет собой акт отстранения кого-либо в социальной среде; сам термин образован из двух слов: "phone" + "snubbing" — относиться с презрением или игнорируя. В наши дни это настолько распространено, что считается практически нормой, нравится вам это или нет. Причиной фаббинга может быть как интернет-зависимость, когда человек импульсивно тянется к телефону, так и просто нежелание с вами разговаривать. Нельзя, однако, исключать, что этот виртуальный разговор действительно более важен для вашего визави, чем происходящее в офлайне. Так что не торопитесь осуждать, выясните сначала причину. Следует учитывать и возраст: молодежь гораздо терпимее относится к фаббингу, чем люди старшего возраста (хотя последние и сами так делают).*

1 *Varoth Chotpitayasunondh, Karen M. Douglas. How "phubbing" becomes the norm: The antecedents and consequences of snubbing via smartphone // Computers in Human Behavior — 63(2016) 9–18 — doi.org/10.1016/j.chb.2016.05.018*

Но что, если у ребенка и правда уже развилась зависимость от соцсетей? Как почитаешь, что пишут в интернете, — страшно становится. Не отнимешь у него телефон, так он круглые сутки будет торчать в своем ВКонтакте. Вон, даже ночью под подушку кладет. В наше-то время книжки читали с фонариком под одеялом, а эти все с телефонами...

Что можно ответить на это? Во-первых, вспомните классика и «...не читайте до обеда советских газет». Никаких не читайте. Тема зависимости от социальных сетей слишком лакомый кусок для прессы, и ажиотаж вокруг нее искусственно разогревается. Как обычно, негатив выпячивается, а факты, свидетельствующие об обратном, замалчиваются — такова беспощадная логика создания хайпа и сенсаций.

Ученые сегодня не имеют четкого представления о прямой связи между социальными сетями и состоянием психического здоровья.

Официально диагноз «зависимость от социальных сетей» не ставится. О подобном психическом расстройстве можно говорить только на обывательском уровне, потому что ученые сегодня не имеют четкого представления о прямой связи между социальными сетями и состоянием психического здоровья. Исследований проводится много, и они дают неоднозначные результаты, но уже точно можно сказать, что психологические проблемы из-за пристрастия к социальным сетям испытывает очень и очень небольшое число людей.

Активный пользователь соцсети и зависимый человек — это не одно и то же.

Поэтому не стоит вешать ярлык «зависимого» на каждого активного пользователя соцсетей и тем более на своего ребенка. Помните, что технология — это всего лишь средство или инструмент. Она

позволяет людям участвовать в определенных формах проявления, таких как социальные сети и игры, но не вызывает привыкание как таковое.

Если вы хотите проверить, не подвержены ли вы риску развития зависимости от социальных сетей, задайте себе шесть простых вопросов[1]:

1. Много ли вы тратите времени на размышления о социальных сетях или планирование их использования?

2. Чувствуете ли вы желание использовать социальные сети все больше и больше?

3. Используете ли вы социальные сети, чтобы забыть о личных проблемах?

4. Часто ли вы пытаетесь сократить использование социальных сетей, причем безуспешно?

5. Испытываете ли вы беспокойство, если не можете использовать социальные сети?

6. Используете ли вы социальные сети в такой степени, что это негативно сказалось на вашей работе или учебе?

Если вы ответили на все шесть вопросов «да», то у вас может возникнуть или уже развивается зависимость от использования социальных сетей. Мы говорим «может», потому

1 *Mark D. Griffiths Ph.D. Addicted to Social Media? // Psychology Today, 7 мая 2018.*

что единственный способ подтвердить это — диагноз, поставленный клиническим психологом или психиатром.

А если не все — то вы обычный пользователь, которому стоит задуматься о контроле над своей привычкой. Отключите звуковые уведомления, реже проверяйте телефон, кладите его на ночь подальше от себя, чтобы не испытывать соблазна, не пользуйтесь им во время еды.

> *Тем не менее, существует растущая база научных данных, позволяющая предположить, что чрезмерное использование соцсетей может привести к симптомам, традиционно связанным с зависимостью от веществ.*

Для некоторых людей это действительно может стать проблемой. Им точно также, как наркоманам, требуется все возрастающая доза социального взаимодействия, а после «отлучения» от источника удовольствия зависимые люди могут испытывать негативные психологические, а иногда и физиологические симптомы, такие как абстиненция[1].

Первоначально эту область исследований полушутя называли «фейсбукологией», потому что подавляющее большинство работ было посвящено зависимости от крупнейшей в мире социальной сети. Но позже было замечено, что аддиктивные качества других соцсетей отличаются от тех, которые характерны для Фейсбука — например, в Instagram работают

---

1 *Daria J. Kuss, Mark D. Griffiths. Social Networking Sites and Addiction: Ten Lessons Learned // Int. J. Environ. Res. Public Health 2017, 14(3), 311; https://doi.org/10.3390/ijerph14030311*

совершенно иные механизмы, и это требует отдельного изучения.

Что касается причин возникновения зависимости от социальных сетей, то у специалистов пока нет единого мнения на этот счет. Ясно только, что слишком драматизировать ситуацию не стоит. На основании имеющихся данных уже можно утверждать: статистика, на самом деле, не столь удручающая по сравнению с тем, как тему преподносят средства массовой информации. Например, в исследовании[1], проведенном на относительно небольшой репрезентативной выборке населения Бельгии (n=1000), результаты показали, что всего 6,5% использовали соцсети компульсивно, причем эта группа имела более низкие баллы по показателям эмоциональной стабильности и способности договариваться, добросовестности, восприимчивости контроля, самооценки, зато более высокие оценки по ощущению одиночества и депрессии. То есть для нормального человека риск попасть в зависимость от пользования соцсетями довольно мал.

Для нормального человека риск попасть в зависимость от пользования соцсетями довольно мал.

В конце концов, для подростков находиться дома онлайн безопаснее, чем бродить по улицам.

---

1 *De Cock, R.; Vangeel, J.; Klein, A.; Minotte, P.; Rosas, O.; Meerkerk, G.J. Compulsive use of social networking sites in Belgium: Prevalence, profile, and the role of attitude toward work and school. CyberPsychol. Behav. Soc. Netw. 2014, 17, 166–171.*

Везде поспеть стало мудрено: синдром FoMO

Помните, как начинал свой день Евгений Онегин? Смартфона у него не было, поэтому посты друзей он получал в виде записочек: «Три дома на вечер зовут — там будет бал, там детский праздник», — и прикидывал, как бы ничего не пропустить. Но автор спешит нас успокоить: «С кого начнет он? Все равно: везде поспеть немудрено».

По сравнению с веком девятнадцатым темп вырос, и теперь жизнь обычного тинейджера куда более насыщена разнообразными событиями, чем жизнь городского щеголя двести лет назад. И это обилие выбора играет с нами злую шутку: боясь пропустить что-нибудь интересное, мы листаем посты друзей, новостные подписки, приглашения на события — и понимаем, что не можем запихнуть в свою голову весь этот информационный поток и поспеть во все места, куда нас позвали.

Человек со здоровой психикой способен отнестись к ограниченности своих возможностей философски.

Человек со здоровой психикой способен отнестись к ограниченности своих возможностей философски. Он отложит в сторону смартфон, «откупорит шампанского бутылку», перечтет «Женитьбу Фигаро» или посмотрит трехчасовой артхаусный фильм. Но не всем так повезло — многих снедает чувство тревоги от того, что они не успевают переработать всю лавину сообщений и из-за этого могут пропустить что-то интересное и неповторимое. Психологи называют такое состояние синдромом FoMO — Fear of Missing Out (синдром упущенной выгоды).

Многих снедает чувство тревоги от того, что они не успевают переработать лавину сообщений и могут пропустить что-то интересное.

Изначально это была полезная «фича», заложенная в наш мозг эволюцией. Чтобы выжить в дикой природе и жесткой социальной среде, человеку нужно было постоянно анализировать открывающиеся возможности и выбирать лучшие — с кем и против кого дружить, где добыть пищу, где укрыться на ночь. Сейчас нами больше движет любопытство, стремление знать обо всем, что происходит у друзей, да и вообще в мире, быть в курсе событий — и социальные сети стали неиссякаемым источником бесполезных данных с редкими вкраплениями чего-то ценного. Это стакан, который всегда полон, а синдром FoMO вызывает жажду, которую невозможно утолить.

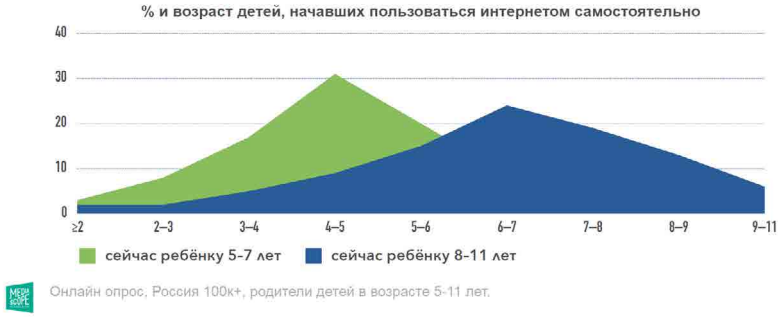
Соцсеть — не причина зависимости, а ее следствие.

В одном исследовании с участием 5280 пользователей из нескольких испаноязычных латиноамериканских стран[1] было установлено, что FoMO указывает на возможность негативных последствий неадекватного использования соцсетей. То есть соцсеть — не причина зависимости, а ее следствие. Если у человека есть выраженные психопатологии — например, тревожность или депрессия, — то бесконтрольное пребывание в соцсетях может ухудшить его состояние. Соответственно, бороться надо не с проявлениями симптомов, а с причинами расстройства психики.

1 *Oberst, U.; Wegmann, E.; Stodt, B.; Brand, M.; Chamarro, A. Negative consequences from heavy social networking in adolescents: The mediating role of fear of missing out. J. // Adolesc. 2017.*

Все возрасты покорны соцсетям. Но особенности надо учитывать

В соцсетях сидят все, от мала до велика. Причем входной порог постепенно снижается: дети, которым сейчас 8–11 лет, стали интернет-пользователями в 6–7 лет, а малыши 5–7 лет освоили этот навык в свои 4–5 лет.



Детский Рунет-2018. Отраслевой доклад. — Институт исследований интернета.

Разумеется, дошкольники не зависают поголовно во ВКонтакте или где-либо еще. Чаще всего их привлекает YouTube, где персональные коммуникации между пользователями минимальны, а доступ к разнообразному контенту довольно прост. Однако, по сути, YouTube — это самая настоящая социальная сеть со всеми присущими ей механизмами, и даже просто смотря видеоролики, дети усваивают основные концепции работы соцсетей. Но многие этим не ограничиваются — они не хотят быть пассивными потребителями, им интересно создавать нечто свое.

По оценке британской неправительственной организации Internet Matters, 13% детей и подростков в возрасте от 11 до 16 лет ведут собственный канал или блог, более трети загружают видео на YouTube или другие платформы.

По данным компании First Choice, которая в 2018 году провела опрос среди тысячи британских детей и подростков в возрасте до 17 лет, 34% респондентов хотели бы стать звездами YouTube, а каждый пятый хотел бы вести собственный канал.

Компания Pew Research Center опубликовала исследование, в котором говорится, что видеоролики популярных YouTube-каналов, где появляются дети до 13 лет, набрали, вне зависимости от целевой направленности ролика, в три раза больше просмотров, чем другие ролики.

Такая популярность YouTube среди детей и подростков доставляет владеющей сервисом корпорации Google много хлопот с регуляторами. Ведь официально завести аккаунт и загружать свои произведения начинающие видеоблогеры могут только с 13 лет. Чтобы снизить для себя юридические риски и сохранить детскую аудиторию, в компании разработали приложение YouTube Kids, предоставляющее версию видеосервиса, ориентированную на детей, с подбором контента, функциями родительского контроля и фильтрацией видеороликов, которые для детей 12 лет и младше считаются неуместными.

*Мобильное приложение для iOS и Android было выпущено в 2015 году, а в августе 2019 года появилась и веб-версия YouTube для детей (**https://www.youtubekids.com/**). Настроить приложение должен кто-то из взрослых — на пути к его*

использованию стоит непреодолимый для самых юных пользователей барьер в виде задачи на умножение. Приложение рассчитано на три возрастные категории: для самых маленьких (до 4 лет), для дошкольников (от 5 до 7 лет) и для детей постарше (от 8 до 12 лет). Хотя, собственно, социальные функции спрятаны — лайкать и комментировать в детском приложении нельзя, можно искать и смотреть видео — и это все равно шаг в сторону киберсоциализации.

Facebook также требует, чтобы возраст создателя аккаунта был не менее 13 лет (в некоторых юрисдикциях возрастной ценз может быть и выше). Создание аккаунта с ложными данными является нарушением правил. Если малолетний пользователь решит немного приврать и накинуть себе несколько годков, то специально его ловить никто не будет. А вот когда он повзрослеет и вдруг захочет показать свой истинный возраст, то соцсеть автоматически удалит его аккаунт со всеми накопленными цифровыми богатствами. Будет обидно!

Аналогичных норм придерживаются и другие соцсети американского происхождения, включая Snapchat, Twitter, Instagram, TikTok и Skype. Их обязывает к этому законодательство США[1].

В некоторых странах установлены более высокие возрастные ограничения. В частности, парламент ЕС одобрил поправки к европейскому праву, согласно которым детям и подросткам до 16 лет для входа в соцсети потребуется согласие родителей. Новое правило вступило в силу в 2018 году. Требование распространяется на Facebook, Snapchat, Twitter, Instagram

1 *Children's Online Privacy Protection Act (COPPA).*

и другие социальные сети, среди пользователей которых много несовершеннолетних по всему ЕС. Если будет установлено, что правила доступа к интернет-сервисам нарушены, виновников накажут штрафом в размере вплоть до 4% годового оборота.

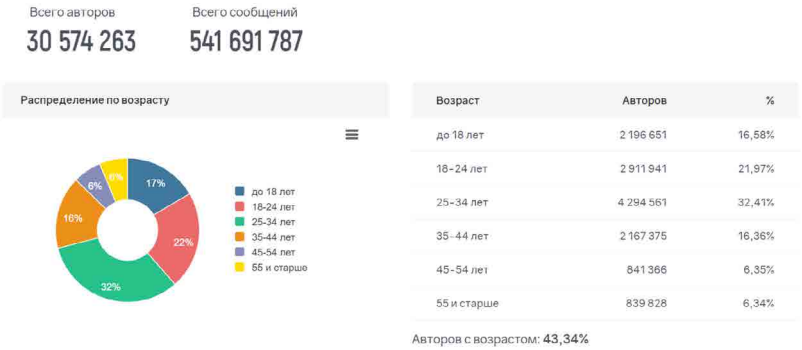
«Всегда будет возможность придумать способы обойти эти правила», — прокомментировал ситуацию сотрудник ведущей американской интернет-компании. По его словам, относительно высокий возрастной ценз принесет больше вреда, чем пользы, поскольку будет заставлять детей нарушать правила.

Для Европы масштабы этой проблемы являются значительными[1]. Так, в Великобритании каждый пятый ребенок младше 11 лет имеет аккаунт в Фейсбуке, хотя это нарушает даже собственные правила крупнейшей социальной сети мира. В возрастной группе от 12 до 17 лет Фейсбук используют до 80% британских детей.

В России легально пользоваться соцсетями могут граждане с 14 лет — этому правилу следует и самая популярная среди подростков площадка ВКонтакте, где только по официальной статистике доля несовершеннолетних авторов составляет 17%. Истинного положения вещей мы не знаем, потому что свой возраст публично показывают только порядка 40% пользователей. И многие, наверное, соврали насчет возраста, чтобы зарегистрироваться, поэтому доля малолетних авторов ВКонтакте на самом деле гораздо выше.

---

1 *Детям до 16 запретят выходить в соцсети без родителей. // Российская газета (спецпроект RG.RU Digital), 22 апреля 2016.*



Возраст	Авторов	%
до 18 лет	2 196 651	16,58%
18-24 лет	2 911 941	21,97%
25-34 лет	4 294 561	32,41%
35-44 лет	2 167 375	16,36%
45-54 лет	841 366	6,35%
55 и старше	839 828	6,34%

Распределение по возрастам авторов публикаций ВКонтакте за октябрь 2019 года[1].

Вообще говоря, искусственные барьеры для доступа подрастающего поколения к соцсетям, возводимые законодателями разных стран, только запутывают ситуацию. Если в баре у посетителя, выглядящего слишком молодо, при заказе алкоголя обычно требуют паспорт, то в интернете нет технически надежного и простого способа проверить возраст пользователя. Будьте уверены, что юристы больших корпораций найдут формулировки, которые помогут им избежать ответственности за невыполнение правил, невыполнимых в принципе, а дети так и будут продолжать врать насчет возраста, чтобы поскорее войти в цифровой мир.

В интернете нет технически надежного и простого способа проверить возраст пользователя.

Пожалуй, наиболее разумным в этом отношении выглядит подход YouTube: лучше создать специальное детское приложение и посте-

1 *Brand Analytics.*

пенно, по мере взросления, открывать доступ к более разнообразному контенту и функциям, чем пытаться «не пущать». К сожалению, почему-то больше никто этого не делает.

> *Россия занимает второе место в мире по участию населения в социальных сетях: 78% российских пользователей интернета имеют аккаунт в какой-либо из них. Нашу страну по этому показателю обгоняет только Япония, где соцсетями пользуются 88% пользователей интернета. За Россией следуют США и Великобритания с 75%, Швеция с 74% и Республика Корея с 72%.*
>
> *Такие данные содержатся в издании «Цифровая экономика: краткий статистический сборник» Высшей школы экономики (ВШЭ) за 2019 г. Сведения предоставлены за 2017 г. или за ближайшие годы, по которым имеются данные. Под населением России понимаются лица в возрасте от 15 до 74 лет*[1].

Надо признать, что возрастные ограничения, установленные законодателями, в целом, разумны. Дело в том, что пребывание в социальных сетях очень по-разному сказывается на младших и старших подростках.

Пребывание в социальных сетях очень по-разному сказывается на младших и старших подростках.

Межкультурные исследования 10 930 подростков из шести европейских стран (Греции, Испании, Польши, Нидерландов, Ру-

1 *Больше россиян в соцсетях сидят только японцы. Цифры. // CNews.ru, 7 февраля 2019.*

мынии и Исландии) показали, что интенсивное использование соцсетей (более двух часов в день) было связано с более низкой успеваемостью и более низкими показателями активности, особенно для младших подростков. Напротив, среди старших подростков более интенсивное использование соцсетей было положительно связано с офлайновой социальной компетентностью[1].

То есть возраст, обуславливающий различия в развитии социальных и регуляторных навыков, по-видимому, смягчает влияние интенсивного использования соцсетей на функциональное поведение подростков.

Как должен поступать ответственный родитель, вооруженный этими знаниями?

- Изо всех сил держать оборону, чтобы не допускать ребенка в соцсети раньше времени. Для общения с близкими достаточно и общего чата в мессенджере, например, в WhatsApp.

- Для младших подростков (14-15 лет) ограничивать время пребывания в соцсетях до двух часов.

- По достижении 16 лет слишком строгий контроль будет неуместен, а риск негативного влияния соцсетей относительно невелик.

---

1 *Tsitsika, A.K.; Tzavela, E.C.; Janikian, M.; Ólafsson, K.; Iordache, A.; Schoenmakers, T.M.; Tzavara, C.; Richardson, C. Online social networking in adolescence: Patterns of use in six European countries and links with psychosocial functioning.// J. Adolesc. Health 2014, 55, 141–147.*

«Так люди (первый каюсь я) от делать нечего друзья»

Пожалуй, Александр Сергеевич сильно преувеличил различия между Онегиным и Ленским. На самом деле, оба они придерживались европейских взглядов, и если бы в наши дни встретились не в деревне, а на просторах Фейсбука, то, вполне возможно, «зафрендились» бы. Конечно, их дружба не была бы безоблачной — они бы нещадно спорили и ругались, но, как правило, диванные споры до дуэли не доходят.

Как вообще люди знакомятся в социальной сети? Сначала они разыскивают своих друзей (в том смысле, как это понимали до интернета), родственников, одноклассников/одногруппников, коллег по нынешней и прежней работе, знакомых по разным тусовкам. Все вместе они составят едва ли сто человек — и на этом реальные контакты будут исчерпаны.

> *А дальше начинается социальная магия — то, ради чего и существуют Фейсбук, ВКонтакте, Одноклассники и другие сети. Мы начинаем знакомиться с незнакомцами, включая в друзья тех, кто (как нам кажется) разделяет наши ценности и публикует что-нибудь интересное — иначе как мы узнаем, что наши ценности совпадают?*

У взрослых это профессиональные темы, политика, хобби, отношения, путешествия, искусство, музыка, ЗОЖ, спорт, и, как говорится, далее везде. Любая тема может стать объединяющей — или разъединяющей. У молодого поколения, в принципе, все то же самое — отношения, музыка, школа, игры, хобби. И обязательно, чтобы было «прикольно» — зануда не может стать популярным в соцсети.

Иногда достаточно случайно увидеть человека в ленте, чтобы рука потянулась нажать кнопку «дружить». Виртуальная дружба не накладывает никаких обязательств — по сути, это подписка на стен-газету, которую публикует этот человек. Можно дружить заочно много лет и ни разу не общаться даже виртуально, не то, чтобы встречаться лично. Точно также появляются и ваши подписчики, которых интересует только ваш контент и вовсе не обязательно ваша персона.

Принцип «не добавлять в друзья тех, кого не знаешь лично» в соцсети не работает, это противоречит ее смыслу.

Поэтому принцип «не добавлять в друзья тех, кого не знаешь лично» в соцсети не работает, это противоречит ее смыслу. Другое дело, что надо быть настороже, когда новый «друг» предлагает «развиртуализироваться», то есть встретиться в реале. Здесь как раз применимы все известные советы по общению с незнакомцами. И, конечно, предварительно следует хорошенько изучить вашего виртуального друга — что он пишет у себя на странице, какие картинки выкладывает, как общается в комментариях. Это гораздо лучше характеризует человека, чем его профиль, информация в котором часто может быть неполной и недостоверной. Не стоит также ориентироваться на заявленные интересы и участие в сообществах, все это может быть просто случайным. Ведь и в реальной жизни надежнее будет оценка не по «одежке», а по тому, как человек ведет себя на самом деле.

Если профиль заведен совсем недавно, то это либо действительно новичок, либо бот — фальшивый аккаунт, созданный с какой-то целью.

Если профиль заведен совсем недавно, то это либо действительно новичок в сети, либо бот — фальшивый аккаунт, созданный

с какой-то целью. Опытные пользователи соцсетей вычисляют большинство ботов с первого взгляда — им помогает киберсоциальный интеллект. Но расслабляться не стоит — по-настоящему опасные преступники могут притворяться очень качественно.

> *Как узнать, что ваш виртуальный друг действительно тот, за кого себя выдает, и что его фото — настоящее? Очень просто: попросите его сделать видеозвонок, чтобы прояснить ваши сомнения.*

Хотя и существует технология глубоких фейков, позволяющая изменить лицо и голос так, что подделку будет невозможно отличить от оригинала, для видеозвонка это пока слишком сложно.

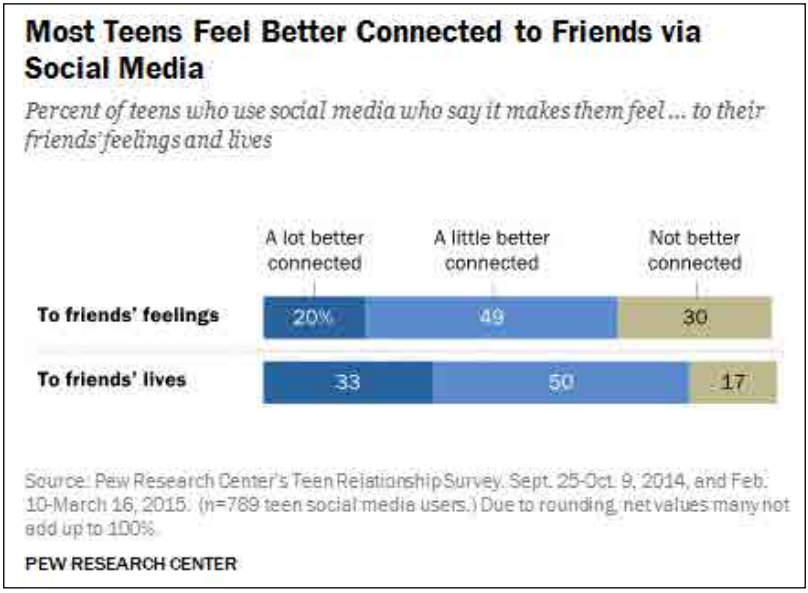
- Почти две трети (64%) американских подростков говорят, что они встретили новых друзей в социальной сети.

- Помимо поиска новых друзей, социальные сети — это основной способ взаимодействия подростков с уже существующими друзьями. Более 94% подтверждают, что проводят время с друзьями в социальных сетях.

- Девочки, которые используют социальные сети, чаще, чем мальчики, считают, что они намного лучше знают о жизни (40% против 26% мальчиков) и чувствах (24% против 16% мальчиков) своих друзей.

- В проблемные периоды почти семь из десяти подростков получают поддержку от друзей через социальные сети. Девочки

чаще получают такую поддержку — об этом рассказали почти три четверти (73%) девочек по сравнению с 63% мальчиков[1].



Когда подростки сидят, уткнувшись в свои телефоны, не торопитесь говорить, что они тупят. На самом деле они так общаются. Социальные сети связывают их с друзьями — так вы можете контактировать гораздо чаще, потому что вам не нужно видеться лично. Но есть у такой социальной открытости и темная сторона: например, подростки могут испытывать негативные эмоции, когда видят сообщения о событиях, куда их не пригласили.

1 *Teens, Technology & Friendship. // Pew Research Center, 6 августа 2015.*

Киберэмоциональный интеллект — ключ к успеху в цифровом мире

Пусть даже у вашего ребенка IQ как у Григория Перельмана — этого недостаточно, чтобы достичь успеха в жизни. Обладая мощным интеллектом, можно приносить пользу человечеству, решать непосильные для других математические задачи — и провести всю жизнь в должности младшего научного сотрудника. Для настоящего гения это ничуть не зазорно, но гениев единицы, а остальным волей-неволей приходится жить в коллективе, где нужно уметь строить отношения с людьми и работать в команде. Ключом к успеху в этом служит эмоциональный интеллект.

> *Мало быть просто умным. Надо еще понимать чувства и эмоции окружающих и уметь адекватно выражать собственные.*

Ребенок учится науке общения с себе подобными сначала в семье, потом в детском саду, в школе, колледже, институте — и вроде бы он отлично социализирован. А потом приходит в рабочий коллектив и — бац! — оказывается в распределенной команде, где проджект-менеджер сидит в Польше, дизайнеры в Питере, разработчики на Кипре и в Воронеже, а руководитель фирмы мотается вокруг глобуса как электрон вокруг ядра атома. Если у него нет навыков виртуального общения, то ему, может быть, весьма некомфортно в такой среде, где никто никого в глаза не видел, но при этом все как-то умудряются вместе делать общее дело.

> *Исследование[1], опубликованное в Журнале профессионального поведения в августе 2017 года, показало, что студенты, имевшие*

1 *Joseph C. Rodea, Marne Arthaud-Day, Aarti Ramaswami, Satoris Howesd. A time-lagged study of emotional intelligence and salary // Journal of Vocational Behavior, Volume 101, August 2017, Pages 77–89.*

более высокий эмоциональный интеллект (Emotional Intelligence, EI) во время учебы в колледже, через 10-12 лет в среднем получали больше своих сверстников с более скромными показателями EI. Дело в том, что люди с высоким EI, как правило, используют свои навыки, чтобы глубоко проникнуть в социальную среду компании — то есть, говоря языком соцсетей, заводят много друзей. Это дает им доступ к большему количеству информации и знающих коллег, что, в свою очередь, повышает их эффективность и приводит к повышению заработной платы.

Звучит логично и вполне совпадает с ироничной народной мудростью: «Сам себя не похвалишь — никто не похвалит». Иначе говоря, ваших достижений могут и не заметить, если вы будете тихо стоять в сторонке и ждать, пока кто-то обратит на вас внимание. Причем проблема не сводится к банальной дихотомии «экстраверт — интроверт» и предположению, что экстравертам общение дается легче. Эмоционально глухой, но чрезвычайно коммуникабельный экстраверт может наломать таких дров своей непосредственностью, что об успешной карьере можно будет забыть. Интроверты же часто обладают эмоциональным интеллектом даже в большей мере, чем экстраверты, но им бывает труднее перейти к реальным действиям на основе своих знаний.

Поэтому действовать нужно тонко и умно, учитывая чувства окружающих, а для этого — обладать целым комплексом навыков, которые в сумме и называют эмоциональным интеллектом.

По теории Майера-Саловея, которая появилась в начале 1990-х годов, эмоциональный интеллект имеет четыре составляющих: восприятие, использование, понимание и управление эмоциями, и оценивают его по этим четырем шкалам.

Так сложилось, что корпоративная культура в большинстве организаций выстроена под экстравертов, а если у них еще и высокий EI, то они получают огромное преимущество. Но едва мир окунулся в электронные коммуникации, квинтэссенцией которых можно считать социальные сети, где перемешаны все мыслимые форматы онлайн-общения, как сразу изменившиеся правила игры устранили одни привычные барьеры и создали новые. Например, есть люди, которые запросто могут подойти к другому человеку и завязать разговор, но написать связно пару строк для них — мучение. А есть те, кому, наоборот, куда проще изложить все письменно, чем сделать короткий звонок. Если раньше вторые чувствовали себя в некотором роде изгоями, то сейчас шансы «писателей» и «ораторов», по меньшей мере, уравнялись.

В социальных сетях появились новые способы выражения эмоций, которые надо уметь воспринимать, использовать и которыми нужно управлять.

И это — лишь поверхностный взгляд. На самом деле изменения гораздо глубже. В социальных сетях появились новые способы выражения эмоций, которые тоже надо уметь воспринимать, использовать, понимать и которыми нужно управлять. Написать кому-то сообщение сплошь заглавными буквами — это все равно, что накричать на человека: такой беззвучный взрыв эмоций способен навек разрушить давнюю дружбу. Поставленный лайк может быть расценен как явное выражение симпатии (хотя иногда лайк — это просто лайк, как мог бы сказать старина Фрейд из известного анекдота). И, наоборот, отсутствие лайка — оказаться поводом для ссоры: поди потом объясни, что ты просто не видел замечательного котика, а не намеренно проигнорировал пост своей подруги!

В этой связи исследователи из университета Nice Sophia-Antipolis[1] сочли возможным говорить о киберэмоциональном интеллекте. «С нашей точки зрения, социальные взаимодействия в интернете изменяют интенсивность и форму выражения эмоций», — пишут они. Их главный вывод заключается в том, что некоторые люди могут иметь низкий эмоциональный интеллект в реальной жизни, но, имея высокий киберэмоциональный интеллект, способны чувствовать себя лучше в киберпространстве (и наоборот). Хотя термин «киберэмоциональный интеллект» не является сегодня общепринятым, он, на наш взгляд, хорошо описывает происходящее, и поэтому мы будем им пользоваться».

Подростки развивают свой киберэмоциональный интеллект интуитивно, общаясь в соцсетях, набивая шишки и делая открытия — точно также, как малыши в детском саду нарабатывают азы обычного эмоционального интеллекта. И они вполне преуспевают в этом, если им не мешать. Нужно иметь достаточно чуткости, чтобы по нескольким постам понять, действительно ли друг в депрессии и ему нужна помощь, или он находится «в образе» и постит мрачные тексты и картинки просто для развлечения.

Взрослые, лишенные этих навыков, часто бьют тревогу на ровном месте — стоит им лишь увидеть на странице своего ребенка вместо радужных пони нечто, по их мнению, зловещее. Впрочем,

---

1 *Adel Ben Youssef, Hamida Ben Youssef. Social Networking on Web 2.0: From Emotional Intelligence to Cyber Emotional Intelligence // Management Information Systems — Vol. 6 (2011), No. 2, pp. 021–028.*

о «синих китах» и прочих «группах смерти» мы уже говорили в Главе 5, и отметили, что проблема деструктивного контента и вовлечения детей и подростков в подобные сообщества действительно существует. Сейчас речь о другом: для успеха в цифровом мире нужно иметь развитый киберэмоциональный интеллект, и приобрести его можно единственным способом — регулярно общаясь в соцсетях. Лишая своего ребенка опыта такого общения, вы, вполне возможно, тем самым уменьшаете его будущую зарплату[1].

Лишая ребенка опыта общения в соцсетях, вы, возможно, тем самым уменьшаете его будущую зарплату.

«Скажите, где можно записать ребенка в группу раннего развития киберэмоционального интеллекта?» — так должен отреагировать ответственный родитель на эту информацию. Но всему свое время. Соцсети — это не балет и не художественная гимнастика, особо спешить с киберсоциализацией не стоит. Сначала маленькому человеку нужно освоить обычное общение, а потом уже переходить в онлайн. Хотя, возможно, мы заблуждаемся, грань между онлайном и офлайном скоро окончательно сотрется, и даже младенцы смогут удаленно общаться с себе подобными и со взрослыми.

---

1 *Существует и противоположная точка зрения. Есть исследователи, считающие, что общение в интернете убивает эмпатию. Дженнифер Аакер, профессор Стэнфордской высшей школы бизнеса и соавтор книги «Эффект стрекозы», проанализировала 72 исследования, в которых приняли участие почти 14 тысяч студентов колледжей в период с 1979 по 2009 год, и показала резкое снижение уровня эмпатии за последние 10 лет.*

Дружить или нет? Решить за 10 секунд

Для многих взрослых, даже считающих себя ветеранами соцсетей, остается загадкой, как подростки ориентируются в этом пространстве. Чем обусловлена их манера поведения и выстраивания коммуникаций, способы поиска и оценки информации? Как они решают, с кем дружить, а с кем нет, на что подписаться, а что игнорировать, когда поставить лайк, а когда и пальцем шевельнуть не стоит? Тем не менее, они с этим справляются — кто-то лучше, кто-то хуже, но в целом успешно. И если понять, как именно они это делают, то можно будет помочь отстающим и не мешать тем, у кого и так все хорошо.

Ученые психологического факультета МГУ попытались разобраться в том, каким образом подростки оценивают информацию в социальной сети и какие модели поведения у них складываются — ведь от этого зависит, в том числе, их безопасность. С этой целью в образовательном центре «Сириус» летом 2019 года было проведено поисковое исследование, в котором приняли участие сорок подростков. Им поочередно показывали в течение 10 секунд один из двадцати специально отобранных профилей ВКонтакте и просили ответить на пять вопросов:

1. *Хотите ли вы добавить этого пользователя в друзья?*
2. *Примите ли вы от него заявку на добавление в друзья?*
3. *Хотите ли вы поставить лайк на его фотографии?*
4. *Хотели бы вы сделать репост записи с его страницы?*
5. *Хотели ли бы вы начать общение с этим человеком?*

На взгляд взрослых, особой разницы между этими действиями, казалось бы, нет. Но на самом деле это не так, и «сириусовцы» продемонстрировали это ученым-психологам весьма наглядно. Например, пригласить кого-то в друзья или самому откликнуться на приглашение оказалось для испытуемых совершенно не одно и то же.

Даже столь малого времени подросткам было достаточно, чтобы принять решение: дружить или нет, и как именно к этому подступиться. Причем среди показанных испытуемым профилей были и фейковые — либо имитирующие страницу какой-либо известной в подростковой среде знаменитости, либо не содержащие реальной информации. Участники эксперимента отлично разобрались, что к чему, и не стали общаться с фейками.

Здесь особо тревожные родители могут немного выдохнуть: профессиональные пользователи соцсетей, каковыми являются почти все подростки, имеют «нюх» на фейковые аккаунты, ввести их в заблуждение не так-то легко. То есть едва ли взрослый дядя, лелеющий грязные намерения, сможет долго притворяться 15-летней девочкой и вести аккаунт как бы от ее имени, чтобы втереться к подростку в доверие. Вероятность такого развития событий существует, но она достаточно мала. А что касается звезд, то все гораздо проще: администрация ВКонтакте ввела верификацию страниц, поэтому достаточно одного взгляда, чтобы распознать, настоящий это аккаунт знаменитости или фейковый.

Некоторое время назад пользователям ВКонтакте стала доступна возможность верификации (подтверждения) стра-

ницы и группы. Это позволяет отличить настоящих звезд от фейков. Например, раньше во ВК было несколько десятков Филиппов Киркоровых, и определить настоящего было очень трудно.

Теперь достаточно одного взгляда — и все ясно: если возле имени в профиле стоит специальная галочка, значит, страница прошла подтверждение. Пока этим пользуются преимущественно известные личности, потому что именно они особенно страдали от фейков. Кроме того, верификация возможна для сообществ, а также для официальных страниц городов и регионов России.

Обычные пользователи теоретически тоже могут получить такой зачетный значок, но им для этого придется изрядно постараться. Самый прямолинейный способ — стать звездой. То есть число поклонников у вас должно быть больше числа друзей, желательно иметь о себе статью в Википедии, публикации в СМИ, не нарушать правил сообщества и быть активным пользователем. Но и это не гарантирует успеха — администрация ВКонтакте может отказать в верификации без объяснения причин[1].

Ставя эксперимент в «Сириусе», ученые хотели выяснить, как коррелируют между собой психологический профиль подростка, и то, как он ведет себя в социальной сети и выбирает друзей. Поэтому перед экспериментом все участники прошли психологическую диагностику по трем блокам факторов.

---

1 *Правила прохождения верификации доступны по адресу* ***https://vk.com/page-22079806_49606709***

Первый блок был посвящен отношениям со сверстниками: насколько испытуемые доверяют этим отношениям; до какой степени могут быть откровенны и рассчитывать, что их поймут; чувствуют ли какое-либо отвержение со стороны своих друзей или нет.

Второй блок касался эмоционального интеллекта, причем проводилась субъективная оценка (как испытуемые думают о себе сами) и объективная (по результатам тестов).

Третий блок включал выявление когнитивных методов оценки информации[1], применяемых подростками при пользовании социальными сетями. Здесь, пожалуй, нужны некоторые пояснения. Когда мы сталкиваемся с новой информацией, у нас в голове прокручивается определенный цикл — грубо говоря, нам нужно понять, что это такое и что со всем этим делать. А если выражаться научным языком, то, по модели Крика и Доджа[2], есть шесть этапов когнитивного оценивания социальной информации: ее восприятие, интерпретация, прояснение целей автора, планирование возможных ответных действий, решение о действии и реализация действия. И на каждом этапе могут проявляться особенности, связанные с психологическим профилем конкретной личности, который обуславливает разные способы когнитивной переработки социальной информации и реакции на нее.

---

1 *Когнитивное оценивание — процесс восприятия и интерпретации субъектом тех или иных обстоятельств, результатом которого является субъективная картина ситуации в сознании человека. Понятие введено Ричардом Лазарусом в рамках транзакционной теории стресса (Википедия).*

2 *Crick N.R. & Dodge K.A. (1994). A review and reformulation of social information-processing mechanisms in children´s social adjustment. // Psychological Bulletin, 115, 74–101. doi:10.1037/0033-2909.115.1.74.*

Годом раньше исследований в «Сириусе», на психологическом факультете МГУ проводилось отдельное исследование[1] на эту тему, в котором участвовали более 200 тинейджеров от 13 до 18 лет. После компьютерной обработки результатов методом кластерного анализа вся выборка разделилась на три группы.

Первую группу условно назвали «поведенцы» — к ней отнесли подростков, действующих методом проб и ошибок. У них плохо работает этап интерпретации и формулирования собственного решения — «чего я хочу в этом общении?» И в этом есть определенные риски: человек вступает в диалог, не имея представления о своих целях. Такие подростки часто становятся членами различных групп, в том числе девиантного и даже деликвентного поведения[2].

Вторую группу составили так называемые «аналитики», у которых все хорошо с восприятием и интерпретацией замысла автора и с формулированием собственного ответа, но нет действия. Такой подросток, встретив даже неприятный для себя контент и понимая, что он ему не нужен, может все равно на нем «залипнуть» просто в силу своей пассивности — ведь нажатие на крестик, закрывающий страницу, тоже требует

---

1 *Молчанов С.В., Алмазова О.В., Поскребышева Н.Н. Когнитивные способы переработки социальной информации из интернет-сети в подростковом возрасте // Национальный психологический журнал. — 2018. — №3(31). — С. 57–68. doi: 10.11621/npj.2018.0306*

2 *Делинквентное поведение — это асоциальное, противоправное поведение, проявляющееся в действиях, которые приносят вред обществу, угрожают жизни других людей и общему социальному порядку, и являются уголовно наказуемым (Википедия).*

усилия. У таких подростков тоже довольно высок риск быть втянутыми в различные деструктивные сообщества.

И, наконец, к третьей группе были отнесены подростки с эффективным типом когнитивной переработки информации. Их показатели по подавляющему большинству параметров оказались высокими: они хорошо понимают содержание информации и то, что именно хотел сказать автор; они способны рефлексировать по поводу того, чего хотят от этого взаимодействия сами; они могут формулировать альтернативы и реализовывать свой выбор.

Исследователей порадовал тот факт, что «эффективных» подростков оказалось около половины, а «поведенцев» и «аналитиков» примерно по четверти от всей выборки. При этом оказалось, что «эффективные» наименее подвержены интернет-зависимости, а два других типа, наоборот, склонны становиться рабами гаджетов.

Также в ходе исследования была изучена связь того, как человек обрабатывает информацию, с базовыми убеждениями личности[1]*. Эффективным подросткам оказалась свойственна вера в доброжелательность окружающего мира, уверенность в контроле над собственной жизнью, способность конструировать адекватное поведение, вера в удачу. У них нет ощущения, что «весь мир против меня» и «обязательно ничего не получится». То есть эффективный способ переработки ин-*

1 *Базовые убеждения личности — это определенные мировоззренческие установки, которые определяют представление о том, как строится взаимодействие человека с окружающим миром, в том числе социальным.*

формации связан с активной позицией человека и стремлением самостоятельно выстраивать свою жизнь.

Но вернемся к эксперименту в «Сириусе». По его результатам выборка тоже разбилась на три сильно отличающихся друг от друга кластера. Их назвали «идеализирующий», «селективный» и «осторожный» — в соответствии с манерой поведения в социальной сети.

«Идеалисты» считают, что у них прекрасные, полные теплоты и доверия отношения со сверстниками, что они очень хорошо распознают эмоции (на самом деле — средне). Но их когнитивные способности оставляют желать лучшего. Отсюда и их манера поведения в соцсети: они легко раздают лайки и готовы общаться со всеми подряд, не разбирая, где профиль «опасный», а где «не опасный». Подростки этого типа практически не дифференцируют способы коммуникации в интернете. Если они ставят лайк, это означает, что они тут же готовы общаться, принять или послать запрос. Сделав какое-то одно действие, они тем самым демонстрируют, что готовы и к остальным.

Подростки, отнесенные ко второму типу (селективному), считали, что у них отношения со сверстниками теплые, очень здоровые, но при этом не отрицали, что друзья не всегда их понимают, и что друзьям может быть не до них. «Селективисты» полагают, что в целом неплохо оценивают и распознают чужие эмоции и могут контролировать свои, но объективные оценки распознавания эмоций у них самые высокие. У этой группы также самые высокие показатели по когнитивному оцениванию и социальным действиям. Изучая предложен-

ные им профили, они несколько раз возвращались к основной информации после просмотра других зон и более взвешенно принимали решение.

Самой многочисленной оказалась третья группа — «осторожные». Они считали, что в их отношениях со сверстниками есть трудности, и что они не очень хорошо распознают эмоции — и это на самом деле именно так. Все циклы обработки информации у них оцениваются низкими баллами. Их активность в соцсети во многом завязана на лайк. Причем для них важнее получать лайки — сами они ставят их реже других.

Конечно, этот эксперимент не дает исчерпывающих ответов на вопрос, как определить возможные риски пребывания в соцсети для конкретного подростка, и чем ему помочь, чтобы эти риски снизить. Ясно, что в «Сириус» попадают не самые обычные дети, и полученную статистику не стоит обобщать широко. Но некоторые выводы сделать все-таки можно.

Во-первых (это уже становится рефреном), не надо паниковать по поводу пребывания подростков в социальных сетях. Именно так с приходом в нашу жизнь технологий происходит сепарация ребенка от родителей, и сегодня это — необходимый этап взросления. Родители перестают быть авторитетом, подросток ищет общения со сверстниками, а общаются они во ВКонтакте и в других соцсетях. Это нормально.

Если вам повезет, и ваш сын или дочь вас «зафрендит», считайте это огромным знаком доверия. Кого ни попадя в свое виртуальное пространство подростки не пускают.

Оказавшись там, вы сможете наблюдать за тем, как ваш ребенок живет, чем интересуется. Только, пожалуйста, не активничайте сверх меры, стойте тихо в сторонке и смотрите. Не надо каждый день постить на его странице разные «мемасики» или встревать со своими комментариями в их дискуссии. Вам достаточно просто быть рядом. Быть со своим ребенком в контакте (и во ВКонтакте) — самый простой и надежный способ избежать опасностей, которые в интернете действительно существуют.

Из чего же сделаны наши девчонки?

Мальчики и девочки пользуются соцсетями по-разному. В принципе, ничего нового: в интернете все то же самое, что и в известной песенке про мальчишек и девчонок, и эта разница играет заметную роль в том, какое влияние соцсети оказывают на психику подростка.

68 % девочек подписаны на аккаунты звезд красоты, моды и реалити-шоу — это похоже на ограниченную диету, состоящую из нездоровой пищи. Мальчики в большинстве своем тоже подписаны на разного рода «мусор», но, в отличие от девочек, их диета разнообразнее: в среднем они имеют по двенадцать сильно различающихся интересов[1].

Требование или просьбу ограничить время пребывания в соцсети девочки-подростки воспринимают как большую жертву.

1 *Terri Apter Ph.D. How to Reduce the Toxicity of Teen Girls' Social Media Use // Psychology Today, 20 октября 2019.*

Требование или просьбу родителей ограничить время пребывания в соцсети девочки-подростки воспринимают как большую жертву, потому что они в этом случае (как они полагают) не будут в курсе происходящего и отстанут от жизни.

Изучение набора данных, содержащегося в профилях 34500 девушек и предоставленного образовательной благотворительной организацией «Женщины-лидеры» (The Female Lead), показало, что среди 50 ведущих знаменитостей, за которыми следили девочки, 72% были мужчинами. Только у 3057 (примерно 10%) девочек среди ключевых слов, описывающих их интересы, были такие как журналист, технология, благотворительность, генеральный директор, женщина, феминистка, основатель, книга, новости и награда. И вот у этих 3057 80% из 50 знаменитостей, за которыми они следили, составляли женщины, по крайней мере две из которых добились серьезного успеха.

Чтобы переключить внимание с бесцельного слежения за жизнью звезд, девочек попросили сделать одну простую вещь: подписаться на профили четырех женщин с высокими достижениями, которые были специально подобраны в соответствии с их интересами. В эксперименте принимали участие 28 девочек в возрасте от 14 до 17 лет из пяти разных школ и разных слоев общества. Примерно через девять месяцев исследователи провели с ними повторные интервью и были поражены тем, насколько изменились интересы девочек в соцсетях. Например, одна из них, подписанная на страницу женщины-астронавта, стала, кроме того, подписчицей NASA

и начала интересоваться физикой, другая увлеклась музыкой, третья обрела еще какой-то интерес.

В принципе, на этот эксперимент можно посмотреть шире, вне связи с феминизмом. Не надо ныть и сетовать, что ваш ребенок смотрит в соцсетях какой-то сплошной «трэш». Нравоучения вроде «почитай что-нибудь полезное» тоже не помогут: он или она просто не умеют найти в Сети то, что им действительно интересно, а часто и не подозревают о том, что именно может вызвать их интерес. Эту работу должны проделать вы, взрослые. Просьба подписаться на несколько найденных вами страниц не будет выглядеть насилием или вторжением в его личное пространство, а эффект может оказаться весьма благотворным.

Да и мальчиков, кстати, это тоже касается.

Вредные советы

Как только что-нибудь становится популярным, сразу появляется толпа «экспертов», раздающих советы на модную тему. Начался сезон грибов — посыпались советы грибникам; замаячил впереди Новый год — пойдут советы, как накрыть стол, что надеть и как встречать. И так до бесконечности.

Разумеется, любители давать советы не могли пройти мимо такого явления, как социальные сети, и поработали на славу — благо спрос на это всесезонный. Только вот большинство этих советов — вредные, причем безо всяких кавычек, совсем

не как у Григория Остера[1]. И, к сожалению, интернет ими переполнен. Знакомо?

«Как не стать «интернет-зомби» и понять, что жизнь без социальных сетей тоже существует».

«10 вещей, о которых нельзя говорить в социальных сетях».

«12 вещей, о которых ни за что нельзя рассказывать в Фейсбуке!».

«13 вещей, о которых нельзя рассказывать в Фейсбуке — ради вашей же безопасности!».

«21 рекомендация для снижения степени зависимости от социальных сетей».

«Что ни в коем случае нельзя публиковать в интернете».

«Почему вам рекомендуется не регистрироваться в социальной сети ВКонтакте?».

«7 причин отказаться от соцсетей».

«Чего не стоит делать в социальных сетях. 4 главных табу».

---

1 *«Вредные советы» — книга писателя, сценариста и телеведущего Григория Остера, в смешной, иронической и парадоксальной форме рассказывающая детям (и родителям) о том, что стоит и чего не стоит делать. Послужила основой для целой серии книг, в той же стилистике касающихся самых разных сторон взаимодействия детей и подростков с окружающим миром (Прим. ред.).*

В чем же их вред? А в том, что крупицы действительно полезного перемешаны в такого рода опусах с абсурдными или невыполнимыми рекомендациями, и фильтровать этот мутный поток очень трудно.

Часто задача автора ограничивается тем, чтобы хорошенько напугать читателя, вызвать шок, желание немедленно удалить все свои аккаунты из всех соцсетей и ни в коем случае не пускать туда своего ребенка. Правда, это желание быстро проходит, и люди забывают не только о нем, но и о реальных рисках. А доходы от рекламы, показанной вам на страницах с броскими алармистскими заголовками, остаются в карманах владельцев сайтов.

Итак, какие советы можно считать точно бесполезными?

Наш рейтинг возглавит совет не публиковать фотографий с чемоданами и не рассказывать про поездки в отпуск или на дачу.

Пожалуй, наш рейтинг вредных советов возглавит совет не публиковать фотографий с чемоданами и не рассказывать про поездки в отпуск или даже на дачу. Якобы преступники будут знать, что вас нет дома, и могут ограбить вашу квартиру. Помилуйте, вот взломщикам больше делать нечего, как листать ваш Инстаграм в надежде увидеть традиционную фоточку из аэропорта! По статистике более 80% взломов и краж совершаются в обычные будние дни, когда большая часть людей находится на работе. Причем к разряду квалифицированных относятся лишь 15% всех краж со взломом; остальные совершаются неопытными подростками, бомжами или алкоголиками. Как правило, у них нет заранее подготовленного и проработанного плана действий[1].

1 *Квартирные кражи, статистика, способы проникновения, меры предосторожности. // Статьи о GSM сигнализациях на сайте* ***Videogsm.ru.***

«Отпускные» фотографии в соцсетях никак не влияют на вероятность квартирной кражи.

Так что «отпускные» фотографии в соцсетях никак не влияют на вероятность квартирной кражи. Даже если вас конкретно «пасут», вы можете так торопиться к самолету, что не успеете «зачекиниться» перед вылетом. Едва ли профессионалы своего дела будут полагаться на такой зыбкий источник информации как соцсеть, когда можно просто подкупить дворника, охранника или консьержа. Или — чтобы не подвергать себя риску возникновения лишних свидетелей — установить наблюдение за вашей квартирой. Короче, врежьте хорошие замки, закройте двери и окна, если в квартире есть что-либо ценное, поставьте ее на сигнализацию и продолжайте радовать друзей жизнерадостными картинками из экзотических мест.

Но есть важная деталь: действительно не стоит публиковать фото посадочного талона, особенно до посадки на рейс. Кто угодно из увидевших его может зайти на сайт авиакомпании, ввести имя, код бронирования и попытаться аннулировать ваш обратный билет.

Но есть важная деталь: действительно не стоит публиковать фото посадочного талона, особенно до посадки на рейс.

Если уж очень хочется похвастаться, то сделайте так, чтобы в кадр не попали никакие личные данные, в том числе и штрих-коды. Прочесть штрих-код не так трудно, как кажется, а в нем содержатся полные данные о пассажире — имя, номер рейса, маршрут, код бронирования, номер билета, номер карточки часто летающего пассажира и многое другое. Зная это, злоумышленник сможет, например, использовать ваши накопленные мили.

Впрочем, этот риск стремительно уходит в прошлое — на смену бумажным посадочным талонам уже приходят электронные, с ними вы будете избавлены от соблазна сделать фото, компрометирующее ваши данные.

Не менее вредным выглядит предложение отключить геолокацию и не использовать геотеги на фотографиях и в постах.

Не менее вредным выглядит и предложение вовсе отключить геолокацию и не использовать геотеги на фотографиях и в постах (опять же, из соображений, что жулики узнают, что вас нет дома). Во-первых, геолокация полезна — многие приложения, в том числе и соцсети, используют геоданные, чтобы давать вам релевантную информацию. Во-вторых, все почему-то забывают одну вещь: вы можете поставить под своей фотографией любую геометку. Например, на самом деле вы лежите на песочке возле пруда на даче, а пишете, что загораете, допустим, на Фиджи. При наличии воображения каждый может создать себе красивую легенду.

Все почему-то забывают, что можно поставить под своей фотографией любую геометку.

Например, Франц Кафка никогда не покидал родной Праги, однако написал роман «Америка», в котором вполне достоверно передана атмосфера жизни эмигрантов из Европы за океаном. Говорят, что и Марко Поло не был в Китае, а пересказал истории персидских купцов, которых встречал на берегах Черного моря. Верить всему публикуемому в соцсети может только очень наивный человек.

Следующим идет совет скрывать свой день рождения и дни рождения своих близких, потому что это якобы ставит под угрозу вашу финансовую безопасность: полной даты рождения иногда бывает достаточно для кражи аккаунта или подбора пароля. А как же тогда ваши друзья узнают, когда вас поздравлять? Пожалуй, правильным советом будет не использовать памятные даты в качестве пароля.

Правильным советом будет не использовать памятные даты в качестве пароля.

Сюда же можно отнести совет не упоминать девичью фамилию матери, поскольку это часто используется как кодовое слово для банка. Когда банкиры придумывали свои правила безопасности, им казалось, что никто посторонний не может узнать, какую фамилию носила ваша мама до замужества. С появлением интернета и соцсетей это перестало быть тайной. Например, на акции «Бессмертный полк» многие участники несут фотографии своих дедов и публикуют их в соцсетях. Никто не спорит, что важно помнить их подвиги и рассказывать о них. Но! Фамилия деда с материнской стороны чаще всего как раз и есть девичья фамилия вашей матери. Впрочем, найдутся и другие способы узнать этот секрет, поэтому разумной тактикой будет в качестве кодового слова указать любую другую фамилию, хоть Плантагенет, если вы являетесь поклонником короля Ричарда Львиное Сердце. Ведь банк не интересует, правда ли это. Главное, чтобы вы не забыли ответ на проверочный вопрос.

Будет разумной тактикой в качестве кодового слова указать любую другую фамилию, а не девичью фамилию матери.

Также «эксперты» советуют не использовать свое настоящее имя, а детям — не указывать школу, класс и домашний адрес. Из всего этого, пожалуй, разумным будет только не раскрывать в Сети свой адрес. Остальное уже утратило актуальность. Во-первых, большинство соцсетей в своих правилах требуют регистрироваться под настоящими именами. Любой аккаунт, который покажется фейковым, может быть заблокирован и удален. Во-вторых, это лишено практического смысла — вымышленные имена и легенды на самом деле не гарантируют безопасности, а только мешают нормальным контактам с потенциальными друзьями. Как одноклассникам найти друг друга, если все будут шифроваться? (Это не касается игровых аккаунтов: там нужно играть роль — на то она и игра).

О чем действительно лучше помалкивать

Есть вещи, о которых и правда не стоит распространяться в соцсетях, чтобы не получить мешок больших и маленьких неприятностей. Условно запретные темы можно разделить на три категории.

- Вам потом будет стыдно.
- Это запрещено правилами соцсети.
- У вас будут проблемы с законом.

Прежде всего, следует помнить, что социальная сеть — это публичное пространство. Даже если вы что-то пишете «под замком», то есть ограничиваете доступ к посту только друзьям или какой-то отдельной группе, это может случайно оказаться

на всеобщем обозрении. Нажали нечаянно не ту кнопку — и все. Или вы сплетничаете о ком-то, а потом этого человека кто-то добавляет в группу. Или запостили какую-то, как вам кажется, забавную фоточку с вечеринки — и забыли. А потом пришли устраиваться на работу в серьезную организацию, где шуток не понимают. Написали что-то ехидное в комментариях какому-нибудь виртуальному знакомому, которого и в глаза не видели, и вдруг неожиданно встретились с ним в общей компании. Упс!

Чтобы не попасть в неловкую ситуацию из-за своих публикаций, лучше заранее настроиться на то, что никаких секретов нет.

В общем, чтобы не попасть в неловкую ситуацию из-за своих публикаций, лучше заранее настроиться на то, что никаких секретов нет. Просто представьте, что все, написанное вами и выложенное в социальную сеть, публикуется во всех центральных газетах и показывается по главным телевизионным каналам. И это видят ваши мама и папа, бабушка и дедушка, друзья и подруги, классный руководитель и директор школы, соседи, прохожие на улице, пассажиры в метро. И все вас узнают и смущенно отводят глаза. Будьте готовы отвечать за каждое свое слово или картинку. Не уверен — не публикуй! Даже Цукербергу приходилось извиняться.

Фейсбук в том виде, в каком мы его знаем, родился не сразу. Сначала Марк Цукерберг сделал сайт, на котором показывались попарно фотографии девушек, и можно было выбрать, которая из них более привлекательна. Прикольная идея, не правда ли? Мужская часть студентов Гарварда мгновенно подсела на новое развлечение, из-за чего в первую же ночь работы сайта упала сеть университетского кампуса.

Секрет успеха был в том, что Цукерберг использовал реальные фотографии студенток, взломав для этого базы данных общежитий. Вполне понятно, что далеко не всем девушкам эта забава понравилась, мягко говоря. И у многих из них были парни, у которых руки чесались объяснить обидчику, где и в чем он неправ. В общем, юный гений угодил в весьма щекотливую ситуацию. Скандальный сайт пришлось закрыть, Цукерберг получил административный выговор за взлом системы безопасности, нарушение авторских прав и неприкосновенности частной жизни. И еще ему пришлось публично извиняться перед всеми девушками. Легко отделался! Могли бы и побить.

Справедливости ради уточним: было так на самом деле или нет, доподлинно неизвестно. Но такова версия авторов фильма «Социальная сеть».

Со вторым пунктом теоретически все довольно просто: внимательно читайте правила конкретной соцсети и не нарушайте их. Следствием нарушений может стать — и, как правило, становится — сначала временная блокировка аккаунта, а потом и пожизненная. Подумаешь, скажете вы, я заведу новый. В принципе, да, это возможно — до тех пор, пока сохраняется возможность регистрироваться в соцсетях без предъявления паспорта. Вы рискуете потерять только собранную на вашей странице информацию и свой рейтинг. Это примерно то же самое, что и гибель вашего персонажа в игре, когда приходится все начинать с нуля и «прокачивать» его заново. Не смертельно, но злоупотреблять этим не стоит. Потому что общий тренд ведет к тому, что идентификация пользователей в соцсетях будет примерно такой же, как в банке или на сайте Госуслуг.

Все идет к тому, что идентификация пользователей в соцсетях будет примерно такой же, как в банке или на сайте Госуслуг.

Судите сами. С одной стороны, мы имеем китайский опыт доступа в интернет по паспорту в интересах государственной цензуры — об этом было объявлено в 2017 году. Форумам и интернет-платформам с возможностью комментирования было вменено в обязанность ввести процедуру привязки реальных паспортных данных пользователей к их аккаунтам для идентификации их личности — это касалось не только новых, но и существующих пользователей. «Положение позволит повысить уровень научности и культуры среди комментариев в интернете, будет содействовать здоровому развитию интернет-сообщества, защитит интересы граждан, юридических лиц и других организаций, а также государственную безопасность и общественные интересы», — гласил официальный документ.

В России принят аналогичный закон об идентификации пользователей в мессенджерах, который должен был начать действовать с 5 мая 2019 года[1], но пока еще не заработал в полную силу.

С другой стороны, Фейсбук добьется почти такого же результата демократическими методами: чтобы пользоваться разными услугами и совершать покупки в социальной сети, вам нужно будет иметь кошелек, который будет привязан к вашему аккаунту, и в этом случае, скорее всего, тоже потребуется идентификация

1 *Федеральный закон от 29 июля 2017 г. № 241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона “Об информации, информационных технологиях и о защите информации”».*

личности. Десять против одного, что американские власти будут настаивать на этом во избежание незаконных финансовых транзакций — отмывания денег, полученных преступным путем, финансирования терроризма и тому подобного.

> *Для обычных граждан это будет означать: однажды заведя аккаунт в соцсети, создать другой будет весьма непросто: паспорт-то у тебя один, если только ты не шпион или спецагент. Так что лучше не злить модераторов, чтобы не оказаться за дверями этого клуба. Второй раз могут и не впустить.*

Правила всех соцсетей, в принципе, похожи[1]. Нельзя публиковать материалы о насилии, терроризме, проявлении ненависти, восхвалять людей или группы, которые этим занимаются, пропагандировать действия, причиняющие вред людям и животным, вандализм, описывать схемы мошенничества так, чтобы их можно было повторить, самоубийства и способы их совершения, и так далее.

Например, вы узнали о какой-то ошибке в работе банкомата и, думая, что это крутой лайфхак, спешите поделиться им с друзьями. А на самом деле это способ незаконного обогащения, который вы пропагандируете. Лучше напишите в службу поддержки банка, а не в соцсеть.

Нельзя допускать враждебные высказывания в отношении людей, мотивированные их расовой или этнической принадлежностью, национальностью, вероисповеданием, сексуальной ориентацией,

---

1 *Подробнее см. Нормы сообщества Фейсбук — **https://www.facebook.com/communitystandards/introduction**. Правила пользования Сайтом ВКонтакте, п. 6.3.4 **https://vk.com/terms***

кастой, полом или гендерной идентичностью, а также наличием серьезного заболевания или инвалидностью; все это так называемые «характеристики, подлежащие защите от дискриминации».

И хотя в правилах сообщества написано: «Мы разрешаем юмор и общественную критику на эти темы», вы не можете заранее знать, как отреагируют люди на вашу шутку про те или иные национальные черты. Вдруг кто-то шуток не понимает? Юмор вообще вещь тонкая, это чувство не всем дано. А в результате вы отправитесь в бан для начала, дней на тридцать.

> *Наконец, самое важное: не нарушать законы РФ. К сожалению, сделать это очень легко: достаточно буквально одного клика — и вы преступник. Случайный репост может обернуться реальным сроком, глупая шутка — серьезным штрафом.*

Особенно, если это произошло в российской сети ВКонтакте. Согласно пункту 6.4. ее правил, «Пользователь несет личную ответственность за любую информацию, которую размещает на Сайте, сообщает другим Пользователям, а также за любые взаимодействия с другими Пользователями, осуществляемые на свой риск».

> *Судебная практика позволяет сделать вывод, что администрация ВКонтакте активно сотрудничает со следственными органами, раскрывает данные пользователей, их адреса, телефоны, время выхода в интернет. Вы даже не успеете и лайками насладиться, как за вами придут.*

Так называемых «экстремистских» статей в российском Уголовном кодексе несколько. Кроме 282-й (возбуждение ненависти и враж-

ды), это статья 354.1 (реабилитация нацизма), 148-я (оскорбление чувств верующих), появившаяся после панк-молебна Pussy Riot в 2012 году, и самая новая — 280.1 (призывы к сепаратизму), которая вступила в силу в мае 2014 года после присоединения Крыма.

Если у вас есть сомнения в законности своих действий, администрация ВКонтакте рекомендует воздержаться от их осуществления. Надо признать, что это весьма разумный совет.

В соцсетях секса нет! (Ну, или не должно быть)

Секс и «обнаженка» — практически табу на Фейсбуке, да и везде. С одной стороны, декларируется, что «мы понимаем важность этой проблемы и поощряем ее обсуждение». А с другой — грань настолько зыбкая, что вы и не заметите, когда ее нарушили. Особенно, если это касается детей. Модераторы в таких случаях считают, что «лучше перебдеть, чем недобдеть» и блокируют все подряд.

В 2016 году Фейсбук удалил пост норвежского писателя Томаса Эгеланда с известной фотографией «Напалм во Вьетнаме», на которой изображены дети, бегущие из деревни, подвергшейся бомбардировке. В службе техподдержки заявили, что фото содержит «элементы наготы» и не соответствует требованиям социальной сети. После этого Фейсбук заблокировал страницу писателя.

Любому здравомыслящему человеку было понятно, что никакого педофильского контекста в этой фотографии нет.

Любому здравомыслящему человеку было понятно, что никакого педофильского контекста в этой фотографии нет и быть не может, и потребовалось даже вмешательство премьер-министра Норвегии, чтобы объяснить руководству Фейсбука, что они неправы. В итоге пост вернули и страницу писателя разблокировали. Но если вы не уверены, что в случае чего за вас вступится премьер-министр, то лучше не рисковать.

Эта истерика началась еще до появления социальных сетей. В 1991 году вышел второй альбом группы Nirvana под названием Nevermind. На обложке альбома был запечатлен голый трехмесячный мальчик, плывущий за долларовый купюрой, подвешенной на рыболовный крючок. Звали малыша Спенсер Элден, это был сын друга фотографа. Как у всех маленьких мальчиков, у него был пенис и — о, боже — его было видно! Курт Кобейн категорически отказался менять обложку: «Вы должны быть латентным педофилом, чтобы вас это оскорбляло», — заявил он. И хотя ему все-таки пришлось согласиться на стикер в виде фигового листа, выход альбома сопровождался скандалом. Особо бдительные (или озабоченные?) граждане требовали запретить его продажу.

Скандал вскоре улегся, а Nevermind оказался самым коммерчески успешным диском группы Nirvana — получил бриллиантовый статус в США и дважды платиновый в Великобритании.

В 2011 году обложка Nevermind заняла второе место в списке лучших обложек альбомов всех времен по мнению читателей интернет-издания Music Radar, попала в список 50-ти самых

знаковых обложек альбомов сайта IGN, а также была отмечена в числе 10-ти самых знаковых обложек рейтинга газеты The Sun.

Мальчик вырос, и теперь каждые пять лет Спенсер Элден погружается в бассейн и воссоздает знаменитую обложку — но уже в плавках. А если вы запостите ее оригинальное изображение у себя в ленте, то и сегодня можете поиметь кучу проблем.

Еще раз, запомните: никакой обнаженки. Даже если вы разместите совершенно невинное фото младенца, найдутся нездоровые люди, которые увидят в этом сексуальный подтекст. Борцы с педофилией имеют претензии даже к фильму «Питер Пен», снятому на киностудии «Беларусьфильм» в 1987 году. Их беспокоит, что дочь индейского вождя носит слишком откровенный наряд — без топика, подумать только! Вы можете считать, что мир сошел с ума, но точка зрения всей этой публики очень близка к официальной, и обычные фотографии детей на пляже, которые можно найти в любом семейном альбоме, будут считаться, если они попадут в интернет, детской порнографией со всеми вытекающими последствиями.

Распространение детской порнографии в Сети интернет — серьезное преступление, подлежащее наказанию в соответствии с Уголовным кодексом РФ, ч. 2 ст. 242.1. Наказание по этой статье — от 3 до 10 лет лишения свободы.

Разумеется, у нормальных людей такого и в мыслях нет. Однако отношения закона с современными технологиями в этой сфере нормальному человеку интуитивно совершенно непонятны, поэтому очень легко угодить под статью. Порнографией могут признать любое обнаженное фото ребенка или подростка, и экспертиза, ско-

рее всего, это подтвердит. При таком подходе Льюис Кэролл, любивший фотографировать маленьких девочек, в наше время, несомненно, сидел бы в тюрьме.

> *Про пляжные фото вы уже знаете, но это далеко не все. Есть еще такое модное увлечение как секстинг — обмен личными интимными фотографиями. Согласно опросу[1], проведенному американскими психологами, этим занимаются 87,8% мужчин и женщин в возрасте от 18 до 82 лет. Авторы исследования считают, что секстинг может принести пользу отношениям и даже предлагают использовать его для психотерапии пар.*
>
> *Совершенно другое дело, когда секстингом балуются дети и подростки. Если вместо игры в «бутылочку» переживающие пубертат мальчики и девочки надумают дразнить друг друга фотографиями эротического содержания, то это сразу потянет на тяжкое уголовное преступление по законодательству большинства стран. Даже в том случае, если юная модель выложила на публичное обозрение свои собственные фотографии совершенно добровольно, — собственно, само слово «секстинг» и появилось, когда так поступила 13-летняя школьница из Новой Зеландии.*

Напомним, что уголовная ответственность в РФ предусмотрена за любые преступные деяния с 16 лет, а за тяжкие преступления — с 14 лет. Можно надеяться, что ввиду явной глупости и малолетства нарушителя закон не будет к нему слишком суров и обойдется условным сроком или штрафом. Но может получиться и хуже: кто-нибудь очень бдительный обнаружит старый снимок, когда его

---

1 *Секстинг полезен взрослым. //* ***Psychologies.ru.***

автору или обладателю уже стукнет 18 — и тогда можно будет получить наказание «на всю катушку» за давнюю детскую шалость.

> *Знайте, что в поисках материалов, хотя бы отдаленно напоминающих детскую порнографию, социальные сети денно и нощно шерстят не только сотрудники правоохранительных органов, но и их многочисленные добровольные помощники.*

Пожалуй, это одна из самых больших неприятностей, в которую можно угодить, не имея никакого преступного умысла. Если что-то подобное с вами или вашим ребенком приключилось, не надейтесь, что все само собой уладится — немедленно ищите хорошего адвоката.

В этом свете угроза шантажа публикацией интимных фотографий, если жертве нет 16 лет, автоматически становится распространением детского порно. Поэтому объясните — прежде всего, мальчикам, — что если какая-нибудь юная нимфа вдруг одарит их фотоснимками своих прелестей, то этого надо бояться не меньше, чем если кто-то подбросит им наркотики. И что такие фото лучше всего немедленно удалить. И уж тем более ни в коем случае не использовать как орудие мести, если их потом отвергнут.

Чьи в соцсети лайки? Немного об авторских правах

Пока вы заходите в соцсеть для того, чтобы почитать и посмотреть что-нибудь интересное, тема авторских прав вас не волнует. А вот тех, кто делает оригинальный контент, особенно когда это начина-

ет получаться хорошо и набирает тысячи, а то и миллионы просмотров (в YouTube такое вполне может произойти), это должно очень беспокоить по двум причинам. Во-первых, будет обидно, если ваш контент украдет кто-то другой, и особенно, если станет на нем зарабатывать; во-вторых — чтобы самим не попасть в неприятную ситуацию из-за публикации чужого контента.

Будет обидно, если ваш контент украдет кто-то другой, и особенно, если станет на нем зарабатывать.

Поэтому внимательно изучите правила соцсети относительно копирайта. Например, YouTube[1] — в этой части они у всех американских соцсетей практически одинаковы.

Все, что вы публикуете, к примеру, на своей странице сети ВКонтакте, считается контентом — «все объекты, размещенные на Сайте, в том числе элементы дизайна, текст, графические изображения, иллюстрации, видео, скрипты, программы, музыка, звуки и другие объекты и их подборки»[2]. Другие пользователи автоматически получают право просматривать, проигрывать и прослушивать опубликованный вами контент, но только с целью личного некоммерческого использования. В том числе, разрешается делать репост, то есть опубликовать копию вашего контента на своей странице, но только пользуясь стандартными функциями ВКонтакте.

А как быть, если ваше фото или рисунок кто-то сначала сохранил на компьютер, а потом запостил на своей странице как собствен-

1 *Об авторском праве* **https://support.google.com/youtube/answer/2797466?hl=ru**

2 *Правила пользования Сайтом ВКонтакте:* **https://vk.com/terms**

ное произведение? Это уже нарушение, так делать нельзя. Сначала нужно спросить разрешения автора. Может быть, вы и не против, но приличные люди так не поступают. Поэтому, если вы обнаружили подобное, делайте скриншот страницы нарушителя и можете жаловаться.

> *Совсем другое дело, когда ваш контент использует сам ВКонтакте. Пункт 7.1.5 Пользовательского соглашения недвусмысленно говорит, что пользователь предоставляет администрации безвозмездную неисключительную лицензию делать с его контентом что угодно без ограничения по территории и в течение всего срока, что контент находится на сайте.*
>
> *Если пользователь удаляет свой контент, то отзывается и право его использования администрацией, однако могут остаться архивные копии — «в случае необходимости, обусловленной техническими особенностями работы Сайта».*
>
> *Естественно, вы не можете загружать чужой контент без согласия автора. Пока ВКонтакте смотрит на это сквозь пальцы и пиратского контента там много, но лучше не рисковать. Вам же не хочется оказаться в первых рядах пойманных пиратов? Снимайте свои видео, сочиняйте музыку, рисуйте, фотографируйте — может быть, это окажется интересно людям.*

Авторские права во всех соцсетях работают похожим образом. Грубо говоря, от посягательств других пользователей на ваши произведения вас защищают, а вот сама администрация может брать у вас все без спроса. Просто примите это как факт и не ведитесь на разные глупости. Вот, например, время от времени по Фейсбуку прокатывается волна публикаций некоего псевдоюридического

текста, якобы способного предотвратить использование вашего контента администрацией соцсети (цитируем с сохранением оригинальной орфографии и стилистики):

> *«Не забывайте, что завтра начинается новое правило Facebook, где они могут использовать ваши фотографии. Не забывайте. Крайний срок сегодня! Это может быть использовано в судебных делах в судебном процессе против вас. Все, что вы когда-либо опубликовали, становится общедоступным с сегодняшнего дня. Даже сообщения, которые были удалены или фотографии запрещены. Это ничего не стоит для простого копирования и вставки, лучше, чем потом сожалеть. Канал 13 News рассказал об изменении политики конфиденциальности Facebook. Я не даю Facebook или другим лицам, связанным с Facebook, разрешение использовать мои фотографии, информацию, сообщения или сообщения, как в прошлом, так и в будущем. Этим заявлением я уведомляю Facebook, что категорически запрещается разглашать, копировать, распространять или предпринимать какие-либо другие действия против меня на основании этого профиля и / или его содержимого. Содержание этого профиля является частной и конфиденциальной информацией. Нарушение неприкосновенности частной жизни может быть наказано по закону (UCC 1-308-1 1 308-103 и Римскому статуту)».*

На самом деле это фейк, который появился в 2012 году и уже много раз гулял по страницам доверчивых пользователей в разных странах. Вреда от этого никакого нет, как, впрочем, и толку. Разве что может быть неловко перед друзьями, когда они это прочитают и посмеются.

С точки зрения закона, страницу в сети (ст. 1225 ГК РФ) можно отнести к следующим видам результатов интеллектуальной деятельности (РИД): произведение науки, литературы и искусства или база данных.

Страница как произведение выступает в качестве так называемых вторичных произведений: сложных объектов (ст. 1240 ГК РФ) или составных произведений (подп. 2 п. 2 ст. 1259 ГК РФ).

При защите прав на страницу как составное произведение следует доказать, что страница в соцсети — это не просто совокупность отдельных составных элементов — постов (текстов, видеороликов, фотографий, гиперссылок на другие страницы в Сети интернет и т.д.), а что указанные элементы страницы являются материалами, подбор и расположение которых представляют результат творческого труда. При этом сами элементы страницы не обязательно должны быть самостоятельными произведениями, а автору составного произведения в соответствии с п. 2 ст. 1260 ГК РФ принадлежат авторские права на осуществленные ими подбор или расположение материалов (составительство).

В случае, если отдельные элементы страницы являются самостоятельными объектами авторских прав, то страница может рассматриваться как сложный объект (ст. 1240 ГК РФ). В случае нарушения прав, в отличие от составного произведения, не нужно будет доказывать творческий характер подбора и расположения элементов, но нужно будет обосновать, что страница включает несколько охраняемых результатов интеллектуальной деятельности.

Страница в соцсети может защищаться и как база данных. В соответствии с абз. 2 п.2 ст. 1260 ГК РФ под базой данных понимается представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ. Страница в соцсети отвечает данным легальным признакам. Для соответствия признаку возможности систематизации материалов следует в материалах страницы (постах) использовать метки (теги), позволяющие делать поиск и сортировку материалов.

Контрольные вопросы

7. Что такое социальная сеть? Расскажите своими словами.

8. Какие социальные сети вы знаете?

9. Что такое эмоциональный интеллект? А киберэмоциональный?

10. Чему вы научились в соцсети? Что узнали полезного?

11. Как отличить настоящий профиль от фейка или бота?

12. Зачем нужна верификация страниц и как это работает?

13. С какого возраста в России можно завести аккаунт в соцсети?

14. Сколько у вас аккаунтов в соцсетях?

15. Как проверить, что виртуальный друг именно тот, за кого себя выдает?

16. Можно ли запретить администрации соцсети использовать ваши фото?

17. Опасно ли постить в соцсети фотографии из отпуска?

18. Геолокация на вашем смартфоне включена или выключена? Почему?

19. Какие данные о себе не надо публиковать?

20. О чем нельзя говорить в соцсети?

21. Что такое секстинг и в чем его опасность?

22. Что такое фаббинг?

23. Что такое синдром упущенной выгоды (FoMO)?

24. Сколько времени вы можете продержаться, не проверяя свою соцсеть?

Глава 10

Кибербуллинг: шутки со смертельным исходом

К сожалению, общение в Сети не всегда бывает уважительным и приятным.
Часто соцсети и различные чаты используются для агрессивного преследования выбранных жертв.
Рассмотрим, что собой представляет механизм онлайн-травли, и каким образом можно и нужно противостоять сетевой агрессии.

В 1983 году Apple выпустила первый настольный компьютер, использовавший мышь и обладавший графическим интерфейсом, а журнал Time назвал персональный компьютер «Машиной года», единственный раз за всю историю присудив это звание не человеку и не группе людей, и признав тем самым начало информационной эры.

По удивительному стечению обстоятельств, в том же году на экраны СССР вышел фильм Ролана Быкова «Чучело», буквально шокировавший советскую общественность. Картина впервые показала, насколько жестокими могут быть дети, когда объединяются в травле одного из сверстников, и насколько трудно жертве противостоять коллективному преследованию.

> *Писатель Владимир Железников написал сценарий «Чучела» по реальным событиям. История произошла с его племянницей, которая в школе взяла на себя чужую вину и стала объектом ненависти одноклассников. Учитель, который должен был разобраться в конфликте, попал в больницу с инфарктом. Травля продолжалась несколько недель, пока не открылась правда. Не будем подробно пересказывать сюжет — современные технологии позволят вам легко найти возможность посмотреть этот фильм. Скажем только, что «Чучелу» присудили Государственную премию СССР. И что еще интереснее для нас — его купили для показа в Америке и в странах Европы: зарубежные прокатчики поясняли, что и у них существуют похожие проблемы с детской жестокостью.*

Говоря в современных терминах, главная героиня фильма «Чучело» — «новенькая» в классе Лена Бессольцева, которую бле-

стяще сыграла Кристина Орбакайте, — стала объектом буллинга[1] со стороны одноклассников. Почему? Да потому, что показалась им странной, непохожей на них. Ведь известно, что детям далеко не всегда требуются веские причины для травли.

Цифровизация меняет способы травли

Цифровизация неумолимо преображает все сферы человеческой деятельности, и травля — не исключение. Если раньше был только буллинг, то теперь в дополнение к нему мы имеем и кибербуллинг — агрессивное преследование на просторах интернета. Появились новые средства как нападения, так и защиты. В этой связи жертвам, особенно ранимым подросткам, стало труднее противостоять агрессорам. А именно в подростковой среде кибербуллинг распространен в наибольшей степени.

> *Обычно подростки начинают практиковать коллективную травлю, учась в пятом-шестом классах общеобразовательной школы. К седьмому классу их нездоровая активность достигает пика, после чего постепенно снижается.*

Все логично. Младшие школьники еще плохо умеют письменно излагать свои (и чужие) мысли, в том числе агрессивные. А в старших

---

1 *Буллинг — агрессивное преследование одного из членов коллектива со стороны другого участника или группы участников. Чаще всего буллинг встречается в школьных и студенческих сообществах, но также нередки случаи травли и вне формальных коллективов. Английское "bulling" происходит от слова "bull" — «бык». Также употребляется в форме глагола "to bull", что означает «действовать с применением насилия». Русский жаргонизм «быковать» имеет аналогичное происхождение, но иной смысл.*

уже воспитывается эмпатия, и в то же время они начинают осознавать меру ответственности за свои действия. Среди взрослых тоже встречается буллинг, но несопоставимо реже.

Основные черты кибербуллинга — целенаправленность и повторяемость. С единичными случаями грубости в интернете, как и с трамвайным хамством, время от времени сталкиваются фактически все пользователи соцсетей. Но единичный случай — это выдохнуть и забыть. А систематическое преследование — ежедневные многоразовые инъекции негатива — может буквально сломать психику жертвы.

Систематическое преследование — ежедневные многоразовые инъекции негатива — может сломать психику жертвы.

В большинстве своем кибернасилию подвергаются те же люди, что терпят регулярные нападки и в реальной жизни. Гораздо менее распространены случаи, когда подросток вообще не подвергается издевательствам в школе и при этом страдает от атак в интернете. Но именно такие редкие ситуации потенциально могут быть наиболее опасными. Как правило, агрессором здесь выступает взрослый преступник, у которого на уме может быть все что угодно, или кто-то из знакомых, притворяющийся дружелюбным, но на самом деле затаивший нешуточную злобу.

Чаще всего площадкой кибербуллинга становятся социальные сети, но агрессор может задействовать и другие каналы коммуникаций.

Чаще всего площадкой кибербуллинга становятся социальные сети, но агрессор может задействовать и другие каналы коммуникаций: электронную почту, мессенджеры, SMS, видеоплатформы

(например, YouTube или TikTok), форумы и общие чаты. При этом преследователю совсем необязательно адресовать сообщения непосредственно объекту травли. Он может публиковать унизительные и дискредитирующие высказывания (рисунки, фото, видео- и аудиозаписи) у себя на странице, отмечать жертву в комментариях к постам друзей или в специально созданном паблике. Такие паблики называют «группами ненависти».

> *Используя имя и фотографию жертвы, кибербуллеры создают ложные страницы, на которых размещают от ее лица оскорбительную информацию в адрес одноклассников, учителей или родителей. Иногда взламывают настоящие страницы и публикуют фейковый контент на них.*

Полностью защитить свое виртуальное пространство невозможно физически, но можно затруднить агрессору доступ на свою страницу. Например, во всех популярных соцсетях предусмотрена функция блокировки нежелательных посетителей. После блокировки буллер не сможет ни присылать вам личные сообщения, ни оставлять комментарии на вашей странице. И всегда есть возможность пожаловаться на буллинг администрации сайта, которая способна удалить аккаунт хулигана.

Разумеется, если буллер одержим идеей вам навредить, он создаст новый аккаунт и продолжит травлю. Но вот что приятно: чтобы заблокировать (забанить) негодяя, нужен один клик, а ему, чтобы заново зарегистрироваться в соцсети, будет необходимо выполнить кучу действий.

> *Команда проекта «Постнаука» опросила почти триста учащихся в пяти московских школах. Выяснилось, что интернет-травля для них — вполне обычный жизненный опыт.*

С этим явлением сталкивались около 72% опрошенных. Из них более 44% выступали агрессорами, 26% ощущали себя жертвами, но в то же время сами проявляли агрессию и отвечали обидчикам оскорблениями. К слову, примерно в 40% случаев бывшие жертвы впоследствии становятся агрессорами.

Около 30% опрошенных заявили, что с травлей в Сети никогда не встречались. Но здесь велика вероятность, что эти респонденты не до конца понимают, что такое кибербуллинг, и не идентифицируют его как нечто предосудительное, ненормальное.

Из тех ребят, которые вели себя агрессивно по отношению к другим детям, только 15% получили удовлетворение от своих действий, 26% почувствовали свою неправоту, а 25% испытали стыд. Этот результат показывает, что травля в интернете не воспринимается как эффективная форма разрешения конфликта и не приводит к эмоциональной разрядке. Так что можно надеяться, что однажды кибербуллинг выйдет из моды[1].

«Чучело» в XXI веке

В 2011 году на американском телеканале ABC Family вышел мини-сериал «Кибербуллинг» (Cyberbully). Его главное достоинство — реалистичное и весьма подробное описание механизма онлайн-травли: какими мотивами руководствуются буллеры (зависть, ревность), как из-за беспечности (простой пароль) главная героиня, 17-летняя школьница, становится легкоуязвимой и, наконец, как быстро и дра-

1 *Кирилл Хломов. Кибербуллинг. // **Postnauka.ru**, 30 мая 2018.*

матично кибербуллинг, начавшись со сравнительно мелкой пакости, может привести к реальной угрозе жизни подростка.

> *Особая ценность сериала заключается в том, что он показывает, как в опасной ситуации, вызванной травлей, следует вести себя родителям жертвы. Часто говорят, что нужно быть в контакте с ребенком, поддерживать его, но никто не объясняет, как именно это делать, чтобы помочь ребенку. А сериал дает понять: именно так, как поступает мать главной героини, которая общается с дочерью, борется за нее, встречаясь с другими родителями, директором школы, адвокатами, психологами, журналистами. Так что всем, кто хочет знать, что нужно делать, если ребенок подвергается преследованию в соцсетях, «Кибербуллинг» просто обязателен к просмотру.*

Многие взрослые, к сожалению, недооценивают риски кибербуллинга. Часто ребенку говорят: «Подумаешь, кто-то пишет о тебе нехорошие вещи на каком-то сайте! Удали профайл, выключи компьютер и забудь». Увы, это так не работает. Человеку, особенно юному, не так-то просто взять и перестать читать и смотреть о себе всякие гадости, когда эти гадости видят и читают все его друзья.

> *Вот недавний случай: 13-летняя школьница из южноафриканской Претории покончила с собой из-за того, что школьники пересылали друг другу в мессенджере WhatsApp ее фотографию. В каком именно виде школьница была изображена на снимке, неизвестно. Но, как выяснила полиция, одноклассники до того ее затравили, что несчастная девочка боялась ходить в школу*[1].

---

1 *Pretoria girl commits suicide allegedly after cyberbullying// **TimesLive.co.za**, 19 февраля 2019.*

Едва ли кто-то из детей желал ей смерти. Просто детки забавлялись таким образом. И вот что здесь важно отметить: при личном (офлайн) буллинге агрессор видит, в каком состоянии находится жертва. И если доходит до крайности, он может остановиться, чтобы не довести жертву до нервного срыва и тем более до самоубийства, а себя — до тюрьмы. Но когда травля происходит онлайн, агрессору ничего не видно, а анонимность рождает у него чувство безнаказанности, добавляя куража.

Когда травля происходит онлайн, агрессору ничего не видно, а анонимность рождает у него чувство безнаказанности, добавляя куража.

Кстати, об анонимности. В большинстве случаев кибербуллинга анонимность весьма условна. Ведь травлей чаще всего занимаются знакомые жертвы, а их круг ограничен. Вычислить непосредственного обидчика при этом можно, хотя и труднее — им может оказаться вовсе не громила-второгодник, а любой ботаник-тихоня. Или даже лучший друг или подруга — из ревности или зависти.

Шутка или издевательство — где грань?

Когда кто-то пытается приструнить буллеров, они часто оправдываются: дескать, это была всего лишь шутка, игра, и жертва напрасно драматизирует ситуацию. Так ли это?

Исследование, проведенное фондом CYBERSMILE[1], показало, что подростки хорошо понимают, где заканчивается шутка

1 *Banter or Bulling? //**CyberSmile.org.***

и начинается издевательство: 65% опрошенных британских подростков считают, что четко знают, где пролегает эта грань, 21% не знают, 14% затруднились с ответом.

Более половины опрошенных (51%) считают, что шутки и сарказм часто используются в качестве прикрытия буллинга. В том, что шутка превращается в издевательство, когда это расстраивает другого человека, уверены 76% участников опроса; когда шутка заставляет людей чувствовать испуг — 71%; когда шутка становится слишком личной — 58%. И сами подростки хорошо понимают, шутят они или издеваются, — об этом заявили 81% опрошенных.

Таким образом, можно смело констатировать, что буллеры в своей массе прекрасно знают, что творят, и лишь прикидываются шутниками.

Гибридный буллинг — и в интернете, и в школе

Особое внимание стоит обратить на разрушительный синергетический эффект, который вызывает объединение онлайн- и офлайн-травли. Если раньше ребенок встречал обидчиков только в школе или на улице, а дома оставался вне зоны их досягаемости, то гибридный буллинг способен «работать» в режиме 24/7. И если жертва травли не может (а она не может) все время сидеть дома с выключенными компьютером, смартфоном и проводным телефоном, то гибридному буллингу нужно присвоить высшую степень опасности. Ведь абсолютно очевидно, что, подвергаясь тотальной

травле и не имея возможности от нее укрыться, подросток очень быстро может впасть в отчаяние и натворить бед.

- *Гибридному буллингу нужно присвоить высшую степень опасности.*

> *Безысходность описанной ситуации очень хорошо показана в одной из сцен уже упоминавшегося сериала «Кибербуллинг». Главная героиня, зайдя в класс, понимает, что все ребята смотрели недавно опубликованный издевательский ролик о ней. Более того, одноклассники демонстративно, во всеуслышание обсуждают это видео, отпуская едкие замечания. Она хочет немедленно убежать, но впадает в растерянность, понимая, что бежать ей некуда.*

Вынужденный спойлер: в сериале агрессор поймет свою неправоту, жертва с ним помирится, и все будут жить долго и, предположительно, счастливо. Однако реальность, как известно, бывает куда суровее сериалов. И надеяться, что настоящий агрессор вдруг поймет, насколько он гнусен и подл, после чего тут же прекратит свою мерзкую деятельность, было бы наивно.

Лена Бессольцева из «Чучела» решила проблему травли, сменив место жительства. Что ж, переезд или просто смена школы — достаточно действенный способ, чтобы избавиться от личного (очного) буллинга, да и от кибербуллинга тоже. Ведь, когда с глаз долой, тогда и из сердца вон. Чаще всего в гибридной травле одни и те же агрессоры участвуют и онлайн, и офлайн.

> *Эти юные негодяи, как правило, сидят за соседними с жертвой партами. Лишившись возможности воочию наблюдать за страданиями объекта своих издевок, они вскоре могут по-*

терять интерес и к преследованию в Сети. Но могут и не потерять, — встречаются такие упертые детишки.

О кое-каких технических способах защиты мы уже рассказывали выше. Здесь же заметим, что все они без исключения малоэффективны, поскольку борются лишь с симптомами. Лечить же, простите за банальность, нужно причину — атмосферу, взаимоотношения в классах и семьях, а также необходимо искать преступников. Осложняет эту и без того непростую задачу тот факт, что дети склонны скрывать проблемы, связанные с буллингом: три четверти подвергающихся преследованию подростков ничего не рассказывают о травле ни родителям, ни преподавателям.

Когда враг неизвестен

Кибербуллинг в чистом виде — когда агрессор и жертва незнакомы в реальной жизни — встречается довольно редко. Оно и понятно. Травля — такое действо, которому нужны зрители. Да и сам агрессор получает удовольствие, только видя страдания жертвы. Пока вы продолжаете «кормить тролля» — то есть отвечать на его нападки и показывать обеспокоенность, — травля будет продолжаться. Площадками для буллинга в интернете могут служить немодерируемые анонимные форумы на имиджбордах и подобных ресурсах, токсичных по своей природе. Достаточно перестать посещать токсичный ресурс, удалить профайл — и все закончится.

Пока вы будете «кормить тролля» — то есть отвечать на его нападки и показывать обеспокоенность, — травля будет продолжаться.

Но беда в том, что не каждый может отказаться от посещений этих площадок — воронка негатива засасывает подростков. В 2013 году 14-летняя английская школьница Ханна Смит покончила с собой из-за агрессивной травли на сайте Ask.fm[1], на котором она задала вопрос о проблемах с кожей лица. В ответ на это на протяжении долгого времени ее буквально заваливали издевательскими сообщениями. Ханна не смогла это пережить.

> *За 2012-2013 годы из-за травли на том же сайте покончили с собой еще девять тинейджеров. Но в 2014-м, когда у площадки сменился владелец, администрация сайта стала активнее бороться с кибербуллигом, и самоубийства прекратились. На сегодняшний день сайт Ask.fm работает без происшествий. У него насчитывается 215 миллионов пользователей, среди которых, кстати говоря, довольно много подростков из России. Однако репутация опасного места сохраняется за этой платформой до сих пор[2].*

> *Травля происходит на всех известных социальных платформах — Facebook, Instagram, WhatsApp, YuoTube, TikTok, Snapchat, ВКонтакте и др. И это несмотря на заявления и реальные усилия администраторов по противодействию кибербуллингу.*

Но взглянем на ситуацию трезво. Когда вашей платформой пользуются миллиард или сто миллионов человек, вы физически

---

1 *Пользователи Ask.fm создают профили, которые используются для ответов на вопросы, задаваемые другими участниками. Согласно политике приватности, вопросы можно задавать анонимно, а отвечающие должны указывать свои имена. В итоге за эти правила сайт прозвали «очагом запугивания».*

2 *9 Teenage Suicides In The Last Year Were Linked To Cyber-Bullying On Social Network Ask.fm. // BuzzFeedNews.com, 11 сентября 2013.*

не в состоянии следить за порядком. И никакому искусственному интеллекту (ИИ)[1] не под силу справиться с этой задачей, поскольку он не чувствует иронию и сарказм, не отличает шутки от издевательств, не понимает двусмысленные намеки и скрытые угрозы. Ресурсы полиции тоже ограничены. И нужно отдавать себе отчет, что пока не случится что-то действительно ужасное, вряд ли органы будут усердно заниматься вашим делом.

> *Единственный полезный совет, который стоит дать ребенку, попавшему под огонь ненависти, — немедленно покинуть соцсеть, в которой его травят. Не все соцсети вообще, а именно эту.*

Выбор, слава богу, широкий, виртуальных друзей можно найти и на других площадках. При этом важно убедить ребенка, чтобы он принял решение покинуть злобную сеть добровольно и самостоятельно. Запреты и технические ограничения, как правило, не помогают.

> *Если преследователь не угомонился и пытается достать свою жертву по другим каналам — например, узнал телефон*

---

1 *Действующих решений на основе ИИ пока не существует. Но работы в этом направлении ведутся. Так, в статье «Автоматическое обнаружение издевательств в текстах социальных сетей» группа исследователей описывает алгоритм, который в ходе экспериментов распознал оскорбительное поведение в интернете на английском и голландском языках. Ученые, стоящие за этим проектом, считают главным достижением способность их системы обнаруживать сигналы запугивания. Также этот алгоритм определяет, кто является хулиганом, жертвой и свидетелями в каждой ситуации, что может помочь модераторам веб-сайтов эффективнее противостоять кибербуллингу. Van Hee C, Jacobs G, Emmery C, Desmet B, Lefever E, Verhoeven B, et al. (2018) Automatic detection of cyberbullying in social media text. PLoS ONE 13(10): e0203794.* ***https://doi.org/10.1371/journal.pone.0203794***

> *или адрес, нашел аккаунт в другой соцсети, — то с этим уже нужно обращаться в полицию или прокуратуру.*

Остается вопрос: как узнать, что у ребенка есть такая проблема? Ответ прост: нужно постоянно быть с ним в контакте. Если вы жестко потребуете, чтобы он открыл свою переписку, это подорвет его доверие к вам и может привести к худшим последствиям. Ничто не помешает ему втайне завести новый аккаунт и так замаскировать все следы, что вы никогда о нем не узнаете. Не забывайте: сегодня дети разбираются в технологиях лучше родителей.

> *Особенно страшно, когда детей травят взрослые. В 2006 году полиция расследовала самоубийство 13-летней Меган Мейер[1], совершенное из-за травли в социальной сети MySpace. Выяснилось, что аккаунтом якобы ее 16-летнего друга по имени Джош Эванс управляла мать бывшей подруги девочки. По ее признанию, она затеяла эту игру, чтобы «завоевать доверие Меган и выяснить, что та думает о ее дочери и других людях». А ведь на самом деле это ничем не отличалось от настоящего издевательства. Например, в последнем сообщении, отправленном псевдо-Джошем в адрес Меган, были такие слова: «Ты плохая и все тебя ненавидят. Без тебя мир стал бы лучше».*

Вероятно, многие скажут, что если бы все начали вешаться после подобных сообщений, самоубийства случались бы каждый день. Да, конечно. Но дело в том, что Меган наблюдалась у психиатра

---

1 *Megan's Story* ***https://meganmeierfoundation.org/megans-story***

и принимала ряд препаратов, у нее был диагностирован СДВГ[1] и депрессия, а также присутствовали проблемы с самооценкой из-за избыточного веса. В результате травля в сети стала для Меган Мейер последней каплей.

Травля на сексуальной почве

Подавляющее число случаев кибербуллинга, которые привели подростков к суициду, имеет сексуальный контекст. Однако тема секса, несмотря на активный секспросвет, остается самой закрытой в отношениях детей и родителей. Поэтому, если подросток переживает негативный (а тем более позитивный) сексуальный опыт, большинство родителей остаются в неведении[2].

Если подросток переживает негативный (а тем более позитивный) сексуальный опыт, большинство родителей остаются в неведении.

Самое плохое, что может случиться с мальчиками — это травля на почве гомосексуальности. Если в классе вдруг станет известно о нетрадиционной ориентации кого-то из учеников, пощады ждать не стоит.

---

1 *Синдром дефицита внимания и гиперактивности (англ. attention deficit hyperactivity syndrome), аббр. СДВГ, расстройство внимания с гиперактивностью или гиперактивное расстройство с дефицитом внимания (англ. attention deficit hyperactivity disorder, аббр. ADHD) — неврологическо-поведенческое расстройство развития, начинающееся в детском возрасте. Проявляется такими симптомами, как трудности концентрации внимания, гиперактивность и плохо управляемая импульсивность. Также при склонности к СДВГ у взрослых возможны снижение интеллекта и трудности с восприятием информации.*

2 *Согласно статистике, средний возраст, в котором российский подросток приобретает первый сексуальный опыт, — около 16 лет. Однако нередки случаи, когда дети начинают половую жизнь уже с 12 лет.*

Вот история, произошедшая в Вермонте, США.

> *Райану было 13 лет, одноклассники считали его геем и третировали на каждом шагу. Интернет пестрил сообщениями соответствующего содержания. Как нетрудно догадаться, жилось Райану не очень хорошо. Но вдруг, за пару недель до летних каникул, одна из одноклассниц начала проявлять к нему интерес и всячески выражать симпатию. Для совсем одинокого, затюканного Райана это стало сродни божественному дару.*
>
> *Конечно же, он с радостью откликнулся, и дети сразу подружились. Потом настало лето, друзья разъехались, но переписывались в каждодневном режиме все каникулы. Райан, которому годами не с кем было обмолвиться и словом, вдохновенно писал обо всех интересных происшествиях, наблюдениях, сомнениях, переживаниях, мечтах. Подруга отвечала ему, хоть и сдержаннее, но примерно тем же. И все было бы чудесно, но его письма она не только читала сама, но, смеха ради, еще и пересылала одноклассникам. А когда осенью Райан пришел в школу, он был высмеян при всех в самой грубой форме. Финал, увы, предсказуем. На следующий день Райан повесился в ванной.*

Теперь о том, как преследуют девочек. Это, без преувеличения, просто ад. В преобладающем числе случаев травля происходит по двум причинам. Первая — изнасилование, часто групповое, с фото- и видеосъемкой и последующим шантажом. Вторая — секстинг: жертва инициативно, или поддавшись на уговоры, пересылает бойфренду интимные фотографии, а тот выкладывает их в Сеть на всеобщее обозрение. По извращенной логике,

хозяйствующей в подростковых головах, виноватой признается сама жертва насилия или обмана, и именно против нее организуется кампания осуждения.

Именно так и случилось в истории с Амандой Тодд.

> *Аманда жила в канадской провинции Британская Колумбия. Когда она перешла в седьмой класс, в соцсети у нее появился бойфренд — ровесник по имени Тайлер Бу. Аманда настолько доверяла своему сетевому приятелю, что однажды уступила его просьбам и продемонстрировала на камеру обнаженную грудь. Сеанс стриптиза длился всего несколько секунд. Но эти секунды, которые бойфренд записал на жесткий диск своего компьютера, стали для легкомысленной девочки роковыми.*
>
> *Позже стало известно, что за именем Тайлер Бу скрывался очень своеобразный 38-летний гражданин Нидерландов. Когда его поймали, для чего потребовались объединенные усилия полицейских Канады, Норвегии и Нидерландов, а также сотрудников центра безопасности Facebook, ему было предъявлено 72 обвинения в сексуальном насилии и вымогательстве с участием 39 жертв, как женщин, так и мужчин. Он пользовался несколькими десятками аккаунтов в различных соцсетях, а также обширным электронным архивом детского порно.*

Но арест, улики, суд, тюрьма были уже потом — уже после того, как этот маньяк успел сломать Аманде жизнь. Он преследовал ее два года. Начал с шантажа: покажи еще что-ни-

будь на камеру, иначе разошлю фото прошлого стриптиза твоим родителям, друзьям и одноклассникам. Она отказалась, а он привел угрозу в исполнение.

И началась травля. Да такая, что родителям пришлось в срочном порядке перевести заплаканную Аманду в другую школу. Однако преследователь нашел контакты новых одноклассников и тоже снабдил их фотографиями Аманды топлес. Травля возобновилась, и Аманда была вынуждена снова сменить школу.

Через какое-то время у нее завязались отношения с мальчиком, но он ее предал и спровоцировал новую травлю. Не выдержав очередного удара, Аманда выпила отбеливатель. Ее спасли, после чего она опять перешла в другую школу. Но онлайн-травля продолжилась. В частности, ей рекомендовали выпить другой отбеливатель.

> *Примерно через год Аманда опубликовала на YouTube 9-минутный видеоролик под названием «Моя история: борьба, запугивание, самоубийство, самоповреждение». На записи девочка молча показывает серию карточек, на которых короткими фразами описывается все, что с ней случилось. Спустя месяц после публикации своего видео девочка повесилась.*

Имя Аманды Тодд стало символом борьбы с запугиванием детей в интернете. Мать девочки организовала фонд, который помогает подросткам бороться с психическими расстройствами, вызванными шантажом и травлей в Сети[1].

---

1 Suicide of Amanda Todd (Википедия).

Что говорит закон

Опасность кибербуллинга признается повсеместно, однако законодатели не имеют единой позиции в отношении этого явления. Во всех штатах США действуют законы о хулиганском поведении и преследовании, в большинстве из них есть прямая ссылка на электронные формы. То есть, пусть формально, кибербуллинг и не является уголовным преступлением, но хороший адвокат может подвести хулигана под статью.

Кроме того, американские законы обязывают школы иметь официальную политику в отношении буллинга и кибербуллинга, определять возможные дисциплинарные меры за соответствующие нарушения. Также школы должны реагировать на случаи травли — особенно по расовым и религиозным мотивам, из-за инвалидности и сексуальной ориентации[1].

Иначе говоря, основная ответственность за недопущение травли в США возлагается на школы. И это, пожалуй, правильно.

Основная ответственность за недопущение травли в США возлагается на школы.

В ряде стран Европы есть законы о кибербуллинге для взрослых — они касаются трудовых отношений.

Например, закон, регулирующий это вопрос, был принят в Швеции еще в 1993 году.

1 См. **https://www.stopbullying.gov/**

В законодательстве Великобритании нет юридического определения кибербуллинга. Однако действует ряд законов, которые могут применяться в случаях травли и домогательств в интернете.

Новая Зеландия в 2013 году приняла закон, предусматривающий уголовную ответственность за кибербуллинг. Теперь человек, признанный виновным в пересылке запугивающих, расистских, сексистских или каких-либо других агрессивных сообщений, приведших к «серьезным эмоциональным переживаниям», может получить до двух лет лишения свободы.

В российском законодательстве определения кибертравли не существует, но могут применяться следующие статьи:

- Доведение до самоубийства (ст. 110 УК РФ);
- Угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ);
- Клевета (ст. 128.1 УК РФ);
- Оскорбление (ст. 5.61 КоАП РФ).

Примечательно, что все эти статьи касаются только взрослых людей, потому что к школьникам 5–7 классов — наиболее активным буллерам — УК РФ едва ли применим. Таким образом, приходится признать, что в рамках правового поля рычагов воздействия на малолетних онлайн-хулиганов в нашей стране практически нет.

В рамках правового поля рычагов воздействия на малолетних онлайн-хулиганов в нашей стране практически нет.

Между тем российские школьники сталкиваются с травлей в интернете от полутора до трех раз чаще своих сверстников из стран Европы и Северной Америки. Россия возглавила список из 42 стран по распространенности кибербуллинга среди детей в возрасте 11 лет: 11% девочек и 8% мальчиков получали сообщения с оскорблениями не менее 2–3 раз в месяц (по исследованию Всемирной организации здравоохранения 2014 года)[1].

Так что пока, видимо, нам остаются только дисциплинарные и воспитательные меры.

Что делать, если ваш ребенок подвергается травле в Сети?

Во-первых, нужно помнить, что корень проблемы, скорее всего, кроется в отношениях в детском коллективе, а не в интернете. Ищите причину, разбирайтесь — не стоит во всех бедах винить соцсети и гаджеты. Часто травля начинается в ответ на глупую шутку или обидный комментарий, отпущенный самим потерпевшим. Но ни в коем случае нельзя возлагать всю вину на жертву (виктимблейминг).

Сообщите классному руководителю и директору. Да, они могут развести руками и заявить, что им неизвестно, кто скрывается под аккаунтами агрессоров. Однако, это не означает, что они ничего не могут сделать. В большинстве случаев ки-

1 *Россия — чемпион мира по травле в Сети. Что с этим делать? // Сайт* ***Mel.fm****, 15 ноября 2017.*

бербуллинг есть отражение нездоровой обстановки в классе. Сам факт того, что взрослые участвуют в разбирательствах, может отрезвить малолетних хулиганов.

Сам факт, что взрослые участвуют в разбирательствах, может отрезвить малолетних хулиганов.

Фиксируйте все факты агрессии: делайте скриншоты, сохраняйте видео- и аудиофайлы. Если придется подключать правоохранительные органы, это станет доказательной базой. К сожалению, кибербуллинг в России формально еще не считается преступлением. Однако в случаях, повлекших реальный вред (суицид и попытка суицида, депрессия, требующая лечения), не стоит оставлять действия хулиганов безнаказанными. Обратитесь в полицию и проконсультируйтесь с юристом, что можно предпринять в сложившейся ситуации.

> *Чаще всего площадкой для травли становятся социальные сети — а раз так, используйте защитные функции, которыми они располагают. Обидчика можно «отправить в бан», и он больше не сможет писать вашему ребенку. Также можно пожаловаться на буллинг администрации сети, которая заблокирует аккаунт нарушителя, если признает вашу жалобу обоснованной. Естественно, это не гарантирует прекращения атаки, — буллер может создать новый аккаунт под другим именем, — но бороться необходимо.*

Если возникнет хоть малейшее подозрение, что преследователь кто-то из взрослых, бейте тревогу. Объясните ребенку опасность ситуации. Обязательно нужно проверять, кто на са-

мом деле прячется за аватаром. Самый простой способ — видеозвонок.

Куда обращаться

Линия помощи «Дети онлайн» — бесплатная всероссийская служба телефонного и онлайн-консультирования для детей и взрослых по проблемам безопасного использования интернета и мобильной связи. Психологическую и информационную поддержку здесь оказывают сотрудники факультета психологии МГУ им. М.В. Ломоносова и «Фонда Развития Интернета».

Телефонный номер (звонки из России бесплатны): 8-800-25-000-15. Часы работы: с 9.00 до 18.00 по рабочим дням, перерыв с 13.00 до 14.00. Электронная почта: helpline@detionline.com

Что делать для профилактики кибербуллинга?

Научить ребенка миролюбивому и корректному поведению в соцсетях. Конечно, это из серии «проще сказать, чем сделать», но никто и не говорит, что воспитание детей — легкое дело.

Объяснить, что такое кибербуллинг и чем это плохо. Ведь ваш ребенок может оказаться как жертвой, так и агрессором.

Посмотреть вместе фильмы «Чучело» и «Кибербуллинг» (второй на английском, заодно и школьный сленг изучите).

Рассказать о реальной ситуации с анонимностью, чтобы у желающих позабавиться травлей было меньше иллюзий насчет собственной неуязвимости, а у пострадавших — уверенность в том, что неизвестных обидчиков можно найти.

Разобраться, как действуют защитные функции в соцсетях (как блокировать хулиганов и куда жаловаться), которыми пользуется ребенок, — чтобы не паниковать в стрессовой ситуации.

Поставить надежный пароль на аккаунт соцсети и не оставлять свой телефон или компьютер без присмотра, чтобы потом не пришлось страдать за чьи-то глупые выходки.

Прежде чем публиковать в Сети высказывания и фотографии, подумать, могут ли они кого-нибудь задеть. Хотя угадать, безусловно, трудно — неадекватного человека (а их много и среди детей) может оскорбить любой пустяк.

Избегать сайтов с плохой репутацией, где администрация не следит за порядком.

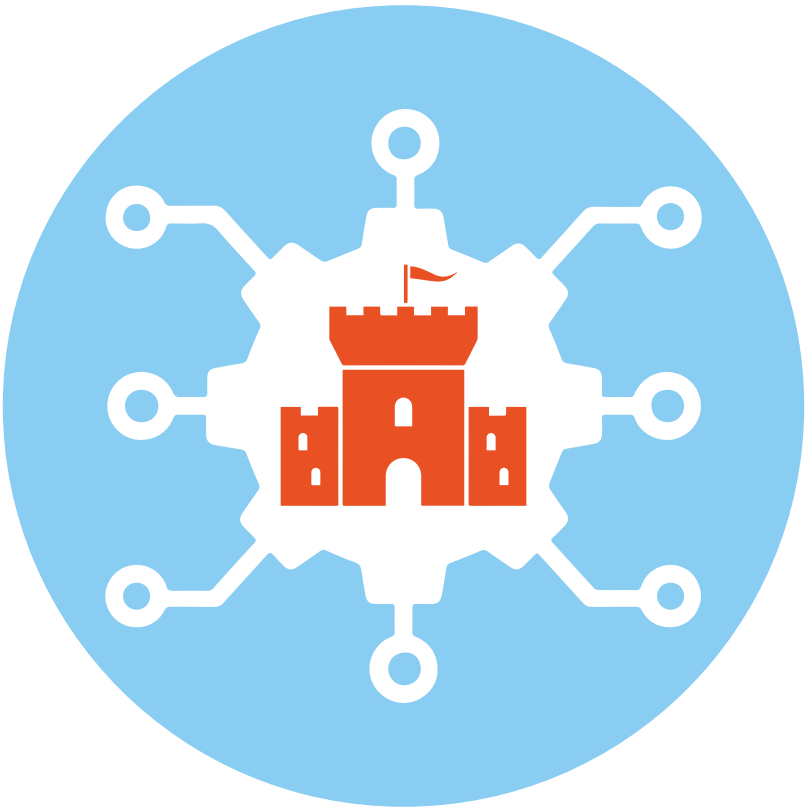
Контрольные вопросы

1. Что такое буллинг и кибербуллинг?

2. В каком возрасте кибербуллинг наиболее распространен?

3. В чем опасность кибербуллинга?

4. Что такое «группы ненависти»?
5. Из-за чего может начаться травля?
6. Как бороться с кибербуллингом?
7. Что такое гибридный буллинг?
8. Чем шутка отличается от издевательства?



Глава 11

Строим цифровую крепость

Заключительная глава,
в которой мы вспомним все полезные советы
и, закончив чтение, тут же начнем применять
их на практике.

В интернете действует то же правило, что и в самолете, — сначала обеспечьте безопасность себе, потом ребенку. То есть взрослым нужно самим освоить правила кибербезопасности и понимать природу разнообразных цифровых угроз, чтобы стать для своего ребенка авторитетом. И, разумеется, разговоры надо подкреплять личным примером.

> *Помните: на одних запретах далеко не уедешь. Дети обязательно найдут способ вырваться за очерченный взрослыми периметр, и, если основы безопасного поведения в онлайн-среде не заложены у них в голове, то велик риск того, что они попадут в какую-нибудь опасную ситуацию.*

Еще одна важная вещь: не стесняйтесь спрашивать и учиться у своих детей. В этом цифровом мире мы все новички, поэтому делиться полезными знаниями друг с другом надо без оглядки на возраст. Стройте свою цифровую крепость вместе!

Итак, коротко повторим основные темы книги.

«В однобортном уже никто не воюет»: обновляйте софт регулярно

Обновление в ИТ — это не бездумная гонка за модой. В новой версии софта, прежде всего, важны не форма и цвет кнопочек, а устранение пробелов в безопасности. Все операционные системы и программы, установленные на компьютере

и телефоне, потенциально уязвимы. Это только вопрос времени и желания хакеров — найти брешь и начать ее использовать.

Поэтому неукоснительно соблюдайте правила обновления:

- Не выключайте функцию автообновления в операционной системе, пусть все патчи и апдейты устанавливаются сами;
- Регулярно проверяйте, не пора ли обновить драйверы;
- Не сидите на старых версиях операционных систем. Windows 7 еще может работать, но защищать ее никто не будет;
- Всегда обновляйте ваш антивирус, VPN и другие средства защиты;
- Не мешайте обновлению браузера, если он хочет это сделать. Прервите работу и дайте ему перегрузиться;
- Обновляйте все прочие приложения, с которыми вы работаете.

Кто-то скажет: «может, ну его»? Не зря же программисты шутят про обновленные версии: старые ошибки исправили, а новые внесли. И уязвимости все равно будут.

Возможно. Однако, про старые «дыры» хакеры уже знают, а про новые — еще нет. Поэтому все-таки лучше обновляться, чем этого не делать.

Всегда носите маску: помните про антивирус

С антивирусом все просто — он должен стоять и работать. Это средство по-прежнему эффективно против большинства известных угроз. Если вам вдруг «повезет» словить какой-то новый вирус, то защита может и не сработать, но это не повод ею пренебрегать. Точно также ношение медицинской маски не гарантирует абсолютной защиты от вируса, но значительно снижает вероятность заразиться.

> *Никогда не выключайте антивирус. Не обращайте внимания на тех, кто считает, что он тормозит работу и зря расходует ресурсы компьютера.*

И уж тем более не делайте этого, если вас попросит какая-нибудь программа, скачанная из Сети: «Ах, ваш антивирус мешает мне установиться!»

Ключи ко всем дверям: наведите порядок в паролях

Беззаботные времена, когда ключ от входной двери прятали под ковриком или в цветочном горшке, увы, прошли. Сегодня мы устанавливаем стальные двери с хитрыми замками, чтобы обезопасить свое жилище. Точно также следует поступить и с вашим цифровым хозяйством: наведите порядок в своих паролях и поддерживайте его.

- В первую очередь, позаботьтесь о паролях к самым важным сервисам — электронной почте, на которую регистри-

руете свои аккаунты, социальным сетям (потому что это доступ к вашей репутации и друзьям), облачным хранилищам, где лежат ваши фотографии и документы. Используйте для них уникальные и сложные пароли, но такие, какие вы сможете запомнить, ибо они могут вам понадобиться в любой момент.

- Включите везде двухфакторную аутентификацию. Лучше лишний раз ввести проверочный код, чем дать шанс злоумышленникам похитить ваши данные.

- Разберитесь с менеджерами паролей, выберете себе один из них и настройте. Потому что запомнить все нереально, все равно вам придется вести какие-то записи, — уж лучше это делать с помощью специального инструмента, чем держать файл с паролями на видном месте.

- Возьмите за правило сразу менять пароли на всех умных устройствах, как только они попадают в ваш дом — wi-fi-роутеры, компьютеры, телефоны, смарт-ТВ, пылесосы, кофеварки, холодильники и так далее. Неважно, новые они или б/у.

- Если есть основания считать, что пароли «утекли», меняйте их немедленно. Например, если вы потеряли телефон или ноутбук, срочно найдите какое-нибудь устройство и поменяйте все важные пароли.

Проследите, чтобы эти правила выполнял весь гарнизон вашей цифровой крепости, включая старых и малых. Если им трудно справиться с чем-то самим, настройте все так, чтобы им было удобно, но не ослабляя при этом безопасность. На-

пример, тот же менеджер паролей избавит их от необходимости ввода сложной последовательности букв и цифр.

Подстелить соломку: облака и резервное копирование

Может случиться так, что, несмотря на все принятые меры защиты, киберпреступники все-таки прорвут вашу оборону. Наиболее реальная угроза сегодня исходит от вирусов-шифровальщиков, поэтому лучше подстраховаться заранее, чтобы не зависеть потом от милости хакеров, которые, даже получив выкуп, могут не дать вам ключ расшифровки.

Для этого настройте резервное копирование (бэкап) всех ценных данных.

> *Проще всего делать бэкап в облако[1] — тогда процедура будет выполняться автоматически хоть каждые 5 минут, и вы почти ничего не потеряете в случае атаки. Если же вы готовы положиться на собственную дисциплину, то можно делать бэкап на внешний жесткий диск.*

Кроме того, резервное копирование убережет ваши данные в случае поломки или утраты компьютера.

Не забудьте и про данные с телефонов — контакты, заметки и особенно фотографии, — все это можно автоматически копировать в облако (или даже в два — для большей надежности).

---

1 Например, с помощью Acronis Ransomware Protection (есть бесплатная версия).

Друзья в соцсетях: никогда не разговаривайте с неизвестными

Надежнее считать, что пока не доказано обратное, все в интернете — неизвестные. Понятно, что не будет большой беды, если вы поговорите с незнакомым человеком о природе и погоде, но ни в коем случае не откровенничайте с ним (или с ней) о личных делах. И уж совершенно точно не перечисляйте сразу никому и никуда никаких денег, даже если просит знакомый. Сначала убедитесь, что его аккаунт не захватили хакеры.

Не перечисляйте сразу никому и никуда никаких денег, даже если просит знакомый.

Как это сделать? Самое простое средство — видеозвонок. Но когда друг новый, то даже такая проверка не гарантирует, что он вам не врет. И если нет возможности проверить информацию о человеке, лучше держаться от него подальше.

Будьте трижды осторожны, получив предложение встретиться в реале, или, как говорят, «развиртуализироваться».

И самое главное: будьте трижды осторожны, получив предложение встретиться в реале, или, как часто говорят, «развиртуализироваться». С одной стороны, мы живем в мире, где онлайн-знакомства стали нормой — люди встречаются, влюбляются, а сейчас уже и женятся в интернете. С другой — маньяки, грабители, шантажисты и другие преступники тоже умеют пользоваться соцсетями и мессенджерами.

Фишинг: а что скажет нам интуиция?

Уж сколько раз твердили миру, что не надо открывать подозрительные письма и кликать на подозрительные ссылки!

> *Кибержулики только того и ждут, чтобы запустить вам вируса-троянца, подсунуть фальшивый сайт вместо настоящего интернет-магазина или банка.*

Как отличить подозрительную ссылку от неподозрительной? Вообще-то говоря, никак. Надо честно признать, что абсолютно надежного способа распознать фишинг не существует. Развивайте интуицию и включите все уровни защиты, о которых мы говорили.

Как это развидеть? Встреча с нежелательным контентом

К сожалению, в интернете полно не только самой разнообразной полезной информации, но и всяческой грязи. Естественно, взрослые хотят оградить детей от встречи с недетским контентом: на уровне страны этим занимается Роскомнадзор, а дома вы можете использовать средства родительского контроля.

Но надо отдавать себе отчет в том, что все технические меры по фильтрации контента эффективны лишь отчасти.

> *Рано или поздно ваш ребенок все равно увидит то, что вы предпочли бы от него спрятать. И тогда от вас потребуется адекватная реакция, открытость и готовность к разговору*

на любые темы. Избежать этого не удастся: наказания и угрозы только разожгут интерес к запретным плодам, а игнорирование проблемы и попустительство может привести к психической травме.

Как быть? Готовьтесь заранее. Подумайте над тем, что и как сказать ребенку. Посоветуйтесь с психологом. Самое главное, что от вас требуется, — выстроить доверительные отношения. Но эта тема уже выходит за рамки нашей книги.

Каждый шаг оставляет след, цифровой

Поэтому все, сказанное вами, может быть использовано против вас. Прежде всего, это касается соблюдения закона: реальность такова, что неразумный пост, комментарий и даже просто неосторожный лайк могут иметь юридические последствия. Например, если размещенный подростком клип модной группы признан экстремистским, то сам подросток становится распространителем экстремистской информации.

Законодательство РФ в части регулирования интернета чрезвычайно динамично и непредсказуемо, поэтому трудно дать исчерпывающие рекомендации на тему того, что можно и чего нельзя делать в Сети. Как минимум, нелишним будет напомнить, что анонимность в интернете весьма условна, — обычному пользователю не под силу запутать следы настолько, чтобы его не нашли.

Поэтому стоит донести до ребенка простую мысль: интернет — это публичное пространство, и вести себя в нем нужно точно так же, как в любом другом общественном месте.

От автора

Современную жизнь невозможно представить без интернета. И чем дальше, тем все более «цифровым» будет становиться наш образ жизни. Невзирая на все опасности и угрозы, мы будем каждый день выходить в Сеть, чтобы узнавать новости, делать покупки, общаться с друзьями, работать, учиться, развлекаться, — другого варианта попросту нет.

Поэтому всем нам придется усвоить правила кибергигиены и обучить им своих детей. Это настолько же жизненно важно, как привычка мыть руки, приходя с улицы. При этом правила должны быть понятны, иначе они превратятся в пустые ритуалы, которые можно заставить выполнять только из-под палки.

Цель этой книги заключается как раз в том, чтобы объяснить, почему ради вашей безопасности в интернете надо поступать именно так, а не иначе. Это знание поможет вам наполнить смыслом те простые, в общем-то, правила кибергигиены, о которых сегодня столько говорится, и позволит относиться к своей кибербезопасности более осознанно.

Станислав Макаров

Родился в Волгограде, с 1983 года учился в МВТУ им. Баумана, где с первого курса увлекся компьютерами. Работал программистом, затем был продавцом ПО, инженером по внедрению, руководителем проектов и бизнес-аналитиком. Участвовал в разработке отечественных тиражных программных продуктов и в корпоративных проектах, в России и за рубежом.

С 2010 года занимается ИТ-журналистикой, автор множества публикаций и модератор конференций по широкому спектру тем из области цифровых технологий, в том числе по информационной безопасности. Сотрудничает с ведущими отраслевыми изданиями – CNews, TAdviser, itWeek, ComputerWorld.

Умеет рассказывать просто о сложных вещах. Зная о рисках информационной безопасности из реальной практики по внедрению ИТ-систем в крупных государственных и коммерческих организациях, решил написать об этом книгу для обычных людей – для детей и родителей, потому что технологии настолько проникли в нашу жизнь, что каждой семье впору об этом задумываться.