ЦИФРОВАЯ ГИГИЕНА

Эта книга посвящена угрозам цифровой среды — деструктивным сообществам, токсичному контенту, травле, цифровой зависимости и прочим факторам разрушительного воздействия на психику. Авторы надеются, что книга поможет родителям и преподавателям научить детей и подростков необходимой цифровой гигиене.

ИГОРЬ АШМАНОВ

НАТАЛЬЯ КАСПЕРСКАЯ

Наталья Касперская
Игорь Станиславович Ашманов
Цифровая гигиена

http://www.litres.ru/pages/biblio_book/?art=67148719
Цифровая гигиена: Питер,; Санкт-Петербург; 2022
ISBN 978-5-4461-1938-7

Аннотация

Цифровая среда – Интернет, социальные сети, приложения – является неотъемлемой частью той «мультиреальности», в которой существует современный человек. Естественно, что вместе с неоспоримой пользой виртуальность приносит в нашу жизнь и огромные риски. Сейчас цифровой мир – это джунгли, подчас населённые не самыми приятными (и небезопасными!) формами жизни. Таким он и останется, пока в нём не будет наведён порядок.

Перед вами не очередная «страшилка», а экспертная оценка цифрового мира на основе большого объёма изученных данных. В книге рассматриваются проблемы цифровой зависимости и отчуждения подростков, воздействия деструктивных сообществ и токсичного контента, защиты от фишинга, поиска и оценки достоверности информации, а также другие явления цифровой среды. Ситуация в Сети очень быстро меняется, порождая новые опасности, поэтому основная задача – не только рассказать

о существующих рисках, но и научить вас самостоятельно разбираться в методах защиты.

В формате PDF A4 сохранён издательский дизайн.

Содержание

Игорь Ашманов, Наталья Касперская
Цифровая гигиена

От авторов: о чём и для кого эта книга

Разрыв поколений

седая мать нашла у сына
в портфеле белый порошок
он даже в школе чистит зубы
с улыбкой думает она

Довольно часто можно услышать мнение, что у нас (и во всём мире) есть разрыв между старшим поколением, непривычным к «технологиям», и молодёжью, для которой цифровые технологии и устройства стали основой жизни и общения.

> Мы в книге не говорим, что подростки лучше владеют технологиями, как это сейчас принято у журналистов и чиновников. На самом деле это иллюзия. Подростки не владеют никакими технологиями, они просто продвинутые пользователи бытовых устройств и сервисов, не более того. *Технологиями* владеют программисты и разработчики сервисов и устройств.

Разрыв же, на наш взгляд, реальный, но связан вовсе не со сложностью «овладения технологиями» для старшего поко-

ления. Эти «технологии» не сложнее бытовых приборов. Да, многие до сих пор не могут толком освоить пульт управления медиацентром или меню стиральной машины, но это не от недостатка ума, а от лени, от нежелания вникать, читать руководства и т. п. То же самое – с технологиями.

купил айфон а чо с ним делать
где кнопки чтобы нажимать
и как мне позвонить сереге
а вот и он звонит и чо

Настоящий цифровой разрыв связан с дефицитом внимания к детям. Это разрыв социальный, а не технологический. Взрослые вручили своим детям смартфоны в надежде, что те не будут их беспокоить и отрывать от важных взрослых дел. Это сработало – детей теперь не слышно и не видно. До тех пор пока с ними не случится какая-то неприятность по «цифровым» причинам.

Естественно, приложения в смартфоне, социальные сети имеют достаточную «клейкость» и засасывают тех, кто готов посвящать им несколько часов в день. Так и возникает разрыв: мама работает, обстирывает и кормит подростка, а тот общается не с ней, а с «френдами» в телефоне.

В книге мы хотим восполнить этот дефицит внимания, напомнить о том, как важно знать, что делают дети в этом цифровом пространстве, и устранить иллюзорное (и часто довольно удобное) чувство беспомощности перед новой циф-

ровой реальностью, выработанное у взрослых, находящихся по эту сторону цифрового разрыва.

Чувство беспомощности у учителей и родителей

К сожалению, большинство современных родителей действительно не владеют цифровыми устройствами и технологиями настолько хорошо, как их дети. Чаще всего потому, что родителям и учителям есть чем заниматься и без развлечений на смартфоне. А подростки делают цифровое общение своим главным занятием, осваивают множество приложений и сервисов, заводят цифровых друзей, вырабатывают цифровую зависимость и отдаляются от родителей.

Взрослые тоже часто сидят в соцсетях. Однако «цифровой разрыв» между поколениями, безусловно, есть: родители обычно не знают, чем занимается их ребёнок в Сети. Это происходит в том числе и потому, что родители воспринимают смартфон как усовершенствованную соску, средство успокоения, позволяющее не обращать внимания на подростка. Чем бы дитя ни тешилось – лишь бы не плакало.

В большинстве случаев, связанных с выявленным деструктивным поведением подростков (уличное насилие, суицид, закладка наркотиков), выясняется, что родители понятия не имели, чем их ребёнок занимается в Сети, кто его «друзья»[1], о чём они общаются. Более того, они не имели

[1] Именно «друзья», а не друзья – между двумя этими понятиями есть огромная

представления, как это узнать, а часто и не интересовались этим в принципе.

Когда же сетевое общение, игры и прочие цифровые увлечения по нескольку часов в день в течение нескольких лет наконец оказывают серьёзное влияние на психику ребёнка, родители начинают открывать для себя, что их ребёнок сильно изменился, они не знают и не понимают его, не могут найти общий язык.

разница, раскрытие которой требует отдельного раздела. Мы подробно разбираем это в главе 6.

Дети, воспитанные смартфоном

Современные дети и подростки меняются: они становятся зависимыми от смартфона, им постоянно нужно общение с «френдами», они теряют фокус внимания, уважение к знаниям и книгам, у них вырабатывается клиповое мышление.

Многие исследователи пишут, что детям и подросткам вообще не стоит пользоваться цифровыми устройствами, поскольку их мозг только формируется. И от постоянного, по 5–7 часов, «общения» с цифровыми устройствами он может сформироваться каким-то другим, неизвестным нам способом.

Серьёзных исследований того, как на мозг детей влияет постоянное использование смартфонов, ещё нет. И, скорее всего, в ближайшие 5–10 лет не будет, так что проблема пока просто не осознана и не исследована.

Мы просто не знаем, что происходит и какой ящик Пандоры мы открыли. Но кое-что понятно уже сейчас – о чём, собственно, эта книга.

Цифровые джунгли

Все современные горожане привыкли жить в основном в контролируемом пространстве: в городе с парками, торговыми центрами, школами, университетами, кинотеатрами, транспортом. В дикой, никем не контролируемой природе мы бываем редко – разве что в походах и поездках.

В контролируемых пространствах убирают мусор, следят за порядком, там есть служба безопасности и камеры, там нет диких животных, опасных ям или обрывов.

Ровно такие же представления мы переносим в цифровую среду: нам «по умолчанию» кажется, что это такой парк с развлечениями и аттракционами.

Подросткам – тем более; они с детства «тусуются» в этой среде, привыкнув к подразумеваемой и обязательной безопасности в школе, торговом центре, парке и дома.

На самом деле за порядком в социальных сетях не следит никто, там полно опасных животных, ям и обрывов. Цифровой мир сейчас – это джунгли, в которых обитают опасные, хищные сущности, растут ядовитые растения, летают назойливые кровососущие насекомые, переносящие опасные инфекции, а под ногами – незаметные трясины и зыбучие пески.

Пока в цифровых джунглях не наведён порядок, вести себя там нужно очень аккуратно, соблюдая цифровую гигиену

и осторожность с их обитателями.

Наша книга – об этом.

Откуда всё это знаем мы, авторы

Мы сами родители, озабоченные вопросом цифровой безопасности для своих семерых детей. К тому же мы специалисты в информационной безопасности. Со своими коллегами в компании «Крибрум» мы с 2010 года профессионально занимаемся мониторингом и анализом социальных сетей русского Интернета (Рунета).

> Мы выкачиваем примерно 340 миллионов зарегистрированных аккаунтов во всех социальных сетях и сервисах Рунета – в сетях «ВКонтакте», Facebook, Twitter, Instagram, YouTube, «Одноклассники», «МойМир», TikTok и др., а также более чем в 20 тысячах интернет-СМИ и сотнях тысяч блогов.
>
> Это примерно 150 миллионов сообщений в день (до 30 000 сообщений и 100 000 лайков в секунду). Все важные и часто обновляемые аккаунты – 75 % от всех сообщений – мы выкачиваем каждые пять минут, а остальное – за час-два.
>
> По сути, «Крибрум» – это большая поисковая машина (вроде Google или «Яндекса»), которая выполняет поиск не на обычных сайтах, а в социальном пространстве Рунета.

«Крибрум» ежесекундно получает так называемые большие данные обо всех пользователях социального Рунета, что

даёт возможность видеть процессы «сверху», с высоты птичьего полёта. И выявлять разные закономерности и тенденции, которых не видно «внизу».

В компании трудится не один десяток аналитиков и дипломированных поведенческих психологов, имеющих опыт работы с трудными подростками и деструктивными движениями. Мы выпускаем регулярные отчёты обо всех деструктивных движениях Рунета.

С помощью «Крибрума» и вместе со специальным государственным Центром исследований и сетевого мониторинга мы изучаем деструктивные движения в социальных сетях (связанные с самоубийствами, криминалом, школьными расстрелами и др.) с 2016 года. О них мы подробно расскажем далее.

> Чтобы предупредить возможный вопрос: «Как же так получается, что в книге вы рассказываете о цифровом следе и предупреждаете о слежке, а сами занимаетесь тем же самым?» – мы сразу скажем: мы не следим за людьми, мы изучаем поведение **аккаунтов**, учётных записей в социальных сетях, в основном исследуя их **массовое** поведение; мы **не устанавливаем личность пользователя**, не вычисляем его Ф.И. О. и адрес, не перехватываем ничьи коммуникации и не показываем рекламу, не продаём наши данные об аккаунтах рекламщикам. Мы наблюдаем за массовым поведением пользователей Сети; таких наблюдений, пусть даже обезличенных, вполне достаточно, чтобы

делать содержательные выводы, о которых мы и говорим, в частности, в нашей книге.

О чём и для кого эта книга

Мы изначально писали эту книгу как пособие для родителей, воспитателей и учителей, которые столкнулись с «цифровым цунами» неожиданно и не будучи подготовленными, – чтобы помочь им осознать риски и проблемы и научить справляться с ними при воспитании детей и подростков.

Однако почти все из нас – родители, старшие братья и сёстры, воспитатели «цифровых туземцев» или хотя бы озабоченные дети пенсионеров, купивших смартфон. Да и вообще, о большинстве описанных здесь угроз и рисков должны знать практически все, кого затрагивает цифровая сфера: те, кто пользуется смартфоном, заходит в Интернет.

Так что можно сказать, что эта книга – для всех, кто в быту или по работе сталкивается с цифровой средой, не будучи цифровым экспертом: профессиональным программистом, разработчиком интернет-сервисов или специалистом по информационной безопасности.

Эта книга не даст вам готовых рецептов «исправления ситуации» в случае цифровой зависимости, отчуждения подростков, как и не предложит гарантированных способов борьбы с деструктивным поведением в Сети. В первую очередь потому, что ситуация в Сети очень быстро меняется, новые движения, новые риски и опасности появляются бук-

вально каждый месяц.

А кроме того, мы вообще против «лечения по переписке».

Мы хотим предложить читателю общий подход, дать представление о том, как происходит вовлечение подростков (и взрослых) в цифровую сферу, какие опасные места и явления там скрыты, какие вредные сущности населяют эти цифровые джунгли, как они охотятся на подростков.

Мы не претендуем на полноту описания всех цифровых явлений. Это невозможно – Сеть слишком велика и быстро меняется.

Но, как говорится, **знание немногих принципов заменяет знание многих фактов**, особенно в эпоху перемен, в которой нам приходится жить. Эти принципы мы описали в последующих главах – про киберриски, цифровой след пользователя, слабые и сильные связи в Сети, качество информации, цифровую зависимость подростков и охотящихся на них хищников в цифровых джунглях.

Основной вывод, который должен сделать читатель, по нашему замыслу в том, что нельзя игнорировать цифровое отчуждение детей, нельзя думать, что если подросток сидит в смартфоне и не отвлекает родителей от важных дел, то всё ОК.

Напротив, мы хотим побудить взрослых сделать над собой усилие и погрузиться в этот цифровой поток вместе с детьми, за которых они несут ответственность перед обществом, государством, самими детьми и своей совестью.

Дать аргументы для разговора с молодёжью

Подростки[2], хотя и «владеют технологиями» – то есть умеют нажимать кнопки на смартфоне, – обычно не склонны к рефлексии, не осознают происходящего с ними в цифровой среде. Они просто плывут по течению, которое может заносить их куда угодно. Кто-то должен разговаривать с ними, объяснять явления вокруг них, озвучивать риски.

Задача взрослых – рассказывать детям, как устроена жизнь и как себя вести с другими людьми. И раньше это не составляло труда: ещё с младенчества детям читали волшебные сказки, в которых были зашифрованы основные жизненные ситуации (условно говоря, «не разговаривай в лесу с незнакомцами и не рассказывай, куда и к кому идёшь»), а в более старшем возрасте давали советы на тему, как строить отношения.

Но объяснить подростку, что происходит в цифровой среде, даже на элементарных примерах, взрослые сейчас обычно не в состоянии. Это создаёт у подростков ложное чувство превосходства, ощущение, что они всё понимают лучше родителей и со всем могут справиться сами.

---

[2] Будем для простоты считать подростком молодого человека в возрасте 14–17 лет, хотя большинство описываемых в книге явлений относится и к детям 7–13 лет.

Это, конечно, неверно и очень опасно.

В книге мы хотим привести родителям и педагогам убедительные аргументы и предложить интересные темы для разговоров с детьми. Возможно, такие разговоры помогут подростку избежать некоторых опасностей цифровой среды.

Конечно, важно просвещать на эту тему и самих взрослых: учителей, родителей, правоохранителей, законодателей.

Мы разрешаем всем, кто занимается проблемой деструктивных движений молодёжи и цифровым образованием подростков, свободно цитировать материалы книги, использовать их для создания курсов, докладов, статей.

Как читать эту книгу

Мы начинаем с общих принципов и переходим к конкретным рискам и опасностям, а дальше (иногда) – к конкретным рекомендациям.

Однако читать книгу можно и выборочно, по главам. Если вам, например, интересно про цифровой след – сразу открывайте главу 2. В ней достаточно информации для понимания темы цифрового следа и слежки за пользователями.

В книге информация иногда намеренно повторяется: описываются случаи рассмотрения одной и той же темы, одного и того же феномена с разных сторон. Это сделано, во-первых, потому, что повторение – мать учения, а во-вторых, именно для тех наших современников с дефицитом времени и/или внимания, кто читает наискось, со случайного места, «методом тыка», наугад, – таким образом, каждая глава оказывается максимально самодостаточной.

Издание предназначено в основном для родителей и учителей, но во многих случаях мы обращаемся как бы к самому подростку напрямую. Это сделано осознанно – чтобы предложить читателям готовые примеры аргументации в разговоре с подопечными.

Создавая книгу, мы не старались провести научное исследование – мы стремились откровенно поговорить на тему цифровых рисков и цифрового отчуждения. И пусть вас не

смущает обилие ссылок на статьи психологов и других специалистов по сетевому общению и цифровым рискам. Мы советуем не полениться и прочитать хотя бы некоторые из них: как правило, материал там изложен подробнее, а рекомендации – конкретнее, чем в главе книги.

В качестве эпиграфов мы иногда используем популярные «русские хокку» – так называемые перашки[3] (нерифмованные четверостишия) и другие «мемасики» из Сети. Это не потому, что мы несерьёзно относимся к описываемым проблемам, а потому, что именно так их воспринимают и вербализируют в Сети сами цифровые деятели: тролли, спамеры, журналисты, рекламщики, обычные пользователи – в общем, нападающие и потерпевшие цифровой среды.

[3] Мы берём их из Сети, где они гуляют свободно, в том числе и с основного сайта http://perashki.ru/.

Дисклеймер, или Отмазка

Мы хотели бы попросить читателя не воспринимать эту книгу как детальный и сверхточный научный труд или энциклопедию сетевой жизни. Хотя авторы и консультанты книги профессионально занимаются информационной безопасностью, анализом соцсетей и деструктивных течений, не было цели в каждой главе полностью рассмотреть проблему и привести абсолютно точные рецепты. Напротив, мы старались дать читателю общее представление о существующих проблемах и угрозах и простимулировать желание разбираться в них и в методах защиты **самостоятельно**.

Если в какой-то главе не рассмотрены все без исключения типы угроз и виды злоумышленников, не рассказано о том, что вы недавно слышали от соседского мальчишки-студента или лектора на YouTube, – это нормально. Сетевые угрозы и явления социальной сферы возникают и мутируют настолько быстро, что никакая книга за ними не угонится.

> Конечно, профессиональные социологи или специалисты по деструктивным сообществам, поведенческие психологи или сотрудники киберотделов спецслужб могут предъявить претензии к недостаточной проработанности конкретных тем, неполноте охвата всего спектра явлений или справочного и ссылочного инструментария. Но

повторимся: это не научная монография и не курс боевых социально-информационных технологий для оперативников МВД.

Кто мы: коллектив авторов и консультантов

Игорь Ашманов

Родился в 1962 году в Москве, в семье математиков и преподавателей. Окончил маткласс средней школы, учился на Мехмате МГУ, стал заниматься программированием и искусственным интеллектом в отделе искусственного интеллекта Вычислительного центра АН СССР в 1983 году. Русский, православный, женат, отец пятерых детей.

■ **Образование и научная деятельность:**

• выпускник мехмата МГУ по кафедре высшей алгебры (1983);

• кандидат технических наук (1995) по прикладной лингвистике и искусственному интеллекту;

• заведующий кафедрой цифровой социологии ВШССН МГУ.

■ **Профессиональная деятельность:**

• разработчик систем ИИ с 1987 года;

• один из авторов системы правописания ОРФО (встроена в Microsoft Office);

• исполнительный директор поискового портала «Рамблер» в 1999–2001 годах;

• разработчик спам-фильтра (в настоящее время «Антиспам Касперского»);

• разработчик систем анализа социальных сетей, виртуальных собеседников, новостных агрегаторов.

■ **Деловая активность:** президент компании «Ашманов и партнёры», президент компании «Крибрум», основатель ещё пяти компаний в области ИИ.

■ **Общественная деятельность:** участник разработки программы «Цифровая экономика», руководитель подгруппы «Защита прав личности в ЦЭ», доверенное лицо В.В. Путина в 2018 году, член Совета по развитию гражданского общества и правам человека при Президенте РФ. Один из разработчиков модуля «Безопасность в информационном пространстве» в учебнике нового поколения для 8–9-х классов по предмету «Основы безопасности жизнедеятельности».

Наталья Касперская

Родилась в Москве в 1964 году, окончила среднюю школу, затем – Московский институт электронного машиностроения (факультет прикладной математики). После рождения двоих детей вышла на работу в отдел антивирусных решений ИТ-компании КАМИ в 1994 году. Основала в 1997 году «Лабораторию Касперского» и была её гендиректором и председателем совета директоров до 2011 года. Основатель компании InfoWatch. Русская (с немецкими корнями), пра-

вославная. Замужем, мать пятерых детей.

■ **Образование:**

• выпускница Московского института электронного машиностроения, факультет прикладной математики (1987);

• бакалавр делового администрирования, Открытый университет бизнеса Великобритании;

• заведующая кафедрой информационной безопасности ВШЭ.

■ **Деловая активность:**

• сооснователь «Лаборатории Касперского», ведущей российской компании в области информационной безопасности;

• сооснователь компании «Крибрум», ведущей системы анализа социальных сетей и СМИ, акционер пяти компаний в области безопасности и искусственного интеллекта;

• глава и основной владелец группы компаний InfoWatch, российского лидера в области борьбы с утечками конфиденциальной информации.

■ **Общественная деятельность:**

• руководитель Рабочей группы по направлению «Информационная безопасность» нацпроекта «Цифровая экономика Российской Федерации»;

• председатель правления Ассоциации разработчиков программных продуктов (АРПП) «Отечественный Софт»;

• член Экспертного совета по российскому программному обеспечению при Минкомсвязи РФ, член грантового ко-

митета Фонда «Сколково»;

• член Рабочей группы по внесению поправок в Конституцию РФ в 2020 году, автор поправки в ст. 71 о защите данных граждан;

• член инициативной группы по выдвижению В.В. Путина на президентских выборах 2018 года, доверенное лицо мэра Москвы С.С. Собянина в 2018 году, член Штаба ОНФ.

Консультанты

Артём Николаевич Курицын – аналитик, руководитель подразделения специальных проектов АО «Крибрум». Сфера интересов: анализ и изучение деструктивного контента и деструктивных явлений и субкультур, распространяющихся в социальных медиа.

В 2013 году окончил Рязанский филиал Московского университета МВД России по специальности «юриспруденция». Проходил службу в подразделениях по противодействию экстремизму. Окончил службу в Центральном аппарате МВД России.

Соавтор аналитических докладов «Фальсификации истории. Манипуляции в социальных сетях», «Демонтаж героических образов», «Информационная война против России. Конструирование образа врага». Один из разработчиков модуля «Безопасность в информационном пространстве» в инновационном учебнике нового поколения для 8–9-х клас-

сов по предмету «Основы безопасности жизнедеятельности» и учебно-методических пособий для преподавателей Центров цифрового образования детей «IT-куб», созданных при поддержке Министерства просвещения Российской Федерации. Один из авторов сборника материалов «Проблемы социальных конфликтов в современной психологии» (2018).

Принимает активное участие в образовательной и просветительской деятельности, проводя лекции в МГУ им. М.В. Ломоносова, МГТУ им. Баумана, НИУ ВШЭ и других вузах страны.

Юрий Сергеевич Синодов – журналист, главный редактор, исследователь социальных сетей. Обучался и публиковался в «Академии журналистики «КоммерсантЪ». С 2019 года директор по развитию «СМИ2», преподаватель журналистики в нескольких вузах (ВШЭ, СевГУ, МГУ), лауреат отраслевой интернет-премии «РОТОР» как журналист и главный редактор года.

Основатель и главный редактор сайта Roem.ru, освещающего работу российской прессы и интернет-компаний, работал в РБК, «Рамблере», «Вебпланете», Lenta.ru.

Член правления Регионального общественного центра интернет-технологий (одна из старейших общественных организаций Рунета, занимающаяся созданием дружественной интернет-среды и популяризацией интернет-технологий).

Много лет исследует коммуникативную специфику социальных сетей.

Сергей Игоревич Тулаев – предприниматель, исследователь проблем безопасности интернет-сервисов и смартфонов.

Принимал участие в создании социальных сетей, масштабных развлекательных проектов.

Изучает особенности поведения интернет-пользователей и пользователей мобильных устройств, вовлечение в интернет-зависимость и технологии сетевого манипулирования.

Автор цикла лекций, посвящённых влиянию широкого использования смартфонов на общество и связанными с этим рисками и угрозами.

Искандер Сулейманович Валитов – публицист, кандидат медицинских наук, нейрофизиолог. Сфера интересов: философия и методология здравоохранения, образования. Общественный деятель, член Зиновьевского клуба МИА «Россия сегодня». В настоящее время занимается разработкой антропотехнического подхода к болезням и здоровью, проблемами формирования мозга и разумной деятельности человека. Соавтор книги «Русский урок истории». Печатался в журнале «Однако».

В 1979 году окончил лечебный факультет Казанского медицинского института. Защитил кандидатскую диссертацию по нейрофизиологии. Руководил Институтом здоровья при Министерстве здравоохранения Республики Татарстан, создал службу скрининга населения г. Казани на сахарный диабет, сеть школ для больных сахарным диабетом, служ-

бу гуманитарной поддержки онкологических больных, научно-производственное объединение по разработке, производству эндохирургического оборудования и подготовке хирургов, службу мониторинга распространения ВИЧ в Республике Татарстан и др.

Работал советником министра здравоохранения Украины, советником вице-премьер-министра Украины по социально-гуманитарным вопросам.

Занимался антикризисным управлением в бизнесе. Управлял крупными политическими проектами, в том числе избирательными кампаниями. Участник Московского методологического кружка, соучредитель и исполнительный директор Фонда «Архив Московского методологического кружка». Инициатор и организатор общественно-политического движения украинских врачей «Пульс Украины».

Введение. Новая эпоха

– Вовочка, ты утром встаёшь на зарядку?
– Нет, Марь Иванна, у меня зарядка сломалась, а родаки свои не дают.

За предыдущие циклы ввода новых технологий мир несколько раз менялся, но как? Лучше стало или хуже? Вообще изменения – это хорошо? И так ли уж неизбежно?

Технологии – благо или зло?

В последнее время вы наверняка слышали немало предостережений об опасности цифрового мира, в том числе от деятелей индустрии информационных технологий.

В книге мы подробно их обсудим. Но сперва нужно ответить на важный для читателя вопрос: действительно ли авторы ретроградны и не видят ничего хорошего в современных цифровых технологиях?

> Надо сказать, что последние 30 лет мы занимаемся исключительно цифровыми технологиями – это наша профессия. Мы окончили технические институты и во взрослой жизни уже четверть века ничем, кроме «цифры», профессионально не занимались.
>
> Мы разрабатываем программы для информационной безопасности, поисковые машины, нейронные сети и приложения искусственного интеллекта. Мы сами участвовали в строительстве этого цифрового мира – построили часть его, хоть и небольшую, в России, именно поэтому видим цифровой мир без прикрас и иллюзий – таким, как он есть.

Но ведь все знают, что технологии – это благо, с их помощью мир изменился!

Мир действительно изменился. Сегодня почти у каждого – персональный компьютер, смартфон, фитнес-браслет, аккаунт в Facebook, фотки в Instagram, чат в WhatsApp, «Ян-

декс. Такси» у подъезда. Круто же? Нет, не круто.

Людям же удобно – современно, быстро. Что не нравится? Не нравятся несколько моментов.

Первый: направление этих изменений определяем не мы. Мы принимаем новинки как есть и послушно подстраиваемся под изменившийся мир.

Второй: все эти новинки – дары данайцев. На самом деле предлагается подмена чего-то настоящего бутафорией. Производительность труда от компьютеров не растёт (да-да, это довольно удивительный, но исследованный и доказанный факт), просто меняются способы и формы работы.

> **Полноценная ли замена?** Работа на компьютере – вместо работы в цеху или на стройке. Общение в соцсетях – вместо живого общения. Слабые связи в Сети – вместо сильных в жизни. Замена традиционного социального уклада и общения подписками в группах и блогах. Замена традиционных ценностей и занятий нажатием кнопок. Вместо реальных знаний – результаты выдачи поисковиков. Вместо чтения книг – чтение комментов. Вместо журналистики – поток жёлтой прессы.

Общение в чатиках не эквивалентно личному общению.

Оглянитесь: на улице, в кафе, в транспорте, на остановке люди «втыкают» в смартфоны. Что они делали 20 лет назад? Они читали книги и газеты, курили, общались, смеялись. Смотрели в окно и на окружающих.

Что они делают сейчас, читают важное? Вообще-то нет. Они одиноки, никого не видят, часами отвечают бессмысленными репликами на бессмысленные реплики малознакомых сетевых сущностей, играют в бессмысленные игры или смотрят бессмысленные ролики бессмысленных видеоблогеров. Что-то не так с новыми технологиями. И мы, разработчики технологий, тоже видим это.

Закон Старджона

Есть довольно простой (даже шуточный) закон Старджона, озвученный писателем-фантастом Старджоном[4] ещё 50 лет назад: **90 % чего угодно – хрень**[5].

Это означает, что в большинстве процессов, событий, контента – всего, что происходит, – основная часть бесполезна или даже вредна. Просто потому, что всё рано или поздно портится, а точнее, **люди склонны портить что угодно**.

То же самое, как ни удивительно, относится и к новейшим, таким удобным информационным технологиям – Интернету, смартфонам, социальным сетям и т. п. По какой-то причине в каждой бочке новых технологий есть ложка дёгтя. Они все – с какой-то червоточиной.

Результат (или цена) внедрения новых технологий в нашу жизнь – множество странных, вредных, негативных явлений: почтовый спам[6], безделье «офисного планктона», зависимость от соцсетей, пожирающая по нескольку часов в день, непрерывное смотрение в смартфон, клиповое мышле-

---

[4] https://ru.wikipedia.org/wiki/Закон_Старджона.

[5] В оригинале это звучит как Ninety percent of everything is crud. Crud – это «бессмыслица» в весьма экспрессивном выражении, но совсем не «дерьмо», как принято думать. Если бы Старджон имел в виду именно такую формулировку, он бы написал crap.

[6] Спам – непрошеная и навязчивая реклама (назван в честь очень навязчивой рекламы консервов «Спам»).

ние, короткая память, неспособность удерживать фокус внимания, постоянный поток фейков и вбросов, массовые манипуляции сознанием, пропаганда, запугивание, разводки.

> Возьмём, к примеру, электронную почту. В ней эти сакраментальные 90 % составляет мусор, спам – нигерийские письма, трафик на сайт, фишинг, финансовые пирамиды, страшилки. Вы можете часть спама не видеть, потому что на его пути к вам уже стоят спам-фильтры (которые пришлось разрабатывать в том числе авторам этой книги), но он там есть и составляет примерно 95 % от всех писем.
>
> В Интернете на 90 % грязь, порно, травля, экстремизм, вирусы, хакеры, торговля наркотиками, рекламная «джинса»[7] и т. д. В смартфонах – тотальная слежка. В соцсетях – абсолютная прозрачность, слежка, фейки, разводки, флешмобы, идеальная манипулируемость. Да что ж такое?

Это всё не случайные, а **необходимые, неизбежные следствия** новых технологий. Червоточина – в сердцевине, в основе. Сразу по внедрении новой технологии приходится начинать бороться с этой грязью, токсинами. Например, первый спам появился в электронной почте буквально в самом начале, когда ею пользовалось всего несколько сотен человек. Первые вирусы пошли по компьютерным сетям в 80-х годах прошлого века, когда пользователей было лишь несколько тысяч.

---

[7] Скрытая реклама под видом содержательной статьи или новости.

Почему так?

Причина очень проста. Дело прежде всего в деньгах, потому что цель внедрения новых продуктов и технологий – всегда *деньги*, это сейчас единственная *метрика*. Мы же живём при капитализме, где всё решает капитал.

А то, что превращается в деньги, на следующем звене обязательно превращается в полную хрень. Фантаст Старджон из этого же мира, поэтому он и описывает свой мир своим законом Старджона.

Это новый цикл, постмарксовский: *технологияденьгихрень* и опять *технологияденьгихрень*. И так далее.

Цифровые маугли: поколения «цифровых туземцев»

Приходит мама за ребёнком в детский сад.

Смотрит, дети в песочнице сидят со смартфонами, а воспитательница спит на скамейке.

– Что ж вы спите? У вас же все дети разбегутся…

– Да куда они денутся, у нас Wi-Fi только в пределах песочницы.

Современные дети рождаются в цифровом мире. Их можно назвать «цифровыми туземцами» или «цифровыми аборигенами» (по-английски *digital native*).

Туземец – не обидное слово, оно просто означает «местный», «родившийся тут, на этой земле». Первое поколение «цифровых туземцев» за последние 20–25 лет – это поколение конца 90-х – начала 2000-х, родившееся, когда у родителей уже были компьютеры и мобильные телефоны. Нынешнее поколение рождается, когда смартфон лежит на каждом столе и в каждом кармане. Условно говоря:

- 1995–2004-й – компьютер у родителей;
- 2005–2014-й – планшет с колыбели;
- с 2015-го – «поколение больших пальцев», родились со смартфоном в руке.

В популярных психологических и социологических статьях сейчас модно делить молодёжь на поколения: «миллениалов», поколения X, Y и Z и т. п. Мы не будем пользоваться этими определениями из прессы, к настоящей социологии они не имеют отношения.

«Цифровые туземцы» имеют общие особенности психики.

■ **Виртуальная реальность им ближе и понятнее реальной** – игры на телефоне важнее игр со сверстниками или чтения книг; вместо общения подростки молча сидят группой каждый в своём смартфоне.

■ **клиповое мышление** – гранулированное потребление информации, неспособность читать больше шести абзацев за раз, смотреть видео дольше двух минут; неспособность удерживать фокус внимания, желание всё время переключаться.

■ **Поиск вместо знаний** – постоянная проверка информации в поисковике вместо запоминания фактов, отрывочные сведения обо всём, презрение к знаниям.

■ **Слабые связи вместо сильных** – ненастоящие, малознакомые «друзья» в Сети, часть из которых – равнодушные незнакомцы или враги.

■ **«Не заинстаграмил – значит, не было»** – вечная публичность, привычка всегда быть на сцене, на публике, сообщать всем о событиях и фактах из своей жизни, постить фотки и «видосики» о себе; полная прозрачность, но при этом показуха, создание фальшивого фасада, зависимость от

«видимости», восприятия другими.

■ **«Цифровое одичание»** – отрывочные сведения обо всём, дикость, нехватка культуры. Нет привычки читать, получать систематические знания, изучать культуру, катастрофическое незнание элементарных вещей из истории, литературы, математики.

■ **Проблемы со здоровьем** – искривление позвоночника, ухудшение зрения, здоровья в целом.

■ **Цифровая наркомания** – зависимость от смартфона, от «друзей», постоянное ожидание сообщений, лайков, комментов.

Это не случайные эффекты и даже не побочное действие технологий, как бывает у полезного лекарства. Это всё встроенные, центральные, ключевые свойства современных цифровых технологий, за счёт которых они и получают распространение и захватывают аудиторию.

Это не случайно: геймификация и аддикция

Основатели и разработчики социальных сетей и других сервисов прямо пишут в своих книгах и мемуарах, что пытались создать и развить у пользователей цифровую зависимость, используя известные или новые психологические технологии вовлечения, небольших поощрений, постоянного ожидания, «дофаминовую наркоманию», «бесконечный стакан» сообщений и тому подобные способы посадить пользователя на крючок.

Часто «интернет-олигархи» в интервью говорят, что собственных детей они ограничивают в использовании смартфонов, Интернета и соцсетей именно потому, что сами хорошо понимают, как устроены эти технологии вовлечения.

Далее мы подробнее разберём социально-психологические особенности игр и сетевого общения.

Соцсети: новое доверие

Люди проводят в социальных сетях по 6–8 часов в день. Иногда больше, чем на работе или в школе!

Пользователи считают их своим интимным пространством, информации от «друзей» доверяют больше, чем любым официальным СМИ, они совершенно не защищены от манипуляций злонамеренных обитателей социального пространства. А между тем в социальных сетях оперирует огромное количество профессиональных манипуляторов: рекламщиков, пропагандистов, политтехнологов, экстремистов и преступников.

Социальное медийное пространство – идеальная среда для рекламы, влияния на умы, криминала, информационной войны, экстремизма и организации беспорядков.

Соцсети: не парк, а джунгли

Представьте, что вы (или ваши дети) заходите в городской парк. Хотя вы этого не замечаете, но в нем постоянно незримо поддерживается безопасность:

• нет хищных животных и ядовитых растений;

• нет опасных людей, хулиганов, пьяных компаний;

• нет обрывов, ям, упавших деревьев, руин, битого стекла под ногами, колючей проволоки в траве;

• нет мусора, стоят урны, дорожки подметены, лавочки покрашены;

• нет опасных продуктов и напитков;

• есть патрули, кнопки вызова полиции, посетители присматривают за порядком.

Кто-то следит за всем этим. Мы с вами знаем кто – городские и районные власти, МВД, дворники и т. д. Но дети и подростки об этих «ком-то» обычно не знают, не задумываются и не подозревают об усилиях по поддержанию общественной безопасности.

Их это и не очень-то интересует, для них это само собой разумеется, как наличие воды в кране и света в квартире. Они воспринимают безопасность улиц, транспорта, парков, торговых центров как данность, как воздух – по какой-то причине она всегда есть, о ней не нужно думать.

Когда подростки заходят в социальные сети, происходит

то же самое – они не думают о безопасности, ведут себя так же, как и в прочих, контролируемых пространствах, как в школе, торговом центре, парке. Однако социальные сети – это не парк, а опасные цифровые джунгли.

В социальных сетях практически никто не следит за порядком, нет специальных структур, которые должны это делать. Собственные службы модерации социальных платформ либо не справляются с контролем, либо просто не имеют задачи поддерживать безопасность.

В результате в социальных сетях таится огромное количество рисков и опасностей:

• много хулиганов, троллей, просто идиотов, неуравновешенных людей;

• много мусора: ругани, мата, травли, негатива, глупостей, гадостей, жёлтого, чернушного и шокового контента;

• много опасных хищников: взрослых, притворяющихся детьми, мошенников, вербовщиков, манипуляторов;

• в Сети работают так называемые *воронки вовлечения*, то есть целые системы вовлечения в цифровые ловушки, опасные группы, мошеннические системы.

Все эти риски неочевидны, не бросаются в глаза, в Сети нет предупреждающих о них знаков.

В общем, цифровая среда полна скрытых рисков, которые угрожают всем её обитателям.

Электронные и информационные риски

Риски цифрового мира можно условно разделить на два вида.

1. **Электронные риски, или киберриски, угрожающие самому устройству** (смартфону, планшету, ноутбуку), установленным на нём программам, банковским счетам, паролям и т. п.

2. **Информационные** (они же контентные) риски, создающие угрозы сознанию владельца цифрового устройства: от развития цифровой зависимости, ухудшения когнитивных способностей до прямых атак на сознание.

К первой категории рисков – киберрискам – относятся компьютерные вирусы, троянские программы, непрошеное рекламное программное обеспечение, тайно устанавливающееся на смартфон, шпионские программы, почтовый спам, разнообразные атаки на пользователя (разводки) с использованием *социотехники*, которые проводят вымогатели, шантажисты, финансовые мошенники. Все они могут привести к потере файлов, разрушению устройства, краже паролей, исчезновению денег с банковского счёта и т. п.

Вторая категория рисков – информационные – включает возникновение цифровой зависимости от общения в социальных сетях, ухудшение когнитивных способностей, фор-

мирование клипового сознания, вовлечение в деструктивные группы, секты, экстремистские организации, а также пропаганду, «перепрошивку» сознания.

Мы считаем, что вторая категория рисков наиболее опасна. Плохо, если цифровые злоумышленники украли у пользователя пароли или деньги, но гораздо хуже, когда они **украли мозги**.

Поэтому наша книга будет в основном посвящена информационным опасностям. А начнём мы всё же с киберрисков.

Глава 1. Киберугрозы в Сети: хищные программы и люди

У некоторых взрослых, слабо знакомых с цифровыми устройствами и Интернетом, сохраняется иллюзия, будто кто-то всё-таки защитит пользователя. Например, иногда можно услышать что-то вроде: «Нет, ну а что, поставлю “Касперского”, всё будет ОК». Спору нет, антивирус Касперского – лучший в стране.

Но от всех существующих угроз цифровой среды и Интернета никакой антивирус защитить не сможет. Прежде всего потому, что вы сами, по доброй воле купили себе устройство, ежеминутно создающее новые киберриски.

Сегодня практически любое электронное устройство (и особенно смартфон) не принадлежит его владельцу в полной мере, несмотря на то что куплено за его кровные деньги. Фактически главное предназначение личного устройства – *следить за пользователем и доставлять ему уведомления от сервисов и приложений, управляя вниманием владельца или эксплуатируя вычислительный ресурс без его ведома, в фоновом режиме.*

Смартфон как источник рисков

Мало кто из подростков (а порой и взрослых) понимает, что современный смартфон – это полноценный маленький компьютер, который, в отличие от настольного компьютера или ноутбука, имеет постоянный доступ в Интернет и потому заведомо несёт в себе большие риски: как обычные компьютерные (вирусы, недокументированные возможности, закладки, слежка), так и информационные (воздействие на сознание своего обладателя, навязчивый контент, вовлечение в опасные группы в соцсетях).

Под воздействием на сознание мы понимаем в первую очередь то, что смартфон – **платформа для загрузки аддиктивного, «клейкого» контента**, несущего целый букет рисков и зависимостей: игры, видеоролики, порнография, пропаганда и т. п. Этим «контентным» рискам посвящена глава 6.

В этой главе мы остановимся на цифровых (компьютерных) рисках. Основные свойства смартфона, порождающие эти риски, таковы:

■ **платформа для доставки навязчивой рекламы**, только малая часть которой подчиняется хоть каким-то правилам;

■ **источник неконтролируемых уведомлений, предложений, приманок, разводок** и других воздействий на

пользователя, количество которых может достигать сотен в сутки;

■ **платформа для установки нежелательного и непрошеного ПО:** вирусов, троянских программ, шпионов, рекламных закладок и т. п.;

■ **источник утечки персональных данных владельца:** фотографий, личных данных, адреса, сведений о перемещении, номеров кредиток и пр. Риски этого вида находятся на стыке цифровых и информационных технологий и будут подробно рассмотрены в главе 2, посвящённой сбору данных.

Сначала поговорим о данных, которые любое устройство пытается собрать о владельце.

Сбор данных с устройства

Общий подход можно сформулировать так: чем более интенсивно используется устройство, тем больше данных о своём владельце оно накапливает. Данные бывают прямыми – фотографии, контакты, сообщения, которые владелец сам сообщил устройству и Интернету. А есть косвенные данные, которые вычисляются самим устройством на основе действий владельца. К ним относятся, например:

- история установки и использования приложений;
- история энергопотребления, то есть циклов и времени зарядки, интенсивности работы;
- история уведомлений и действий;
- история магазина приложений;
- история браузера, его кэш (просмотренные недавно страницы) и DNS[8];
- история перемещений по городу и многое другое.

Данные собирают производитель устройства (например, Apple, Huawei, Samsung и др.), платформа (iOS или Android), а также легальные и нелегальные (вредоносные) приложения. Короче говоря, данные собирают все, кто может.

Многие приложения при установке требуют дать им разрешение на доступ к вашей телефонной книге, файлам, фотографиям и т. д. Бесплатному приложению они нужны для

[8] То есть история адресов, запрашиваемых в браузере.

заработка путём получения и перепродажи ваших персональных данных.

> Есть классический пример бесплатного приложения «Фонарик», которому для функционирования никаких разрешений не требуется; тем не менее для установки оно требовало разрешение на доступ к звонкам и адресной книге.

Подробнее о сборе данных устройствами и слежке мы расскажем в главе 2.

Вредные приложения

У большинства вредных приложений на смартфоне и ноутбуке – экономические цели, то есть им нужно как-то получить или украсть деньги пользователя либо нажиться на нём другими способами.

Основные источники дохода таких приложений следующие.

■ **Продажа внимания.** Дороже всего продаётся внимание пользователя: это валюта, которой оплачивается доступ практически к любым сервисам. Монетизация внимания может быть различной – показ рекламы, создание искусственных неудобств, за снятие которых необходимо заплатить, участие в совместном создании контента (лайки и просмотры). Количество контактов с пользователем, плотность удержания его внимания напрямую влияют на доходность любого подобного сервиса. Таким образом, самым доходным бизнесом является продажа доступа к вниманию пользователя путём показа ему рекламы и другого контента в браузере и приложениях.

■ **Продажа профиля пользователя.** Несколько дешевле продаётся профиль – совокупность данных о пользователе: история просмотра сайтов, история использования приложений, список контактов, история геолокаций устройства, списки беспроводных сетей и Bluetooth-устройств, записи

звукового окружения, параметры среды (версия ОС, используемый мобильный оператор, характеристики устройства) и т. д.

Обычно эти данные продаются обезличенными: сама по себе **личность** пользователя для рекламодателей не очень интересна, притом что его персональные данные могут быть чувствительными (и стать источником юридических рисков для продавца).

Совокупность таких данных продаётся через цепочку посредников маркетинговым компаниям и позволяет им принимать решение о потенциальной ценности конкретного пользователя для рекламодателя.

Например, сочетание устаревшей версии ОС и отсутствие признаков активного использования современных технологий (мало установленных приложений, устройство редко используется) привлекает рекламодателей, продвигающих сомнительные платные мобильные сервисы, незаметно «снимающие» деньги со счёта неопытного пользователя.

Кроме того, может быть востребовано окружение пользователя. Распространённый сценарий: при регистрации в мессенджере или другом похожем сервисе пользователю сразу доступен список его контактов из памяти устройства. Причём контакты, как правило, получают уведомление о том, что он начал пользоваться сервисом.

На основании списка контактов, беспроводных

сетей, Bluetooth-устройств в зоне видимости пользователя можно делать выводы о его ближайшем окружении, примерном уровне дохода, семейном положении.

■ **Продажа неявного доступа к устройству.** Ещё дешевле продаётся невидимый, неявный доступ к устройству: накрутка рекламы в фоновом режиме, майнинг (добыча) криптовалюты, рассылка спама, «проксирование трафика» без ведома пользователя, то есть использование телефона как маршрутизатора стороннего интернет-трафика, что позволяет злоумышленникам маскировать свою мошенническую деятельность в Сети под обычную пользовательскую активность – например для накрутки показов рекламы.

Всё это могут делать без вашего ведома на вашем смартфоне вредные приложения, если вы их установите – вольно или невольно.

Рассмотрим подробнее некоторые типы таких приложений – фальшивые программы, вымогатели и денежные пиявки. У каждого типа – свой способ заработка на ничего не подозревающем пользователе.

Фальшивые приложения – это мимикрия под популярные приложения, как правило связанные с платежами (приложения мобильных операторов, клиент-банк и т. п.). Для работы требуют прямого участия пользователя (установки, ввода паролей, номеров счетов или карт и т. д.). Их цель – кража денег с мобильного телефона или с банковского счета

пользователя.

Вымогатели – «локеры» (вирусы-вымогатели) и шифровальщики, блокирующие телефон и требующие денег за разблокировку. Попадают на устройство при скачивании или установке сомнительного контента, а также под видом «хороших» приложений.

> Самым известным шифровальщиком в последние годы был вирус Petya, который заразил в 2017 году сотни тысяч компьютеров. Он шифровал жёсткий диск компьютера жертвы, а за расшифровку требовал выкуп. Правда, в некоторых версиях вируса содержалась ошибка, в результате которой данные можно было восстановить. Его последователь, вирус Non Petya, такой ошибки уже не содержал. Данные после него восстановлению не подлежали.
>
> Petya – пример вируса-шифровальщика, работающего и на персональных компьютерах, и на мобильных устройствах.

Ещё одна категория вредных приложений – так называемые **денежные пиявки**, программы со скрытой подпиской или однократными платежами, эксплуатирующие экосистему магазинов приложений и беспечность пользователя.

Таким образом, основные цели вредных приложений следующие:

- **кража денег со счёта мобильного телефона** через платные услуги операторов или непрошеные подписки;
- **кража денег с банковских счетов** через фальшивые

мобильные приложения банков;

■ **использование вычислительной мощности устройства для своих целей:** создание искусственного трафика, рассылка спама, майнинг криптовалюты и т. п. без ведома пользователя;

■ **наращивание трафика передачи данных**, за который владелец телефона будет вынужден заплатить своему оператору;

■ **сбор личных данных для перепродажи** (геолокация, списки беспроводных сетей, контактов, тексты SMS, история пользования приложениями и пр.);

■ **маркетинговое «профилирование» пользователя:** анализ личных данных, составление профилей поведения пользователя, перепродажа рекламным системам.

Вредные приложения могут устанавливаться добровольно самим пользователем, например для получения доступа к какому-то интересному или привлекательному контенту. Вам предлагают что-то установить, чтобы скачать свежий фильм? Скорее всего, это вредоносное ПО.

Косвенные признаки вредных приложений

Есть категории приложений, наличие которых на устройстве должно насторожить пользователя.

■ **«Защищённые» мессенджеры.** Мессенджеры с за-

щищённым чатом могут сигнализировать о желании подростка иметь секреты от взрослых. Особенно подозрительны **мессенджеры с «исчезающим контентом»**, которые удаляют сообщения по прошествии некоторого времени (например, Snapchat, Wickr). В таких приложениях возникают риски втягивания в игру «в секретики» со сверстниками, в ходе которой подростка могут сделать объектом шантажа, вовлечь в криминал, склонить к суициду и т. п.

■ **Приложения для анонимного доступа в сеть (VPN, Tor).** Эти приложения обычно используются для доступа к пиратскому контенту, прежде всего к фильмам (например, к Rutracker.org и другим торрент-сайтам, на которые иначе из России не попадёшь). Но могут сигнализировать и о желании подростка тайно получать доступ к запрещённому контенту.

■ **Приложения-«улучшатели».** Подозрительны любые приложения, якобы расширяющие функционал популярных программ – «дополнения» (или «аддоны») для WhatsApp, Instagram, Minecraft и т. д.

Подобные приложения, как правило, являются пустышками, использующими популярность чужого бренда для своего продвижения. Встречаются также модифицированные версии приложений-«улучшателей», в которые встроен вредоносный код. Как правило, мотивация пользователя для установки подобных приложений – какая-либо дополнительная функциональность, которой нет в исходном приложении, на-

пример возможность всегда видеть сетевой статус контактов в WhatsApp.

Игра Minecraft – общеизвестный чемпион по вирусам среди дополнений в категории «Игры». А многочисленные инструменты для накрутки аккаунтов в Instagram – чемпионы по встроенным вирусам среди мобильных приложений для коммуникаций. Раскрутить бот-лайками аккаунт в Instagram они, конечно, помогут, но нельзя заранее предугадать, нет ли у них негативных последствий для аккаунта или устройства.

■ **Приложения, скрывающие данные в памяти устройства.** Позволяют скрыть фотографии, видео и другие файлы от стандартных средств просмотра в телефоне. Сам факт использования подобных приложений вызывает вопрос: а что такого может быть на телефоне, что нужно скрывать?

Вирусы и трояны

Для начала дадим два базовых определения.

Компьютерный вирус – это вредоносная программа, написанная специально для причинения вреда программам и устройствам или для криминальной активности. Способна распространяться по Сети и заражать другие устройства.

Троянская программа[9] – это вредоносный агент, проникающий на устройство под видом легитимных программ. Имеет не только заявленную функциональность, но и побочные, нежелательные для пользователя функции: хищение данных, скрытое использование устройства для создания трафика на сайты, рассылки спама и т. п.

> **Пример.** Экранную клавиатуру для Android Ai.type скачали более 40 миллионов раз. Осенью 2019 года оказалось, что это троян, ворующий деньги владельцев смартфонов.
>
> Ai.type – экранная клавиатура с большим количеством смайликов для быстрого набора сообщений. В фоновом режиме открывает рекламные баннеры и накручивает на них клики, одновременно передавая рекламным сетям данные о реальных действиях пользователя. Ai.type без ведома пользователей подписывает их на дорогие сервисы и

[9] Троянская программа, или троян, названа так в честь троянского коня из поэмы Гомера – подарка богам Трои, в котором прятался штурмовой отряд греков.

приобретает от их имени премиальный контент. По оценкам компании Secure-D, в 2019 году с помощью приложения было украдено не менее 18 миллионов долларов.

На заре цифровой эпохи (конец 1980-х годов) первые компьютерные вирусы создавались для развлечения, из хулиганских побуждений. В начале 1990-х годов их было уже много, но они не имели коммерческих целей. Создатели вирусов – начинающие или опытные программисты – в основном стремились к самоутверждению, демонстрации мастерства. При этом, конечно, причиняя реальный вред миллионам пользователей компьютеров.

С тех пор вирусы и троянские программы стали коммерческими инструментами, позволив создать огромную индустрию с оборотом десятки миллиардов долларов в год.

Сейчас в этой развитой индустрии налажено детальное разделение труда: одни пишут конструкторы вирусов, другие генерируют эти вирусы и запускают в Сеть, третьи продают доступ к заражённым компьютерам, четвёртые получают заказы и распространяют спам и установки непрошеных программ и т. д.

С появлением Интернета вирусы обрели свойства сверхпроводимости, а вирусные эпидемии стали захватывать десятки миллионов устройств за считаные дни.

Сегодня в Интернете в сутки появляется несколько десятков тысяч новых вирусов, а в год – до 3–5 миллионов. Типо-

вая схема запуска нового вируса обычно такова: злоумышленник берёт тот или иной готовый генератор вирусов, задаёт ему желаемые параметры, генерирует варианты вируса и сразу проверяет их на установленных на своём сервере антивирусах – «пробьёт» или нет. Как только находится вариант, который «пробивает» большинство популярных антивирусов, вирус запускается в Сеть.

Есть несколько способов получить вирус на компьютер или смартфон.

■ **Открыть электронное письмо с вирусом и тем более открыть файл, приложенный к письму.** Обычно такие письма содержат различные обещания, интересные предложения или другие уловки, называемые *социотехникой*. Поскольку подобные письма вызывают немедленную реакцию антивируса, вирус обычно запакован в архив. Пользователя уговаривают открыть этот архив – и, по сути, самостоятельно запустить установку вируса.

■ **Зайти на заражённый сайт.** Довольно многие сайты в Интернете, особенно нелегального содержания (порно, пиратские видео, музыка или софт), в состоянии установить вирусы на компьютер при открытии веб-страниц.

■ **Установить на своё устройство неизвестное приложение с неизвестного сайта.** С приложением в процессе установки на устройство могут незаметно установиться вирусы, рекламные программы и прочий электронный мусор.

■ **Запустить загрузку MMS**, присланного с неизвестного номера.

Зачем мошенникам нужны вирусы на вашем устройстве? У них есть несколько основных целей.

1. **Кража финансовых данных (а впоследствии и денег).** Украсть номера кредитных карт, пароли к банковским приложениям или счетам мобильного телефона и т. п. с целью кражи денег или совершения покупок от вашего имени.

2. **Навязчивая реклама.** Установить на ваш компьютер или смартфон рекламное программное обеспечение (ПО) (или «адварь» – от английского adware), которое будет показывать вам непрошеную рекламу. Владелец «адвари» будет зарабатывать на продаже этого «рекламного пространства» (то есть вашего внимания) на вашем устройстве.

3. **Кража персональных данных.** Установка на ваш компьютер «невидимого» приложения, которое будет воровать ваши персональные данные о посещениях сайтов, покупках, установленных приложениях, активности в течение дня, перемещениях и перепродавать их рекламщикам, коллекторам, интернет-сервисам и т. п.

4. **Превращение компьютера или телефона в зомби, бота.** Установка программы, которая управляет вашим устройством удалённо. Это нужно для создания так называемых ботнетов – сетей из сотен тысяч или даже миллионов заражённых устройств с центром удалённого управления. Ботнеты используются для рассылки спама, массовых

атак на сайты и т. п. без ведома владельцев инфицированных устройств.

Дистрибуция программного обеспечения

Выше мы уже рассказывали про риски установки незнакомых приложений и программ. Часто такие же риски несёт и установка программ от знакомых брендов.

Крупные интернет-сервисы договариваются с распространителями – файловыми хостингами, каталогами программного обеспечения, а порой и с пиратскими сайтами – о распространении своего ПО (браузеров, поисковиков, почтовых клиентов, игровых и новостных агентов, мессенджеров и т. п.). Это называется *дистрибуцией* интернет-сервисов.

> Дистрибуцией программ, призванных «привязать» пользователя к сервису, занимаются даже такие «белые и пушистые» крупные интернет-компании, как Google, «Яндекс» и Mail.ru. Более того, их доли рынка существенно зависят от энергичности дистрибуции их браузеров, агентов и т. п. Мы не будем обсуждать этичность этой деятельности, интерес интернет-гигантов понятен: они пытаются создать свою замкнутую вселенную, где у пользователя есть всё, от поисковика до кошелька.

Очень многие из этих распространителей «цепляют» к основному продукту, за который заплатил владелец известного бренда, ещё 5–10 программ. Одни из них могут быть без-

вредны или даже полезны (хоть и получены без спроса пользователя); другие же могут оказаться вирусами и троянами.

Относительно честная программа-установщик даже показывает пользователю список этих дополнительных программ с уже проставленными галочками, разрешающими установку. Но так происходит далеко не всегда.

Легальные хозяева основного продукта, с которым «едет» такой неавторизованный «прицеп», официально борются с таким использованием их бренда, но им не всегда удается обнаружить подобное мошенничество и контролировать всю цепочку дистрибуции.

Скрытая или бессознательная установка этих дополнительных программ в лучшем случае заражает компьютер или смартфон непрошеным рекламным ПО, а в худшем случае и вовсе превращает его в часть большого хакерского ботнета.

Проталкивание мошеннического программного обеспечения в составе пакета с легальным ПО от известных брендов – это один из видов так называемой *социальной инженерии*.

From: Maersk Shipping <info@maersk.com>
Sent: Tuesday, November 12, 2019 4:40 AM
Subject: Your Shipping Documents

MAERSK

Original Shipping Documents

Dear Customer,

Please find below attached the bill of lading (BL), Packing List and COA for the new shipment headed to your port as requested by your shipping agent.

Your email address was listed as the consignee/receiver of the goods in transit.

Check the below shipping documents:

Download File

Социальная инженерия: спам, вирусы, фишинг, вымогательство

…Великие специалисты по человеческим душам, профессиональные мошенники, знают превосходно, что существует весьма небольшой процент людей, обладающих иммунитетом к чуду вообще.

Существует также небольшое, но не вымирающее (в полном соответствии с присказкой о мамонте) меньшинство, которое ведётся практически на всё и практически всегда. Трудно сказать, каков этот процент, но мошенники, знатоки душ знают, что их задача всего лишь просеять лохоносный песок масс, чтобы а) намыть себе представителя этого процента и б) застать его в момент, когда у него опять, после предыдущего рывка к чуду, есть немного денег.

Виктор Мараховский, 2020

Мошенничество старо как мир. Но в последние десятилетия не без помощи электронных коммуникаций (телефонов, факсов, Интернета, электронной почты) оно стало особенно изощрённым искусством, использующим так называемую *социальную инженерию*, или *социотехнику*.

Социальная инженерия, или социотехника, – набор приёмов психологической манипуляции, вынуждающих жертву (владельца телефона, банковского счёта, кошелька, маши-

ны и т. п.) сделать то, что нужно мошеннику-манипулятору (открыть вложение к письму, перейти по ссылке, перевести деньги, установить приложение на смартфон).

Социотехникой владеют цыганки на улице, организаторы финансовых пирамид, сектанты, телефонные мошенники, создатели компьютерных вирусов. В основе всей «индустрии азарта» – казино, лотерей, игры на «Форексе», игровых автоматов – огромная и разнообразная социотехника.

Современная социотехника – это смесь психологических трюков с технологическими приёмами.

Мошенники используют так называемые типовые крючки, играя на основных человеческих слабостях: жадности, глупости, тщеславии, стыде и т. п. Социотехника же является инструментом мошенничества и обращается к архетипам пользователя, его привычкам, типовым представлениям и типовым действиям.

> Например, прежде чем заразить компьютер или смартфон, вирус нужно туда доставить и запустить. Доставить можно через электронные письма или мобильные приложения. Но антивирусные программы сейчас довольно легко распознают вирус, так что его нужно скрыть: кибермошенники присылают его электронной почтой в виде вложения в зашифрованном архиве. Пользователя нужно уговорить самостоятельно открыть этот архив, ввести пароль и запустить содержащийся там заражённый файл или программу.
>
> Тут в игру вступает социотехника: например,

заражённый архив или документ в сопровождающем письме преподносят как счёт, платёжку, распоряжение начальника, судебную претензию или результаты вчерашнего совещания, которые обязательно нужно открыть и прочесть.

Ниже приведен пример спамерского письма с предложением загрузить якобы накладную на товар (файл с вирусом). Спамер маскируется под известный бренд компании-экспедитора. Расчёт на то, что адресат или его фирма работает с этой компанией. Обратный адрес, конечно, подставной.

Спам

Если вы пользуетесь электронной почтой, на ваш адрес ежедневно идёт непрерывный поток спама – непрошеной рекламы, писем от вымогателей и так называемых фишеров, писем с вирусами.

Спам – это массовые анонимные непрошеные рассылки электронной почты и SMS. Обычно спам содержит рекламу сомнительных товаров и услуг (дешёвого барахла, порносайтов, новостей мелких СМИ, блогов и т. п.). Но порой спам – это носитель для вирусов или фишинга (о фишинге речь пойдет ниже).

Большую часть спама (до 90–99 %) ещё на «подлёте» к вашему почтовому ящику уничтожают спам-фильтры и антивирусы, которые установлены сейчас на всех публичных поч-

товых сервисах (Mail.ru, «Яндекс», Gmail и т. п.), так что вы его не видите. Но часть таких писем время от времени прорывается к вам во «Входящие».

Практически все непрошеные рассылки сейчас основаны на развитой социотехнике в том или ином виде.

Вот что нужно как минимум понимать про спам.

■ **Социотехника спама.** Обычно в теме спамерского письма пишут что-то стандартное, чтобы вы приняли рассылку за сообщение от знакомого или коллеги. Часто и текст письма «мимикрирует» под личную или деловую переписку. Наиболее распространённая цель социотехники – заставить вас перейти по ссылке в теле письма на сайт с товаром или услугой. Однако спамерское письмо может содержать и средства слежки за получателем.

■ **Слежка.** Спамерское письмо иногда содержит незаметную картинку размером 1 × 1 пиксел, которая служит для определения того, дошло ли письмо до получателя, то есть до вас, и для сбора данных о вас.

Эта картинка подгружается со стороннего сайта. Если ваш почтовый клиент автоматически скачивает картинки, вставленные в письма, он незаметно скачает и этот шпионский «пиксел» с сайта спамеров. Таким образом спамеры узнают, что ваш адрес реальный, «живой», письма читаются. Они также получат информацию о факте и времени прочтения письма, IP-адрес вашего устройства, данные о почтовом кли-

енте, в котором вы открыли письмо и скачали картинку[10].

■ **Поддельный обратный адрес.** Нужно понимать, что обратный адрес письма очень легко подделать (это делается автоматически по большим спискам краденых настоящих адресов), поэтому «красивый» и «надёжный» адрес отправителя в спаме – это просто часть социотехники.

■ **Ссылка «Отписаться».** Спамерские письма часто содержат предложение отписаться от их рассылки, для чего предлагают перейти по ссылке с соответствующим текстом (как правило, в конце письма).

Обычно это делается для того, чтобы понять, «живой» ваш адрес или нет, ведь спамеры запускают рассылку по огромным спискам адресов, собранным за многие годы, среди которых много давно брошенных.

Кроме того, переход по такой ссылке сообщает спамеру множество дополнительных данных о вас и вашем устройстве (как в случае со шпионским «пикселом»). Поэтому «отписываться» ни в коем случае нельзя.

■ **Папка «Спам».** Почтовый клиент на компьютере обычно имеет встроенный фильтр спама и соответствующую папку «Спам» для отфильтрованных писем с подозрительным содержимым. Иногда в этой папке оказываются и нормальные письма от настоящих отправителей, но это сейчас довольно редкий случай. Нужно помнить, что большинство

[10] Эти данные о вас спамеры смогут потом использовать, например для того чтобы рассылать письма от вашего имени вашим коллегам и знакомым.

писем в папке «Спам» опасны. Не открывайте их, не переходите по ссылкам и не загружайте картинки, если не хотите «поймать» вирус или троян.

В разделе «Что делать и чего не делать? Простые правила кибергигиены» далее в этой главе мы подробнее поговорим о гигиене электронной почты.

Фишинг

Одной из разновидностей мошенничества с помощью социотехники является *фишинг*. Фишинг (от английского fishing – «рыбная ловля») – это разнообразные приёмы выуживания у пользователя его паролей и логинов для доступа к счетам, номеров кредитных карт и другой финансовой информации. Цель фишинга очевидна: в первую очередь это кража денег с кредитной карты, банковского счёта или счёта мобильного телефона.

Фишинг в формате «нигерийского письма» или писем счастья – очень старое явление, просто раньше такой спам распространялся по обычной почте, в конвертах. Электронному фишингу уже 20–25 лет, и за это время он приобрёл самые разнообразные формы.

Нигерийцы, юристы и прочие мошенники

Надоело, что тебя считают лохом? Надоели разводки?

Включайся в нашу акцию «Нет разводкам»!
Отправь SMS на короткий номер 2277 с текстом НЕ ЛОХ.
Чем больше SMS – тем больше ты не лох!

На электронную почту (а сейчас уже и через SMS, MMS, в мессенджеры) постоянно идёт мощный поток писем от мошенников, которые хотят втянуть адресата в тот или иной сложный и детально проработанный сценарий отъёма денег.

Деньги с неба. Самый распространённый крючок – внезапное предложение заработать много денег. Эта схема, известная как «Афера-419», существует уже минимум 30 лет (со времён бумажной почты). У неё есть множество вариантов, например:

> «Вам пишет бывший бухгалтер Саддама Хусейна, у меня есть доступ к сокрытым им 50 миллионам долларов, мне нужен надёжный и честный партнёр, чтобы получить эти деньги в вашей стране за комиссию 20 %».

Замечательно, кстати, что этот адресант хочет найти *честного* партнёра для кражи и обналичивания чужих денег. На самом деле ему, конечно, нужен не очень честный, но зато жадный и доверчивый человек, которого можно будет втянуть в многоступенчатый сценарий открытия счёта «для перевода денег», занесения туда небольшой суммы «для подтверждения», передачи реквизитов и паролей мошенникам «для осуществления перевода» и т. п. Деньги, естественно,

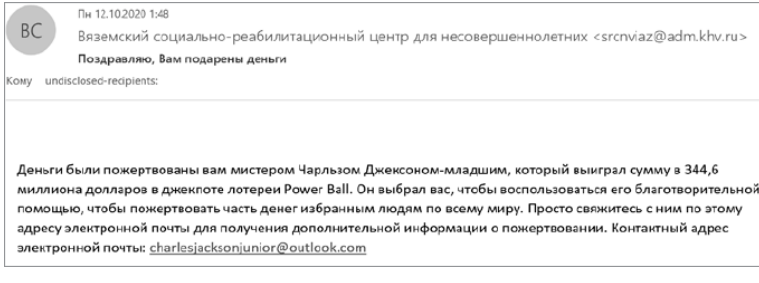
потом исчезают, как и «бухгалтер».

Вот ещё пример свежей разводки от некоей Ann Johnson:

> I'm diagnosed with end-stage cancer, I've got a charity proposition I want to put in your care by entrusting you with my fund. Respond if interested, so I know you got this.
>
> («У меня диагностировали рак в последней стадии, у меня есть к вам предложение организовать благотворительный фонд под вашим управлением, куда я переведу мои средства. Ответьте, чтобы я знала, что вы это получили».)

Дальше, очевидно, при ответе на письмо включится обычный для этого сложный сценарий выманивания маленькой суммы под обещание дать большую. Крючок жадности – самый популярный.

Вот ещё образец письма про «благотворительность» от американского дядюшки:


Пн 12.10.2020 1:48

ВС Вяземский социально-реабилитационный центр для несовершеннолетних <srcnviaz@adm.khv.ru>

Поздравляю, Вам подарены деньги

Кому undisclosed-recipients:

Деньги были пожертвованы вам мистером Чарльзом Джексоном-младшим, который выиграл сумму в 344,6 миллиона долларов в джекпоте лотереи Power Ball. Он выбрал вас, чтобы воспользоваться его благотворительной помощью, чтобы пожертвовать часть денег избранным людям по всему миру. Просто свяжитесь с ним по этому адресу электронной почты для получения дополнительной информации о пожертвовании. Контактный адрес электронной почты: charlesjacksonjunior@outlook.com

Деньги для пенсионеров. С недавних пор очень попу-

лярны письма от «юристов», рассчитанные на пенсионеров, с сообщением о том, что в последние годы им неверно начисляли пенсию, и обещаниями её пересчитать и вернуть десятки тысяч рублей.

Пенсионер старательно собирает документы и пересылает их «юристам». Потом, естественно, нужно платить «юристам» за эту работу, причём они собирают деньги несколько раз: сначала «за перерасчёт пенсии», чтобы начисления впредь были больше; потом, когда доверчивый пенсионер спрашивает, когда же наконец произойдёт перерасчёт, – ещё раз за перерасчёт за три предыдущих года с получением не выплаченных якобы десятков тысяч рублей (этот крючок возможности получения «живых» денег отвлекает пенсионера от вопросов по поводу предыдущих обещаний относительно перерасчёта) и т. д.

> Например, осенью 2020 года мошенники заманивали пенсионеров с помощью фейкового ролика, смонтированного из фрагментов заседания правительства, в том числе выступлений глав Министерства труда и соцзащиты, Министерства цифрового развития, а также Федеральной налоговой службы.
>
> Начинался ролик как выпуск новостей, а заканчивался «пошаговой инструкцией» того, как граждане могут получить якобы причитающиеся им выплаты от государства.
>
> В комментариях к ролику была вставлена ссылка

на сайт – якобы страницу Госуслуг, где пользователя просили ввести личные данные и номер банковской карты: так мошенники получали данные карт. Кроме того, пользователя могли попросить внести небольшую сумму на оплату услуг юриста. Естественно, никакого перерасчёта или возврата денег не предполагалось.

Основной признак этих схем – обещание нежданно-негаданно свалившихся денег и сложный сценарий общения, требующий от наивного получателя выполнения разных действий. Часто мошенник даже не заморачивается объяснением, зачем он вообще помогает пенсионеру восстановить справедливость, а тому и в голову не приходит спросить об этом!

Чудо-лекарства. Ещё один крючок для пожилых людей и хронических больных – обещание суперлекарств и БАДов от хронических болезней: радикулита, диабета, катаракты и др.

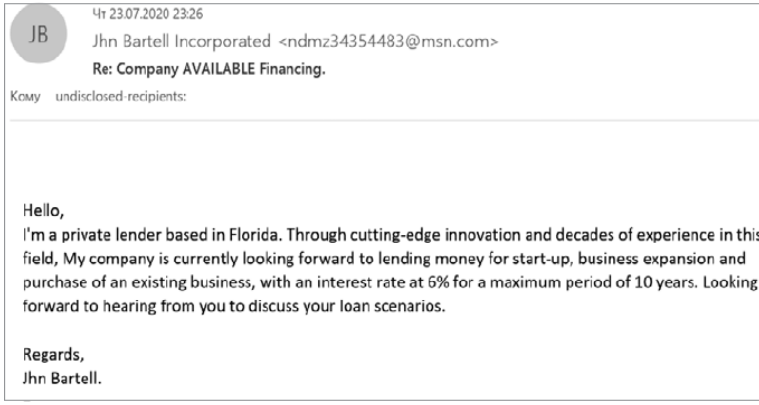
Обычный способ мошенников «выключить» рациональное мышление – создание искусственного цейтнота, спешки (требование заплатить как можно скорее, потому что *только сегодня в течение 2 часов* предлагаются невероятные скидки). В лучшем случае мошенники продают плацебо втридорога, в худшем – просто пропадают с деньгами.

Супермодные товары. Жертвами становятся не только пенсионеры – молодёжь часто ловят на обещание доставить новейшие гаджеты и аксессуары; после сессии «личного» об-

щения в мессенджере или по почте и перевода денег «продавец» исчезает.

Средства для снижения веса также отлично работают как крючок, потому что желающие похудеть всегда ищут чудо-таблетку и ждут волшебных обещаний стройности без диет и упражнений. Бывает, конечно, что за большие деньги продают и действительно доставляют какую-нибудь дрянь, но чаще «продавцы» просто пропадают с деньгами.

«Инвестиции». В последнее время популярны предложения о финансировании от «венчурных инвесторов», предлагающих вложить деньги в стартап. Часто уши мошенника торчат из таких предложений довольно явственно (неизвестная фирма, почтовый адрес, зарегистрированный на бесплатном почтовом сервисе, скрыт список получателей, есть опечатки и т. п.).



Чт 23.07.2020 23:26

JB

Jhn Bartell Incorporated <ndmz34354483@msn.com>

Re: Company AVAILABLE Financing.

Кому undisclosed-recipients:

Hello,
I'm a private lender based in Florida. Through cutting-edge innovation and decades of experience in this field, My company is currently looking forward to lending money for start-up, business expansion and purchase of an existing business, with an interest rate at 6% for a maximum period of 10 years. Looking forward to hearing from you to discuss your loan scenarios.

Regards,
Jhn Bartell.

В общем, распознать мошенников довольно легко, если быть внимательным и помнить, что деньги с неба не падают.

Платные опросы, конкурсы и «выигрыши»

На жадину не нужен нож,
ему покажешь медный грош —
и делай с ним что хошь.

На пользователей Сети лавиной валятся сообщения о деньгах с неба: социальных выплатах от вымышленных фондов, беспроигрышных лотереях от крупных компаний, конкурсах с большими призами.

Это большой бизнес. В Сети создаются и работают тысячи мошеннических сайтов с платными опросами и конкурсами. Компании, занимающиеся аналитическими исследованиями в области информационной безопасности, оценивают потери пользователей от фальшивых опросов в миллиарды рублей [11].

[11] По данным «Лаборатории Касперского». https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-v-2020-godu-zloumishlenniki-aktivno-ispolzuyut-temu-oprosov-v-skam-shemah.

Мошенники зазывают пройти опрос сообщениями в соцсетях, мессенджерах, чатах и на форумах. Ссылки на опросы и конкурсы также активно рассылают спамом по электронной почте и SMS.

Злоумышленники обещают хорошее вознаграждение за прохождение опроса – десятки, а иногда и сотни тысяч рублей. Но сначала нужно заплатить небольшую «комиссию», как правило 200–300 рублей. Потом, конечно, никакого вознаграждения за опрос не платится, а деньги не возвращаются. Иногда при оплате похищаются данные кредитных карт пользователей, с которых они платили эту «комиссию».

> Популярность именно мошеннических опросов объясняется сравнительно низкими затратами на создание, публикацию и рекламу страницы «опроса». Кроме того, при небольших суммах нанесённого ущерба (до 5000 рублей) это мошенничество квалифицируется как административное правонарушение, которое карается лишь штрафом, так что правоохранителям неинтересно заниматься такими делами. На то, чтобы по странице

в Сети вычислить и поймать мошенника, укравшего у пользователя 300 рублей, у полиции часто нет ни времени, ни ресурсов, ни желания.

Это классический крючок – поманить большими деньгами, попросив скромную сумму ниже порога «импульсного платежа».

«Как это работает: пользователь получает сообщение, в котором обещают крупное вознаграждение за прохождение опроса, например о качестве предоставляемых известной компанией услуг. Но для получения денег есть условие: нужно заплатить комиссию или закрепительный платеж порядка 300 рублей. В итоге выплату человек не получает, а комиссия достается мошенникам.

Есть и более изощрённый вариант. В соцсетях якобы крупный производитель, например, косметики просит ответить на несколько вопросов. Взамен пользователю обещают либо ценный приз, либо деньги – довольно крупные, до 200 тысяч рублей. Как правило, рекламирует акцию якобы известная медийная личность, и многие доверчивые граждане этому верят. После опроса пользователя также просят заплатить комиссию.

После перечисления денег предлагают сделать ещё один, последний платёж (причину задержки, как правило, приводят убедительную). Затем история повторяется снова и снова – до тех пор, пока человек не

остановится»[12].

Вымогательство

Кроме различных вариантов социотехники, втягивающей пользователя в сложные сценарии, основанные на его желании получить много денег, существуют разнообразные схемы вымогательства с запугиванием, где крючком служит страх.

Наиболее показательный пример последних лет – письмо от «хакера», который якобы взломал ваш компьютер.

Я видел, как ты скачивал порно!

Довольно известный современный пример вымогательства – электронное письмо от «хакера» примерно следующего содержания:

«Это твой пароль – XXXXXXX, верно? Откуда я его знаю? Я установил на твой компьютер шпионскую

[12] За спрос деньги берут: число мошеннических опросов выросло в 2,6 раза // Известия, 2020. – 18 октября [Электронный ресурс]. – Режим доступа: https://https://iz.ru/1074245/anastasiia-gavriliuk/za-spros-dengi-berut-chislo-moshennicheskikh-oprosov-vyroslo-v-26-raza.

программу и знаю и вижу через камеру всё, что ты делаешь. Я записал, как ты просматривал очень нехорошее порно! Если не хочешь, чтобы я опубликовал видео с этим порно и твоим лицом (хе-хе-хе) во время его просмотра, перечисли столько-то биткоинов/ долларов/рублей на такой-то кошелёк».

Конец ознакомительного фрагмента.