**BIG DATA и Всеобщий контроль**

Оглавление

[Как Big Data и пара ученых обеспечили победу Трампу и Brexit 2](#_Toc3127351)

[Android-приложения тотально следят за пользователями 9](#_Toc3127352)

[Как смартфоны следят за нами 9](#_Toc3127353)

[Опасности технического прогресса 11](#_Toc3127354)

[В сети обнаружена крупнейшая база адресов и паролей электронной почты 11](#_Toc3127355)

[Что знает о нас Telegram 12](#_Toc3127356)

[Яндекс знает о нас всё 19](#_Toc3127357)

[Как защитить данные бизнеса по цене кофе в офисе 27](#_Toc3127358)

[«За нами следят»: что знают о пользователях интернет-компании и сколько стоит такое знание 30](#_Toc3127359)

[Как за нами следят наши гаджеты 32](#_Toc3127360)

[«Лаборатория Касперского» рассказала об уязвимости 60 компьютеров в автомобиле 36](#_Toc3127361)

[Интернет вещей оказался под ударом 36](#_Toc3127362)

[Восемь угроз: чем опасны Facebook, Google, Amazon и Apple 38](#_Toc3127363)

[За нами следят 43](#_Toc3127364)

[Взлом смартфонов 46](#_Toc3127365)

[Эксперт по ИТ-безопасности Игорь Ашманов: заклейте камеру телефона! 46](#_Toc3127366)

[Присмотритесь к кофеварке. Возможно, именно сейчас она передает хакерам ваши личные данные 48](#_Toc3127367)

[Большие данные как большие риски 52](#_Toc3127368)

[Государство отказалось нести ответственность за утечку персональных данных россиян 60](#_Toc3127369)

[ОС Ubuntu будет следить за пользователями 61](#_Toc3127370)

[Конец приватности 61](#_Toc3127371)

[«За нами следят»: что знают о пользователях интернет-компании и сколько стоит такое знание 64](#_Toc3127372)

[Всевидящее око по-китайски 66](#_Toc3127373)

[Приватность в сети: вы даже не знаете, насколько вы уязвимы 69](#_Toc3127374)

[Названы самые масштабные утечки 2017 года 72](#_Toc3127375)

[Цифровые души. Сколько стоят ваши персональные данные 74](#_Toc3127376)

[Тотальная слежка Google 76](#_Toc3127377)

[За нами следят. FinFisher шпионит за пользователями семи стран 77](#_Toc3127378)

[Банки тоже следят 78](#_Toc3127379)

[Из-за технологий исчезло слово "граммофон". Следующее — слово "свобода" 78](#_Toc3127380)

[Рот не на замке: где границы информационной открытости 80](#_Toc3127381)

[Смартфон в доспехах. Как защититься от слежки на 100% 82](#_Toc3127382)

[Наука поняла, как взломать человеческий организм 84](#_Toc3127383)

[**Вернуться в каталог сборников по менеджменту**](http://учебники.информ2000.рф/management2/management3.shtml)

[**Вернуться в электронную библиотеку по экономике, праву и экологии**](http://учебники.информ2000.рф/index.shtml)

[**НАПИСАНИЕ на ЗАКАЗ: дипломы и диссертации, курсовые и рефераты. Переводы с языков, он-лайн-консультации. Все отрасли знаний**](http://учебники.информ2000.рф/napisat-diplom.shtml)

# Как Big Data и пара ученых обеспечили победу Трампу и Brexit

*By*[*The Insider*](http://theins.ru/author/the-insider)[***@the\_ins\_ru***](http://twitter.com/the_ins_ru)*· On 06.12.2016*

*В субботу швейцарский журнал Das Magazin опубликовал*[***расследование***](https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/)*о том, как технологии персонализированной рекламы в сети Facebook повлияли на итоги выборов в США и референдума о выходе Великобритании из ЕС. Как*[***отмечает***](http://www.spiegel.de/netzwelt/netzpolitik/donald-trump-und-die-daten-ingenieure-endlich-eine-erklaerung-mit-der-alles-sinn-ergibt-a-1124439.html#spRedirectedFrom=www&referrrer=https://t.co/XLkO9egVVe)*немецкий Spiegel, многие журналисты уже стали называть расследование «текстом года». В нем есть все: и новейшие технологии; и универсальное оружие, которое попало из хороших рук в плохие; и ежедневная слежка за каждым из нас; и таинственные заказчики; и превращение из нищего в принца (и наоборот). The Insider публикует полный перевод текста с немецкого языка.*

В половине девятого утра 9 ноября Михал Козинский проснулся в цюрихском отеле Sunnehus. 34-летний ученый приехал, чтобы выступить в Федеральной высшей технической школе (ETH) с докладом на конференции об опасности Big Data и так называемой «цифровой революции». С подобными лекциями Козинский разъезжает по всему миру, ведь он является ведущим экспертом в психометрии — разделе психологии, основанном на анализе данных. Включив тем утром телевизор он понял: бомба разорвалась. Дональд Трамп избран президентом США, несмотря на все прогнозы социологов.

Козинский долго смотрит новости о триумфе Трампа, о результатах голосования по разным штатам. Он подозревает, что произошедшее как-то связано с его научными разработками. Козинский вздыхает и выключает телевизор.

В тот же день доселе малоизвестная лондонская фирма рассылает пресс-релиз следующего содержания: «Мы поражены тем, что наш революционный подход к основанным на данных коммуникациям внес такой существенный вклад в победу Дональда Трампа». Пресс-релиз подписан неким Александром Джеймсом Эшбернером Никсом. Ему 41 год, он британец и возглавляет компанию Cambridge Analytica. Никс всегда носит костюм, модные роговые очки, а свои светлые волнистые волосы обычно зачесывает назад.

Задумчивый Козинский, прилизанный Никс и широко улыбающийся Трамп — первый сделал цифровую революцию возможной, второй осуществил ее, последний стал благодаря ей победителем.

**Насколько опасна Big Data?**

Сейчас каждый, кто не жил на Луне последние пять лет, знаком с термином Big Data. Этот термин значит и то, что все, что мы делаем — в интернете или «офлайн» — оставляет цифровой след. Покупка по кредитке, запрос в Google, прогулка со смартфоном в кармане, каждый лайк в соцсети: все это сохраняется. Долгое время никто не мог понять, для чего хорошего могли бы пригодиться эти данные — кроме тех случаев, когда в ленте Facebook всплывает реклама средств от гипертонии, потому что недавно мы искали в Google «как понизить давление». Непонятно было и то, чем же является Big Data для человечества — большой опасностью или большим достижением? Но с 9 ноября мы знаем на это ответ. Ведь и за предвыборной кампанией Трампа в интернете, и за кампанией в поддержку Brexit стоит одна и та же компания, исследующая Big Data: Cambridge Analytica и ее директор Александр Никс. Тот, кто хочет понять природу этих голосований (и природу того, что ожидает Европу в ближайшие месяцы), должен начать с примечательного события, произошедшего в 2014 году в британском Кембриджском университете. А именно, на кафедре психометрии Козинского.

Психометрия, которую иногда зовут психографией, представляет собой попытку измерить человеческую личность. В современной психологии стандартом является так называемый «метод океана» (по буквам OCEAN, анаграмму пяти измерений на английском языке). В 1980-е годы два психолога доказали, что каждая черта характера может быть измерена при помощи пяти измерений. Это так называемая «большая пятерка»: открытость (насколько вы готовы к новому), добросовестность (насколько вы перфекционист), экстраверсия (как вы относитесь к социуму), доброжелательность (насколько вы дружелюбны и готовы к сотрудничеству) и нейротизм (насколько легко вас вывести из себя) На основе этих измерений можно точно понимать, с каким человеком имеешь дело, в чем его желания и страхи, наконец, как он себя может вести. Проблема была в сборе данных: чтобы что-то понять о человеке, от него требовалось заполнить огромный опросник. Но потом появился интернет, затем Facebook, затем Козинский.

В 2008 году студент из Варшавы Михал Козинский начал новую жизнь: он поступил в престижный английский Кембридж, в Центр психометрии, лабораторию Кэвендиш, самую первую лабораторию по психометрии в мире. Со своими однокурсниками он придумал и запустил приложение для Facebook под названием MyPersonality. Пользователю предлагалось ответить на огромный список вопросов («легко ли вас вывести из себя в состоянии стресса? Есть ли у вас склонность критиковать окружающих?»), получив затем свой «профиль личности», а создатели приложения получали бесценные личные данные. Вместо ожидавшихся данных по дюжине однокурсников создатели получили информацию по сотням, тысячам, а затем и миллионам людей. Два докторанта собрали тем самым крупнейший «урожай» данных в истории психологических исследований.

Процесс, который Козинский сотоварищи разработал за последующие несколько лет, достаточно прост. Во-первых, тестируемый получает список вопросов, онлайн-тест. Из ответов на него ученые вычисляют личные ценности испытуемого. Далее, Козинский с командой изучают действия испытуемого: лайки и репосты в Facebook, а также его пол, возраст и место жительства. Так исследователи получают связи. Из простого анализа данных в сети могут получится необычные выводы. Например, если мужчина подписан на страничку бренда косметики MAC, он с высокой вероятностью является геем. Наоборот, сильный показатель гетеросексуальности — если человек поставил лайк хип-хоп группе Wu-Tang Clan из Нью-Йорка. Поклонник Леди Гаги с высокой долей вероятности экстраверт, а человек, ставящий «нравится» философским постам — интроверт.

Анализа 68 лайков в Facebook достаточно, чтобы определить цвет кожи испытуемого (с 95% вероятностью), его гомосексуальность (88% вероятности) и приверженность Демократической или Республиканской партии

Козинский и его коллеги беспрестанно совершенствовали свою модель. В 2012 году Козинский доказал, что анализа 68 лайков в Facebook достаточно, чтобы определить цвет кожи испытуемого (с 95% вероятностью), его гомосексуальность (88% вероятности) и приверженность Демократической или Республиканской партии США (85% вероятности). Но процесс идет дальше: интеллектуальное развитие, религиозные предпочтения, пристрастие к алкоголю, курению или наркотикам. Данные даже позволяли узнать, развелись ли родители испытуемого до его совершеннолетия или нет. Модель оказалась настолько хороша, что стало возможным предугадывать ответы испытуемого на определенные вопросы. Опьяненный успехом, Козинский продолжал: скоро модель смогла лучше узнавать личность после десяти изученных лайков, нежели его коллеги по работе. После 70 лайков — лучше, чем друг. После 150 лайков — лучше, чем родители. После 300 лайков — лучше, чем партнер. С еще большим количеством изученных действий можно было бы узнать о человеке лучше, чем он сам. В день, когда Козинский опубликовал статью о своей модели, он получил два звонка: жалобу и предложение работы. Оба звонка были из компании Facebook.

**Только для друзей**

Теперь на Facebook можно отмечать свои посты как открытые и приватные, «подзамочные»: во втором случае просматривать их могут лишь определенный круг друзей. Но для сборщиков данных и это не проблема. Если Козинский всегда запрашивал соглашения пользователей Facebook, современные тесты требуют доступа к персональным данным как обязательного условия для их прохождения.

Но речь не только об отметках «нравится» в Facebook: Козинский и команда могут оценивать людей по Большой пятерке критериев исходя из их юзерпика, фотографии в соцсетях. Или даже по числе друзей: хороший показатель экстраверсии! Но мы также сдаем личные данные, когда находимся не в сети. Датчик движения в смартфоне показывает, размахиваем ли мы рукой с ним, как далеко ездим (коррелирует с эмоциональной нестабильностью). Как замечает Козинский, смартфон — это огромный психологический опросник, который мы вольно или невольно заполняем. Что особенно важно, это работает и в обратную сторону: можно не только создавать из данных психологический портрет, вы можете искать среди этих портретов нужные. Например, обеспокоенные папаши, озлобленные интроверты, не определившиеся с выбором сторонники демократов. По сути, Козинский изобрел поисковую систему по людям.

Все явственнее Козинский понимал и потенциал, и опасность своей работы.

Всемирная сеть для него всегда казалась даром небес. Всегда хочется «вернуться», «поделиться». Это дух нового поколения, начало новой эпохи без физических границ. Но что случится, думал Козинский, если кто-то решит воспользоваться этой поисковой системой по людям, чтобы ими манипулировать? Он начинает ставить предупреждения на всех своих научных публикациях. Предупреждения о том, что его методы «могут нести угрозу благополучию, свободе или даже жизни людей». Но никто, кажется, не понимал, к чему он ведет.

Примерно в это время, в начале 2014 года, к Козинскому обратился молодой ассистент профессора по имени Александр Коган. У него был запрос от некой фирмы, заинтересованной в методе Козинского. Предложение состояло в том, чтобы проанализировать путем психометрии 10 млн американских пользователей Facebook. С какой целью, собеседник не сказал из соображений конфиденциальности. Козинский сначала согласился, ведь речь идет о больших суммах в пользу его института, но потом начал медлить с согласием. В итоге, он выжал из Когана название фирмы: SCL, [**Strategic Communications Laboratories**](https://sclgroup.cc/) («Лаборатории стратегических коммуникаций»). Козинский погуглил название компании. «Мы являемся глобальной компанией по управлению предвыборными кампаниями», — гласил сайт фирмы, предлагая маркетинг на основе психологии и логики. Фокус на влиянии на исход выборов. Козинский недоуменно щелкал по страничкам сайта, раздумывая, чем же может заниматься эта фирма в США.

*Александр Коган*

Чего Козинский на тот момент еще не знал: за SCL стоит сложная корпоративная система, завязанная на «налоговых гаванях»: позднее это было показано в «Панамских документах» и разоблачениях Wikileaks. Часть этой системы ответственна за кризисы в развивающихся странах, другая помогала НАТО разрабатывать методы психологической манипуляции гражданами Афганистана. Одна из дочерних компаний SCL — та самая Cambridge Analytica, зловещая маленькая компания, организовавшая интернет-кампании в поддержку Brexit и Трампа.

Козинский ничего об этом не знает, но подозревает неладное. Проводив изучение, он узнал, что Александр Коган создал тайную компанию, которая ведет дела с SCL. Из документа, который есть в распоряжении Das Magazin, следует, что SCL получила данные о методе Козинского именно из рук Когана. Внезапно Козинского осенило, что Коган мог скопировать или выстроить заново его систему, чтобы затем продать ее политтехнологам из SCL. Ученый незамедлительно разрывает связь с Коганом и информирует о ситуации своего институтского начальника. Внутри института зреет конфликт, учреждение опасается за свою репутацию. Коган переехал в Сингапур, женился и начал именовать себя доктором Спектром. Козинский переехал в Штаты, начав работать в Стэнфорде.

Больше года все идет спокойно, но в ноябре 2015 года лидер радикальных сторонников Brexit Найджел Фарадж [**объявил**](http://www.express.co.uk/news/politics/620409/nigel-farage-people-want-britain-quit-EU), что его сайт подключает к работе со своей интернет-кампанией некую компанию, специализирующуюся на Big Data, а именно, Cambridge Analytica. Ключевая компетенция фирмы: политический маркетинг нового типа — так называемый «микротаргетинг» — основанный на «методе океана».

Козинский начинает получать множество писем — учитывая слова «Кембридж», «океан» и «аналитика», многие думают, что он как-то с этим связан. Однако только тогда он сам узнает о существовании такой компании. С ужасом он просматривает сайт фирмы. Кошмар стал былью: его методология используется в большой политической игре.

В июле 2016 году, уже после референдума по Brexit, на его голову начинают обрушиваться проклятия. Дескать, посмотрите, что вы сделали! Каждый раз Козинскому приходится оправдываться и доказывать, что к той фирме он не имеет никакого отношения.

**Вначале Brexit, затем Трамп**

Прошло десять месяцев. На календаре 19 сентября 2016 года, избирательная кампания в США в самом разгаре. Зал нью-йоркского отеля Grand Hyatt, выполненный в темно-синих тонах, наполняют гитарные риффы: играет песня Bad Moon Rising группы Creedence Clearwater Revival. Проходит ежегодный саммит Concordia, мировой экономический форум в миниатюре. Приглашены сильные мира сего, даже действующий президент Швейцарии Йоханн Шнайдер-Амманн. «Прошу приветствовать Александра Никса, директора Cambridge Analytica», — раздается приятный женский голос. На сцену поднимается долговязый мужчина в темном костюме. В зале царит тишина. Многие уже знают, что перед ними новый digital-специалист Трампа. «Скоро вы будете называть меня Мистер Brexit», — таинственно написал Трамп в своем Twitter несколькими неделями ранее. Действительно, политологи уже писали тогда о сходстве программ у Трампа и у сторонников выхода Великобритании из ЕС. И лишь немногие знали о связи Трампа с малоизвестной Cambridge Analytica.

*Директор Cambridge Analytica Александр Никс*

До тех пор digital-кампания Трампа состояла более-менее из одного человека: Брэда Парскейла. Маркетинговый энтузиаст и основатель одного провалившегося стартапа, он создал для Трампа простенький веб-сайт за $1500. 70-летнего Трампа едва ли можно назвать человеком цифровой эпохи: на его рабочем столе даже компьютера нет. Как однажды поведала его персональная ассистентка, нет даже такого явления, как электронное письмо от Трампа. Сама ассистентка приучила его к смартфону — с которого он с тех пор льет потоки мыслей в Twitter.

Хиллари Клинтон, напротив, опиралась на наследие Барака Обамы как первого «президента соцсетей». У нее были адресные листы Демократической партии, миллионы подписчиков, поддержка Google и Dreamworks. Когда в июне 2016 года Трамп нанял Cambridge Analytica, многие в Вашингтоне скорчили мину. Иностранные чуваки в костюмах, которые ничего в этой стране не понимают? Серьезно?

«Это честь для меня, уважаемые дамы и господа, рассказывать вам сейчас о силе Big Data и психометрии в избирательной кампании», — говорил на саммите Никс. За его спиной в тот момент появился слайд с логотипом его фирмы: изображение мозга, составленное из сетей, подобно карте. «Еще пару месяцев назад Тед Круз был одним из наименее одобряемых кандидатов, — говорил блондин с английским акцентом, да таким, что присутствовавшие американцы ощущали себя подобно швейцарцам, которые слышат литературный немецкий. — Всего 40% электората знали его имя». Все присутствовавшие помнили историю стремительного взлета сенатора-консерватора Круза, едва ли не самое необъяснимое событие предвыборной гонки. Последний из серьезных оппонентов Трампа внутри Республиканской партии буквально выскочил из ниоткуда. «Ну и как же так произошло?» — вопрошал Никс. В конце 2014 года Cambridge Analytica вошла в предвыборную кампанию в США именно как советник Теда Круза, которого финансировал миллиардер Роберт Мерсер. До тех пор, утверждал Никс, предвыборные кампании велись по демографическим критериям: «Глупейшая идея, если всерьез об этом подумать: все женщины получают одинаковый месседж, потому что они одного пола, все афроамериканцы получают другой посыл, исходя из их расы». Таким дилетантским способом (и тут даже Никсу можно ничего не добавлять) вела кампанию команда Клинтон: разделить общество на формально гомогенные группы, подсказанные социологами. Теми самыми, что до самого конца отдавали ей победу.

*Cambridge Analytica утверждает, что Тед Круз обязан ей своим успехом*

И тут Никс щелкает на другой слайд: пять лиц, каждое соответствует определенному профилю личности, Большая пятерка измерений. «Мы в Cambridge Analytica разработали модель, которая позволит высчитать личность каждого совершеннолетнего гражданина США», — продолжает Никс. В зале полная тишина. Маркетинговый успех Cambridge Analytica основан на трех китах. Это психологический поведенческий анализ, основанный на «модели океана», изучение Big Data и таргетированная реклама. Последнее означает персонализированную рекламу, а также такую рекламу, которая максимально близко подстраивается под характер отдельного потребителя.

Никс искренне объясняет, как его компания этим занимается (лекция [**доступна**](https://www.youtube.com/watch?v=n8Dd5aVXLCc) на YouTube). Его фирма закупает персональные данные из всех возможных источников: кадастровые списки, бонусные программы, телефонные справочники, клубные карты, газетные подписки, медицинские данные. В США возможно купить почти любые персональные данные. Если вы хотите узнать, допустим, где живут женщины-еврейки, можно спокойно купить базу данных. Затем Cambridge Analytica скрещивает эти данные со списками зарегистрированных сторонников Республиканской партии и данными по лайкам-репостам в Facebook — вот и получается личный профиль по «методу океана». Из цифровых данных вдруг возникают люди со страхами, стремлениями и интересами — и с адресами проживания.

Процедура идентична разработанной Козинским модели. Cambridge Analytica также использует IQ-тесты и прочие небольшие приложения, чтобы получать осмысленные лайки от пользователей Facebook. И компания Никса делает то, от чего предостерегал Козинский: «У нас есть психограммы всех совершеннолетних американцев, это 220 млн человек. Наш контрольный центр выглядит так, прошу внимания», — говорит Никс, щелкая слайды. Появляется карта Айовы, где Тед Круз [**собрал**](http://www.rbc.ru/politics/02/02/2016/56b027f79a7947cace0ad867) неожиданно большое число голосов на праймериз. На карте видны сотни тысяч маленьких точек: красные и синие, по партийным цветам. Никс выстраивает критерии. Республиканцы — и синие точки исчезают. Еще не определились с выбором — точек становится меньше. Мужчины — еще меньше, и так далее. В итоге, появляется имя одного человека: с возрастом, адресом, интересами, политическими предпочтениями. Но как Cambridge Analytica обрабатывает отдельных людей своим месседжем?

В другой презентации Никс рассказал, как на примере закона о свободном распространении оружия: «Для боязливых людей с высоким уровнем нейротизма мы представляем оружие как источник безопасности. Вот, на левой картинке изображена рука взломщика, который разбивает окно. А на правой картинке мы видим мужчину с сыном, которые идут по полю с винтовками навстречу закату. Очевидно, утиная охота. Эта картинка для богатых консерваторов-экстравертов».

**Как удержать электорат Клинтон от голосования**

Противоречивая натура Трампа, его беспринципность и исходящая из этого целая прорва различных сообщений внезапно сыграла ему на руку: для каждого отдельного избирателя свой месседж. «Трамп действует как идеальный оппортунистский алгоритм, который опирается лишь на реакцию публики», — отмечала в августе математик Кэти О’Нил. В день третьих дебатов между Трампом и Клинтон команда Трампа отправила в соцсети (преимущественно, Facebook) свыше 175 тыс. различных вариаций посланий. Они различались лишь в мельчайших деталях, чтобы максимально точно психологически подстроиться под конкретных получателей информации: заголовки и подзаголовки, фоновые цвета, использование фото или видео в посте. Филигранность исполнения позволяет сообщениям находить отклик у мельчайших групп населения, пояснил Das Magazin сам Никс: «Таким способом мы можем дотянуться до нужных деревень, кварталов или домов, даже до конкретных людей». В квартале Маленький Гаити в Майами была запущена информация об отказе Фонда Клинтон участвовать в ликвидации последствий землетрясения в Гаити — чтобы разубедить жителей отдавать свои голоса Клинтон. Это было еще одной целью: удержать электорат Клинтон (например, сомневающихся леваков, афроамериканцев и молодых девушек) от урны для голосования, «подавлять» их выбор, по выражению одного из сотрудников Трампа. Использовались и так называемые «темные посты» Facebook: платные объявления посреди ленты новостей, которые могли попадаться только определенным группам лиц. Например, афроамериканцам показывали посты с видео, на котором Клинтон сравнивала чернокожих мужчин с хищниками.

*Хиллари Клинтон оказалась одной из жертв антирекламы Cambridge Analytica*

«Мои дети не смогут больше объяснить, что значит рекламный плакат с одинаковым сообщением для всех и каждого», — завершает Никс свое выступление на саммите Concordia, благодарит за внимание и спускается со сцены.

Насколько американское общество в данную конкретную минуту обрабатывается специалистами Трампа, сказать трудно, ведь они крайне редко атакуют на центральных телеканалах, а чаще всего используют социальные сети и цифровое ТВ. И пока команда Клинтон, работавшая по лекалам социологов, пребывает в летаргии, в Сан-Антонио, где располагается «цифровой штаб» Трампа, возникает, по словам корреспондента Bloomberg Саши Иссенберга, «вторая штаб-квартира». Всего дюжина сотрудников Cambridge Analytica получила от Трампа в июле $100 тыс., в августе еще $250 тыс., в сентябре еще $5 млн. По подсчетам Никса, общая сумма оплаты услуг составила $15 млн.

Но и проводимые мероприятия тоже радикальны: с июля 2016 года волонтеры кампании Трампа получили приложение, которое подсказывает политические предпочтения и личностные типы жителей того или иного дома. Соответственно, волонтеры-агитаторы модифицировали свой разговор с жителями исходя из этих данных. Обратную реакцию волонтеры записывали в это же приложение — и данные отправлялись прямиком в аналитический центр Cambridge Analytica.

Фирма выделяет у американских граждан 32 психотипа, сконцентрировавшись лишь на 17 штатах. И как Козинский выяснил, что мужчины-поклонники косметики MAC скорее всего являются гомосексуалами, в Cambridge Analytica доказали, что приверженцы американского автопрома однозначно являются потенциальными сторонниками Трампа. Помимо прочего, подобные открытия помогли самому Трампу понять, какие послания где лучше всего применять. Решение предвыборного штаба сконцентрироваться в последние недели на Мичигане и Висконсине было принято на основе анализа данных. Кандидат стал моделью применения системы.

**Чем занимается Cambridge Analytica в Европе?**

Но насколько велико было влияние психометрии на результат выборов? Cambridge Analytica не спешит предъявлять доказательства успешности своей кампании. Вполне возможно, что это вообще вопрос без ответа. Хотя вот, есть один факт: благодаря поддержке Cambridge Analytica Тед Круз превратился из ничего в серьезнейшего конкурента Трампа на праймериз. Вот рост голосов сельских жителей. Вот сокращение электоральной активности афроамериканцев. Даже тот факт, что Трамп потратил на проект так мало денег, может говорить об эффективности персонализированного продвижения. И даже то, что он пустил три четверти рекламного бюджета в цифровую сферу. Facebook превратился в совершенное оружие и лучшего помощника на выборах, как написал в Twitter один из сподвижников Трампа. К слову, в Германии антиэлитарная «Альтернатива для Германии» имеет в Facebook больше подписчиков, чем ведущие партии ХДС и СДПГ вместе взятые.

Кроме того, ни в коей мере нельзя утверждать, что социологи, статистики, проиграли выборы, потому что сильно ошиблись со своими прогнозами. Верно обратное: статистики выиграли, но лишь те, что использовали новейшие методы. Шутка истории: Трамп постоянно критиковал эту науку, но выиграл во многом благодаря ей.

Второй победитель — компания Cambridge Analytica. Издатель главного консервативного рупора Breitbart Стив Бэннон входит также в совет директоров этой фирмы. Недавно он был назначен старшим стратегом в команде Трампа. Марион Марешаль Ле Пен, активистка французского «Национального фронта» и племянница лидера партии, уже радостно сообщила о сотрудничестве с компанией, на внутреннем корпоративном видео которой изображено совещание по теме «Италия». По словам Никса, сейчас им заинтересованы клиенты со всего мира. Уже были запросы на сотрудничество из Швейцарии и Германии.

*Мари Ле Пен хочет стать следующим клиентом Cambridge Analytica*

Все это наблюдает и Козинский из своего кабинета в Стэнфорде. После выборов в США в университете все стоит вверх дном. На развитие событий Козинский отвечаем самым острым оружием из доступных исследователю: научным анализом. Вместе со своей коллегой Сандрой Матц он провел серию тестов, результаты которых скоро будут опубликованы. Некоторые из этих выводов, которыми ученый поделился с Das Magazin, шокируют. Например, психологическое таргетирование, подобно тому, что использовали в Cambridge Analytica, повышает число кликов на рекламе в Facebook на 60%. Вероятность же того, что после просмотра персонализированной рекламы люди перейдут к действиям (купят ту или иную вещь или проголосуют за нужного кандидата) возрастает на 1400%.

Теперь мир перевернулся: Brexit состоялся, в Америке скоро будет править Трамп. Все это началось с человека, который хотел предупредить нас об опасности. Сейчас он снова получает кучу жалоб на рабочую почту. «Нет, — говорит Козинский. — Тут нет моей вины. Это не я соорудил бомбу, я лишь показал, что они существуют».

# Android-приложения тотально следят за пользователями

5.03.2019

В эпоху повсеместного использования мобильных гаджетов человеку всё труднее защититься от тотальной слежки и повсеместного контроля. Исследователи из Калифорнии, работающие в Международном институте компьютерных наук, выявили ошеломляющие факты. Оказывается свыше 17 тысяч Android-приложений внимательно следят за действиями пользователей.

Технология слежки за хозяином гаджета с установленным приложением использует рекламный идентификатор (Advertising ID), по заверениям Google, являющийся единственным поставщиком данных пользователя для разработчиков. Однако калифорнийские инженеры пришли к выводу, что свыше 65% приложений получают уникальную персональную информацию, способную идентифицировать пользователя.  
Никакие судебные разбирательства, связанные с утерей личных данных не могут остановить разработчиков в охоте за конфиденциальной информацией, ведущейся с нарушением политики Google. Фактически все настройки приложений влияют только на ограничения при передаче информации рекламному идентификатору. Однако любая другая конфиденциальная информация может быть получена приложением вне зависимости от желания клиента.  
  
Энтузиасты выявили, что собирать приватные данные могут самые популярные приложения, такие как игра Angry Birds, аудиокниги Audible, прикладные приложения Battery Doctor и Clean Master, установка которых осуществлена на более чем 1 млрд устройств. Команда Google пока никак не отреагировала на данные исследования.

Как смартфоны следят за нами  
  
01 марта 2019 в 13:48  
Роскачество раскрыло информацию о том, каким образом с помощью смартфонов и других гаджетов можно собрать фото, аудио и даже видео, а после эти данные о своих владельцах использовать в маркетинге. Другими словами, специалисты рассказали, как смартфоны шпионят за своими владельцами, а также дали советы, как обезопасить себя от «слежки».Смартфон, зараженный вредоносной программой, становится «мобильным шпионом»: он может перехватывать и отправлять смс, активировать видеозапись, делать снимки экрана, копировать контакты, фотографии и сохраненные документы. Однако немногие знают, что «шпионить» за пользователями могут вполне безобидные на первый взгляд приложения, например, мессенджер, который распознает и анализирует речь в своих целях, или фонарик, запрашивающий доступ к фотографиям и контактам. Роскачество совместно с экспертами по кибербезопасности расскажет, как безопасно жить с этим знанием.«Мобильные приложения могут осуществлять запись разговоров пользователей. Разработчики объясняют необходимость запросов приложениями доступа к пользовательским данным, в том числе к содержимому голосовых сообщений, именно требованиями функциональности. Хотя зачастую эти функции не являются первостепенными, например, тот же голосовой поиск в геоприложениях. В общем, вещь удобная, но не первой значимости для подобной программы», - комментирует Даниил Чернов, руководитель направления Solar appScreener компании Ростелеком-Solar.Собранные голосовые данные разработчики приложений активно используют в маркетинговых целях, назойливо демонстрируя пользователям таргетированную рекламу. Например, вы поговорили рядом с телефоном о своем любимом хобби или предстоящей поездке – и в вашем мобильном браузере стала активно демонстрироваться реклама товаров и услуг на эту тему. Принято считать, что пользовательские данные собираются и используются в обезличенном виде. Однако с помощью сбора дополнительной информации о пользователе, например, в социальных сетях, такие данные из обезличенных можно легко превратить в однозначно идентифицирующие пользователя. И здесь уже открывается возможность для различного рода злоупотреблений.Реклама, которая преследует тебя, повышенное энергопотребление устройства - как еще прослушка может повлиять на вашу жизнь?Открываются широкие горизонты для шантажа - нередки случаи, когда пользователю звонит мошенник и сообщает, что у него есть некие видео-и аудиозаписи, которые будут опубликованы, если не перевести крупную сумму. Чаще всего это обычный блеф, однако пользователи, которым есть, что скрывать, вступают в диалог с мошенниками и даже высылают им деньги за молчание. Если человек более-менее известен и дорожит своей репутацией, он будет готов заплатить внушительную сумму за неразглашение приватной информации.Мы рекомендуем пользователям внимательнее относиться к запросам доступа к микрофону, камере, контактам и фото от приложений и всегда задумываться, действительно ли им нужна эта функция, или без нее можно обойтись. Стоит проверить все доступы уже сейчас, это делается в настройках. Наверняка какие-то из них вас удивят.Антон Куканов, руководитель Центра цифровой экспертизы Роскачества, дал конкретные рекомендации, как избежать прослушки:«Если вы всерьез озадачены вопросом конфиденциальности и не хотите, чтобы мобильные приложения вас прослушивали, - ограничьте доступ мессенджеров и других приложений к микрофону и не используйте аудиосообщения, тем более что это еще и не всегда удобно для получателей. Менее радикальный способ - не использовать голосовые команды для выполнения функций мобильных приложений. Они ждут от нас ключевые слова и поэтому слушают и анализируют всю поступающую информацию».Однако есть приложения, которые сами по себе являются мобильными шпионами. Вячеслав Васин, ведущий аналитик департамента аудита и консалтинга Group-IB:«Раньше при установке мобильного приложения на платформу Android владелец смартфона, не читая внимательно условия пользовательского соглашения и запрашиваемые права, кликал «Установить» - в его телефоне поселялся мобильный шпион, который получал достаточно широкие возможности: включать микрофон пользователя, фронтальную или тыловую камеры и т.д. Причем большинство из этих действий выполнялись в фоновом режиме - незаметно для пользователя. Однако теперь, уже с версии Android 6.0, получить «расширенные» права незаметно для пользователя мобильному приложению стало гораздо сложнее, так как был внедрен специальный механизм запроса прав (по аналогии с iOS)».Осталось незначительное количество случаев, когда мобильные приложения смогут «прослушивать» пользователя:Пользователь сам доверяет вредоносному программному обеспечению и подтверждает нажатием право на запись (игнорирует предупреждения). Здесь следует оговориться, что на последних версиях Android прослушивание в фоне может быть запрещено.Вредоносное программное обеспечение использует технику Tapjacking (overlay) для получения необходимых прав на прослушивание.Корпоративные приложения или приложения, установленные с правами администратора (например, могут быть установлены при временном физическом доступе к устройству). Подобные программы могут не только прослушивать пользователя, но и контролировать его интернет-трафик, блокировать устройство и т.д.Приложения, которые используют открытые или закрытые уязвимости производителей смартфонов для повышения прав в системе.Большинство опасностей подстерегают пользователей операционной системы Android. Разработка вредоносных программ под iOS пока еще стоит больших денег, хотя такие вирусы, конечно, существуют и нацелены, в основном, на устройства с джейлбрейком (jailbreak), где отключены встроенные средства защиты и используются права администратора.Общие рекомендации для пользователей:устанавливать приложения только из официальных магазинов (App Store и Google Play);своевременно обновлять операционную систему;внимательно изучать список запрашиваемых прав на операционной системе Andorid до версии 6.0;внимательно относиться к запрашиваемым доступам мобильных приложений: ограничивать доступ к микрофону, камере, фотогалерее, геолокации и пр., если это не сказывается на работоспособности необходимых функций приложений.В своих исследованиях Центр цифровой экспертизы Роскачества опирается на Стандарт, в котором одним из требований к мобильным приложениям является наличие запроса только оправданных разрешений.

# Опасности технического прогресса

Современные технологии готовы сильно изменить привычный нам уклад общества. Правительство РФ намерено повсеместно распространить проект «Умный город». Данный проект был протестирован в ряде городов, где проходил чемпионат мира по футболу – 2018. Данную программу можно будет использовать для голосования собственников жилья, заказов новых сервисов от управляющих компаний, оснащения зданий датчиками запаха, задымлений, затопления, работы лифтов и другими датчиками. То есть все для безопасности и комфортного проживания в квартирах многоквартирных домов. Как говорится, любой каприз за ваши деньги.Также активно внедряется видеокамера, которая не требует каких-либо ключей, либо карточек. Сенсор реагирует на ваше лицо, включается освещение и дверь открывается, то есть уже существующая база данных распознавания лиц будет активно пополняться базами данных жильцов многоквартирных домов с данными видеокамерами. Действительно, зачем МВД собирать изображения лиц, обрабатывать их данные, кодифицировать, если люди сами за этот процесс заплатят и добровольно в целях собственной безопасности передадут внутренним органам страны?Данное новшество внедряется крупными телекоммуникационными компаниями под видом сервиса по управлению многоквартирными домами: платишь ежемесячную плату и спишь спокойно.А также есть дополнительные сервисы по дистанционному включению отопления, освещения в квартире с мобильного приложения телефона. Можно провести голосование как по общедомовым вопросам, так и общегородским. Из этого следует, что чиновники муниципалитетов, МВД и другие специальные службы будут знать, кто как голосует, когда приходит домой и в каком состоянии.В течение 3–5 лет в крупных городах России будут установлены камеры с распознаванием лиц, данные камеры будут распознавать также эмоции и настроение человека. Проект «Умный город», по заявлению заместителя министра строительства и ЖКХ РФ Андрея Чибиса, должен радикально повысить уровень безопасности в наших городах, ведь это и помощь, когда потерялся человек, когда потерялся ребенок (идентифицировать, найти его, затем отследить путь).То есть возможно появление новой квитанции по оплате в вашем почтовом ящике.А людей спросили?Задаемся вопросом, откуда такая уверенность в том, что людям это надо и как можно быстрее. Ответ очевиден – федеральный закон «О внесении изменений в федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» от 06.07.2016 г. № 374-ФЗ.  
  
'Использована информация юридической социальной сети https://www.9111.ru'

# В сети обнаружена крупнейшая база адресов и паролей электронной почты

6.02.2019

Исследователь по кибербезопасности Трой Хант (Troy Hunt) объявил, что обнаружил в облачном сервисе MEGA базу из около 773 миллионов уникальных ящиков электронной почты и более 21 миллиона уникальных паролей. По мнению специалиста, выявленная им коллекция является крупнейшим раскрытием данных такого рода за всю историю Интернета.

Казалось бы, беспрецедентная экспозиция, получившая название «Collection [#1»](https://mirtesen.ru/hashtags/1%C2%BB) и содержащая в общей сложности 1.16 млрд комбинаций адресов электронной почты и паролей, ужасает своими масштабами, но Хант показывает, что проблема не столь серьёзна, как многие считают. Хотя у людей может сложиться впечатление, что все учётные данные были получены в результате одного мега-нарушения, данные представляют собой просто набор электронных писем и паролей, собранных из многочисленных ранее известных источников.   
  
Сервис от Ханта, именуемый [«Have I Been Pwned»](https://haveibeenpwned.com/) («Взламывали ли меня?»), позволяет любому желающему проверить, была ли его электронная почта взломана. Как отмечает исследователь, что более 80% электронных писем в Collection [#1](https://mirtesen.ru/hashtags/1) уже были известны его сайту.  
  
Брайан Кребс, эксперт по безопасности, поговорил с хакером, продающим данные Collection [#1](https://mirtesen.ru/hashtags/1) и ему сказали, что контенту уже несколько лет. Тем не менее, стоит убедиться, что вашей почты нет в коллекции, в обратном случае необходимо заменить пароль.

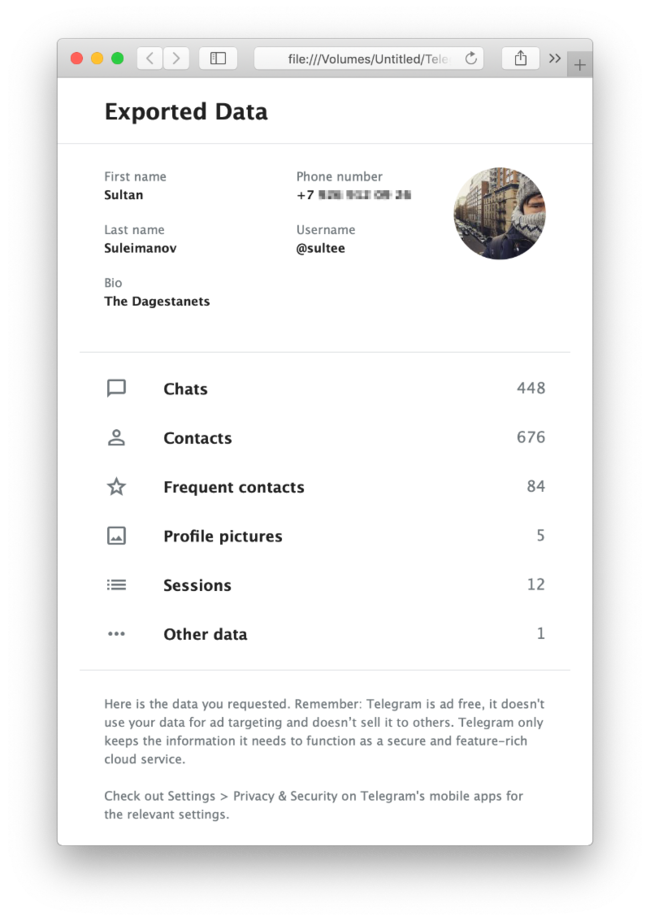
# Что знает о нас Telegram

Telegram позволяет пользователям выкачать все свои данные. Мы это сделали — и вот что обнаружили в архиве

11 октября 2018

В конце августа 2018 года мессенджер Telegram [согласился](https://meduza.io/feature/2018/08/28/telegram-soglasilsya-delitsya-dannymi-nekotoryh-polzovateley-so-spetssluzhbami-k-etomu-est-voprosy) выдавать властям данные предполагаемых террористов (хотя еще ни разу этого не делал — по крайней мере, мы об этих случаях не знаем). За пару месяцев до этого мессенджер открыл пользователям возможность скачать все их данные. В теории, в этом архиве должно оказаться все, что у мессенджера есть на пользователя — а значит, власти не смогут получить что-то больше. Журналист «Медузы» Султан Сулейманов выкачал и изучил данные своего аккаунта в Telegram — и нашел там личные сообщения за всю историю существования аккаунта, а также IP-адреса входа в Telegram за последние 12 месяцев и другую информацию.

Процедура

В конце мая 2018 года Telegram запустил специального [бота](https://t.me/gdprbot), через которого пользователи могут запросить свои данные. Создать такую процедуру интернет-компании обязывает европейский регламент защиты персональных данных GDPR.****

Сама процедура появилась у Telegram только через месяц, и она не задействует созданного ранее бота (все, что он может сделать — прислать инструкцию или связать со службой поддержки).

Чтобы получить данные, нужно зайти в свой аккаунт через клиент мессенджера для Windows или macOS, скачанный с [сайта](https://desktop.telegram.org/), перейти в настройки, и в разделе Advanced выбрать пункт Export Telegram Data. Обратите внимание, что у вас должна быть версия приложения 1.3.8 или выше (на момент написания заметки — 1.4.2). При этом в версиях клиента, начинающихся на четверку, как и в мобильных приложениях, возможности скачать данные нет.

Во всплывшем окне можно выбрать, какие именно данные хочется скачать:

* личные сообщения;
* переписки с ботами;
* переписки в группах;
* публикации в каналах;
* список контактов;
* активные сессии;
* другие данные.

Кроме того, в настройках экспорта можно указать, какие медиафайлы скачивать: фотографии, видео, аудиосообщения и так далее. Пользователь также может выбрать, в каком формате получить данные — html-файл, который можно открыть в браузере, или csv, удобный для компьютерного анализа.

Скачивание архива начнется сразу — никаких дополнительных подтверждений личности Telegram не запрашивает.

Что нашлось в архиве

* имя, фамилия и описание пользователя (из профиля);
* привязанный номер телефона;
* текущая и прошлые аватарки (они тоже видны в профиле);
* список контактов с телефона (в том числе номера пользователей, не зарегистрированных в Telegram);
* список наиболее близких контактов (формируется автоматически);
* личные сообщения — отправленные и полученные — со всем медиаконтентом;
* сообщения, отправленные в групповые чаты и каналы;
* активные сессии;
* установленные и созданные стикеры;
* неотправленные черновики;
* список IP-адресов, не совпадающий с адресами активных сессий.

Чего в архиве не оказалось

Секретных чатов — даже следов того, что они создавались. Вероятно, потому, что секретные чаты привязаны к конкретным устройствам и не хранятся в «облаке» Telegram в расшифрованном виде.

Удаленных сообщений. Правда, мне удалось найти переписку от 2013 года (одну из первых после создания аккаунта), для которой в архиве оказалось сообщение, которого уже не видно в приложении Telegram. Но было ли оно удалено, или пропало по другой причине, неизвестно.

Обновлено: читатель «Медузы» Руслан предположил, что исчезновение этого сообщения может быть связано с ограничением на количество сообщений, которые видны в приложении: в 2017 году [сообщалось](https://vk.com/wall-64980878_25960), что если их больше миллиона, то старые помещаются в архив на сервере Telegram.

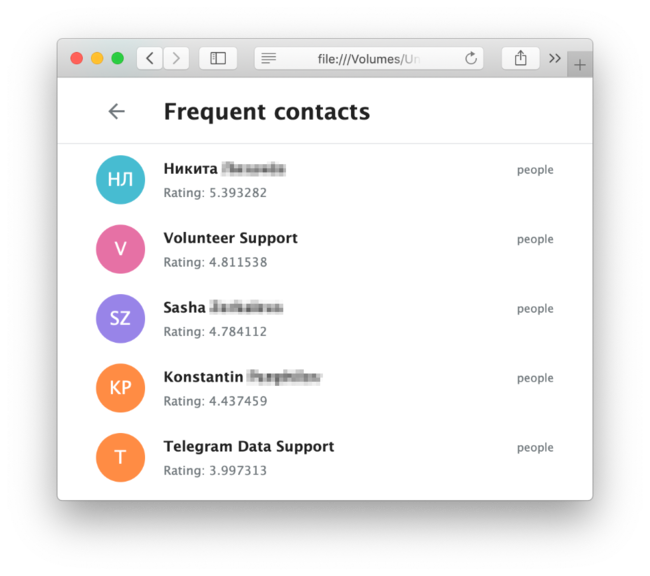
Истории звонков. Информацию о последних звонках можно просмотреть в приложении Telegram, но в отчете эта категория информации никак не упоминается.

Заблокированных пользователей. Опять же, их список можно получить в приложении Telegram, но не просмотреть в отчете.

Теперь подробнее о некоторых разделах

Телефонная книжка

Telegram после входа в аккаунт просит дать доступ к списку контактов в телефоне пользователя. Если согласиться, мессенджер будет хранить имена и номера контактов у себя на сервере (и добавлять новые, если они у вас появятся). Telegram объясняет, что список контактов используется, чтобы уведомлять вас, когда ваши знакомые тоже зарегистрируются в мессенджере. Еще одна причина: знакомых людей Telegram подпишет по имени, которое вы записали в список контактов, а не тому, которое он указал в своем профиле.

Близкие контакты****

На основе того, как много и часто вы общаетесь с человеком, Telegram высчитывает специальный рейтинг — число, обозначающее степень вашей «близости». Оно нужно, чтобы на экране поиска отображать блок с людьми, которым вы вероятнее всего захотите написать. В скачанном архиве можно увидеть это число; само по себе оно ничего не даст, но если скачивать данные раз в несколько месяцев, можно проследить, как (по мнению Telegram) менялись ваши отношения с друзьями.

Личные сообщения

В архиве оказались все отправленные и полученные сообщения, к которым остался доступ у пользователя. Мессенджер в том числе сохраняет переписки с пользователями, которые позже удалили свой аккаунт — тогда вы не увидите имя собеседника, но сможете прочитать саму переписку. Правда, эти же переписки остаются доступными в приложении Telegram.

Если выставить соответствующие настройки, вместе с сообщениями скачаются и все медиафайлы, которыми вы обменивались с собеседниками. Причем, в отличие от «ВКонтакте», присылавшей ссылки на фотографии, Telegram присылает сами файлы (из-за этого архив может занимать несколько гигабайт или даже больше).

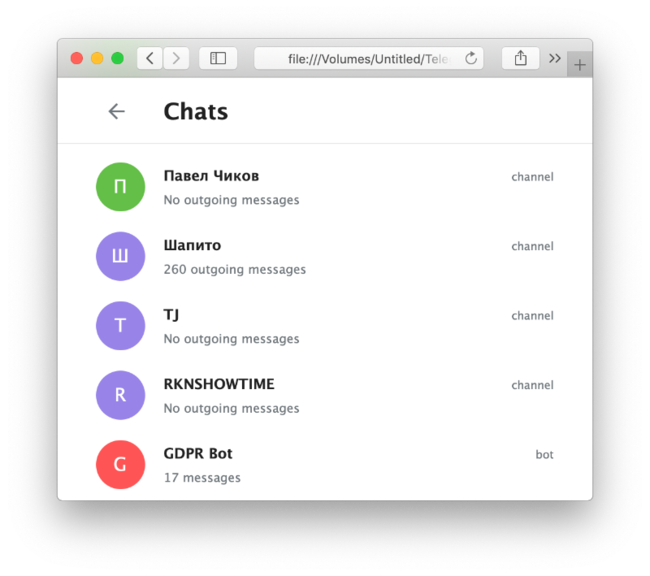
Групповые чаты

Кроме личных переписок, Telegram включил в архив содержимое групповых чатов, в том числе тех, в которых пользователь больше не состоит. Но не всех.

Логика, по которой Telegram сохраняет или не сохраняет содержимое групповых чатов, довольно сложная:

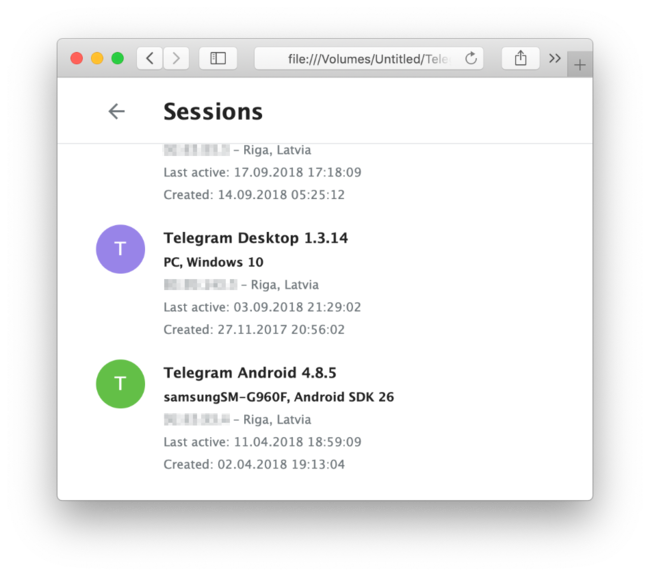
* в некоторых чатах, в которых я состоял, но вышел (или был удален), остались все сообщения за то время, что я был в нем;
* в некоторых — только мои сообщения и действия, но не чужие;
* чат, созданный с моего аккаунта (и позже удаленный), остался в архиве целиком.

Каналы

****

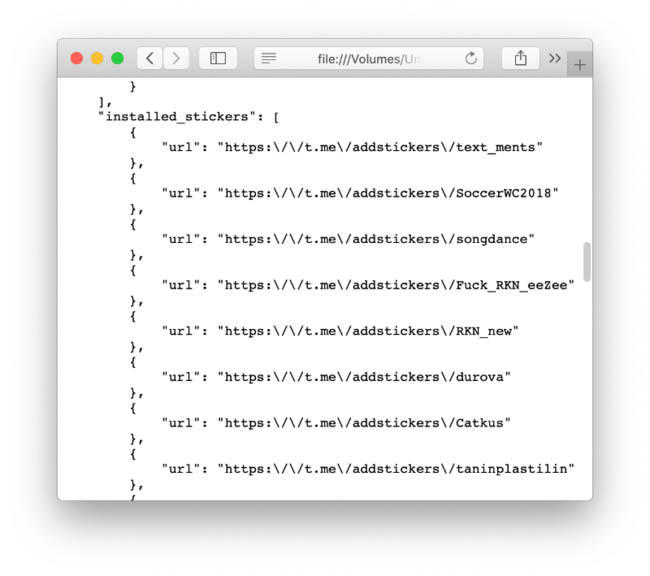
В отчете Telegram в списке чатов можно найти все каналы, в которых состоит или когда-нибудь состоял пользователь (отдельной секции для каналов в архиве не предусмотрено). При этом прочитать содержимое этих каналов нельзя — в отчет вошли только сообщения, отправленные с моего аккаунта.

IP-адреса



Информация об активных сессиях Telegram. IP-адреса в «Других данных» выглядят иначе (это просто список)

В отчете, присланном Telegram, есть секция «Другие данные». В ней оказались черновики сообщений (мессенджер автоматически сохраняет то, что вы ввели в поле для текста, но не отправили), пустое поле для адреса электронной почты, а также — список IP-адресов, с которых я входил в аккаунт.

****

Ссылка на установленные наборы стикеров в разделе «Другие данные»

Этот список шире, чем тот, что представлен в секции «Активные сессии»: как утверждает Telegram, компания хранит историю IP-адресов, изменений имени пользователя и номера телефона за последние 12 месяцев, чтобы пресекать спам и другие нарушения правил. При этом список может быть неполным — эта функция еще находится в процессе совершенствования.

Яндекс знает о нас всё

Журналист «Медузы» запросил у «Яндекса» полный архив своих данных. Он получил десятки файлов из разных сервисов — но там не оказалось почты

1 февраля 2019

Хотя «Яндекс» остается преимущественно российской компанией, он все же подчиняется Общему регламенту по защите данных (GDPR) — документу, который обязывает интернет-компании ответственно относиться к данным жителей Евросоюза. В частности, GDPR обязывает компании выдавать по запросу пользователя полную копию данных о нем (в противном случае ей грозит штраф до 20 миллионов евро). Журналист «Медузы» Султан Сулейманов, живущий в Латвии, воспользовался GDPR, чтобы запросить у «Яндекса» данные о себе. Вот что из этого получилось.

Процедура

У «Яндекса» нет отдельной формы или страницы, позволяющей скачать архив с данными о себе — поэтому я просто написал письмо на общую почту службы поддержки support@yandex.ru, где сослался на GDPR и указал фамилию, имя и место жительства. В моем профиле (это называется «Яндекс.Паспорт») при этом не было указано полное имя, а в качестве страны проживания была указана Россия.

Комментарий пресс-службы «Яндекса»: «В данном случае пользователь — это аккаунт, а не конкретный человек. Если нам поступил запрос от аккаунта с привязанной к нему Почты, то мы выгружаем данные на Диск этого же аккаунта. Третьи лица доступа к этим данным не получат. Дополнительных проверок не требуется».

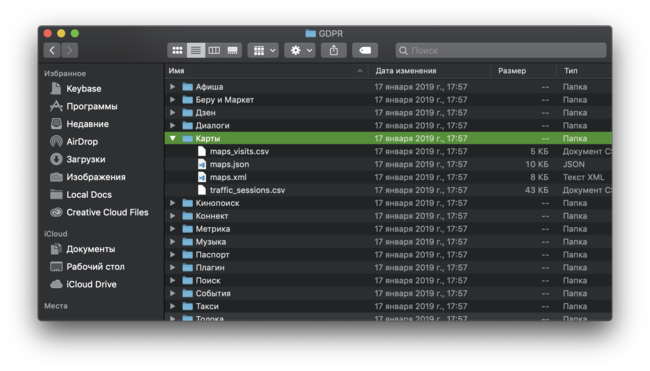
Несмотря на это расхождение, в службе поддержки не стали ничего уточнять и не попросили прислать документы, подтверждающие личность. 4 декабря — почти через месяц после того, как был отправлен запрос — «Яндекс» ответил, что не успевает собрать все данные, и попросил подождать еще (GDPR позволяет продлить время на ответ со стандартного одного месяца до трех).

Окончательный ответ пришел 21 января — через два с половиной месяца после запроса. В письме оказалась ссылка на мой «Яндекс.Диск», в который загрузили архив с копией данных, а также ссылки на две инструкции: как выгрузить письма из «Яндекс.Почты» и все файлы с «Яндекс.Диска» (поэтому рекурсии с копией «Диска» на «Диске» не вышло).

Что нашлось в архиве

Размер файла gdpr.zip, который загрузили на «Яндекс.Диск», — всего полмегабайта. В распакованном виде он занимает 8 мегабайт: внутри были исключительно текстовые документы в машиночитаемом виде (для сравнения, Telegram [присылает](https://meduza.io/feature/2018/10/11/telegram-pozvolyaet-polzovatelyam-vykachat-vse-svoi-dannye-my-eto-sdelali-i-vot-chto-obnaruzhili-v-arhive) пользователю аккуратно сверстанные HTML-страницы).

Документы разложены по папкам, примерно соответствующим сервисам «Яндекса»: есть, например, «Карты», «Такси», «Кинопоиск» и «Поиск». Никаких пояснений к данным нет: чаще всего о том, что значит то или иное поле, можно понять по контексту, но иногда сделать это непросто.



Содержимое архива, присланного «Яндексом»

Вот что содержится в каждой папке:

«Афиша». Логично предположить, что файлы относятся к сервису «Яндекс.Афиша». Но точно установить, что за данные они содержат, у меня не получилось. В одном файле приводился короткий список мероприятий, которые я, видимо, когда-то просматривал (их названия зашифрованы — прочитать можно только теги, которые к ним относятся). Во втором — список музыкантов и групп, чьи песни, по всей видимости, я слушал в «Яндекс.Музыке». Вероятно, он нужен, чтобы предлагать подходящие события: в списке нет конкретных треков, но указано, сколько раз я слушал песни того или иного исполнителя.

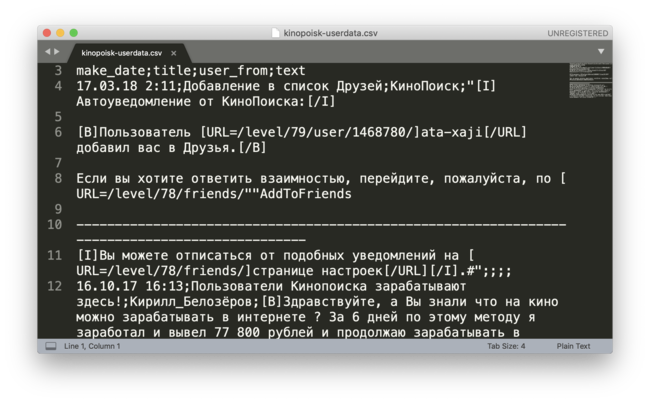
«Беру и Маркет». Еще два файла, очевидно, связанных с «Яндекс.Маркетом»: в одном оказался отзыв 2014 года, который я оставлял интернет-магазину знакомого, во втором — наушники, которые я в 2018-м добавил в «отложенные». И то, и другое можно посмотреть и через стандартный интерфейс «Маркета». Списка товаров, которые я искал в сервисе, в отчете «Яндекса» нет — то ли компания не хранит эту информацию, то ли забыла ее включить в архив.

«Дзен». Здесь оказался огромный файл почти на 50 тысяч строк (или примерно на 10 тысяч записей) с историей страниц и сайтов, которые я просматривал через «Яндекс.Дзен» с июля 2018 года. Причем в документ, судя по всему, попали не только материалы, которые я читал, но и страницы, которые просто попадались в ленте рекомендаций: параметр event где-то принимал значения click и visit, а где-то — show.

«Диалоги». Несколько небольших файлов, связанных с навыками для голосового помощника «Алиса», которые я начинал разрабатывать. В одном из них перечислены пользователи, установившие эти навыки — но так как они непубличные, в списке оказался только я сам.

«Карты». Один из документов в этой папке содержал описание точек и маршрутов, созданных через сервис «Мои карты» (в нем можно пометить определенные места на карте мира и поделиться результатом с другими). Второй — даты (с точностью до секунды), когда я заходил на сайт «Яндекс.Карт» с компьютера за последний год. Третий — с историей запуска приложения «Карт» на айфоне с точными координатами, где это происходило. Значение еще одного файла я так и не понял: в нем перечислены названия и координаты 77 мест, которые я, вероятно, искал (хотя вспомнить, зачем мне понадобилось бы вбивать в поиск по карте «РЖД Южно-Уральская железная дорога Моторвагонное депо Курган», я не смог). Все места в этом списке приведены один раз и не совпадают с историей моего поиска в «Яндекс.Картах».

«Кинопоиск». В октябре 2018 года сервис «Кинопоиск» начал переход на авторизацию через аккаунты в «Яндексе». Поэтому у «Яндекса» оказалась часть информации обо мне: судя по присланному архиву, это список моих друзей и общие сведения об аккаунте. Но и то, и другое пришло в странном виде: в списке друзей в файле «Яндекса» указано три пользователя, хотя сайт «Кинопоиска» сообщает, что друзей у меня вообще нет. Один из указанных пользователей добавлял меня в друзья, но откуда взялись двое других — загадка. В файл с информацией об аккаунте попали также фрагменты двух из трех личных сообщений, присланных мне в «Кинопоиске» — судя по их виду, это случилось по ошибке.



Как это выглядит

«Метрика». В эту папку вошла одна таблица со списком счетчиков «Яндекс.Метрики», которые я устанавливал на разных сайтах — в том числе на страничке, созданной в 2011 году на «Народе». Никакой статистики в таблице нет, только идентификаторы счетчиков и контактный адрес электронной почты.

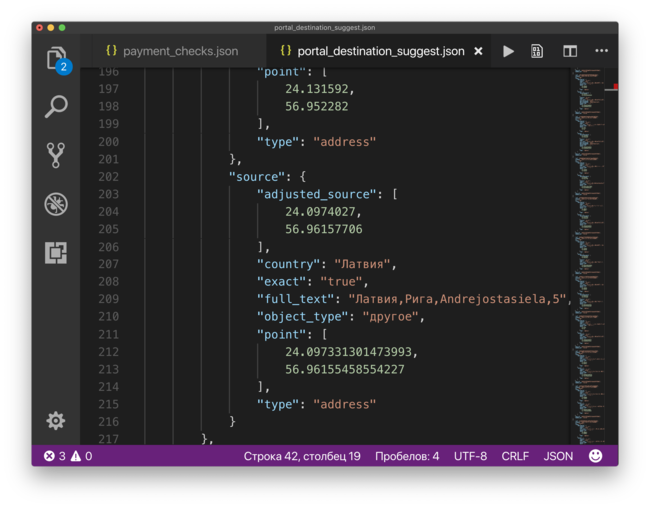
«Музыка». Самый большой файл в архиве — более пяти мегабайт. Внутри — история прослушивания шести тысяч треков из «Яндекс.Музыки» с уточнением, какую песню, когда и на какой платформе я слушал. Значительный вклад в этот список внесла «Яндекс.Станция», на которой последние полгода постоянно играет музыка. В тот же файл вошли лайки, которые я поставил песням (список, присланный «Яндексом», почему-то не совпадает со списком в профиле «Яндекс.Музыки»), и плейлисты, которые я составлял в сервисе. Еще несколько полей оказались пустыми: настройки, трансляции, совместные плейлисты и некий «волшебник» (wizard).

«Паспорт». Документы в этой папке связаны с самим аккаунтом в «Яндексе». В первом приведены неполные данные о том, на каких устройствах я авторизован (с указанием IP-адресов входа), во втором — данные профиля, которые я заполнял сам: имя, фамилия, дата рождения, номер телефона, резервный почтовый ящик и ссылки на аккаунты в соцсетях и «Кинопоиске».

«Поиск». При подготовке этого материала я выяснил, что в «Яндексе» больше нельзя посмотреть историю своих поисковых запросов — функция «Мои находки», существовавшая с 2007 года, исчезла в 2017-м. В отчете компании таблица с поисковыми запросами есть: в ней указаны записи с 2015 года с датой и временем поиска. В таблицу попали не только запросы, которые я вводил непосредственно в «Яндексе», но и то, что по моей просьбе искала в интернете голосовая помощница «Алиса» на телефоне. Еще две таблицы в этой папке содержат историю поиска картинок и видео в поисковике.

«Такси». Здесь оказалось сразу 12 файлов, в которых приведены:

* банковские карты, привязанные к аккаунту (номера карт приводятся без части цифр, CVV-кода в документе нет);
* адреса, которые, судя по названиям файлов, приложение «Яндекс.Такси» должно предлагать установить в виде начальной и финальной точки поездки;
* список трех десятков моих поездок на такси с указанием, на какой машине я ездил, какой картой и какую сумму заплатил, какую оценку поставил и какие промежуточные точки проехал. В файле также даны ссылки на сами маршруты, нарисованные на карте. Вся эта информация также доступна в меню «История поездок» в приложении «Яндекс.Такси»;
* еще один список с историей поездок, уже на 64 записи; здесь приведены, в частности, рассчитанная и фактическая длина пути, год производства автомобиля и размер чаевых;
* несколько ссылок на чеки, оформленные по итогам поездок;
* жалоба, которую я подал на одного из водителей;
* мой email, номер телефона и сохраненные в «Яндекс.Такси» адреса.



«Datasync». Наконец, в этой папке лежал файл с набором баз данных, содержащих разрозненную информацию обо мне. В этом наборе оказались, в частности:

* адреса, на которые я заказывал доставку каких-то товаров;
* закладки в «Яндекс.Картах»;
* история точек, которые я ставил на тех же картах;
* история поисковых запросов в «Картах»;
* какая-то информация, связанная с моими фотографиями на «Яндекс.Диске» (в документе есть ссылки на их превью) — вероятно, она используется, чтобы присылать уведомления в духе «Посмотрите фото, сделанное ровно три года назад»;
* мой рабочий адрес, который, по всей видимости, «Яндекс» вычислил самостоятельно: он указан в блоке extracted\_addresses («извлеченные адреса») и не совпадает с фактическим адресом — вместо улицы Кришьяна Валдемара указана соседняя Сколас.

Кроме того. В отчете, присланном «Яндексом», нашлись поисковые запросы, введенные в строку поиска в «Яндекс.Телефоне»; данные об использовании платформы «Яндекс.Коннект»; сообщение о баге, которое я отправил в службу поддержки «Яндекс.Такси» (оно приводится в двух разных документах); информация о профиле и выполненных заданиях в сервисе «Яндекс.Толока».

Чего в архиве не оказалось

Запрашивая у «Яндекса» всю информацию о себе, я в первую очередь думал о почте и облачном хранилище: остались ли на серверах компании удаленные письма и файлы? И сохраняется ли история изменения файлов? К сожалению, узнать ответы на эти вопросы не получилось: компания не стала включать содержимое этих двух сервисов в отчет, вместо этого предложив скачать письма и документы через стандартную процедуру.

Данные из «Почты» «Яндекс» [предлагает](https://yandex.ru/support/mail/download-all-letters.html) скачать с помощью одного из почтовых клиентов для компьютера (вроде Outlook или The Bat). Очевидно, что они получат только те письма, которые доступны пользователю в веб-интерфейсе — и узнать, не осталось ли на серверах «Яндекса» следов удаленных сообщений, так не выйдет.

Похожая ситуация с «Диском»: компания [советует](https://yandex.ru/support/disk/actions-files/download-all.html) просто выделить все файлы и нажать «Скачать». В таком случае можно восстановить только документы, лежащие в «Корзине» (оттуда все удаляется через 30 дней).

Кроме писем и содержимого «Диска», в отчете «Яндекса» не нашлось:

* данных из календаря;
* задач из сервиса «Дела», встроенного в почту;
* списка контактов;
* черновиков публикаций в «Дзене»;
* отзывов об объектах на «Яндекс.Картах»;
* истории событий на сервисах «Яндекса» (в «Паспорте» можно посмотреть, когда и с какого браузера я заходил);
* привязанной к аккаунту в «Яндексе» (не «Такси») банковской карты;
* «Яндекс.Денег» целиком (хотя можно предположить, что это отдельная компания, и у «Яндекса» нет никаких данных оттуда);
* товаров, купленных через «Яндекс.Маркет» (хотя в профиле пользователя они видны);
* информации об использовании «Яндекс.Погоды» (например, городов, для которых я проверял информацию);
* истории использования «Яндекс.Станции» — например, опробованных навыков (если эти сведения хранятся в «Яндексе»);
* данных, которые собрал обо мне «Яндекс.Браузер» в процессе использования — например, истории посещенных страниц, если она хранится не локально.

**В этом контексте можно вспомнить информацию Эдварда Сноудена, так и более свежие инциденты. Например, недавний случай в Великобритании, когда лайк, оставленный под неполиткорректным стихотворением, моментально привел к тому, что к его автору явилась полиция. Январь 2019 г.**

# Как защитить данные бизнеса по цене кофе в офисе

**«Шифровальщики — это бич времени». Как защитить данные бизнеса по цене кофе в офисе**

**Бизнес находится под постоянными кибератаками злоумышленников, цель которых — опустошить счета компании или похитить данные ее клиентов. Компании, особенно небольшие, часто экономят на информационной безопасности (ИБ), и половина директоров по ИБ уверены: расплатой за это станут финансовые потери.**

**Как можно предотвратить атаки и на что обратить внимание для защиты бизнеса? Рассказывает**[**Тимур Бигулов**](http://www.dk.ru/wiki/bigulov-timur)**, руководитель отдела продаж клиентам малого и среднего бизнеса «Лаборатории Касперского».**

**— Зачастую руководители в сфере информационной безопасности понимают неминуемость угроз, но сталкиваются с нехваткой бюджетов. Насколько велики масштабы этой проблемы и как бизнесу с ней справляться?**

**— К сожалению, кибербезопасность в России действительно недофинансирована.**

**Вероятно, это связано с тем, что многие руководители и собственники бизнеса недооценивают масштабы потерь, к которым могут привести киберинциденты.**

**Важно трезво оценивать, какие убытки понесет компания при простое в течение нескольких дней — если перестанет работать сайт или все корпоративные компьютеры. Конечно, для продавца цветов, ведущего бухгалтерию в тетрадке, двухдневная блокировка компьютера не станет серьезной проблемой. Но доступ к данным критически важен для турагентства, страховой компании, ритейлера, который ведет бухгалтерию в электронном виде, поставляет товар в кредит, делает записи о будущих платежах и долгах. Это все реальные случаи из нашей практики.**

**Объем предстоящих платежей и средств, которые еще не поступили на счета компании, может составлять 20-30% от годового оборота.**

**Когда предприниматель понимает, сколько может потерять, то примерно представляет, сколько готов инвестировать в бесперебойную работу, сохранение интеллектуальной собственности компании и ее репутации — то есть обеспечение кибер и ИТ-безопасности. С одной стороны, это немного эфемерные расчеты — как оценить стоимость репутации? С другой стороны, они вполне очевидны. Например, если авиакомпания не сможет продавать билеты онлайн, клиенты не будут долго ждать и просто купят билеты у другого перевозчика.**

**http://www.dk.ru/system/ckeditor_pictures/000/181/779_content.png?1544441306Утеря данных приведет к сложностям, как минимум с доступом к 20-30% годового оборота средств компании**

**Обычно бюджет на кибербезопасность и информационную безопасность составляет 10–15% от всего ИТ-бюджета. Затраты на мобильные устройства, компьютеры, картриджи, интернет в среднем составляют 30–50 тыс. руб. на одного сотрудника в год. А качественная защита одного рабочего места в малом и среднем бизнесе — от 1 тыс. до 3,5 тыс. руб.**

**Поэтому экономия на ИТ-безопасности — это экономия на спичках. Офисные траты на кофе, туалетную бумагу и канцелярские принадлежности могут быть выше.**

**Важно понимать, что защита информации — это критически важная статья расходов, которой не стоит пренебрегать.**

**Малый и средний бизнес сейчас находится под пристальным вниманием злоумышленников — в некоторых случаях кибератаки даже приводили к банкротству предприятий.**

**Киберпреступники выискивают пути, как проникнуть в организацию. Чаще всего для этого рассылаются письма в бухгалтерию, а затем — в юридический, кадровый и маркетинговый отделы.**

**В электронных сообщениях может содержаться вредоносное ПО или предложение перейти на фишинговую страницу. После заражения злоумышленники начинают собирать различные данные: отслеживают нажатия клавиш на клавиатуре, перемещение мышки, изучают переписку, контакты и должности отправителей писем и т.д.**

**http://www.dk.ru/system/ckeditor_pictures/000/181/780_content.png?1544441313Изучив процессы в компании, злоумышленники могут составить целевое фишинговое письмо, направленное на конкретного сотрудника.**

**К примеру, работнику отдела кадров написать с просьбой рассмотреть резюме, приложив файл в формате Word.**

**Подобными документами сотрудники компаний пользуются каждый день, однако они могут содержать исполняемый скрипт, который запустит вирус и начнет шифровать данные внутри компании — на всех локациях, куда имеет доступ данный сотрудник. Обычные антивирусы, работающие только сигнатурным методом, не могут отследить подобную программу-вымогатель.**

**Шифровальщики — это бич текущего времени. Их активность увеличивается в четвертом квартале года, когда идут наиболее активные продажи, и с конца марта до июня, когда компании подают налоговую отчетность за прошедший период. Какие угрозы со стороны компетентных органов могут быть, если не подать налоговую декларацию вовремя?**

**Теперь представьте, что все данные на серверах были зашифрованы, и доступа к бухгалтерским и учетным программам просто нет.**

**Компания вынуждена заплатить злоумышленникам, либо сообщить налоговой, что не может сдать отчетность. Поэтому сумма выкупа в пиковые периоды растет.**

**— Есть статистика, какая часть атакованных компаний соглашается заплатить, а какая пытается расшифровать данные и бороться со злоумышленниками?**

**— Восстановить данные без ключа шифрования после атаки современного шифровальщика невозможно. Если раньше был один универсальный ключ на все пострадавшие компьютеры, то современное вредоносное ПО создает ключи для каждой отдельной машины.**

**Защитой от шифровальщиков будет использование не обычных антивирусов, а многослойной системы кибербезопасности. Она должна включать мониторинг активности программ, пользователей, эвристический поведенческий анализ, возможность 100-процентного предотвращения запуска шифровальщика.**

**http://www.dk.ru/system/ckeditor_pictures/000/181/781_content.png?1544441321Если проверять входящие сообщения на почтовых серверах, то вложения с вредоносными файлами даже не дойдут до компьютера работника**

**Второй рубеж обороны — на рабочем месте сотрудника: контроль запуска программ проверяет все используемые файлы. Третий барьер — веб-контроль: администратор сети составляет «белые» списки сайтов, где перечисляются разрешенные ресурсы, а все остальные считаются запрещёнными.**

**Максимальное внимание в вопросах кибербезопасности надо уделить защите рабочих станций бухгалтера, юриста, финансового и генерального директоров — людей, имеющих доступ к деньгам компании. Чаще всего они и подвержены целевым атакам злоумышленников.**

**Следующий уровень защиты от шифровальщиков — антикриптор или мониторинг системы. Антикриптор отслеживает поведение пользователя: если он вдруг начинает шифровать данные, чего никогда раньше не делал, то подозрительная деятельность будет приостановлена, а компьютер отсечен от всей остальной сети. Часть данных поместят в бэкап для последующего восстановления. Таким образом мы предотвращаем развитие атак шифровальщиков на наших заказчиков.**

**— Один из самых нашумевших зловредов — Buhtrap. Как можно с ним бороться?**

**— Buhtrap — это вредоносная программа, позволяющая получить доступ к электронному банку, к возможности проводить финансовые трансакции в компании.**

**Попытки злоумышленников найти людей, которые могут проводить такие операции, становятся все изощреннее. Заражаются сайты специализированных СМИ, которые чаще всего посещают бухгалтеры и финансовые директора, сайты, на которые заходят руководители компаний, собственники бизнеса.**

**http://www.dk.ru/system/ckeditor_pictures/000/181/782_content.png?1544441328В некоторых случаях хакеры даже создают ресурсы с интересным контентом, чтобы привлечь к себе больше специализированных пользователей.**

**— Каковы последствия заражения Buhtrap?**

**— Сумма ущерба российских компаний от подобных вредоносных программ только за прошлый год оценивается в десятки миллионов долларов. Справиться с Buhtrap можно, но нужно бороться не с последствиями атаки, а с ее первоисточником.**

**Квалифицированные решения, как у «Лаборатории Касперского», позволяют обнаружить вредоносные новостные ресурсы, с помощью которых Buhtrap попадает на рабочие станции, и полностью их заблокировать вместе со зловредом.**

**— Иногда кибербезопасностью в компаниях малого и среднего бизнеса занимаются неспециалисты. Как руководителю бизнеса осознать важность этой задачи и передать ее в правильные руки?**

**— Специализированные решения для компаний среднего и малого бизнеса, например, Kaspersky Small Office Security, позволяют защитить компании, у которых менее 25-ти рабочих станций. Этот продукт включает защиту финансовых трансакций, менеджер паролей, защиту мобильных устройств, серверов и рабочих станций. В программе использованы технологии, которые разрабатывались с том числе и для защиты крупных компаний.**

**В более крупном сегменте будет интересно решение Kaspersky Security Cloud. Оно подойдет компаниям, в которых работает до 250 сотрудников.**

**При этом управлять защитой можно не только с рабочего места, а из любой точки мира, где есть доступ в интернет.**

**То есть сотрудник может уехать в отпуск на Бали и оттуда следить за кибербезопасностью компании. Консоль интуитивно понятна и адаптирована для неспециалистов — разобраться с настройками сможет даже главный бухгалтер или руководитель бизнеса.**

**— Может ли бизнес положиться на бесплатные решения по защите от финансовых угроз?**

**— Как и решения для домашних устройств, они не подходят для корпоративных пользователей, потому что не предназначены для защиты организаций. А злоумышленники совершенствуются в своих методах работы. В основном бесплатные версии включают только базовую защиту от вредоносного ПО, они не могут обеспечить безопасность финансовых операций онлайн, не блокируют мошеннические ссылки, не помогают контролировать использования ресурсов и программ и т.д.**

# «За нами следят»: что знают о пользователях интернет-компании и сколько стоит такое знание

**12 января 2018|Натали НахайТомас Чаморро-Премузик**

**Ходят**[**слухи**](https://www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook)**, что Марк Цукерберг закрывает камеру и микрофон своего ноутбука. Как пишет Антонио Гарсиа Мартинес в своей новой провокационной книге Chaos Monkeys, посвященной основателю Facebook, «первыми с тонущего корабля бегут не крысы, а члены команды, умеющие плавать». Эндрю Гроув, один из основателей компании Intel и пионеров Кремниевой долины, высказался примерно в том же духе: «Выживают только параноики».**

**Во времена, когда люди проводят больше времени онлайн, чем офлайн, мы производим море личных данных, и мысли о хакерах и кибербезопасности преследуют нас как никогда прежде. Когда-то «личное» означало «конфиденциальное», но не сегодня, когда наши персональные и интимные отношения (и генерируемые ими данные) развиваются в интернете, который становится все более публичным местом. Даже когда на нас никто не смотрит, мы редко остаемся в одиночестве.**

**Что если бы у вас появился шанс выкупить все данные, оставленные вами в интернете с первой минуты выхода онлайн и до сегодняшнего дня? Сколько бы вы заплатили? Что бы вы отдали ради 100% безопасности? Прежде чем ответить, подумайте о следующих издержках.**

**1. Больше никаких «бесплатных» услуг. Всем известны слова Эндрю Льюиса с сайта**[**MetaFilter**](http://www.metafilter.com/user/15556)**: «Если вы не платите, то вы не потребитель, а продукт, который продается». Но что если провайдеры электронной почты, социальные сети и даже поисковые серверы, которыми мы пользуемся каждый день, перестали бы быть бесплатными? Мы можем жаловаться на отсутствие конфиденциальности и быстрое проникновение в личное пространство поставщиков подобных услуг, однако широко распространенных альтернатив, по-видимому, не существует.**

**Дело не в отсутствии идей. Новаторы в области технологий предлагают альтернативные бизнес-модели, например,**[**Джарон Ланье**](http://www.niemanlab.org/2013/05/jaron-lanier-wants-to-build-a-new-middle-class-on-micropayments/)**предложил использовать персональные микроплатежи для вознаграждения пользователей, предоставляющих данные. Представьте себе, что вы будете получать небольшой платеж за каждое отправленное письмо или сообщение по Whatsapp — может ли такое решение помочь избежать избытка информации? Другим вариантом, конечно, может стать подписка на сервисы, такие как Facebook, плата за которую будет гарантировать конфиденциальность данных пользователей и заменит продажу данных в рекламных целях.**

**Проблема заключается не столько в технической стороне вопроса, сколько в психологической: в неосязаемости наших данных и их воспринимаемой ценности. Для большинства из нас «бесплатные» услуги, которыми мы пользуемся онлайн, позволяют удовлетворить конкретную потребность — связаться с другими людьми. Общаясь по электронной почте, в групповых чатах или социальных сетях, мы производим данные, которые не только неосязаемы, но и ценность которых среднестатистическому потребителю сложно понять и оценить. Большинство людей содрогнутся при мысли, что чужой человек придет к ним домой и начнет просматривать фотоальбомы, банковские выписки и личные дневники, однако многие и глазом не моргнут, когда нечто подобное произойдет онлайн, вероятно, потому, что в этом случае вторжение и его последствия менее заметны. Только столкнувшись с конкретным сценарием, таким как утечка данных (номера кредитной карты или личных фотографий), мы начинаем понимать, чем грозит в реальном мире наши действия в онлайне.**

**Если говорить о социальных сетях, то даже когда люди понимают риски и беспокоятся о конфиденциальности, они все равно редко придерживаются защитной**[**стратегии поведения**](https://dl.acm.org/citation.cfm?id=2166524)**. Они все чаще сетуют на нарушение конфиденциальности, но продолжают публично раскрывать данные о себе и позволяют компаниям беспрецедентный доступ к ним, что ведет к «парадоксу конфиденциальности». Если коротко, такое поведение свидетельствует о том, что люди на деле не так сильно беспокоятся о конфиденциальности, как на словах. Им нравится сама идея, но, по-видимому, они не настолько ценят свои данные, чтобы предпринимать конкретные шаги по их защите. Справедливости ради следует отметить, что такое несовпадение отношения и поведения наблюдается во всех областях жизни. Например, большинство людей ценит свое здоровье и отношения, однако ведет себя так, что регулярно рискует и тем, и другим, даже когда осознает потенциальные последствия.**

**2. Больше никакой персонализации. При взаимодействии в интернете мы привыкли к некоторой степени соответствия результатов поиска и онлайн-услуг или продуктов нашим персональным характеристикам и контексту. Один из руководителей Alphabet Эрик Шмидт давно отмечал, что в отличие от традиционных СМИ интернет занимается «узким вещанием». Персонализация не выражена явно, и мы начинаем понимать, насколько скорректированы именно под нас сервисы (например, поиск по картам Google, реклама, которую мы видим в YouTube или Facebook), только когда меняем настройки приватности или стираем cookies и историю поиска.**

**Мы так привыкли к легкости и удобству, что не спешим отказываться от них в пользу более конфиденциальных (но и более неэффективных) методов. Конечно, можно отключить настройки геолокации для приложения вызова такси, чтобы оно перестало отслеживать каждый ваш шаг, но тогда каждый раз, когда вы захотите воспользоваться им, придется вручную вводить свое местоположение, то есть тратить слишком много сил ради конфиденциальности.**

**Конечно, у персонализации есть и оборотная сторона, например, когда вы начинаете получать на разных платформах (в социальных сетях, сервисах ТВ по запросу и по цифровом радио) рекламу продукта или услуги, которую искали, но не подозревали, что вас отслеживают. Этот «пугающий фактор» — ощущение, что каждый ваш шаг, публичный и приватный, отслеживают, анализируют его и извлекают из него выгоду — может привести к ситуации, известной как**[**психологическое сопротивление**](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4675534/)**. Если нам кажется, что мы теряем свободу или она находится под угрозой, желание восстановить ее может заставить людей воспротивиться социальному влиянию: у пользователя возникнет ощущение насилия над собой, и репутация компаний, надеявшихся с помощью персонализации увеличить доходы, будет запятнана.**

**3. Больше никакого мгновенного удовлетворения запросов. Данные, которые мы производим в ходе повседневных взаимодействий, также можно использовать для разработки сервисов, пользующихся нашим желанием получать то, что нам нужно, немедленно и в удобном формате. Мы живем в век, когда только мгновенное удовлетворение запроса считается достаточно быстрым. Учитывая наши ограниченные возможности удерживать внимание, на рынке, уже страдающем из-за нехватки времени и внимания у потребителей, сервисы, предлагающие мгновенные решения, не только обеспечивают ощущение немедленного удовлетворения запроса, но и могут более эффективно добиться того, чтобы клиент серьезно не задумывался. Когда, например, вы в последний раз читали условия использования загружаемого приложения? Иными словами, когда мы подписываемся на новую услугу, стремление к удобству часто перевешивает рациональные рассуждения, и мы соглашаемся на использование наших данных такими способами, которых не могли даже представить. Стремясь потратить как можно меньше времени и умственных усилий, возможно, мы обрекаем себя в будущем на значительный риск в виде утечки персональных данных или отказа в определенных**[**медицинских**](https://gizmodo.com/23andme-is-selling-your-data-but-not-how-you-think-1794340474)**или финансовых услугах в связи с выводами, сделанными о нас на основе цифрового следа.**

**Как нам кажется, нам следует ожидать гораздо большего в обмен на конфиденциальность. Между количеством раскрываемых нами данных и получаемыми услугами должно быть больше симметрии. Например, рекомендательные сервисы должны действительно помогать находить то, что нам нужно, даже если мы не знали, чего хотим. До некоторой степени это реализуется в области музыки и кино, но не когда речь идет о покупках. Аналогично те же данные, что собираются в рекламных целях, могут использоваться для более точного предложения вакансий, так как они указывают на множество психологических качеств, которые десятилетиями связывают с карьерными результатами. Например, если ваши предпочтения на Netflix или Spotify показывают, что вы любознательный или творческий человек, алгоритм поиска работы может предложить вам вакансии, где требуется любознательность и творческий подход. И самое главное: ни один из этих сервисов не должен предлагаться без согласия потребителя, эти сервисы должны объяснять, как и зачем они используют наши данные. Мы заслуживаем право знать, какие выводы делаются из наших данных и насколько они точны.**

**Об авторах. Натали Нахай — лектор и автор бестселлера Webs of Influence: The Psychology of Online Persuasion». Ее лекции, статьи и подкасты посвящены цифровому применению бихевиоризма. Томас Чаморро-Премузик — профессор психологии бизнеса в Лондонском университетском колледже и Колумбийском университете, участник Entrepreneurial Finance Lab Гарвардского университета, гендиректор Hogan Assessment Systems.**

# Как за нами следят наши гаджеты

18 ДЕКАБРЯ 2018 [АНТОН ИВАНОВ](https://www.gq.ru/author/anton-ivanov)

**222 страницы – именно столько потребовалось Facebook, чтобы описать все способы сбора информации о пользователях. GQ хватило пяти абзацев, чтобы объяснить: за каждым из нас следят через наши цифровые устройства. Добро пожаловать в мир, где все, что вы купите, будет использовано против вас.**

У нас две новости: хорошая заключается в том, что все мы скоро будем жить как в кино; плохая – это кино будет очень похоже на «Матрицу». То, о чем нас предупреждали фантасты, начинает сбываться: искусственный интеллект становится все умнее и вот-вот придет к заключению, что общество, помешанное на роликах про котов, не имеет права на жизнь. Причем мы сами открываем двери в наше сознание. В китайских компаниях все более популярным становится отслеживание мозговых импульсов сотрудников. Датчики, вмонтированные в униформу, фиксируют всплески эмоций, а искусственный интеллект решает, насколько они скажутся на производительности труда. Пока ярость, печаль и беспокойство еще не могут стать причиной увольнения, но они легко лишат работника места на ответственном участке. Человеку с «неправильными» эмоциями поручат что-то простое и безобидное, и чем чаще компьютер будет фиксировать нерабочий настрой, тем меньше шансов на движение по карьерной лестнице и больше поводов для новых приливов ярости, печали и беспокойства. Звучит мрачновато, но если в Поднебесной хотя бы известно, кто и зачем собирает данные, то нам о такой роскоши остается только мечтать.

Это похоже на сделку с дьяволом: получив смартфоны, дающие возможность в любой момент узнавать о мире практически все, люди в обмен дали полный доступ к своей жизни. Перемещения и переговоры, покупки и фотографии, личные контакты и списки друзей, переписки и запросы в поисковиках – никогда прежде человек не оставлял столько следов, как в XXI веке, когда интернет из зоны полной анонимности стал пространством постоянного сбора данных о каждом.

«Все, что попало в сеть, навсегда останется в ней. Как бы вы ни хотели сохранить тайну, если будут желающие, они смогут ее узнать», –

разводит руками технический директор «ВКонтакте» Александр Константинов.

Google, YouTube и «Яндекс» хранят историю наших запросов; электронные карты, навигаторы, приложения такси, каршеринга и авиакомпаний – маршруты поездок; а Facebook мгновенно опознает на фотографии каждого из двух миллиардов своих пользователей. Сегодня за нами следят настолько пристально, что остается лишь завидовать Саре Коннор: Терминатору приходилось искать ее по телефонной книге, о нашем же местоположении машинам известно все и всегда.

Откройте настройки геолокации в смартфоне, и вы увидите, что прямо сейчас вас на карте видят ваш банк, несколько магазинов и ресторанов, операторы такси и, конечно, соцсети. Этим роботам не нужны ваши «одежда и мотоцикл», их интересуют более ценные вещи: ваше время и деньги. По мере того как смартфон берет на себя функции телевизора, компьютера и кошелька, он превращается в источник исчерпывающей информации о каждом из нас и главную цель маркетологов и злоумышленников. «Если за нами и следят, то последние лет пять. Раньше это было трудно, ведь наши с вами гаджеты не были так массово подключены к интернету, – продолжает Константинов. – У телефонов и ноутбуков есть возможность «подсматривать» и «подслушивать». Все зависит от того, какие настройки приватности вы выбрали и разрешали ли отдельным программам и сайтам доступ к камере и микрофону». У вас бывало так: вы только что поговорили с коллегой у кулера о чем-то, что никогда не искали в сети, а вернувшись за компьютер, увидели контекстную рекламу этого еще вчера неведомого вам продукта? Думаете, у стен есть уши? На самом деле они растут из вашего смартфона.

«Достаточно установить приложение с рекламным модулем, и оно сможет сливать данные сторонним лицам, – подтверждает антивирусный эксперт «Лаборатории Касперского» Виктор Чебышев. – Кроме того, существуют шпионские программы, которые включают микрофон, когда смартфон оказывается в нужной локации, – в начале года такую функцию мы обнаружили у троянца Skygofree».

Так что никаких «Ok, Google» или «Привет, Siri» – они и так здесь, слушают и повинуются, только не нам.

Александр Константинов не столь категоричен: «Всегда легко представить самое страшное, но все намного проще. Скорее всего, кто-то из ваших друзей, когда вы были в одном помещении и с одинаковым IP-адресом, искал информацию. Именно так работает обычный таргетинг – с учетом интересов, поисковых запросов и активности друзей. Если говорить про «ВКонтакте», мы ориентируемся на то, что указано у человека в профиле, и на тематику постов, которые он предпочитает. Учитываем, например, указанный на странице город проживания, возраст, образование, подписки, операционную систему. Благодаря этому показываем более интересную и подходящую рекламу. Причем, когда рекламодатель настраивает какие-то объявления, он видит лишь обезличенную информацию и не может знать, что нравится именно вам или какому-то другому конкретному человеку».

Звучит разумно, но всегда ли эта информация остается в секрете? Недавно журналисты The New York Times выяснили, что Facebook более десяти лет делился данными о своих пользователях с Apple, Samsung, Microsoft, Blackberry и еще более чем с пятью десятками производителей гаджетов, оправдываясь улучшением «пользовательского опыта». Это стало вторым за год скандалом с утечками личных данных из главной социальной сети планеты Земля. Первый скандал, разразившийся весной, касался компании Cambridge Analytica, получившей информацию о 87 миллионах пользователей Facebook и применившей ее для таргетированной рекламы, в том числе во время предвыборной кампании Трампа. Последовавшее падение акций привело к тому, что детище Цукерберга разом обеднело на $13 миллиардов и на время рассталось с мечтой стать первой в мире компанией с капитализацией более одного триллиона долларов. В рамках расследования были обнародованы все средства сбора информации, которые использует соцсеть, но от этого стало только тревожнее.

Оказалось, что Facebook известно об установленных у вас приложениях, операторе связи, интернет-провайдере, скорости передачи данных, ваших Wi-Fi-сетях и Bluetooth-устройствах, уровне заряда батареи, объеме памяти, расположении окон на экране и смартфонах, находящихся поблизости. Более того, в систему «зашита­» даже возможность следить за движением ваших губ (официальная причина – необходимос­ть уметь отличить живого пользователя от бота). Может быть, пора выходит­ь в интернет в масках? Если так, то к ним стоит добавить и темные очки. В этом году Apple купили компанию, занимающуюся разработкой систем слежения за глазами пользователя. Цели вполне безобидные – избавиться от мышки и научить курсор следовать за взглядом, но эта же технология позволит узнавать, на сколько секунд наше внимание привлекает тот или иной предмет на экране, так что и без того толстые досье о наших предпочтениях будут пополнены новыми фактами.

Сегодня данные о каждом человеке, ведущем активную интернет-жизнь, – это тома из тысяч страниц. И именно они – самое ценное, что есть в сети, ведь если в реальном мире журналы и газеты продают информацию вам, то в виртуальном пространстве идет торговля данными о вас.

Обидно сознавать, что наши смартфоны – это жучки, торгующие нашими секретами, но, скорее всего, мы сами превратили их во вражеское оружие. «Как показывает практика, злоумышленникам проще всего взять под контроль то, что либо плохо настроено пользователем, либо содержит уязвимость, – рассуждает Виктор Чебышев. – Мы не читаем пользовательское соглашение и не знаем, на что подписываемся. Скажем, приложению «фонарик» явно не нужен доступ к телефонной книге, но многие просто жмут «Ок» и открывают двери в свой цифровой мир настежь».

Хотим попасть в вашу ленту на [Facebook](https://www.facebook.com/GQRussia)

ПОДПИСАТЬСЯ

«Яндекс» на запрос «Как взломать Wi-Fi?» выдает 48 миллионов ответов, это на 12 миллионов больше, чем по запросу «Как защитить Wi-Fi?». Получается, спрос на цифровую атаку куда выше, чем на оборону от нее. В Америке злоумышленники прямо из машин проверяют сети частных домов и, найдя не защищенные паролем, вторгаются с целью выведать у подключенных к ним устройств данные о кредитных картах. И это не единственный сценарий: были зафиксированы атаки через «умный» телевизор, который вел слежку за помещением, и через видеоняню, с помощью которой преступники общались с детьми.

Попадаются на цифровые удочки не только обычные люди. Известен случай, когда зараженная Wi-Fi-сеть отеля, где регулярно останавливались правительственные делегации и топ-менеджеры крупных компаний, после подключения присылала «обновление ПО», установка которого давала доступ к файлам гостей. Так что стоит десять раз подумать, прежде чем подключаться к неизвестной сети в общественном месте, и сто раз – перед тем, как, находясь в ней, совершать покупки онлайн. Тем не менее, по статистике, 20 % россиян в публичных сетях совершают финансовые операции, а 39 % вводят свои учетные данные для входа на веб-сайты. «Киберпреступникам всегда будут интересны наши деньги, – кивает Чебышев. – Поэтому с новыми приложениями и технологиями, которые каким-либо образом связаны с нашим кошельком, будут появляться и новые угрозы. Недавно мы изучали приложения для каршеринга, и оказалось, что мошенники потенциально могут получить доступ к учетным данным. В Санкт-Петербурге и Москве уже ловили школьников, которые купили краденый аккаунт. Представляете ребенка за рулем автомобиля? По-моему, очень страшно».

Еще страшнее звучат рассказы о кибервойнах между государствами.

Особенно когда эти рассказы касаются ядерных угроз. В этом году исполнилось десять лет с первого такого «удара». В 2008 году компьютерный червь Stuxnet атаковал иранский завод по обогащению урана: на компьютеры операторов выводились данные о штатной работе всех систем, пока установки многократно раскручивались до предельных скоростей и резко останавливались. В итоге ядерная программа страны была отброшена на несколько лет назад, и хотя никаких гуманитарных катастроф не произошло, сам факт удаленного управления ядерным объектом рисует в воображении апокалиптические картины. Не менее пугающе звучит и описание опыта американских программистов Чарли Миллера и Криса Валасека. Пока один из них находился за рулем, второй смог удаленно подключиться к мультимедийной системе автомобиля и через нее перехватить управление. Он заставил бортовой компьютер поверить, что скорость движения в несколько раз ниже, и активировать систему автопарковки (ту самую, когда руль крутится сам). Водителю пришлось на ходу сражаться с «баранкой», которой управлял хакер, и вскоре машина оказалась в кювете. После этого эксперимента автопроизводители озаботились созданием автомобильных антивирусов. Также удаленно можно уничтожить смартфон. «Если в результате атаки был получен привилегированный доступ к устройству, то злоумышленник может сделать все что угодно. Например, сжечь его. У нас такое было в ходе исследования троянца Loapi. Через двое суток от перегрева вздулась батарея», – говорит Чебышев. Вообще возможности удаленного вмешательства в цифровую жизнь растут. Были зафиксированы случаи, когда компьютер перепрограммировался таким образом, чтобы воткнутые в него наушники начинали работать как микрофон. Известны эксперименты, в которых на расстоянии по электромагнитным импульсам отслеживались данные, записываемые на жесткий диск.

Сегодня каждый день Google обрабатывает больше данных, чем было создано человечеством за всю его историю до появления интернета, и по мере переноса все большего числа документов в «цифру» база данных о каждом человеке обрастает все новыми подробностями: налоги, недвижимость, автомобили, авиаперелеты, счета и штрафы образуют огромный массив данных, а так как жесткие диски и флеш-память все время дешевеют, из этих досье никогда не выкинут ни страницы. Более того, их будут пополнять видео с камер наблюдения, среди которых все больше обладающих возможностью ­распознавания лиц. Похоже, в ближайшем будущем станут очень востребованы услуги профессиональных чистильщиков, стирающих нежелательные моменты цифровой жизни, но, чтобы удалить все, им придется повозиться.

# «Лаборатория Касперского» рассказала об уязвимости 60 компьютеров в автомобиле

Около 60 компьютеров установлено в автомобиле, каждый из них теоретически может быть атакован извне, рассказал «РИА Новости» директор по развитию бизнеса «Лаборатории Касперского» Александр Моисеев. «Сейчас, наверное, все крупные физические системы — от заводов и пароходов до автомобилей — управляются компьютерными системами, которые еще и напрямую или опосредованно соединены с интернетом»,— сообщил он

«Как думаете, сколько компьютеров стоит в машине? Шестьдесят в среднем. Каждый чем-то управляет, и каждый теоретически может быть подвержен внешней кибератаке»,— сказал господин Моисеев.

По его словам, компания в настоящее время работает с несколькими автопроизводителями, в первую очередь, в Европе. «Названия, к сожалению, не разглашаем. В первую очередь наши специалисты проводят аудит внутренних устройств автомобилей, насколько они уязвимы»,— сообщил собеседник агентства.

# Интернет вещей оказался под ударом

**Чем вызвана обеспокоенность специалистов МЧС**

30.04.2018

**Чрезвычайные службы предупреждают о грядущих кибератаках на автомобили и бытовые приборы. Уже в ближайшие месяцы может вырасти вероятность массового взлома компонентов интернета вещей. Почему об этом сообщается именно сейчас? И какие последствия грозят пользователям? Об этом — Николай Долгополов.**

Об угрозе вторжения хакеров в личную жизнь через «умные приборы» сообщает Всероссийский центр мониторинга и прогнозирования чрезвычайных ситуаций «Антистихия». При этом самому большому риску, судя по отчету, подвергаются автомобилисты.

Эксперт по информационной безопасности компании «Монитор безопасности» Тарас Татаринов, сообщил, что происходит с машиной, если в систему управления вторгаются хакеры, и рассказал, как они это делают.

«Я сам видел демонстрацию кибервзлома систем управления автомобилем, вплоть до того, что можно было вмешиваться в торможение и вызвать срабатывание подушек безопасности. Если это случится на большой скорости, то, конечно, управлять машиной станет невозможно,— пояснил эксперт.— Хакеры используют уязвимости в программном обеспечении, так что выход в интернет совсем не обязателен. Ведь в автомобиле часто присутствуют и Bluetooth-интерфейс, и точка Wi-Fi-доступа, так что можно через них спровоцировать многие вещи».

[**В чем преимущества быстрого внедрения в бытовые процессы умных устройств**](https://www.kommersant.ru/doc/3592692?from=doc_vrez)

Участники рынка говорят, что кибератаки на уровне интернета вещей — это уже сегодняшний день. Злоумышленники могут использовать бытовые приборы для организации масштабных DDoS-атак, утверждает технический директор компании Check Point Software Technologies Россия-СНГ Никита Дуров. Еще одна актуальная угроза — персональные медицинские приборы, например, кардиостимуляторы, которые поддерживают жизнеспособность пациентов, подчеркивает эксперт.

«Если кардиостимулятор связан с мобильным приложением, в котором можно какие-то параметры заменить, то в случае вмешательства хакеров он будет работать не так, как запрограммировал его врач. Что произойдет тогда с человеком, можно только догадываться. Могут наступить и необратимые последствия,— добавил он.— Появилось много телевизоров, пылесосов, которые подключаются к интернету.

*Обычно с помощью них совершаются DDoS-атаки. Их владелец в таком случае будет просто ее соучастником.*

Он может даже не подозревать о том, что, к примеру, его телевизор отправляет все его персональные данные злоумышленникам».

Разговоры об угрозах со стороны «умных» чайников, утюгов и кофеварок идут уже не первый год. Обычно все ограничивается стандартными рекомендациями не заходить на незнакомые ресурсы и не открывать неизвестные ссылки. Тот факт, что к обсуждению подключилось МЧС, говорит о переходе проблемы на новый качественный уровень, констатирует аналитик компании «Финам» Леонид Делицын.

[**Как использовать интернет вещей для предупреждения природных катаклизмов**](https://www.kommersant.ru/doc/3591185?from=doc_vrez)

«Ближайшие годы станут временем кибервойн и активизации хакеров. Сейчас интернет вещей — это, в первую очередь, транспорт, то есть сфера, вообще говоря, связанная с деятельностью МЧС. Эта индустрия, в которой случаются катастрофы, большие потери. Представим себе, что кто-то вывел из строя спутниковые системы: такси, грузовики едут не туда, поезда вообще вылетают с ЖД-веток. То есть урон может быть большой»,— отметил Леонид Делицын.

По мнению экспертов, заявления МЧС, в первую очередь, сыграют на пользу разработчикам. Некоторые уже объявили, что готовят продукты по кибербезопасности автомобилей и интернета вещей. Объем этого сегмента рынка может в ближайшее время вырасти на 5%, в денежном выражении это порядка 4 млрд руб.

*По данным МЧС, за минувший год число хакерских атак на российские информационные объекты увеличилось более чем в четыре раза.*

# Восемь угроз: чем опасны Facebook, Google, Amazon и Apple

**17 апреля 2018 Морис Стаки**

«Бесполезно пытаться победить в избирательной гонке, оперируя лишь фактами, — [заявил](https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation) управляющий директор Cambridge Analytica работавшему под прикрытием репортеру, — потому что это вопрос эмоций».

Чтобы прицельно воздействовать на американских избирателей, апеллируя к их надеждам, неврозам и страхам, этой консалтинговой фирме требовалось обучить алгоритм прогнозировать их поведение и составлять их психологические портреты. Для этого им было нужно большое количество персональных данных. Для составления этих психографических профилей Cambridge Analytica пригласила профессора Кембриджского университета, чье приложение собрало данные 50 млн пользователей Facebook и их друзей. В то время социальная сеть позволяла разработчикам приложений собирать такого рода информацию. Facebook утверждает, что Cambridge Analytica и сотрудничавший с ней профессор нарушили правила соцсети по работе с данными. Однако подобное нарушение произошло [не в первый раз](https://www.wsj.com/articles/facebooks-lax-data-policies-led-to-cambridge-analytica-crisis-1521590720?mod=ITP_pageone_0&tesla=y) — и, вероятно, не в последний.

Этот скандал разразился вслед за попытками из России, используя Facebook, Google и Twitter, «[посеять раздор](https://www.justice.gov/file/1035477/download) в политической системе США, включая президентские выборы в США 2016 года». Он способствовал увеличению недоверия к современным технологическим гигантам и росту беспокойства о масштабе их влияния.

Одна из причин этого влияния — данные. Facebook, Google, Amazon и аналогичные компании являются информационными монополистами, контролирующими крупные платформы, которые, как коралловый риф, привлекают в свою экосистему пользователей, продавцов, рекламодателей, производителей ПО, приложений и аксессуаров. Apple и Google, к примеру, контролируют популярные мобильные операционные системы (и основные приложения для них), Amazon — крупнейшую торговую платформу, а Facebook — крупнейшую социальную сеть. Через эти платформы проходят разнообразные данные большого объема, а скорость получения и применения этой персональной информации позволяет монополистам усиливать свое влияние на рынке.

Правильно ли, что несколько компаний располагают таким количеством данных и имеют такое влияние? Антимонопольные органы США, по-видимому, не имеют однозначной позиции по информационным монополиям. «Данные бесплатны, — думают многие, — какой может быть вред от их сбора?» Но подобные рассуждения ошибочны. Информационные монополии создают огромные риски для потребителей, работников, конкуренции и благосостояния демократии в целом. Ниже я объясню, почему это так.

**Почему антимонопольные органы США не волнуют информационные монополии**

Ряд европейских антимонопольных служб недавно предъявил иски четырем компаниям: Google, Apple, Facebook и Amazon. Европейская комиссия, к примеру, [оштрафовала](http://europa.eu/rapid/press-release_IP-17-1784_en.htm) Google на рекордные €2,42 млрд за использование монопольного положения на рынке поисковых систем при продвижении своего сервиса для шопинга. Комиссия также предварительно заключила, что Google злоупотребляет своим доминирующим положением в отношении мобильной операционной системы [Android](http://europa.eu/rapid/press-release_IP-16-1492_en.htm) и сервиса контекстной рекламы [AdSense](http://europa.eu/rapid/press-release_IP-16-2532_en.htm). Антимонопольные органы Германии сделали предварительный [вывод](http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html), что Facebook злоупотреблял доминирующим положением, «сделав обязательным условием пользования социальной сетью согласие на неограниченный сбор данных, созданных в результате посещения пользователем сторонних сайтов, и их привязку к его учетной записи».

Вероятно, в ближайшие несколько лет мы увидим еще больше штрафов и других методов воздействия от европейских регуляторов. В США, однако, информационным монополистам в основном удавалось избежать расследований со стороны антимонопольных органов как при администрации Барака Обамы, так и Джорджа Буша-младшего. Примечательно, что Европейская комиссия признала преференции в поисковой выдаче Google антиконкурентной практикой, а Федеральная торговая комиссия США — нет. Начиная с 2000 года, Министерство юстиции США возбудило всего один иск по делу о монополизации. (Для сравнения — за период 1970–1972 гг. было возбуждено [39 гражданских и 3 уголовных дела](https://www.justice.gov/atr/antitrust-division-workload-statistics-fy-1970-1979)против монополий и олигополий).

Действующий глава антимонопольного подразделения министерства юстиции США [признал](https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-college-europe-brussels) отличия в антимонопольном контроле между США и Европой. Он отметил, что его организация испытывает «особенное беспокойство в отношении цифровых рынков». Но в отсутствие «наглядного ущерба конкуренции и потребителям» министерство «не желает налагать взыскания на цифровые платформы, так как это может задушить инновации, которые и способствуют росту конкуренции в интересах потребителей».

Подобное расхождение в контроле соблюдения антимонопольного законодательства может отражать различия взглядов на ущерб, который способны нанести информационные монополисты. Обычно ущерб от монополий выражается в росте цен, уменьшении количества товаров или ухудшении их качества. На первый взгляд, информационные монополии практически не способны нанести подобный ущерб. В отличие от, скажем, фармацевтических компаний они не могут установить неоправданно высокую цену на свою продукцию. Большинство продуктов, которые предоставляют Google и Facebook, формально бесплатны, а рост информационных монополий ведет к повышению качества их услуг. Чем больше людей пользуются поисковой системой, тем лучше ее алгоритмы обучаются предпочтениям пользователей и тем более релевантные результаты она выдает. Это, в свою очередь, привлекает новых пользователей, и положительный эффект сохраняется.

Как [считал](http://articles.chicagotribune.com/2012-04-06/opinion/ct-perspec-0405-bork-20120406_1_unpaid-search-results-search-engines-search-algorithms)Роберт Борк (Роберт Борк работал [генеральным солиситором США](https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%81%D0%BE%D0%BB%D0%B8%D1%81%D0%B8%D1%82%D0%BE%D1%80_%D0%A1%D0%A8%D0%90) в 1973—1977 годах, позднее был советником компании Google, скончался в 2012 году — ***прим. ред.***), «поисковые системы вроде Google невозможно однозначно обвинить в монополизации, так как они бесплатны для пользователей, и те могут в любой момент переключиться на альтернативу».

**Какой вред наносят информационные монополии**

Повышение цен — это не единственный способ, которым влиятельные компании могут нанести ущерб своим потребителям и всему обществу. При более [близком рассмотрении](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144045) можно заметить, что информационные монополии потенциально могут нести, по меньшей мере, восемь угроз.

**Продукты худшего качества и меньшая информационная безопасность.**Антимонопольные органы все чаще признают, что компании могут конкурировать за счет приватности и защиты данных. Но в отсутствие конкурентов монополисты не чувствуют необходимого давления и могут *меньше* заботиться о защите персональных данных и собирать *больше*личной информации, чем в условиях здоровой конкуренции. Сбор слишком большого количества персональных данных можно считать эквивалентом слишком высокой цены. Кроме того, компании могут не раскрывать, *какие*данные собирают и *как*будут их использовать. Они не испытывают давления со стороны конкурентов, чтобы менять непрозрачную политику конфиденциальности. Даже если они улучшат положение о конфиденциальности, ничего не изменится. Распространенная сегодня концепция согласия на использование данных по факту уведомления со стороны сервиса бессмысленна в условиях отсутствия реальных конкурентов и из-за неравных рыночных позиций.

**Слежение и риски безопасности.** На монополизированном рынке персональные данные сконцентрированы в руках нескольких компаний. Возможности потребителей получить более качественную защиту конфиденциальности ограничены. Это повышает дополнительные риски, среди них:

**— Поглощение государством.** Чем меньше число компаний, контролирующих персональные данные, тем выше потенциальный риск, что государство поглотит ту или иную организацию. Компаниям многое нужно от государства, а государству часто нужен доступ к данным. Когда ими располагают всего несколько компаний, растет вероятность, что компании начнут тайно сотрудничать с правительством и предоставлять доступ к персональной информации. Так, к примеру, Китай использует информационные монополии, чтобы [следить за своим населением](https://www.wsj.com/articles/internet-tightens-popular-chinese-wechat-app-to-become-official-id-1514541980).

**— Скрытый контроль.** Даже если государство не может поглотить монополию, ее сокровищница данных побуждает обойти защиту и воспользоваться ими все равно. Даже если правительство не может заключить сделку и получить прямой доступ, оно может сделать это тайно.

**— Последствия нарушения политики конфиденциальности/кражи данных.** У монополистов больше стимулов предотвращать кражу информации, чем у обычных компаний. Но когда большое количество персональных данных сконцентрировано в руках нескольких игроков, у хакеров, маркетологов, политических консультантов и других заинтересованных лиц появляется еще больший стимул найти способ обойти меры безопасности наиболее влиятельного игрока. Концентрация данных означает, что, если безопасность нарушена, ущерб будет на порядок выше, чем если бы жертвой оказалась обычная компания. Несмотря на негодование потребителей, у компании, занимающей доминирующее положение, меньше причин беспокоиться, что ее клиенты уйдут к конкурентам.

**— Получение выгоды информационными монополистами.** Даже когда их продукты формально «бесплатны», монополии могут извлекать значительную выгоду путями, которые были бы им недоступны в условиях здоровой конкуренции.

Во-первых, они получают персональные данные пользователей, не платя за них справедливую рыночную цену. Собранные данные могут стоить гораздо больше, чем предоставление «бесплатных» услуг. Тот факт, что сервис является «бесплатным», не означает, что мы получаем справедливую компенсацию за наши данные. Таким образом, у монополистов есть сильный экономический стимул сохранять статус-кво, при котором пользователи, как [выразились](https://www.technologyreview.com/s/517356/if-facebook-can-profit-from-your-data-why-cant-you/) авторы MIT Technology Review, «плохо понимают, сколько персональных данных они предоставили, как они используются и сколько стоят». Владея этой информацией и имея альтернативы, люди могли бы потребовать компенсацию.

Во-вторых, нечто аналогичное может произойти с создаваемым пользователями контентом. Монополисты могут извлекать выгоду, бесплатно присваивая результаты творческой деятельности пользователей. На конкурентном рынке пользователи могли бы потребовать компенсацию не только за свои данные, но и за контент, который они размещают на YouTube и Facebook. В отсутствие реальных альтернатив они не могут этого сделать.

В-третьих, информационные монополии могут получать прибыль от продавцов услуг. Например, они [заимствуют](http://graphics.wsj.com/google-ftc-report/) ценный контент у фотографов, авторов, музыкантов и веб-сайтов и используют его на собственной платформе. В этом случае монополии получают выгоду за счет других участников цепочки создания ценности.

В-четвертых, монополисты могут зарабатывать на пользователях косвенным образом, когда высокая стоимость их рекламных услуг закладывается в стоимость рекламируемой продукции. Если бы информационные монополии имели больше конкурентов на этом рынке, реклама стоила бы меньше — как и товары их клиентов.

Наконец, монополисты могут получать выгоду как от продавцов товаров и услуг, так и от покупателей, способствуя так называемой [«поведенческой дискриминации»](https://ora.ox.ac.uk/objects/uuid:a0d72ab9-0b42-4351-8696-366259ce508b), форме ценовой дискриминации, основанной на прошлом поведении потребителя — например, на его истории просмотров в браузере. Они могут использовать персональные данные, чтобы заставить людей покупать то, в чем они на самом деле не нуждаются, — по самой высокой цене, которую они готовы заплатить.

По мере того как информационные монополии расширяют размеры своих платформ и включают в них цифровых персональных помощников, интернет вещей и умные технологии, растет беспокойство, что с помощью полученных данных они повысят свое конкурентное преимущество и влияние на рынке. В результате их прибыль увеличится за наш счет.

**Утрата доверия.** Рыночная экономика опирается на доверие. Чтобы онлайн-рынки приносили пользу, люди должны доверять компаниям и тому, как они используют персональные данные. Но по мере развития технологий и увеличения объема предоставляемой нами личной информации мы все лучше понимаем, что влиятельные организации используют ее для своей, а не нашей выгоды. Когда монополии снижают уровень защиты конфиденциальности данных ниже конкурентного уровня, некоторые потребители, как отмечает [Антимонопольная служба Великобритании](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf), предпочитают «не делиться данными, ограничивать количество предоставляемой информации или даже предоставлять ложные данные». Потребители могут воздерживаться от услуг технологических компаний, которыми воспользовались бы в условиях здоровой конкуренции. Это пример того, что экономисты называют общественными издержками монополии. Иначе говоря, с утратой доверия ухудшается общее благосостояние общества.

**Значительные затраты третьих сторон.** Информационная монополия, под контролем которой находится та или иная ключевая платформа, например, мобильная операционная система, может легко устранить конкурентов следующими способами:

**—** Подталкивать пользователей и рекламодателей к приобретению собственных продуктов и услуг в ущерб фирмам-конкурентам, которые пользуются их платформой (и вопреки желаниям потребителей).

**—**Снижать функциональность независимых приложений.

**—** Уменьшать трафик независимых приложений, занижая их позицию в поисковой выдаче и магазине приложений.

Информационные монополии могут также причинять финансовый ущерб компаниям, стремящимся защитить нашу конфиденциальность. В написанной мной вместе с Ариэлем Эзрахи книге «Virtual Competition» мы, помимо прочего, рассказываем о том, как Google выкинула приложение «Disconnect», предназначенное для защиты персональных данных пользователей, из своего магазина Android-приложений.

**Меньше инноваций на рынках, где доминируют монополии.**Информационные монополисты могут тормозить инновационный процесс, используя инструмент, которого не было у монополий раньше. Мы с Алленом Грюнсом называем его «радаром для краткосрочных прогнозов». В нашей книге «Big Data and Competition Policy» мы описываем то, как преимущества при получении и анализе данных, которые есть у ряда платформ, позволяют им раньше других распознавать потребительские тренды. Монополии могут пользоваться этим преимуществом, чтобы понять, какие продукты или услуги набирают популярность, и с помощью своего «радара» уничтожать эти зачатки конкуренции.

**Социальные и моральные проблемы.**Антимонопольные органы не раз беспокоились о том, как монополии могут препятствовать индивидуальной автономии граждан. Информационные монополии тоже вредят индивидуальной автономии. Они могут определять (и ограничивать) возможности, которые доступны стартапам, пользующимся их суперплатформой. Это влияет на работу сторонних продавцов, пользующихся платформой Amazon для поиска потребителей, газеты и журналисты, которые используют Facebook и Google, чтобы привлекать более молодых читателей, а также, как [говорится](http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740) в деле, возбужденном Европейской комиссией против Google, компании, чей трафик зависит от механизмов этого поисковика.

Но вопрос автономии касается не только разработчиков приложений, продавцов, журналистов, музыкантов, писателей, фотографов и художников, которые полагаются на информационные монополии, чтобы установить контакт с пользователями. Речь идет об автономии каждого. В январе хедж-фонд Jana Partners совместно с пенсионным фондом учителей штата Калифорния [потребовал](https://hbr.org/2018/01/why-an-activist-hedge-fund-cares-whether-apples-devices-are-bad-for-kids) от компании Apple прилагать больше усилий к устранению отрицательного влияния ее устройств на детей. Как [заметил](https://www.economist.com/news/briefing/21735026-which-antitrust-remedies-welcome-which-fight-techlash-against-amazon-facebook-and)журнал The Economist, «у вас проблемы, если компания с Уолл-стрит рассказывает вам о морали». Общественность беспокоит, что продукты технологических монополистов разработаны специально, чтобы вызывать привыкание, и лишают людей способности делать свободный выбор.

Отметим интересный контраргумент, касающийся взаимодействия монополий и конкуренции. С одной стороны, на монополизированных рынках у потребителей меньше выбор, поэтому, возможно, у компаний есть меньшая необходимость вызывать у них привыкание. С другой стороны, монополисты вроде Facebook и Google, даже не имея сильных конкурентов, могут повысить свою прибыль, увеличив время нашего взаимодействия с их продуктами. Это может служить стимулом для информационных монополий использовать особенности человеческого поведения и слабую силу воли, чтобы вызывать привыкание пользователей — будь то просмотр роликов на YouTube или публикация фотографий в Instagram.

**Политические проблемы.** Экономическое влияние часто переходит в политическое. В отличие от монополий доцифровой эпохи, информационные монополии, учитывая формат их взаимодействия с людьми, обладают более мощным инструментом: способностью влиять на общественное мнение и представления о правильном и неправильном.

[Многие](http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/)получают сегодня новости через соцмедиа. Однако соцмедиа не просто пассивно передают новости. Технологические компании могут влиять на наши мысли и чувства. Например, компания Facebook в рамках исследования [«заразительности эмоций»](http://www.pnas.org/content/111/24/8788.full) манипулировала чувствами 689 003 пользователей, внося изменения в их новостную ленту. Другие подобные риски включают:

**— Предвзятость.**Фильтруя информацию, получаемую нами на основе наших предпочтений, монополии могут ограничивать количество мнений, которые мы получаем, что ведет к возникновению так называемых «эхо-камер» и «информационных пузырей».

**— Цензура.** Монополии могут с помощью своих платформ контролировать или блокировать контент, получаемый пользователями, и осуществлять цензуру политической или религиозной информации.

**— Манипуляции.** Монополии могут продвигать истории, рекламирующие их деловые или политические интересы, но не соответствующие интересам пользователей.

**Ограничение влияния информационных монополий**

При более подробном рассмотрении может оказаться, что информационные монополии более опасны, чем обычные монополии. Они могут влиять не только на наши кошельки, но и на частную жизнь, автономность, демократию и благосостояние.

Совсем не обязательно, что рынки, где доминируют эти компании, скорректируются самостоятельно. Сетевой эффект, высокие затраты на смену поставщика услуг для потребителей (учитывая невозможность переноса данных и отсутствие у пользователей прав на свою информацию) и слабая защита конфиденциальности помогает монополиям сохранять свое доминирующее положение.

К счастью, на помощь может прийти международный антимонопольный контроль. Администрация Рональда Рейгана в свете популярных в те времена идей Чикагской школы экономики скептически относилась к волнениям, связанным с монополиями. Верховный суд, опираясь на неверную экономическую аргументацию, [постановил](https://www.law.cornell.edu/supct/html/02-682.ZO.html), что монопольные цены являются «важным элементом свободного рынка». С [подъемом](https://hbr.org/2017/12/the-rise-fall-and-rebirth-of-the-u-s-antitrust-movement)прогрессивной антимонопольной Новой Брандейской школы маятник качнулся в обратную сторону. В ситуации роста информационных монополий эти перемены не могут не радовать.

Тем не менее, хотя глобальный контроль соблюдения антимонопольного законодательства является необходимым инструментом сдерживания, одного его недостаточно. Антимонопольные органы должны координировать свои действия с органами защиты потребителей, чтобы обеспечить необходимые условия для эффективной конкуренции за конфиденциальность и инклюзивность экономики.

**Об авторе.** **Морис Стаки** — сооснователь Konkurrenz Group, профессор юриспруденции в университете Теннеси.

# За нами следят

 «За нами следят»: что знают о пользователях интернет-компании и сколько стоит такое знание

**12 января 2018 Натали НахайТомас Чаморро-Премузик**

Ходят [слухи](https://www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook), что Марк Цукерберг закрывает камеру и микрофон своего ноутбука. Как пишет Антонио Гарсиа Мартинес в своей новой провокационной книге Chaos Monkeys, посвященной основателю Facebook, «первыми с тонущего корабля бегут не крысы, а члены команды, умеющие плавать». Эндрю Гроув, один из основателей компании Intel и пионеров Кремниевой долины, высказался примерно в том же духе: «Выживают только параноики».

Во времена, когда люди проводят больше времени онлайн, чем офлайн, мы производим море личных данных, и мысли о хакерах и кибербезопасности преследуют нас как никогда прежде. Когда-то «личное» означало «конфиденциальное», но не сегодня, когда наши персональные и интимные отношения (и генерируемые ими данные) развиваются в интернете, который становится все более публичным местом. Даже когда на нас никто не смотрит, мы редко остаемся в одиночестве.

Что если бы у вас появился шанс выкупить все данные, оставленные вами в интернете с первой минуты выхода онлайн и до сегодняшнего дня? Сколько бы вы заплатили? Что бы вы отдали ради 100% безопасности? Прежде чем ответить, подумайте о следующих издержках.

**1. Больше никаких «бесплатных» услуг.** Всем известны слова Эндрю Льюиса с сайта [MetaFilter](http://www.metafilter.com/user/15556): «Если вы не платите, то вы не потребитель, а продукт, который продается». Но что если провайдеры электронной почты, социальные сети и даже поисковые серверы, которыми мы пользуемся каждый день, перестали бы быть бесплатными? Мы можем жаловаться на отсутствие конфиденциальности и быстрое проникновение в личное пространство поставщиков подобных услуг, однако широко распространенных альтернатив, по-видимому, не существует.

Дело не в отсутствии идей. Новаторы в области технологий предлагают альтернативные бизнес-модели, например, [Джарон Ланье](http://www.niemanlab.org/2013/05/jaron-lanier-wants-to-build-a-new-middle-class-on-micropayments/) предложил использовать персональные микроплатежи для вознаграждения пользователей, предоставляющих данные. Представьте себе, что вы будете получать небольшой платеж за каждое отправленное письмо или сообщение по Whatsapp — может ли такое решение помочь избежать избытка информации? Другим вариантом, конечно, может стать подписка на сервисы, такие как Facebook, плата за которую будет гарантировать конфиденциальность данных пользователей и заменит продажу данных в рекламных целях.

Проблема заключается не столько в технической стороне вопроса, сколько в психологической: в неосязаемости наших данных и их воспринимаемой ценности. Для большинства из нас «бесплатные» услуги, которыми мы пользуемся онлайн, позволяют удовлетворить конкретную потребность — связаться с другими людьми. Общаясь по электронной почте, в групповых чатах или социальных сетях, мы производим данные, которые не только неосязаемы, но и ценность которых среднестатистическому потребителю сложно понять и оценить. Большинство людей содрогнутся при мысли, что чужой человек придет к ним домой и начнет просматривать фотоальбомы, банковские выписки и личные дневники, однако многие и глазом не моргнут, когда нечто подобное произойдет онлайн, вероятно, потому, что в этом случае вторжение и его последствия менее заметны. Только столкнувшись с конкретным сценарием, таким как утечка данных (номера кредитной карты или личных фотографий), мы начинаем понимать, чем грозит в реальном мире наши действия в онлайне.

Если говорить о социальных сетях, то даже когда люди понимают риски и беспокоятся о конфиденциальности, они все равно редко придерживаются защитной [стратегии поведения](https://dl.acm.org/citation.cfm?id=2166524). Они все чаще сетуют на нарушение конфиденциальности, но продолжают публично раскрывать данные о себе и позволяют компаниям беспрецедентный доступ к ним, что ведет к «парадоксу конфиденциальности». Если коротко, такое поведение свидетельствует о том, что люди на деле не так сильно беспокоятся о конфиденциальности, как на словах. Им нравится сама идея, но, по-видимому, они не настолько ценят свои данные, чтобы предпринимать конкретные шаги по их защите. Справедливости ради следует отметить, что такое несовпадение отношения и поведения наблюдается во всех областях жизни. Например, большинство людей ценит свое здоровье и отношения, однако ведет себя так, что регулярно рискует и тем, и другим, даже когда осознает потенциальные последствия.

**2. Больше никакой персонализации.** При взаимодействии в интернете мы привыкли к некоторой степени соответствия результатов поиска и онлайн-услуг или продуктов нашим персональным характеристикам и контексту. Один из руководителей Alphabet Эрик Шмидт давно отмечал, что в отличие от традиционных СМИ интернет занимается «узким вещанием». Персонализация не выражена явно, и мы начинаем понимать, насколько скорректированы именно под нас сервисы (например, поиск по картам Google, реклама, которую мы видим в YouTube или Facebook), только когда меняем настройки приватности или стираем cookies и историю поиска.

Мы так привыкли к легкости и удобству, что не спешим отказываться от них в пользу более конфиденциальных (но и более неэффективных) методов. Конечно, можно отключить настройки геолокации для приложения вызова такси, чтобы оно перестало отслеживать каждый ваш шаг, но тогда каждый раз, когда вы захотите воспользоваться им, придется вручную вводить свое местоположение, то есть тратить слишком много сил ради конфиденциальности.

Конечно, у персонализации есть и оборотная сторона, например, когда вы начинаете получать на разных платформах (в социальных сетях, сервисах ТВ по запросу и по цифровом радио) рекламу продукта или услуги, которую искали, но не подозревали, что вас отслеживают. Этот «пугающий фактор» — ощущение, что каждый ваш шаг, публичный и приватный, отслеживают, анализируют его и извлекают из него выгоду — может привести к ситуации, известной как [психологическое сопротивление](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4675534/). Если нам кажется, что мы теряем свободу или она находится под угрозой, желание восстановить ее может заставить людей воспротивиться социальному влиянию: у пользователя возникнет ощущение насилия над собой, и репутация компаний, надеявшихся с помощью персонализации увеличить доходы, будет запятнана.

**3. Больше никакого мгновенного удовлетворения запросов.** Данные, которые мы производим в ходе повседневных взаимодействий, также можно использовать для разработки сервисов, пользующихся нашим желанием получать то, что нам нужно, немедленно и в удобном формате. Мы живем в век, когда только мгновенное удовлетворение запроса считается достаточно быстрым. Учитывая наши ограниченные возможности удерживать внимание, на рынке, уже страдающем из-за нехватки времени и внимания у потребителей, сервисы, предлагающие мгновенные решения, не только обеспечивают ощущение немедленного удовлетворения запроса, но и могут более эффективно добиться того, чтобы клиент серьезно не задумывался. Когда, например, вы в последний раз читали условия использования загружаемого приложения? Иными словами, когда мы подписываемся на новую услугу, стремление к удобству часто перевешивает рациональные рассуждения, и мы соглашаемся на использование наших данных такими способами, которых не могли даже представить. Стремясь потратить как можно меньше времени и умственных усилий, возможно, мы обрекаем себя в будущем на значительный риск в виде утечки персональных данных или отказа в определенных [медицинских](https://gizmodo.com/23andme-is-selling-your-data-but-not-how-you-think-1794340474) или финансовых услугах в связи с выводами, сделанными о нас на основе цифрового следа.

Как нам кажется, нам следует ожидать гораздо большего в обмен на конфиденциальность. Между количеством раскрываемых нами данных и получаемыми услугами должно быть больше симметрии. Например, рекомендательные сервисы должны действительно помогать находить то, что нам нужно, даже если мы не знали, чего хотим. До некоторой степени это реализуется в области музыки и кино, но не когда речь идет о покупках. Аналогично те же данные, что собираются в рекламных целях, могут использоваться для более точного предложения вакансий, так как они указывают на множество психологических качеств, которые десятилетиями связывают с карьерными результатами. Например, если ваши предпочтения на Netflix или Spotify показывают, что вы любознательный или творческий человек, алгоритм поиска работы может предложить вам вакансии, где требуется любознательность и творческий подход. И самое главное: ни один из этих сервисов не должен предлагаться без согласия потребителя, эти сервисы должны объяснять, как и зачем они используют наши данные. Мы заслуживаем право знать, какие выводы делаются из наших данных и насколько они точны.

**Об авторах. Натали Нахай** — лектор и автор бестселлера Webs of Influence: The Psychology of Online Persuasion». Ее лекции, статьи и подкасты посвящены цифровому применению бихевиоризма. **Томас Чаморро-Премузик** — профессор психологии бизнеса в Лондонском университетском колледже и Колумбийском университете, участник Entrepreneurial Finance Lab Гарвардского университета, гендиректор Hogan Assessment Systems.

# Взлом смартфонов

Российские силовые структуры закупили программное и аппаратное обеспечение, которое позволяет взламывать любые смартфоны на базе **Android** и все модели **iPhone**. Об этом пишет [«Русская служба Би-би-си»](http://www.bbc.com/russian/news-43298602), ссылаясь на информацию с сайта госзакупок.

ФСБ, МВД и Следственный комитет закупили инструменты **UFED**, разработанные израильской компанией **Cellebrite**. По неофициальной информации, именно специалисты Cellebrite в 2016 году помогли ФБР [обойти защиту iPhone](https://www.igromania.ru/news/59770/FBR_vzlomalo_iPhone_prestupnika_bez_pomoschi_Apple.html). В среднем региональные управления силовых ведомств потратили на покупку оборудования для взлома мобильных устройств по одному миллиону рублей.

Cellebrite утверждает, что UFED позволяет обойти блокировку старых смартфонов за несколько минут, а для взлома новых моделей понадобится несколько дней. Инструменты можно использовать для получения всех хранящихся на смартфоне данных, включая SMS и переписку в мессенджерах.

# Эксперт по ИТ-безопасности Игорь Ашманов: заклейте камеру телефона!

Статья из газеты: [Еженедельник "Аргументы и Факты" № 10 07/03/2018](http://www.aif.ru/gazeta/number/37185)

Как следит за вами смартфон и почему тесты в соцсетях проходить опасно, рассказывает известный эксперт по ИТ-безопасности Игорь Ашманов.

Игорь Ашманов.

**— Говорят, что вся техника с камерами — ноутбуки, планшеты, телефоны — следит за нами, снимает фото и видео, когда ей вздумается. Это правда?**

— Да. Не зря **Марк Цукерберг**, основатель сети Фейсбук, технически очень продвинутый человек, заклеивает камеру своём ноутбуке скотчем— и начал делать это еще 7 лет назад! Ваш телефон всегда вас «слушает», всегда определяет ваше местоположение, и постоянно смотрит в камеру на вас — даже когда, казалось бы, не активен. При этом телефон понимает, если снимок сделан в кармане, и на экране темно. Снимки же с лицами, людьми, какие-то ситуациями аппараты отправляют на «центральные сервера» — кто выгодоприобретатели этой информации, можно только предполагать... К данным с аппаратов с ОС Андроид имеют доступ не только производители телефона, но и АНБ, которому владелец ОС обязан отдавать данные по закону.

**— Выходит, нужно выключать телефон, когда им не пользуешься?**

— Это не поможет. Надо понимать, что каналов слежки много. Надо стараться не совершать ничего компрометирующего. Потому что даже если вы считаете, что телефон выключен, далеко не факт, что это так. Гарантия отключения — съем батареи с аппарата. Почти все современные телефоны имеют несъёмную батарею. С выключением тоже не всё просто: аппарат может проигрыватьт вам анимацию выключения и гасить экран — но оставаться активным. Есть другой вариант, как осложнить слежку — купить «бабушкофон» вроде Нокии-6610 и не пользоваться смартфонами.

**— Вы известный эксперт в области цифровой безопасности — покажите, а какой у вас телефон?**

— Я не эксперт, извините. У меня — один из последних корейских смартфонов. И камера не заклеена, вот, смотрите. Прослушка и слежка несёт непосредственный риск для людей, которые имеют дело с какими-то тайнами. Это чиновники, представители спецслужб, крупные бизнесмены и преступники. Сервера же собирают массивы данных, не выделяя из них конкретно меня как личность (пока). Скорее всего, производитель телефона и АНБ не следят за личными перипетиями моей жизни. В любом случае я стараюсь не использовать телефон в специфических ситуациях: на переговорах, в сауне, спальне и т.п.

**— То есть бояться, что чья-то жена узнает об измене, потому что за мужем следит телефон, не стоит?**

— Ну, у жены обычно нет доступа к данным, которые смартфон отправил в США. Жене проще взять мужнин смартфон и прочитать, о чем и с кем он там переписывается. А вот тем спецслужбам, кто собирает данные, шантажировать мужа, конечно, можно. Если муж того стоит (он большая шишка, например)

[](http://static1.repo.aif.ru/1/b1/1032838/af683754d8a5712769f2874750fbcb18.jpg)

**Шифрование не работает?**

**— Говорят, мессенджеры (Телеграм, Вотсап, Вайбер — ред.) шифруют информацию — и в отличие от смс и электронной почты они безопаснее. Это так?**

— Не уверен. Этого никто не может знать доподлинно. Это же маркетинг. Надежный ли алгоритм шифрования, на чьих серверах и в каком виде хранится ваша переписка? Простой пример: знаете, что публичная почта (например, Гугла) «читает» содержимое ваших писем? Она предлагает вам рекламу того, о чём шел разговор в письмах. А Гугл по закону обязан отдавать данные разведке. Аналогично устроены все коммуникационные сервисы: конечно, читают не живые люди, а искусственный интеллект с лингвистическим анализом. А операционная система Windows-10 в изначальной поставке имеет встроенного клавиатурного шпиона, который все ваши нажатия клавиш отправляет в Майкрософт.

**Берегите детей**

**— Многие выкладывают в соцсетях фото детей, отмечают свое местонахождение — насколько это безопасно?**

— В нашей семье был такой опыт — у жены похитили сына. Все, кому не лень, тогда сообщали, что он выкладывал о себе все в соцсетях. И хотя это было не так, а сына украли по наводке, мы к информации о детях в цифровом пространстве относимся крайне нервно, и дочерям подобного не позволяем. Если в сети можно посмотреть, как выглядят наши дети и где они бывают — это значит, потом их можно будет узнать на улице, в парке, песочнице.

**— В соцсетях постоянно расшаривают тесты: каким вы будете в старости, какая вы собака... При этом для получения результата нужно предоставить доступ к данным профиля. Это безопасно?**

— Выкачать публичный профиль можно и внешними программами. Опасность тестов, на мой взгляд, в другом. Это массовая дрессировка людей, натаскивание их на выполнение чего-то по команде. Механизм прост: большинству людей не хватает внимания к себе, а тут из говорят, что ты талантливый кулинар или похож на знаменитость. Приятно! Какое ты животное, кем ты был в прошлой жизни — миллион идиотских результатов, которыми все делятся с друзьями. Дрессировка состоит именно в «поделиться». Такой же смысл несут флэшмобы: облей себя водой, или напиши, как тебя изнасиловали. Так тренируют бездумное массовое поведение, как у леммингов. Мне говорят — я делаю: все побежали, и я побежал. Тот, кто собирает массовые данные, ставит пометку: вот эти пользователи склонны вестись на массовые действия. Работа такая же, по сути, как в «группах смерти» (которые далеко не самое страшное, что сейчас есть в сети). Дрессированным массам людей можно подкидывать задания всё сложнее, и они охотно их выполнят.

**— Вы сказали, есть что-то страшнее «групп смерти». Что?**

— группы блатной романтики АУЕ, группы романтизации школьных расстрелов (по-английски «скулшутинга»). На самом деле, вот такая кибербезопасность должна волновать и семью, и государство в первую очередь. Когда пароль украли — это полбеды. А вот когда украли мозги — это гораздо хуже. Манипуляторов в сети сейчас тысячи, и они становятся все изощреннее. Проверяйте, чем занимаются в интернете ваши дети, в каких группах с км они общаются, какие задания выполняют — это может спасти им жизнь.

# Присмотритесь к кофеварке. Возможно, именно сейчас она передает хакерам ваши личные данные

13 февраля 2018

Как защититься от мошенников Интернет вещей

Александр Лямин, генеральный директор Qrator Labs, рассказывает, в чем слабые места IoT-устройств и чем они могут быть опасны именно для вас.

К 2020 году количество IoT-устройств достигнет 50 миллиардов

Электронные устройства, «общающиеся» друг с другом через облака, умные дома, интеллектуальные промышленные системы – все это становится нашей новой реальностью. В далекие 90-е первой вещью, которая смогла подключиться к интернету, стал самый обыкновенный тостер в исполнении Джона Ромки.

Спустя почти 30 лет число вещей класса Internet of Things превысило население планеты: количество умных устройств в 2017 году (с учетом гаджетов) составило, по оценке Juniper Research, порядка 15 миллиардов.

К 2020 году, по прогнозам Cisco IBSG, количество вещей, подключенных к интернету, достигнет 50 миллиардов. Иными словами, на одного жителя планеты будет приходиться по шесть smart-вещей.

«Умные» машины уже фактически окружают нас. Они работают и в быту, и в бизнесе, и в промышленности: чайники, телевизоры, фоторамки, подключенные к сети, – это лишь верхушка айсберга.

Класс устройств IoT сулит нам светлое будущее с автоматизацией процессов, сокращением материальных затрат и экономией времени, однако вводимые новшества добавляют серьезные проблемы с безопасностью.

Более 70% устройств IoT имеют «дыры» в прошивке

Как шутят безопасники, S в аббревиатуре IoT означает Security. Как можно заметить, безопасность в Internet of Things отсутствует так же, как и буква S. Объяснение простое: класс IoT нацелен на простого пользователя, разрабатываются эти устройства супербыстро, по минимальной цене и с минимальной маржой, поэтому времени и желания, задуматься о безопасности у производителя умных решений попросту нет.

Многие вендоры осознают, что безопасность — это долгий процесс, требующий существенных материальных вложений, а потому, стремясь снизить свои издержки, они радикально экономят на обеспечении защиты. Так, например, самый нашумевший ботнет этого десятилетия Mirai состоял в основном из устройств видеонаблюдения. Взломать их помог зашитый в камеры пароль, который просто нельзя изменить.

Весь IoT — это устройства класса «включил и забыл». Причем со стороны пользователя такие действия вполне ожидаемы и логичны, ведь порой многие вещи кажутся совершенно безопасными, хотя это далеко не так.

Большинство пользователей не ассоциируют свои «умные» утюги, кофеварки и чайники с компьютерами, а потому совершенно не склонны задумываться о необходимости обеспечения их безопасности.

Тем не менее эти предметы уже получили доступ в интернет, стек протоколов TCP/IP и весь необходимый софт, в котором есть огромное количество уязвимостей. По оценке Hewlett-Packard, более 70% подключенных к интернету устройств имеют «дыры» в прошивке. В среднем в каждом проверенном устройстве выявлено 25 различных уязвимостей.

Хакеры устраивают DDoS, пользуясь уязвимостью IoT

По идее вендоры должны брать на себя ответственность за выпускаемое оборудование и гарантировать его безопасное использование: своевременно выпускать апдейты прошивки с исправленными уязвимостями и применять защитные технологии на этапе разработки. Но вендоры в целях экономии средств зачастую тоже вводят режим «выпустил, включил и забыл». Потому «умные» устройства никогда не получат апдейтов, а даже если и получат, то как заставить пользователя установить это обновление?

Большинство из нас заходят в интерфейс управления лишь единожды, делая первоначальную настройку. В итоге мы получаем устройства, которые годами производятся миллионными сериями с известными уязвимостями, что приводит к атакам, способным поставить интернет во всем мире на колени.

Наличие большого количества незащищенных устройств интернета вещей, пусть даже с невысокой вычислительной мощностью, делает их легкой добычей для злоумышленников. Эксплуатируя уязвимости или просто пользуясь слабостью встроенных систем защиты, хакеры создают масштабные ботнеты и используют их для вредоносной активности, например, для организации DDoS-атак.

С помощью все того же нашумевшего ботнета Mirai в конце 2016 года была устроена DDoS-атака против французского хостинг-провайдера OVH, достигшая рекордной скорости 1,2 Тбит/с. Специалисты тогда стали поговаривать, что интернету «конец» и далее функционировать он не сможет, раз появились атаки такого уровня.

Однако это не финал, а лишь начало целого класса угроз, связанных с «коробочками» IoT. Далеко ходить не надо: история 2016 года о ботнете, состоящем из более чем 25 тысяч городских и частных камер наблюдения и созданном для совершения DDoS-атак, уже стала притчей во языцех. Хуже того, как показало исследование WhiteScope LLC, даже автоматизированные мойки автомобилей могут быть взломаны за счет эксплуатации критической уязвимости и использоваться для нападения на ничего не подозревающих клиентов.

Развитие мобильных сетей создает новые проблемы для IoT

Масла в огонь подливает и развитие мобильного интернета. Все заметили, каким быстрым и надежным он стал за последнее десятилетие. Проводная связь зачастую бывает в разы медленнее беспроводной, и разница отставания будет только наращиваться, особенно в пригородной зоне.

Уже сегодня появляются сети пятого поколения 5G, и вскоре устройства класса IoT будут подключать уже не к домашним роутерам и маршрутизаторам, а к беспроводным сетям операторов связи напрямую. Вместе с тем развитие скорости и надежности мобильных сетей добавляет новый пласт проблем.

Поскольку умные устройства имеют быстрый доступ в интернет, располагают достаточно высокими вычислительными мощностями, они могут быть использованы как инструментарий для проведения различных атак, в том числе и DDoS.

Если раньше мы видели попытки использовать сети мобильных операторов как плацдарм для DDoS-атак, и жертвой становилась, прежде всего, сама инфраструктура мобильных операторов, что приводило к отключениям сетей, то сейчас все иначе.

В связи с тем, что сети стали выносливее, при проведении атак они «выживают», но проблемы получают все подключенные к ним устройства. И если включая устройство в свою домашнюю сеть, пользователь может ее администрировать, то управление сетью оператора связи целиком зависит от его службы эксплуатации. Пользователь никак не может на нее повлиять, а это несет в себе дополнительные риски.

Самые опасные – роутеры

Зараженные сети, состоящие из миллионов взломанных устройств, становятся по-настоящему угрожающей силой, притом не только для бизнеса, но и для частных пользователей. Если в домашней сети появляется устройство, контроль над которым получил злоумышленник, скорее всего, эта «железка» не только участвует в DDoS-атаках, но и собирает огромное количество информации о своем «хозяине»: крадет личную информацию, пароли, банковские данные, перехватывает трафик.

По данным исследования Positive Technologies, наиболее уязвимыми и потенциально самыми опасными устройствами класса IoT являются роутеры. В среднем по миру ежемесячно обнаруживается около десяти уязвимостей в программном обеспечении домашних Wi-Fi и 3G-роутеров.

Злоумышленник, завладев паролем от него, сможет проникнуть в домашнюю сеть и перехватывать передаваемый трафик, то есть вся веб-активность пользователя будет как на ладони, а значит, персональные данные жертвы будут моментально считаны и использованы по усмотрению хакера.

Особенно неприятно то, что злоумышленники добрались не только до клавиатур, мышей, GPS-навигаторов и прочих умных приборов, но даже до бэби-мониторов.

Как защитить устройства интернета вещей

Решение назревшей проблемы следует искать в области регулирования интернета вещей. Очевидно, что рынок остро нуждается в разработке нового подхода к обеспечению безопасности всех устройств IoT. Безусловно, видение самих вендоров, которые привыкли получать «быстрые» деньги и не вкладываться в дорогостоящую разработку, может резко отличаться от мнения профессионального сообщества.

Ответственность в этом вопросе должны взять на себя регулирующие органы, которые помогут построить безопасность интернета вещей на фундаменте стандартов защиты smart-устройств, оперируя тем фактом, что вещи IoT несут в себе действительно серьезную опасность как для пользователей, так и для бизнеса.

Бизнес бизнесом, но как быть в этой ситуации пользователям, пока вендоры не договорились и не разработаны методы защиты IoT?

Ответ напрашивается довольно банальный – защищать данные. То есть на этом этапе пользователям стоит взять этот вопрос в свои руки и заручиться рядом мер, опираясь на которые можно защититься от наиболее распространенных угроз в мире «умных» вещей.

Необходимо содержать свою сеть «в чистоте»:

Сменить установленные по умолчанию пароли

Своевременно устанавливать обновления прошивок

Защищать маршрутизаторы и роутеры, о чем многие даже не задумываются (по данным исследования Positive Technologies, пароли примерно 15 из 100 роутеров не менялись никогда)

Приобретать smart-устройства только у известных вендоров, имеющих опыт в области обеспечения защиты

Подобный комплекс мер не дает 100-процентной гарантии, но существенно снижает шансы попасть «в переплет».

Почему простому пользователю нужно знать об этих опасностях

Конечно, на первый взгляд рядового пользователя, проблема интернета вещей – это не проблема: «Взломали мою кофеварку и с ее помощью кого-то «ддосят»? Ну и пусть, как это касается меня?».

К сожалению, касается, и в будущем коснется еще больше.

Если в домашней сети завелось хотя бы одно взломанное устройство, оно создало отличный плацдарм для кражи данных. Причем воровать могут не только финансы, но и личные данные.

Парадоксально, но факт: на черном рынке данные кредитной карты будут стоить в 3-4 раза дешевле цифровой идентичности пользователя: кто он, где живет, чем увлекается, кто его друзья и прочее. Мошенники могут легко эти данные монетизировать: перепродавать втридорога, использовать их для вымогательства средств у родственников и друзей, взломав аккаунт человека, например, в скайпе.

Кредитная карта ограничена лимитом и защищена программой «антифрод», поэтому украсть можно в лучшем случае несколько тысяч долларов, а обладая персональными данными можно незаконно получать десятки тысяч.

Поэтому главный совет всем, кто задумывается о приобретении умной техники или уже является обладателем таковой: своевременно устанавливайте обновления, следите за чистотой своей сети, не рискуйте, поскольку риск может стоить вам иногда слишком больших средств.

Угрозы IoT будут только нарастать

Современные технологии во многом опережают наше собственное восприятие и понимание цифровой культуры. Мы пока не имеем привычки защищать личные данные не только на телефонах и компьютерах, но и на других устройствах, подключенных к сети.

Однако человечество семимильными шагами движется в сторону гиперподключений и роста трафика. И когда каждая «булавка» в интернете сможет посылать 10 байт, возникнут новые проблемы безопасности, которые надо будет решать, разрабатывая современную инфраструктуру и стандарты защиты устройств.

В будущем угрозы IoT будут только нарастать, и впереди нас еще ждет множество громких атак, связанных с нахождением брешей в умных, но пока таких опасных интернет-вещах.

# Большие данные как большие риски

Все и повсюду массово и с пользой накапливают гигантские базы данных. Беда в том, что никто и нигде не знает, как эти горы данных защищать от злоупотреблений  
  
Проблемы разные – суть одна  
  
В ленту текущих новостей из разных концов планеты недавно попали три сообщения, рассказывающие о существенно разных, казалось бы, проблемах у людей и властей в связи с особенностями новейших инфотехнологий. Единственное, на первый взгляд, что их объединяет, – это общая тема рисков и угроз, с которыми сталкивается общество по мере все более масштабного освоения Больших данных.  
  
Но вот если с этими неприятностями начать разбираться чуть внимательнее, то довольно быстро становится ясно, что на самом деле речь везде идет о разных сторонах одной и той же проблемы. Такого рода серьезные вещи обычно принято именовать «системными дефектами конструкции». Специалисты-профессионалы об этой беде, конечно же, отлично знают. Вот только как это дело эффективно лечить – вопрос более чем дискуссионный, поскольку варианты ответов сильно зависят от того, кому они адресованы.  
  
Иначе говоря, владельцы баз с Большими данными трактуют безопасность системы одним образом; профессионалы ИТ-сектора, занимающиеся разработкой и анализом защиты подобных систем, видят проблемы по-другому; ну а те люди, чьи персональные данные накапливаются и обрабатываются в этих системах в гигантских количествах, представляют себе заботу об их личной, чувствительной к разглашениям информации существенно иначе — по-третьему.  
  
Проиллюстрировать суть возникающих здесь проблем и коллизий, ясное дело, удобнее всего на живых примерах. Самое время процитировать сообщения из ленты текущих новостей.  
  
В Индии члены Верховного суда своим единогласным решением постановили, что персональная приватность, или право на тайну личной жизни, является фундаментальным правом каждого человека. Теперь вердикт высшей в стране судебной инстанции не только должен оказать существенное влияние на то, каким образом корпорации обращаются с персональными данными граждан, — он уже нанес серьезный удар по намерениям нынешнего правительства во главе с Нарендрой Моди. Это самое правительство пыталось доказать, что право на приватность не является фундаментальным правом человека, защищаемым конституцией, а потому все граждане якобы обязаны предоставлять свои отпечатки пальцев, снимки радужки глаза и прочую биометрию в общенациональную биометрическую базу данных, присваивающую на этой основе каждому индийцу уникальный номер-идентификатор.  
  
Новость номер два: в Швеции разгорелся серьезный политический скандал вокруг национального Транспортного агентства. Высшее руководство этого правительственного ведомства решило сэкономить на расходах, воспользовавшись столь модным нынче аутсорсингом – перенеся свои базы данных в облачное хранилище компании IBM, территориально расположенное в другой стране. Вообще говоря, законы Швеции подобные вещи не запрещают. Вот только именно в этом конкретном случае базы данных Агентства содержат немало такой информации, которая может классифицироваться как государственная тайна (например, персональные данные всех водителей транспортных средств в вооруженных силах и спецслужбах; данные о всех гражданах, сменивших имена по государственной программе защиты свидетелей; ну и прочие подобные сведения весьма деликатного характера). Однако позаботиться о том, чтобы доступ ко всем этим сведениям, размещенным в зарубежном хранилище, имели исключительно люди с соответствующим образом оформленным допуском к секретам, руководство Агентства почему-то не сочло необходимым. Попутно оно наделало и других ошибок, скомпрометировавших доверенные им массивы чувствительных к разглашению данных.  
  
Из США пришла новость номер три — о серьезном конфликте, назревшем между крупными полицейскими управлениями мегаполисов (Лос-Анджелеса и Нью-Йорка), с одной стороны, и знаменитой датамайнинговой компанией Palantir — с другой. Поначалу мощные системы Palantir были разработаны для помощи в аналитической работе разведывательного сообщества и спецслужб типа ФБР – чтобы увязывать, синтезировать и визуализировать большие массивы разнородных данных из множества источников.  
  
А еще через несколько лет, когда системы анализа БД от Palantir начали охватывать не только особо скрытные федеральные спецслужбы, но и региональные управления полиции, попутно стали появляться и сигналы о существенных проблемах с этим инструментарием. В частности, ныне стало известно, что системы Palantir не обеспечивают эффективное «секционирование» (compartmentation) информации, то есть не способны надлежащим образом контролировать выдачу секретных сведений разным пользователям – будь то внутри одного учреждения или даже при объединении данных от разных ведомств. По этой причине – в конкретных условиях полиции – тайный осведомитель отдела по борьбе с организованной преступностью становится видимым и известным, к примеру, для сотрудников дорожной полиции и для полицейских совсем других подразделений. Последствия таких утечек, как несложно догадаться, могут оказываться весьма трагическими.  
  
Из трех приведенных примеров уже понятно, наверное, что правильная работа с Большими данными – это дело весьма и весьма непростое. А грубейшие ошибки здесь продолжают регулярно совершать даже те профессионалы, которых принято считать лидерами отрасли. Поэтому для более глубокого понимания проблем каждую из перечисленных новостей имеет смысл разобрать чуть подробнее – за конкретными национальными особенностями во всех этих историях отчетливо проступают нерешенные задачи универсального характера.  
  
Аадхаар, или Кошмар с безопасностью  
  
Во всем, что касается озабоченности рядовых граждан своей приватностью как фундаментальным правом на тайну личной жизни, Россия гораздо больше похожа на Индию, нежели на страны Западной Европы или США. Это, как говорится, самоочевидный факт. Убедиться в котором обычно проще простого – достаточно лишь заглянуть в национальные СМИ и обратить внимание, насколько редко там обсуждаются проблемы вторжения государства и корпораций в область приватной жизни граждан.  
  
В Индии, однако, эта ситуация довольно резко переменилась в феврале нынешнего года – когда об откровенных посягательствах на приватность начали вдруг говорить и писать чуть ли не все. Не то чтобы причиной, а скорее поводом для давно назревшего обсуждения проблемы – сначала в обществе, а затем и в Верховном суде – стал один "твит".  
  
Суть данного твита, опубликованного 3 февраля 2017 года, заключалась в наглядной демонстрации того, насколько легко и быстро можно устанавливать ныне личности случайных людей из толпы. Это делается благодаря системе «Аадхаар», охватившей уже практически все население Индии централизованной базой данных, в которой накоплена биометрическая информация на более чем миллиард граждан страны.  
  
Название Aadhaar переводится как «фундамент» или «основы». А означает это то, что власти Индии в качестве основ своей государственности решили провозгласить создание общенациональной базы данных для биометрической верификации личности. Единой и тотальной базы на все население страны с гигантской численностью, 1,2 миллиарда человек, – начиная с младенцев и заканчивая глубокими стариками.  
  
Биометрическая основа Aadhaar задумана и реализована так, чтобы на каждого человека в базе имелись отпечатки всех пальцев на руках, снимок радужки глаза, цифровая фотография лица плюс текстовое описание особенностей в наружности резидента. Итогом же занесения людей в базу является выдача им уникального идентификационного номера на специальной Aadhaar-карте.  
  
Формально участие граждан в наполнении базы «Аадхаар» объявлено делом как бы добровольным. Однако в реальности вся эта система выстроена таким образом, что совершить практически любую необходимую по жизни официальную процедуру человек теперь может лишь в том случае, если предъявит свой ИД-номер и часть тела для сканирования-верификации – как правило, радужку глаза или отпечаток пальца. Биометрическая проверка личности увязана, в частности, с любыми услугами и получением буквально всего — от талонов на еду, социальных субсидий и топлива для кухни до водительских прав, расчетного счета в банке, кредитов, страховки, пенсии и так далее.  
  
Гигантская же проблема с Aadhaar заключается вот в чем. С одной стороны, никто в обществе толком не представляет, как устроено в этой системе обеспечение защиты, целостности и верификации данных. А с другой, регулярно появляющиеся в СМИ публикации свидетельствуют, что средства безопасности работают в базе не просто плохо, а очень плохо. Для примера, в данных «Аадхаар» уже многократно выявлены заведомо неверные и фальшивые записи. Под эту категорию, в частности, подпадают такие случаи, когда собственные ИД-номера и карточки оформлены на собак и коров. В другом нашумевшем случае было обнаружено, что персональная карта заведена на Ханумана, одного из богов индуистского пантеона.  
  
Даже неспециалисты понимают, что систематическое появление ложных данных в такой системе – это признаки создания новых каналов для отмывания денег и прочих форм мошенничества. Причина же очевидных проколов, судя по всему, заключается в том, что база данных Аадхаар никогда по-настоящему не проходила подобающие процедуры аудита и верификации.  
  
Так, во всяком случае, считают многие специалисты по инфобезопасности, а также юристы, правозащитники и политики, пытавшиеся ознакомиться с работой системы поглубже. Но многочисленные призывы оппозиции, обращения правозащитников и требования профессионалов инфозащиты к независимому и открытому аудиту Aadhaar остаются в правительстве, по сути дела, без ответа.  
  
Именно по этой причине общественность Индии сочла чрезвычайно важным нынешнее решение Верховного суда о том, что персональная приватность является фундаментальным гражданским правом каждого человека. А чтобы стало понятнее, отчего признанию этой идеи так активно сопротивляется правительство и почему данный конфликт теснейшим образом связан с развертыванием системы «Аадхаар», имеет смысл прояснить такие моменты.  
  
Общепринятая в мире юридическая практика такова, что признание фундаментальных прав людей на тайну приватной жизни сопровождается принятием соответствующего государственного закона о приватности и защите персональных данных. Причем в подлинно демократических странах (к которым Индия, безусловно, себя относит) законы подобного рода обычно требуют, чтобы все граждане, на которых собираются их персональные данные, включая и биометрию, не только знали, кто и зачем это делает, но и могли бы со своей стороны проконтролировать аккуратность и актуальность накапливаемой о них в базах данных информации.  
  
Ну а нынешняя ситуация в Индии такова, что в государстве до сих пор нет никакого четкого законодательства, которое могло бы защищать приватность и права миллиарда с лишним человек, предоставивших в базу Aadhaar свои данные. Мало того, что система работает абсолютно непрозрачно, так у людей при этом нет ни инструментов, ни возможностей каким-то образом контролировать или менять свои данные в базе в тех ситуациях, когда они оказываются скомпрометированы. Ибо жульничеством с биометрией уже никого не удивишь, кражи личности с целью мошенничества – в подобных централизованных базах дело обычное, а изменить свое лицо, радужку глаза или отпечатки пальцев граждане, ясное дело, уже не могут.  
  
И дабы этих неприятностей не показалось мало, еще одним очень существенным фактором в разворачивании Aadhaar стала энергичная коммерциализация системы. Иначе говоря, вокруг своей тотальной базы данных, охватившей все население, власти совершенно официально создали и активно наращивают специальную коммерческую инфраструктуру India Stack. Ее цель – обеспечивать разнообразные формы сотрудничества между правительственными ведомствами и частными компаниями, которым предлагается опереться на богатейшие возможности Аадхаар по персональной идентификации всех людей, внесенных в базу.  
  
Демонстрацией именно этих замечательных возможностей и была, собственно, нашумевшая twitter-публикация в феврале, отметившая таким образом плодотворное сотрудничество между India Stack и коммерческой фирмой OnGrid. Таких компаний, подобно OnGrid уже подключившихся к освоению Aadhaar, ныне насчитывается свыше двух сотен. А это означает, что у граждан Индии сегодня нет не только возможностей проконтролировать состояние и защиту записей о своей личности в центральной базе данных, но и никакой информации о том, сколько еще десятков или сотен компаний купили у правительства доступ ко всем их персональным данным ради наращивания собственных прибылей.  
  
Самое же примечательное, что наиболее характерные особенности – настойчивое желание сохранять непрозрачность системы Больших данных в сочетании с мощным коммерческим фактором – свойственны не только Индии, но и всем прочим новостям о проблемах в данной области.  
  
Большая шведская утечка  
  
В последних числах июля 2017 серьезнейший ИТ-скандал в Швеции заставил главу правительства Стефана Лёвена отправить в отставку двух министров – министра внутренних дел Андерса Игемана и министра инфраструктуры (транспорта) Анну Йоханссон. Блок оппозиционных партий требовал также отставки министра обороны Петера Хультквиста, замешанного в скандале не меньше уволенных коллег, однако его было решено оставить на посту – «дабы не вызывать общий правительственный кризис» в государстве.  
  
Из весьма скупых и лаконичных комментариев премьер-министра Лёвена на экстренной пресс-конференции по поводу отставок стало известно, что произошедшее – «это очень серьезное дело, подвергшее риску Швецию и жизни шведских граждан». Из-за неправильной работы с национальной информационной системой в бесконтрольном доступе оказались личные данные практически всех граждан Швеции, включая военных, сотрудников спецслужб и полиции.  
  
Хотя публично известно о данной утечке стало лишь только летом 2017-го, на самом деле история эта началась довольно давно, еще весной 2015 года. Более того, если судить формально, то можно говорить, что по большому счету она все еще продолжается. Причину такого казуса удобнее пояснить чуть позже. А пока куда полезнее просто обратить внимание на то, насколько больше власти здесь были озабочены сохранением своих проколов в тайне, нежели исправлением очевидно неблагополучной ситуации с защитой данных.  
  
Когда же о произошедшем все-таки стало известно народу, а за собственные расследования взялись журналисты и инициативные энтузиасты от общественности, то восстановленная ими суть истории стала выглядеть вкратце так. Фактически компрометация безопасности правительственной инфосистемы произошла в марте 2015 года, когда государственное Транспортное агентство всю работу по поддержанию своих баз данных переложило по коммерческому контракту на корпорацию IBM и на её технические ресурсы (включая людской персонал), базирующиеся в республике Чехия.  
  
Примерно

таким же аутсорсингом и размещением своих данных во внешних облачных сервисах занимаются ныне чуть ли не все, особенно, если хочется сэкономить. Однако именно в данном конкретном случае критично важным результатом предпринятого шага стало вот что. Огромные массивы чувствительной к разглашению информации, включая полный национальный реестр Швеции по водительским лицензиям и сведения о гражданах с засекреченными по той или иной причине персональными данными, оказались доступны посторонним людям, в основном иностранцам, которые не проходили никакой проверки в службах безопасности Швеции на предмет доступа к гостайне.  
  
Что именно там было скомпрометировано, в каких масштабах и с какими именно базами – практически всё это является предметом домыслов и фантазий, не подтверждаемых какими-либо конкретными документами. Ведь правительство и поныне изо всех сил старается сократить до минимума любые утечки о конкретных фактах произошедшего. Но вот в тех ситуациях, когда непосредственными свидетелями явно некомпетентного обращения с секретными сведениями оказывались очень многие коммерческие клиенты Транспортного агентства, утаивать очевидное становилось уже совершенно невозможно. Особую известность, в частности, обрел такой недавний случай.  
  
С наступлением весны, в марте, Агентство подготовило свежую версию полного реестра транспортных средств Швеции и их владельцев – распространив его среди всех маркетинговых и бизнес-структур, купивших подписку на данную рассылку. Само по себе это вполне нормально, поскольку реестр транспортных средств является публично доступной информацией. Но то две вещи с этой рассылкой пошли совсем не так.  
  
Во-первых, в открытый реестр, распространяемый для всех желающих по коммерческой рассылке, оказались включены люди, чье настоящее имя было изменено по программе защиты свидетелей и прочим подобным государственным программам.  
  
А во-вторых, когда эта грубейшая ошибка была обнаружена, то Агентство не стало рассылать новую, подчищенную версию реестра с инструкцией уничтожить прежний вариант как ошибочный. Вместо этого все уже и без того скомпрометированные имена были собраны в отдельный перечень, и теперь уже данный поименный список разослали еще раз открытым письмом по электронной почте – с требованием, чтобы подписчики сами занялись уничтожением в реестре всех записей на перечисленных в списке людей.  
  
Следует подчеркнуть, что это всего лишь один из достоверно известных ляпов. Сколько же их было всего и насколько серьезными была раскрываемые при этом сведения – такой информации публика не имеет. Но зато хорошо известно, кого и когда назначили главным виновником столь серьезных и систематических нарушений в правилах обращения с данными конфиденциального и секретного характера.  
  
В официальном заявлении нового руководства Транспортного агентства сообщается, что их бывшая генеральная директриса Мария Агрен одобрила контракт с IBM на аутсорсинг, хотя он нарушал сразу несколько законов страны: Закон о национальной безопасности, Закон о защите личных данных и Закон о публичности и приватности. В качестве наказания за допущенные нарушения госпожа Агрен в начале 2017 года была уволена и оштрафована на 70 000 крон «за беспечность с секретной информацией» (в пересчете на более известную валюту эта сумма составляет около 8,5 тысяч долларов и равна половине ее ежемесячной директорской зарплаты).  
  
За скупыми словами этой официальной информации, однако, очевидно скрывается куда более мутная и масштабная история. Независимые расследования показали, что шведская контрразведка, военные и прочие информированные люди в правительстве знали обо всех нарушаемых здесь законах страны если и не заранее, то как минимум с начала 2016 года. Однако наказать Марию Агрен решили только в январе 2017-го, когда случился особо серьезный прокол, о котором стало известно премьер-министру Лёвену.  
  
Глава же правительства, судя по всему, счел происходящее делом чрезвычайно серьезным и требующим пресечения и наказания. Так что уже в марте 2017-го дело бывшего гендиректора Агентства было рассмотрено в суде, так же стремительно был вынесен и вердикт о её «виновности». Вот только наказание за это уголовное преступление оказалось в высшей степени странным и непонятным – административный штраф в размере половины месячной зарплаты.  
  
Непонятными эти события, впрочем, выглядят лишь для тех, кто слабо разбирается в тонкостях шведской судебно-правовой кухни. А вот для людей, знакомых с правилами и особенностями юридических процедур, суть произошедшего представляется достаточно ясной. Поскольку наказание административным штрафом уже не может быть пересмотрено в случае признания вины обвиняемой стороной (а именно так и произошло), то теперь публика никак не сможет увидеть никаких документов, собранных и рассматривавшихся судом по этому делу. Иначе говоря, фактически тут был ловко и профессионально выполнен известный трюк типа «концы в воду»...  
  
Казалось бы, понятно, что директор государственного агентства совершила преступление. Она подписала документ, санкционировавший «исключение из текущего законодательства», – а это нечто такое, чего делать никаких прав у нее не было. Директор правительственного учреждения не может по собственному выбору подчиняться или не подчиняться закону. Однако от адвокатов Агрен стало известно, что с её точки зрения данная ситуация выглядела существенно иначе.  
  
Линия защиты на слушаниях в суде сводилась к тому, что «отход от текущего законодательства», который она лично санкционировала, не только считался вполне приемлемым в нынешних обстоятельствах, но и не был чем-то новым – «раньше такого рода решения уже принимались, поскольку это часть процесса, который позволялось применять при необходимости». Иначе говоря, если бы публика имела возможность копнуть данную историю поглубже, то стало бы понятнее, отчего именно Марию Агрен назначили тут крайней.  
  
Все примерно то же самое было в других ведомствах и раньше, ей же просто сильно не повезло, похоже, с тем, что «облако» IBM именно в данном случае оказалось расположено в Восточной Европе. Кроме того, по словам Агрен, она всегда работала в гражданском учреждении, а с вступлением на высокий пост с ней никто не проводил никаких специальных инструктажей об аспектах безопасности этой работы. Так что она в подобных условиях просто старалась делать всё так же, как и остальные, только еще лучше. Почему же спецслужбы Швеции, давно знавшие о том, кто и где работает с базами Транспортного агентства, только в 2017 году решили озаботиться подбором соответствующих кадров с допуском к гостайне – и обещают их укомплектовать «где-то к концу осени»? На этот естественный вопрос внятного ответа у властей нет.  
  
Из лагеря шведских правозащитников, активно выступающих за более эффективные инструменты, обеспечивающие право граждан на приватность, по поводу всей данной истории вполне резонно прозвучала следующая идея. Уж если государство оказывается столь неуклюжим и некомпетентным в защите собственных тайн и персональных данных о своих секретных сотрудниках, то что тут вообще можно говорить о защите государством персональной информации обычных граждан? Вполне возможно, что нечто компетентное и содержательное на данный счет могла бы поведать еще одна важнейшая фигура шведского скандала – американская корпорация IBM. Однако там, по давно уже заведенным известным правилам, полностью дистанцировались от внутренних политических разборок в скандинавском государстве и вообще отказываются от каких-либо комментариев к данной истории...  
  
Парадоксальный бизнес Palantir  
  
Случилось так, что корпорация IBM некоторым существенным, но одновременно незаметным образом оказывается непосредственно замешана и в третьей из разбираемых здесь новостей. Но здесь (точнее, в США) центральной фигурой конфликта являются не системы IBM, а их главный конкурент в области датамайнинговых услуг для властей – корпорация Palantir Technologies.  
  
Ну а поскольку две уже выявленных ранее проблемы в теме «государство и Большие данные» – непрозрачность системы и активная коммерциализация информации – в специфическом бизнесе Palantir проступают особенно ярко и отчетливо, имеет смысл рассмотреть эту историю как своего рода эталон. Или как архетипический образец, наглядно демонстрирующий не только корневые причины серьезных проблем, но и то, почему решить их в нынешних условиях, по сути, невозможно – на принципиальном уровне.  
  
Как многим, вероятно, известно, термин «палантир» появился в нашем лексиконе из толкиеновской эпопеи «Властелин колец», где данным словом именуют магические каменные шары, позволяющие их владельцам знать и видеть всё, что происходит в мире Средиземья. Аналитические компьютерные системы Palantir делают для их владельцев по сути то же самое – накапливая, просеивая и сопоставляя гигантские массивы самых разных данных и выстраивая на этой основе визуально внятные картины событий со взаимосвязями между их участниками.  
  
Подробности о создателях и лидерах, о занятной истории восхождения Palantir Tech и не менее любопытных идеологических основах этой фирмы можно найти в материале «Бизнес на мифах». Ну а здесь следует рассказать о тех особенностях ее продукции, благодаря которым бизнес молодой и «как бы либертарианской» компании стал гиперуспешным благодаря государственным заказам – с одной стороны. А с другой — уже успел ярко продемонстрировать, что опора властей на системы Palantir – это, очевидно, путь «не туда», если для государства важнее интересы общества, а не прибыли корпорации. В сообщениях из текущей ленты новостей, естественно, никто столь сильных обобщений не делает. Однако неоспоримые факты тут говорят сами за себя. Надо лишь соответствующим образом на эти факты смотреть. Иначе говоря, далее будут рассмотрены не просто свежие новости о Palantir, но и то, что они означают в более общем контексте.  
  
Одна новость — про руководство NYPD, крупнейшего в США регионального Управления полиции Нью-Йоркского мегаполиса, которое сильно повздорило с корпорацией Palantir из-за ее «волшебной» системы анализа. Точнее говоря, причиной конфликта стала не собственно система, уже несколько лет применяемая в NYPD, а трудности перехода полицейских к более дешевому и более удобному для них альтернативному ПО, разработанному корпорацией IBM.  
  
Причина же затруднений здесь такова, что всю ту бездну информации, которая была наработана полицией в их системе за время эксплуатации, Palantir категорически отказывается переносить в систему IBM, ссылаясь на защиту своих ценнейших «коммерческих тайн». Точнее говоря, они с готовностью и сразу выдают все первичные или сырые данные, на основе которых база наполнялась. Но вот самое главное – собственно аналитику – выводить для переноса отказываются наотрез. Ибо это раскроет их методы обработки, то есть главную интеллектуальную собственность корпорации.  
  
Суть обозначившегося здесь конфликта имеет смысл обозначить как можно отчетливее. Формально имеется работающая исключительно на общество правоохранительная структура, а также есть некая бизнес-фирма, технически обслуживающая эту структуру в своих сугубо коммерческих интересах. В реальном же итоге оказывается так, что вся действительно необходимая для работы информация, формально собранная и как бы принадлежащая полиции, на самом деле не только принадлежит бизнес-фирме, но и отдавать её на защиту общества она решительно не желает – по причине своих сугубо шкурных коммерческих интересов...  
  
Новость другая – о проблемах с системой Palantir у полицейских LAPD, другого крупнейшего в США Управления полиции Лос-Анджелеса. Проблемы тут обозначились существенно иного рода, однако и они очень наглядно рисуют, сколь опасным сочетанием оказываются для государства непрозрачность и коммерция при анализе Больших данных.  
  
Одним из главных факторов для аналитических успехов системы Palantir является как можно более широкий охват разнообразных источников входной информации. В частности, для эффективной работы с полицейскими базами данных оказывается очень полезным просеивать и сопоставлять не только записи разных баз одного региона, но и одновременно выявлять их взаимосвязи с записями в базах других регионов. Поскольку при таком расширении общей базы не только повышается эффективность полицейской аналитики, но и заметно растут прибыли корпорации, в Palantir очень энергично работают над расширением клиентов в регионах, предоставляя существенные скидки всем новичкам.  
  
Столь замечательная бизнес-стратегия, однако, находится в сильнейшем противоречии с известным принципом «секционирования» информации, общепринятым в работе структур, имеющих дело с секретными сведениями. Проще всего суть этого принципа можно пояснить на основе прямоугольной таблицы, где строки соответствуют разным уровням допуска сотрудников к гостайне – «для служебного пользования», «секретно», «совершенно секретно», «особой важности». А колонки таблицы – это разные секретные дела или «объекты», с которыми работает именно данное ведомство. Тогда любой из сотрудников этого ведомства имеет доступ лишь к той информации, которая находится в клетках или «секциях» таблицы, соответствующих (а) уровню их общего доступа к гостайне и одновременно (б) разрешению на доступ к сведениям конкретно по данному объекту.  
  
Официально провозглашается, что в аналитических программах Palantir эти ясные принципы реализованы совершенно замечательно. Здесь не только имеется строгая система допусков, гарантирующая, что всякий сотрудник может получить доступ к данным исключительно на уровне своих полномочий, но и автоматически создается аудиторский след, в котором фиксируется всё – кто именно видел определенные фрагменты информации и что именно с этими фрагментами делалось.  
  
В реальной работе лос-анджелесской полиции, однако, вся эта картина выглядит существенно иначе (наверняка то же самое происходит и у других пользователей системы, но их недовольство просто не доходит до прессы). Сотрудники спецподразделения LAPD, занимающиеся борьбой с организованной преступностью, на протяжении многих и многих месяцев безуспешно пытались добиться от Palantir всего лишь того, чтобы особо чувствительные файлы о людях и операциях, которые они помечают конфиденциальными, не становились свободно доступными для всех остальных пользователей системы. Однако даже эта тривиальная, казалось бы, техническая проблема, оказывается практически неразрешимой, когда для корпорации-подрядчика гораздо важнее максимально широкий охват анализируемой информации, нежели узкие интересы копов-оперативников...  
  
Описанные здесь проблемы – это не что-то новое и неожиданное. Все подобные трудности с большими базами данных известны профессионалам очень давно. Как они выражаются, «приватность масштабируется очень плохо». И если в работе секретных спецслужб об этой серьезнейшей беде широко вещать обычно не принято (как и обо всех прочих гостайнах), то в работе всеобщей системы здравоохранения – где в обращении с деликатными данными пациентов прослеживается много аналогий – о том же самом специалисты по инфозащите говорят давно и громко.  
  
Медицинские базы данных с цифровыми картами пациентов очень полезны врачам, и все там работает замечательно – когда штат из 20 человек в медицинском учреждении имеет доступ к медкартам десяти тысяч пациентов, зарегистрированных в их картотеке. Но вот когда создается единая централизованная система, позволяющая каждому доктору или медсестре данной страны просматривать медицинские записи любого пациента – вот это всегда получается однозначно плохо, организовано неправильно и тут же ведет к злоупотреблениям разной тяжести (от сливов болезней знаменитостей в таблоиды до отказов людям в работе, кредитах или в страховке на основании данных об их здоровье в цифровых медкартах, считающихся как бы «приватной информацией», а на самом деле доступных кому угодно.

Всем понятно, что решать проблему по-любому необходимо – все базы Больших данных постоянно только прирастают, а отказываться от их преимуществ совершенно никак невозможно. Но одновременно понятно и то, что простых и эффективных решений c защитой здесь, похоже, не существует. Ярчайшим подтверждением тому являются регулярные и мощные сливы информации из наиболее секретных недр разведслужб – начиная от демарша Эдварда Сноудена и заканчивая массами свежих публикаций о хакерском инструментарии АНБ и ЦРУ США. Причем сами спецслужбы оказываются зачастую не в силах как определить то, кто именно стоит за компрометацией, так и оценить объемы скомпрометированных данных.  
  
Отсюда понятно, наверное, что с защитой приватности для всех обычных граждан государство разберется не раньше, чем решит проблемы с массовыми утечками компромата из спецслужб. А это две стороны одной и той же проблемы...  
  
Бёрд Киви

# Государство отказалось нести ответственность за утечку персональных данных россиян

26.02.2018

У власти становится все больше информации о гражданах, но отвечать за нее правительство не собирается, и получить компенсацию за утечку данных очень трудно.

Утечка персональных данных граждан из государственных баз не является ответственностью государства. Как пишет [**The Bell**](https://thebell.io/utechki-ne-nashi-gosudarstvo-ne-budet-otvechat-za-poteryu-personalnyh-dannyh/) со ссылкой на «Ведомости», это следует из ответа российских властей в Европейский суд по правам человека ([ЕСПЧ](http://www.dk.ru/wiki/espch#binding)) по иску об одной из утечек из базы [ГУВД](http://ekb.dk.ru/wiki/guvd#binding) Москвы. Иск подал москвич, который обнаружил информацию о своих судимостях и заражении ВИЧ в купленной на рынке базе столичного ГУВД. Замминистра юстиции Михаил Гальперин от имени РФ разъяснил: у полиции есть право собирать о гражданах все необходимые данные, защита их от несанкционированного доступа осуществляется, а информация из купленной истцом базы недостоверна.

[Следственный комитет](http://ekb.dk.ru/wiki/sledstvennyy-komitet#binding), прокуратура и суд отказались проверять утечку персональных данных по требованию истца: проводилось внутреннее расследование, но его результаты закрыты. Добиться возбуждения уголовного дела об утечках в России практически невозможно, отмечают юристы.

 Официальная российская позиция, разъясненная в ЕСПЧ, может иметь большие последствия: с этого года [**начнется**](http://ekb.dk.ru/news/stat-klientom-udalenno-kak-edinaya-biometricheskaya-sistema-izmenit-zhizn-rossiyan-237099590#binding) внедрение единой биометрической системы. Например, там появятся все биометрические данные банковских клиентов. В отличие от похищенных номеров банковских карт и паспортов, изменить биометрические данные невозможно, что делает их утечку особенно опасной. Сейчас доступ к базам данных есть у десятков тысяч госслужащих, а всеобъемлющая проверка потребует несоразмерного количества ресурсов.

 Разработкой единой биометрической системы занимается «[Ростелеком](http://ekb.dk.ru/wiki/rostelekom#binding)». В компании отмечали, что персональные данные граждан будут храниться в защищенном контуре, а передавать их будут по защищенным каналам связи, с использованием отечественных криптоалгоритмов.

# ОС Ubuntu будет следить за пользователями

Операционная система Ubuntu на данный момент является самой популярной среди дистрибутивов Linux, но этот статус она в очень скором будущем потеряет. Как стало известно, компания Canonical, ведущая разработку данной ОС, собирается внедрить в нее функционал слежки за пользователями.

Ubuntu начнет собирать всю информацию о компьютере пользователя — его конфигурации, расположенных в его памяти файлах, истории посещаемых страниц,

предустановленных программах и так далее. Об этом стало известно из открытого письма команды разработчиков настольной версии Ubuntu Уильяма Кука. Более того, Ubuntu будет отслеживать даже местоположение пользователя как во время установки, так и во время эксплуатации, причем есть намек на сбор IP-адресов.

Как сообщается, слежку в Ubuntu, в отличие от Windows 10, можно будет отключить без особого труда — можно будет сделать это на этапе установки. Проблема в том, что нужную галочку по незнанию можно и не заметить, и тогда потребуется еще одна переустановка. Пользователи уже выступили с критикой готовящегося нововведения и прямо сравнили Ubuntu с Десяткой от Microsoft, которая собирает вообще все пользовательские данные, даже личные, пока вручную не обрубить ей все каналы связи с серверами Microsoft. В общем, совсем скоро популярность Ubuntu заметно снизится, и на первый план выйдет не менее качественный дистрибутив Mint, который ни за кем не следит.

# Конец приватности

Пользовательская информация, а также доступ к ней у крупнейших IT-компаний — одна из наиболее острых тем в последнее время. Масло в огонь подливают сами разработчики платформ для взаимодействия с искусственным интеллектом. Возможно ли мировое господство ведущих IT-компаний и стоит ли доверять свои секреты интернет-сервисам — в материале «Газеты.Ru».  
**Республика FAMGA**  
В феврале в сети появился материал от разработчика программ для работы с искусственным интеллектом Энди Перта, в которой говорится о том, что через несколько лет влияние таких крупных интернет-компаний как Facebook, Amazon, Microsoft, Google и Apple (FAMGA) возрастет до таких масштабов, что можно будет говорить, что именно они будут иметь власть над большинством жителей Земли.  
Их влияние будет основываться на огромном массиве информации на каждого человека, который пользуется продуктами этих компаний — все-таки на Земле осталось мало современных горожан, которые не пользуются сервисами Google или операционной системой Windows на своем компьютере. По мнению Перта, именно рост спроса на голосовые помощники говорит о таком развитии событий.  
С помощью искусственного интеллекта и постоянного сбора данных о привычках, интересах, политических, религиозных и иных предпочтениях, можно построить очень полный портрет человека, а самое главное — предсказать его поведение, что является большой ценностью само по себе.  
У корпораций появятся действительно сильные экономические и политические рычаги и они смогут выводить на рынок по-настоящему успешные продукты и сервисы. Также, по мнению эксперта, возможно возникновение крупнейших транснациональных банков и других коммерческих структур, организованных на мощностях «большой пятерки».  
**Без вины виноватые**  
Пользователи голосовых ассистентов, чатботов и социальных сетей сами доверяют им большое количество личной информации о себе, которая формально должна впоследствии использоваться для более точных рекомендаций и машинного обучения.  
Так, большинство приложений сразу при установке запрашивает доступ к микрофону, геолокации, списку контактов, камере и другим инструментам взаимодействия с пользователем.  
Поэтому весьма странно удивляться подсказкам о достопримечательностях рядом с вашим местом работы, интересных фильмах в любимом кинотеатре или предложению дружбы от человека из дома напротив, который нашел вас по геометке в Instagram.  
Большинство личной информации, получаемой разработчиками, собирается либо при непосредственном участии пользователя, когда он оставляет оставляет отзыв о посещенном кафе, усердно заполняет поля с информацией о себе в социальной сети или даже просто «лайкает» понравившиеся записи, но и когда он бездумно нажимает «принимаю», «согласен» и «далее», устанавливая очередную программу на свой компьютер или смартфон.  
Сложно сказать, как используются личные данные, кроме как для машинного обучения, и есть ли специальные базы данных с досье на каждого человека или нет. В любом случае, данная информация является коммерческой тайной корпораций.  
**Сила — в правде**  
Можно долго рассуждать о махинациях компаний с личными данными пользователей, но гораздо показательнее реальные случаи, где видно, что крупные IT-гиганты вовсе не желают или не могут дать доступ к пользовательской информации спецслужбам и правительствам стран.  
Так, одним из самых нашумевших случаев был связан с терактом в США, когда преступник Саид Фарук пользовался смартфоном от Apple и, возможно, осуществлял подготовку к теракту и вел переговоры с его помощью. ФБР обратилось за помощью к компании Apple с требованием убрать ограничение на количество попыток ввода пароля, чтобы иметь возможность разблокировать смартфон преступника.  
На данное требование руководство Apple ответило отказом. Глава компании Тим Кук в своем открытом письме заявил, что в Apple не будут создавать лазейки в операционной системе, а конфиденциальность личной информации — один из основных приоритетов.  
Дело закончилось тем, что спецслужбам удалось получить доступ к желаемой информации без помощи Apple, однако как это удалось сделать, остается неизвестным.  
**В бой идут старики**  
Проблемой возможной гегемонии IT-компаний озаботились даже бывшие сотрудники гигантов Кремниевой долины — Facebook, Google и других.  
Они запустили кампанию «Правда о Технологиях», цель которой ограничить влияние социальных сетей на детей и подростков, а также уменьшить время активного пребывания их в Сети вообще.  
В интервью, данном The Guardian представителями движения, они утверждают, что большое количество молодежи проводит в социальных сетях от шести до девяти часов ежедневно, а происходит это благодаря манипулятивному влиянию онлайн-платформ, их построению на уязвимостях человеческой психологии.  
Кроме того, социальные сети провоцируют активно делиться с общественностью личной информацией, давая возможность компаниям использовать получаемую информацию в своих целях, манипулировать интересами и желаниями молодого поколения.  
**Суды против «Большого брата»**  
Распространена точка зрения о том, что судебные и исполнительные системы разных государств активно сотрудничают с крупными телекоммуникационными компаниями, операторами связи и производителями мобильных устройств. В опровержение этого мнения можно привести недавнее судебное дело, рассмотренное Апелляционном судом Великобритании.  
Суть его сводится к тому, что суд признал незаконным полный доступ следователей к личной информации подозреваемых на ПК и смартфонах.  
По мнению суда, такой доступ противоречит нормам права Европейского Союза и нарушает базовые права человека, такие как право тайны личной переписки.  
Однако стоит отметить, что правоохранительные органы все же могут получить доступ к необходимой информации, но для этого они должны пройти процедуру разрешения в суде.  
Другой важный судебный процесс сейчас слушается в высшей судебной инстанции США — Верховном суде. Решение по делу Тимати Карпентера должно стать прецедентом для всех последующих судебных кейсов. Верховный суд может обязать следователя получать соответствующий ордер для получения истории геолокаций смартфона подозреваемого или оставить существующий упрощенный порядок получения.  
Если суд будет на стороне Карпентера, то правоохранительным органам будет значительно труднее получать доступ к личной информации.  
**Что будущее нам готовит**  
Директор по росту и исследованиям социальной сети «ВКонтакте» Андрей Законов сообщил «Газете.Ru», что предоставление доступа для интернет-платформ к личным данным является еще одним этапом развития технологий, который проходит сбалансированно.  
«Мессенджеры не заменили личное общение, но сделали многие аспекты коммуникации удобнее. Электронные книги не привели к исчезновению бумажных, но дали доступ к огромному количеству информации. Онлайн-курсы никак не испортили университеты — наоборот, они помогают людям в учебе и делают процесс обучения интереснее. Также и большие данные — при правильном и ответственном подходе к вопросу это новые возможности для компаний и удобные продукты для пользователей», — заключил Законов.  
Он добавил, что социальные сети серьезно относятся к данным и всегда запрашивают у пользователя доступ к той или иной информации.  
«Компании должны заслужить доверие пользователей, иначе у них не будет данных», — сообщил представитель российской соцсети.  
Генеральный директор компании «Облакотека» Максим Захаренко настроен более пессимистично и отметил, что «Большой брат» действительно очень опасен для личной жизни любого человека.  
«Просто находясь со смартфоном в кармане, каждый абсолютно прозрачен географически уже сейчас. Никто из нас не может скрыть никакой аспект личной жизни. За каждым, помимо смартфона, уже следят ноутбуки, телевизоры и, как мы видели в одном рекламном ролике, чайники... Если ваши данные используются для

улучшения рекламы, это куда ни шло, но этим же не ограничится, они обязательно будут украдены хакерами и обращены во вред каждому из нас», — считает эксперт.  
  
На текущий момент особенно большие и разнообразные данные накапливаются у государства и ИТ-корпораций.  
Захаренко отметил, что наибольшую опасность представляет собой их синергия, успешное развитие которой мы наблюдаем прямо сейчас.  
«Вообще говоря, вариантов всего два. Первый — это ликвидация понятия приватности. Так было еще 100 лет назад в деревнях, где все про всех все знали. Но есть и второй вариант, а именно надежда на некий общий разум человечества, которое осознает и пока еще может пытаться регулировать эту тему. Даже в России уже идут разговоры о расширении защиты персональных данных в сторону «биг дата»», — заявил собеседник «Газеты.Ru».

# «За нами следят»: что знают о пользователях интернет-компании и сколько стоит такое знание

Натали Нахай, Томас Чаморро-Премузик 12 января 2018

Ходят слухи, что Марк Цукерберг закрывает камеру и микрофон своего ноутбука. Как пишет Антонио Гарсиа Мартинес в своей новой провокационной книге Chaos Monkeys, посвященной основателю Facebook, «первыми с тонущего корабля бегут не крысы, а члены команды, умеющие плавать». Эндрю Гроув, один из основателей компании Intel и пионеров Кремниевой долины, высказался примерно в том же духе: «Выживают только параноики».

Во времена, когда люди проводят больше времени онлайн, чем офлайн, мы производим море личных данных, и мысли о хакерах и кибербезопасности преследуют нас как никогда прежде. Когда-то «личное» означало «конфиденциальное», но не сегодня, когда наши персональные и интимные отношения (и генерируемые ими данные) развиваются в интернете, который становится все более публичным местом. Даже когда на нас никто не смотрит, мы редко остаемся в одиночестве.

Что если бы у вас появился шанс выкупить все данные, оставленные вами в интернете с первой минуты выхода онлайн и до сегодняшнего дня? Сколько бы вы заплатили? Что бы вы отдали ради 100% безопасности? Прежде чем ответить, подумайте о следующих издержках.

1. Больше никаких «бесплатных» услуг. Всем известны слова Эндрю Льюиса с сайта MetaFilter: «Если вы не платите, то вы не потребитель, а продукт, который продается». Но что если провайдеры электронной почты, социальные сети и даже поисковые серверы, которыми мы пользуемся каждый день, перестали бы быть бесплатными? Мы можем жаловаться на отсутствие конфиденциальности и быстрое проникновение в личное пространство поставщиков подобных услуг, однако широко распространенных альтернатив, по-видимому, не существует.

Дело не в отсутствии идей. Новаторы в области технологий предлагают альтернативные бизнес-модели, например, Джарон Ланье предложил использовать персональные микроплатежи для вознаграждения пользователей, предоставляющих данные. Представьте себе, что вы будете получать небольшой платеж за каждое отправленное письмо или сообщение по Whatsapp — может ли такое решение помочь избежать избытка информации? Другим вариантом, конечно, может стать подписка на сервисы, такие как Facebook, плата за которую будет гарантировать конфиденциальность данных пользователей и заменит продажу данных в рекламных целях.

Проблема заключается не столько в технической стороне вопроса, сколько в психологической: в неосязаемости наших данных и их воспринимаемой ценности. Для большинства из нас «бесплатные» услуги, которыми мы пользуемся онлайн, позволяют удовлетворить конкретную потребность — связаться с другими людьми. Общаясь по электронной почте, в групповых чатах или социальных сетях, мы производим данные, которые не только неосязаемы, но и ценность которых среднестатистическому потребителю сложно понять и оценить. Большинство людей содрогнутся при мысли, что чужой человек придет к ним домой и начнет просматривать фотоальбомы, банковские выписки и личные дневники, однако многие и глазом не моргнут, когда нечто подобное произойдет онлайн, вероятно, потому, что в этом случае вторжение и его последствия менее заметны. Только столкнувшись с конкретным сценарием, таким как утечка данных (номера кредитной карты или личных фотографий), мы начинаем понимать, чем грозит в реальном мире наши действия в онлайне.

Если говорить о социальных сетях, то даже когда люди понимают риски и беспокоятся о конфиденциальности, они все равно редко придерживаются защитной стратегии поведения. Они все чаще сетуют на нарушение конфиденциальности, но продолжают публично раскрывать данные о себе и позволяют компаниям беспрецедентный доступ к ним, что ведет к «парадоксу конфиденциальности». Если коротко, такое поведение свидетельствует о том, что люди на деле не так сильно беспокоятся о конфиденциальности, как на словах. Им нравится сама идея, но, по-видимому, они не настолько ценят свои данные, чтобы предпринимать конкретные шаги по их защите. Справедливости ради следует отметить, что такое несовпадение отношения и поведения наблюдается во всех областях жизни. Например, большинство людей ценит свое здоровье и отношения, однако ведет себя так, что регулярно рискует и тем, и другим, даже когда осознает потенциальные последствия.

2. Больше никакой персонализации. При взаимодействии в интернете мы привыкли к некоторой степени соответствия результатов поиска и онлайн-услуг или продуктов нашим персональным характеристикам и контексту. Один из руководителей Alphabet Эрик Шмидт давно отмечал, что в отличие от традиционных СМИ интернет занимается «узким вещанием». Персонализация не выражена явно, и мы начинаем понимать, насколько скорректированы именно под нас сервисы (например, поиск по картам Google, реклама, которую мы видим в YouTube или Facebook), только когда меняем настройки приватности или стираем cookies и историю поиска.

Мы так привыкли к легкости и удобству, что не спешим отказываться от них в пользу более конфиденциальных (но и более неэффективных) методов. Конечно, можно отключить настройки геолокации для приложения вызова такси, чтобы оно перестало отслеживать каждый ваш шаг, но тогда каждый раз, когда вы захотите воспользоваться им, придется вручную вводить свое местоположение, то есть тратить слишком много сил ради конфиденциальности.

Конечно, у персонализации есть и оборотная сторона, например, когда вы начинаете получать на разных платформах (в социальных сетях, сервисах ТВ по запросу и по цифровом радио) рекламу продукта или услуги, которую искали, но не подозревали, что вас отслеживают. Этот «пугающий фактор» — ощущение, что каждый ваш шаг, публичный и приватный, отслеживают, анализируют его и извлекают из него выгоду — может привести к ситуации, известной как психологическое сопротивление. Если нам кажется, что мы теряем свободу или она находится под угрозой, желание восстановить ее может заставить людей воспротивиться социальному влиянию: у пользователя возникнет ощущение насилия над собой, и репутация компаний, надеявшихся с помощью персонализации увеличить доходы, будет запятнана.

3. Больше никакого мгновенного удовлетворения запросов. Данные, которые мы производим в ходе повседневных взаимодействий, также можно использовать для разработки сервисов, пользующихся нашим желанием получать то, что нам нужно, немедленно и в удобном формате. Мы живем в век, когда только мгновенное удовлетворение запроса считается достаточно быстрым. Учитывая наши ограниченные возможности удерживать внимание, на рынке, уже страдающем из-за нехватки времени и внимания у потребителей, сервисы, предлагающие мгновенные решения, не только обеспечивают ощущение немедленного удовлетворения запроса, но и могут более эффективно добиться того, чтобы клиент серьезно не задумывался. Когда, например, вы в последний раз читали условия использования загружаемого приложения? Иными словами, когда мы подписываемся на новую услугу, стремление к удобству часто перевешивает рациональные рассуждения, и мы соглашаемся на использование наших данных такими способами, которых не могли даже представить. Стремясь потратить как можно меньше времени и умственных усилий, возможно, мы обрекаем себя в будущем на значительный риск в виде утечки персональных данных или отказа в определенных медицинских или финансовых услугах в связи с выводами, сделанными о нас на основе цифрового следа.

Как нам кажется, нам следует ожидать гораздо большего в обмен на конфиденциальность. Между количеством раскрываемых нами данных и получаемыми услугами должно быть больше симметрии. Например, рекомендательные сервисы должны действительно помогать находить то, что нам нужно, даже если мы не знали, чего хотим. До некоторой степени это реализуется в области музыки и кино, но не когда речь идет о покупках. Аналогично те же данные, что собираются в рекламных целях, могут использоваться для более точного предложения вакансий, так как они указывают на множество психологических качеств, которые десятилетиями связывают с карьерными результатами. Например, если ваши предпочтения на Netflix или Spotify показывают, что вы любознательный или творческий человек, алгоритм поиска работы может предложить вам вакансии, где требуется любознательность и творческий подход. И самое главное: ни один из этих сервисов не должен предлагаться без согласия потребителя, эти сервисы должны объяснять, как и зачем они используют наши данные. Мы заслуживаем право знать, какие выводы делаются из наших данных и насколько они точны.

Об авторах. Натали Нахай — лектор и автор бестселлера Webs of Influence: The Psychology of Online Persuasion». Ее лекции, статьи и подкасты посвящены цифровому применению бихевиоризма. Томас Чаморро-Премузик — профессор психологии бизнеса в Лондонском университетском колледже и Колумбийском университете, участник Entrepreneurial Finance Lab Гарвардского университета, гендиректор Hogan Assessment Systems.

# Всевидящее око по-китайски

Январь 2018

В Китайской Народной Республике создается система тотального контроля населения.

В КНР начато создание механизмов тотального контроля. «Система социального рейтинга» позволяет следить за поведением жителей и присваивать им рейтинги. В стране называют их рейтингами доверия. Пользующиеся высоким доверием граждане будут вознаграждены разнообразными бонусами, жизни граждан с низким рейтингом – не позавидуешь. При подготовке материала использованы публикации журнала Wired, Фонда Карнеги, РБК.

14 июня 2014 года государственный совет Китая опубликовал документ «Проект плана по созданию системы социального кредита доверия». В качестве основной идеи в нем предлагалось каждому гражданину страны присваивать на государственном уровне рейтинг доверия. «В обществе будет процветать доверие. Оно укрепит искренность во взаимодействии с госструктурами коммерции и общества, а также усилит юридическую надежность».

В чем замысел

Основная цель системы – «построение гармоничного социалистического общества», говорится в программе. Также описывается в ней и главная ценность такого общества – честность. «Жить по закону, вовремя погашать кредиты, платить налоги, соблюдать правила ПДД, не нарушать нравственные устои общества, и все будет в порядке. Не убрал во дворе за своей собакой – минус пять баллов. Проводил пожилого соседа до поликлиники – получил пять баллов», – поясняет суть системы информационный ресурс «Хуаньцюван».

Кто будет реализовывать проект

Система социального рейтинга будет отслеживать жизнь китайского гражданина во всей ее полноте – от законопослушности и честности до потребительского поведения и проступков в быту. Ответственным за создание, внедрение в жизнь и работу системы назначен государственный комитет по развитию и реформам КНР. Текущую работу курирует замглавы комитета по развитию и реформам Лянь Вэйлан.

Как формируется китайский рейтинг

Система оценки поведения гражданина – балльная, как в школе. За любую положительную деятельность, например, отсутствие нарушений закона, полезную общественную работу, своевременную выплату кредитов и т.д. будут начисляться баллы, за неблаговидные проступки –вычитаться.

Участвуют ли в рейтинге компании

Компании тоже участвуют в рейтинге: проверяются на соответствие экологическим, юридическим нормам, условиям труда, финансовой отчетности. Если все хорошо – компании присваивается высокий рейтинг, а вместе с ним и возможность пользоваться льготным режимом налогообложения, кредитования и т.д. Если у компании низкий рейтинг, ее жизнь усложняется дорогими кредитами, повышенными ставками налогов, запретами на эмиссию ценных бумаг и инвестирование в другие компании.

Откуда берутся данные

Данные о человеке будут собираться из государственных структур, правоохранительных и муниципальных органов. Также данные будут собирать восемь частных компаний. Первые две из них – Alibaba и Tencent. Tencent – владелец мессенджера WeChat, которым пользуются 500 млн человек. Alibaba – платформа онлайн торговли с аудиторией 448 млн китайцев. Они могут собрать самую ценную информацию о своих пользователях.

Кто обрабатывает данные

Все данные стекаются во всекитайскую объединенную платформу кредитной информации. Она будет обрабатывать этот массив данных и формировать рейтинги. Корпоративные рейтинги компаний можно будет посмотреть в национальной информационной системе публичной кредитной информации для компаний, данные о физических лицах – на информационном портале Credit China.

Как рейтинг влияет на кредит

Alibaba уже запустила собственный рейтинговую систему Sesame Credit, которая начисляет пользователям баллы за их потребительское поведение. Sesame оценивает клиентов по шкале от 350 до 950 баллов. Начиная с 600, пользователь имеет право на беззалоговый кредит на $800 для покупок онлайн, с 650 – может арендовать машину без залога, с 700 – экспресс-оформление разрешения на поездки в Сингапур, с 750 предоставляется шенгенская виза.

Что ждет китайских «двоечников»

В сентябре 2017 года правительство КНР опубликовало уточненный перечень санкций, которым будут подвергаться обладатели низких рейтингов: запрет на работу в госучреждениях, отказ в соцобеспечении, особо тщательный досмотр на таможне; запрет на занятие руководящих должностей в пищевой и фармацевтической промышленности; отказ в авиабилетах и спальном месте в ночных поездах; отказ в местах в люксовых гостиницах и ресторанах; запрет на обучение детей в дорогих частных школах.

Какие выгоды у «отличников»

Если рейтинг больше 1050 баллов, его обладатель считается образцовым гражданином и маркируется тремя буквами ААА. С 1000 баллов можно рассчитывать на АА, с 900 – на B. Если рейтинг упал ниже 849 (С), гражданина выгоняют со службы в государственных и муниципальных структурах.

Когда проект заработает

Система работает в пилотном режиме в тридцати городах Китая. Например, в городе Жунчэн в провинции Шаньдун, всем жителям дали стартовый рейтинг 1000 баллов. В зависимости от их поведения, баллы растут или убывают. Информация о поведении поступает из муниципальных, коммерческих, правоохранительных, судебных органов, а также из доносов в единый информационный центр.

Кто судит судей?

Верховная власть должна стать локомотивом и примером для подражания в новой системе социального кредита, говорится в официальных документах. Система будет анализировать посещаемость партийных собраний, образование, семейное положение, сопоставлять данные о доходах чиновника и членов его семьи с данными о приобретенной недвижимости и предметах роскоши. Пока система работает на уровне низших партийных чиновников. А кто будет отслеживать верховных бонз? Ответа на этот вопрос пока нет.

Могут ли люди стать жертвами ошибок?

Могут. Алгоритмы не учитывают контекст, например, один человек может не оплатить счета, потому что попал в больницу, а другой намеренно уклоняется от выплат. Также непонятно, что делать, если аккаунты в соцсетях будут взломаны, данные украдены или неправомерно исправлены? Уже сейчас на основании этих данных выносятся судебные решения. В 2015 году верховный суд КНР, опираясь на данные Sesame Credit, наложил санкции на 5300 человек. Летом 2017 года таких людей было уже 7,3 млн.

Когда система заработает в полную силу

К 2020-му году она должна быть внедрена полностью и повсеместно. Каждая компания и каждый житель Китая будут отслеживаться и оцениваться системой в режиме реального времени. Система повлияет и на личную жизнь: крупнейшая в Китае служба знакомств Baihe продвигает странички пользователей в зависимости от баллов Sesame. «Благосостояние партнера гарантирует комфортную жизнь», – так определяет мотивацию один из сотрудников компании.

Может ли кошмар выйти за пределы Китая

Корейский институт политических исследований Asan назвал систему «кошмаром Джорджа Оруэлла». «Пока у нас еще есть выбор и права, которыми можно воспользоваться. Нам нужно сделать так, чтобы оценивать можно было самих оценщиков», – пишет Wired. «Надзиратели и наблюдаемые должны свободно следить друг за другом, – считает писатель Кевин Келли. – Нам предстоит выбрать: либо слежка будет секретной и односторонней, либо взаимной и открытой».

# Приватность в сети: вы даже не знаете, насколько вы уязвимы

Александр Родионов

Директор по развитию, Краснодар

Крупные IT-корпорации, монополизировавшие сбор данных, знают о вас то, чего вы сами о себе не знаете.

Аккаунты в соцсетях становятся цифровым паспортом личности, и, чем сильнее мы привыкаем к удобству использования виртуальных идентификаторов, тем больше данных физических лиц и коммерческих организаций продается, покупается и снова продается сторонними компаниями без их ведома. И дело тут не в хакерских атаках или воровстве информации, а в самой архитектуре информационного общества.

Как собираются данные

Вот несколько сюжетов за последние пару месяцев.

1. Британский провайдер провел социальный эксперимент, включив в пользовательское соглашение пункт о добровольном выполнении общественных работ. За две недели 22 000 человек подписались на 1000 часов очищения канализационных завалов и уборку парков. Что и требовалось доказать. Не думаю, что подобное соглашение, не окажись оно шуткой, имело бы юридическую силу в физическом мире, но бесспорно развязывает компаниям руки в части обработки персональных данных. Если вы считаете, что такой конфуз грозит лишь частным пользователям (да и то безалаберным), прочитайте пару абзацев ниже – я покажу, что это не так. Бизнес (и не только малый) защищен немногим больше. И подчас ведет себя столь же беспечно.

2. Джейсон Дитжиан изначально не доверял Facebook и не пользовался им. Но «фэйсбук-мафия» настигла и его. Джейсон не смог воспользоваться услугой каршэринга (продвинутый вариант краткосрочной аренды авто), потому что не имел аккаунта в соцсети. Он справедливо рассуждает о том, что интернет-аккаунт становится для западного мира своего рода кредитной историей, универсальным идентификатором, без которого получить доступ к некоторым услугам будет сложнее и сложнее.

3. Редактор New York Times рассуждает о скандале с приложением Unroll.me. Я, кстати, использовал этот сервис. За одну минуту он показывает все подписки с твоего e-mail, и позволяет избавиться от лишнего, расчистив жизнь и почту от мусора. Правда, между делом приложение сканировало и корзину, находило там квитанции сервиса такси Lyft и анонимно отправляло эти данные их главному конкуренту – Uber.

4. Четвертый сюжет напоминает второй, только ближе и понятнее. Pornhub ввел обязательную аутентификацию российских пользователей через соцсеть «ВКонтакте». Мол, эта мера позволит избежать появления на сайте несовершеннолетних посетителей. Снова просвечивается история с виртуальным паспортом, не так ли?

Ну, поскольку мне уже есть 18, можно попробовать зарегистрироваться. Жмем на огромную кнопку в центре страницы и видим открывающееся модальное окно. По сути, это отдельная страница, имеющая собственный url. Давайте посмотрим, какой.

аутентификация

Я выделил цифры после символов client\_id и скопировал их в буфер обмена. Теперь сайт нужно быстро закрыть (иначе затянет) и перейти в рекламный кабинет «ВКонтакте».

При выборе аудитории есть область «Интересы», внутри которой находим поле «Приложения и сайты». Вставляем туда нашу комбинацию цифр – VK показывает, что мы не ошиблись.

целевая аудитория

«ВКонтакте» нашел примерно 300 тыс. человек. Дальше можно настраивать географию, соотносить аудиторию с посетителями собственного сайта и настраивать рекламу. Креативы придумайте сами. Повесьте скрытым постом безобидную шутку или мотивирующую карточку, а лайки и комментарии к ней – суть деанонимированные пользователи Pornhub. Печально. Люди ведь не знают, по какому принципу видят у себя в ленте вполне безобидную запись. Это не гипотеза, я потратил 150 руб., чтобы убедиться. Так что ставьте лайки аккуратно. Если покликать по демографии, то можно прийти к одному из двух заключений:

Pornhub не знает, что делает «ВКонтакте» с данными, которые соцсеть получает через авторизацию.

Pornhub показывает всем и каждому, что в России на сайте зарегистрировано 30 000 несовершеннолетних пользователей, 2500 из которых нет и 14 лет. Кроме того, дает возможность настраивать рекламу на них кому угодно.

Такие дела. Впрочем, регистрация через «ВКонтакте» стоит не только на порносайтах, но и на классических коммерческих приложениях. Доставка еды, финансовые услуги, подписка на книги через Bookmate или, например, покупка одежды в магазине LaModa. Здесь существенно ниже чувствительность пользователя к приватным данным, но вот для бизнеса – это, на мой взгляд, дыра.

Как данные перетекают из рук в руки

99% зарегистрировавшихся – реальные клиенты, а не случайные подписчики странички в соцсетях. Что вы скажете, если вас попросят передать клиентскую базу конкурентам? Звучит странно, но очень многие – от крошечных интернет-магазинов до лидеров – делают это не задумываясь.

Я называю это уязвимостью данных. Мой пример далек от эксплуатации программного бага и изощренного механизма кражи данных. Абсолютно белый инструмент «из коробки», хорошо знакомый многим директологам. Таких «уязвимостей» довольно много. Некоторые из них может использовать каждый, доступ к другим получаешь, воспользовавшись услугами компаний, занимающихся сбором и сегментаций данных из открытых и закрытых источников. И даже если подходить к вопросу максимально серьезно, быть на 100% защищенным, как показывает пример Lyft, практически невозможно.

Вернемся в «ВКонтакте» и возьмем примеры малого бизнеса. Вы – модный и дорогой стилист. Клиенты вас знают лично, связи и мастерство – ваш главный архив. Есть десятки парсеров для «ВКонтакте», которые помогают не просто собрать и сегментировать ваших друзей, но и выбрать среди них тех, кто охотнее других ставит вам лайки, комментирует публикации, ходит на мероприятия или дружит с другими модными персонами. То же относится к любым бизнес-страницам. Нехорошо, да? Мы часто читаем про откровенно грубое и нахальное вмешательство в частную жизнь пользователей, про сомнительное использование личных данных, но редко говорим об этом в контексте бизнеса. Я абсолютно убежден, что и на правовом, и на техническом, и на информационном уровне бизнес нуждается в такой же защите. Особенно малый.

Новость №5. В «Яндекс.Аудиториях» появилась возможность покупать сегменты у сторонних поставщиков. Интересные срезы, рекомендую изучить. К примеру, можно найти посетителей торговых центров Москвы и Петербурга.

Яндекс.Аудитория

Пока только два региона и крупные центры, но вскоре непременно появятся другие точки. Сюжет напоминает историю с Джейсоном, который отчаянно не желал регистрироваться в Facebook, но «мафия» его достала. Ваша торговая точка может появиться в таргетинге крупных платформ, даже если у вас нет страниц в соцсетях, а на сайте не стоят Google Analytics, Яндекс.Метрика, пиксели соцплатформ и кнопки share.

Нужно ли контролировать индустрию данных?

Информацию о ваших клиентах можно получить откуда угодно (хотя бы через геолокацию на мобильном, бесплатный Wi-Fi, как это делает «Максимателеком»...), а потом вполне официально торговать данными через «Яндекс.Аудитории» или другой сервис. Если уж этого нельзя полностью избежать, то контролировать данные, которые проникают во внешний мир, определенно нужно. Вот самый простой пример, который я приводил в статье про базовую стратегию в соцсетях. Если вы расстались с подрядчиком, штатным маркетологом или просто офис-менеджером, имевшим доступ к базе клиентов, показывать им рекламу сможет кто угодно. Но поскольку пользователь не знает, кто и по каким параметрам таргетирует рекламные сообщения, доказать это или хотя бы заметить практически невозможно.

Обычно под безопасностью данных подразумевают защиту от взломов. Но большая проблема не в хакерских атаках, а в данных, которые в рабочем режиме отправляются на сторонние платформы и гипотетически могут быть использованы конкурентами и частными лицами. Это относится к приватности конкретных людей и защищенности организации. Например, если вы работаете в сфере недвижимости и ставите у себя на сайте кнопку «Зарегистрироваться через Facebook», ваши конкуренты могут получить доступ к части вашей аудитории через таргетинг «недвижимость» в Facebook. Однако там она будет сильно размыта множеством других источников. Показывать рекламу исключительно клиентам вашей компании я не смогу. «ВКонтакте» ситуация иная. Таких нюансов довольно много, будет все больше. Уверен, в скором будущем специализация «контроль данных» станет более популярной, чем просто защита. Специалисты, работающие на стыке права и технологий, которые помогут бизнесу и частным лицам, оставаясь частью информационного сообщества и пользуясь его преимуществами, защитить самые критичные данные, станут крайне востребованы.

Лирический финал

Я либертарианец. И идея вмешательства государства во что-либо мне не близка. Когда слышишь о государственном регулировании интернета, на ум приходят «закон Яровой», стремление регистрировать блогеров как СМИ и прочее средневековье. Однако нелепое исполнение не должно отвлекать от сути. Госрегулирование – единственная возможность обеспечить достаточную приватность и контроль над личными данными. Аманда Хесс из NYT делает точное замечание: компании, собирающие данные, знают о нас практически все (в том числе, что мы сами о себе не знаем), но мы – совсем немного. О том, какие именно данные они собирают, откуда, как используют, кому отдают/продают, как долго хранят, как интерпретируют, в какие стеки собирают и так далее. Эти сведения должны быть открыты как для частных лиц, так и для бизнеса. Продажа и границы использования этих данных – предмет серьезной общественной дискуссии. Но в одном я уверен абсолютно точно. Главная угроза – вовсе не торговцы наркотиками, террористы или несчастные оппозиционеры, за которых их выдают, а крупные IT-корпорации, фактически монополизировавшие сбор, обработку и коммерческое использование пользовательских данных.

# Названы самые масштабные утечки 2017 года

В течение года эксперты «СёрчИнформ» следили за новостями утечек и, подводя итоги, собрали самые громкие инциденты.

С инцидентами безопасности приходится сталкиваться даже IT-мастодонтам вроде IBM и корпорациям-гигантам вроде Yahoo!. Среди причин – старый человеческий фактор и новые инсайдерские трюки, непреходящая угроза уязвимости. В 2018 году едва ли станет лучше, поэтому работайте с персоналом, контролируйте активы компаний, просчитывайте риски и совершенствуйте системы безопасности.

По объему скомпрометированных данных

«Матерь всех утечек»: в открытом доступе оказались 560 млн адресов электронной почты и паролей

Персданные 198 миллионов избирателей США хранились на «облаке» Amazon в открытом доступе

В Индии из государственной системы биометрической идентификации Aadhaar «утекли» уникальные ID-номера 135 млн граждан

О находке в мае 2017 года сообщил Центр изучения безопасности MacKeeper. Упорядоченную и удобную для чтения базу весом 75 гигабайт назвали «матерью всех утечек» из-за данных, которые уже были скомпрометированы ранее. Эксперты установили, что речь идет как минимум о десяти известных утечках данных пользователей MySpace, LinkedIn, Last.fm, Dropbox, Tumblr и других популярных ресурсов.

База размером 1,1 терабайт включала обширные сведения об избирателях для предвыборного штаба Дональда Трампа: их имена и даты рождения, телефоны и домашние адреса, данные о регистрации избирателя и даже религиозные и этнические взгляды. Информация о 198 миллионах граждан – 62% населения США – не была защищена даже паролем. Федеральные власти узнали об уязвимости 12 июня 2017 года, утечку устранили в течение двух суток. Ответственность за инцидент понес один из подрядчиков предвыборного штаба Республиканской партии.

По кодам из 12 цифр можно было установить имена и фамилии, номера телефонов и адреса проживания, а также реквизиты банковских счетов жертв. Анкеты из крупнейшей в мире базы с биометрической информацией также включали снимки радужной оболочки глаза и отпечатки пальцев. Такой ID-номер используется как удостоверение личности в разных ситуациях, от покупки SIM-карты до оформления госдотаций, поэтому утечка могла обернуться волной создания поддельных личностей. По данным Центра изучения интернета и общества (The Centre for Internet and Society, CIS) причиной утечки не могли стать уязвимость системы или внешняя атака. Ответственность за майский инцидент 2017 года несут чиновники, организующие сбор и обработку персональных данных.

По национальному масштабу

Данные медстраховки всех жителей Австралии выставили на продажу

Базу с персданными «почти каждого» жителя Малайзии предложили за один биткоин

Персональные данные миллионов граждан Швеции утекли по вине IT-подрядчика

В июле 2017 года на одном из популярных форумов в даркнете появилось объявление о продаже данных Medicare Australia– системы государственного медицинского страхования. Автор сообщал, что готов передать персданные любого австралийца всего за 0,0089 биткоина (порядка $22). По данным Guardian Australia, за 10 месяцев автор объявления продал не меньше 75 файлов, информации в которых было достаточно для создания поддельных карт Medicare с реальными данными.

Пользователь сообщил журналистам, что пропуском в государственную систему стала ее уязвимость. Однако расследование продолжается.

В ноябре 2017 года была зафиксирована одна из крупнейших утечек клиентских данных в Азии. База, размещенная в «темном интернете», включала 46,2 млн мобильных телефонов и данных SIM-карт, а также домашние адреса и номера ID-карт клиентов минимум 12 местных операторов связи. Для сравнения: население Малайзии едва превышает 31 млн человек. Министерство связи страны рассматривает несколько возможных источников утечки. В частности, инсайдером мог быть работник подрядчика, который обеспечивал обработку этих данных для Малазийской комиссии по коммуникациям и мультимедиа (МСМС).

Государственное транспортное агентство Швеции поручило обслуживание IT-инфраструктуры, включая обработку персданных, корпорации IBM. А те делегировали задачу подрядчикам в Румынии и Чехии. Фотографии, имена и адреса миллионов граждан Швеции утекли уже оттуда. В частности, рассекретились данные о владельцах транспортных средств, принадлежащих полиции и армии, о сотрудниках спецслужб и пилотах ВВС, подозреваемых в преступлениях и участниках программы защиты свидетелей. Утечку данных обнаружили в 2016 году. По итогам расследования глава агентства получил штраф в 70 тыс. шведских крон (примерно 7,5 тыс. евро) и был уволен. 27 июля 2017 года из-за скандала вокруг утечки постов также лишились министр внутренних дел и министр инфраструктуры.

По величине потерь

Американская розничная сеть Target выплатила $75 млн за утечку четырехлетней давности

Расходы, связанные с утечкой данных кредитного бюро Equifax, превысят $100 млн

В результате утечек бизнес Yahoo! потерял 87% от своей рыночной стоимости

Шестой по величине ритейлер США оплошал в декабре 2013: уязвимость платежных терминалов стала причиной утечки платежных данных 40 млн банковских карт. Через месяц количество пострадавших достигло 70 млн. $39 млн Target возместила банкам, $10 млн – жертвам инцидента, $6,75 млн – юристам. А в мае 2017 года ритейлер выплатил еще $18,5 млн штрафа. Правление компании согласилось на сделку с генеральными прокурорами 47 штатов и округа Колумбия. Сумму штрафных санкций распределили пропорционально между штатами. Итоговая «стоимость» одного инцидента с учетом штрафа достигла $74,75 млн. Соглашение Target с властями стало крупнейшей сделкой в новейшей истории США.

Мошенники проникли в сеть компании в мае 2017 года и в течение трех месяцев могли беспрепятственно обращаться к личной информации минимум 143 млн клиентов. Среди данных фигурировали имена и даты рождения, адреса, номера соцстрахования, а в некоторых случаях и реквизиты банковских карт. Известно, что утечка произошла в результате внешней атаки, однако злоумышленники использовали уязвимость платформы Apache Struts для создания веб-приложений. Причем об ошибке было известно за месяц до инцидента. А после него команда Hold Security начала изучать другие домены Equifax и в том числе подразделения в Аргентине. Сократили URL-адрес местной службы по работе с претензиями – и попали на внутренний портал Veraz. Использовали в качестве логина и пароля «admin» и «admin» – и вошли в систему. Так под угрозой находились номера удостоверений личности минимум 14 тыс. аргентинцев, и потенциально утечка могла коснуться десятков тысяч клиентов. Адвокаты оценили «небрежность КБИ в 70 млрд долларов компенсации. Расследование ведется при участии госорганов на федеральном уровне. Акции компании продолжают дешеветь, чистая прибыль сократилась на 28%. По оценкам компании, расходы с учетом исков и штрафов могут превысить $100 млн.

Решение было принято 30 августа 2017 года в окружном суде Сан-Хосе, штат Калифорния: компания ответит за три масштабные утечки и более трех лет их сокрытия. Первый инцидент произошел в 2013 году – утекло более миллиарда учетных записей. В 2014-м были скомпрометированы данные более 500 млн аккаунтов. Третье нарушение произошло в 2015-2016 гг. Вскоре после того, как инциденты получили огласку, Verizon Communications Inc. выкупила интернет-бизнес Yahoo!, сбив цену с $37 млрд. до $4,76 млрд. Но теперь предстоящие судебные тяжбы обещают компании немалые расходы.

Адвокат истцов и глава исполнительного комитета, курирующего дело, заявил, что это самое большое нарушение конфиденциальности в истории. В 93-страничном обосновании судебного решения отмечается, что данные некоторых пострадавших уже использовались мошенниками и могут быть использованы в будущем. Из заявлений истцов также следует, что некоторым из них пришлось потратить деньги на защиту личной информации.

# Цифровые души. Сколько стоят ваши персональные данные

Ноябрь 2017

У каждого есть цена. Причем в буквальном смысле — волосы, кости, внутренние органы стоят дорого. На черном рынке все тело человека [стоит](https://www.popmech.ru/science/387862-skolko-stoit-chelovek-ot-volos-do-pochek-i-skeleta/) не менее 58 млн долларов. Персональные данные пользователя стоят намного меньше — но продаются и перепродаются гораздо активнее.  
  
Массовые утечки данных происходят регулярно. Вот несколько самых громких инцидентов за последние несколько лет:

* летом 2016 года хакеры [взломали](https://club.esetnod32.ru/news/novosti_it/kto-vinovat-i-chto-delat/) более 100 млн аккаунтов ВКонтакте
* в декабре 2016 года стало известно о взломе миллиарда (!) аккаунтов Yahoo
* в июле 2017 в результате взлома компании Equifax (бюро кредитных историй США) года в руки злоумышленников [попали](https://meduza.io/news/2017/09/26/glava-krupneyshego-byuro-kreditnyh-istoriy-ssha-podal-v-otstavku-posle-utechki-dannyh-143-millionov-chelovek) персональные данные 143 млн человек
* в 2015 году хакерская группа The Impact Team опубликовала архив с данными 32 млн пользователей сайта знакомств Ashley Madison

Цена персональных данных зависит от целей покупателя. По данным Financial Times, дешевле всего стоят общие данные потенциальных клиентов: возраст, пол и место жительства — цена за одного пользователя составляет всего $0,0005.   
  
Информация о покупательской активности стоит вчетверо дороже — $0,0021. Выше всего ценятся медицинские данные — за них платят до $0,26 (да-да, 26 центов). Если сложить стоимость всех «пакетов», то цена информации о каждом пользователе не превышает одного доллара.   
  
На черном рынке данные о пользователе стоят примерно столько же, однако там можно приобрести более детальные досье.  
  
Используемая для краж и мошенничества финансовая информация ценится очень высоко: так, стоимость аккаунта на eBay или PayPal может составлять от $200 до $500. Учетные записи с продолжительной историей оцениваются выше, т.к. они выглядят менее подозрительно. Таким образом злоумышленники «покупают» дополнительное время для использования полученных данных, прежде чем мошенничество будет раскрыто. Для сравнения, новый аккаунт в PayPal оценивается всего в $10.  
  
По [статистике](https://www.ibm.com/security/data-breach/) IBM, средние потери от краж данных в 2017 году составили $3,62 млн (в исследовании участвовало 419 компаний по всему миру). За прошедший год данные пользователей упали в цене на 10% — в 2016 году убытки компаний составляли $4 млн. Зачем тратиться на защиту корпоративной сети, если издержки уменьшаются сами собой?  
  
В то же время растут объемы информации о пользователях, которыми вполне легально владеют Google, Facebook, Apple и другие IT-гиганты.   
  
Австрийский студент Макс Шермс (Max Schrems) в ходе длительных переговоров [вынудил Facebook](https://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/#220a18087b0b) предоставить все имеющиеся у компании данных о нем. PDF-файл объемом 1 222 страницы содержал информацию о работе Марка, его личной жизни, отношениях с окружающими, а также переписку и фото (в т.ч. давно удаленные из профиля снимки).  
  
Некоторые пользователи считают передачу персональных данных третьим лицам неизбежной и пытаются извлечь из этого выгоду. В 2012 году веб-разработчик Федерико Заньер (Federico Zannier) запустил на Kickstarter [проект A bite of Me](https://www.kickstarter.com/projects/1461902402/a-bit-e-of-me), в рамках которого продавал свои личные данные всем желающим: историю просмотров браузера, скриншоты страниц, фото с веб-камеры, [геоданные](https://club.esetnod32.ru/articles/analitika/shpion-vyydi-von/) и даже записи видео с экрана ПК. Данными Федерико заинтересовались 213 человека, которые заплатили более $2700. Это не единичный случай, однако далеко не все подобные проекты принесли создателям известность и хоть какую-то прибыль.  
  
Узнать стоимость ваших собственных данных можно с помощью [этого сервиса](http://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2xm2lDgsY). Цена потребительских портретов редакторов «Мы ESET» составляет $0,5915 и $1,1010. Досье на нашего стажера обойдется условной [E Corp](https://club.esetnod32.ru/articles/analitika/mr-robot-s02-e01/) в $0,7957.   
  
Стоимость растет для женатых людей с детьми, людей с лишним весом и разнообразными хобби, а также для владельцев недвижимости. Логично, ведь таким пользователям можно предложить гораздо больше товаров и услуг.  
  
Если вы решили подзаработать на продаже личных данных, не стоит спешить. Скорее всего, ваши данные давно уже выставлены на продажу в даркнете или даже на местном радиорынке. Поэтому мы рекомендуем [сократить объем](https://club.esetnod32.ru/articles/analitika/ukhodim-s-radarov/) информации, которую вы передаете крупным IT-компаниям, а также подумать о том, чтобы [удалить свои профили](http://justdelete.me/) из ряда сервисов.

# Тотальная слежка Google

По данным интернет-издания Quartz, с начала 2017 года мобильные устройства на базе Android собирают информацию об адресах соседних сотовых вышек и отправляют эти данные в Google. В результате компания имеет доступ к данным о местонахождении отдельных лиц и их передвижениях, даже если сами пользователи этого не хотят.  
  
По данным источника Quartz, Google стала применять Cell ID после изменения в службе push-уведомлений Firebase Cloud Messaging, которая принадлежит компании и работает на телефонах Android по умолчанию. Таким образом, даже устройства, сброшенные до заводских установок, с отключенными службами геолокации отправляли информацию в Google. Смартфоны с сотовыми данными или Wi-Fi соединением, предполагает Quartz, отправляли данные каждый раз, когда они попадали в зону действия новой сотовой вышки. Когда Android-устройства были подключены к сети Wi-Fi, они отправляли адрес в Google, даже если у них не было установленных сим-карт.  
  
В Google подтвердили информацию Quartz о сборе данных о местоположении пользователей смартфонов, однако заявили, что эти данные никогда не использовались и не хранились. В компании также заявили, что до конца ноября планируют отказаться от подобной практики.  
  
«В январе нынешнего года мы начали изучать идентификатор сотовой связи Cell ID в качестве дополнительного способа для повышения скорости доставки сообщений. Тем не менее мы никогда не добавляли Cell ID в нашу систему сетевой синхронизации, так что эти данные немедленно

уничтожались.

Мы обновили нашу систему, чтобы она больше не запрашивала идентификатор сотовой связи»,— сообщил представитель Google в письме Quartz. Также, по словам Google, система Firebase Cloud Messaging, которая контролирует push-уведомления и сообщения, отделена от служб геолокации, которые предоставляют местоположение пользователей в Google.

# За нами следят. FinFisher шпионит за пользователями семи стран

25 сентября 2017

Вирусная лаборатория ESET обнаружила новые операции кибершпионажа с использованием вредоносного ПО FinFisher в семи странах мира. Вектор заражения указывает на возможное участие в распространении шпионской программы крупного интернет-провайдера.   
  
FinFisher (FinSpy) – шпионское ПО, разработанное компанией Gamma Group International, которое ранее продавалось правоохранительным органам и правительственным структурам по всему миру. В программе предусмотрен широкий спектр возможностей для слежки через веб-камеру и микрофон, а также функции кейлоггинга (перехват нажатия клавиш), кражи файлов, прослушивания через Skype и др.   
  
Для распространения FinFisher используются различные механизмы заражения, включая целевой фишинг, установку вручную (если у атакующих есть физический доступ к устройству), уязвимости нулевого дня и watering hole атаки (заражение сайтов, которые предположительно посещают потенциальные жертвы).   
  
В последних операциях FinFisher обнаружен новый вектор – схема man-in-the-middle (атака посредника) с возможным участием интернет-провайдера. Вектор используется в двух странах, где обнаружены последние модификации FinFisher.   
  
В рамках этой схемы, когда объект слежки собирается скачать одно из популярных приложений, его перенаправляют на версию программы, зараженную FinFisher. Процесс переадресации невидим для пользователя. После скачивания на устройстве появляется не только легитимное приложение, но и шпионское ПО.  
  
Аналитики ESET обнаружили троянизированные версии WhatsApp, Skype, Avast, WinRAR, VLC Player и некоторых других программ, но теоретически так можно использовать любое легитимное приложение.   
  
Один из образцов FinFisher, обнаруженный ESET, был замаскирован под исполняемый файл мессенджера Threema. Приложение обеспечивает безопасный обмен мгновенными сообщениями со сквозным шифрованием, его устанавливают пользователи, стремящиеся к конфиденциальности.   
  
Акцент на пользователей, интересующихся технологиями шифрования, не ограничивается мессенджерами. Например, один из установочных файлов, зараженных FinFisher, предназначался для установки ПО для шифрования диска TrueCrypt.

# Банки тоже следят

Внедрить скоринг заемщиков по психометрическим моделям Сбербанк планирует в 2018 г., пишет RNS со ссылкой на вице-президента кредитной организации Александра Ведяхина.

Идеальный вариант — что лицо, телефон, чтобы мы поняли кто, все следы, все источники, чтобы стало понятно, что это за человек, и если он лайкает тюремные четки и «Владимирский централ», то навряд ли ему надо сразу одобрять кредит, скорее всего, еще раз надо что-нибудь посмотреть, — пояснил он (цитата по «Интерфаксу»).

Сейчас банк тестирует эту технологию на ограниченной выборке согласившихся клиентов, и корреляция очень серьезная, отметил г-н Ведяхин. По его словам, метод основан на технологии сбора психометрических данных через социальные сети, которую создал ученый Стэнфорда Михаил Косински.

Банкиры не впервые говорят об использовании соцсетей для проверки благонадежности клиентов. Ранее об этом рассказывал председатель правления СКБ-банка Денис Репников: «По поведению человека в соцсетях, его профилю, его знакомым можно определить, находится он в зоне риска или нет».

«Человеческую сущность и его поведение сегодня можно точно проанализировать. По кликам в Facebook с достаточной точностью можно определять поведенческие и психологические аспекты личности. 11-12 лайков позволяют сделать вывод о вас, который будет совпадать с оценкой коллег. А примерно 230 лайков позволяют понимать вашу личность лучше, чем понимают ее ваши близкие, например, муж или жена», — говорил президент Сбербанка Герман Греф, имея в виду исследование ученых Кембриджского и Стэнфордского университетов.

Автор: Андрей Пермяков

Примерно такую же технологю внедряет СКБ-банк.



# Из-за технологий исчезло слово "граммофон". Следующее — слово "свобода"

Анатолий Темкин: 21.09.2017

В ближайшие 10 лет при помощи телефона или компьютера можно будет узнать абсолютно все о человеке, который находится на расстоянии 50-ти метров от вас. Для этого даже не надо будет знакомиться.

Профессор Бостонского университета и заведующий кафедрой компьютерных наук колледжа Метрополитен при Бостонском университете Анатолий Темкин выступил на конференции Big Data Conference и заставил слушателей задуматься о том, куда исчезла наша свобода, как скрыть пин-код от своей карты и при чем тут большие данные. Главные тезисы выступления публикует портал [RB.RU](https://rb.ru/).

Про свободу, которой у нас больше нет

— Люди медленно и плохо считают, зато замечательно распознают образы. А что делают компьютеры? Компьютеры считают быстро и без ошибок, но образы распознают не очень хорошо. Значит, что мы стремимся сделать? Мы стараемся создать нейронные сети, которые бы распознавали образы и определяли корреляции так же хорошо, как это делаем мы. При этом мы сами не очень понимаем, как наш мозг работает.

Если нейронные сети будут обладать такой же структурой, как наша голова, тогда компьютеры будут делать все то же, что делаем мы. При этом заметьте, что человеческая голова — это звучит красиво — работает на 3 или 4% от того, как могла бы работать.

Получается, что на меньшем количестве нейронных сетей нам удастся добиться того, что сейчас получается, когда доходит до нашего мышления. Преподаватели русского языка поставили бы мне двойку за такие выражения, но все так и есть.

Непонятно, будем ли мы, как человечество, довольны этим, потому что мы абсолютно потеряли нашу прайваси. Прайваси — это не безопасность, это свобода. Именно ее мы и потеряли. Мы ее потеряли безвозвратно и навсегда. Я докажу вам это на нескольких примерах.

Пример 1. Дьявольское устройство

Каждый из нас носит дьявольское устройство в кармане. Когда вы покупаете это устройство, вы как бы заключаете договор с государством.

Договор такой: нам разрешают звонить, обмениваться сообщениями и так далее, но за это мы разрешаем государству знать, где мы находимся. Даже когда ваш телефон выключен, это не имеет абсолютно никакого значения. Государство знает, где вы находитесь 24 часа в сутки.

Есть еще такая штука, называется [GPS](http://www.dk.ru/wiki/gps-navigator#binding), она есть и в машинах, и в телефонах. Государство знает, где мы находимся, с точностью до метра 24 часа в сутки. Но это еще не все.

Пример 2. С [Google](http://www.dk.ru/wiki/google#binding) вы всегда откровенны

Сейчас я вам расскажу, как мы теряем прайваси. У нас по закону не имеют права прослушивать телефонные разговоры. Я думаю, что этот закон не нарушается, потому что это ведет к большим проблемам. Телефоны не прослушиваются. Если простой американец звонит за границу, то все разговоры записываются, машина анализирует их, но это другой разговор. Что важно — это meta data: кто звонил, куда звонил, откуда и длина разговора.

Если у вас имеется огромное количество meta data, то вам даже не нужно знать содержание разговора, чтобы понять, о чем разговор.

Разбираем кейс... Итак, вы немножко заболели. Что вы делаете?

1.      При условии, что у вас есть компьютер. Вы идете в Google. Вбиваете туда все симптомы. При этом, если кому-нибудь вы могли бы и соврать, то с Google вы всегда откровенны.

2.      Вы написали все симптомы. Это одна data, которую Google запомнит навсегда. Что вы делаете дальше?

3.      Вы звоните врачу с целью прийти и полечиться. Позвонили врачу, очень хорошо, известно, когда вы звонили, известно, как долго вы разговаривали.

4.      После этого вы пришли к врачу. Врач вам выписал лекарства. Вы пошли в аптеку и заплатили вашей кредитной картой. Абсолютно вся эта информация сохраняется.

5.      Потом ваш врач отправил вас еще к какому-нибудь специалисту. И к нему вы тоже записались и тоже прогуглили все, что касается того, что вам сказал врач. Вся эта информация соединяется и коррелируется.

Где мы здесь потеряли прайваси? Не там, где появляются конкретные данные о каждом факте, а там, где это все коррелируется.

Теперь о нашем будущем...

Наше будущее очень светлое. Оно заключается в следующем: вы идете по улице, навстречу вам идет человек. Вы хотите познакомиться с этим человеком, расстояние 50 метров. Вы смотрите на ваш телефон. Там вся информация об этом человеке: имя, фамилия, отчество, где живет, женат — не женат. Болел: да — нет. Если да, то чем. Это все будет максимум через 10 лет.

Дальше вы хотите пойти в магазин, открываете дверь, входите, на вас внимательно смотрит продавец. У него в телефоне полная информация о вас. А главное — какой у вас доход. Потому что в зависимости от дохода вам будут предлагать разные товары.

Например, вчера я гулял по Малой Бронной и видел такое количество Майбахов, какое за 30 лет жизни в Америке не видел. Так вот, если вы заходите в магазин дилера, то продавец вместо [Toyota](http://ekb.dk.ru/wiki/toyota#binding) сразу предложит вам Майбах. По-английски это называется pointed advertisement — когда вы совершенно точно знаете, кто ваш клиент и чего он хочет, еще до того, как он появился. Я считаю, что это полная потеря прайваси.

А где будущее Big Data?

Будущее в том, что все нейронные сети будут совершенствоваться, они будут более мощными. Мы будем делать намного более мощные вычисления. Для биологии и медицины это совершенно замечательно, потому что лекарства будут тестироваться вне человеческого организма и тестироваться намного быстрее. Это очень хорошо.

При этом мы абсолютно потеряем нашу прайваси. Ее просто не будет. Слово будет, а смысла, который оно несет, не будет. Я пытался придумать слово, которое есть, но смысла его для меня уже нет. Это слово «граммофон». Эта же судьба ждет и слово «прайваси».

Возвращаясь к Big Data, самое большое значение будет иметь интеграция разных платформ, если не брать в расчет нейронные сети. Big data будет вылавливать закономерности и корреляции. Вопрос в том, а что они будут означать. У вас имеется огромное количество данных, компьютер описал закономерность, а что это означает, с точки зрения здравого смысла? Это отдельная проблема.

Закономерностей в мире множество, но что-то мы просто не понимаем. Например, такая закономерность: поездка в метро от одной станции до другой занимает 11 минут, а мороженое стоит 50 рублей. Имеет ли это какой–то смысл?

Глупый пример, но такая закономерность тоже может быть выявлена. Это то, что нас ждет в будущем.

# Рот не на замке: где границы информационной открытости

Константин Евдаков Генеральный директор, Москва

Почему полезно информировать сотрудников о зарплатах коллег и обсуждать в коллективе другие

Информация всегда будет разделяться в компании по разным уровням. Одни темы – для разговоров в кругу владельцев бизнеса, другие – для ушей топ-менеджеров, третьи – для обсуждения всеми сотрудниками. В большинстве бизнесов работа – это не друзья и не семья. И любая деятельности внутри компании, в том числе разговоры и обращения, должна быть нацелена на достижение результата.

Другой вопрос, что часто такое разделение происходит потому, что некоторые факты, например, зарплату сотрудников, принято держать в секрете. Хотя реальной пользы от сокрытия такой информации мало. Например, финтехи – тот бизнес, с которым сталкиваюсь я – по большей части предельно прозрачны. И я не припомню, когда в последний раз сталкивался с тем, чтобы кто-то из сотрудников был недооценен или переоценен. В подавляющем большинстве случаев каждый зарабатывает ровно столько, сколько стоит. А получение новых навыков и умений, которые, предположим, есть у коллеги, чья работа оплачивается более высоко, могут позитивно сказаться на собственном благосостоянии.

И это лишь один из примеров. Прагматизм в определении публичности той или иной информации должен стоять во главе угла. Где границы открытости в разных бизнес-сферах?

Финансовая информация

В категорию «лучше промолчать» она чаще всего попадает вполне заслуженно. С одной стороны, утечка информации может нанести ущербу бизнесу. Особенно для компаний, которые торгуются на бирже. Взять тот же «Тинькофф Банк», в штате которого несколько десятков финансистов. Все они примерно представляют, как обстоят дела в компании и когда ждать скачка или падения котировок. Нужно ли объяснять, почему раскрывать эту информацию невыгодно? Признаться, я не представляю, как именно решается этот вопрос в самом банке. Думаю, что сотрудники подписывают специальное соглашение о неразглашении.

Проблема также в том, что финансовая информация по своей сути является узкопрофессиональной. И непрофессионалом может быть воспринята неправильно. То, что является совершенно рядовой работой директора по привлечению инвестиций (к примеру, привлечение к отчетной дате большой суммы денег), сотруднику логистического отдела может показаться тревожным сигналом.

Ошибки и критика

Презентации всех американских компаний начинаются со слайда об успехах и достижениях. Презентации японцев – с того, какие ошибки были допущены. И этот восточный подход мне кажется более конструктивным и близким. Второй шанс нужно давать каждому, а третий – никому. Ошибки – это один из наиболее эффективных инструментов собственного роста. Поэтому их конструктивное обсуждение – закономерный бизнес-процесс, который должен быть отлажен в компании.

Конечно, критика не должна быть эмоциональной, переходящей в разговор на повышенных тонах и скатывающаяся до оскорбительных формулировок. Но я не вижу ничего плохого в том, чтобы выносить обсуждение в общее пространство. Тогда этот разговор поможет другим сотрудникам не допустить подобную ошибку.

Собственные ошибки и негативные новости

С такой же степени откровенности и конструктива руководитель должен оценивать собственные промыхи. Любой опыт, которым он может поделиться с подчиненными, – это позитивный опыт.

Здесь, правда, стоить сделать небольшую оговорку. Те ошибки, которые могут привести к фатальным для компании последствиям и которые еще не исправлены, вряд ли предназначены для ушей коллег, не способных повлиять на процесс. Безвыходных ситуаций не бывает, на уровне топ-менеджмента всегда может прийти решение той или иной проблемы. Но на уровне исполнителей, которые не могут (и не должны уметь) решить вопрос, дискуссия такого рода зародит сомнения в будущем компании, спровоцирует поиск нового места работы.

К слову, на те же критерии стоит ориентироваться, решая, какие новости сообщать коллегам, а о каких стоит умолчать. Вызовы, которые получает компания, способны принять не все сотрудники. По меньшей мере, на этапе планирования стратегии выхода из кризисной ситуации. Эта информация должна обсуждаться на уровне топ-менеджмента до того момента, пока эта стратегия не будет определена.

Обсуждение коллег

В большинстве случаев, этот вопрос лежит не в плоскости правильного бизнес-поведения, а самой элементарной этики. Конечно же, плохо обсуждать кого бы то ни было за его спиной. Но и в этом случае стоит придерживаться прагматичного подхода. К примеру, если мне не нравится работа заместителя операционного директора, то я вполне могу обсудить этот вопрос с ним самим. Но я вряд ли стану обсуждать его с директором по маркетингу.

Что касается оценки результатов работы сотрудников, то она может быть публичной. Обсуждение этой темы мне не кажется чем-то предосудительным.

Перевернутая пирамида

Чаще всего руководство компании рисуют на вершине пирамиды, а сотрудников – на различных низовых уровнях. В последнее время становится все более успешной модель перевернутой пирамиды. В ней многие процессы идут от подчиненных к руководству, а не наоборот. В таком мире единственная возможность для руководителя услышать своих сотрудников – общение с ними без предосудительных офисных табу. И потому максимальная открытость со своими коллегами может оказаться преимуществом, позволяющим достичь новых коммерческих успехов.

# Смартфон в доспехах. Как защититься от слежки на 100%

10 января 2018

Советы

Пока одни пользователи пытаются не нарушать хотя бы базовые правила инфобезопасности, другим недостаточно даже корпоративного уровня защиты. И последние в чем-то правы — инфобезопасности не может быть слишком много. Как говорится, даже если у вас паранойя — это не значит, что за вами не следят.

Для самых осторожных пользователей мы локализовали руководство по безопасности от Wired.

Изолировать нельзя подключить

Лучший способ защиты от взлома — полная изоляция устройства от сети. Нереалистично? Если на ПК хранятся суперсекретные данные или пара биткоинов на черный день, то отключение от интернета не кажется неоправданной мерой.

Отключить беспроводные соединения (Wi-Fi и Bluetooth) можно в настройках ОС, однако сотрудник отдела безопасности Фонда свободы прессы Дэвид Уэрта (David Huerta) рекомендует физически удалить все беспроводное оборудование.

Также стоит использовать мини-компьютеры с широким выбором комплектующих. В качестве примеров можно назвать Intel Nuc и Gigabyte Brix. По умолчанию эти устройства поставляются без встроенных модулей беспроводной связи.

Таким образом, единственной угрозой останется физический доступ к ПК. Можно запереть устройство в сейфе и заблокировать вход в систему надежным паролем, а можно пойти еще дальше — удалить жесткий диск. Вместо него можно использовать загрузочную флэшку с анонимной операционной системой Tails, которая не оставляет следов работы на компьютере. Если на ПК не будет данных, то он перестанет быть целью хакеров.

Клетка Фарадея

Известный факт — отключение телефона не препятствует работе сложного шпионского ПО. Эксперты по инфобезопасности предупреждают, что ряд вредоносных программ отслеживают местоположение и следят через камеру выключенного гаджета.

Предотвратить прослушку поможет извлечение аккумулятора. Владельцам iPhone и других мобильных устройств, у которых извлечь батарею не так просто, остается надеяться только на клетку Фарадея. Это устройство представляет собой сетку из токопроводящего материала для защиты техники от внешних электромагнитных полей. Купить «чехол» Фарадея для мобильного гаджета можно в обычном интернет-магазине, а стоит он совсем не дорого.

В крайнем случае в качестве клетки Фарадея можно использовать любой сейф и даже микроволновая печь. Например, когда Эдвард Сноуден прятался в отеле в Гонконге, он просил посетителей класть смартфоны в холодильник.

Клетка Фарадея поможет скрыть местоположение устройства, однако не обеспечивает никакой защиты от прослушки — устройство было взломано до изоляции. Пока смартфон в доспехах — все хорошо, но стоит его извлечь, как шпионская деятельность сразу возобновится.

Птичка на лазере принесла

Если злоумышленники очень захотят кого-то подслушать, они используют лазерный микрофон. Устройство посылает инфракрасный луч с большого расстояния, который возвращается обратно на световой сенсор вместе с чужими секретами. Лазер измеряет вибрации на стекле и восстанавливает звук. Помешать этому способу прослушки могут плотные шторы и громкая музыка.

Одеялко безопасности

Обычно хакеры воруют пароли с помощью вредоносных программ или взломов сервисов, которыми пользуется жертва. Однако не стоит забывать о самом эффективном способе — просто подсмотреть пароль через плечо. Сейчас повсюду установлены камеры наружного наблюдения, получить доступ к которым не так уж и сложно. В таких условиях идея накрыться одеялом с головой и только после этого разблокировать смартфон уже не кажется такой уж безумной.

Прикройте голову и руки теплым пледом и смело вводите секретные данные. Эдвард Сноуден не стесняется быть эксцентричным, когда речь идет об инфобезопасности. Об этом рассказывается в документальном фильме «Правда Сноудена» (Citizenfour). Сноуден в шутку называл одеяло своей «магической мантией силы».

Советы экспертов безопасности (коротко):

Дополнительные советы для супершпионов: после того, как вы купили клетку Фарадея, удалите микрофон с ваших устройств.

Если вы публичный человек, вы автоматически становитесь целью для слежки: Зашифруйте все с помощью VeraCrypt, зарегистрируйтесь в Google Advanced Protection и примите физические меры для повышения инфобезопасности.

Совет для обычных пользователей (хакеры все еще рядом): Используйте мастер-пароли, заблокируйте смартфон с помощью PIN-кода, обезопасьте себя от фишинга и позаботьтесь об онлайн-безопасности ваших детей.

# Наука поняла, как взломать человеческий организм

   06.05.2018

«Даже КГБ или испанская инквизиция не знали о человеке столько, сколько знают те, кто собирает информацию в сети сегодня. Эти сведения в итоге разделят человечество даже не на классы, а на виды».

Историк Юваль Ной Харари выступил на Всемирном экономическом форуме в Давосе с лекцией об опасности «технологической диктатуры». Он [**уверен**](https://www.youtube.com/watch?v=7Xs3auqcX7k), что технологический прогресс очень скоро приведет к появлению нового человеческого вида, и то, каким он будет, сегодня решают те, кто контролирует цифровые данные и информационные потоки.

— Из хорошего: мы получим сверхчеловеческие способности. Из плохого: мир захватят «цифровые диктатуры» — государства, которые благодаря технологиям будут знать о нас больше, чем мы сами. Даже когда советский КГБ или испанская инквизиция следовали за вами 24 часа в сутки, у них не было возможности знать, что происходит в ваших голове и теле, и понимать, что вы чувствуете и чего хотите. Но теперь все поменялось.

**Причиной тому — две революции нашего времени. Цифровая революция дает возможность владеть огромными массивами информации и анализировать личные данные миллиардов людей. Однако эти люди не задумываются, что информацию об их ежедневном поведении (от постов в соцсетях до оплаты картой в супермаркетах) можно собрать, оценить, монетизировать или превратить в рычаг политического давления.**

Вторая грядущая революция, по мнению Харари, будет биотехнической. Современная наука уже достигла глубокого понимания, что все живые организмы (будь то вирусы, люди или бананы) — это биохимические алгоритмы, которые можно расшифровывать. Революционные процессы, помноженные один на другой, позволяют взломать человеческий организм точно так же, как взламывают компьютеры, — считает историк.

**Через 100-200 лет земля будет принадлежать существам, которые будут отличаться от нас больше, чем мы отличаемся от неандертальцев и шимпанзе. Эволюция естественного отбора сменится эволюцией интеллектуального моделирования. И моделировать будет не какой-нибудь бог на облаке, а мы сами и наши собственные облака — облако IBM, облако Microsoft.**

Тот, кто владеет данными, будет владеть миром. Если мы не наладим регулирование этого процесса, мировая элита будет не только контролировать человеческие общества, но и решать, какие формы жизни должны населять планету.

**Теперь наиболее важным активом становятся данные, — уверен Харари. — И если слишком много данных сконцентрируется в руках элиты, то человечество расколется не на классы, оно расколется на виды.**

[**Вернуться в каталог сборников по менеджменту**](http://учебники.информ2000.рф/management2/management3.shtml)

[**Вернуться в электронную библиотеку по экономике, праву и экологии**](http://учебники.информ2000.рф/index.shtml)

[**НАПИСАНИЕ на ЗАКАЗ: дипломы и диссертации, курсовые и рефераты. Переводы с языков, он-лайн-консультации. Все отрасли знаний**](http://учебники.информ2000.рф/napisat-diplom.shtml)

|  |  |
| --- | --- |
| [**КНИЖНЫЙ МАГАЗИН**](http://учебники.информ2000.рф/chitai.shtml) |  |

|  |  |
| --- | --- |
| [**ТОВАРЫ для ХУДОЖНИКОВ и ДИЗАЙНЕРОВ**](http://учебники.информ2000.рф/kar.shtml) |  |

|  |  |
| --- | --- |
| [**АУДИОЛЕКЦИИ**](http://учебники.информ2000.рф/lectr.shtml) |  |

|  |  |
| --- | --- |
| [**IT-специалисты: ПОВЫШЕНИЕ КВАЛИФИКАЦИИ**](http://учебники.информ2000.рф/otu.shtml) |  |

|  |  |
| --- | --- |
| [**ФИТНЕС на ДОМУ**](http://учебники.информ2000.рф/fit1.shtml) |  |