**МАТРИЦА НАСТУПАЕТ**

**Вып. 3**

Оглавление

[Батарея смартфона может раскрыть все, что печатают или читают на его экране 2](#_Toc83819737)

[Отслеживание с помощью современных методов связи 2](#_Toc83819738)

[Загадочная микросхема ME и для чего Intel ставит её в материнские платы 4](#_Toc83819739)

[За вами следят, а потом продают данные государству и компаниям. Как устроена Big Data 6](#_Toc83819740)

[В чем польза Big Data для каждого 8](#_Toc83819741)

[«Большой Брат - 2» уже наблюдает 11](#_Toc83819742)

[Как опыт Uber и Facebook может помочь в борьбе с COVID-19 14](#_Toc83819743)

[Вскрылась вся правда о чипизации 18](#_Toc83819744)

[Цифровая дилемма: как слежка помогает победить Covid-19 20](#_Toc83819745)

[Москва создаст новую платформу для анализа данных жителей города 22](#_Toc83819746)

[Почему мировым IT-гигантам наплевать на персональные данные россиян 25](#_Toc83819747)

[За кем и как еще «присматривает» Google 26](#_Toc83819748)

[Улыбнитесь, вас снимают. Как работает технология распознавания лиц 28](#_Toc83819749)

[Big Data Большого Брата 29](#_Toc83819750)

[Любой гаджет может шпионить 35](#_Toc83819751)

[Эксперт CBS: распознавание лиц — компромисс между безопасностью и частной жизнью возможен 39](#_Toc83819752)

[ФСБ направила в «Яндекс» требование предоставить ключи 41](#_Toc83819753)

[«Директора часто пренебрегают правилами защиты». Как избежать проблем с утечками данных 44](#_Toc83819754)

[**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)

# Батарея смартфона может раскрыть все, что печатают или читают на его экране

В ходе недавнего исследования, проведенного специалистами Техасского университета в Остине, Еврейского университета и Израильского технологического института Технион, было установлено, что аккумулятор смартфона может обладать еще одной необычной, неизвестной ранее функцией.

Как оказалось, источники питания, способны фиксировать каждое нажатие телефонной клавиши и могут собирать большой объем конфиденциальной информации, которой в итоге вполне могут воспользоваться хакеры.

Исследователи внедрили микроконтроллер в батарею телефона, чтобы записывать колебания мощности, как внутри ее, так и снаружи. Затем они подключили ИИ для вычисления соответствия этих колебаний нажатиям на клавиши или сенсорный экран. Зная такой алгоритм, хакеры смогут записывать интересующие их пароли и прочую конфиденциальную информацию. Все, что им нужно — чтобы смартфон работал от батареи, а не от сети.

налогичный метод отслеживания уже используется в так называемых интеллектуальных батареях, которые все чаще встречаются в современных смартфонах. Они контролируют потребление энергии с помощью приложений и обладают функциями, которые повышают энергосбережение и увеличивают продолжительность автономной работы.

**Отслеживает ли правительство наше местоположение и передвижения?**

Вариантов отследить местоположение человека с точностью до метра бесконечное количество. Сделать это не составляет особого труда для служб и людей, обладающих специальным уровнем доступа к необходимой информации.

# Отслеживание с помощью современных методов связи

Всё, что необходимо знать о человеке, – зарегистрированный на него номер телефона. Сейчас в век современных технологий, все смартфоны автоматически отсылают и хранят информацию о модели и серийном номере (IMEI) используемого телефона на определенной сим-карте.

Прежде всего, рассмотрим схему отслеживания местоположения устройства с помощью GPS-навигации. GPS – это спутниковая навигационная система, первоначально разработанная в военных целях, позволяет определить местоположение в любом месте Земли по системе координат WGS 84.

Суммарная погрешность определения точки составляет не более 13 метров.

Именно по данной системе работают все навигаторы, которыми сейчас пользуется подавляющее количество населения. Яндекс-карты, Гугл-карты и иные приложения отправляют все данные передвижения устройства на спутник.

Простое отключение функции GPS-сигнала на смартфоне немногим спасет ситуацию, поскольку смартфон продолжает отсылать радиочастотные сигналы спутникам и на вышки сотовой связи. За данную функцию отвечает BBP, передающий сигналы связи в режиме реального времени на всех без исключения телефонах. Baseband processor (BBP) – чип, который исполняет real-time operating system (RTOS).

Минимальной информации о совершенном звонке или отправленной смс также будет достаточно, чтобы определить местоположение устройства с точностью до 50 метров.

Телефон без SIM-карты может общаться с любой доступной ему базой, не регистрируясь в сети и сделать только звонок по номеру 112. Эта возможность прописана в стандарте GSM и закреплена в законе о связи — статья 52.

В случае если вы не пользуетесь интернетом и телефоном вовсе, но он находится во включенном состоянии, он продолжает осуществлять связь. После процедуры идентификации в сети запускается счетчик времени, задающий момент перерегистрации в случае отсутствия каких-либо сеансов связи. Обычно период обязательной регистрации составляет несколько часов. Перерегистрация необходима для того, чтобы сеть получила подтверждение, что телефон по-прежнему находится в зоне ее действия.

Пользоваться и управлять смартфонами сейчас также можно через удаленный доступ. При взломе прошивки телефона на девайс устанавливается специальная программа, которая передает всю информацию о действиях, совершаемых с телефоном, включая совершение звонков, отправления смс, просто информацию на экране, и конечно, местоположение лица, установившего программу. О том, что Ваш телефон отслеживается, Вы и не узнаете.

**Банковские карты**

Платежные системы также не всегда служат во благо человечества. Полное передвижения человека можно отследить через платежи, совершаемые с помощью банковских карт.

История платежей не просто расскажет, где и когда вы расплачивались картой, но и какую именно покупку совершали, на какую сумму. В случае снятия денежных средств с карты с помощью банкомата остается вся информация о времени, дате и месте снятия, что укажет ваше последнее известное местоположение. Сейчас с помощью личного кабинета любого банка вы самостоятельно можете отследить собственное передвижение с помощью истории операций по карте за неделю, месяц или даже год.

**Социальные сети**

Для любителей социальных сетей также есть «хорошая» новость. Не будем говорить о добровольно выложенной в общей доступ личной информации, с этим всё понятно.

Местоположение можно узнать по интернет-провайдеру и в частности по IP-адресу, который выдаётся устройству пользователя. Пользователь переходит по определенной ссылке и тем самым передает свой IP-адрес и вместе с ним и свое местоположение. В настоящий момент существует несколько бесплатны сервисов для генерирования «специальной» ссылки.

После перехода по данной ссылке сервис определит Ваш IP-адрес и автоматически узнает его расположение с помощью логгера (пассивный трекер GPS).

Обычно данные о местонахождении ограничиваются городом, но бывает, что оборудование провайдера, обеспечивающее интернет, находится в другом месте и, соответственно, местоположение IP-адреса и человека будет определяться с существенными неточностями. Также этот способ неприменим к пользователям, сидящим в интернете через анонимайзеры или прокси, т.к. эти способы заменяют IP-адреса.

А теперь речь пойдет о фотографиях, выкладываемых в сеть. При фотографировании смартфон оставляет в памяти точное местоположение совершения данного действия по системе координат. Данная информация является неотъемлемой частью фотографии и, соответственно, выкладывается вместе с изображением в сеть.

Сейчас, если вы пользуетесь социальной сетью Вконтакте, при добавлении изображения, вы можете заметить, что место, где сделана фотография, «прикрепляется» к изображению самостоятельно, и с помощью мобильного приложения не всегда получается удалить эту метку. Избавиться от данной информации можно только с помощью специальных приложений по типу Exif.

Хочется добавить от себя, что не стоит быть параноиком и ходить в шапочке из фольги. Если Вы не совершаете ничего противозаконного, намеренно искать Вас никто не будет.

Билеты на поезда, самолеты и межобластные автобусы без паспорта не продают!

Больше им делать нечего, как сидеть и следить за каждым. Вот вы, чем интересны ФСБ?

**А между тем…**

Во время пандемии коронавируса в Китае следили за КАЖДЫМ жителем. Если конкретный человек находился вблизи от заболевшего ковидом, ему немедленно приходило сообщение с требованием пройти тест. И пусть он попробует не подчиниться!

# Загадочная микросхема ME и для чего Intel ставит её в материнские платы

24 сентября 2020

С далёкого 2008 года и до сегодняшних дней во все чипсеты на базе intel встроена интересная микросхема, которая называется Intel Management Engine.

Про данную систему известны некоторые факты, **которые очень понравятся любителям теории заговоров**, каждый для себя из этих сведений сможет сделать свой вывод.

Факт первый: работает когда компьютер выключен

Intel ME это микросхема, которая встроена в серверный мост материнской платы компьютера (на новых платах в PCH). За счёт дежурного напряжения, подаваемого на чипсет, на эту микросхему подаётся питание даже тогда, когда компьютер выключен.

Факт второй: как работает — большой секрет

Программа, работающая с микросхемой, находится в закрытой области BIOS и зашифрована.

Сама микросхема имеет нетипичную архитектуру. Функции этой системы Intel не документирует. А прошивка ещё и дополнительно запутана.

Факт третий: у неё прямой доступ к сети

Система имеет прямой доступ к сетевой карте, а микросхема отдельный MAC адрес, что уже наводит на мысли.

Вход сетевой карты на материнской плате

Более того, **каждый** бит данных входящий в сетевую карту компьютера из интернета в обход windows передается в intel me...

Факт четвертый: подозревают давно

Фонд электронных рубежей - известная правозащитная организация, уже давненько обвинила intel в том, что в их чипсете содержится троян, который может давать доступ к любому компьютеру в мире.

Но так никто и не показал полную документацию на микросхему.

Факт пятый: её невозможно отключить

Существовали прошивки умельцев в которых чип был отключен, но компьютер на таких прошивках работал нестабильно.

BIOS

Вместе с отключением микросхемы урезалась часть полезных функций.

К тому же, теперь intel перенесли в ME часть функций BIOS, что ещё сильнее затруднило отключение системы.

Некоторые экспериментаторы отключали чип програмно, но получали довольно странную ошибку, вследствии которой **компьютер выключался ровно через полчаса работы.** Срабатывал так называемый watch dogs timer.

Факт шестой, её развивают и улучшают

Как я уже писал выше, часть функций из BIOS, например ACPI (отвечает за кулеры, оверклокинг и много чего еще) была перенесена в intel me.

Кроме того в новых сериях чипсетов была добавлена поддержка NFC и Wi-Fi.

Факт седьмой

Intel является стратегическим партнёром АНБ. Ну может кто не знал...

Выводы

Официально компания заявляет, что intel me нужна для стабильности и повышения производительности системы. Очень туманное на мой взгляд объяснение.

**Довольно удобно переложить важные функции ПК из BIOS в микроконтроллер с незадокументированной архитектурой и зашифрованной программой.**

**Делая, таким образом, эту микросхему обязательной для использования и абсолютно неконтролируемой для пользователя.**

**Для чего это нужно - пока не понятно. Интересно будет послушать ваши версии.**

***Мнение.***

***Касперский еще лет 5 назад рассказывал об этой схеме. Интел признал, что этот чип умеет направлять данные с гаджета в силовые структуры США. Но, кто бы сомневался, только по решению суда.***

# За вами следят, а потом продают данные государству и компаниям. Как устроена Big Data

23 октября 2020

[Александра Морозова](https://66.ru/news/editor/43/)

На самом деле большие данные — это неотъемлемая часть жизни людей и необходимая составляющая бизнеса. Однако понятие «Big Data» в российском законодательстве не особо прописано, что несет правовые риски. Какую информацию о вас могут собирать соцсети, банки, магазины, сотовые операторы и что могут продавать третьим лицам — в материале 66.RU.

**Что такое Big Data**

|  |
| --- |

В классическом определении Big Data — огромные массивы структурированной и неструктурированной информации, собранной из разных источников. Сейчас под большими данными понимают не только информацию, но и различные инструменты, подходы и методы их обработки.

Основные источники Big Data:

* корпоративные базы данных;
* интернет (соцсети, блоги, форумы и др.);
* информация с датчиков, измерительных устройств и сенсорных сетей.

Три главные характеристики Big Data:

* Volume. Большой объем информации — потоки данных свыше 100 Гб в день. Big Data считается та информация, которая выходит за пределы возможностей обработки вручную.
* Velocity. Большая скорость накопления и необходимость в быстрой обработке.
* Variety. Большое разнообразие данных.

**Кто и как собирает информацию**

|  |
| --- |

Под сбором информации подразумевается любое действие потребителя, которое можно отследить. Например, передвижение абонентов мобильных операторов, подключение к wi-fi в общественном месте или оплата покупки банковской картой.

Первыми с большими данными начали работать сотовые операторы и поисковые системы. Сегодня к анализу Big Data в России присоединились банки, ретейлеры, интернет-компании и др. Несмотря на то, что рынок больших данных в РФ уступает масштабами западному, 54% российских компаний начали инвестировать в аналитику Big Data. По разным оценкам он составляет от 10 до 30 млрд рублей. В Ассоциации участников рынка больших данных прогнозируют, что к 2024 году его объем достигнет 300 млрд рублей.

**Сотовые операторы**

К июлю 2019 года в России было зарегистрировано 260,6 млн мобильных абонентов. По подсчетам компании Mediascope, 78% населения пользуется мобильным интернетом.  
Мобильный оператор определяет, где находится каждый из его абонентов, их ежедневные маршруты. Но речь идет не только о геолокации. Компания знает, как часто абоненты ездят за границу, где любят гулять, какие сайты просматривают, в каких интернет-магазинах совершают покупки.

**Банки**

По карточным транзакциям банки видят, сколько, на что и где вы тратите деньги, сколько вам перевел работодатель. Эта информация также позволяет анализировать кредитоспособность клиента, что в конечном итоге сокращает время рассмотрения кредитных заявок.

**Магазины**

Ретейл также собирает сведения о покупателях: персональные данные (оформляя бонусную карту, вы оставите дату рождения, телефон и ФИО), историю покупок, информацию из чеков.

**Поисковики, соцсети, сайты, приложения**

Информацию собирают «Яндекс», Google, Facebook и еще бесконечное множество компаний. Например, «Яндекс» с помощью технологии «Крипта» анализирует 300 факторов и создает условный портрет пользователя — обезличенный человек без имени и конкретной даты рождения, со своими интересами и пристрастиями. Google собирает личные данные, информацию о действиях, созданный контент. Подробную инструкцию о том, как избавиться от слежки Google хотя бы частично, читайте [здесь](https://66.ru/news/internet/214035/).

Даже лайки и комментарии, которые вы оставляете в социальных сетях, — часть Big Data. Например, Facebook [признался](https://66.ru/news/internet/224055/) в прослушке и расшифровке голосовых сообщений пользователей. Правда, в компании заявили, что предупреждали пользователей о прослушивании и расшифровке голосовых сообщений.

**Какие ваши данные могут продать по закону**

|  |
| --- |

В России нет отдельного законодательства, которое регулировало бы обработку больших данных. Занимаясь этим, компании должны руководствоваться Законом о персональных данных. Однако участники рынка и эксперты признают его размытость.

Попытки регулирования Big Data в России выглядят так:

* В октябре 2018 года депутаты «Единой России» Михаил Романов и Алексей Кобилев внесли в Госдуму законопроект, который обязывал интернет-компании уведомлять пользователей, что их данные будут обрабатываться в обезличенном виде. Документ не приняли и отправили на доработку.
* В августе 2019 года Ассоциация больших данных и Институт развития интернета объявили о создании кодекса этики использования Big Data. Кодекс, который приняли в декабре 2019-го, включает в себя принципы профессиональной этики, а также предполагает ведение реестра добросовестных участников. В комитете Госдумы по информполитике посчитали саморегулирование недостаточной мерой для рынка.
* В сентябре 2019 года Минкомсвязь разместила законопроект, предлагающий ввести понятие «обезличенные данные». Однако законопроект так и не внесли в Госудуму.
* В феврале 2020 года Минкомсвязь подготовила законопроект, который должен был закрепить подходы к обработке больших данных. Предложенные поправки предусматривают введение понятий «большие данные», «оператор больших данных» и «обработка больших данных». Однако в июне ведомство отозвало законопроект о регулировании рынка Big Data.

Компании, сайты и сервисы могут собирать персональную информацию (например, чтобы выдавать потом таргетированную рекламу), но не имеют права продавать ее третьим лицам.  
Операторы Big Data обезличивают персональную информацию, обрабатывая ее в агрегированном виде, и получают статистические или демографические данные. Собственно, для тех, кто использует Big Data, не нужны конкретные имена, адреса и номера телефонов. Смысл больших данных завязан на объеме — чем он больше, тем эффективнее и точнее будет анализ поведения.

Для тех, кто собирает и покупает большие данные, вы будете не инженером с завода Ивановым Иваном Ивановичем 1987 года рождения, а мужчиной от 30 до 40 лет со средним достатком.  
Правда, существует риск утечки персональных данных, что происходит регулярно. Тогда хакеры получают доступ к ФИО, телефонным номерам, паспортным данным и другой личной информации.

# В чем польза Big Data для каждого

Польза для компаний от собранного массива информации понятна — они оптимизируют продажи, логистику, составляют портреты клиентов. Соответственно, доходы растут. Но Big Data приносит пользу и конечному потребителю.

**Big Data и транспортная система города**

|  |
| --- |

Big Data применяют в развитии транспортных систем городов. С помощью информации, полученной от сотовых операторов, интернет-провайдеров, камер наблюдения, можно оптимизировать потоки транспорта. Мегаполисы используют Big Data для объединения транспортной инфраструктуры с другими видами коммунальных услуг в единое целое. Зная данные о передвижениях, можно корректировать маршруты общественного транспорта, управлять светофорами, анализировать очаги аварийности, места скопления машин и своевременно устранять их.

В октябре 2019 года МБУ «Центр организации движения» заключило контракт с МТС на проведение анализа данных по изменению плотности и динамике перемещения людей в Екатеринбурге. Эта информация ляжет в основу научно-исследовательской работы, посвященной разработке транспортно-экономической модели города на перспективу до 2035 года. Обезличенная информация о количестве людей, направлении их перемещения и скорости даст «истинную картину плотности заселения» и позволит рассчитать реальную потребность в транспорте. Аналогичные проекты реализуют в Москве, Санкт-Петербурге и Тюмени Tele2 и «Мегафон».

В Москве Big Data используют для решения транспортных проблем давно и активно. В 2018 году в столице внедрили систему, которая определяет участки дороги с высоким риском ДТП. Она учитывает внешние факторы (осадки, освещение, температуру) и анализирует саму дорогу (ширину, пропускную способность, скорость потока). В итоге Ситуационный центр ЦОДД принимает решение о приоритетном вызове ГИБДД на место аварии с учетом расположения этих участков.

Большие данные используют для прокладывания маршрутов общественного транспорта: за перемещением пассажиров следят с помощью чипов в билетах, которые считываются при валидации.

С 2015 по 2018 год департамент информационных технологий Москвы потратил на покупку геоаналитики и мобильных операторов 516 млн рублей.

**Big Data и магазины**

|  |
| --- |

В Екатеринбурге 60% торговых точек на рынке продуктового ретейла поделили между собой четыре компании. [Активнее всего город захватывает «Пятерочка»](https://66.ru/news/business/220437/) — магазины сети открывают в домах друг напротив друга. Причем, как правило, покупатели из одного магазина не ходят в другой, хотя ассортимент и стоимость товаров одинаковые.

Это значит, что в районе есть несколько независимых основных пешеходных маршрутов. И покупатель выберет «магазин у дома», а не пойдет через дорогу. Информацию о потоках покупателей как раз и собирают с помощью больших данных. Например, у сотовых операторов можно получить информацию о геопозиции устройств и их перемещении. Поставьте wi-fi и Bluetooth-точки в разных местах района — они соберут информацию о проходящих потенциальных покупателях через телефоны.

Один из известных примеров использования Big Data в продуктовом ретейле — опыт «Ленты». Основной источник данных о клиентах — карта лояльности. От 93 до 95% продаж в супермаркетах составляют транзакции с участием карт лояльности. Такой покупатель — часть клиентской базы, и магазин фиксирует и запоминает историю покупок, что позволяет спрогнозировать динамику спроса, создать адресные рекламные предложения и рассчитать оптимальный размер скидки.

Big Data помогает сузить поток информации для конечного потребителя — он получает уже целевую рекламу, которая заточена под него и, скорее всего, будет интересна.

**Big Data и рестораны**

|  |
| --- |

Как и в случае с магазинами, в пищевой индустрии большие данные используют для оптимизации меню и цен, для контроля качества и поставок продуктов. Однако рестораны также накапливают информацию из чеков, сумм чаевых, времени визитов, чтобы в итоге предугадывать предпочтения гостей.

**Big Data и туризм**

|  |
| --- |

Чтобы его развивать, в Свердловской области властям нужен срез — какие потоки туристов куда едут, где останавливаются, сколько платят и т. д. Его можно получить именно с помощью Big Data.

Коме того, анализируя данные мобильных операторов, можно контролировать спросы на авиа- и железнодорожные билеты, менять и добавлять направления. Например, понимая, что люди летают в определенную точку через их аэропорт, но с пересадками, воздушная гавань может привлечь авиакомпании, чтобы те открыли прямые рейсы.

**Big Data и развитие бизнеса в городах**

Министерство инвестиций и развития и Фонд поддержки предпринимательства Свердловской области с помощью Big Data анализируют потребность жителей небольших городов в предприятиях сфер услуг — кафе, парикмахерских, салонах красоты и т. д. В итоге бизнес получает развитие, а людям не приходится ездить за услугами в другой район или город.  
Чтобы получить представление, какие ниши пустуют, специалисты анализируют платежные данные по банковским картам. Это позволяет выявить спрос и предложения. По словам директора СОФПП Валерия Пиличева, проект стал возможен после того, как массив людей, которые пользуются банковскими картами и цифровыми устройствами, вырос, а количество перешло в качество.

Сфер применения Big Data — бесконечное множество — от медицины до горного дела, от экологии до рекламы, и описать их все невозможно. С каждым годом рынок Big Data будет расти и развиваться. По прогнозам агентства ResearchAndMarket, рынок аналитики больших данных будет повышаться в среднем на 11,9% с 2020 по 2028 год. По прогнозам экспертов, он вырастет до 115,13 млрд долларов.

**Использование банком Big data о клиентах**

|  |  |
| --- | --- |
| **Использование банком Big data о клиентах *Информация о клиентах, используемая банками путем автоматизированной обработки Big data*** | ***Цели анализа Big data*** о клиентах банка |
| Сценарии клиентских платежей, кредитная история, суммы переводов, на какие счета они совершались.  Аномалии в поведении клиентов нестандартные покупки, перевод значительной суммы денег. | 1) Безопасность: противодействие терроризму и отмыванию денежных средств |
| Кредитная история заемщика, его положение в социальных сетях, предпочтительность покупок, тон его комментариев в интернете. | 2) Использование в риск-менеджменте |
| Данные о счетах клиента, его транзакции, поведение в социальных сетях, история поиска в интернете, покупки в интернет-магазинах, круг общения, праздники и информация об отпусках. | 3) Предоставление клиентам персонифицированных предложений |
| Анализ трендов, предпочтений клиентов | 4) Создание новых продуктов, которые будут пользоваться спросом |

# «Большой Брат - 2» уже наблюдает

**Июль 2020**

**Еще не всеведущ, но знает о вас куда больше, чем вы думаете**

Привыкая к мысли о неизбежности тотального цифрового контроля, мы успокаиваем себя ограниченностью его возможностей.

* Подумаешь, Большой Брат может обнаружить меня среди протестующих по геолокации смартфона, — но ведь его можно и дома оставить.
* Подумаешь, ББ может распознавать лица демонстрантов, — но поди найди среди тысяч часов видеозаписи момент, когда я бросил в космонавта пластиковый стаканчик.

Старый «китайский подход» — решать проблемы числом, а не умением, усадив за анализ видео армию «видеоаналитиков», имеет массу недостатков. А при масштабировании наблюдения за пределы отдельных «горячих точек» и, тем паче, на весь мегаполис и страну, «китайский подход» вообще не реализуем, — слишком много нужно «видеоаналитиков» и, следовательно, слишком высока стоимость технологии наблюдения.

*Так может ИИ в состоянии решить эту проблему, взяв на себя автоматизированный поиск, так сказать, «потенциальных правонарушителей»?*

Мы успокаиваем себя, что это не под силу современному ИИ, умеющему решать лишь задачи статистического распознавания паттернов (в изображениях, текстах, речи и т.д.), но ни черта не понимающему, что он распознает. Он может распознать в потоке речи редкие слова, известные лишь немногим (типа, Frankenfood — генетически модифицированные продукты). Но при этом, на вопрос «How many legs does a centipede have» (сколько ног у сороконожки), ответ может быть и 4, и 8, но уж никак не [30 или 382](https://nat-geo.ru/fact/arifmetika-mnogonozhek/).

Конечно, и этот ничего не понимающий ИИ можно научить распознавать что угодно. Но для этого нужно, чтобы его научили. А для обучения нужно иметь *море размеченных данных*(например, тысячи фото кошек с пометкой для ИИ, что это кошка, и тысячи фото собак, людей, птиц и т.д. с пометкой, что это не кошка).

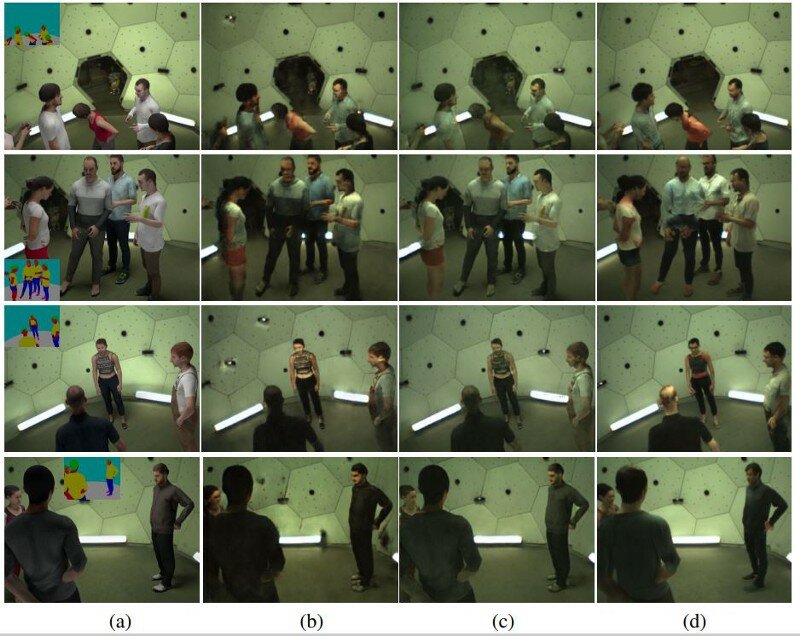
Когда же встает задача, научить ИИ распознавать факт бросания в космонавта пластикового стаканчика, нужно загрузить на вход ИИ тысячи таких сцен.

*Но и после того, как ИИ научится это делать, он не сможет распознать, когда в космонавта бросят урну (она же совсем не похожа на стаканчик).*

**Казалось бы, нам можно расслабиться. ББ далеко не всеведущ, хоть и научился распознавать наши лица.**

*Но тут появляется Большой Брат — 2, умеющий автоматически распознавать, что люди делают:*

*стаканчик в космонавта бросают, урну или заточенную копьём арматуру. И не только это, но и вообще что угодно: закурил не там, где можно, или пописал в неположенном месте, — да мало ли что еще.*



Трансформация синтезированных изображений, чтобы быть визуально реалистичными. В верхних левых углах каждого синтезируемого изображения (a) находится карта его сегментации. Изображения (b) получено на системе CycleGAN, ( c) на CyCADA, (d) на системе Amazon Go. Источник: https://arxiv.org/abs/2006.02110

В основе ББ-2 тот же подход, что позволил достичь недостижимого для людей уровня мастерства в играх, типа Го, шахматы и т.д. Главное, что оказалось для этого нужно — *уменьшить зависимость от больших данных*, содержащих примеры сделанных людьми ходов. Победившая в 2016 чемпиона по Го программа AlphaGo была обучена на 30 млн. примеров, сделанных людьми игровых ходов. А превзошедшая её в 2017 программа AlphaZero вообще обошлась без человеческих примеров ходов, тренируясь в игре сама с собой.

*Вот только как сделать, чтобы машина сама генерировала для своего собственного обучения миллионы трехмерных сцен, изображающих всевозможные действия людей, и чтоб эти сцены были автоматически размечены (например, метка: молодой человек бросает пластиковый стаканчик (урну, арматуру …) в космонавта)?*

**Кудесники из Amazon Go показали, как это делается.**

* Строится модель анализа сцен по смеси реальных и синтетических (искусственно созданных) данных.
* Затем эту модель используют для автоматической маркировки (разметки) кадров из набора данных, в котором создаются синтетические изображения.
* Затем используется условная генеративно-состязательная сеть (cGAN) для создания реалистичного изображения из данных, сгенерированных моделью анализа сцены (см. рис. выше).

Исследователи планируют создать набор данных, состоящий из 100 тыс. полностью аннотированных изображений нескольких людей, взаимодействующих в *Panoptic-среде CMU*.

Последнее означает следующее. Для детектирования объектов на изображении используется самая продвинутая *Panoptic-сегментация*, объединяющая в себе преимущества семантической сегментации (выделяет разные классы объектов на изображении: это человек, это урна …) и instance-сегментаций (разделяет объекты одного класса на разные объекты: это космонавт, это хулиган …).

Как тут не вспомнить про *Panopticon — проект «идеальной тюрьмы»* (или обобщенно, — институционального здания и системы управления), разработанный английским философом и социальным теоретиком Джереми Бентамом в конце 18-го века (подробней в моем посте «[Тотальная идеальная е-тюрьма по-китайски](https://zen.yandex.ru/media/the_world_is_not_easy/idealnaia-etiurma-pokitaiski-5b460baf569b5100aa030e3c?integration=desktop_browser_with_morda_yandex&place=more)»).

*Суть проекта в том, чтобы обеспечить централизованное наблюдение за всеми заключенными одним сторожем без того, чтобы заключенные знали, наблюдаются они в данный момент или нет.*

Цель проекта Паноптикум:

* сделав Большого Брата -2 хоть и не всеведущим, но знающим о действиях каждого из людей,
* обеспечить для власти прозрачность социальной реальности, тем самым делая власть для общества невидимой.

И если это удастся, то мы или наши ближайшие потомки довольно скоро лишимся не только свободы слова и собрания, но и свободы действий, выбора, воли … И все это добровольно, и даже не очень заметив этого.

*Он умеет автоматически распознавать, что люди делают: стаканчик в космонавта бросают, урну или заточенную копьём арматуру. И не только это, но и вообще что угодно: закурил не там, где можно, или пописал в неположенном месте, — да мало ли что еще.*

Эту систему (пока что лабораторную) сделали кудесники из *Amazon Go*, тем самым доказав, что ИИ в состоянии решить проблему **автоматизированного поиска «потенциальных правонарушителей»**.

*Но Китай не был бы Китаем, если бы ответка американцам не прилетела мгновенно. И какая ответка! «Большой Брат — 2» в Китае работает уже не в лабах, а в промышленной эксплуатации.*

[Пятеро молодых ребят из шанхайского НИИ сделали по заказу крупного девелопера систему социального контроля поведения в лифтах в реальном времени.](https://arxiv.org/abs/2006.15873)

Система автоматически выявляет (сама!) любую «ненормальную активность» в лифтах, — т.е. если люди делают что-то не то, что обычно делается в лифтах. Это может быть что угодно: торговля наркотиками, проституция, сексуальное домогательство, хулиганство … Или что-то не столь очевидное, но подозрительное — например, слишком много человек проживает на каком-то этаже (прямо мечта Собянина).

В настоящее время система развернута и обкатывается вживую на 100 000 лифтов. Заказчик не нарадуется. Система стучит на жителей весьма креативно. Например, настучала, что служба общественного питания работает из квартиры (что запрещено).

*Это значит, что теперь возможна автоматическая идентификации любого, кто отклоняется от какой-либо нормы.*

И это очень перспективно для авторитарных режимов.

# Как опыт Uber и Facebook может помочь в борьбе с COVID-19

30 июля 2020|Кьяра ФарронатоМарко ЯнситиМарчин БартосякСтефано ДениколаиЛука ФерреттиРоберто Фонтана

*От редакции. Эту статью и другие материалы, опубликованные в рубрике*[***«2020: Уроки стойкости»***](https://hbr-russia.ru/biznes-i-obshchestvo/uroki-stoikosti-2020)*, вы можете читать бесплатно. Если наш контент помогает вам преодолевать трудности нынешнего кризиса, лучший способ поддержать HBR Россия —*[***оформить подписку.***](https://hbr-russia.ru/podpiska)

В большинстве случаев платформы терпят неудачу потому, что им так и не удается набрать критическую массу вовлеченных пользователей. Провалы Google+, музыкальной соцсети Apple iTunes Ping и Webvan — это лишь несколько примеров, подтверждающих эту мысль.

Если принципиально не переосмыслить подход к разработке, запуску и масштабированию приложений для отслеживания контактов с носителями COVID-19, результат в большинстве случаев будет тот же. Да, государство может обязать граждан установить приложение на свои устройства, как это было сделано в Китае, но подобные драконовские меры вызовут жесткое неприятие, во всяком случае в Европе и США. История развития платформ показывает, что единственный альтернативный путь к успеху — набрать критическую массу на локальном уровне, продемонстрировав с самого начала полезность предлагаемого решения в малых сконцентрированных сообществах: например, в семьях, среди жителей отдельных районов или сотрудников офисов, — а в дальнейшем масштабировать его на региональный или национальный уровень.

Мобильное приложение для отслеживания контактов позволяет контролировать, с кем каждый из пользователей находился рядом, и при появлении подтвержденного случая заражения направляет уведомления всем, кто мог соприкасаться с вирусом. Кроме того, в некоторых приложениях предусмотрены уведомления о нахождении рядом инфицированного, что помогает предупреждать возможное заражение, или есть возможность отслеживать, соблюдает ли инфицированный пользователь рекомендации о социальном дистанцировании.

Однако, чтобы это работало, приложение должно быть установлено почти у всех. Определяющая черта подобных сервисов — сильные сетевые эффекты, то есть их полезность зависит от того, сколько человек загрузит и будет регулярно использовать программу. Если это сделает только небольшая часть окружения пользователя, в приложении для него не будет никакого прока, более того, оно может навредить: неточные показатели внушат ложное чувство безопасности. [**По некоторым оценкам**](https://science.sciencemag.org/content/368/6491/eabb6936), чтобы остановить распространение инфекции, на приложение должны перейти не менее 60% населения — мягко говоря, трудновыполнимое условие. А для надежности на индивидуальном уровне — чтобы каждому пользователю поступала точная информация обо всех, а не только некоторых контактах — уровень использования должен быть намного выше. Без широкого внедрения эти приложения могут быть не просто бесполезными, но даже опасными.

Серьезную сложность в стимулировании использования приложений представляют вопросы конфиденциальности: чем в понимании пользователей выше уровень конфиденциальности, тем охотнее они будут подключаться; в то же время защита частных данных ограничивает эффективность инструмента в отслеживании распространения вируса, а это замедляет его внедрение. Например, было бы полезно, если бы приложение предупреждало пользователей о том, что люди, с которыми они предполагают встретиться, заразились. Но во многих странах было решено не включать такую функцию из соображений конфиденциальности.

Один из способов стимулировать использование приложения — требовать этого в обязательном порядке, что [**сработало в Китае**](https://www.cidrap.umn.edu/news-perspective/2020/04/study-contact-tracing-slowed-COVID-19-spread-china). Но в большинстве стран, где технология внедряется на добровольных основах, [**подключаются к ней неактивно**](https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-COVID-tracing-tracker/). Например, в Сингапуре, где гарантировали, что технология будет применяться по желанию и с учетом требований конфиденциальности, ее используют лишь 35% населения. В Исландии, которая первой в Европе запустила свое приложение (в начале апреля), по состоянию на 8 июля менее 40% жителей пользуются сервисом. В других европейских странах показатели еще ниже — и это при том, что в апреле ЕС выпустил [**рекомендации**](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670) о скоординированном подходе к разработке надежных, безопасных и функционально совместимых приложений для отслеживания контактов.

Когда использование предлагается на добровольной основе, с приложениями для отслеживания контактов возникает классическая проблема курицы и яйца (или «холодного старта»), с которой сталкиваются все платформы, рассчитанные на сильные сетевые эффекты: они практически бесполезны до тех пор, пока не наберут критической массы пользователей. Многое в решении этой проблемы зависит от того, каким будет запуск платформы. На самом деле это иногда важнее, чем инвестиции в НИОКР или маркетинг, особенности дизайна и даже стратегия в целом. И лучшая стартовая стратегия часто нелогична. Вместо запуска на неограниченную аудиторию лучше действовать адресно: ориентируйтесь на небольшое сообщество, добейтесь широкого освоения на локальном уровне, наращивайте вовлеченность, сформируйте критическую массу и затем постепенно масштабируйте.

С помощью такой стратегииFacebookпостроил теперь уже глобальную социальную сеть. Начиналось все с сообщества колледжа Гарвардского университета, потом присоединились другие колледжи, отдельные компании, и после, спустя долгое время после накопления критической массы, продукт был выведен на глобальный уровень. Такую же стратегию применили в WhatsApp, сосредоточившись на семьях экспатов, и в Uber, где выбрали центр Сан-Франциско и после расширяли охват, город за городом. Напротив, в Google проект Google+ запустили без ограничений для всех, у кого есть Gmail, и не достигли критической массы даже при многомиллионной численности пользователей. В Apple таким же образом предложили iTunes Ping всей аудитории iTunes — вовлеченность получилась крайне низкой. Без адресной стратегии запуска даже гиганты терпят неудачу.

То же касается и приложений по отслеживанию COVID-19. Вместо того чтобы запускать их повсеместно и бессистемно, лучше внедрять их в сконцентрированных, ограниченных и взаимосвязанных сообществах, где они с самого начала могут быть полезны: в семьях, религиозных сообществах, на рабочих местах, в школах, барах и ресторанах, на пляжах, в отелях, поездах, самолетах и т. д. Так их мгновенно оценят, и в каждом малом сообществе доля тех, кто перейдет на их использование, может приблизиться к 100%. Когда приложения наберут критическую массу в небольших сегментах, их можно постепенно масштабировать и интегрировать на региональном или национальном уровне. Рекомендованная ЕС функциональная совместимость позволила бы обеспечить даже трансграничное взаимодействие. Все это просто выводы из опыта развертывания Facebook, WhatsApp и Uber.

На самом деле заинтересованность многих сообществ в отслеживании распространения инфекции для сдерживания COVID-19 велика, потому что это означало бы открытие школ, предприятий и общественных заведений. Где-то могли бы выбрать предписания об обязательном использовании приложений, в других местах сервис применялся бы в рекомендательном порядке. Так, в пятом крупнейшем банке Италии UBI Banca решили, что сотрудникам необходимо с 1 июля и по возвращении в офисы использовать приложение для отслеживания контактов UBI Safe. Оно было автоматически установлено на корпоративные смартфоны, которые есть у 40% сотрудников. Планировалось предложить и остальным 60% загрузить приложение на свои личные устройства. Когда мы разговаривали с ИТ-директором UBI Banca Марко Чеккеллой в середине июня, он выражал уверенность, что [**охват будет очень высоким**](https://www.corriere.it/economia/consumi/20_giugno_18/app-tracciamento-entrano-azienda-caso-ubi-banca-rivale-immuni-e6e9a756-b09e-11ea-960e-a5a2de99a416.shtml).

Так же можно действовать и в других сообществах. В студенческих общежитиях можно предлагать установить приложение перед заселением. В семьях родственники могли бы договариваться подключить его перед общими мероприятиями. Авиакомпании могут просить об этом пассажиров перед посадкой в самолет. По мере того как приложение набирает критическую массу в каждом сообществе, оно получает мгновенную вовлеченность, и при условии внимательной и последовательной реализации можно постепенно объединять сформированные сети и наращивать объемы использования до уровня, когда программа будет загружена у большей части населения.

Приложение для отслеживания контактов должно быть спроектировано таким образом, чтобы оно могло сразу стать полезным. Продуманный подход в разработке в целом важен для привлечения первых пользователей, и это особенно относится к приложению для отслеживания контактов, поскольку из-за ограничений, связанных с соблюдением конфиденциальности, никому неизвестно, сколько еще человек его используют. Один из способов сделать программу полезной с самого начала — предоставлять информацию о локальном распространении инфекции, чтобы пользователи понимали риски. Другой вариант — предусмотреть функцию контроля симптомов, чтобы можно было вводить свои показания и получать рекомендации, когда следует обратиться за помощью.

Но лучше всего, разумеется, если приложение сможет максимально полно отслеживать релевантные контакты. Удачный первый шаг — протокол Apple/Google, результат совместной работы Appleи Googleнад наиболее продуманным с точки зрения конфиденциальности стандартом для приложений по отслеживанию контактов. Сейчас предусматривается фиксация близкого местоположения только для тех, кто установил на свой смартфон приложение. Но в принципе это могло бы работать для любого пользователя, обновившего операционную систему iOSили Androidдо версий, в которых используется этот протокол. Тогда сразу же при загрузке приложение могло бы предоставлять информацию о контактах, которые подключили его ранее.

Наконец для стимулирования использования приложения важно работать с ожиданиями пользователей. Человек может подключиться, если у него будет четкое понимание, что при поступлении уведомления о контакте с вирусом можно будет оперативно и без дополнительных издержек сделать тесты. Даже в Европе, где медицинское обслуживание в большинстве стран бесплатное, не всегда удается быстро сдать анализы. Если служба здравоохранения страны или сообщество (например, работодатель) обязуется обеспечить пользователям приложения оперативное, недорогое (или бесплатное) прохождение теста, это может поспособствовать его быстрому внедрению и использованию.

Приложения для отслеживания контактов могут и должны стать важным фактором в борьбе с пандемией. Нужна масштабная и тщательно скоординированная между национальными правительствами и местными сообществами стратегия, которая будет опираться на сосредоточенное, систематическое локальное внедрение и незамедлительный эффект. В сочетании с обширными мощностями в тестировании и рациональным вдумчивым подходом к поиску баланса между интересами здравоохранения и соображениями конфиденциальности такие приложения дали бы нам шанс на победу в борьбе против пандемии.

Об авторах

Кьяра Фарронато (Chiara Farronato) — преподаватель Гарвардской школы бизнеса, аффилированный научный сотрудник Лаборатории теории инноваций при Гарвардском университете, DigIta4GoodLab и программы Digital Initiative Гарвардской школы бизнеса.

Марко Янсити (Marco Iansiti) — профессор бизнес-администрирования Гарвардской школы бизнеса. Консультировал такие ИТ-компании, как Microsoft, Facebookи Amazon. Автор книги «Competing in the Age of AI» (в соавторстве с Каримом Лахани) (Harvard Business Review Press, 2020).

Марчин Бартосяк (Marcin Bartosiak) — преподаватель в Павийского университета (Италия), член лабораторий Digital Data Streams Lab, DigITA4Good Lab и Центра исследований искусственного интеллекта и киберкоммуникаций.

Стефано Дениколаи (Stefano Denicolai) — преподаватель курса управления инновациями в Павийском университете (Италия), руководитель магистратуры в области международного бизнеса и предпринимательства, директор программы Executive MBA. Входит в состав рабочей группы Министерства инноваций Италии по применению технологий данных в борьбе с COVID-19, руководит лабораторией DigIta4Good Lab.

Лука Ферретти (Luca Ferretti) — ведущий научный сотрудник в области статистической генетики и динамики патогенов в Институте больших данных Наффилдского отделения медицины Оксфордского университета.

Роберто Фонтана (Roberto Fontana) — преподаватель прикладной экономики в Павийском университете, исследователь центра ICRIOS Университета Боккони.

# Вскрылась вся правда о чипизации

Май 2020

Сегодня мы поговорим на очень странную тему. Она одновременно дико смешная и максимально серьёзная, нелепая и абсолютно фантастическая, но при этом абсолютно реальная, потому что это уже происходит. Это вопрос не про будущее, это вопрос настоящего. Конечно же это чипизация!

Давайте посмотрим на каком уровне сейчас находятся технологии. Конечно смотреть здесь нечего и некуда, потому что это известно всем уже давным-давно и в этом признаются сами создатели. И они не просто признаются, но и рекламируют это. Слышали ли вы такое слово-нейролинк? Если нет. То предлагаю вам посмотреть презентацию Илона Маска <https://www.youtube.com/watch?v=YKzCD2IEYUQ>. Это уже даже не чипизация, это весь ваш мозг подключен к компьютеру. И это совершенно не относится к конспирологии, а является одной из самых обсуждаемых тем. В интервью Илона Маска у Джо Рогана 2020 они спокойно обсуждают, что **через 5-10 лет людям речь вообще не будет нужна**. Как видите развенчивать здесь нечего.

Конечно чипирование будет. Оно уже есть. На инвалидах уже давно опробовали все эти вещи и Анатолий Каплан спокойно рассказывает, что на сегодняшний день уже есть 100-200 тысяч людей с вживленными чипами.

Будет ли это массово? Конечно да! Ведь Илон Маск не просто так это всё разрабатывает и продвигает. Будет ли это принудительно? В тоталитарных странах скорее всего да. В демократических странах может и нет. Но не в этом дело.

Система будет выстроена так, что вы сами будете ещё платить деньги, чтобы вам вживили эти чипы. Точно так же, как сейчас. Если вы не хотите иметь телефон, то не имейте. Вас ведь никто не принуждает его покупать. Но всё вокруг создано таким образом, что без телефона обходиться в некоторых случаях практически не возможно. Так же будет и с вживленными чипами. Хотите, живите без них, но скорее всего это будет не легко.

Сейчас уже Маск говорит, что первые, кто пойдет на чипизацию, настолько опередят всех остальных, что возникнет черезвычайный спрос и огромное желание приобрести этот чип и подключить его к своему мозгу. И в этом случае Илона Маска нельзя рассматривать как какого то злодея и поработителя. Он вполне здравомыслящий человек и в интервью объясняет, что это абсолютно объективные тенденции и если не можешь победить тренд, то возглавь его. Так он и делает.

Так что мне кажется, что понятно, что технологические возможности есть и всё вполне можно реализовать. С этим разобрались.

Теперь давайте рассмотрим есть ли политическая воля к реализации таких целей.

Здесь так же долго мудрить не нужно. Первое, что вы можете сделать, это открыть сайт мэра Москвы Собянина mos.ru. Это официальный сайт с программой "Умный город 2030", которую очень просто скачать и ознакомиться с этим довольно увлекательным проектом. И кстати, когда они там описывают свою стратегию, они честно сообщают, что стратегия основана на принципах транс гуманизма и принципах устойчивого развития.

Также существует приказ Минпромэнерго от 2007 года №311 "Об утверждении Стратегии развития электронной промышленности России на период до 2025 года" Вот одна цитата: "Облик промышленного производства при этом все более будет напоминать **микроэллектронно-фармацевтические** производства, а не традиционные приборно-машиностроительные производства, существующие в настоящее время." Или ещё " Широкое внедрение достижений отечественных нанотехнологий, **биоэлектроники**и микросистемной техники в повседневную жизнь человека в сферах здравоохранения, образования, жилищно-коммунального хозяйства, транспорта и связи".

Что такое биоэлектроника? Вот простой пример - это органические полимерные дисплеи, вживленные в лист живой розы.

В открытом доступе также можно ознакомиться с проектом "Образование 2030". Там указано в разделе" Предпосылки: ключевые технологии, влияющие на трансформацию образования": массовые нейроинтерфейсы (2017-20), НТТР 2.0: протокол "обмена мыслями" (2025), массовые виртуальные миры(2015-2020) и тому подобное.

И последнее, это для чего всё это делается? Просто человечество сейчас переходит на новую ступень эволюции. Мы должны создать эусоциальное общество, типа муравейника, где каждый муравей это как клетка одного организма. А наше человеческое общество не совершенно, не эусоциум. Мы только на пути к нему.

То есть, нам предложат или быть единым организмом без собственной воли, но имеющим преимущества в плане здоровья, финансов, работы и так далее. Но быть готовым к тому, что управлять нашей жизнью будет искусственный интелект. Он будет решать, куда ты должен пойти, что съесть, кого любить и когда умереть. Или остаться у обочины жизни, но свободным. Другого варианта не предусмотрено.

К сожалению как это остановить или изменить я не знаю.

Мыши киборги научная статья [https://www.nature.com/articles/s4159...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Fwww.nature.com%2Farticles%2Fs41593-018-0072-x) Научпоп-статья о том же [https://yandex.ru/turbo?text=https%3A...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Fyandex.ru%2Fturbo%3Ftext%3Dhttps%253A%252F%252Fnaked-science.ru%252Farticle%252Fsci%252Fkoreyskie-uchenye-sozdali-distancionno) Лекция Каплана по нейрокомпьютерным интерфейсам [https://www.youtube.com/watch?v=dGNoc...](https://www.youtube.com/watch?v=dGNoceDeLfo) Сайт мэра Москвы, где можно скачать программу "Умный город 2030" [https://www.mos.ru](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Fwww.mos.ru) Цели устойчивого развития, документ ООН [https://unctad.org/meetings/en/Sessio...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Functad.org%2Fmeetings%2Fen%2FSessionalDocuments%2Fares70d1_ru.pdf) Приказ МинПромЭнерго от 2007 года [https://legalacts.ru/doc/prikaz-minpr...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Flegalacts.ru%2Fdoc%2Fprikaz-minpromenergo-rf-ot-07082007-n-311%2F) (обсуждаемые цитаты проще всего найти в тексте, нажав ctrl+F и введя ключевые слова) Один из форсайтов Образование 2030, сделанный Агентством Стратегических Инициатив [https://asi.ru/upload\_docs/Forsight/e...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Fasi.ru%2Fupload_docs%2FForsight%2Fedu2030print_3364x1189.jpg) Статья на Википедии "Детство 2030" [https://ru.wikipedia.org/wiki/%D0%94%...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Fru.wikipedia.org%2Fwiki%2F%25D0%2594%25D0%25B5%25D1%2582%25D1%2581%25D1%2582%25D0%25B2%25D0%25BE-2030) Заметка об "образовании 2030" на сайте мэра Москвы [https://www.mos.ru/mayor/themes/15299...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Fwww.mos.ru%2Fmayor%2Fthemes%2F15299%2F5901050%2F) Форсайт "Образование 2030" на сайте Института Образования Высшей Школы Экономики [https://ioe.hse.ru/data/2013/10/07/12...](https://www.youtube.com/redirect?event=video_description&v=uR7tXlqe3z8&redir_token=LIW3loAHMc9NQKyOmz4FTa-OSUR8MTU5MDM1MzUyNEAxNTkwMjY3MTI0&q=https%3A%2F%2Fioe.hse.ru%2Fdata%2F2013%2F10%2F07%2F1280643910%2F%25D0%259F%25D1%2580%25D0%25B5%25D0%25B7%25D0%25B5%25D0%25BD%25D1%2582%25D0%25B0%25D1%2586%25D0%25B8%25D1%258F%2520%25D0%259F.%25D0%259B%25D1%2583%25D0%25BA%25D1%2588%25D0%25B0%2520-%2520Global%2520Report%2520Education%25202030.pdf) Не факт, что он официальный, возможно, просто студенческий. Тем не менее, он отражает царящие там настроения.

# Цифровая дилемма: как слежка помогает победить Covid-19

|**15 мая 2020**|**Яшэн ХуанМэйцэнь СуньЮйцзе Суй**

Covid-19 продолжает свое шествие по миру, не замечая государственных границ. И чиновники изучают страны, которым удалось замедлить распространение инфекции. Можно ли повторить их успех? Главный вопрос — есть ли у автократий преимущество над демократиями, ведь первым легче объявить карантин и отслеживать контакты и перемещения зараженных. Министр иностранных дел Китая Ван И даже заявил: «Только в Китае и только под руководством председателя КНР Си могли быть приняты такие эффективные меры, которые помогли нам взять под контроль эту внезапную и быстро распространяющуюся эпидемию».

Но согласно графику ресурса [Our World in Data](https://ourworldindata.org/grapher/covid-confirmed-cases-since-100th-case" \t "_blank), на котором показана скорость удвоения числа пациентов в разных странах, тип государственного режима не очень важен. И среди лидеров по борьбе с вирусом, и среди отстающих есть как автократии, так и демократии. Да, Китаю действительно удалось замедлить рост заражений, но и демократической Южной Корее это удалось тоже. А вот в других демократиях — например, в США, Испании, Италии и Франции — дела шли и идут не так хорошо.

Что же объединяет те страны, которым пока что удается сдерживать эпидемию? Во-первых, все они находятся в Восточной Азии: это Китай, Южная Корея, Тайвань, Сингапур и в меньшей степени Япония. Возможно, их коллективистский дух укрепляет чувство гражданского долга, и люди охотнее соблюдают требования властей. Кроме того, эти страны активно используют современные технологии для сбора данных о распространении вируса: например, следят за заболевшими и теми, кто с ними контактировал. Эти два фактора не независимы, а только укрепляют друг друга.

Очевидно, что такое использование технологий может помочь в борьбе с пандемией. Но оно поднимает непростые вопросы о неприкосновенности и конфиденциальности данных, которые вызывают в западных демократиях куда больше полемики, чем в Азии. Чтобы слежение оказалось эффективным, необходимо выполнить три условия, каждое из которых поставит перед западными демократиями непростые дилеммы: внедрение технологий (настоятельно рекомендуемое или строго обязательное), создание государственной цифровой инфраструктуры и легкий обмен информацией между государством и бизнесом, при котором конфиденциальность может потеряться.

Рассмотрим каждое из этих условий подробнее.

**Внедрение технологий**

Судя по опыту стран, которые успешно внедрили систему отслеживания контактов, первый и необходимый шаг — рекомендовать людям установить на свои телефоны приложения для отслеживания, а лучше сделать их обязательными. В странах Восточной Азии такие меры чаще принудительны, чем добровольны. Например, в Сингапуре — стране, правительство которой славится своей жесткостью и эффективностью — граждан попросили установить приложение TraceTogether, через которое находящиеся близко друг к другу телефоны обмениваются сигналами по Bluetooth. Это улучшенная версия традиционного способа отслеживания контактов, который занимает слишком много времени и зависит от ненадежной человеческой памяти.

Nikkei Asian Review сообщает, что, согласно опросу общественного мнения, более 70% респондентов поддержали эту меру. Гонконг, который тоже успешно сдерживает вирус, ввел обязательный 14-дневный карантин для всех, кто прибывает в страну из-за рубежа. Чтобы следить за соблюдением карантина, власти обязали всех прибывших установить приложение StayHomeSafe и выдали им браслеты с технологией геозонирования. По данным Quartz, за несоблюдение карантина гонконгцам грозит штраф 3200 долларов и до полугода тюремного заключения.

Южной Корее удалось сделать еще больше в борьбе с вирусом. Washington Post пишет, что корейские частные разработчики даже выпустили свои приложения для слежения — многим корейцам казалось, что государственных мер недостаточно. Например, [приложение Corona](https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html) 100m собирает данные из открытых официальных источников и оповещает пользователей, если в радиусе 100 метров от них оказывается человек с диагнозом Covid-19. Приложение показывает дату постановки диагноза, национальность, возраст, пол и список посещенных мест. Согласно данным MarketWatch, всего за несколько недель Corona 100m было скачано 1 млн раз и получило «исключительно положительные отзывы». А приложение CoronaMap публикует местонахождение пациентов с коронавирусом, чтобы люди могли избегать этих мест. Business Insider пишет, что CoronaMap заняло второе место в Южной Корее по количеству скачиваний.

Еще одна демократическая страна, успешно сдерживающая Covid-19, — Тайвань, — возможно, первой начала следить за телефонами людей, чтобы убедиться, что они соблюдают карантин. Кроме того, власти два раза в день звонят им, чтобы убедиться, что они не оставили телефон дома в попытке избежать слежки.

Идее отслеживать заразные болезни через мобильные телефоны уже почти десять лет. Например, в 2011 году Кембриджский университет выпустил приложение FluPhone, но популярность таких приложений сильно зависит от региона. Wired [пишет](https://www.wired.com/story/phones-track-spread-covid19-good-idea/), что FluPhone установили менее 1% жителей Кембриджа. Это не идет ни в какое сравнение с популярностью приложений для отслеживания контактов в Восточной Азии. Опасения о конфиденциальности и гражданских свободах могут стать препятствием для внедрения таких технологий в западных демократиях — возможно, именно поэтому приложение FluPhone оказалось так непопулярно. И даже в разных демократических странах процент добровольной установки таких приложений будет различаться. Но если их почти никто не будет использовать, они окажутся бесполезны.

**Цифровая инфраструктура**

Скорее всего, Южной Корее удалось так успешно сдержать вспышку Covid-19 благодаря свежему опыту борьбы с другими эпидемиями. Так, во время вспышки MERS в 2015 году заразились 186 корейцев, 36 из них погибли. Некоторые считают, что активная публикация данных о Covid-19 — это попытка исправить ошибки, допущенные во время эпидемии MERS, когда власти действовали недостаточно прозрачно. Опрос 1 тыс. корейцев [показал](https://www.nature.com/articles/d41586-020-00740-y), что большинство из них одобрили публикацию данных о перемещениях пациентов с Covid-19 и «поставили общественное благо выше прав личности».

# Москва создаст новую платформу для анализа данных жителей города

Май 2020  
Москва потратит 201 млн руб. на платформу, которая должна позволить без риска утечек анализировать данные из разных систем о горожанах. Как именно город намерен использовать полученные выводы, пока не ясно  
Правительство Москвы построит общегородскую платформу совместных вычислений на основе агрегированных данных, которая должна позволить городу использовать информацию, полученную от государственных и частных учреждений, не передавая сторонним компаниям или агентствам.  
  
Соответствующий тендер провел департамент города Москвы по конкурентной политике. Стоимость разработки платформы город оценил в 203,5 млн руб., победителем стала компания Ubic (ООО «УБИК»), предложившая выполнить контракт за 201 млн руб.  
Как пояснил РБК директор отдела исследований и разработки Ubic Петр Емельянов, платформа будет использовать современный метод информационной безопасности — протоколы совместных конфиденциальных вычислений, благодаря чему власти столицы не будут видеть или передавать данные в исходном виде, а смогут лишь получать выводы и результаты проведенного на их основе анализа.  
  
**Что такое совместные вычисления**  
  
Совместные конфиденциальные вычисления — это набор техник, позволяющих множеству пользователей объединить их данные, обработать их и получить результат, не раскрывая секретной информации друг другу, объясняет руководитель лаборатории криптографии НПК «Криптонит» Василий Шишкин.  
  
«Представим, что группа людей решила определить средний размер их заработной платы. Для этого каждый участник процесса передает значение размера своего дохода единому доверенному судье, который, получив все данные, вычисляет среднее и оглашает его всем сторонам, сохранив конкретные значения заработка людей в секрете. Протокол совместных конфиденциальных вычислений, базируясь на строгих математических обоснованиях, играет роль такого беспристрастного судьи», — привел пример Шишкин.  
  
Сейчас данные россиян защищаются законом «О персональных данных», это усложняет их использование и обмен информацией между компаниями даже в обезличенном виде, говорит гендиректор Ubic Виталий Саттаров. Метод конфиденциальных вычислений позволяет бизнесу и государству работать с данными, не нарушая прав граждан и снизив риск утечки информации, утверждает он. В компании рассчитывают, что новая платформа поможет городу усовершенствовать антифрод-мониторинг, устраивать более безопасные онлайн-голосования и аукционы, а также проводить социологические и медицинские исследования.  
  
Какие данные попадут на новую платформу и зачем это правительству Москвы, разбирался РБК.  
  
**С какими данными будет работать платформа**  
  
Из материалов закупки следует, что исполнитель должен будет организовать поступление данных из нескольких информационных систем города, среди которых:  
  
система управления данными в распределенной вычислительной среде (УДРВС), которая хранит различную информацию, имеет подсистему для обработки неструктурированных данных по медицинским обследованиям и интернет-трафику. Например, для поиска признаков раковой опухоли на снимках КТ с помощью технологий компьютерного зрения и нейронных сетей. В 2018 году контракт на модернизацию этой системы за 88 млн руб. также выиграла Ubic;  
система мониторинга и анализа интернет-активности пользователей (СТАТС), которая предназначена для наблюдения интернет-активности посетителей ресурсов города. Среди прочего она должна обеспечить возможность выявления уникального интернет-посетителя в условиях отсутствия файлов cookies (данные, которые отправляет сайт, когда пользователь обращается к нему через web-браузер, и которые могут храниться на устройстве пользователя. — РБК) в его браузере. Система обошлась городу в 52,4 млн руб. Исполнителем работ также выступает Ubic;  
ГИС «Единая мобильная платформа города Москвы», которая обеспечивает информационное взаимодействие подключенных к ней федеральных и городских органов власти, различных организаций с гражданами через мобильные устройства (СМС- и USSD-сообщения). Платформа обрабатывает запросы на предоставление госуслуг, обеспечивает идентификацию пользователей при выходе в интернет в пунктах коллективного доступа и т.п. В 2019 году конкурс на техническую поддержку этой системы в 2019–2021 годах стоимостью 200,4 млн руб. выиграло ООО «Интермобилити». Оно же получило контракт на модернизацию этой системы за 96,2 млн руб. в начале этого года;  
интегрированная автоматизированная информационная система «Единое геоинформационное пространство города Москвы» (ИАИС ЕГИП), которая используется для автоматизации деятельности городских властей для формирования, консолидации, хранения пространственных данных, осуществления связывания, поиска данных и предоставления доступа к ним. В 2019 году тендер на техническое обслуживание этой системы выиграло ООО «Антисистемс» за 47,2 млн руб.  
Что известно о подрядчике  
  
Ubic — разработчик сервисов фильтрации и анализа трафика, основанный бывшим техническим директором Rambler Mobile Виталием Саттаровым и бывшим руководителем платформы электронной коммерции Rambler Алексеем Ворониным. В 2016 году компания привлекла 50 млн руб. инвестиции от Фонда развития интернет-инициатив (ФРИИ), в 2018 году — 115 млн руб. от ФРИИ и Российской венчурной компании (РВК). По данным СПАРК, сейчас Саттарову принадлежит 28% УБИК, Воронину — 27%, ФРИИ — 32%, РВК — 13%. Выручка в 2018 году — 170,9 млн руб., чистая прибыль — 62,7 млн руб.  
  
В рамках выполнения работ Ubic также должен подключить к платформе не менее пяти внешних информационных систем. Представитель исполнителя не уточнил, системы чьих компаний это могут быть, но сообщил, что видит интерес к технологии со стороны рынка.  
  
Представители МТС, «ВымпелКома» и «Ростелекома» в проекте не участвуют, но готовы его изучить в последствии. Представитель «МегаФона» рассказал, что вопрос о возможном присоединении к платформе может быть рассмотрен только после проведения успешных испытаний системы и итоговой аттестации по требованиям безопасности информации.  
  
Департамент информационных технологий Москвы переадресовал вопросы про новую платформу в мэрию, представитель последней не смог оперативно представить комментарий.  
  
По словам Саттарова, Ubic сейчас разрабатывает инструмент вычислений данных, о конкретных кейсах, как будут применятся обработанные данные, можно будет говорить позднее. «Платформу планируется интегрировать с системой СТАТС, в которой есть вероятностные характеристики посетителей московских информационных порталов. Таким образом, можно вычислить, например, вероятность отношения пользователя к сегменту «автомобилисты». Платформа позволит лучше понимать текущие потребности целевой аудитории (в данном случае — жителей столицы), использовать эти знания при проектировании городских электронных сервисов и информационных систем. Также она позволит повысить точность моделирования за счет заполнения ранее имеющихся пробелов, например частоты использования каршеринга жителями Москвы», — рассуждает представитель Ubic.  
  
**Зачем власти Москвы собирают данные о гражданах**  
  
По данным Би-би-си, у московской мэрии есть около 170 разнообразных информационных систем. С 2012 года из бюджета Москвы на сбор и анализ данных москвичей правительство выделило около 500 млрд руб. (с учетом средств, которые будут потрачены в 2020 году). Как рассказывал изданию бывший сотрудник московского правительства, еще в момент прихода на должность мэра Москвы Сергей Собянин поставил задачу собрать информацию о том, что происходило в разных отраслях. С 2015 года власти столицы закупают у сотовых компаний геоаналитические данные, что позволяет получить достоверную информацию о месте жительства и перемещениях жителей столицы. Эта информация, например, используется при развитии транспортной системы. Система городского видеонаблюдения с системой видеоаналитики помогают сотрудникам правоохранительных органов разыскивать правонарушителей, а городским службам — контролировать качество уборки дворов, тротуаров и дорог и т.д.  
  
Особенно актуальными многочисленные информационные системы Москвы оказались в последние месяцы в связи с пандемией коронавируса. Так, система видеонаблюдения теперь используется для выявления нарушителей карантина. «По итогам межведомственных проверок были аннулированы рабочие пропуска для 23,5 тыс. пациентов с COVID-19 и 36,6 тыс. горожан с симптомами ОРВИ, подписавших постановление главного санитарного врача о соблюдении изоляции, что позволило обезопасить других горожан от инфекции, — рассказал представитель ДИТ. — Благодаря технологиям электронного мониторинга местоположения было зафиксировано порядка 47 тыс. нарушений режима изоляции — то есть случаев, когда пациенты с коронавирусом или симптомами ОРВИ, которые подписали соответствующие документы и обязаны соблюдать карантин, выходили на улицу и подвергали риску заражения остальных жителей».  
  
По мнению Василия Шишкина из НПК «Криптонит», платформа с совместными конфиденциальными вычислениями может быть полезной для развития информационных сервисов, сохраняющих конфиденциальность пользовательских данных. В то же время он отметил, что это новая область, которая на текущий момент не регламентирована российскими и международными стандартами, поэтому ее применение на практике требует ответственности и масштабной экспертизы на этапах проектирования, внедрения и использования криптографических средств.  
  
Вариантов воплощения системы может быть несколько, но до ее запуска сложно сказать, как будет реализован алгоритм совместных вычислений, рассуждает руководитель направления Big Data, ИТ-компании КРОК Егор Осипов. По его словам, если к хранилищу данных ни у кого не будет прямого доступа, то решится фундаментальная проблема утечки данных.  
  
https://www.rbc.ru/technology\_and\_media/14/05/2020/5ebadba69a79478f96365342?utm\_source=yxnews&utm\_medium=desktop&utm\_referrer=https%3A%2F%2Fyandex.ru%2Fnews

# Почему мировым IT-гигантам наплевать на персональные данные россиян

В западных странах процессы обработки личных данных находятся под строгим контролем государства. Например, в марте 2018 года широкий резонанс получил скандал, связанный с утечкой данных 50 миллионов пользователей социальной сети Facebook. Компания потеряла 60 миллиардов долларов в результате вынесенного судебного решения. Власти также установили, что, предположительно, компания знала об утечке информации, но не предпринимала никаких мер, блокирующих незаконное использование персональных данных. Летом 2019 года Facebook был оштрафован Федеральной комиссией США по торговле на 5 миллиардов долларов, что составило 9% от ее выручки в 2018 году. По схожему финальному сценарию развернулся судебный процесс против компании Google, которую обязали выплатить штраф в 22,5 миллионов долларов за нарушения, связанные с политикой конфиденциальности поисковика, а затем оштрафовали на 170 миллионов долларов за незаконный сбор данных о маленьких детях через видеохостинг YouTube. За рубежом наказания за подобного рода правонарушения ИТ-гиганты получают сравнительно регулярно.

В том же 2019 году, но уже в России, был вновь наложен штраф на Facebook, а также на другого гиганта информационного рынка — Twitter. Однако, в соответствии с российским законодательством, они отделались незначительными для своих бюджетов суммами. Каждая корпорация выплатила по 3000 рублей за нарушение условий хранения персональных данных россиян. Факт скандальный и смешной одновременно, поскольку за многие менее серьезные административные правонарушения в России взимаются штрафы, гораздо сильнее превышающие эту сумму.

Такой разрыв правоприменительной практики ведет к тому, что в своих домашних юрисдикциях иностранные компании гораздо ответственнее подходят к вопросу безопасности данных пользователей, так как никто не хочет побить следующий рекорд по величине взысканного штрафа. В нашей стране эти же самые компании могут позволить себе даже не явиться на заседание суда, так как выплата суммы в 3000 рублей является для них ничего не значащей.

Отношение со стороны крупных корпораций с многомиллионными или миллиардными оборотами не вызывает удивления. В России, в соответствии с Кодексом об административных правонарушениях, максимальное наказание по одному составу достигает 75 000 рублей, что в переводе составляет около 1 тысячи евро, а общая сумма выплат по всем составам правонарушения не превышает 300 тысяч рублей! Таким образом, соблюдать российское законодательство иностранные ИТ-компании никаким образом не мотивированы.

Для сравнения, в Европе в мае 2018 года были обновлены правила обработки персональных данных, установленные «Общим регламентом по защите данных» от 2016 года. В соответствии с ним ужесточается ответственность за нарушение правил обработки личных данных. Будучи довольно высокими и ранее, штрафы в настоящий момент могут достигать 20 миллионов евро или 4% годового глобального дохода компании.

В США, по аналогии с ЕС, решили разработать единый федеральный закон по регулированию работы с персональными данными. Процесс пока регламентируется только специальными нормативными актами в отдельных отраслях и на уровне штатов, в которых сосредоточена большая часть ИТ-компаний страны, а также с помощью Федеральной торговой комиссии — агентства, которое призвано защищать права потребителей.

Лидирующие в технологическом плане штаты оказались более быстрыми. Они уже разработали и вводят у себя аналоги европейского закона. Например, закон «О конфиденциальности данных» штата Калифорния, который регулирует права на доступ, хранение и удаление личных данных, вступит в силу уже в 2020 году. Нарушение обозначенной нормы может повлечь за собой штраф в размере 7500 долларов. Сумма невелика, если сравнить аналогичные европейские штрафы, но иск по калифорнийскому закону предъявлять может каждый отдельный пользователь. В таком случае выплата по коллективному требованию составит вполне внушительную цифру.

Таким образом, вопрос ужесточения ответственности в России за несоблюдение правил обработки персональных данных является актуальным др сих пор. Принятие мер необходимо в кратчайшие сроки, иначе отношение к работе с личной информацией россиян останется все на том же низком уровне, а случаи нарушения закона будут наблюдаться регулярно и повсеместно.

# За кем и как еще «присматривает» Google

Довольно часто то и дело всплывает очередная история о том, как крупнейшие ИТ-гиганты следят за нами. В этот раз опять «отличился» Google. Теперь корпорация залезла в медкарты.

Во вторник The Wall Street Journal шокировал американское общество своей новостью о том, что Google имеет доступ к медицинским данным: врачебным записям, именам и адресам. Компания получила доступ к огромному массиву данных о пациентах из США без необходимости уведомлять этих пациентов благодаря сделке с одной из крупнейших медицинских фирм.

The Guardian передает, что сотрудник, который работает в проекте «Nightingale», был разгневан тем, что пациентов держат в неведении о крупной сделке. Как он заявил: «Я должен рассказать о том, что творится за кулисами», — после чего слил в сеть подтверждающее видео. На платформе Daily Motion он выложил архив из сотен изображений конфиденциальных файлов, относящихся к проекту Nightingale.

Секретная схема предусматривает передачу в Google медицинских данных, принадлежащих Ascension, второму по величине поставщику медицинских услуг в США.

В отличие от других аналогичных ситуаций, анонимность не была обеспечена, хотя обычно в таких случаях применяется процесс удаления личной информации, известный как деидентификация. \

Раскрытые документы включают в себя строго конфиденциальные сведения о проекте, описывающие четыре его фазы.

К моменту завершения сделки в марте следующего года компания Ascencion должна передать Google персональные данные 50 миллионов пациентов в 21 штате, из которых около 10 миллионов уже передано. Пациентов и врачей, конечно же, ставить в известность нужным не посчитали.

Стоит отметить, история происходит в США, где люди боятся говорить врачам даже свой вес. Поэтому сотрудники проекта и поделились секретной информацией. Они заявили: «Большинство американцев чувствовали бы себя неловко, если бы узнали, что их данные передаются в Google без надлежащих гарантий безопасности. Это совершенно новый способ ведения дел. Вы хотите, чтобы ваша самая личная информация была передана в Google? Я думаю, многие люди скажут „нет“».

В корпорации лишь отмахиваются от журналистов, называя подобное «обычной» практикой. Ну, а с «обычными» практиками Google мы знакомы не понаслышке.

Ранее уже был выявлен случай слежки компании за своими сотрудниками. В этом году пару недель назад компанию обвинили сами сотрудники. Они выявили инструмент внутреннего наблюдения, который, по их мнению, в перспективе мог быть использован для мониторинга возможных акций протеста и любых дискуссий о трудовых правах.

Данный инструмент отслеживает любые крупные собрания, организованные с помощью программы Google Календарь. Наиболее вероятным объяснением, как утверждается в меморандуме, подписанном 3 анонимными сотрудниками компании и опубликованном в Bloomberg, «является то, что это попытка руководства немедленно узнать о любых способах самоорганизации трудящихся».

Но это хотя бы объяснимо, минимум корпоративной безопасностью. Объяснить новый выявленный случай сложнее. Ведь к медицинским данным всегда применялась особая политика конфиденциальности. Что будет, если эти данные утекут из Google?

Какой ущерб могут принести данные о заболеваниях и медицинских показателях людей? Новый выявленный случай свидетельствует о том, что компания ведёт целенаправленную политику по сбору данных разных категорий людей.

Кроме того, важен и тот аспект, что такими методами компания выходит в теневой сектор и получает конкурентное преимущество.

Ведь доступ к такому количеству данных для запуска в перспективного сервиса кому-то и как-то гарантирует сверхприбыль, вот только явно она достанется не самим людям, чьи данные вновь были втихую заполучены.

# Улыбнитесь, вас снимают. Как работает технология распознавания лиц

Функция распознавания лиц используется не только для подтверждения платежей и [разблокировки iPhone](http://club.esetnod32.ru/articles/analitika/kak-za-yablochnoy-stenoy/). Этой технологией пользуются все, кому не лень — от агентов спецслужб до производителей умных устройств. Из-за этого часто возникают проблемы с утечкой личных данных, но обо всем по порядку.   
Наши коллеги из CNET [рассказали](http://www.cnet.com/how-to/facial-recognition-apple-amazon-google-and-the-race-for-your-face-facebook%20), что такое распознавание лиц и как оно работает, а мы адаптировали материал. **Что такое распознавание лиц?**

Технология распознавания лиц — это вид биометрической аутентификации для подтверждения личности. В 1960-х годах ее разработал американский ученый Вудро Бледсоу на основе двумерных изображений. В то время приходилось вручную просматривать фото и вносить данные в компьютер. Сейчас это [делает нейросеть](http://habr.com/ru/company/odnoklassniki/blog/350566/) со скоростью 400 фотографий в секунду.   
Принцип распознавания по лицу схож с распознаванием по голосу или отпечатку пальца — механизм запоминает индивидуальные параметры для дальнейшей идентификации.  **Как работает система распознавания лиц?**

Система фиксирует изображение лица, а затем сравнивает оригинал с новым фото. Сейчас большинство механизмов работают с двумерными изображениями. На это есть две причины: во-первых, не все камеры воспринимают объем носа или глаза, а во-вторых, большинство справочных баз состоят из двумерных изображений — это фотографии из соцсетей или паспорта.  
2D-распознавание использует параметры носа, рта и глаз для идентификации лица. Система измеряет их ширину и форму, а также расстояние между ними. Эти показатели преобразуются в цифровой код, который называется отпечатком лица. **3D-распознавание лиц**

Камеры, которые чувствуют глубину, могут дополнить отпечаток лица высотой носа и глубиной глаз. Устройства проецируют невидимые спектры света на поверхность и улавливают обратный сигнал с помощью специальных датчиков. Это позволяет точно измерить расстояние между разными точками лица.   
В Face ID Apple использует 30 тысяч инфракрасных точек, которые сканируют даже самые мелкие черты внешности. Такой механизм обмануть практически невозможно, чего нельзя сказать про функцию распознавания лиц в смартфонах на Android. Ее удалось [ввести в заблуждение](http://hitech.vesti.ru/article/1126168/) с помощью искусственной головы.  **Распознавание по текстуре кожи**

Компания Identix разработала метод анализа текстуры кожи, который избавляет пользователя от недостатков стандартной технологии распознавания лиц.  
Анализ текстуры кожи отличается тем, что механизм работает в гораздо меньшем масштабе — вместо расстояния между носом и глазами он измеряет расстояние между порами. Полученная информация преобразуется в цифровой код, который называется отпечатком кожи.  
Этот метод так хорошо работает, что может определить разницу между близнецами. Сама Identix [утверждает](http://impactlab.media/2019/05/17/tehnologiya-raspoznavaniya-lits/), что технология повышает точность распознавания на 25%. **Где используется система распознавания?**

Распознавание лиц активно используется с конца 80-х годов. Тогда это было доступно только государственным структурам, но постепенно функция пришла в массы.   
Facebook уже несколько лет внедряет систему распознавания, точно так же, как Google Photos и другие IT-гиганты. Полученную информацию сервисы используют для повышения удобства и показа [таргетированной рекламы](http://club.esetnod32.ru/articles/analitika/ukhodim-s-radarov/).   
Механизм распознавания лиц используется в аэропортах, чтобы уменьшить очереди на паспортном контроле. А в 2020 году [пройдут первые](http://tass.ru/vef-2019/6839437) Олимпийские игры, в которых будет применяться функция распознавания лиц для обеспечения безопасности. **Чем опасно распознавание лиц?**

Эксперты по безопасности предупреждают о множестве проблем, начиная со слежки на улице и заканчивая получением хакерами личной информации.  
Самое неприятное, что камеры могут собирать информация без вашего ведома — в аэропортах, торговых центрах или других общественных местах. Но даже если вы узнаете об этом, то удалить свое фото из базы будет очень тяжело.   
Сегодня система распознавания лиц используется далеко не всех сферах, но уже сейчас возникают проблемы с нарушением частного пространства и вмешательством в личную жизнь.  
Многим не нравится такое пристальное внимание камер, если вы в их числе, советуем присмотреться к [средствам защиты](http://rb.ru/story/clothes-vs-facial-recognition/) от алгоритмов для распознавания лиц.[Фото](https://mirtesen.profile.ru/_/photo)

# Big Data Большого Брата

[**Журнал «Профиль»**](https://mirtesen.profile.ru/blog?utm_referrer=mirtesen.ru)

9 ноября 2019

У моего друга заболела спина. Он сделал МРТ позвоночника в крупной частной клинике, а потом купил себе дорогой ортопедический матрас. После этого он долго не мог отбиться от звонков с предложениями пройти «уникальный курс лечения спины» с «бесплатной» диагностикой. Практически каждый россиянин тут же приведет аналогичный пример (а то и несколько) из собственной жизни.

₽[](https://an.yandex.ru/count/GpiS7lL-Y18500W3CL0mnbq00000ECgO2q02I09Wl0Xe172QgvU02O01yTkUiWA80UYWvPa-a06scjNiCvW1oeIsrpUW0VwiWUmpg06YqhhIDxW1vFF1inp00GBO0VYSznZW0OgMf1Ne0Ou1-06Uzzw-0OW2jW6O0fogmHUW0k2YhHUv0cbxEX4EHWSTy0Btzwcq0e03dRIcnGI80uFNz8G7c0EPk0Ee0mYm0mIu1Fy1m0G8w0IG1VW4flKYY0MczIAG1T288w05-VODg0NvzWsm1Vds3RW5rFuDm0NmY1t81R3C2z05t9i4u0K-y0K1c0R4qPu2e0Pig0PioGO0kqoYZ4NfOT4604-26Or5wM7P1W00000N0000gGU1cGmaMySZNB07W82G3C07e9MmwWRG1mBW1v0DW0WCq0YwYe21m820Xe01u0YmqTOBW0e1g0he1y4A00000000y3_O2WBW2e29UeWBx0Ag2n3GADdLWPa00CjBkLxXbWK0m0k0emN82u3Kam7P2u6P32HRnoDSw0kczIBm2mQ839xtthu1w0mRc0svfK3W3OA0W0693W0000000F0_a0x0X3sO3e3sifBAiT7qOQ0E-fuvi0u1eGy00000003mFwWFWRF2uP_hyP5SsGy7ueQOA4tpF-0F0O0GeRh6590GsCRsyyhCrQk40PeG2H400000003mFyWG3D0GXeclN_WG-F__________0O0H-F__________0OWH0P0H0Q4H00000000y3-e4S24FR0H0SWHq8gOjGFW4R_HmG7e4PVSoyZLkuxmtW7n4G000000aBz0-X4P3VwQLpuLklCXFntTswaz9G00000j000008WI0P0I0QaIb4A9W5sCCp_m4lZ__________m7u4WE04nc84m6G4sIO4mIe4wRklBpyXjZg5S0J____________0TeJ2WW0400O0200A03W4zJ-3OWKmVd3tQ63Zkj1e1JK_Wse5D288yWK1D0K____________0TWKrCY0xWK0?stat-id=182&test-tag=274328394424321&format-type=24&actual-format=40&banner-test-tags=eyI2OTU5MDQ4MzQ3IjoiMjY4NDY4MjI0In0%3D)[Дома из бруса с экономией до 20%Строительство **домов** из **бруса** с 2009 г. Под Ключ и Под Усадку. Рассчитайте цену!lp.uralregionstroy.ru](https://an.yandex.ru/count/GpiS7lL-Y18500W3CL0mnbq00000ECgO2q02I09Wl0Xe172QgvU02O01yTkUiWA80UYWvPa-a06scjNiCvW1oeIsrpUW0VwiWUmpg06YqhhIDxW1vFF1inp00GBO0VYSznZW0OgMf1Ne0Ou1-06Uzzw-0OW2jW6O0fogmHUW0k2YhHUv0cbxEX4EHWSTy0Btzwcq0e03dRIcnGI80uFNz8G7c0EPk0Ee0mYm0mIu1Fy1m0G8w0IG1VW4flKYY0MczIAG1T288w05-VODg0NvzWsm1Vds3RW5rFuDm0NmY1t81R3C2z05t9i4u0K-y0K1c0R4qPu2e0Pig0PioGO0kqoYZ4NfOT4604-26Or5wM7P1W00000N0000gGU1cGmaMySZNB07W82G3C07e9MmwWRG1mBW1v0DW0WCq0YwYe21m820Xe01u0YmqTOBW0e1g0he1y4A00000000y3_O2WBW2e29UeWBx0Ag2n3GADdLWPa00CjBkLxXbWK0m0k0emN82u3Kam7P2u6P32HRnoDSw0kczIBm2mQ839xtthu1w0mRc0svfK3W3OA0W0693W0000000F0_a0x0X3sO3e3sifBAiT7qOQ0E-fuvi0u1eGy00000003mFwWFWRF2uP_hyP5SsGy7ueQOA4tpF-0F0O0GeRh6590GsCRsyyhCrQk40PeG2H400000003mFyWG3D0GXeclN_WG-F__________0O0H-F__________0OWH0P0H0Q4H00000000y3-e4S24FR0H0SWHq8gOjGFW4R_HmG7e4PVSoyZLkuxmtW7n4G000000aBz0-X4P3VwQLpuLklCXFntTswaz9G00000j000008WI0P0I0QaIb4A9W5sCCp_m4lZ__________m7u4WE04nc84m6G4sIO4mIe4wRklBpyXjZg5S0J____________0TeJ2WW0400O0200A03W4zJ-3OWKmVd3tQ63Zkj1e1JK_Wse5D288yWK1D0K____________0TWKrCY0xWK0?stat-id=182&test-tag=274328394424321&format-type=24&actual-format=40&banner-test-tags=eyI2OTU5MDQ4MzQ3IjoiMjY4NDY4MjI0In0%3D)Скрыть объявление[](https://an.yandex.ru/count/GpiS7YMRZli500u3CL0mnbq00000ECgO2q02I09Wl0Xe172QqvNR3O01Zlp4FeW1-yN9oYUG0QQDhlKXc07Klzgm8g01j8skzI6e0Rw_sh0Yk07Kmygd5S010jW1hhdY3-01i8Ee3UW1a0Bu0Swkthu1Y0As0Q02ngN35ha2QNiw4Gv61ntm0lVtgRG2W0EytzIp3uW3Xv3DsWUO0xBK0w031AW32B031BW4_m7010Ze1CWK-0J1ZGY81S6D2905tUa8e0N4l0Ae1UE70h05uuS2k0MSdmB01QY51SW5YAG1q0MbVU05Fl050PW6_BoLo0AW1coe1cp91W2xJAACHUbXqGO0Ju8PZKNfOTa6000001S0002f1u6P32HRnoDSi0U0W90Cm0UWbR3g1j070k07XWg020pG2BgAW870W826W07W2EFIeGk02W6e2kW7mGe00000003mFzWA0k0AW8bw-0g0jHY82-m2gWiGq2ZPrO6P003BIxbUuPO50C0BWAC5o0k0r9C1sGk1cGmaMySZNEWBmOq8y0i6Y0pEhjw-0UWC6vWDkQL0u0s2W801YGu00000002mFf0Em8Gzc0w0zhAIoh7Hz66W3i24FR0E0Q4F00000000y3-e3u6pmk6Vw_6HNDaFk2HEKk-BzJ_W3m604EN_-0sG4DZ6zlFApDMhX06Q4189G0000000000HpSpCpCpCz3_848o01FWG-F__________0O0H-F__________0OWH0P0H0Q4H00000000y3-e4S24FR0H0SWHq8gOjGFW4R_HmG7e4PVSoyZLkuxmtW7n4G000000aBz0-X4P3V-xMpuLqZk1FntG6fGy9G00000j000008WI0P0I0QaIUcg3w7pT6p_m4lZ__________m7u4WE04nc84m6G4sIO4mIe4wRklBpyXjZg5S0J____________0TeJ2WW0400O0200A03W4voV0eWKmVd3tQ63Zkj1e1ISdmAe5Dtf2CWK1D0K____________0TWKtEEDwmK0?stat-id=182&test-tag=274328394424321&format-type=24&actual-format=40&banner-test-tags=eyI0NTUyMjQ2MDk5IjoiMjY4NDY4MjI0In0%3D)[Удиви соседей новым забором!8 видов **штакетника**! По размерам за 1 день. Доставка. Выбирай на сайте!купить-штакетник.рф](https://an.yandex.ru/count/GpiS7YMRZli500u3CL0mnbq00000ECgO2q02I09Wl0Xe172QqvNR3O01Zlp4FeW1-yN9oYUG0QQDhlKXc07Klzgm8g01j8skzI6e0Rw_sh0Yk07Kmygd5S010jW1hhdY3-01i8Ee3UW1a0Bu0Swkthu1Y0As0Q02ngN35ha2QNiw4Gv61ntm0lVtgRG2W0EytzIp3uW3Xv3DsWUO0xBK0w031AW32B031BW4_m7010Ze1CWK-0J1ZGY81S6D2905tUa8e0N4l0Ae1UE70h05uuS2k0MSdmB01QY51SW5YAG1q0MbVU05Fl050PW6_BoLo0AW1coe1cp91W2xJAACHUbXqGO0Ju8PZKNfOTa6000001S0002f1u6P32HRnoDSi0U0W90Cm0UWbR3g1j070k07XWg020pG2BgAW870W826W07W2EFIeGk02W6e2kW7mGe00000003mFzWA0k0AW8bw-0g0jHY82-m2gWiGq2ZPrO6P003BIxbUuPO50C0BWAC5o0k0r9C1sGk1cGmaMySZNEWBmOq8y0i6Y0pEhjw-0UWC6vWDkQL0u0s2W801YGu00000002mFf0Em8Gzc0w0zhAIoh7Hz66W3i24FR0E0Q4F00000000y3-e3u6pmk6Vw_6HNDaFk2HEKk-BzJ_W3m604EN_-0sG4DZ6zlFApDMhX06Q4189G0000000000HpSpCpCpCz3_848o01FWG-F__________0O0H-F__________0OWH0P0H0Q4H00000000y3-e4S24FR0H0SWHq8gOjGFW4R_HmG7e4PVSoyZLkuxmtW7n4G000000aBz0-X4P3V-xMpuLqZk1FntG6fGy9G00000j000008WI0P0I0QaIUcg3w7pT6p_m4lZ__________m7u4WE04nc84m6G4sIO4mIe4wRklBpyXjZg5S0J____________0TeJ2WW0400O0200A03W4voV0eWKmVd3tQ63Zkj1e1ISdmAe5Dtf2CWK1D0K____________0TWKtEEDwmK0?stat-id=182&test-tag=274328394424321&format-type=24&actual-format=40&banner-test-tags=eyI0NTUyMjQ2MDk5IjoiMjY4NDY4MjI0In0%3D)Скрыть объявление[](https://an.yandex.ru/count/GpiS7lSYnkm50Fy2CL0mnbq00000ECgO2q02I09Wl0Xe1720hSPGW061ZBQV1OW1ahR8enkG0T3_gzGJc06SaeZp5Q01pl-hr1Ee0V2HYFCLk07evFha3i010jW1slB-2k01pjlZ2kW12FW1dlVUlW680hO1e0AUXg4AkG9fUpeH3aO77V02z_Ufj0AO0_GDe0C6g0C8i0C4k0J_0S042EW4ZXtu1DAk1OW5qgu5a0NIZ0QW1RxH0QW5oQu1i0N9hW6u1Rp60S05bSq9o0N0k0BG1VLIu0K_y0K1c0RahO-k1g06RAW6RCa60BjCeen5wM7H1W1FWXcDHUbXsGO000005m000Aa7WPaC95l78rom1u20a0p01w2LiEe6q0S2s0S1u0U62e083D08keg0WS20W8Q00U08ZyEG1O0A0QWAw0V12W0000000F0_s0e2u0g0YNhu2e2r68WBx0Ag2n3GADdLWPa00CjBkLxXbWK0m0k0emN82u3Kam7P2u6P32HRnoDSw0lIhWNm2mQ839xtthu1w0mRc0svfK3W3OA0W0693W000000070za0x0X3sO3e3sifBAiT7qOQ0Em8Gzi0u1eGy00000003mFwWFWRF2uP_hyP5SsGyXAK7WOS_sF-0F0O0Gfesp2f0GsCRsyyhCrQk40PeG4Wa08000000001400000003WFyWG3FWG-F__________0O0H-F__________0OWH0P0H0Q4H00000000y3-e4S24FR0H0SWHq8gOjGFW4R_HmG7e4PVSoyZLkuxmtW7n4G000000aBz0-X4P3GC_Y3uLWeboFnqzdXaz9G00000j000008WI0P0I0QaI9IKv9a717Z_m4lZ__________m7u4WE04nc84m6G4sIO4mIe4wRklBpyXjZg5S0J____________0TeJ2WW0400O0200A03W4xp60OWKmVd3tQ63Zkj1e1IynW6e5DAC1iWK1D0K____________0TWK_BJtuGK0?stat-id=182&test-tag=274328394424321&format-type=24&actual-format=40&banner-test-tags=eyIyNjM4NTc3NjQwIjoiMjY4NDY4MjI0In0%3D)[Дом 6х9 м. за 395 000 рублей!Комплект **дома** с монтажом из **бруса** 150х150 мм. Под крышу. 84 м. кв. Звоните!ekaterem.ru](https://an.yandex.ru/count/GpiS7lSYnkm50Fy2CL0mnbq00000ECgO2q02I09Wl0Xe1720hSPGW061ZBQV1OW1ahR8enkG0T3_gzGJc06SaeZp5Q01pl-hr1Ee0V2HYFCLk07evFha3i010jW1slB-2k01pjlZ2kW12FW1dlVUlW680hO1e0AUXg4AkG9fUpeH3aO77V02z_Ufj0AO0_GDe0C6g0C8i0C4k0J_0S042EW4ZXtu1DAk1OW5qgu5a0NIZ0QW1RxH0QW5oQu1i0N9hW6u1Rp60S05bSq9o0N0k0BG1VLIu0K_y0K1c0RahO-k1g06RAW6RCa60BjCeen5wM7H1W1FWXcDHUbXsGO000005m000Aa7WPaC95l78rom1u20a0p01w2LiEe6q0S2s0S1u0U62e083D08keg0WS20W8Q00U08ZyEG1O0A0QWAw0V12W0000000F0_s0e2u0g0YNhu2e2r68WBx0Ag2n3GADdLWPa00CjBkLxXbWK0m0k0emN82u3Kam7P2u6P32HRnoDSw0lIhWNm2mQ839xtthu1w0mRc0svfK3W3OA0W0693W000000070za0x0X3sO3e3sifBAiT7qOQ0Em8Gzi0u1eGy00000003mFwWFWRF2uP_hyP5SsGyXAK7WOS_sF-0F0O0Gfesp2f0GsCRsyyhCrQk40PeG4Wa08000000001400000003WFyWG3FWG-F__________0O0H-F__________0OWH0P0H0Q4H00000000y3-e4S24FR0H0SWHq8gOjGFW4R_HmG7e4PVSoyZLkuxmtW7n4G000000aBz0-X4P3GC_Y3uLWeboFnqzdXaz9G00000j000008WI0P0I0QaI9IKv9a717Z_m4lZ__________m7u4WE04nc84m6G4sIO4mIe4wRklBpyXjZg5S0J____________0TeJ2WW0400O0200A03W4xp60OWKmVd3tQ63Zkj1e1IynW6e5DAC1iWK1D0K____________0TWK_BJtuGK0?stat-id=182&test-tag=274328394424321&format-type=24&actual-format=40&banner-test-tags=eyIyNjM4NTc3NjQwIjoiMjY4NDY4MjI0In0%3D)Скрыть объявление

А вот классика европейской практики. Человек сказался больным, укатил в отпуск и выложил фотки с пляжа в Facebook. Возмущенный работодатель предъявил эти фотографии вернувшемуся с «больничного» сотруднику, но в итоге сам и пострадал: компанию оштрафовали за нарушение правил обработки персональных данных, поскольку сотрудник не давал согласия на использование их в соцсетях.

В этом и заключается принципиальное отличие российского законодательства о персональных данных от европейского, рассказали эксперты на II ежегодной конференции, которая так и называлась: «Работа с персональными данными: новые правила безопасности в цифровом мире». В Европе компании, уличенные в противоправном использовании таких данных, рискуют заплатить многомиллиардные (в рублевом эквиваленте) штрафы. Но при этом законодательство, особенно действующий с начала прошлого года Генеральный регламент о защите персональных данных (GDPR), а также судебная практика во главу угла ставят права человека.

В России штрафуют на смехотворные по сравнению с этим суммы – до 75 тыс. рублей. Правда, в первом чтении уже приняты поправки в КоАП, по которым штрафы за нарушения требования хранить персональные данные россиян на территории РФ будут достигать аж 18 млн рублей. Но не факт, что законопроект дойдет до финала в таком виде – слишком уж не вяжется такая строгая санкция с другими аналогичными правонарушениями.

Но в целом государство уже взяло курс на создание баз данных своих граждан со всеми сведениями о них. Первая, под патронатом ФНС, должна заработать в ближайшие два-три года. А потом, глядишь, посчитают всех и вся. Вот только от спамеров с рекламными предложениями нам никак не отбиться, жалуйся не жалуйся – ответа не получишь. Потому что главная цель охраны персональных данных в России – безопасность и государственные интересы, а права человека, увы, вторичны.

Устрицы не предлагать

Кажется, совсем недавно мы и знать не знали о том, что такое персональные данные. И вот они уже превратились в некую «священную корову», «новую нефть» – big data, большие данные. В кафе при одном из американских университетов, например, студентам предлагают расплачиваться персональными данными за кофе. И разве так страшно соглашаться на «печеньки» (cookies) с различных платформ, которые потом, отследив наши предпочтения, услужливо предложат те товары, которые мы давно разыскиваем?

Люди поделились на две категории, говорит директор по связям с госорганами Baring Vostok Марина Амелина. Первые стараются оставлять о себе как можно меньше данных в Сети, блюдут свою анонимность. Вторые, наоборот, с удовольствием делятся информацией и наблюдают, как их обогащенные данные используются для улучшений сервисов. Последние, конечно, должны соблюдать законы и с пользователями заключать соглашения. «Платформа может обмениваться вашими обогащенными данными с букингом, сервисами доставки еды, как бы намекая: устрицы предлагать не нужно, вы любите окрошку, – говорит эксперт. – Но об этом нужно договориться, юридически зафиксировать».

Но и у тех, кто ратует за анонимность, есть на то резоны. Однажды в Америке зашел человек в «Макдоналдс». Настроение было у него плохое, день не задался, и он сорвался на беременную девушку-кассира – нагрубил, запустил стаканчиком. Эту сцену зафиксировала видеокамера, запись попала в интернет. Человека возненавидели, подвергли обструкции. Он потерял работу и долгое время не мог найти новую – куда бы он ни приходил, везде всплывала та история. Несчастный оказался в полной социальной изоляции и застрелился в собственной машине.

Конечно, не все утечки столь фатальны по своим последствиям. Но даже спамерам тоже никто не рад. А в России уже известны случаи взломов портала госуслуг, последствия которых могут причинить существенный материальный вред. Кража личности – больше не миф, а суровая реальность. Недавно «Профиль» подробно рассказывал о том, насколько массовыми стали утечки персональных данных и как ими могут воспользоваться мошенники. Техники и технологии киберпреступников разнообразны и постоянно совершенствуются. Специалистам по кибербезопасности приходится работать на опережение, но их старания не будут достаточно эффективными, если законодатели будут топтаться на месте.

Пока за нарушения правил хранения персональных данных россиян на территории РФ штрафуют всего на 5 тыс рублей. В скором времени эта сумма может измеряться в миллионахShutterstock / Fotodom

Персональные хроники

История законотворчества в области защиты персональных данных берет свое начало ни много ни мало с Декларации «О правах человека» ООН 1948 года, рассказывает старший менеджер KPMG России и СНГ Кристина Боровикова. «Это один из первых документов в мире, которым были определены фундаментальные права человека, в том числе право на частную жизнь, тайну переписки, на свободу высказываний», – говорит она.

В 1953 году те же постулаты были закреплены в Европейской конвенции «О защите прав человека и основных свобод». Но само определение «персональных данных» родилось в период с 1968‑го по 1974 год, когда Совет Европы дорабатывал конвенцию и принял рекомендации по обеспечению неприкосновенности частной жизни, а также по развитию технологий и научных разработок. Также в 1973 и 1974 годах были выпущены резолюции и рекомендации по обеспечению обработки личных данных человека с использованием автоматизированных банков данных в частном и государственных секторах. В этих резолюциях были определены и права субъектов персональных данных.

Вся последующая эволюция законодательства была обусловлена тем, что страны Европы тесно общались между собой, обменивались информацией. Экономические связи крепли, а правила обращения с персональными данными у всех были разные. Нужно было все унифицировать. К выходу конвенции такие страны, как Германия, Великобритания и Франция, уже имели в конституциях формулировки, которые гарантируют тайну переписки и сохранность личной информации. Другие страны в период с 1968‑го по 1980‑й тоже начали дорабатывать локальное законодательство.

В 1980‑м Организация экономического сотрудничества и развития (ОЭСР) разработала рекомендации по обработке личных данных, а также передаче этой информации. Эти рекомендации легли в основу создания в 1981 году Конвенции «О защите физлиц при автоматизированной обработке персональных данных» (ETS‑108). Россия ратифицировала ее в 1998 году. Эта конвенция легла в основу российского федерального закона «О персональных данных» 2006 года. На основе этой конвенции был построен и GDPR.

В 1995 году была принята самая известная директива по обработке персональных данных. Она распространяется на Европейский союз и обязует страны ЕС дорабатывать свое законодательство с учетом требований директивы. Это был серьезный шаг к унификации законодательства. Затем в 2000‑м принципы обработки персональных данных закрепили в Хартии по правам человека ЕС. А в 2007‑м единое определение персональных данных для ЕС было принято Лиссабонским соглашением.

«Но им чего-то не хватало, – рассказывает Кристина Боровикова. – Законодательство в странах ЕС все равно было разрозненным. Где-то нужно было уведомлять контролирующие органы о занесении в специальный реестр (по аналогии с российским реестром организаторов распространения информации), а где-то – нет. В одних странах назначались ответственные за обработку данных, в других их не было. Тогда и случился GDPR».

Генеральный регламент вступил в силу в 2018 году и сразу ошарашил бизнес-сообщество: раньше таких колоссальных штрафов не было не только в европейских странах, но и вообще в мире, включая США. Вслед за GDPR обновили и конвенцию ETS‑108 Совета Европы, а это означало, что новые правила стали обязательными не только для Евросоюза, но почти для всего остального континента, включая Россию.

Удар по кошельку

Один из первых штрафов по GDPR в размере 400 тыс. евро получила больница в Португалии в начале прошлого года, рассказала директор по консалтингу InfoWatch Мария Воронова. Регулирующий орган посчитал, что к данным пациентов имело доступ большее число персонала, чем это было необходимо. А немецкий сайт знакомств Knuddles оштрафовали на 20 тыс. евро за то, что логины и пароли хранились в незашифрованном виде. Датская компания-перевозчик Taxa 4×35 была оштрафована на 160,8 тыс. евро за хранение в своих системах более 8 млн записей личной контактной информации, в том числе геолокацию, без правового основания – просто так, про запас.

«Штрафы по GDPR очень высокие, и бизнес реально за это наказывают, – говорит Кристина Боровикова. – Для российского бизнеса такие суммы – смерть». При этом суммы штрафов прямо пропорциональны нанесенному ущербу. В сети отелей Marriott, например, из-за утечки данных пострадали гости из 31 страны, некоторым пришлось менять паспорт. За это компании пришлось заплатить сумму, эквивалентную 7,8 млрд рублей.

Кроме утечек, поводом для штрафа могут стать жалобы субъектов персональных данных. «А они очень активно их пишут, – продолжает эксперт. – Недавно European Data Protection Board (контролирующий орган по GDPR) приводил статистику по росту количества жалоб – число выросло в среднем до 100 жалоб на одну компанию».

Испанская футбольная La Liga за свою хитрую слежку за пользователями была наказана на сумму, эквивалентную 17,8 млн рублей. Лига использовала мобильное приложение, которое во время трансляций матчей запускало запись и отслеживало болельщиков в барах. По геолокации компания могла проследить, какие из баров оплатили подписку на трансляцию, а какие – нет. Есть и другие примеры. Райффайзенбанк наказали за то, что тот передавал кредитные истории и личные данные клиентов по WhatsApp. Google оштрафовали в пересчете на рубли на 3,6 млрд только за то, что их политика по обработке персональных данных была недостаточно ясной.

При этом GDРR ориентирован на защиту прав человека, подчеркивает Мария Воронова. Поэтому в нем очень подробно расписаны категории персональных данных. В отличие от российского законодательства, например, в GDPR к ним относят cookies, IP-адреса, геолокацию, номер машины. Есть и специальная категория: расовая принадлежность, этническое происхождение, политические взгляды, состояние здоровья и т. д. «Даже ФИО супругов и их пол – тоже спецкатегория, – добавляет эксперт, – потому что по ним можно определить ориентацию человека».

Потому и приведенный в начале статьи случай с отправившимся на пляж прогульщиком для Европы – обычная практика. Мария Воронова привела еще несколько примечательных примеров. Человек получил взыскание за служебное нарушение, доказательством которого стала видеозапись этого проступка, сделанная его сослуживцем на мобильный телефон. Но в итоге за незаконную запись оштрафовали саму компанию.

Работница другой европейской компании потребовала удалить дату ее рождения и возраст из справочника сотрудников на портале компании. Женщина заявила, что уже немолода и опасается, что ее могут уволить по причине возраста. Даму из системы удалили. Многие компании в Европе используют биометрический вход в свой офис (по сетчатке глаза, например). Но можно отказаться от биометрического профилирования, и для таких сотрудников в компании организуют отдельный вход. При переходе из одного банка в другой можно потребовать удаления всех своих данных из первого банка, и это обязательно будет сделано.

«Если я не хочу, чтобы мои данные, даже обезличенные, использовались где-то для каких-то статистик, я могу реализовать это право в Европе, – продолжает эксперт. – В России нас даже никто об этом не спрашивает». Или вот еще пример. Телеком-оператор OTE был оштрафован на 400 тыс. евро за отправку рекламных рассылок без согласия пользователей и без возможности отписаться от рассылки. «Можете представить себе такую ситуацию у нас?» – задает вопрос Мария Воронова. Это утопия, уверена она, поскольку сама провела эксперимент: рассылала запросы (по всей форме, по действующим регламентам) по разным организациям с требованием уточнения ее данных в рамках закона «О персональных данных», писала отказы от их обработки. «Ни разу ответа не получила,– сообщила о результате эксперимента эксперт. – Пока это у нас не работает».

Русская вольница

Не стоит думать, однако, что российским компаниям европейские штрафы не грозят. Если у наших компаний есть свои филиалы в Европе, они тоже подпадают под действие GDPR. Как и онлайн-магазины с доставкой по ЕС, как и открытые для пользователей всего мира соцсети с хостингом в России, как и поставщики услуг (туркомпании, перевозчики). Таргетированный сбор cookie-файлов для рекламы и поведенческих моделей (если на сайте организации установлена, например, Яндекс Метрика или Google Analytics) даже для общедоступной обезличенной статистики тоже может стать объектом внимания контролирующих органов ЕС. Если у российской компании заключен договор с европейцами, то ответственность (и штраф) в случае нарушения обращения с персональными данными наступит на его основании. Если такого договора нет, то компании могут запретить деятельность в Европе.

Но в самой России с персональными данными «в определенном смысле полная вольница», признает Марина Амелина. «Государство до сих пор не определилось, кто же на самом деле коренной владелец данных», – говорит она. Например, уже сейчас есть миллионы датчиков, которые собирают данные об автомобилистах, их стиле вождения, предпочтениях, геолокации. Но никто не знает, куда передаются эти данные и как используются.

Конечно, ответственность за нарушение законодательства РФ в области персональных данных есть. Она предусмотрена статьей 13.11 КоАП. Только вот максимальная санкция за эти нарушения всего 75 тыс. рублей. Для большинства компаний это не деньги. При этом каждое третье дело по привлечению к ответственности заканчивается отказом по процессуальным основаниям – просто не успевают привлечь, отмечает ведущий юрист ФБК Legal Валентина Полякова. Срок привлечения к ответственности – три месяца. Роскомнадзор и суд в него часто не укладываются.

Еще хуже дела обстоят с нарушением правил о локализации персональных данных – обязанности хранить данные граждан РФ на территории РФ. Специальной статьи для этого нарушения нет, поэтому наказывают по ст. 19.7 КоАП («Непредставление сведений»), а максимальная санкция по ней и вовсе 5 тыс. рублей.

Проблема в том, что закон «О персональных данных» безнадежно устарел – в этом году ему стукнуло 13 лет. Закон даже толком не определяет, что такое персональные данные, и дает туманное объяснение, что это «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». «Роскомнадзор буквально месяц назад признал, что email и номер телефона также являются персональными данными», – говорит Мария Воронова.

Изменения планируются, и весьма кардинальные. Так, Госдума приняла в первом чтении поправки в КоАП, добавив в ст. 13.11 еще два пункта о нарушениях требований о локализации персональных данных. Санкции приблизятся к европейским: юрлиц будут штрафовать на сумму от 2 млн до 6 млн рублей, а за повторное нарушение – от 6 млн до 18 млн рублей.

«Меры ответственности просто пугают, – говорит Валентина Полякова. – Непонятно, как будет определяться степень вины и размер наказания. Почему суммы такие большие? Для всех ли юрлиц и ИП они будут идентичными, как это коррелируется с их оборотами?». Правда, профильный думский комитет по законодательству тоже отметил: санкции слишком высоки и не соответствуют подходам, которые применяются в КоАП в аналогичных ситуациях. «Например, ответственность за разглашение в интернете сведений, содержащих гостайну, составляет от 100 тыс. до 1 млн», – добавила эксперт.

По идее, законодательство в области персональных данных в России должно развиваться симметрично GDPR. Поскольку конвенцию Совета Европы ETS‑108 в этой сфере уже поправили, а Россия ее подписала, то теперь очередь за ратификацией и внесением соответствующих изменений во внутреннее законодательство. Сейчас проект ратификации находится на стадии общественного обсуждения. «Но ходят слухи, что на этом этапе он и останется», – говорит Кристина Боровикова.

Россия пошла по пути огосударствления персональных данных, говорят эксперты. Это означает, что операторами баз данных россиян будет либо само государство, либо госкомпанииАнтон Денисов / РИА Новости

Под недреманным оком государства

Если это так, то по какому пути пойдет Россия? Похоже, что он уже выбран: государство, по всей видимости, вознамерилось стать единоличным владельцем всех персональных данных россиян. Во всяком случае, именно такую версию обрисовал депутат Госдумы, заместитель председателя комитета по информационной политике и информационным технологиям Андрей Свинцов.

«Недавно мы приняли законопроект о создании единой базы населения на основе данных ЗАГСов, – сказал он. – Ее оператором будет ФНС. Наверное, по таким лекалам в целом пойдет развитие системы big data и защиты персональных данных». Таким образом, ФНС получит сведения не только о каждом гражданине, но и обо всех его ближайших родственниках. «Наверняка там будут еще агрегироваться взаимосвязи физлица, его окружения, юрлиц, бизнеса, налогов, доходов, расходов – всего, что важно для государства, чтобы высосать последнее из людей», – предполагает депутат. Пока в этой базе не будет, например, сведений о недвижимом имуществе или транспортных средствах.

Но это пока. Скорее всего, предполагает депутат, после того как в течение двух-трех лет эта база заработает, в ближайшие 10 лет будут созданы еще 5–10 аналогичных баз, операторами которых станут госорганы (Роскомнадзор, ФСБ) или госкомпании. «Весь остальной бизнес на контрактах будет получать тот объем данных, за который он заплатит», – рассуждает Андрей Свинцов. Ну а потом, лет через 20, появится и единая база.

И зря бизнес протестует и угрожает сворачиванием развития технологий, уверяет депутат. Технологии развиваются слишком быстро, государству за ними не поспеть все равно. И для него «обеспечение безопасности важнее, чем развитие того или иного сервиса, которое может привести к непредсказуемым последствиям».

Такими последствиями стали последние выборы в Мосгордуму, на которых проводился эксперимент с электронным голосованием, привел пример депутат. «Единая Россия» с треском пролетела, – напомнил Свинцов. – Точнее, как бы не участвовала. Но представители «как бы от этой партии» большинство в Думе чуть не потеряли. На это они пойти не могли, и пять округов они ночью «перерисовали» за счет электронного голосования».

Проблема в том, что проверить подлинность такого волеизъявления невозможно. Зашел человек в свой аккаунт на госуслугах, проголосовал, сигнал поступил в КОИБ (комплекс обработки избирательных бюллетеней), и тот распечатал бюллетень. «Но таким образом можно получить 100% за «Единую Россию», – рассуждал депутат. – Так и вышло. В этих пяти округах, в электронных КОИБах, рейтинг за «как бы «Единую Россию» 50–80%. На всех остальных участках 20–30%».

Может быть, «там не было чистого мошенничества», предполагает он: «Просто заранее собрали (в этих округах) свой ядерный электорат, раздали пароли, заставили пройти регистрацию через «личный кабинет» и за счет этого выиграли. Но это очередная технология, уловка». Проверить это нельзя – бюллетени обезличены. «Это технология, которая позволит правящей на момент выборов партии выигрывать всегда», – считает депутат.

«Ключевое в любой стране – политические процессы, экономические идут как следствие», – резюмировал Свинцов. Но все зависит от того, куда движется этот процесс. «В России на митингах телевизионщики снимают публику, запускают это в эфир, – приводит еще одно сравнение Мария Воронова. – В Европе любой намек на распознавание политических взглядов гражданина – это обработка спецкатегории персональных данных без его согласия. Там съемка митингов должна вестись либо удаленно, чтобы не было возможности идентифицировать лицо и опознать гражданина, либо фон с митингующими должен быть размытым».

# Любой гаджет может шпионить

Ядра процессоров ARM, которые есть абсолютно в любом телефоне, а также в планшетах, умных телевизорах, устройствах интернета вещей и бытовой технике, можно использовать для слежки — об этом «Известиям» рассказали специалисты по информационной безопасности. Они провели ряд экспериментов, которые предполагают загрузку в секретную зону процессора шпионского ПО и доказали, что таким образом можно получить доступ ко всем функциям используемого телефона. Это исследование позволяет сделать вывод о невозможности обеспечения информационной безопасности без налаживания отечественного производства подобных устройств.

**Санкционированный доступ**

Британская корпорация ARM (Advanced RISC Machines) сегодня является абсолютным лидером на рынке микропроцессорных ядер. По последней информации, в 2018 году она лицензировала 22 млрд процессорных ядер, то есть по три на каждого жителя Земли. Их покупают практически все производители телефонов, умной и бытовой техники, планшетов, телевизоров, фитнес-трекеров, умных часов и т.д.

К каждому такому ядру прилагается подробное описание на десятки тысяч страниц. В нём есть упоминание о секретной зоне, с существованием которой покупающий чип производитель электроники может согласиться или же предпочесть другую конфигурацию, но в этом случае ему не гарантируется безопасность. Стоит ли говорить, что все предпочитают более защищенный чип.ото: ТАСС/Александр Демьянчук

Российские специалисты компании «Аладдин Р.Д.», ведущего российского разработчика продуктов и решений для обеспечения информационной безопасности и защиты конфиденциальных данных, провели подробный анализ используемых ARM-процессоров в современных телефонах. Выяснилось, что секретная зона может использоваться для загрузки в нее шпионского ПО, которое работает с широким спектром задач.

— С моей точки зрения, это пример идеальной «мягкой силы», с помощью которой можно получить контроль над информацией, а значит, и рычаг влияния на весь мир, — считает руководитель отдела развития доверенной платформы «Аладдин Р.Д.» Андрей Волков. — Представьте, что ваша компания просто сделала хорошие чипы с подробной документацией. Потом их купили все производители телефонов и других умных устройств. И теперь вы можете подключиться к любому такому устройству в мире с помощью изменения настроек в секретной зоне. Причем основная операционная система, которая расположена в видимой зоне, даже не подозревает о том, что такое подключение произошло.

**На темной стороне**

Чтобы проверить возможности секретной зоны, специалисты компании «Аладдин Р.Д.» загрузили туда софт с разными возможностями несанкционированной кражи данных.

Стоит понимать, что секретная зона (или так называемая TrustZone) — это не какая-то физическая область, а режим работы процессора. Код, исполняемый в таком режиме, имеет неограниченный доступ ко всем интерфейсами процессора, а значит, к любым функциям устройства.

В первом эксперименте планировалось доказать, что программа, действующая в секретной зоне, сможет фиксировать и передавать по назначенному адресу все нажатия на экранной клавиатуре. В результате исследователи получили успешно переданные: пароль, номера и сообщения, а также введенные номера кредитных карт и пароли для доступа в личные платежные кабинеты.Фото: TASS/Markku Ulander

Во втором эксперименте ставилась цель записать и передать аудиофайлы, используя только работу ПО из секретной зоны. Как выяснилось, с этой задачей также можно легко справиться.

В третьем эксперименте исследовались возможности эксплуатации секретной зоны, когда телефон находится в спящем режиме. Как оказалось, этот алгоритм действий является особенно эффективным. Ведь когда телефон засыпает, система управления питанием выключает ядра процессора, при этом передавая управление секретной зоне, оставляя ровно столько энергии, сколько ей нужно для работы. А дальше по тому же маршруту, паразитируя на соединениях главной ОС, то есть не вызывая никакого подозрения, запрашиваемые сведения отсылаются по нужному адресу.

— Если эта технология так классно работает, то может быть именно так ею и пользуются создатели ARM-чипа, — предположил Андрей Волков. — Хотя утверждать мы этого не можем. И всё же ясно: для того чтобы обеспечить госбезопасность, такие чипы использовать нельзя. То есть, получается, что вторая — секретная — операционная система, которая обитает в темной зоне, крутится на тех же самых ядрах, что и главная, но при этом совершенно недоступна для понимания.

**Раскопки & закладки**

Чтобы подробно проанализировать возможности одного ядра, которое является высокотехнологическим устройством, нужны усилия целого научного института, отметили специалисты компании. Это работа уровня «белых хакеров», которые ищут уязвимости нулевого дня. И главное, речь в данном случае идет о самом изученном устройстве — ARM-чипе, который тестируется и применяется по всему миру. Тем не менее его сложность такова, что до сих пор разобраться в нем на 100% не получается. Всегда остается вероятность не обнаруженных возможностей — преднамеренных закладок.

Ведущий эксперт компании «Инфовотч» Андрей Юршев рассказал «Известиям» о том, что центральные процессоры (ЦП) давно перестали быть набором аппаратных элементов.

— Теперь они включают в свой состав микропрограммы, обеспечивающие выполнение «сложных» команд. Соответственно, для хранения таких микропрограмм в ЦП выделяются отдельные области энергонезависимой памяти. Наличие такой памяти в ЦП, особенно с ростом их сложности и производительности, создает вероятность включения в состав ЦП подобных недекларированных возможностей. Так что технически это вполне реально. Возможно, этим воспользовались и другие производители чипов, — отметил эксперт.Фото: ТАСС/Донат Сорокин

По мнению директора департамента информационных технологий ФГБУ «НИЦ «Институт имени Н.Е.Жуковского» Георгия Петросюка, желание разработчиков ARM-процессоров или стоящих за ними спецслужб тайно контролировать или даже влиять на критические и стратегические сферы деятельности и пользователей «умных» устройств похоже на проведение активных разведывательных мероприятий.

— Разработчики ARM-процессоров имеют доступ к любой нужной им информации, они могут также с их помощью проводить какие-либо деструктивные действия. В этой связи видится крайне необходимым проведение на постоянной основе анализа всей используемой в нашей стране вычислительной техники иностранного производства на наличие подобных аппаратных и программных «закладок» и осуществление перехода на использование отечественных разработок как минимум в стратегических областях и в критической информационной инфраструктуре РФ, — подчеркнул Георгий Петросюк.

Правильно было бы, по мнению специалистов, постепенно перейти на российское железо.

# Эксперт CBS: распознавание лиц — компромисс между безопасностью и частной жизнью возможен

**Сегодня в США конгрессмены и активисты обеспокоены тем, что органы правопорядка могут начать злоупотреблять получающей всё большее распространение технологией распознавания лиц. По мнению эксперта CBS News Адам-Скотта Уондта, с усовершенствованием систем искусственного интеллекта и разработкой чётких инструкций применения технологий противостоящие стороны могут прийти к компромиссу.**

На сегодняшнем слушании члены палаты представителей опрашивают сотрудников Министерства безопасности на тему использования ведомством технологий распознавания лиц. Как стало известно из недавнего доклада, иммиграционная и таможенная полиция США, а также другие государственные службы штудируют национальную базу водительских удостоверений на предмет совпадений по технологии распознавания лиц, чтобы отслеживать нелегальных иммигрантов. Некоторые конгрессмены считают, что использование подобных технологий нарушает права граждан. Однако представители госучреждений настаивают, что преимущества применения этих технологий перевешивают сомнения относительно моральной стороны вопроса.

**ДЖОН ВАГНЕР, заместитель помощника комиссара в оперативном отделении погранично-таможенной службы США:** *Эта технология даёт нам возможность в течение 2—3 секунд установить биографические данные человека, что также устраняет необходимость физически проверять его удостоверение личности. Это позволяет нам без лишнего риска определить, является ли тот, кто сейчас перед нами находится, тем же человеком, в отношении которого мы у себя провели проверки безопасности, Администрация транспортной безопасности провела свои проверки по международным рейсам.*

**ОСТИН ГУЛД, помощник руководителя по вопросам оценки потребностей и возможностей Управления транспортной безопасности:** *Мы посчитали, сколько людей отказались предоставить свои данные для биометрической идентификации на наших контрольно-пропускных пунктах — меньше одного процента. Сложилось впечатление, что людям весь процесс нравится, пассажиры очень быстро продвигаются через идентификационные пункты. Но, что самое важное здесь, мы занимаемся усовершенствованием процесса проверки личности с помощью усиления мер безопасности.*

У меня в гостях Адам-Скотт Уондт, специалист по вопросам государственной политики, доцент и технолог Колледжа уголовного правосудия имени Джона Джея. Адам, спасибо, что пришли к нам на передачу.

**АДАМ-СКОТТ УОНДТ, специалист по государственной политике, доцент и технолог Колледжа уголовного правосудия имени Джона Джея:** *С удовольствием. Спасибо вам.*

Мы говорим о технологиях распознавания лиц, и, вы сами знаете, они представляют великое множество преимуществ,  в особенности для правоохранительных органов. Но перевешивают ли эти преимущества определённые недостатки, которые выделяют некоторые люди? Я имею в виду относительно вмешательства в личное пространство.

**АДАМ-СКОТТ УОНДТ:** *На мой взгляд, у этого вопроса есть две стороны. С одной, технология распознавания лиц — невероятно могущественный инструмент, который может помочь обеспечивать нашу безопасность, в особенности во время каких-нибудь масштабных мероприятий вроде спортивных состязаний или, скажем, на таможенных КПП. Эта технология может очень быстро просматривать человеческие лица и идентифицировать интересующих субъектов. Я считаю, это всё преимущества.*

*Тем не менее конгрессмены и некоторые эксперты по внедрению технологий в разных уголках страны выражают опасения, что такими технологиями, если они станут широко распространёнными, могут начать злоупотреблять. Зачастую вы понятия не имеете, где и когда используются такие механизмы, не знаете, за какими именно представителями населения они следят. И законодатели, и некоторые активисты беспокоятся, что эти технологии применяются для поиска незарегистрированных мигрантов и прочих без их ведома.*

Если мы говорим о незарегистрированных иммигрантах, относительно чего существуют наибольшие опасения?

**АДАМ-СКОТТ УОНДТ:** *Мне кажется, главным образом опасения касаются того факта, что мы не знаем, сколько хранятся все эти записи. Среди прочего люди всерьёз опасаются, что с течением времени власти наберут целую базу данных о гражданах страны и тех, кто ими не является, их местонахождениях, местах, куда они ездят. И очень скоро власти смогут просто прийти и задержать необходимых им людей, поскольку они будут знать, где те находятся.*

*Мы не знаем, где хранятся все эти записи, не знаем, насколько они точны. Ведь технологиям распознавания лиц свойственна некоторая изначально заложенная предвзятость…*

Верно.

**АДАМ-СКОТТ УОНДТ:** *И очень часто эта предвзятость выражается по отношению к меньшинствам.*

И к женщинам тоже, не так ли?

**АДАМ-СКОТТ УОНДТ:** *Определённо. Как мы видели, в процессе обучения технологии распознавания лиц участвовало множество белых мужчин, так что часто, когда система смотрит на кого-то, кто не является белым мужчиной, она выдаёт неверные идентификации. А это уже может привести к немалым неудобствам для кого-нибудь, в особенности когда его приедут задерживать органы правопорядка.*

Если уж мы заговорили об этой проблеме искусственного интеллекта, когда белых мужчин опознают правильно, а женщин и представителей меньшинств — нет, работают ли специалисты над устранением этих сбоев, главным образом в сфере применения искусственного интеллекта?

**АДАМ-СКОТТ УОНДТ:** *Обязательно. Этика искусственного интеллекта — одна из самых горячо обсуждаемых тем в сфере технологий в наши дни. И поиск способов успешного обучения искусственного интеллекта и путей сделать эти технологии безопасными является приоритетным направлением работы не только для большинства IT-компаний, но и для конгресса. Они там постоянно обсуждают эти темы. Думаю, по прошествии времени неполадки такого рода сведутся к минимуму.*

Некоторые защитники права на частную жизнь настаивают, что подобные технологии нужно запретить и точка. Мы не должны их использовать. Как вы считаете, может ли быть какой-то компромисс в потенциальном законодательстве, чтобы обе стороны были довольны?

**АДАМ-СКОТТ УОНДТ:***Думаю, что может. По-моему, полный запрет — это просто смешно, это слишком. На мой взгляд, власти и правоохранительные органы должны использовать подобные технологии только в строго определённых случаях, с целью обеспечения нашей безопасности. Изучая инструкции, в которых зафиксированы текущие случаи применения этих технологий и сроки, на протяжении которых следует хранить записанные данные, совершенствуя сами системы искусственного интеллекта, когда-нибудь мы найдём компромиссный вариант, при котором технологии распознавания лиц помогают обеспечивать нашу безопасность, но при этом не нарушают наши права.*

# ФСБ направила в «Яндекс» требование предоставить ключи

Несколько месяцев назад ФСБ направила в «Яндекс» требование предоставить ключи для дешифровки данных пользователей сервисов «Яндекс.Почта» и «Яндекс.Диск», рассказали РБК источник на ИТ-рынке и собеседник, близкий к «Яндексу». Оба собеседника РБК утверждают, что за прошедшее время «Яндекс» так и не предоставил в спецслужбу ключи, хотя по закону на это отводится не более десяти дней. Ранее из-за отказа поделиться ключами в России по решению суда был заблокирован мессенджер Telegram.  
  
Почему «Яндекс» не готов передавать ключи и чем это обернется для компании, разбирался РБК.  
  
Общество  
ЕСПЧ принял жалобу Telegram на штраф за отказ дать ФСБ ключи шифрования  
Почему ФСБ потребовала от «Яндекса» ключи  
  
«Яндекс.Почта» и «Яндекс.Диск» находятся в реестре организаторов распространения информации (ОРИ), то есть интернет-площадок, на которых пользователи могут обмениваться сообщениями. Согласно так называемому закону Яровой, с 20 июля 2016 года Центр оперативно-технических мероприятий ФСБ может потребовать от любого сервиса из реестра ОРИ передать ему «информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей сети интернет».  
  
В ФСБ не ответили на запрос РБК. В случае с Telegram, который был заблокирован в апреле 2018-го, правоохранительные органы хотели получить ключи для дешифровки пользователей, которые подозревались в организации терактов в метро Санкт-Петербурга. В свою очередь, основатель Telegram Павел Дуров отказался передавать информацию, мотивируя это защитой частной жизни и политикой конфиденциальности.  
  
Что ответил «Яндекс»  
  
Представитель пресс-службы «Яндекса» сообщил РБК, что компания «работает в полном соответствии с действующим законодательством». Он отказался отвечать на вопросы о том, действительно ли «Яндекс» получил требование от ФСБ предоставить ключи шифрования и не передал их.  
  
По словам источника РБК на ИТ-рынке, в «Яндексе» считают, что ФСБ слишком широко трактует норму «закона Яровой». «Спецслужба требует от компании предоставить сессионные ключи, которые, по сути, дают доступ не только, например, к сообщениям в почте, но и позволяют анализировать весь трафик от пользователей к находящимся в реестре ОРИ сервисам «Яндекса». Не говоря уже о том, что дешифровка всего трафика в рамках пользовательской сессии несет значительные риски в плане безопасности», — говорит он. Информацию про то, что ФСБ требует от компании именно сессионные ключи, подтвердил и второй собеседник РБК, близкий к интернет-холдингу.  
  
Сессионный ключ — это ключ шифрования, который используется только для одного соединения между пользователем и сервером, то есть одной сессии, пояснил бывший разработчик The Tor Project Леонид Евдокимов. «В случае с «Яндекс.Почта» он вырабатывается, когда пользователь только заходит на страницу mail.yandex.ru, а прекращает свое действие в зависимости от настроек через какое-то время, после того как пользователь либо закроет вкладку «Яндекс.Почта», либо полностью закроет браузер, либо выключит компьютер», — говорит он. Таким ключом шифруются не только сообщения пользователя, но и все метаданные (когда, кто, с какого IP-адреса заходил в аккаунт и т.д.), а также логин и пароль, которые пользователь отправляет на серверы «Яндекса» в процессе авторизации. «Поэтому передача сессионного ключа какого-либо пользователя спецслужбам может позволить им завладеть логином и паролем от почтового ящика этого пользователя», — утверждает Евдокимов. Он согласен с тезисом собеседника РБК о возможном снижении уровня безопасности в случае дешифровки пользовательского трафика. «Сама идея сессионного ключа состоит в том, что он не сохраняется. Тем самым обеспечивается безопасность передачи данных, так как в случае их перехвата злоумышленник не сможет их расшифровать. В этом смысле хранение и передача сессионных ключей создают определенные риски», — отметил он.  
  
  
Фото: Сергей Коньков / ТАСС  
Консультант по информационной безопасности Cisco Systems Алексей Лукацкий подтверждает, что «сессионный ключ в любом случае шифрует логин и пароль, которые пользователь передает на сервер в процессе авторизации, так что передача такого ключа ФСБ может дать доступ к аутентификационным данным пользователя». Он указал, что «Яндекс» использует систему Single Sign-On, при которой, авторизовавшись в «Яндекс.Почта», можно без повторной аутентификации перейти в «Яндекс.Музыка», «Яндекс.Диск» и любой другой сервис. «Ключ шифрования при переходе в разные сервисы должен быть свой, но если это не так, то это архитектурная проблема, которая может открыть доступ к данным в разных сервисах «Яндекса». Тогда передавать сессионный ключ, конечно, небезопасно», — рассуждает Лукацкий.  
  
Леонид Евдокимов считает, что сессионные ключи позволяют получить не только доступ к данным, но и анализировать само поведение пользователей. Например, в «Яндекс.Диск», завладев сессионным ключом, можно смотреть, кто и какие данные скачивал, отметил он.  
  
По словам собеседника РБК, близкого к «Яндексу», компания обеспокоена тем, что сотрудничество с ФСБ может привести к оттоку пользователей, потере доли на рынке и, как следствие, существенным денежным потерям. «Иностранные компании, например Google, ФСБ не принуждает к такому сотрудничеству, поэтому «Яндекс» тут видит угрозу своему конкурентному положению», — говорит он.  
  
Чем грозит «Яндексу» отказ  
  
Непредоставление ключей шифрования в установленный срок является нарушением действующего Кодекса об административных правонарушениях. По закону ФСБ должна составить протокол об административном правонарушении и, если суд признает «Яндекс» виновным по статье 13.31 КоАП, может назначить компании штраф в размере до 1 млн руб., пояснил партнер Центра цифровых прав Саркис Дарбинян.  
  
По его словам, если компания и после этого не предоставит ключи шифрования, Роскомнадзор вынесет ей предписание об устранении нарушения, на исполнение которого дается не менее 15 дней. «В случае неисполнения предписания Роскомнадзор, в теории, может обратиться в суд с требованием заблокировать на территории России сервисы, ключи шифрования от которых отказываются предоставить. Во всяком случае такая процедура была использована в истории с блокировкой Telegram, в законе же прямо не указаны полномочия Роскомнадзора и ФСБ в данной ситуации», — говорит Дарбинян.  
  
Однако он считает маловероятным развитием событий блокировку сервисов «Яндекса» на территории России, как это было с Telegram. «Скорее, они будут долго торговаться и в итоге придут к какому-то компромиссу. У государства здесь есть сильный рычаг. Если «Яндекс» совсем не будет идти на диалог, допускаю, что в целях устрашения они могут ограничить доступ к его сервисам на день-два — и это сразу же приведет к большим убыткам для компании. Но это будет просто кошмар, если спецслужбы начнут блокировать сервисы крупнейшей российской интернет-компании на постоянной основе», — говорит Саркис Дарбинян.  
  
По данным SimilarWeb, число посещений «Яндекс.Почта» в апреле 2019 года составило 432 млн, а «Яндекс.Диск» — 27,32 млн.  
  
По закону «Об оперативно-розыскной деятельности» ФСБ уже на протяжении многих лет может получать доступ к телефонным переговорам граждан или запрашивать у интернет-компаний их переписку, но для этого ей необходимо получать постановление суда. По данным Судебного департамента при Верховном суде России, за 2018 год российские суды удовлетворили 828,5 тыс. ходатайств правоохранительных органов об ограничении конституционных прав граждан на тайну переписки и контроле их телефонных переговоров. Еще 6,6 тыс. таких ходатайств было отклонено.  
  
«Получение ключей шифрования и последующего доступа к переписке для ФСБ — более удобная схема, чем идти в суд, просить постановление и лишь затем запрашивать переписку, как это работало ранее. Не вижу никаких логичных и понятных причин, кроме возможного сокращения скорости информационного обмена (то есть отсутствия необходимости ждать постановление суда) и потенциального перехвата сессий для выемки данных и других действий в обход стандартных процедур», — считает Леонид Евдокимов.  
  
У кого еще могут потребовать ключи шифрования  
  
В реестр ОРИ на данный момент включено более 170 сервисов, среди которых Tinder, «ВКонтакте», «Одноклассники», BlaBlaCar, Badoo, Vimeo и др. У любого из этих сервисов ФСБ в какой-то момент может потребовать предоставить ключи для дешифровки переписки пользователей.  
  
Собеседников РБК тревожит включение в реестр ОРИ в январе 2019 года сервиса «Сбербанк Онлайн» — это система дистанционного банковского обслуживания для клиентов Сбербанка.  
  
Включение «Сбербанк Онлайн» в реестр ОРИ выглядит довольно странно, хотя и понятно с точки зрения законодательства, поясняет Алексей Лукацкий. Многое зависит от того, как разделены в этом сервисе функции защиты финансовых транзакций и встроенного мессенджера, из-за которого, собственно, сервис и попал в реестр Роскомнадзора. «Если они шифруются разными ключами, то тогда все более-менее в порядке. Если же нет, то передача ключей шифрования от такого «чувствительного» сервиса — законодательно понятное, но с точки зрения безопасности очень сомнительное решение», — отмечает собеседник РБК. Представитель пресс-службы Сбербанка отказался от комментариев.  
  
Подробнее на РБК:  
https://www.rbc.ru/technology\_and\_media/04/06/2019/5cf50e139a79474f8ab5494b

# «Директора часто пренебрегают правилами защиты». Как избежать проблем с утечками данных

29.04.2019

«Информация на рабочем компьютере — собственность компании, а не трудового коллектива. Это кажется очевидным директору, но не для сотрудников». Как избежать передачи важных данных в чужие руки?

**Директор по безопасности компании «[СёрчИнформ](https://www.dk.ru/wiki/syorchinform" \l "binding" \o "СёрчИнформ)» Иван Бируля:**

— В Интернете [**всплыла**](https://ekb.dk.ru/news/v-set-utekli-dannye-120-tys-figurantov-chernogo-spiska-tsb-kakie-problemy-im-grozyat-237120247#binding) база данных с информацией о 120 тысячах клиентов из «черного списка» [Центробанка](https://www.dk.ru/wiki/centralnyy-bank-rossiyskoy-federacii#binding) — от физлиц до компаний. Критично здесь не количество строк в базе — в российской истории были утечки гораздо глобальнее, — а полнота и качество информации, а также ее причины.

Доступ к этой базе строго авторизированный, а сами данные передавались по защищенным,каналам, поэтому нужно предполагать инсайдерскую утечку. Но кто ее допустил, сказать невозможно. Доступ к базе был у сотрудников многих российских банков, Центробанка и [Росфинмониторинга](https://www.dk.ru/wiki/rosfinmonitoring#binding) — у всех участников обмена данными.

Нельзя сказать, что банки и ЦБ защищены плохо. В России действуют постановления, распоряжения и национальные стандарты по информационной безопасности для финансовой сферы. Основные — ГОСТ Р 57580.1-2017 и СТО БР ИББС 1.3-2016. Документы предписывают банкам обязательно использовать программные средства защиты от утечек информации с конкретными функциональными возможностями.

В частности, ГОСТ предписывает обеспечивать автоматизированный контентный анализ передаваемой информации по сетевым каналам, вести архив коммуникаций, ограничивать хранение отдельных типов данных, предотвращать передачу данных на устройства хранения и т.д.

**Почему при таком жестком регулировании банки допускают утечки данных?  Все просто — человеческий фактор.**

Отраслевые стандарты — это рамки, которые добропорядочным банкам дают в руки инструментарий, практики, кейсы и советы. Но всегда существует вероятность халатного выполнения требований. Формально риски будут закрыты, по факту — нет. Только в Сбербанке за прошлый год произошло три громких инцидента, информация о которых попала в сеть. А ведь в крупнейшем российском банке стоит система защиты от утечек информации и штат службы безопасности один из самых укомплектованных в отрасли.

Если такова ситуация в банках, что происходит в менее защищенных бизнесах? Удовлетворительной можно назвать ситуацию с безопасностью в компаниях со штатом от 500 сотрудников. Тут и специально выделенные люди есть, и программное обеспечение. При этом в России больше 20 тысяч компаний со штатом до 250 человек, и тут ситуация совсем другая. А ведь вопросы кибербезопасности в этих компаниях стоят не менее остро. В лучшем случае их решает IТ-специалист (вариант совсем не идеальный, но на безрыбье не самый худший). Но часто и выделенного человека нет. Пока практика аутсорсинга только приобретает доверие, руководству приходится справляться имеющимися ресурсами.

Чтобы эта работа имела результат, нужна системность. Что можно сделать в формате «дешево и сердито»? Ввести режим коммерческой тайны в компании.

**Придется говорить с работниками и доносить, что информация на рабочем компьютере — собственность компании, а не трудового коллектива. Это кажется очевидным директору, но для сотрудников это совсем не так.**

Но одними беседами не обойтись. Правила, как и в каких целях могут использоваться компьютеры, интеллектуальная собственность и другие ресурсы организации должны быть прописаны в трудовом контракте, внутренних инструкциях. Сам факт принятия договоренностей с работодателем о том, что есть регламент и ответственность за его нарушение — большой шаг к воспитанию новой трудовой дисциплины. Одно дело уповать на сознательность, другое — доносить под подпись, что утеря грифованных документов карается штрафом в размере 1,5 млн рублей или даже риском получить 7 лет тюрьмы за кражу данных.

Следующий шаг — повышение киберграмотности, и это куда более сложное дело. По статистике Сбербанка, треть продвинутых пользователей открывают фишинговые письма. Получается, что на уловки мошенников попадаются даже те, кто в курсе угрозы. Происходит это не только по невнимательности. Атаки мошенников становятся почти совершенными: фишинговые письма и сайты похожи на настоящие как братья-близнецы.

Беседы и тренинги сами по себе рабочий инструмент, но как только у компании растет размах деятельности, положиться только на них уже нельзя. На такие случаи существуют технические «заборы», которые уберегут и от случайного инсайдерства, и от злонамеренного. На первых порах бизнесу оказывается достаточно антивирусных программ, средств администрирования Windows, программ контроля продуктивности сотрудников. Дальше организации приходят к пониманию необходимости использования Firewall, Proxy, IDS/IPS, DLP- и SIEM-систем. По моим наблюдениям планка снижается. Если раньше профессиональные инструменты были необходимостью только крупному бизнесу, сейчас их приобретают собственники компаний совершенно разного калибра.

**Все эти инструменты работают тогда, когда и сам руководитель придерживается правил информационной безопасности. Парадокс заключается в том, что директора, которые понимают важность защиты информации, часто пренебрегают правилами.**

В сентябре [PwC](https://ekb.dk.ru/wiki/pwc#binding) рассказала о результатах опроса руководителей российских компаний, и 81% членов советов директоров хранят на своих телефонах закрытую и дорогостоящую информацию.

[**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) |  |