

Skype врага

Microsoft готова сдать коды Skype российским спецслужбам. Skype-технологии закономерно лишили людей личной жизни, но оказались плохо защищены от утечек в спецслужбы и криминальные структуры.

В России утечки персональных данных стали еще и элементом политической борьбы. На Западе ограничить «сливы» может угроза публичного скандала и миллионных штрафов, в России таких инструментов нет.

Купив Skype, корпорация Microsoft может передать российским спецслужбам исходные коды сервиса.

«Я бы хотел это сделать», — заявил президент «Microsoft-Россия» Николай Прянишников, которого в среду процитировал «Интерфакс». «Общий подход Microsoft в России — сотрудничество и партнерство с государством», — уточнил он.

Ранее Microsoft открыла российским спецслужбам исходные коды собственных программных продуктов. «Мы хотим развивать нашу совместную с ФСБ лабораторию», — аргументирует Прянишников.

Если исходные коды Skype попадут в ФСБ, это станет завершением многолетнего противостояния российских спецслужб с администрацией сервиса. Победителем вышла ФСБ. Исходники позволят специалистам ФСБ провести аудит программы на предмет обнаружения «дыр», в том числе для прослушки.

Государство давно требовало открыть исходники Skype. Но американская штаб-квартира Skype до продажи компании Microsoft всегда сопротивлялась этим попыткам.

Все течет

«Моя почта, хотя она находится на Gmail, утекает. Думаю, это происходит не без участия наших компетентных органов», — сетует депутат, член комитета Госдумы по связи и информации Илья Пономарев. Он говорит, что видел распечатки писем из своей электронной почты «в руках посторонних».

«Вопрос не в том, что ФСБ запрашивает мои и других пользователей данные у «Яндекса», тем более что скрывать тут нечего. Вопрос в том, каким образом от ФСБ эти данные попадают в третьи руки», — говорит и юрист Алексей Навальный, столкнувшийся с похожей проблемой.

Он курирует проект «Роспил», фиксирующий факты коррупции. «Роспил» существует на перечисления доброжелателей. Данные о тех, кто перечислял деньги на проект, с помощью системы «Яндекс.Деньги» запросила Федеральная служба безопасности, а потом на их телефоны стали поступать звонки. В организации обзвона Навальный подозревает связанное с властями политическое движение «Наши».

Без основы интернет-бизнеса — адресности — компании не смогут развиваться. Персонализированный интернет растет быстрее традиционной экономики, которая, в свою очередь, тоже ускоряется благодаря интернету. «Человек сам соглашается предоставить нам эту информацию, а мы используем ее только для того, чтобы давать наиболее релевантную информацию по пробкам, при поиске, а также для таргетирования рекламы», — говорит Владимир Долгов, гендиректор Google Russia.

Но цена быстрого роста начинает вызывать вопросы: принцип неприкосновенности личной жизни не всегда срабатывает в экономике нового формата.

В апреле американские ученые Аласдэр Аллан и Питер Уорден обнаружили, что гаджеты iPhone4 и iPad от корпорации Apple незаметно для пользователей ведут запись координат устройства в файл consolidated.db. Координаты берутся с открытых точек доступа WiFi и вышек сотовой связи, записываются и данные GPS. Местоположение гаджета определяется с точностью от 20 до 6 метров.

Файл с информацией не зашифрован, на нем записаны данные за несколько месяцев. Исследователи возмутились: «Записывая ваши передвижения без спроса, Apple дает возможность каждому — как ревнивой жене, так и частному сыщику — получить детальную информацию о ваших передвижениях».

Apple могла собирать историю перемещений около 20 млн планшетов iPad и нескольких миллионов iPhone 4, оснащенных ОС iOS4.

Apple утверждала, что запись информации велась в результате системного сбоя, и выпустила обновление программы: если его установить, геотаргетированные данные сохраняются в iPhone не больше недели, а резервное копирование в компьютер не производится.

Вскоре выяснилось, что интернет-корпорация Google тоже собирает данные с WiFi и GPS на смартфонах, оснащенных операционной системой Android.

Глав крупнейших американских компаний сразу вызвали на доклад в конгресс, желая знать, почему за страной следят.

«Да, мы знаем, где находится человек, — говорит Долгов, — потому что он посылает сигналы и принимает информацию со спутника, для того чтобы найти дорогу».

Google никогда не передает эти данные третьим компаниям, уверяет он.

В Apple говорят, что передача информации о местонахождении предоставляется третьей стороне, если пользователь согласился на это.

Но, как правило, люди не задумываются над тем, кому они открывают доступ к данным, признают представители корпораций и владельцы приложений.

«Все, что интересует любого пользователя, — это где находится кнопка «я согласен», — признает Долгов, имея в виду то, что потребители не вчитываются в детали пользовательского соглашения.

Машины для шпионажа

Социальная сеть Facebook — это тоже «машина для шпионажа», сказал в разгар скандала вокруг Apple и Google основатель самого известного хакерского проекта современности Джулиан Ассанж. Создатель Wikileaks как в воду глядел: через несколько дней стало известно о возможной утечке личных данных пользователей соцсети, аудитория которой превышает 600 млн человек во всем мире.

Сотрудники антивирусной компании Symantec Нишант Доши и Кандид Вест выяснили: в течение нескольких лет посторонние имели возможность не только просматривать, но и управлять данными профилей пользователей сети.

Доступ к личным данным открылся через тэг IFRAME, с помощью которого загружаются приложения в Facebook. При установке приложений разработчики получали аутентификационные токены (ключи), которые содержались в ответной ссылке от Facebook. К рекламодателям утекли миллионы аутентификационных ключей к профилям пользователей социальной сети.

Используя ключи, через приложения Facebook рекламодатели могли получить доступ к профилю пользователя, от его имени читать «стену», переписку в чате, профили «друзей», оставлять сообщения на «стене» профиля пользователя и его «друзей», приглашать на мероприятия участников Facebook от имени пользователя.

Возможно, утечка затронула и российских пользователей сети. «У нас нет информации относительно географической разбивки пользователей, которые пользовались приложениями, работающими с устаревшими параметрами, в рамках которых Facebook и возвращал токен в ссылке», — поясняет глава российского офиса социальной сети Екатерина Скоробогатова.

Разработчики игровых приложений для крупнейших российских социальных сетей «Одноклассники», «В Контакте» и «Мой мир» тоже получают доступ к «друзьям» пользователя, его фотографиям, аудио и видеозаписям, а также возможность применить «расширенные методы работы с сообщениями и со «стеной».

«Само по себе приложение не может получить никаких данных, пока ты не разрешишь, — говорит Евгений Гацалов, гейм-директор компании Addicted. — Но фишка в том, что приложения при установке просят те или иные доступы (обычно к списку друзей, к возможности записи на стену). И если ты не дашь приложению доступ, оно не установится».

Серьезные компании не заинтересованы в манипулировании персональными данными пользователей, уверяет Гацалов.

Пресс-служба «ВКонтакте» не ответила на запрос «Газеты.Ru».

Соцсети и телекоммуникационные компании знают, что люди покупают в магазинах. С момента запуска в Facebook приложение торговой сети «М.Видео», с помощью которого можно выбрать товары, установили около 2000 человек. Компания использует стандартную систему аутентификации Facebook, но при этом персональные данные пользователей не хранятся и нигде не используются, утверждает Антон Пантелеев, представитель розничной сети «М.Видео».

Но электронные магазины могут (теоретически) сохранять записи обо всем, что вы купили, пишет в книге «Секреты и ложь. Безопасность данных в цифровом мире» эксперт Брюс Шнайер.

Приложение интернет-магазина KiriVIP работает в социальной сети «Одноклассники»: при покупках пользователи вводят свое имя, адрес, телефоны, но о том, имеет ли к ним доступ администрация социальной сети, представитель KiriVIP Джулианна Каспранова отвечать не стала.

Геотаргетированную информацию, которую получают со смартфонов Apple, Google и рекламодатели в интернете, нельзя назвать полностью анонимной. Люди сутками держат смартфоны при себе, поэтому любое раскрытие геолокационных данных становится серьезным вторжением в частную жизнь. При утечках из смартфонов министров и членов парламента появляется угроза их физической безопасности, объясняет Ульф Бергстрем из European Network and Information Security Agency (ENISA).

Технологии на службе

Источников любой утечки персональных данных только два – компания, собирающая информацию, и спецслужбы, с которыми компания обязана ею делиться. В России порядок работы операторов с ФСБ описан в законах «О связи» и «Об оперативно-розыскной деятельности».

Технические устройства проходят обязательную нотификацию в ФСБ. «Нотификация – это «зеленый коридор», когда компания говорит, что в устройстве используется устройство шифрования только для общего пользования, и мы им верим», – объясняет собеседник в спецслужбе.

Кроме того, сотовые операторы и интернет-провайдеры по закону должны собирать персональные данные – имена, номера и серии паспортов, местонахождение и т. д. – для органов госбезопасности и хранить их в течение трёх лет. Сотрудничество со спецслужбами в рамках СОПМ (Система оперативно-розыскных мероприятий) – одно из условий выдачи лицензии на оказание услуг связи.

Правозащитники всегда сомневались, что СОПМ законодательно защищена от злоупотреблений. Прослушку можно начинать по решению суда, но предъявлять решение оператору связи сотрудники ФСБ не должны. В противном случае их обвинят в разглашении тайны следствия.

По аналогичному принципу работают телекоммуникационные и интернет-компании во всем мире. Каналы связи используются в оперативно-розыскных мероприятиях, данные пользователей выдаются по решению суда.

Но у западных компаний есть опыт противостояния попыткам спецслужб получить данные о клиентах, выходящие за рамки расследуемых уголовных дел.

Два года назад минюст США потребовал у поисковых систем Google, Yahoo! и Microsoft IP-адреса людей, которые делали запросы по определенному набору тем. Google счел это требование неправомерным. Министерство юстиции подало на Google в суд. Решение судьи было такое: отдать выборочно 10 тысяч IP-адресов без последних трех цифр.

Но обычно компании предпочитают не провоцировать конфликты с властями. Ранее в базе данных Cryptome были размещены внутренние инструкции крупнейших интернет-корпораций, определяющие порядок взаимодействия с правоохранительными органами. Спецслужбам по решению суда открыты персональные данные абонентов сотовой связи и зарегистрированных пользователей интернет-ресурсов — имена, телефоны, адреса электронной почты, номера кредиток и т. д., в том числе тех, кто просто оставляет комментарии. По отдельному запросу интернет-сервисы могут устанавливать постоянное наблюдение за пользователем.

«Сормируются» все каналы связи, рассказывает отраслевой консультант. ФСБ до сих пор не могла получить возможность оперативного доступа только к Skype, Gmail и Hotmail – управляющие сервисами Microsoft и Google рассматривают обращения ФСБ в американских штаб-квартирах, задерживая процесс.

Сотрудник управления К (отвечает за информационную безопасность) МВД это подтверждает и признается, что вел конфиденциальные разговоры только по Skype.

Российский офис Google не отвечает за поддержку Gmail, рассказывает Долгов: «Сервис является собственностью американской компании Google Inc. Есть совершенно четкие правила, каким образом какие-то государственные органы могут получать доступ к той или иной конфиденциальной информации: это регулируется американским законодательством».

Но и Skype в итоге оказался не полностью защищен от «вскрытия». В мае Wall Street Journal сообщила сенсацию: у египетских спецслужб, разгонявших недавно антипрезидентские выступления, обнаружили записи разговоров лидеров оппозиции, которые велись по IP-сервису. Слушать Skype можно, но пока только путем адресного заражения конкретного компьютера, пришли к выводу эксперты газеты. Если исходные коды будут открыты, процесс прослушки будет облегчен.

Дыры в системе

Проблема утечки данных в России приобретает специфический характер. «В условиях бесконтрольности ключевых госинститутов и невозможности в результате общественного недовольства заставить силовые органы исполнять законы, утечки персональных данных становятся опасным оружием, которое может применяться уже не просто против обычных граждан, но и против оппозиционных активистов», – считает Пономарев. В условиях отсутствия независимой судебной системы привлечь силовиков к ответственности за подобные действия практически невозможно, добавил он.

Утечки в таких условиях не только возможны, но могут быть вызваны «политической целесообразностью».

СОРМ не защищена от утечек, подтверждает источник в спецслужбах, добавляя, что «сливы» возможны «скорее теоретически и чреваты серьезными проблемами для источника». В начале мая интернет-корпорация «Яндекс» сообщила, что передала в ФСБ данные о людях, финансировавших «Роспил». «Яндекс» передал информацию о проводках по запросу службы в рамках «стандартной процедуры» (основания запроса не были названы). Но потом финансовые доноры «Роспила» заявили, что им начали звонить противники Навального из политического движения «Наши» – интересовались перечислениями средств.

Источник в ФСБ признает, что данные могли утечь к «Нашим». «Подонки есть везде. Но у нас их процент ниже», – уверен он. «Наши» сами могли узнать о запросе со стороны спецслужбы, потом перечислить Навальному деньги, а затем намекнуть на утечку из ФСБ, – полагает сотрудник службы. – Скандал с акцентом на ФСБ мог испугать людей, которые хотели профинансировать проект Навального и придать «Нашим» имидж структуры, которая якобы способна влиять на всех».

Но ведомственная информация утекает регулярно. На рынках можно легко найти базы данных ГИБДД и коллекторских агентств, медицинских учреждений и Центробанка. Ведомственная съемка ГИБДД тоже утекала в интернет и тоже как орудие политической дискредитации.

На сервисе Youtube был размещен ролик «Орешкин, Яшин, Фишман – коррупционеры», в котором неустановленные лица показали, как журналист Михаил Фишман, политик-оппозиционер Илья Яшин и обозреватель «Новой газеты» Дмитрий Орешкин (все трое открыто критиковали то же движение «Наши») говорили о готовности дать взятку постовым инспекторам. В записях фигурировала оперативная съемка в салоне служебного автомобиля ГИБДД.

Сейчас в России ситуация с защитой коммерческих и ведомственных баз данных недалеко ушла от 1990-х, когда можно было на любом рынке купить практически любую базу на нескольких компакт-дисках, говорит аналитик компании SearchInform Роман Идов.

«Многие даже не поняли, что произошло»

Отделить неизбежное проникновение интернет-компаний в личную жизнь в условиях новой экономики от злоупотреблений и «сливов» могут средства массовой информации и суды, показала американская и европейская практика. Информация об утечках всплывала после журналистских расследований. Владелец гаджетов от Apple и Google уже обвинили корпорации во вторжении в частную жизнь и подали групповые иски.

В частности, от Google истцы требуют «за слежку» \$50 млн.

Евросоюз тоже отреагировал: организация, координирующая защиту персональных данных в интернете, готовит предложение о внесении локационных данных в перечень персональных данных наравне с именем, датой рождения и домашним адресом.

Но в России скандалы с утечками не вызвали публичного резонанса. «Многие даже не поняли, что произошло, поэтому и в Госдуме слушания не проводились», – отмечает депутат Ольга Носкова, которая входит в комитет Госдумы по связи и информации.

Автор: Владислав Новый, Петр Канаев © Газета.Ru ИНТЕРНЕТ И ИТ, РОССИЯ 👁 3242 09.06.2011, 21:02

URL: <https://babr24.com/?ADE=94091> Bytes: 15969 / 15934 [Версия для печати](#) [Скачать PDF](#)

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

newsbabr@gmail.com

Автор текста: **Владислав
Новый, Петр Канаев.**

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot

Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь

Телеграм: @bur24_link_bot

эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова

Телеграм: @irk24_link_bot

эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская

Телеграм: @kras24_link_bot

эл.почта: krsyar.babr@gmail.com

Новосибирск: Алина Обская

Телеграм: @nsk24_link_bot

эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин

Телеграм: @tomsk24_link_bot

эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"

Телеграм: @babrobot_bot

эл.почта: equatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)