

НБУ курс:

USD 41,12 ▼ -0,13 EUR 48,29 ▼ -0,09

Наличный курс:

USD 41,30 | 41,23 EUR 48,55 | 48,35

Топ налогоплательщиков 2025

Історії успіху з Ощадом

Лучшие работодатели 2025

Свое дело

Инвестиции в образование

Обучение для жизни



ЭКСКЛЮЗИВ IT и Телеком 04 сентября 2013

Стоит ли бояться слежки в интернете

Ведущий аналитик компании Searchinform Кикеня Максим рассказал Delo.UA о мировых практиках слежки за людьми



СПЕЦПРОЕКТ: Історії успіху з Ощадом

Ощадбанк розпочав спецпроект, що розповідає історії підприємців, яким вдалося досягти сталого розвитку навіть у найскладніші часи. В основі – досвід представників малого та середнього бізнесу, для яких банк став не лише фінансовим партнером, а й точкою опори для зростання.

[Дізнайтесь більше](#)

После утечки информации о специализированном шпионском софте АНБ (Агентства Национальной Безопасности США) наверное каждый из нас в какой-то мере задумался о том, может ли этот софт нанести нам ущерб. Глядя на то, с каким энтузиазмом мировые СМИ освещают подробности шпионажа американской разведки, казалось бы, не стоит даже упоминать, вокруг чего образовалась "трагедия" и почему полемика вокруг данной "шпиономании" продолжается и по сегодняшний день. Мы лишь вкратце резюмируем некоторые факты, чтобы можно было легко от них оттолкнуться и разобраться в том, действительно так страшен черт, как его описывают СМИ?

Поводом для размышления и в тоже время неожиданным "сюрпризом" для мировой общественности стала публикация засекреченной информации о шпионских программах PRISM и Xkeyscore британской газетой The Guardian. Шутки шутками, но Эдварду Сноудену действительно хочется сказать спасибо за проявленные смелость и мужество, потому что пойти на такой шаг способен не каждый, и прежде всего за ту обнародованную информацию, без которой не было бы таких массовых волнений.

Обнародованные данные о шпионском ПО гласят, что секретные службы США "без суда и следствия" могут получать доступ к любой переписке любого человека посредством своего шпионского софта. Теперь американские фильмы про шпионов не кажутся фантастикой.

Но если нам с вами не все равно, следят за нами или нет, то бабушке из соседнего подъезда скрывать нечего. Она "чиста". У нее нет электронного ящика, она предпочитает письма отправлять в бумажном конверте по почте. У нее нет аккаунта в социальных сетях, она социальна на лавочке возле дома в кругу таких же бабушек, как и она сама. У нее нет смартфона, которым сегодня можно изменить направление движения Земли вокруг своей оси. Проще говоря, ей программы PRISM, как коту сосиски. Аналогичным образом ощущать себя можем и мы, несмотря на то что у нас есть все то, чего у бабушки Клавды нет. Один из рядовых слушателей, дозвонившихся на радио, сказал: "А что если человек не моет деньги, не продает государственные секреты, не совершает ничего плохого. Да пусть хоть хором все следят, это не имеет никакого

значения... Не вижу проблемы. Мне кажется, что все это достаточно сильно раздуто. Там, где криминал, там по-любому это надо и это правильно".

Свою фантастическую способность следить за всем и вся программы PRISM и Xkeyscore получили благодаря сотрудничеству спецслужб с такими мировыми гигантами, как Microsoft, Google, Facebook, Youtube, Skype, Apple и другими. Причем все руководители корпораций утверждали, что о данных программах слышат в первый раз и никакого сотрудничества со спецслужбами не ведут. По словам Ларри Пейджа, разработчика и сооснователя поисковой системы "Google", компания Google удовлетворяет запросы спецслужб только в рамках закона и не участвует ни в каких правительственных программах. Практически аналогичное высказывание сделал Марк Цукерберг, руководитель компании Facebook Inc. на своей официальной странице в социальной сети.

Представители Microsoft также настояли на своей непричастности к шпионскому ПО и программам спецслужб США, заявив, что действуют только в рамках закона и предоставляют запросы и личную информацию по единичным аккаунтам и идентификаторам.

На фоне разоблачений весьма саркастично смотрятся высказывания от Google "Google заботится о безопасности данных наших пользователей" и от Microsoft "Ваша конфиденциальность — наша безопасность".

Теперь давайте обратим внимание на другие страны. В кругу разоблачений оказалась также британская программа "Tempora" посредством, которой Британский Центр правительственной связи (GCHQ), по данным The Guardian, подключался к трансатлантической оптико-волоконной связи и отслеживал все виды электронной коммуникации: телефонные разговоры, электронную почту, разговоры по Skype, сообщения в социальных сетях. Также GCHQ анализировал и сохранял личные данные пользователей интернета. На этот счет свое недовольство высказало правительство Германии, которое видимо и само подзабыло, что ведет наблюдение за телекоммуникационными процессами и прослушивает разговоры подозреваемых с помощью программ интернет-телефонии. В 2008 году Федеральный конституционный суд Германии позволил правоохранительным органам применять так называемый "бундестроянец" или Quellen-TKÜ, посредством которого и становится доступна возможность шпионажа. Программа устанавливала на зараженный компьютер дополнительные модули, которые открывали доступ к личным файлам. Также появилась информация, что и у Франции есть собственный аналог PRISM, но в отличии американской версии французская версия отличается большей скромностью — она может собирать лишь информацию о метаданных отправленных сообщений (то есть кто, откуда, кому и во сколько).

Позже стало известно, что электронные разведки всех вышеупомянутых стран в разной степени сотрудничают с АНБ, выполняя антитеррористическую международную миссию. Потенциально же с США сотрудничают еще как минимум 3 страны: Канада, Новая Зеландия и Австралия. Все эти страны являются членами альянса Five Eyes, созданного для сотрудничества в области разведки.

В России без шпионажа дело также не обошлось, однако, за своими гражданами там следят с помощью программ COPM и COPM-2. COPM разрабатывался для телефонной связи, а COPM-2 — для Интернета. COPM — Система Оперативно-Розыскных Мероприятий, представленная в виде комплекса оборудования и ПО. Она представляет отдельную отрасль, включающую научные исследовательские вопросы, производство и техническую поддержку оборудования, разработку программных продуктов и интерфейсов. Отрасль, которая распространяет свое влияние на все существующие сети связи, за исключением телеграфных каналов.

Шпионаж — явление не новое. Доносчики, информаторы, стукачи, "тайна полиция" существовали и ранее. Сегодня же шпионаж обрел электронный формат. Однако не стоит панически бояться слежки. На фоне всех разоблачений АНБ опубликовало отчет, где только 1,6 процента из 1826 петабайтов перехватывается каждый день по сети. Из этих данных только 0,025 процента отбираются для анализа. Даже если цифры в отчете занижены, все равно до абсолютной слежки спецслужбам еще далеко. Да, осуществлять слежку они могут, но если вы предоставляете какую-либо серьезную опасность, в противном случае вы мелкая "рыбешка". Кроме того, если желание скрыть информацию от сторонних глаз все же осталось, существуют технологии шифрования хранящихся и пересылаемых данных, о которых активно заговорили после разоблачения PRISM пользователи Интернета. Такие технологии как PGP, Tor, Bitmessage и другие окажут помощь в шифровании данных. При этом многие эксперты считают, что данных технологии являются реальной контрмерой

глобальной слежке. Но было бы эффективнее, чтобы ими начали пользоваться массово, вот тогда бы спецслужбам пришлось попотеть. Поэтому тем, кому есть что скрывать, "шифруемся", а все остальные — набираемся спокойствия и ждем новых разоблачений.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



Do Not Sell or Share My Personal Information