САХАРОВСКИЙ ЦЕНТР

Анонимность в Сети.

Как защитить себя от Большого Брата

Москва, 2014

Авторы: Андрей Солдатов, Ирина Бороган

Анонимность в Сети. Как защитить себя от Большого Брата.
Москва: Сахаровский центр, 2014. 32 с.

Сегодня во многих странах мира граждане каждый день сталкиваются с необходимостью защищать свою информацию. Перехваты электронной переписки и телефонных переговоров политиков, общественных деятелей, знаменитостей регулярно выкладываются в Сеть. Журналистам, которым всегда было необходимо сохранять анонимность источников, с развитием технологий стало еще сложнее обеспечивать конфиденциальность своих контактов. В этой брошюре вы найдете информацию о том, какие угрозы тайне частной жизни (privacy) несут современные электронные технологии и как защитить себя и свою технику?

Проект финансируется
Европейским Союзом.

Публикация подготовлена при поддержке Европейского Союза.
Содержание данной публикации является предметом ответственности Сахаровского центра и не отражает точку зрения Европейского Союза.

ОГЛАВЛЕНИЕ

Сегодня политические активисты, журналисты, правозащитники и просто активные граждане во многих странах мира каждый день сталкиваются с необходимостью защищать свою информацию от Большого Брата. Перехваты электронной переписки и телефонных переговоров оппозиционеров и гражданских активистов регулярно выкладываются в Сеть с целью повлиять на их позицию.

Журналистам, которым всегда было необходимо сохранять анонимность источников, с развитием технологий стало еще сложнее обеспечивать конфиденциальность своих контактов.

Последние два года, с момента принятия закона о черных списках сайтов, доступ к информации в России перестал быть свободным.

Многие интернет-ресурсы, включая независимые онлайн-СМИ и общественно-политические сайты, блокируются. За это время российские законодатели приняли несколько законов, ограничивающих право на свободный доступ к информации в Рунете.

Недавно были приняты законы, по которым персональные данные россиян должны храниться на территории страны, что принуждает глобальные компании, такие как Google и Facebook, перенести свои серверы в Россию. Это делает наши контакты в соцсетях еще более уязвимыми для перехвата информации.

Поскольку в России мы столкнулись с такими проблемами намного позже, чем активисты и правозащитники в других странах, то там за многие годы накопился серьезный опыт противостояния электронной слежке и сложилась вполне конкретная практика защиты частных коммуникаций, а также были разработаны эффективные инструменты доступа к блокируемой информации в Интернете.

Такие организации, как Privacy International и Electronic Frontier Foundation, годами учились противостоять слежке и блокировкам по всему миру и достигли в этом определенных успехов. Было бы нерационально не использовать опыт программистов и экспертов по защите privacy (тайны частной жизни) в Сети для обучения и просвещения российских пользователей.

Мы благодарны за помощь и консультации при подготовке этой работы Руне Сандвик (Center for Democracy and Technology, Washington), Якубу Далеку (CitizenLab, Toronto), Еве Гальперин (Electronic Frontier Foundation, San Francisco) и Эрику Кингу (Privacy International, London) и нашим коллегам – журналистам, работающим в сложных условиях в самых разных регионах мира.

Андрей СОЛДАТОВ, Ирина БОРОГАН
Agentura.Ru

Как построить модель угроз

Сегодня утверждение, что Интернет опасен, стало общим местом. Однако если вы все время стараетесь от всего защититься, очень легко впасть как в полную фрустрацию, так и в противоположное состояние – отрицание privacy: вы считаете, что защита бессмысленна и, соответственно, можно ничего не делать.

Для того, чтобы рассчитать, насколько необходимо защищать безопасность своей частной жизни в интернете, надо определить модель угрозы. Это поможет понять, с чем именно вы можете столкнуться. Конечно, специальное программное обеспечение – большая помощь в сохранении конфиденциальности, но безопасность, в первую очередь, связана не с программным обеспечением, а с тем, насколько четко вы понимаете угрозы и насколько точен ваш план, направленный на снижение рисков.

Очень важно определить, что именно вы хотите защитить, какую именно информацию вы цените больше всего и что, образно говоря, является вашим активом. Скорее всего, вашим активом является электронная почта, список контактов или

ваши сообщения в режиме онлайн, ваша история поиска сайтов, данные о вашей геолокации. Ваши компьютеры, ваши телефоны являются ценным для вас активом, которые также нуждаются в защите.

Второй вопрос: от кого вы хотите все это защитить? Для того, чтобы ответить на этот вопрос, очень важно понять, для кого вы являетесь мишенью для нападения. Кто для вас является источником угрозы, насколько вероятна представляемая им потенциальная угроза вам и вашим активам.

Кто может быть заинтересован в получении вашей информации – это может быть ваше руководство, ваше правительство, правительство другой страны. Это может быть какая-то атака со стороны вашего партнера, сослуживца, родителей, преступников, хакеров в открытой сети. Насколько вероятна атака с их стороны?

Чтобы на этот вопрос ответить, нужно подумать об угрозе. Угроза – это то, что может случиться с активом, и существует много разных способов, с помощью которых противник может нанести вред вашим данным. Например, он может читать то, как вы общаетесь с кем-то в сети. Он может повредить или удалить ваши данные, а также сделать невозможным ваш доступ к собственным данным.

Таких моделей угроз может быть очень много. Прежде всего – это хакерские атаки.

Например, провайдер вашего мобильного телефона имеет доступ ко всем вашим телефонным звонкам, соответственно, все эти данные возможно использовать против вас.

Хакеры по сети WiFi могут получить доступ ко всей вашей кодированной информации. Именно поэтому все, кто занимается исследованиями по кибербезопасности, знают, что самое важное здесь – понять потенциал угрожающих вам хакеров, потенциал любого, кто может нести угрозу вашей безопасности.

Важно разделять риски и угрозы. Угрозы – это то плохое, что может случиться, а риск – это вероятность того, что это плохое случится.

Например, есть угроза того, что разрушится ваше здание. Но риск этого намного выше в Сан-Франциско, где часты землетрясения, чем в Москве, где землетрясений не бывает. Оценить риск – это принципиальная задача, и это процесс личный и субъективный.

Не у всех одинаковые приоритеты и не все видят угрозы в одном и том же.

Например, есть люди, которые считают что-то неприемлемым безотносительно риска. С другой стороны, есть те, кто берет на себя высокие риски, а может быть, просто не знают, что угроза может являться проблемой.

Я всё время работаю с журналистами и рассказываю им, что очень важно защищать свои коммуникации. Но они говорят, – я военный репортёр, военный журналист, я смелый человек, я бываю на поле боевых действий и меня там могут в любой день убить. Почему я, собственно, должен беспокоиться о зашифровке своих данных? Я им говорю, что здесь есть риск, о котором они просто не задумывались. Энди Кервина (Andy Carvin), который очень много лет работал на NPR и занимался Сирией, однажды спросили – как он интервьюировал и как записывал свои данные. Он ответил: «Я всегда рекомендую всем использовать Tor. Почему? Потому что абсолютно все, кто Tor не использовал, погибли».

Ева ГАЛЬПЕРИН, эксперт
Electronic Frontier Foundation

Переписка по электронной почте должна быть доступна, в первую очередь, а ее конфиденциальность может быть меньшим приоритетом.

Моделирование угрозы. Вы задаете себе вопрос – закрыть ли дверь, запереть ли дверь, какие замки купить, где нужны более продвинутые системы защиты. Если у меня большое количество дорогостоящих вещей, насколько высока степень защиты частной жизни в моем доме? Какова угроза, боюсь ли я, что полиция будет ломиться в дверь, что соседи придут и украдут мое имущество? Волнуюсь ли я о том, что какие-то группы бродят около моего дома? Сколько раз в этом микрорайоне происходили взломы? Когда вы задаете себе эти вопросы, вы уже можете оценивать свои риски.

Если, например, ваше имущество очень дорогостоящее, но риск очень невелик, то инвестиции того, наверное, и не стоят.

С другой стороны, если вы храните очень дорогие ценности, и при этом велик риск кражи со взломом, то, в соответствии с этой моделью, нужно поступать совсем по-другому. Все модели угроз индивидуальны.

Несколько вещей, о которых стоит подумать при построении своей модели угроз. Отправляясь в командировку, стоит заранее продумать, кто именно может представлять угрозу вашим электронным устройствам.

Если речь идет об опасности изъятия ноутбука и смартфона спецслужбами, шифрование может быть решением проблемы. Но если опасность исходит не от государственных служащих? И если существует опасность физического воздействия, не стоит ли оставить ваши электронные устройства дома, а в командировку взять абсолютно новый, «чистый» ноутбук и смартфон? При этом нужные контакты и информацию можно сохранить в облаке и по мере необходимости извлекать оттуда сведения.

Корреспондент «Новой газеты» Павел Каныгин пропал в Донецкой области 11 мая 2014 года. Его похитили с главной площади Артемовска четверо вооруженных мужчин. На блокпосту между Артемовском и Славянском его раздели, забрали компьютер, телефон, начали допрос:

«На Володарке (поселок между Славянском и Артемовском) было что-то вроде штаба. Горели костры в бочках. В большой тентованной палатке – электрический свет. Вокруг палатки находилось несколько женщин и примерно двадцать молодых мужчин с автоматами и ружьями, некоторые были в масках. Меня вывели из машины и повели в палатку. Башня приказал мне раздеться. Я уточнил, как именно.

– Снимай все. Все вещи на стол, – повторил Башня. – Шнурки тоже вынимай, ремень.

Другие ополченцы уже разбирали мою сумку и рюкзак. Меня посадили на скамейку, вокруг обступили люди. Боевик в маске потребовал сообщить пароль от телефона и ноутбука. Я отказался. Тогда Башня снова ударил меня локтем по лицу.

– Ты еще не понял, что ли? Пароль!
– Пусть напишет на бумажке, – сказал кто-то.
– Он не даст.
– Сука такая.
Я поднялся с земли. Ополченец без маски взял меня за запястье и сказал, что сейчас сломает палец, если я не продиктую пароль. Я продиктовал.»

«Новая газета» Павел Каныгин, 16.05.2014
«Это не выкуп, это твой взнос в нашу войну»
http://www.novayagazeta.ru/politics/63567.html

Павла Каныгина отпустили только на следующий день.

Как осуществляется информационный контроль

В информационном пространстве есть много различных акторов: государство, сюда входят военные, правительственные структуры, спецслужбы, есть гражданское общество, есть незаконные сети (негражданское общество), это киберпреступники,и те, кто пытается использовать интернет незаконно для личного и профессионального обогащения. Есть частный сектор, который владеет и использует большую часть интернета, по которой уходит трафик.

Интернет сегодня – это продукт взаимодействия этих групп. Контроль осуществляется по трем направлениям: отказ в доступе, искажение информации и мониторинг информации.

Первый способ – это отказ в доступе к информации. Первое о чем думают люди, когда говорят об информационном контроле – блокировка доступа к веб-сайту. Фильтр в интернете, как один из примеров: когда вы пытаетесь подключиться к сайту, где запрещенный контент, вы видите такую картинку. Фильтр

может быть и транспарентным, когда вы, допустим, попадаете на сайт и видите, что он заблокирован. Вам объяснят, почему он заблокирован: допустим, это порнография, и вам об этом пишут. А иногда это выглядит, как просто ошибка сети, нет страницы, показывающей запрет доступа, просто будто нет соединения.

В России так выглядит страница на «Билайне» или у провайдера «Ростелеком». Вы получаете такую страницу, если пытаетесь попасть на заблокированный сайт. Мы пытаемся отследить продукты, программы, которые используются в различных странах для того, чтобы осуществлять фильтрацию. Часто эти продукты продаются западными компаниями.

Вот, например, компания BlueCoat, которая базируется в Калифорнии в Соединенных Штатах. Мы видим, что ее продукты используются в Сирии, в Бирме. Это мы недавно узнали. Мы проводим мониторинг, чтобы отследить эти продукты, обычно мы обнаруживаем, где находятся продукты, следующим образом: допустим, мы сканируем сети, есть какие-то блоки, которые фильтруют продукты, и кто-то в стране говорит, что подозревает, что заблокирован какой-то веб-сайт, мы пытаемся определить, где провайдер, где он расположен.

Из Торонто мы можем просканировать, посмотреть, где расположен блок. Затем мы сравниваем с известными нам подписями, определяем, кто за этим стоит. Также мы изучаем базы данных и какую-то информацию на этот счет, чтобы найти следы.

Якуб ДАЛЕК,
эксперт исследовательской лаборатории
Citizen Lab при Университете Торонто (Канада)

Отказ от предоставления доступа может произойти, если веб-сайт подвергается атаке и компьютер не выдерживает, потому что слишком много подключений. Есть еще и нетехнические способы отказа в предоставлении информации: юридические, правовые и действия регуляторов.

В Китае, если вы хотите быть хостером веб-сайта, вы должны получить лицензию. Лицензию обычно получают компании, и здесь возникает такое препятствие, что нужно много работы бумажной провести, и плюс люди не хотят писать, что они реально думают, потому что они не хотят быть искренними, плюс они в бумагах пишут, кто отвечает за какой контент, а это тоже мешает честной работе.

Якуб ДАЛЕК,
эксперт исследовательской лаборатории
Citizen Lab при Университете Торонто (Канада)

Второй вид контроля позволяет манипулировать информацией и представлять какие-то сообщения, которые не соответствуют реальным, например, можно хакнуть веб-сайт, изменить его содержание, но также можно манипулировать социальными сетями для того, чтобы представить какое-то послание, которое совершенно не соответствует тому, каким оно должно было быть.

Вот, например, сирийская электронная армия, это группа хакеров за Асада. Они активно взламывают сайты, меняют содержимое и пропагандируют режим Асада. Аналогичную атаку они произвели на Гарвардский университет, разместили там фотографию Асада на одной из страниц. Недавно Сирийская электронная армия вскрыла электронную почту одного из советников Обамы и изменила ссылки. И затем, когда Белый дом размещал сообщения, и пользователи переходили по этим ссылкам, они попадали на сайты, поддерживающие Асада и читали их пропаганду. Вот пример 2008 года, это история известного блогера Терри Уилсон. Хакеры вскрыли ее сайт, и сейчас на этой странице содержатся записи в поддержку Китая, оскорбляющие свободный Тибет и так далее, компрометирующие ее. Еще один пример – март 2012 года, все поиски по тэгу «Тибет» приводили на пустые страницы. Задумка заключалась в том, что если кто-то ищет информацию о Тибете, он информацию не найдет.

Якуб ДАЛЕК,
эксперт исследовательской лаборатории
Citizen Lab при Университете Торонто (Канада)

Еще один вид контроля информации – это мониторинг, в результате которого отслеживается пароль и осуществляется взлом. Здесь особую роль играет так называемое вредоносное ПО. Говоря о вредоносном ПО – давайте сначала поймем, что это такое. Это вредоносное программное обеспечение, которое должно наносить какой-то ущерб вашему компьютеру – такова задумка. И стандартный пример такого вредоносного ПО, с которым мы сталкиваемся, оно не направлено против вас лично, то есть направлено против всех пользователей. 90% вредоносного ПО просто ищет финансовую информацию. К примеру, информацию о вашей кредитной карточке. И такая программа, в принципе, должна использоваться единожды на каждом конкретном компьютере, она запускается и собирает вашу финансовую информацию. Однако есть и целенаправленное вредоносное ПО, которое используется против конкретных лиц. Как правило, хакеры рассылают такие вредоносные программы в приложениях к сообщениям и пытаются собрать персональную информацию. Такие шпионские программы известны под именем «троян» (trojan). Что же может сделать «троян», попав на ваш компьютер или смартфон?

Троян – это компьютерная программа, которую можно прислать на ваш компьютер, и на ваш мобильник. Троян, внедряясь в систему, полностью контролирует ваше устройство. И троян позволяет осуществлять массу действий. К примеру, удаленным способом включить вебкамеру вашего компьютера и делать фотографии или записи. Может регистрировать все нажатия клавиш на клавиатуре, каждый клик мыши. То же самое можно сделать с вашим смартфоном. Можно включить удаленным способом микрофон мобильного телефона и слушать ваши разговоры, где бы вы ни находились. Если задуматься, то вы носите с собой устройство слежения, которое может использоваться любой спецслужбой, которая купила эту технологию. А вы, кстати, прилагаете огромные усилия, чтобы не выключать свое это устройство, вы заряжаете каждый вечер. Мы установили, что эти технологии используются минимум в 36 странах.

Эрик КИНГ,
глава исследовательского направления Privacy International

Сейчас такого рода шпионская деятельность стала достаточно прибыльным видом коммерческой деятельности.

Правоохранительные органы по всему миру активно закупают такое оборудование, к примеру есть Vupen, которые продают данные об уязвимости, которые есть в компьютерах, правительствам, правоохранительным органам.

Далее, DaVinci продает «трояны», которые позволяют получить удаленный доступ к компьютерам. Для законного перехвата информации такие компании как Gamma International продают программу Finfisher. Я активно исследовал эту программу, и она тоже используется для шпионажа. Мы обнаружили серверы Finfisher в Индии, Катаре, Эмиратах, Бахрейне, Эфиопии, Германии, Индонезии – это по итогам самых первых исследований.

Очень сложно понять, кто заказчик, потому что серверы находятся в Индии, а мы вообще не можем утверждать, что индийцы имеют к этому какое-то отношение, поэтому сложно определить, кто заказчик, но мы можем оценить масштаб. Через полгода после первого исследования мы провели повторное исследование и увидели, что количество целей увеличилось. Появились новые цели: Пакистан, Румыния, Нигерия, Венгрия, Литва – список не исчерпан, поэтому похоже, что такие программы используются все более активно.

Якуб ДАЛЕК,
эксперт исследовательской лаборатории
Citizen Lab при Университете Торонто (Канада)

Сценарии безопасного поведения в Интернете

Прежде чем придумывать сложные пароли, устанавливать на компьютер шифровальные средства, осваивать способы надежного удаления данных и делать другие шаги в области информационной безопасности, нужно убедиться, что компьютер защищен от вредоносного кода.

Антивирусы. Не запускайте на компьютере одновременно два антивируса. Эти программы часто конфликтуют между собой. Перед тем как устанавливать новый антивирус, лучше удалить прежний.

- Убедитесь, что и антивирус, и его базы данных – самых последних версий. Некоторые платные антивирусы работают и, кажется, успешно справляются со своей задачей, но их базы данных безнадежно устарели. Чтобы вернуть возможность обновлений, нужно снова платить.

- Антивирусный щит должен быть постоянно включен (обычно на системной панели, в правом нижнем углу экрана, появляется соответствующий значок). Только тогда он

сможет следить за общим здоровьем компьютера и перехватывать подозрительные попытки использования системных ресурсов.

- Время от времени полезно проверять жесткий диск компьютера «на вирусы» с помощью антивирусного сканера. А если вам приносят незнакомую флешку или диск, лучше протестировать их перед использованием.

Двухступенчатая идентификация. Что это такое – эта опция добавляет новый слой защиты для твоего аккаунта Google или Yahoo, требуя во время входа в систему с незнакомого устройства не только ввести привычные логин и пароль, но еще иметь доступ к телефону. Это значит, что если кто-то украдет или подберет пароль, то не сможет пройти авторизацию из-за отсутствия специального кода, который можно получить только с помощью телефона.

Эта функция была введена в Google для аккаунтов gmail, а потом добавлена другими почтовыми сервисами, начиная с Yahoo!.

Как включить эту опцию в gmail:

Кнопка для включения двухступенчатой авторизации находится в настройках твоего аккаунта Google (google.com/accounts). В группе настроек «Personal Settings» и подразделе «Security» есть ссылка «Using 2-step verification», которая переадресует на мастера по настройке двухступенчатой авторизации. Процесс начинается с выбора телефона. Устройство должно поддерживать программу Google Authenticator (она доступна для iPhone, Android и Blackberry), то «мастер» попросит установить его на телефон. Позже его нужно будет настроить, прописав в мобильном приложении параметры своей учетной записи Google, и ввести secret key с экрана монитора.

Ссылка на подробную инструкцию на сайте Google (рус.)
https://support.google.com/a/answer/175197?hl=ru

Шифрование с помощью технологии Pretty Good Privacy (PGP). Главное преимущество этой технологии состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи, т.к. эта программа построена на другом принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.

Еще одно преимущество этой программы состоит также в том, что она бесплатная.

- Ссылка на сайт, с которого можно загрузить программу генерирования ключей и инструкцию
  https://gpgtools.org/index.html

- Ссылка на подробную инструкцию (на русском) по установке PGP на сети XMPP/Jabber
  http://habrahabr.ru/post/50982/

Защита данных на диске ноутбука. Большинство современных ноутбуков по умолчанию предлагают поставить пароль на доступ.

Однако эта мера защищает ваши данные только от случайно проходящего человека, если вы ненадолго отлучились от своего компьютера. Если ваш компьютер изъяли, его жесткий диск может быть подключен к другому компьютеру, и ваш пароль не будет иметь смысла. Единственный выход в этой ситуации – шифровать ваш жесткий диск с помощью встроенных программ или программ сторонних производителей.

Анонимность при посещении сайтов. Есть несколько подходов к сохранению анонимности при посещении сайтов. Первое, с чего стоит начать – заходить только на сайты с адресом HTTPS. Сегодня уже очень многие сайты перешли на эту технологию. Однако есть технология, которая автоматически будет направлять вас на HTPS вместо обычного, незащищенного HTTP. Она разработана сотрудниками Electronic Frontier Foundation и называется HTTPS everywhere

- Ссылка на страницу, где можно скачать эту программу для вашего браузера:
  https://www.eff.org/https-everywhere

Кроме того, существует проект TOR, специально созданный для сохранения анонимности в сети.

Не только Tor может сохранить вашу анонимность в интернете. Можно установить приватность в настройках браузера, и он не будет хранить историю посещений сайтов, при этом она сохраняется у провайдера.

Можно пользоваться виртуальной частной сетью, VPN (то есть между вами и сайтом работает один узел), и в большинстве случаев провайдер VPN ведет запись ваших действий в интернете – хранит, к примеру, номера кредиток, которые вы используете, и т.д., и эту информацию у него можно получить. В случае с Tor узлов больше, и никаких логов не ведется.

Руна САНДВИК,
Ведущий технолог
Center for Democracy&Technology,
четыре года проработавшая в Tor Project

Поучительные примеры

Тибет

Статус Тибета является предметом споров. По мнению китайской стороны, Китай с XIII века непрерывно осуществлял свои суверенные права в Тибете и, таким образом, Тибет никогда не был независимым государством. Тибетская сторона утверждает, что в ходе своей истории Тибет всегда оставался независимым.

В настоящее время ни одно государство не признает независимость Тибета, считая его частью КНР. В 1950 года китайские войска захватили контроль над Тибетом, пока в 1959 году Далай-лама не сбежал в Индию, с тех пор ведется борьба за независимость Тибета. При этом общественное мнение за пределами КНР, в особенности в западных странах, склоняется в пользу независимости или широкой автономии Тибета.

Якуб Далек, эксперт исследовательской лаборатории Citizen Lab при Университете Торонто (Канада), занимался консультированием тибетских активистов:

Как-то мы занимались письмом, которое было отправлено по e-mail активисту. В нем мы обнаружили вредоносное про-

граммное обеспечение («троян»). Письмо было отправлено от имени Ченг Ли, со следующим текстом: «Я на следующей неделе буду в Шанхае, хочу встретиться с тибетцами, у меня есть список тибетцев, которые могли бы мне помочь в моих исследованиях, и был бы очень признателен, если бы вы могли заглянуть в предполагаемый список и сказать – правильная ли там содержится информация». И дальше подпись и приложение – якобы Excel'евский файл.

Так вот, если вы получили аналогичное письмо, если у вас возникли сомнения, вы могли бы спросить – кто такой Ченг Ли. Если вы погуглите его, вы увидите, что это реальный человек, что он действительно является исследователем в университете, и вы увидите, что действительно занимается вопросами, о которых говорится в письме. К счастью, активист, который получил это письмо, начал что-то подозревать, потому что Ченг Ли работает в престижной организации, однако почему-то у него была почта на America online.

Возникает вопрос, почему, если человек пишет по работе, он не пишет с рабочего адреса? Таким образом, у активиста закрались подозрения, но ему было интересно, с одной стороны – возникли подозрения, с другой стороны, захотелось поиграть с этим человеком. И он ответил на это письмо: «Спасибо, Ченг Ли, я попытался открыть документ, но у меня компьютер макинтош и документ не открылся». Ну и через две недели примерно с того же адреса пришел еще один e-mail, в котором говорилось: «О, простите, пожалуйста, надеюсь, что вы сможете открыть этот документ во вложении...» – там уже было два вложения и две программы – для Мака и для Windows. То есть это там не какой-то ленивый хакер, это человек, который проводит активную исследовательскую работу, понимает, какие вопросы вам могут быть интересны, и он достаточно креативен, чтобы подстраиваться под ситуацию. Что интересно, такие e-mail'ы технически достаточно примитивны, вирусы эти, по большей части, были написаны еще в 2010 году, поэтому мы здесь сталкиваемся не со сложным техническим решением, а с творческим подходом, когда человек вкладывает большие усилия, например, в написание текста.

Киев-Тунис

В феврале 2014 года в Киеве активисты, находящиеся на Майдане, стали получать на свои мобильные телефоны смс-ки с текстом, что все они идентифицированы и внесены в список лиц, которые присутствуют на несанкционированном мероприятии. Понятно, что такое возможно только с использованием продвинутых технологий слежки.

Эрик Кинг, глава исследовательского направления Privacy International, много лет занимается исследованием рынка технологий слежки, выясняя почему западные технологии слежки, разработанные для того, чтобы выслеживать преступников, оказываются в руках репрессивных режимов:

Мы предполагаем, что в данном случае была использована технология под названием IMSI catcher, это фальшивая сотовая вышка, раньше они были огромными, и помещались в небольшом грузовичке. Сейчас эти приборы могут быть очень компактными. С помощью этого устройства вы можете определить, какие мобильные устройства находятся в определенном радиусе. Этот радиус вы создаете сами, дальше вы можете получить данные об идентификационных номерах всех этих устройств. Кроме того, можно перехватывать все телефонные переговоры, смс-сообщения, более того, редактировать сообщения, которые рассылаются определенным адресатам. В Тунисе полиция перехватывала и изменяла сообщения. Когда протестующие обменивались сообщениями: «Идите туда-то», полиция перехватывала сообщения и писала: «Ждите, оставайтесь на месте». Мне нравится этот пример, поскольку он очень показателен.

Олимпиада Сочи-2014

Российские власти не скрывали, что вложили огромные усилия в меры безопасности вокруг Олимпиады, включая установку новейших систем электронной слежки, объясняя это угрозой терроризма. Многие эксперты говорили перед играми, что приезжающим в Сочи не стоит рассчитывать на сохра-

нение тайны частной жизни. Под особое внимание спецслужб попали журналисты: в постановлении правительства РФ от 3 ноября 2013 года, которое утвердило систему сбора метаданных на Олимпийских играх («сведения о расчетах за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонентов»), журналисты были упомянуты трижды.

Как журналистам работалось в этих условиях? Как они защищали свою информацию и свои источники?

Наталья ВАСИЛЬЕВА, Associated Press:
У нас был отдельный офис во время Игр, где мы все подключались через провод, у нас была локальная сеть. И наши техники нам рекомендовали не пользоваться Wi-Fi. Но все равно приходилось им пользоваться, когда куда-то уходишь. И система там была такая: ты выбираешь сеть для журналистов, сначала вводишь в эту сеть один пароль, а потом ты каждый раз вводишь номер своей аккредитации, то есть каждый раз входишь и как бы говоришь: «Здравствуйте, это я». Нам наши техники не рекомендовали это делать. Но нам приходилось это делать. Потому что практика показывала, что мы и так все, как на рентгене, поэтому терять особо нечего.

Ксения БОЛЬШАКОВА, France 24:
У меня единственный был момент. В ноябре как раз, когда я ездила снимать небольшой сюжет, у меня был с собой, как и всегда, французский телефон, номер французской линии.

Если надо кому-то позвонить, чтобы точно это никуда не попало, я пользовалась французским телефоном. А так понятно, что уже все где-то... хранится. Потом монтаж я уже делала в Москве. Все делала здесь. Эфир прошел в январе, время уже прошло, на месте просто аккуратно звонила со своей трубки.

Анастасия КИРИЛЕНКО, Радио Свобода:
У меня была особая ситуация, потому что я была с активистами группы «Pussy Riot», и мы общались якобы в безопасном чате до того, как сюда приехать. А потом купили телефоны новые, они сами, и там было считанное количество журналистов, всем

раздали новые телефоны, и мы звонили только по ним. Но это не спасло от проколотых шин в машине (два раза их прокалывали), других разных историй. К нам потом присоединился адвокат – Александр Попков, который стал объяснять, что на самом деле и проверка документов просто так – это незаконно. И самый последний день, когда улетали, мы уже обнаглели.

Подходит к нам кто-то и спрашивает документы, а мы не предъявляем, и человек уходит. Что касается регистрации... Я там три раза была и останавливалась в разных гостиницах. В какой-то момент я даже попросила, выдайте мне регистрацию, где она, на что мне в гостинице ответили, столько бумаги не хватит, что они подают списки всех проживающих куда-то в паспортный стол, ФМС, но мне ничего на руки не выдают, и если полиция вдруг меня спросит регистрацию, я должна показать карточку гостя. Потом действительно, когда спрашивали регистрацию, я говорила, я знаю, нужно просто карточку гостя показать, они в конце концов соглашались с этим.

Следили за машиной, скорее всего. Мы успели заехать в гостиницу, а потом мы куда-то поехали в Красную поляну, но по дороге нас уже задержали якобы для проверки документов, а права водителя были не в порядке, и все это закончилось пребыванием почти до утра в УВД. Провели мы в УВД несколько часов. ДПСники до этого говорили, что видеокамеры следят за машиной, и поэтому им поступила ориентировка на машину.

Полезное программное обеспечение

В этом разделе речь пойдет об инструментах для защиты от сетевых и компьютерных угроз. Все эти программы – бесплатные.

Многие из описанных программ распространяются с открытым кодом. Это значит, что любой специалист может познакомиться с программным кодом и убедиться, что там нет «черных дверей» или ошибок.

- Для уничтожения вирусов / Avast
- Для надежного хранения паролей / KeePass
- Для хранения данных на флешке / TrueCrypt
- Для безопасного чата / Pidgin, Adium. Adium работает на Маке, Pidgin работает на Windows. Кроме того, есть программа, называется ChatSecure, которая работает на телефонах с Android. Эти программы можно подцепить к чатам в Фейсбуке и тогда ваша переписка перехвачена не будет.

- Для доступа на сайты без цензуры и сохранения анонимности / Tor
- Безопасная альтернатива Скайпу / Jitsi
- Для шифрования почты / PGP

Антивирус: Avast

Лучшие антивирусы необязательно должны быть платными. Бесплатный avast! – предлагает защиту от проникновения в компьютер из Интернета и блокировку подозрительных вложений в электронных письмах.

Пользователю антивирусной программы следует помнить две вещи:

- Постоянно появляются новые вирусы. Поэтому нужно держать антивирусную базу данных в актуальном состоянии. Avast! сам, автоматически скачивает обновления базы из сети, главное – не препятствовать ему.
- Попытка одновременно запустить два или несколько антивирусов может привести к серьезному конфликту и «зависанию» всей системы. Перед тем как устанавливать avast!, убедитесь, что на компьютере нет какого-либо другого антивируса.
- Ссылка на подробную инструкцию по установке (на русском) на сайте Tactical Technology Collective: https://securityinabox.org/ru/avast_main

Безопасное хранение данных: TrueCrypt

Программа создает на компьютере специальную защищенную область. Операционная система воспринимает эту область как файл или диск. Отличие между обычным диском и защи-

щенным пространством TrueCrypt в том, что на обычном диске данные (по умолчанию) никак не защищены, а TrueCrypt шифрует данные «на лету», практически незаметно для пользователя, и тем самым обеспечивает надежную защиту без каких-либо специальных манипуляций с файлами.

Более того, внутри «обычной» защищенной области TrueCrypt умеет размещать данные, которые не просто зашифрованы, но и совершенно скрыты от посторонних глаз: никто, кроме вас, не будет подозревать об их существовании.

- Ссылка на подробную инструкцию по установке (на русском) на сайте Tactical Technology Collective: https://securityinabox.org/ru/truecrypt_main

Безопасный чат: Pidgin / Adium

Pidgin (искаженное англ. «pigeon», голубь), один из альтернативных клиентов, умеющий работать не только в системе ICQ, но и с рядом других протоколов, включая социальные сети.

OTR (Off-the-Record Messaging) – модуль, который можно установить дополнительно к программе Pidgin, обеспечивающий безопасность сообщений, а именно:

- шифрование (никто не сможет прочесть сообщения),
- аутентификацию (возможность удостовериться, что собеседник – тот, за кого он себя выдает),
- анонимность (после того, как разговор окончен, полученные сообщения нельзя однозначно связать с личностями собеседников),
- сохранность прежних сообщений (если ваш закрытый ключ оказался в чужих руках, можно не беспокоиться за сохранность сообщений).

Установив Pidgin, вы сохраняете и список контактов (если он у вас уже есть), и способность связываться с другими пользователями; важно лишь, чтобы все вы обменивались информацией по одному протоколу (например, ICQ).

Сначала нужно установить Pidgin, затем OTR.

- Ссылка на подробную инструкцию по установке (на русском) на сайте Tactical Technology Collective: https://securityinabox.org/ru/pidgin_main

Средство обхода цензуры: Tor

Tor (The Onion Router) возник как исследовательский проект в 2000 году в исследовательской лаборатории Военно-морских сил – «Центре высокопроизводительных вычислительных систем».

Сейчас военная разведка не финансирует проект, но большая часть денег выделяется государством, через гранты. Первоначально над проектом работало 2 человека, сейчас – 20 человек.

В проекте Tor нет центрального координирования, специалисты занимаются разработкой открытого кода и исправлением ошибок в нем. Проект управляется волонтерами, к узлам они доступа не имеют. По задумке сеть была максимально децентрализована и независима, чтобы было физически невозможно контролировать происходящее в ней.

Tor работает следующим образом: данные проходят через прокси-серверы в произвольном порядке.

При загрузке клиента Tor система автоматически произвольно выбирает более чем из пяти тысяч узлов три, которые пользователь будет использовать в текущей сессии. Каждые 10 минут компьютер меняет текущие прокси-сервера на три новых, отдавая преимущество наиболее быстрым.

Сейчас действует примерно 5,3 тысячи узлов на полмиллиона пользователей, которые выходят в интернет со всего мира. Большая часть серверов находится в США и Германии.

- Ссылка на подробную инструкцию по установке (на русском) на сайте Tactical Technology Collective: https://securityinabox.org/ru/tor_main
- Ссылка на сайт Tor Project: https://www.torproject.org

Безопасная альтернатива Скайпу: Jitsi

Это частная защищенная система коммуникаций, которая включает голосовую связь и видеозвонки.

Jitsi поддерживает много разных протоколов, а значит, умеет связываться с пользователями, которые работают с другими программами. Иногда эти программы предлагают близкую функциональность (в смысле обеспечения безопасности), включая шифрования текстовых и голосовых сообщений (OTR и ZRTP). Jitsi позволяет общаться в приватной атмосфере: вы просто добавляете шифрование к своему привычному аккаунту. Таким образом ваши данные становятся недоступны для провайдеров и вероятных «третьих лиц». Jitsi использует метод шифрования Off-the-Record (OTR) для текстовых чатов и ZRTP/SRTP для голоса.

- Ссылка на подробную инструкцию по установке (на русском) на сайте Tactical Technology Collective: https://securityinabox.org/ru/jitsi

Шифрование почты: PGP

- Ссылка на подробную инструкцию по установке (на русском) на сайте Tactical Technology Collective: https://securityinabox.org/ru/thunderbird_main