ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для анархистов и не только

Александр Володарский
"Основы информационной безопасности для анархистов и не только"

Автономный союз трудящихся, Киев, 2014
Иллюстрации: Давид Чичкан
Оформление: Сергей Соловей

Для кого важна информационная безопасность?

Информационная безопасность важна для всех. Даже если вы не активист, дыры в вашей защите могут нанести ущерб вашей репутации или финансам, они могут испортить ваши отношения с друзьями или разрушить личную жизнь. Ваши аккаунты в социальных сетях могут быть использованы мошенниками, чтобы вымогать деньги у ваших друзей и близких, ваши банковские счета могут оказаться в чужих руках. Да и банальная безобидная рассылка спама от имени вашего аккаунта нанесёт ущерб репутации.

Даже для человека, не занятого протестной активностью, отсутствие элементарных представлений об информационной гигиене является непростительным. Не нужно быть хирургом, чтобы мыть руки перед едой.

Но если вы политический активист, то небрежное отношение к безопасности может угрожать вашей жизни и свободе, а также жизни и свободе ваших товарищей. Неонацисты, менты или спецслужбы — все на свой лад могут использовать содержимое вашего почтового ящика или аккаунта в социальной сети.

Слабая защита системы может привести не только к утечке вашей информации, но и к тому, что вам "подбросят" файлы, содержащие запрещённую информацию или же подделают историю активности в интернете. Помните, что информация может стать причиной для ареста и возбуждения уголовного дела — подкинуть файл с порнографией или "экстремистским призывом" ещё проще, чем наркотики или оружие.

Проанализируем основные источники уязвимостей.

Человеческий фактор

Самая слабая составляющая любой системы — это человек. Человека можно напугать, его можно завербовать, его можно перехитрить.

Если в вашем кругу общения или в почтовой рассылке есть сознательная "крыса", от утечки информации не защитит никакая конспирация. Поэтому не говорите лишнего и, что важно, не стремитесь узнать лишнего. Ни один человек не может полностью ручаться за своё молчание, поэтому иногда лучше вовсе не знать чего-то, чтобы не выдать.

Помните, что дурак подчас хуже предателя. Если информация передаётся многим людям, то её секретность будет зависеть от уровня защиты самого уязвимого элемента. Один человек без антивируса, со слабым паролем, или же с длинным языком может подставить десятки. Приучите себя и товарищей делать друг другу замечания за нарушение культуры безопасности — ошибки допускают все и это не стыдно, действительно стыдно — не работать над ошибками и не пытаться их предотвратить.

Не хвастайтесь без нужды ни в интернете, ни в личных разговорах. Красивая фотография с коктейлем Молотова (даже постановочная) сможет стать доказательством в суде.

Технический фактор

Сложнее всего перехватить то, что было сказано тихим голосом с глазу на глаз. Если при обсуждении важных вопросов можно не использовать интернет и телефон — не используйте их.

При использовании текстовых средств связи будьте уверены, что вы действительно говорите со своим собеседником, заготовьте на этот случай несколько проверочных вопросов.

Прежде чем продолжить описание основных уязвимостей и средств защиты, выучим…

Самое Главное Правило

Не стесняйтесь читать справку и пользоваться поиском.

Культура безопасности начинается с информационной культуры. Ответ на почти любой интересующий вас вопрос можно найти в документации, которая в изобилии находится в интернете. Для того, чтобы более-менее полно описать все возможные инструменты, потребовалась бы не одна тоненькая брошюра, а толстые тома, которые устарели бы еще в процессе написания. В любой непонятной ситуации — RTFM (если вы не понимаете что это такое и не нашли ответа в гугле, значит, вы недостаточно уяснили Самое Главное Правило, RTFM повторно).

Ложные друзья

Не верьте баннерной рекламе, обещающей вам чудодейственные инструменты, способные одновременно защитить ваш компьютер, ускорить его работу, убить вредоносные программы и увеличить член. Как правило, все эти чудо-программы на поверку оказываются крайне неприятными вирусами.

Используйте только проверенные инструменты, а прежде чем скачать антивирус или утилиту — примените к ним золотое правило из предыдущего пункта — поищите, что пишут об этой программе люди.

Операционная система

Время, когда ***Linux*** был уделом "красноглазиков", прошло. Любой пользователь без труда может скачать и установить бесплатную копию ***Ubuntu***[1], процесс установки и поиска драйверов — едва ли не проще, чем в Windows.

Возьмите за правило использовать Linux тогда, когда есть опасность заражения вирусом. Вы можете даже не инсталлировать его на компьютер, просто держите установочную флешку. Это не застрахует вас от многих способов взлома, но в десятки раз снизит опасность случайного заражения. Также заведите себе загрузочную флешку или компакт-диск с набором инструментов по восстановлению системы, например ***Ultimate Boot CD***[2] или ***Hirens Boot CD***[3].

Не забывайте ставить пароль на вход в систему, это мелочь, которая может защитить ваш компьютер, если вы оставляете его на короткое время в недружественном окружении.

Публичные места и перехват данных

Если пользователь забывает выйти из своего аккаунта на работе / в университете / в интернет-кафе / в гостях — есть шанс, что его коллеги-недоброжелатели этим воспользуются. Шанс быть “взломанным” таким образом больше, чем может показаться. Особенно

это касается государственных служащих и студентов, но и в офисе вполне могут найтись крысы, особенно если вы занимаетесь профсоюзным активизмом и вступаете в конфликты на рабочем месте. Приучите себя использовать на чужих компьютерах анонимный режим браузеров (есть, например, в ***Chrome*** и ***Firefox***), при котором вся ваша информация будет удалятся из компьютера после окончания работы. Если есть вероятность лишиться своего ноутбука или домашнего компьютера — используйте этот режим и там: лучше лишний раз ввести пароль, чем отдать его в руки милиции.

Есть небольшая вероятность того, что на общественных компьютерах в интернет-кафе могут стоять программы — "кейлоггеры", записывающие всю введенную информацию включая пароли. Не доверяйте им сколь-нибудь важную информацию, и меняйте использованные пароли сразу, как только попадёте за надёжный компьютер.

Будьте осторожны с публичным вайфаем, особенно во время массовых протестов, когда милиция и спецслужбы активно отслеживают неугодных. Помните, что любые не зашифрованные данные могут легко быть легко перехвачены. Используйте WPA2-шифрование со сложным паролем в своей домашней сети. Смысл этого не столько в том, чтобы уберечься от соседей, ворующих траффик, сколько в защите от перехвата данных. Если вы заслужили персональное внимание спецслужб, то считывание сигнала вашей вайфай-точки — вполне реальный сценарий.

Обращайте внимание на подписи https протоколов и не передавайте важные данные через http. Большинство сервисов и логин страниц используют https.

Вирусы, трояны, кейлоггеры

Вирус — это автоматически размножающаяся автоматически компьютерная программа, которая может совершать вредоносные действия или управлять вашим компьютером. Троян — это вирус, который маскируется под что-то полезное. Кейлогтер — программа, записывающая нажатия клавиш в системе, может быть разновидностью трояна.

- Опасность заражения вирусом многократно сокращается при переходе на ***Linux*** или подобную основанную на ***Unix*** операционную систему.

- Пользуйтесь антивирусами, не открывайте незнакомых файлов, отключите автозапуск компакт-дисков и флешек, будьте аккуратны с тем, что скачиваете.

- Не ставьте непонятные аддоны в свой браузер, вообще минимизируйте число устанавливаемых дополнений.

- Помните о вирусах, пользуясь чужими компьютерами: вы можете быть защищены дома, но даже один-единственный заход с другого компьютера может закончиться плачевно.

- Регулярно проверяйте hosts-файл. Многие вирусы могут переадресовывать ваш интернет-траффик подобным банальным способом, и вместо социальной сети, почты или банка отправлять вас сперва на сайт, который украдёт ваши пароли.

Антивирус

Выбор антивируса — дискуссионный вопрос, "лучшего" не существует, все имеют преимущества и слабости. Но и держать в системе несколько антивирусных программ одновременно тоже не рекомендуется: они могут начать охоту на вирусные базы друг друга, и систему будут существенно замедлять работу системы. Так что примените золотое правило и подберите антивирус по вкусу, базируясь на сравнительных оценках, которые найдёте в интернете. Можно посоветовать держать несколько разных антивирусов на загрузочных флешках — если не справится основной, можно будет просканировать диски дополнительным. Из бесплатных программ достаточно эффективны и популярны ***Avast***[4], ***AVG***[5], ***Avira***[6], но все они имеют свои недостатки.

Помните, антивирус не защитит вас от качественных шпионских программ, поэтому если вы всерьез опасаетесь слежки — следите за тем, какие из приложений используют интернет соединение.

Перед открытием скачиваемых файлов, проверьте их используя сервис http://virustotal.com.

Взлом паролей

Самый очевидный и простой способ взлома до сих пор иногда бывает актуальным. Это подбор паролей. Он может в равной мере быть применен к социальным сетям и почте. Но это работает лишь с простыми паролями. Поэтому пароль должен быть длинным и непредсказуемым — он не должен быть словом или датой, он не должен быть даже простой фразой. Русское слово, набранное

латиницей, и наоборот — это давно уже не оригинальный пароль.

- Используйте длинные случайные сочетания (не менее 8, лучше более 10 символов) из букв, цифр и знаков препинания. Пароль не должен включать в себя слова, имена, даты из вашей жизни.

- Пароли в разных аккаунтах ни в коем случае не должны совпадать.

- Если паролей много и вы рискуете их забыть, используйте программу-менеджер паролей наподобие ***KeePas***[7]. Эта программа позволит хранить ваши пароли в зашифрованном виде, защитив их единым "мастер паролем". Мастер-пароль забывать нельзя ни в коем случае. Впрочем, вы можете его забыть, если ваш компьютер конфискуют, и тогда ментам не будет никакого проку от файла с базой, без мастер-пароля расшифровать её не удастся.

- Не храните пароли в письмах, не храните их в текстовых файлах, не храните их в переписке, не сохраняйте их в браузере.

- Не записывайте пароли на бумажке: один из частых способов "взлома" — это прочтение пароля, записанного в неудачном месте.

- Помните, что "секретный вопрос" подбирается так же просто и даже проще, чем пароль. Так что он должен быть таким же сложным и непредсказуемым.

- Помните о социальной инженерии. Пароль можно узнать обманом. Не верьте "письмам из службы поддержки", спрашивающих у вас пароль, не верьте фальшивым почтовым сообщениям о взломе "вашу почту взломали, введите пароль чтобы её вернуть".

- Всегда будьте уверены, что вы вводите пароль на правильном сайте, а не на подделке (смотрите строку браузера: вместо mail.google.com там может оказаться, например, mail.goooogle.com или mail.google.com). Есть плагины для браузеров, защищающие от фишинга (например ***avast! plugin***), но ничто не является панацеей.

Прикладная криптография

Криптография — это искусство шифрованной переписки. Мы не будем углубляться в теорию и рассмотрим способ шифрования, который может пригодиться нам в повседневной жизни — ***PGP*** (Pretty Good Privacy), шифрование с открытым ключом. Оно работает по очень простому принципу: представьте себе, что вы рассылаете всем своим друзьям замки, а единственный ключ храните у себя. Теперь вам можно посылать запертые посылки, которые сможете открыть только вы.

Этот принцип может использоваться как в почте, так и при переписке в мессенджерах.

Запомните: публичный ключ вы должны разослать всем своим контактам. Приватный ключ вы должны сберегать в строгой секретности, только лишь для себя.

Для генерации ключей вы можете использовать бесплатный инструмент ***GnuPG***[8].

Иногда криптография создаёт ложное чувство безопасности, не поддавайтесь ему. Даже если ваше зашифрованное послание не

удастся взломать после перехвата — его всегда можно прочесть после расшифровки уже на вашем компьютере, поэтому не забывайте о других способах защиты.

Как защититься от взлома почты?

Защита вашей электронной почты должна быть одним из главных приоритетов. При регистрации на сайтах вы указываете свой почтовый адрес, так что взломщик, получив доступ к нему, автоматически получает доступ не только к вашей переписке, но и к вашим страницам в социальных сетях, сайтам, а в самых запущенных случаях — электронным кошелькам.

- Не кладите все яйца в одну корзину. Заведите отдельные почтовые ящики для регистрации в социальных сетях, отдельные — для всяких сомнительных форумов, отдельный — для переписки с людьми, отдельный — для рассылок. Разделяйте политику, работу и личную жизнь. По возможности удаляйте письма после прочтения: это расстроит виртуальных археологов будущего, но может спасти вашу репутацию или свободу.

- Для регистрации на сайтах вы можете использовать одноразовую почту, например http://mailforspam.com/

- Используйте защищённые пароли. Помните, что “секретный вопрос” — это всё тот же пароль, он не должен угадываться или подбираться грубой силой (девичью фамилию вашей мамы можно узнать по старым телефонным книгам, номер паспорта — узнать при обыске, а имя первого домашнего животного — найти просматривая фотографии вконтакте, будьте непредсказуемы).

- Не открывайте писем сомнительного содержания, не запускайте программ из приложений к письму, не скачивайте и не открывайте файлов, если не уверены на 100% в их предназначении. Не верьте сообщениям, которые просят повторно ввести ваш пароль.

- Используйте защищённые почтовые сервисы. Gmail несовершенен, но он удобен и подойдёт для работы, безобидной личной переписки и политических вопросов не противоречащих букве закона. Для более рискованных задач используйте активистские сервисы. Забудьте об отечественных провайдерах: получить у них вашу личную информацию на порядок проще, чем у зарубежных. По возможности включите двухэтапную аутентификацию с использованием SMS, но используйте для этих целей отдельную сим-карту, не следует пользоваться ею же для звонков. Альтернативой может быть использование программы для генерации кодов доступа.

Как вести шифрованную переписку с PGP?

Если вы используете веб-интерфейс для почты, то вам могут пригодиться соответствующие плагины для браузера. Обратите внимание на ***Mailvelope***[9].

Если вы используете почтовую программу, то, как правило, она либо уже оборудована поддержкой PGP, либо позволяет подключить её через плагины. К примеру, поддержка PGP неплохо реализована в бесплатном приложении ***Thunderbird***[10], существующем для основных операционных систем.

Используя GnuPG, создайте соответствующие ключи и пропишите их в настройках.

Социальные сети

Как правило, социальные сети взламываются вслед за почтой. Но иногда бывают и исключения. Вконтакте, Фейсбук, Твиттер содержат возможность подключения приложений, иногда за этими приложениями стоят спаммеры или хакеры. Большая часть взломов в социальных сетях не имеет отношения к спецслужбам или происка врагов, это чистая коммерция, аккаунты жертв используются для рассылки навязчивой рекламы. Но подумайте — если вас может обмануть безмозглый робот, то у специально-обученного человека шансов гораздо больше шансов.

- Никогда не выкладывайте в социальные сети то, что вы не хотели бы сказать громко и публично в присутствии милиционера. Приватность и режим "только для друзей" в социальных сетях — не защита: вспомните, что защита системы равна защите её самого слабого звена. Даже если у вас лишь 12 друзей, среди них может оказаться один, который станет причиной утечки.

- Не злоупотребляйте играми в социальных сетях, не открывайте приложения, предназначение которых вам не ясно, никогда не указывайте в приложениях свой пароль.

- Будьте аккуратны с переходом по ссылкам, которые вы получили в приватных сообщениях. Если ссылка ведет на незнакомый сайт и не сопровождается поясняющим сообщением, или же сопровождается чем-то невнятным наподобие ("ПОСМОТРИ КАКОЕ ФОТО Я НАШЕЛ"), игнорируйте её или переспросите собеседника, что он имеет ввиду. Убедитесь, что говорите именно с настоящим человеком и лишь тогда идите по ссылке. Если в процессе перехода по ссылке вам предлагают ввести пароль —

скорее всего, это попытка взлома.

- Берегите свою почту, связанную с социальной сетью. В идеале никто не должен знать вашего почтового адреса, привязанного к аккаунту.

- Помните о паролях, они должны быть сложными и непредсказуемыми.

- В случае, если социальная сеть просит телефонную активацию, соглашайтесь, но не используйте свой основной номер.

Обмен сообщениями, мессенджеры

Забудьте о чатах Фейсбука и Вконтакта, они не подходят для обсуждения серьёзных вопросов. Используя эти ресурсы, вы полностью зависите от администрации сервиса. Схожая опасность подстерегает и пользователей Google Talk или Skype.

Неплохим выбором будет анонимный ***Jabber*** с PGP-шифрованием. Jabber — это открытая технология, которую каждый может использовать на своём сервере, нет какого-то центра, который можно было бы взломать или контролировать. Существует огромный список jabber-серверов, мы можем порекомендовать дружественный к криптографии нидерландский сервис ***JWChat***[11].

Точно так же есть множество клиентских программ для использования джаббера, неплохой выбор — ***Psi***[12]. В Psi/Psi+ есть модуль поддержки PGP, вы можете воспользоваться им, чтобы обеспечить действительно защищённую переписку. Как

более простую альтернативу PGP в мессенджере, вы можете использовать OTR-шифрование, которое поддерживается в ***Psi***+ и ***Pidgin***.

Помните о том, чтобы не сохранять архивы переписки на локальном компьютере.

Неплохим и простым решением является браузерный чат ***Cryptocat***[15], который существует в виде плагина для большинства браузеров. Действует он просто: пользователь открывает "комнату", те, кто знает её название, могут к ней подключиться. Разговоры идут в зашифрованном виде, нигде не сохраняются. Для большей защищённости внутри чата можно открыть приватную комнату для двух пользователей.

Мобильные устройства

Как правило, на многих современных мобильных устройствах социальные сети и почта подключены всегда. Таким образом, если у вас "отожмут мобилу" — вам не поможет ни сложный пароль, ни многоэтапная авторизация, ни шифрование папки. Блокировка экрана и защита от угона может защитить вашу информацию от туповатого гопника, но не от милиции и тем более не от спецслужб. Можно дать несколько советов:

- Телефоны легко прослушиваются, SMS читаются. Не доверяйте телефонной связи ничего действительно важного.

- Не используйте смартфоны там, где их использование не нужно. Обзаведитесь простеньким телефоном, поддерживающим долговременный заряд и ходите на акции с ним.

- Если вам важно постоянно писать в социальные сети, фотографировать и т.д. — убедитесь, что с вашего смартфона нет автоматического доступа к приватной информации: захватив его, менты не должны узнать больше, чем и так написано в вашем блоге/на странице в соцсетях.

- Не используйте излишних приложений. Чем меньше у вас программ — тем лучше. Там где просачивается спам и навязчивая реклама, может просочиться и что-то более серьёзное.

- Отключите геолокацию: она не только разряжает аккумулятор, но и упрощает ваше отслеживание. Впрочем, даже с отключенной геолокацией вас легко могут выследить при участии оператора мобильной связи, так что если нужно быть незамеченным — просто выключайте телефон, а лучше — извлеките аккумулятор.

- Продумайте способ быстрого уничтожения информации на смартфоне. Иногда лучше разбить телефон о камень, чем дать сесть другу, которого вы сфотографировали в момент стычек с милицией. Но в случае, если у вас есть несколько минут — есть возможность сбросить настройки устройства до заводских с одновременным удалением всей информации — не стесняйтесь читать инструкции к своим гаджетам. При разбивании телефона озаботьтесь судьбой карты памяти, лучше проглотить micro- или даже mini-SD, чем позволить ей стать вещественным доказательством.

- Помните, что вас могут идентифицировать не только по номеру телефона, но и по уникальному номеру IMEI телефона. Если вы использовали одну и ту же симкарту с двумя телефонами, оба телефона при желании можно отождествить с вами. То же самое

если вы вставляли две симкарты в один телефон. Когда нужна конспирация (например, следует скрыть своё местонахождение в определённом месте), следует завести отдельный телефон для отдельной симкарты, и ни в коем случае не переставлять их. При этом, ваш "активистский" телефон не должен включаться если находится рядом с обыкновенным.

- Как альтернативу WhatsApp и Viber, вы можете использовать ***Telegram***[14], более защищённый сервис для мобильного общения. Кроме того, большинство смартфонов вполне может использовать Jabber-мессенджер с PGP. Стоит также обратить внимание на сервис ***whispersystems***[15], который позволит защитить ваши телефонные переговоры на смартфоне.

- Не забывайте об антивирусной защите своего смартфона или планшета.

- В случае, если вам критически важно заниматься чем-то секретным на мобильном устройстве, то обратите внимание на такой инструмент, как ***SSH-туннель***[16]. Этот инструмент был разработан для того, чтобы преодолеть Большой Китайский Файервол, так что он вполне может оказаться полезен и в наших, куда более гуманных условиях.

TOR, прокси и анонимность

Иногда вам нужно скрыть свой IP-адрес от сайта, на который вы заходите. А иногда вам нужно скрыть от провайдера какие сайты вы посещаете. В обоих случаях на выручку приходит прокси. Прокси — это промежуточный сервер. К примеру, вам

нужно зайти на запрещенный сайт: вместо того, чтобы заходить на него напрямую, вы используете прокси, и для перехватчика очевидной является лишь ваша связь с промежуточным сервером. Самые ленивые могут воспользоваться веб-интерфейсом ***Anonymouse***[17].

Если вам нужно использовать заблокированный сайт, или посмотреть видео с ютуба в регионе, где оно не показывается, попробуйте плагин для вашего браузера под названием ***Stealthy***[18].

Для регулярной анонимной работы мы посоветуем программу ***TOR***[19]. Это инструмент, автоматически выбирающий вам работающие прокси-сервера. Вы можете скачать готовый браузер с предустановленным и настроенным Тором, сохранить его на usb-stick, и у вас всегда под рукой будет возможность анонимного серфинга в интернете.

Шифрование дисков

Секретные данные полезно хранить в зашифрованном виде. Можно зашифровать целый диск, usb-stick или домашнюю директорию.

Ubuntu и некоторые другие дистрибьютивы Linux позволяют шифровать файловую систему ещё на стадии установки, также, имея пакет ***cryptsetup***, вы можете отформатировать любой внешний диск. В Windows для этих целей вы можете воспользоваться программой ***BitLocker***.

Если вы вынуждены хранить действительно компрометирующую информацию — не пожалейте немного времени на её шифрование, в случае обыска и изъятия техники это сослужит вам добрую службу.

Уничтожение данных

Простого удаления файла, как правило, бывает недостаточно. На самом деле удаляется лишь имя файла в оглавлении, а сами данные при желании вполне можно восстановить, если на соответствующее место на диске не было записано ничего нового.

Программы-"шредеры" служат для безвозвратного уничтожения данных, многократно перезаписывая секторы на диске, соответствующие удаляемому файлу. К примеру, для Windows вы можете использовать ***CCleaner***[20]. Для Linux подойдёт приложение ***shred***.

Но помните: не факт, что вы успеете удалить файлы вовремя, так что не забывайте о шифровании, а также о том, что хранить компрометирующую информацию на домашнем или рабочем компьютере — крайне неразумная затея, ведь не один человек поплатился за это своей, а то и чужой свободой.

20

И ЗАПОМНИТЕ САМОЕ ГЛАВНОЕ:
НЕТ НИКАКОГО ВОЛШЕБНОГО ТЕХНИЧЕСКОГО СРЕДСТВА, КОТОРОЕ ОБЕСПЕЧИТ ВАШУ БЕЗОПАСНОСТЬ И ПРИВАТНОСТЬ.

ВАШИ ГЛАВНЫЕ ИНСТРУМЕНТЫ — ЛОГИКА И ЗДРАВЫЙ СМЫСЛ

ССЫЛКИ:

1. http://www.ubuntu.com/download
2. http://www.ultimatebootcd.com/
3. http://www.hirensbootcd.org/
4. www.avast.com
5. http://free.avg.com
6. www.avira.com/
7. http://keepass.info/
8. http://gpg4win.org/ или http://www.gnupg.org
9. http://www.mailvelope.com
10. http://www.mozilla.org/ru/thunderbird/
11. https://unstable.nl/jwchat/
12. http://psi-im.org/
13. https://crypto.cat/
14. https://telegram.org
15. https://whispersystems.org
16. https://play.google.com/store/apps/details?id=org.sshtunnel
17. http://anonymouse.org/
18. http://www.stealthy.co/
19. https://www.torproject.org/
20. http://www.piriform.com/ccleaner

Онлайн-версия текста:
http://avtonomia.net/security/

Содержание

Для кого важна информационная безопасность?	3
Человеческий фактор.	4
Технический фактор	4
Самое Главное Правило	5
Ложные друзья	5
Операционная система	6
Публичные места и перехват данных	6
Вирусы, трояны, кейлоггеры	8
Антивирус	9
Взлом паролей	9
Прикладная криптография	11
Как защититься от взлома почты?	12
Как вести шифрованную переписку с PGP?	13
Социальные сети	14
Обмен сообщениями, мессенджеры	15
Мобильные устройства	16
TOR, прокси и анонимность	18
Шифрование дисков	19
Уничтожение данных	20
Ссылки	22

Электронная версия публикации:
http://avtonomia.net/security/