The Hitchhiker's Guide to Online Anonymity

Русский перевод руководства The Hitchhiker's Guide to Online Anonymity о приватности, анонимности и практической операционной безопасности.

Больше крутых материалов в моём телеграм-канале @grogrigs

Предосторожности при чтении этого руководства и переходе по разным ссылкам

1. **Хотите понять текущее состояние приватности и анонимности в интернете, но без чрезмерного погружения в технические детали?**
   • Прочитайте Введение, Требования и ограничения, разберитесь с некоторыми основами, начиная с вашей сети, и прочитайте заключительные замечания.

2. **Хотите учиться и одновременно понять, как удалить часть информации о себе из интернета?**
   • Прочитайте всё из пункта 1, а также раздел о том, как очистить свои идентичности из поисковых систем и других платформ, чтобы получить хорошее представление о том, как убирать свои данные из сети.

3. **Хотите сделать всё перечисленное выше и безопасно создавать анонимные онлайн-идентичности?**
   • Читайте всё руководство целиком. Позже появится отдельный список самых важных разделов, но в идеале стоит прочитать всё.

• Рядом с ссылками на **видео YouTube** есть ссылка **Invidious** для просмотра через экземпляр Invidious (в данном случае yewtu.be, размещённый в Нидерландах) ради большей приватности. По возможности рекомендуется пользоваться такими ссылками. Подробнее см. github.com Archive.org.

• Рядом с ссылками на **Twitter** есть ссылка **[Nitter]** для доступа через экземпляр Nitter (в данном случае nitter.net) ради большей приватности. По возможности рекомендуется пользоваться такими ссылками. Подробнее см. github.com Archive.org.

• Рядом с ссылками на **Wikipedia** есть ссылка **Wikiless** для доступа через экземпляр Wikiless (в данном случае wikiless.tiekoetter.com) ради большей приватности. По возможности рекомендуется пользоваться такими ссылками. Подробнее см. codeberg.org Archive.org.

• Рядом с ссылками на **Medium** есть ссылка Scribe.rip для доступа через экземпляр Scribe.rip ради большей приватности. И снова: по возможности рекомендуется пользоваться такими ссылками. Подробнее см. scribe.rip Archive.org.

Также можно установить расширение LibRedirect в браузер, чтобы упростить такие перенаправления. Archive.org:

• Firefox: addons.mozilla.org

• Браузеры на основе Chromium (Chrome, Brave, Edge): github.com

Если у вас возникают трудности с доступом к многочисленным академическим статьям, на которые ссылается это руководство, из-за платного доступа, можно воспользоваться Sci-Hub (en.wikipedia.org Wikiless Archive.org) или LibGen (en.wikipedia.org Wikiless Archive.org) для поиска и чтения этих материалов. Потому что наука должна быть свободной. Вся. Если при доступе к каким-то ресурсам вы сталкиваетесь с платным доступом, можно попробовать 12ft.io.

Наконец, обратите внимание: в этом руководстве упоминаются и даже рекомендуются разные коммерческие сервисы (например, VPN, сети доставки контента, поставщики электронной почты, хостинг-провайдеры...), **но ни один из них не одобряет и не спонсирует это руководство. Здесь нет реферальных ссылок и нет коммерческих связей с этими поставщиками. Проект полностью некоммерческий и существует только за счёт пожертвований.**

Требования и ограничения

• Понимание английского языка (в данном случае американского варианта английского).

• Быть постоянным жителем Германии, где суды подтвердили законность отказа от использования настоящих имён на онлайн-платформах (§13 VI Закона Германии о телемедиа 2007 года[1][2]). **Либо быть жителем любой другой страны, где вы можете самостоятельно подтвердить и проверить законность применения этого руководства.**

• Это руководство предполагает, что у вас уже есть доступ к какому-либо ноутбуку (Windows/Linux/macOS), желательно не рабочему и не общему устройству, а также базовое понимание того, как работают компьютеры.

• Наберитесь терпения: если вы хотите пройти весь материал, процесс может занять несколько недель.

• У вас должно быть свободное время, которое вы сможете посвятить этому процессу (объём зависит от выбранного пути).

• Будьте готовы внимательно прочитать множество источников (читайте их), руководств (не пропускайте их) и учебных материалов (их тоже не пропускайте).

• Не творите зло (на этот раз серьёзно)[3].

• Понимайте, что не существует общего пути, который одновременно был бы быстрым и лёгким.

Это руководство не предназначено для:

• создания учётных записей ботов любого вида;

• создания учётных записей, выдающих себя за существующих людей (например, для кражи личности);

• помощи злоумышленникам в неэтичной, преступной или незаконной деятельности (например, в травле, преследовании, дезинформации, распространении ложной информации, домогательствах, запугивании или мошенничестве);

• использования несовершеннолетними.

Введение

Краткая суть всего руководства: «Странная игра. Единственный выигрышный ход — не играть»[4].

Создать учётную запись в социальной сети под псевдонимом, творческим именем или названием бренда легко. В большинстве случаев этого достаточно, чтобы защитить личность «следующего Джорджа Оруэлла». Очень многие используют псевдонимы в Facebook/Instagram/Twitter/LinkedIn/TikTok/Snapchat/Reddit/... Но подавляющее большинство таких людей совсем не анонимны: их легко связать с реальной личностью силами местной полиции, случайных участников сообщества OSINT[5] (разведка по открытым источникам) и троллей[6] с 4chan[7].

Это хорошо, потому что большинство преступников и троллей не особенно технически грамотны, и их обычно легко устанавливают. Но это же и ужасно, потому что политических диссидентов, правозащитников и информаторов тоже часто можно отследить довольно легко.

Цель этого руководства — дать введение в разные техники деанонимизации, отслеживания, проверки личности и, при необходимости, показать, как безопасно создавать и поддерживать **достаточно настоящие** анонимные онлайн-идентичности, включая учётные записи в социальных сетях. Речь идёт в том числе о массовых платформах, а не только о сервисах, ориентированных на приватность.

Важно понимать: цель этого руководства — анонимность, а не просто приватность. При этом многие рекомендации здесь помогут улучшить приватность и безопасность даже тем, кого анонимность не интересует. У приватности, безопасности и анонимности есть важная общая область техник и инструментов, но в какой-то момент они расходятся:

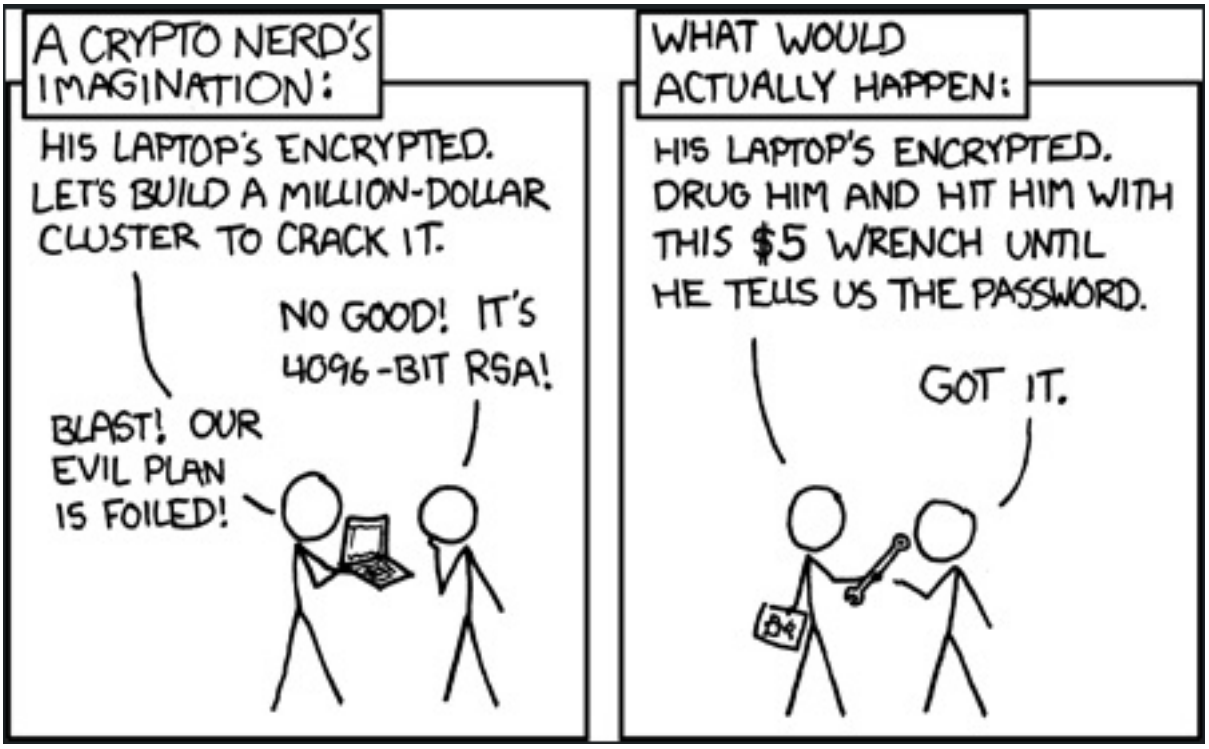
• **Приватность — это когда люди знают, кто вы, но не знают, что вы делаете.**

• **Анонимность — это когда люди знают, что вы делаете, но не знают, кто вы[8].**

(Иллюстрация из[9])

Поможет ли это руководство защититься от АНБ, ФСБ, Марка Цукерберга или Моссада, если они целенаправленно ищут именно вас? Вероятно, нет... Моссад будет делать «дела Моссада»[10] и, скорее всего, найдёт вас, как бы тщательно вы ни прятались[11].

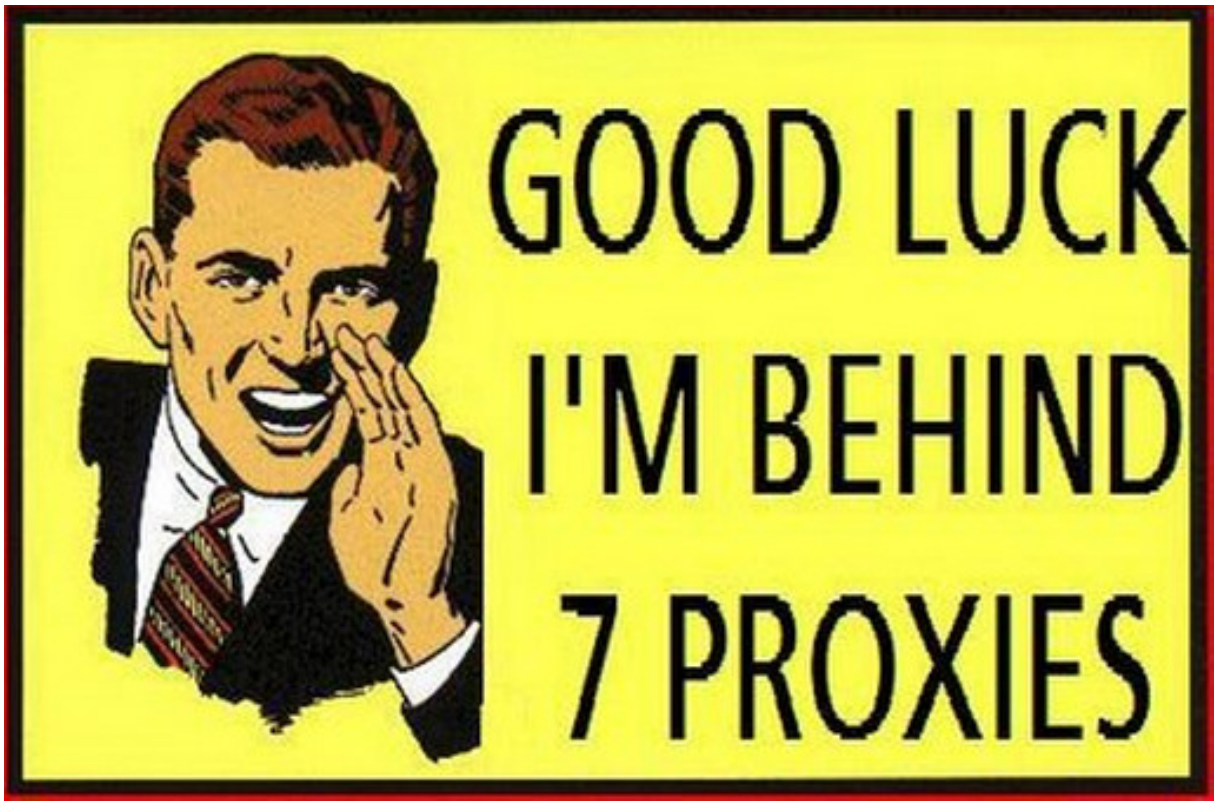
Прежде чем идти дальше, вы должны обдумать свою модель угроз[12].



(Иллюстрация Рэндолла Манро, xkcd.com, лицензия CC BY-NC 2.5)

Поможет ли это руководство защитить приватность от исследователей OSINT вроде Bellingcat[13], троллей с 4chan[14], занимающихся доксингом[15], и других людей, у которых нет доступа к инструментарию АНБ? Скорее всего, да. Хотя насчёт 4chan мы бы не были так уверены.

Вот базовая упрощённая модель угроз для этого руководства:



(Обратите внимание: шутки про «магические амулеты/подводную лодку/инсценировку собственной смерти» взяты из отличной статьи James Mickens «This World of Ours», 2014.[10])

Отказ от ответственности: если отложить шутки в сторону (магический амулет и прочее), конечно, существуют и продвинутые способы смягчать атаки со стороны таких сильных и умелых противников. Но они находятся за пределами этого руководства. Крайне важно понимать ограничения модели угроз, принятой здесь. Поэтому руководство не будет увеличено вдвое ради таких продвинутых мер: это слишком сложно и требует очень высокого уровня знаний и навыков, которого не предполагается у целевой аудитории.

EFF приводит несколько сценариев безопасности, которые стоит учитывать в зависимости от вашей деятельности. Некоторые советы могут выходить за рамки этого руководства (они скорее о приватности, чем об анонимности), но их всё равно стоит прочитать как примеры. См. ssd.eff.org Archive.org.

Если хотите глубже разобраться в моделировании угроз, см. ресурсы по моделированию угроз.

Вам может показаться, что у этого руководства нет законных применений, но их много[16][17][18][19][20][21][22], например:

• обход онлайн-цензуры[23];
• обход онлайн-угнетения;
• защита от онлайн-преследования, доксинга и домогательств;
• защита от незаконной государственной слежки в интернете;
• анонимное информирование о нарушениях;
• анонимная онлайн-активность;
• анонимная онлайн-журналистика;
• анонимная юридическая практика в интернете;
• анонимная академическая деятельность в интернете (например, доступ к научным материалам, заблокированным по стране).

Это руководство написано с надеждой помочь **людям с добрыми намерениями**, которым может не хватать знаний, чтобы увидеть всю картину целиком.

Наконец, используйте его на свой риск. Всё написанное здесь не является юридической консультацией, и перед применением вы должны проверить соответствие местному законодательству (я не юрист[24]). «Доверяй, но проверяй»[25] всю информацию самостоятельно, а ещё лучше — «никогда не доверяй, всегда проверяй»[26]. Мы настоятельно рекомендуем вам самостоятельно разбираться в теме и при сомнениях сверять любую информацию из этого руководства с внешними источниками. Пожалуйста, сообщайте нам о найденных ошибках: мы приветствуем критику. Даже резкая, но обоснованная критика приветствуется и приводит к внесению необходимых исправлений как можно быстрее.

А теперь — неполный список некоторых из многих способов, которыми вас могут отслеживать и деанонимизировать:

Ваша сеть

Ваш IP-адрес

Отказ от ответственности: весь этот раздел относится к вашему публичному интернет-IP, а не к IP-адресу в локальной сети.

Ваш IP-адрес[27] — самый известный и очевидный способ отслеживания. Это IP-адрес, с которого вы выходите в интернет. Обычно его выдаёт ваш интернет-провайдер (xDSL, мобильная сеть, кабель, оптоволокно, кафе, бар, друг, сосед). Во многих странах действуют правила хранения данных[28], обязывающие хранить журналы того, кто каким IP-адресом пользовался в определённые дату и время, вплоть до нескольких лет или бессрочно. Ваш провайдер может сообщить третьей стороне, что вы использовали конкретный IP-адрес в конкретные дату и время, даже спустя годы. Если этот исходный IP-адрес в какой-либо момент и по любой причине утечёт, его можно использовать, чтобы выйти напрямую на вас. Во многих странах получить доступ к интернету без предоставления провайдеру какой-либо формы идентификации (адреса, документа, настоящего имени, электронной почты...) невозможно.

Само собой, большинство платформ (например, социальные сети) тоже будут хранить, иногда бессрочно, IP-адреса, с которых вы регистрировались и входили в их сервисы.

Вот несколько онлайн-ресурсов, с помощью которых можно прямо сейчас узнать информацию о вашем текущем **публичном IP-адресе**:

- Узнать свой IP-адрес:
  - resolve.rs
  - dnsleaktest.com (дополнительно можно проверить утечки DNS)
- Узнать географическое положение своего IP-адреса или любого другого IP-адреса:
  - resolve.rs
- Проверить, считается ли IP-адрес «подозрительным» (в чёрных списках) или скачивал ли он «вещи» по некоторым публичным данным:
  - mxtoolbox.com
  - virustotal.com
  - iknowwhatyoudownload.com (относитесь к этому скептически: сервис может не показать ничего интересного и имеет ограниченные источники данных. Это скорее развлечение, чем серьёзный инструмент.)
- Регистрационные сведения об IP-адресе (скорее всего, это ваш провайдер или провайдер подключения, который, вероятнее всего, знает, кто пользуется этим IP-адресом в любой момент времени):
  - whois.domaintools.com
- Проверить открытые сервисы или открытые устройства на IP-адресе (особенно если там есть «умные» устройства, которые могут что-то раскрывать):
  - shodan.io (замените IP-адрес на свой или любой другой либо измените запрос в строке поиска; примерный IP здесь — выходной узел Tor)
- Разные инструменты для проверки IP-адреса, включая проверку по спискам блокировки и другое:

    - browserleaks.com
    - whatismyip.com

- Хотите узнать, подключены ли вы через Tor?
    - check.torproject.org

По этим причинам вам придётся запутывать и скрывать этот исходный IP-адрес (тот, который связан с вашей личностью) или прятать его сочетанием разных способов:

- использовать публичный Wi-Fi (бесплатно);
- использовать анонимизирующую сеть Tor[29] (бесплатно);
- использовать VPN-сервисы[30] анонимно (с анонимной оплатой наличными или Monero).

Учтите, к сожалению, что эти решения не идеальны и вы столкнётесь с проблемами производительности[31].

Все эти варианты будут объяснены далее в руководстве.

Ваши DNS- и IP-запросы

DNS означает «система доменных имён»[32]. Это служба, которую браузер (и другие приложения) используют, чтобы находить IP-адреса сервисов. По сути, это огромный «список контактов» — телефонная книга, если пользоваться старым сравнением: вы спрашиваете имя, а она возвращает номер, по которому надо звонить. Только вместо номера она возвращает IP-адрес.

Каждый раз, когда браузер хочет открыть какой-то сервис, например Google через www.google.com, он (Chrome или Firefox) обращается к DNS-службе, чтобы найти IP-адреса веб-серверов Google.

Если вы уже потерялись, вот видео с наглядным объяснением DNS: youtube.com Invidious

Обычно DNS-службу предоставляет ваш интернет-провайдер, и она автоматически настраивается сетью, к которой вы подключаетесь. Эта DNS-служба тоже может подпадать под правила хранения данных или просто вести журналы по другим причинам, например для сбора данных в рекламных целях. Поэтому провайдер сможет рассказать всё, что вы делали в интернете, просто посмотрев эти журналы, а затем передать их противнику. Удобно и то, что для многих противников это самый простой способ вводить цензуру или родительский контроль через блокировку DNS[33]. Выданные DNS-серверы будут отдавать другой адрес вместо настоящего для некоторых сайтов, например перенаправляя thepiratebay.org на какой-нибудь государственный сайт. Такая блокировка широко применяется по всему миру для отдельных сайтов[34].

Использование частной DNS-службы или собственной DNS-службы может смягчить эти проблемы, но есть и другая: большинство таких DNS-запросов по умолчанию всё ещё отправляется по сети открытым текстом, без шифрования. Даже если вы открываете PornHub в приватном окне, используете HTTPS и частную DNS-службу, вероятность крайне высока, что браузер отправит на какие-то DNS-серверы незашифрованный запрос открытым текстом, по сути спрашивая: «Какой IP-адрес у www.pornhub.com?».

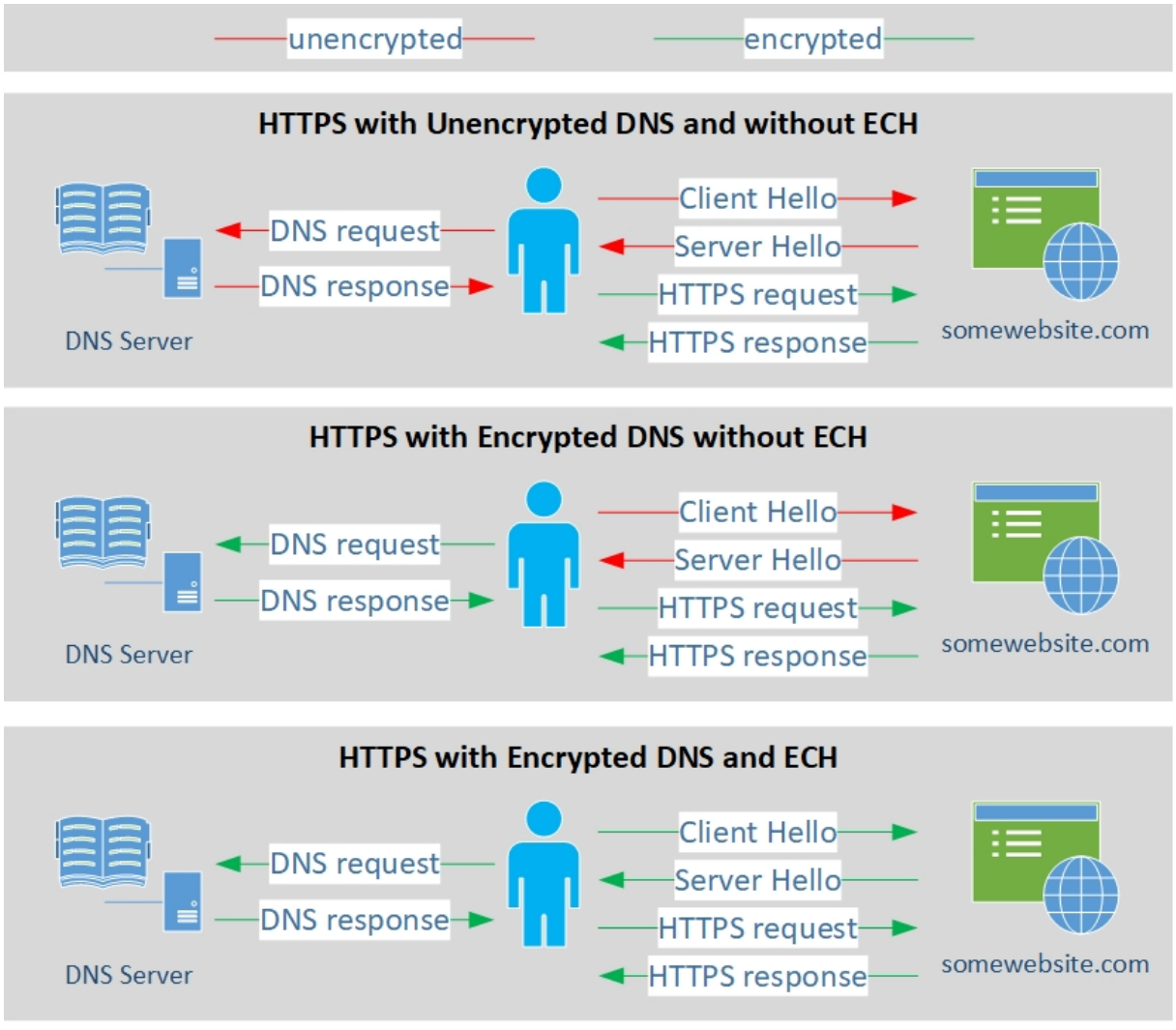
Поскольку запрос не зашифрован, ваш провайдер и/или любой другой противник может перехватить его (используя атаку «человек посередине»[35]), узнать, что искал ваш IP-адрес, и, возможно, записать это в журнал. Тот же провайдер может подменять DNS-ответы, даже если вы используете частный DNS. В таком случае польза частной DNS-службы пропадает.

Вдобавок многие устройства и приложения используют жёстко заданные DNS-серверы, обходя любые системные настройки. Так, например, поступает большинство (70%) «умных» телевизоров и значительная часть (46%) игровых приставок[36]. Для таких устройств придётся принудительно заставлять их[37] не пользоваться жёстко заданной DNS-службой, что может нарушить их нормальную работу.

Решение — использовать зашифрованный DNS: DoH (DNS поверх HTTPS[38]) или DoT (DNS поверх TLS[39]) с частным DNS-сервером. Его можно разместить самостоятельно локально, например через pi-hole[40], разместить удалённо через решение вроде nextdns.io либо использовать решения, предоставляемые вашим VPN-провайдером или сетью Tor. Это должно помешать провайдеру или посреднику подсматривать ваши запросы... но может и не помешать.

Небольшой промежуточный отказ от ответственности: **это руководство не обязательно одобряет или рекомендует сервисы Cloudflare, даже если они несколько раз упоминаются в этом разделе для технического понимания.**

К сожалению, протокол TLS, используемый в большинстве HTTPS-соединений в большинстве браузеров (в том числе Chrome/Brave), снова раскрывает доменное имя через рукопожатия SNI[41] (это можно проверить у Cloudflare: cloudflare.com Archive.org). **На момент написания этого руководства только браузеры на основе Firefox поддерживают ECH (Encrypted Client Hello[42], ранее известный как eSNI[43]) на некоторых сайтах; ECH шифрует всё сквозным образом (в дополнение к безопасному частному DNS поверх TLS/HTTPS) и позволяет скрывать ваши DNS-запросы от третьей стороны[44].** И этот параметр тоже не включён по умолчанию, поэтому его придётся включать вручную.



Помимо ограниченной поддержки в браузерах, на этом этапе ECH/eSNI поддерживают только веб-сервисы и сети доставки контента[45], находящиеся за Cloudflare CDN[46]. Это означает, что ECH и eSNI на момент написания руководства не поддерживаются большинством массовых платформ, например:

• Amazon (включая AWS, Twitch...);

• Microsoft (включая Azure, OneDrive, Outlook, Office 365...);

• Google (включая Gmail, Google Cloud...);

• Apple (включая iCloud, iMessage...);

• Reddit;

• YouTube;

• Facebook;

• Instagram;

• Twitter;

• GitHub;

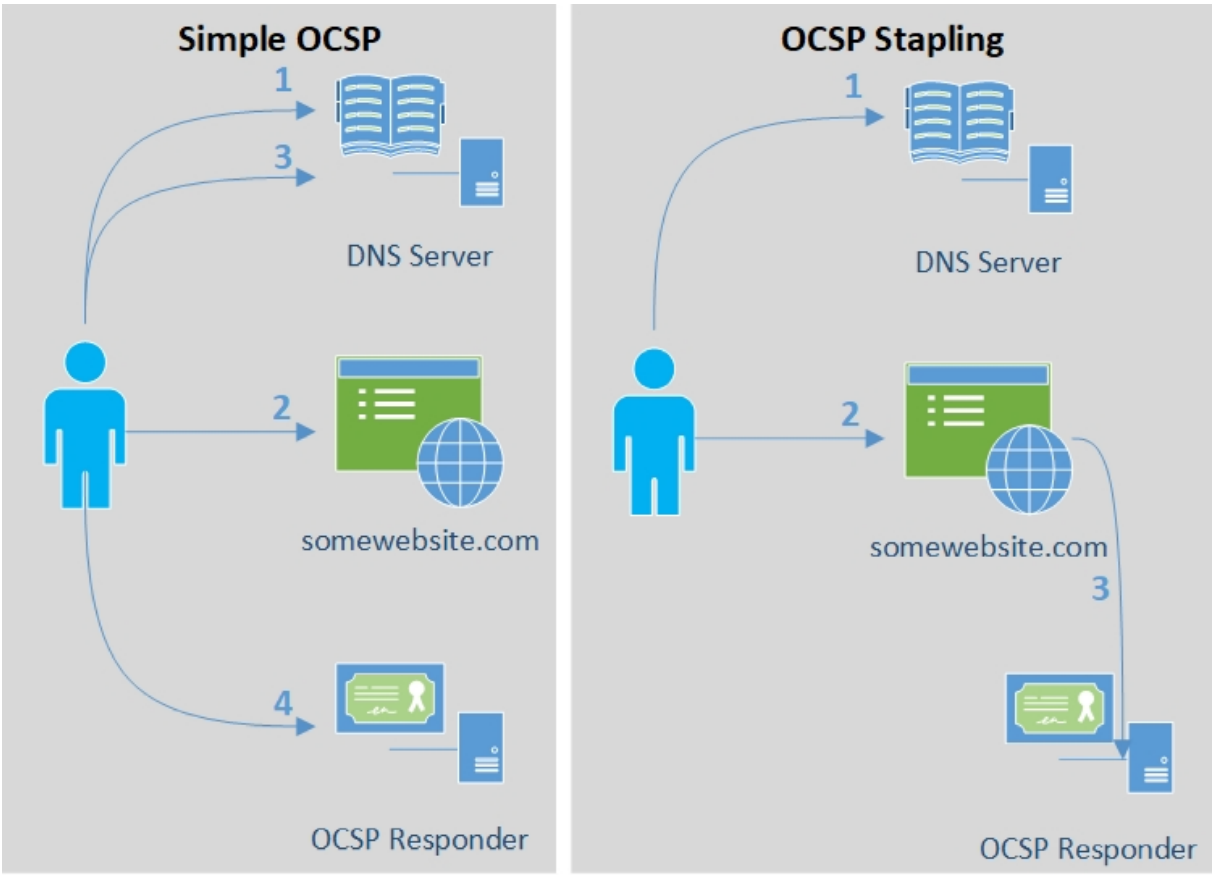
• ...

Некоторые страны, например Россия[47] и Китай[48], могут (это не подтверждено, несмотря на статьи) блокировать рукопожатия ECH/eSNI на сетевом уровне, чтобы сохранять возможность слежки и не допускать обхода цензуры. Это означает, что вы не сможете установить HTTPS-соединение с сервисом, если не позволите им увидеть, что это был за сервис.

На этом проблемы не заканчиваются. Часть проверки TLS в HTTPS называется OCSP[49], и этот протокол, используемый браузерами на основе Firefox, раскрывает метаданные в виде серийного номера сертификата посещаемого сайта. Затем противник может легко понять, какой сайт вы посещаете, сопоставив номер сертификата[50]. Эту проблему можно смягчить с помощью OCSP stapling[51]. К сожалению, в Firefox/Tor Browser эта функция включена, но не является обязательной по умолчанию. Кроме того, посещаемый сайт тоже должен её поддерживать, а поддерживают её не все. Браузеры на основе Chromium, в свою очередь, используют другую систему, CRLSets[52][53], которая, вероятно, лучше.

Вот список того, как разные браузеры ведут себя с OCSP: ssl.com Archive.org

Вот иллюстрация проблемы, с которой можно столкнуться в браузерах на основе Firefox:



Наконец, даже если вы используете собственный зашифрованный DNS-сервер (DoH или DoT) с поддержкой ECH/eSNI и OCSP stapling, этого всё равно может быть недостаточно: исследования анализа трафика[54] показали, что нежелательные запросы всё ещё можно надёжно распознавать по цифровому отпечатку и блокировать. Только DNS поверх Tor показал эффективную приватность DNS в недавних исследованиях, но даже его можно обойти другими средствами (см. Ваш анонимизированный трафик Tor/VPN).

Можно также решить использовать скрытую DNS-службу Tor или ODoH (Oblivious DNS over HTTPS[55]), чтобы дополнительно повысить приватность и анонимность, но, **к сожалению**, насколько нам известно, на момент написания эти методы предоставляет только Cloudflare (blog.cloudflare.com Archive.org, blog.cloudflare.com Archive.org). Это рабочие и достаточно безопасные технические варианты, но остаётся и моральный выбор: хотите ли вы пользоваться Cloudflare или нет (несмотря на риск, на который указывают некоторые исследователи[56]).

Обратите внимание: Oblivious DNS защищает от противника, который подслушивает одно из перечисленных ниже соединений, но не все сразу. Он не защищает от глобального пассивного противника (GPA), который может подслушивать многие или все эти соединения:

• трафик между клиентским преобразователем имён и рекурсивным преобразователем;
• трафик между рекурсивным преобразователем и преобразователем ODNS;
• трафик между преобразователем ODNS и авторитетным сервером.

Наконец, есть и новая возможность под названием DoHoT, то есть DNS over HTTPS over Tor: DNS поверх HTTPS поверх Tor. Она тоже может дополнительно повысить вашу приватность и анонимность, и её можно рассмотреть, если вы уверенно работаете с Linux. См. github.com Archive.org. На этом этапе руководство не будет помогать с этим вариантом, но такой раздел может появиться позже.

Вот иллюстрация текущего состояния приватности DNS и HTTPS, насколько мы его сейчас понимаем.

Для обычного повседневного использования (не чувствительного) помните: пока только браузеры на основе Firefox поддерживают ECH (ранее eSNI), и на этом этапе он полезен только для сайтов, размещённых за Cloudflare CDN. Если вы предпочитаете вариант на основе Chrome (что для некоторых понятно из-за лучше встроенных функций вроде перевода на лету), мы бы

рекомендовали Brave: он поддерживает все расширения Chrome и предлагает гораздо лучшую приватность, чем Chrome.

Но история на этом, конечно, не заканчивается. Даже если вы зашифруете DNS и примените все возможные меры смягчения, простые IP-запросы к любому серверу, вероятно, всё равно позволят противнику понять, какой сайт вы посещаете. Причина проста: у большинства сайтов есть уникальные связанные с ними IP-адреса, как объясняется здесь: blog.apnic.net Archive.org. Это означает, что противник может создать набор данных известных сайтов с их IP-адресами, а затем сопоставлять его с IP-адресами, к которым вы обращаетесь. В большинстве случаев это даст правильную догадку о посещаемом сайте. Иными словами, несмотря на OCSP stapling, несмотря на ECH/eSNI, несмотря на зашифрованный DNS... противник всё равно может угадать, какой сайт вы посещаете.

Поэтому для смягчения всех этих проблем, насколько это возможно и насколько мы умеем, далее руководство будет рекомендовать два решения: использовать Tor и виртуализированное (см. Виртуализация) многоуровневое решение VPN поверх Tor (DNS поверх VPN поверх Tor или DNS поверх Tor). Другие варианты тоже будут объяснены (Tor поверх VPN, только VPN, без Tor/VPN), но они менее рекомендуемы.

Ваши устройства с поддержкой RFID

RFID означает радиочастотную идентификацию[57]. Это технология, которая используется, например, для бесконтактных платежей и разных систем идентификации. Разумеется, ваш смартфон тоже относится к таким устройствам и имеет возможность бесконтактных платежей через NFC[58]. Как и всё остальное, такие возможности могут использоваться для отслеживания разными участниками.

Но, к сожалению, дело не ограничивается смартфоном. Скорее всего, вы постоянно носите с собой несколько устройств или предметов с поддержкой RFID, например:

• банковские карты с бесконтактной оплатой;
• карты лояльности магазинов;
• транспортные карты;
• рабочие карты доступа;
• ключи от автомобиля;
• национальное удостоверение личности или водительские права;
• паспорт;
• ценники и противокражные метки на предметах или одежде.

Хотя всё это нельзя использовать для деанонимизации удалённым онлайн-противником, такие метки могут сузить поиск, если известно ваше примерное местоположение в определённое время. Например, нельзя исключать, что некоторые магазины фактически сканируют и записывают все RFID-чипы, проходящие через дверь. Они могут искать свои карты лояльности, но попутно записывать и другие метки. Такие RFID-метки можно связать с вашей личностью, что позволит деанонимизировать вас.

Подробнее в Wikipedia: en.wikipedia.org Wikiless Archive.org и en.wikipedia.org Wikiless Archive.org

Единственный способ смягчить эту проблему — не носить с собой RFID-метки или снова экранировать их чем-то вроде клетки Фарадея. Можно также использовать специальные кошельки и чехлы, которые блокируют RFID-связь. Многие из них сейчас выпускают известные бренды, например Samsonite[59]. Просто не носите такие RFID-устройства во время чувствительных действий.

См. Предупреждение о смартфонах и умных устройствах.

Устройства Wi-Fi и Bluetooth вокруг вас

Геолокация выполняется не только через триангуляцию по антеннам мобильной связи. Она также выполняется с помощью устройств Wi-Fi и Bluetooth вокруг вас. Разработчики операционных систем, такие как Google (Android[60]) и Apple (iOS[61]), поддерживают удобную базу данных большинства точек доступа Wi-Fi, устройств Bluetooth и их местоположения. Когда ваш смартфон Android или iPhone включён (и не находится в авиарежиме), он активно сканирует точки доступа Wi-Fi и устройства Bluetooth вокруг вас, если вы специально не отключили эту функцию в настройках, и может определять ваше местоположение точнее, чем при использовании GPS.

Такое активное и постоянное зондирование затем может отправляться Google/Apple/Microsoft как часть телеметрии. Проблема в том, что это зондирование уникально: по нему можно однозначно распознать пользователя и отслеживать его. Например, магазины могут использовать эту технику, чтобы распознавать покупателей, включая повторные посещения, перемещения по магазину и время, проведённое в конкретном месте. Есть несколько научных работ[62][63] и статей[64], подробно описывающих эту проблему.

Это позволяет им предоставлять точные данные о местоположении даже при выключенном GPS, но также позволяет вести удобную запись всех устройств Wi-Fi и Bluetooth по всему миру. Затем доступ к этим данным могут получать они сами или третьи стороны для отслеживания.

Примечание: если у вас смартфон Android, Google, вероятно, знает, где он находится, что бы вы ни делали. Настройкам нельзя по-настоящему доверять. Вся операционная система создана компанией, которая хочет ваши данные. Помните: если сервис бесплатен, значит товар — вы.

Но это ещё не всё, на что способны все эти точки доступа Wi-Fi. Недавно разработанные технологии могут даже позволить точно отслеживать ваши движения только по радиопомехам. Это означает, что движение внутри комнаты или здания можно отслеживать по проходящим радиосигналам. Это может звучать как конспирология в шапочке из фольги, но вот источники[65] с демонстрациями этой технологии в действии: rfpose.csail.mit.edu Archive.org и видео здесь: youtube.com Invidious

Другие исследователи нашли способ считать людей в заданном пространстве, используя только Wi-Fi, см. news.ucsb.edu Archive.org

Отсюда можно представить множество применений таких технологий: например, записывать, кто входит в определённые здания или офисы (отели, больницы, посольства), а затем выяснять, кто с кем встречается, отслеживая людей снаружи. Даже если у них нет с собой смартфона.

И снова: такую проблему можно смягчить только находясь в комнате или здании, которое действует как клетка Фарадея.

Вот ещё одно видео с похожей технологией в действии: youtube.com Invidious

См.: Предупреждение о смартфонах и умных устройствах.

С этим мало что можно сделать, кроме как изначально быть неидентифицируемым.

Поддельные точки доступа Wi-Fi

Такие атаки используются как минимум с 2008 года, в том числе через атаку под названием «Jasager»[66]. Их может выполнить кто угодно, используя самодельные инструменты или коммерчески доступные устройства вроде Wi-Fi Pineapple[67].

Вот несколько видео, объясняющих тему подробнее:

• HOPE 2020, archive.org

• YouTube, Hak5, Wi-Fi Pineapple Mark VII youtube.com Invidious

Такие устройства помещаются в небольшую сумку и могут захватить Wi-Fi-среду любого места в пределах досягаемости, например бара, ресторана, кафе или холла отеля. Они могут принудительно отключать Wi-Fi-клиентов от текущей сети (атаки деаутентификации и разрыва связи[68]), одновременно подделывая обычные Wi-Fi-сети в этом месте. Атака будет продолжаться, пока ваш компьютер или вы сами не попытаетесь подключиться к поддельной точке доступа.

Затем эти устройства могут имитировать captive portal[69] с точно таким же оформлением, как у Wi-Fi, к которому вы пытаетесь подключиться, например портал регистрации в аэропорту. Или они могут просто предоставить вам неограниченный доступ в интернет, который сами получают из того же места.

После подключения через поддельную точку доступа она сможет выполнять разные атаки «человек посередине» для анализа вашего трафика. Это могут быть вредоносные перенаправления или простое прослушивание трафика. Так легко выявить любого клиента, который, например, пытается подключиться к VPN-серверу или сети Tor.

Это полезно, когда известно, что человек, которого хотят деанонимизировать, находится в людном месте, но неизвестно, кто именно. Такой противник сможет по анализу трафика, как уже отмечалось выше в разделе DNS, возможно распознать по цифровому отпечатку любые посещаемые вами сайты, несмотря на использование HTTPS, DoT, DoH, ODoH, VPN или Tor.

Эти техники также можно применять для создания сложных фишинговых сайтов, нацеленных на кражу ваших учётных данных или на убеждение установить вредоносный сертификат. Такой сертификат может позволить атакующим перехватывать и расшифровывать ваш зашифрованный трафик.

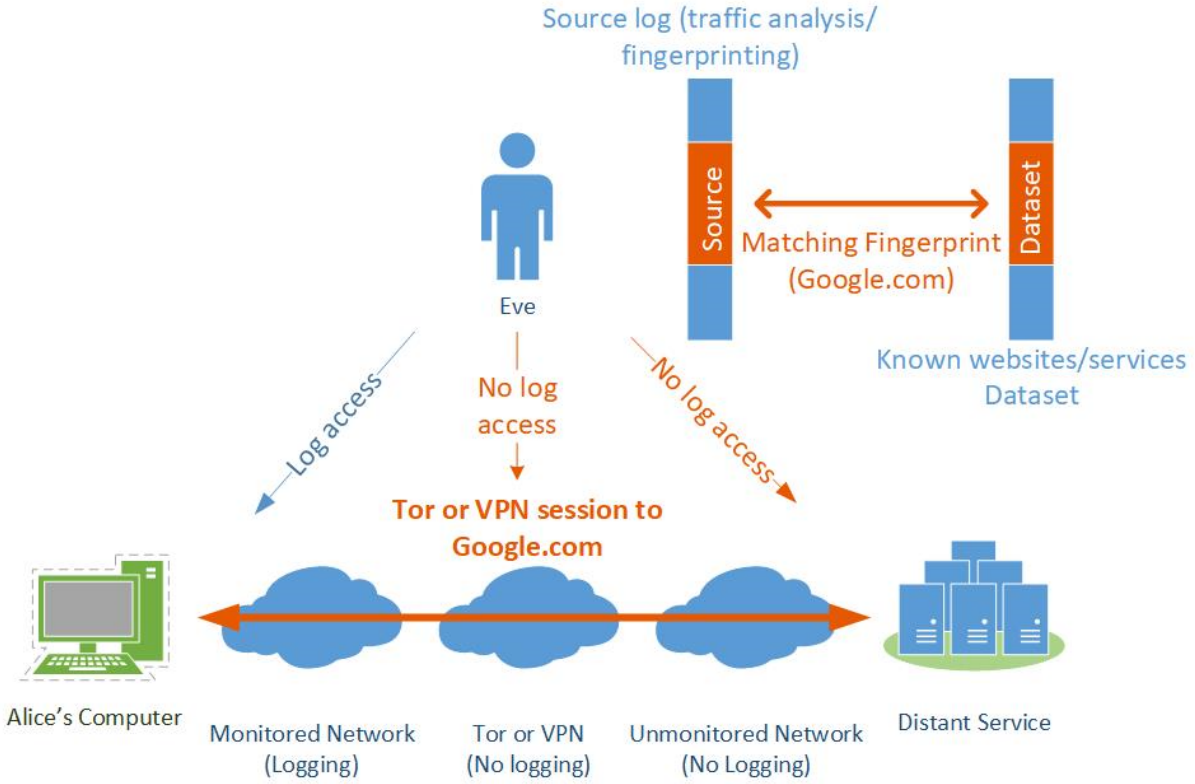
Как смягчить это? Если вы подключаетесь к публичной точке доступа Wi-Fi, используйте Tor либо VPN, а затем Tor (Tor поверх VPN), или даже VPN поверх Tor, чтобы запутать трафик для поддельной точки доступа, продолжая пользоваться ею.

Кроме того, стоит посмотреть доклад конференции BlackHat USA Surveilling the Masses with Wi-Fi Positioning Systems Invidious. В докладе подробно разбирается критическая уязвимость в API позиционирования Wi-Fi от Apple, которую можно использовать для геозонирования населения через уникальные идентификаторы. См.: Предупреждение о смартфонах и умных устройствах. iPhone ваших соседей тоже представляют отдельную угрозу.

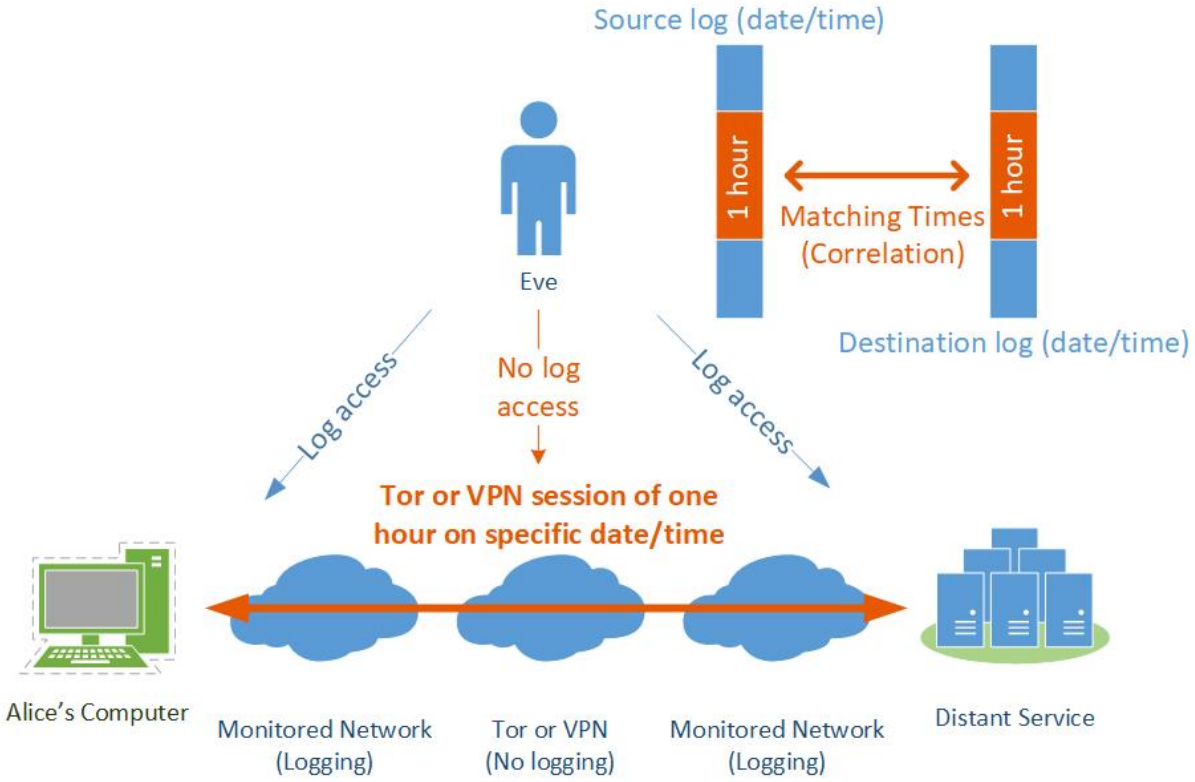
Анонимизация трафика

Tor и VPN — не универсальное средство. За годы было разработано и изучено множество продвинутых техник деанонимизации зашифрованного трафика Tor[70]. Большинство таких техник — корреляционные атаки: они тем или иным образом сопоставляют ваш сетевой трафик с журналами или наборами данных. Вот несколько примеров:

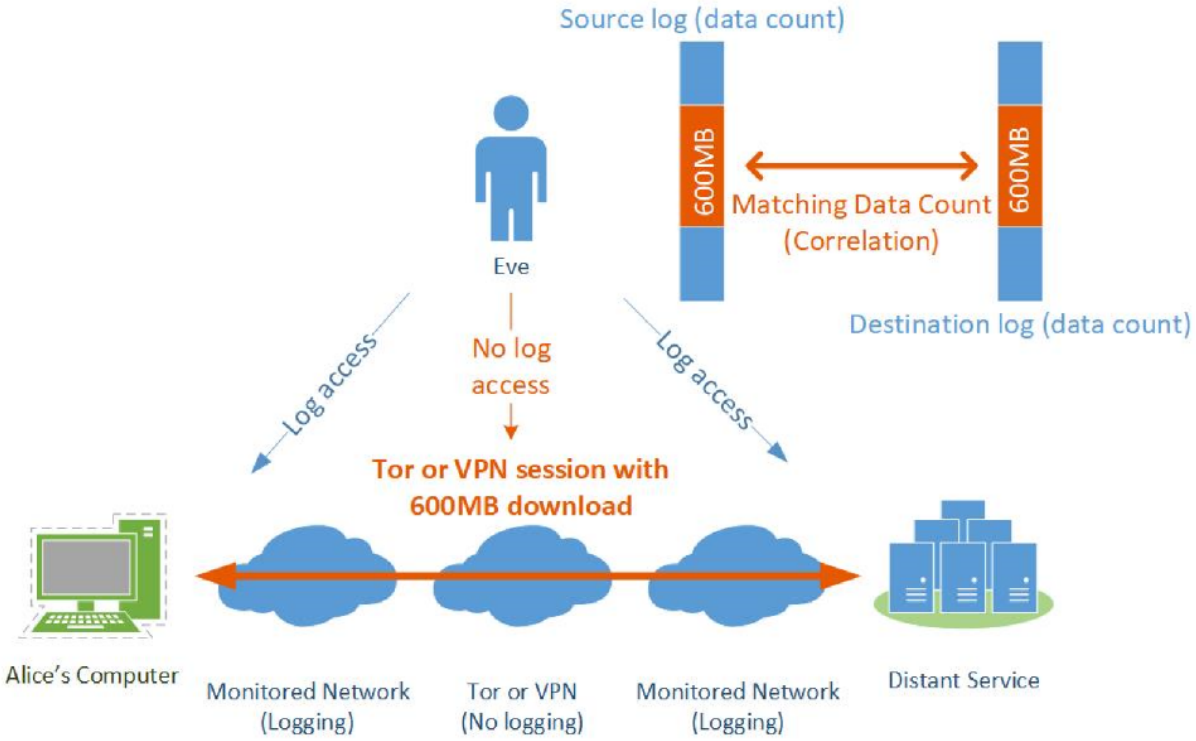
- **Корреляционная атака по цифровому отпечатку:** как упрощённо показано ниже, эта атака распознаёт ваш зашифрованный трафик Tor (например, посещённые сайты) по анализу зашифрованного трафика без его расшифровки. Некоторые из таких методов достигают 96% успешности **в закрытой среде**. **Эффективность этих методов в реальной открытой среде пока не доказана, и, вероятно, потребовала бы огромных вычислительных ресурсов, из-за чего маловероятно, что местный противник будет применять такие техники в ближайшем будущем.** Однако гипотетически такие методы может использовать продвинутый и, вероятно, глобальный противник с доступом к вашей исходной сети, чтобы определить часть вашей активности. Примеры таких атак описаны в нескольких научных работах[71][72][73], как и их ограничения[74]. Сам Tor Project опубликовал статью об этих атаках и некоторых мерах смягчения: blog.torproject.org Archive.org.



• **Корреляционные атаки по времени:** как упрощённо показано ниже, противник, имеющий доступ к журналам сетевых соединений (например, IP или DNS; помните, что большинство VPN-серверов и большинство узлов Tor известны и публично перечислены) у источника и у назначения, может сопоставить время событий и деанонимизировать вас без какого-либо доступа к сети Tor или VPN между ними. Реальный пример применения этой техники был у ФБР в 2013 году при деанонимизации[75] ложной угрозы взрыва в Гарвардском университете.



• **Корреляционные атаки по объёму:** как упрощённо показано ниже, противник, не имеющий доступа к подробным журналам соединений (он не видит, что вы использовали Tor или Netflix), но имеющий доступ к журналам учёта объёма данных, может увидеть, что вы скачали 600 МБ в определённые дату и время, совпадающие с загрузкой 600 МБ на стороне назначения. Затем такую корреляцию можно со временем использовать для деанонимизации.



Есть способы смягчить такие атаки, например:

• Не используйте Tor/VPN для доступа к сервисам, находящимся в той же сети (у того же провайдера), что и сервис назначения. Например, не подключайтесь к Tor из сети университета, чтобы анонимно получить доступ к университетскому сервису. Вместо этого используйте другую исходную точку, например публичный Wi-Fi, которую противнику будет трудно сопоставить.

• Не используйте Tor/VPN из явно сильно контролируемой сети, например корпоративной или государственной. Вместо этого попробуйте найти неконтролируемую сеть, такую как публичный Wi-Fi или домашний Wi-Fi.

• Рассмотрите использование нескольких уровней, например того, что далее будет рекомендовано в этом руководстве: VPN поверх Tor. Тогда противник может увидеть, что кто-то подключился к сервису через Tor, но не сможет увидеть, что это были вы, потому что вы были подключены к VPN, а не напрямую к сети Tor.

Снова помните: этого может быть недостаточно против мотивированного глобального противника[76] с широким доступом к массовой слежке по всему миру. Такой противник может иметь доступ к журналам независимо от того, где вы находитесь, и использовать их для деанонимизации. Обычно эти атаки относятся к тому, что называется атакой Сивиллы[77]. **Такие противники находятся за пределами этого руководства.**

Также помните, что все остальные методы, описанные в этом руководстве, например анализ поведения, тоже могут косвенно использоваться для деанонимизации пользователей Tor (см. также Ваш цифровой след).

Я также настоятельно рекомендую прочитать это очень хорошее, полное и подробное руководство по большинству известных векторов атак на Tor: github.com Archive.org, а также недавнюю исследовательскую публикацию researchgate.net Archive.org

А ещё вот эту отличную серию публикаций в блоге: hackerfactor.com Archive.org

Недавно одну из таких атак попытались провести против сети Tor; подробнее здесь: arstechnica.com Archive.org

Наконец, помните, что само использование Tor уже может считаться подозрительной активностью[78], а некоторые могут считать его использование вредоносным[79].

Далее руководство предложит некоторые меры смягчения таких атак через изменение исходной точки с самого начала, например через публичный Wi-Fi. Помните, что такие атаки обычно проводят высококвалифицированные, хорошо обеспеченные ресурсами и мотивированные противники, и они выходят за рамки этого руководства. Также рекомендуется узнать о практических корреляционных атаках в исполнении разведывательных служб: officercia.mirror.xyz Archive.org

Отказ от ответственности: также следует отметить, что Tor не предназначен для защиты от глобального противника.[80]

Анализ трафика и пределы Tor

Примечание: этот раздел расширяет раздел Анонимизация трафика выше. Далее следует более подробный разбор конкретных классов атак, которые имеют значение на практике.

Tor[29] обеспечивает сильную анонимность против большинства противников большую часть времени. Однако она не безусловна. Понимать, что это означает на практике и кто в реальности может быть таким противником, полезнее, чем либо отмахиваться от проблемы, либо замирать от страха перед ней.

Корреляционные атаки по времени

Базовая атака против сетей анонимности — корреляция трафика: если противник может наблюдать трафик, входящий в сеть Tor с вашего компьютера, и трафик, выходящий к месту назначения, он может сопоставить два потока по времени, объёму и шаблонам пакетов, вообще не взламывая шифрование Tor.

Murdoch и Danezis в 2005 году показали[81], что противник с относительно малыми ресурсами, контролирующий даже небольшое число узлов Tor, может использовать анализ времени, чтобы определить, какой узел использует скрытый сервис, резко сужая множество возможных анонимных участников. Это был ранний результат, и сеть Tor с тех пор значительно развилась, но основной принцип — корреляция между точками наблюдения не требует ничего расшифровывать — последующие исследования только подтвердили.

RAPTOR[82] (2015) показал, что противники на уровне автономных систем (AS) — крупные интернет-провайдеры и точки обмена трафиком, а не только разведывательные агентства — могут выполнять анализ трафика, наблюдая маршрутизацию BGP и выводя пересечение путей между пользователем Tor и его назначением. Ключевая идея в том, что одна и та же автономная система может нести и трафик пользователя к сторожевому узлу, и трафик выходного узла к назначению, что делает корреляцию возможной без компрометации какого-либо узла Tor.

DeepCorr (2018) использовал глубокое обучение для сопоставления потоков Tor со значительно большей точностью, чем предыдущие методы, достигая уровня корреляции выше 96% в контролируемых условиях. Авторы осторожно отмечают, что оценка проводилась в лабораторной закрытой среде — фиксированный набор сайтов, контролируемые условия — и что реальная работа против большой открытой сети с разнообразным трафиком была бы существенно сложнее. Это различие важно: показатели точности из закрытой среды часто неверно цитируют так, будто они применимы к реальным развёртываниям. Они к ним не применимы, по крайней мере пока.

Кто на практике является глобальным пассивным противником?

Настоящего глобального пассивного противника — того, кто одновременно может наблюдать произвольный интернет-трафик по всему миру, — не существует в той форме, в какой его часто представляют. Существуют национальные разведывательные агентства с широкой, но не безграничной видимостью интернет-трафика (TEMPORA у GCHQ, PRISM и программы upstream-сбора у NSA), крупные интернет-провайдеры и точки обмена трафиком, через которые проходит непропорционально большая доля мирового трафика, а также облачные провайдеры, чья инфраструктура охватывает большинство мировых путей автономных систем.

Для подавляющего большинства пользователей Tor ни одна из этих сущностей не нацелена на них специально. Для журналиста, который общается с источником внутри страны, чьи спецслужбы тесно сотрудничают с крупными западными агентствами, или для активиста, чей трафик проходит лишь через небольшое число путей автономных систем, картина тревожнее. Честный ответ таков: **если агентство Five Eyes целенаправленно охотится именно за вами, одного Tor, вероятно, недостаточно. Для всех остальных Tor обеспечивает сильную защиту.**

Распознавание сайтов по цифровому отпечатку

Атаки распознавания сайтов по цифровому отпечатку пытаются определить, какой сайт посещает пользователь Tor, анализируя шаблон зашифрованного трафика — размеры пакетов, время, последовательности направлений — без его расшифровки. Точность в оценках закрытой среды, где атакующий знает, что пользователь посещает один из N отслеживаемых сайтов, в исследованиях достигала высоких значений. В условиях открытой среды, где пользователь может посещать любой из миллионов сайтов, доля ложных срабатываний делает эти атаки гораздо менее практичными. WTF-PAD и связанные меры добавления маскирующего трафика, частично развёрнутые в Tor Browser, дополнительно снижают точность распознавания. Это активная область исследований, и ситуация будет меняться.

Постоянство сторожевых узлов и его значение

Tor использует **сторожевые узлы** — небольшой устойчивый набор входных узлов, которые ваш клиент повторно использует неделями, — именно для ограничения риска корреляции по времени. Если бы для каждой цепочки использовался случайный входной узел, противник, контролирующий даже умеренную долю узлов Tor, со временем напрямую увидел бы ваш вход в сеть. Сохраняя небольшой набор сторожевых узлов, Tor ограничивает вероятность того, что конкретный противник контролирует вашу входную точку. Компромисс в том, что если ваш сторожевой узел вредоносен или находится под наблюдением, это сохраняется на весь период его использования. В целом исследования Tor Project показывают, что постоянство сторожевых узлов улучшает анонимность для большинства людей большую часть времени.

Когда Tor достаточен, а когда нет

Tor достаточен против: наблюдателей в локальной сети (вашего провайдера, университета, Wi-Fi в кафе), большинства правоохранительных органов без партнёрств с разведывательными службами, коммерческих брокеров данных и рекламодателей.

Tor недостаточен против: целевой операции хорошо обеспеченного ресурсами национального разведывательного агентства с видимостью магистрального интернет-трафика, противника, который одновременно контролирует ваш сторожевой узел и выходной узел у назначения, или противника, способного сопоставить время вашего использования Tor с известными событиями в реальном мире (например, вы были единственным человеком в определённом месте в определённое время).

Самая практичная мера сверх самого Tor — сменить входную точку: подключение к Tor из публичного Wi-Fi, а не с домашнего подключения, полностью убирает из уравнения самый надёжный якорь корреляции — IP-адрес, выданный вашим провайдером. Для чувствительных действий это руководство повсюду рекомендует именно такой подход.

Некоторые устройства можно отслеживать даже офлайн

Вы видели это в боевиках, шпионских фильмах, научной фантастике и сериалах: главные герои всегда вынимают батарею из телефона, чтобы его нельзя было использовать. Большинство людей решило бы, что это перебор. Увы, нет: теперь это становится правдой хотя бы для некоторых устройств:

• iPhone и iPad (iOS 13 и выше)[83][84];

• телефоны Samsung (Android 10 и выше)[85];

• MacBook (macOS 10.15 и выше)[86].

Такие устройства продолжают передавать идентифицирующую информацию ближайшим устройствам даже в офлайн-режиме, используя Bluetooth Low Energy[87]. Они не имеют прямого доступа к устройствам (которые не подключены к интернету), а вместо этого используют BLE, чтобы находить их через другие находящиеся рядом устройства[88]. Они применяют одноранговую ближнюю связь Bluetooth, чтобы передавать свой статус через ближайшие онлайн-устройства.

Теперь такие устройства можно находить и сохранять их местоположение в какой-либо базе данных, которую затем третьи стороны или сами владельцы базы могут использовать для разных целей, включая аналитику, рекламу, сбор доказательств или разведывательной информации.

См. Предупреждение о смартфонах и умных устройствах.

Кратко: не берите такие устройства с собой, когда выполняете чувствительные действия.

Ваши аппаратные идентификаторы

Ваши IMEI и IMSI

IMEI (International Mobile Equipment Identity[89]) и IMSI (International Mobile Subscriber Identity[90]) — это уникальные номера, создаваемые производителями мобильных телефонов и операторами сотовой связи.

IMEI напрямую связан с телефоном, которым вы пользуетесь. Этот номер известен операторам сотовой связи, отслеживается ими и известен производителям. Каждый раз, когда телефон подключается к мобильной сети, он регистрирует в сети IMEI вместе с IMSI (если вставлена SIM-карта, хотя даже это не всегда требуется). Его также используют многие приложения, например банковские приложения, злоупотребляющие разрешением доступа к телефону на Android[91], и операционные системы смартфонов (Android/iOS) для идентификации устройства[92]. Изменить IMEI на телефоне возможно, но трудно (и во многих юрисдикциях не незаконно[93]); вероятно, проще и дешевле найти и купить старый рабочий одноразовый телефон за несколько евро (помните, это руководство ориентируется на Германию) на блошином рынке или в случайном маленьком магазине.

IMSI напрямую связан с мобильной подпиской или предоплаченным тарифом, которым вы пользуетесь, и привязан вашим мобильным оператором к вашему номеру телефона. IMSI жёстко записан на SIM-карте и не может быть изменён. Помните: каждый раз, когда телефон подключается к мобильной сети, он также регистрирует IMSI в сети вместе с IMEI. Как и IMEI, IMSI используется некоторыми приложениями и операционными системами смартфонов для идентификации и отслеживается. Например, некоторые страны ЕС ведут базу связей IMEI/IMSI для удобного поиска правоохранительными органами.

Сегодня передать кому-то свой настоящий номер телефона — то же самое или даже хуже, чем передать номер социального страхования, паспортный номер или номер национального удостоверения личности.

IMEI и IMSI можно связать с вами как минимум шестью способами:

- Журналы абонентов мобильного оператора обычно хранят IMEI вместе с IMSI и базой данных абонентской информации. Если вы используете анонимную предоплаченную SIM-карту (анонимный IMSI, но известный IMEI), оператор может понять, что этот телефон принадлежит вам, если раньше вы использовали его с другой SIM-картой (другой анонимный IMSI, но тот же известный IMEI).
- Журналы антенн мобильного оператора удобно хранят записи о том, какой IMEI и IMSI подключались, а также некоторые данные соединения. Например, они знают и записывают, что телефон с такой комбинацией IMEI/IMSI подключался к набору сотовых антенн, и насколько

сильным был сигнал к каждой из них; это позволяет легко выполнить триангуляцию и геолокацию сигнала. Они также знают, какие другие телефоны, например ваш настоящий, подключались в то же время к тем же антеннам с тем же уровнем сигнала. Это позволяет точно понять, что этот «одноразовый телефон» всегда был подключён в том же месте и в то же время, что и другой «известный телефон», который появляется каждый раз, когда используется одноразовый телефон. Эту информацию могут использовать и используют разные третьи стороны для довольно точной геолокации и отслеживания[94][95].

• Производитель телефона может отследить продажу телефона по IMEI, если телефон был куплен неанонимно. У производителя действительно есть журналы каждой продажи телефонов, включая серийный номер и IMEI, а также сведения о том, в какой магазин, какому человеку или кому именно он был продан. Если вы используете телефон, купленный онлайн или у человека, который вас знает, по этой информации его можно связать с вами. Даже если вас не найдут на записях камер наблюдения[96] и вы купили телефон за наличные, по журналам антенн всё равно можно узнать, какой другой телефон (ваш настоящий, лежавший в кармане) находился там, в магазине, в эти дату и время.

• Один только IMSI тоже может использоваться, чтобы найти вас, потому что большинство стран теперь требует предъявлять документ при покупке SIM-карты (по подписке или предоплаченной). IMSI затем привязывается к личности покупателя карты. В странах, где SIM-карту всё ещё можно купить за наличные, например в Великобритании, всё равно известно, где именно и когда она была куплена. Затем эту информацию можно использовать, чтобы получить данные из самого магазина, например записи камер наблюдения, как и в случае IMEI. Либо, опять же, журналы антенн можно использовать, чтобы выяснить, какой другой телефон был там в момент продажи.

• Разработчики операционных систем смартфонов (Google/Apple для Android/iOS) тоже хранят журналы идентификаций IMEI/IMSI, связанных с аккаунтами Google/Apple, и сведения о том, какой пользователь ими пользовался. Они также могут отследить историю телефона и аккаунты, к которым он был привязан в прошлом[97].

• Государственные ведомства по всему миру, заинтересованные в вашем номере телефона, могут использовать и используют[98] специальные устройства под названием «IMSI-перехватчики»[99], например Stingray[100] или более новый Nyxcell[101]. Эти устройства могут выдавать себя за сотовую антенну и принудительно заставлять конкретный IMSI (ваш телефон) подключиться к ним для доступа к сотовой сети. После этого они смогут применять разные атаки «человек посередине»[35], которые позволят им:

  • прослушивать ваш телефон (голосовые вызовы и SMS);

  • перехватывать и изучать ваш трафик данных;

  • выдавать себя за ваш номер телефона, не контролируя сам телефон.

Вот также хорошее видео YouTube на эту тему: DEFCON Safe Mode - Cooper Quintin - Detecting Fake 4G Base Stations in Real-Time Invidious

По этим причинам крайне важно получить отдельный анонимный номер телефона и/или анонимный одноразовый телефон с предоплаченной SIM-картой, купленной за наличные и никак не связанной с вами ни в прошлом, ни в настоящем, для выполнения чувствительных действий. Также можно получить анонимный, но желательно отдельный предоплаченный номер через бесплатные и платные онлайн-сервисы, принимающие анонимные криптовалюты вроде Monero. Более практические рекомендации см. здесь: Получение анонимного номера телефона.

Некоторые производители смартфонов, например Purism с серией Librem[102], заявляют, что учитывают вашу приватность, но всё равно не позволяют рандомизировать IMEI. Мы считаем это

ключевой функцией против отслеживания, которую такие производители должны предоставлять. Такая мера не предотвратит отслеживание IMSI на SIM-карте, но как минимум позволила бы оставлять тот же «одноразовый телефон» и менять только SIM-карты, вместо того чтобы ради приватности менять и телефон, и SIM-карту.

См. Предупреждение о смартфонах и умных устройствах.

Ваш MAC-адрес Wi-Fi или Ethernet

MAC-адрес[103] — это уникальный идентификатор, связанный с вашим физическим сетевым интерфейсом (проводной Ethernet или Wi-Fi). Разумеется, его можно использовать для отслеживания, если он не рандомизирован. Как и в случае с IMEI, производители компьютеров и сетевых карт обычно ведут журналы продаж, часто включая серийный номер, IMEI, MAC-адреса и т.п.; поэтому они снова могут отследить, где, когда и кому был продан компьютер с конкретным MAC-адресом. Даже если вы купили его за наличные в супермаркете, у супермаркета могут быть камеры наблюдения (или камера прямо снаружи магазина), а дата и время продажи снова могут использоваться, чтобы по журналам антенн мобильного оператора выяснить, кто там находился в тот момент (IMEI/IMSI).

Разработчики операционных систем (Google/Microsoft/Apple) тоже хранят в журналах сведения об устройствах и их MAC-адресах для идентификации устройств, например в сервисах типа «найти моё устройство». Apple может сказать, что MacBook с конкретным MAC-адресом раньше был привязан к конкретному Apple Account. Возможно, к вашему, до того как вы решили использовать MacBook для чувствительных действий. А возможно, к другому пользователю, который продал его вам, но помнит вашу электронную почту или номер с момента продажи.

Ваш домашний маршрутизатор или точка доступа Wi-Fi ведёт журналы устройств, зарегистрированных в Wi-Fi, и к ним тоже можно получить доступ, чтобы выяснить, кто пользовался вашим Wi-Fi. Иногда это можно сделать удалённо и незаметно со стороны провайдера, в зависимости от того, управляет ли он этим маршрутизатором или точкой доступа удалённо. Такое часто бывает, когда провайдер сам выдаёт маршрутизатор клиентам.

Некоторые коммерческие устройства записывают MAC-адреса, которые появляются поблизости, для разных целей, например для оценки дорожных заторов[104].

Поэтому снова важно не брать телефон с собой туда, где вы выполняете чувствительные действия. Если вы используете собственный ноутбук, крайне важно скрывать его MAC-адрес (и адрес Bluetooth) везде, где вы им пользуетесь, и быть особенно осторожным, чтобы не раскрыть никакую информацию. К счастью, многие современные операционные системы теперь имеют или позволяют включить рандомизацию MAC-адресов (Android, iOS, Linux и Windows 10/11); заметное исключение — macOS, которая не поддерживает эту функцию даже в последней версии Big Sur.

См. Предупреждение о смартфонах и умных устройствах.

Ваш MAC-адрес Bluetooth

Ваш MAC-адрес Bluetooth похож на описанный выше MAC-адрес, только относится к Bluetooth. Его тоже можно использовать для отслеживания, поскольку производители и разработчики операционных систем хранят такие сведения. Его можно связать с местом, датой и временем продажи или с аккаунтами, а затем использовать для отслеживания вместе с платёжной информацией магазина, камерами наблюдения или журналами мобильных антенн.

В операционных системах есть защиты для рандомизации таких адресов, но они всё ещё подвержены уязвимостям[105].

По этой причине, если Bluetooth вам действительно не нужен, лучше полностью отключить его в настройках BIOS/UEFI, если это возможно, или иначе в операционной системе.

В Windows 10, чтобы принудительно рандомизировать адрес при следующем использовании и предотвратить отслеживание, нужно отключить и снова включить устройство Bluetooth непосредственно в диспетчере устройств.

В целом это не должно быть такой большой проблемой по сравнению с MAC-адресами. Адреса Bluetooth рандомизируются довольно часто.

См. Предупреждение о смартфонах и умных устройствах.

Ваш процессор

Все современные процессоры[106] теперь включают скрытые платформы управления, такие как печально известный Intel Management Engine[107] и AMD Platform Security Processor[108].

Эти платформы управления — небольшие операционные системы, работающие прямо на вашем процессоре, пока на него подаётся питание. Они имеют полный доступ к сети вашего компьютера, и противник может получить к ним доступ, чтобы деанонимизировать вас разными способами, например через прямой доступ или вредоносное ПО, как показано в этом поучительном видео: BlackHat, How to Hack a Turned-Off Computer, or Running Unsigned Code in Intel Management Engine youtube.com Invidious.

В прошлом они уже затрагивались несколькими уязвимостями безопасности[109], которые позволяли вредоносному ПО получать контроль над целевыми системами. Многие защитники приватности, включая EFF и Libreboot, также обвиняют их в том, что они являются скрытым входом в любую систему[110].

Есть не самые простые способы[111] отключить Intel IME на некоторых процессорах, и если можете, стоит это сделать. На некоторых ноутбуках с AMD это можно отключить в настройках BIOS, отключив PSP.

Отметим в защиту AMD: для ASP не были найдены уязвимости безопасности и скрытые входы. См. youtube.com Invidious. Кроме того, AMD PSP, в отличие от Intel IME, не предоставляет возможностей удалённого управления.

Если вы чувствуете себя чуть более смело, можно установить собственный BIOS с помощью Coreboot[112] или Libreboot (дистрибутива Coreboot), если ваш ноутбук это поддерживает. Coreboot позволяет добавить собственный микрокод или другие двоичные компоненты прошивки, необходимые для работы машины, но это остаётся выбором пользователя; по состоянию на декабрь 2022 года Libreboot принял похожий прагматичный подход, чтобы поддерживать более

новые устройства в дереве Coreboot. (Спасибо доброму анониму, который исправил предыдущую информацию в этом абзаце.)

Проверьте сами:

• Если вы используете Linux, можно проверить состояние уязвимости процессора к атакам Spectre/Meltdown с помощью github.com Archive.org. Этот инструмент доступен как пакет для большинства дистрибутивов Linux, включая Whonix. Spectre — это атака временного выполнения. Также есть демонстрационный код для Spectre v1 и v2 на устройствах iPhone здесь: github.com Archive.org и здесь misc0110.net Archive.org

• Если вы используете Windows, можно проверить состояние уязвимости процессора с помощью inSpectre grc.com Archive.org

У некоторых процессоров есть неисправимые недостатки, особенно у процессоров Intel, которые может использовать разное вредоносное ПО. Вот хороший актуальный список таких уязвимостей, затрагивающих распространённые современные процессоры: en.wikipedia.org Wikiless Archive.org

Некоторых из них можно избежать настройками программ виртуализации, которые смягчают такие эксплойты. Подробнее см. руководство Spectre/Meltdown Hardening Archive.org (предупреждение: это может серьёзно повлиять на производительность ваших виртуальных машин).

Это руководство не будет слишком глубоко погружаться в побочные каналы и микроархитектурные атаки, но мы обозначим некоторые проблемы архитектур процессоров Intel и AMD, которые будут смягчаться далее. Важно понимать: аппаратное обеспечение так же подвержено ошибкам, а значит и эксплуатации, независимо от производителя.

Некоторые из этих проблем мы будем смягчать, рекомендуя использовать виртуальные машины на отдельном анонимном ноутбуке для чувствительных действий, который будет использоваться только из анонимной публичной сети.

Кроме того, мы рекомендуем использовать процессоры AMD вместо процессоров Intel. Подробнее см. Типы атак на процессор.

• Уязвимости процессоров, найденные за последние несколько лет:

  • Meltdown
  • Spectre
  • Æpic
  • SGAxe
  • LVI
  • Plundervolt
  • MicroScope replay attack
  • Enclave
  • Prime+Probe
  • Crosstalk
  • Hertzbleed
  • Squip attack
  • Zenbleed

Телеметрия вашей ОС и приложений

Будь то Android, iOS, Windows, macOS или даже Ubuntu, большинство популярных операционных систем теперь по умолчанию собирают телеметрию, даже если вы никогда не давали согласия или с самого начала отказались от сбора[113]. Некоторые, например Windows, даже не позволяют полностью отключить телеметрию без технических ухищрений. Этот сбор информации может быть обширным и включать поразительное количество подробностей (метаданных и данных) о ваших устройствах и их использовании.

Вот хорошие обзоры того, что собирается этими пятью популярными ОС в последних версиях:

• Android/Google:

  • Просто прочитайте их политику конфиденциальности: policies.google.com Archive.org

  • School of Computer Science & Statistics, Trinity College Dublin, Ireland Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google scss.tcd.ie Archive.org

• iOS/Apple:

  • Подробнее: apple.com Archive.org и support.apple.com Archive.org

  • School of Computer Science & Statistics, Trinity College Dublin, Ireland Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google scss.tcd.ie Archive.org

  • Apple утверждает[114], что обезличивает эти данные с помощью дифференциальной приватности[115], но вам придётся поверить им на слово.

• Windows/Microsoft:

  • Полный список обязательных диагностических данных: docs.microsoft.com Archive.org

  • Полный список необязательных диагностических данных: docs.microsoft.com Archive.org

• macOS:

  • Подробнее: support.apple.com Archive.org

• Ubuntu:

  • Ubuntu, несмотря на то что это дистрибутив Linux, сегодня тоже собирает телеметрию. Однако эти данные довольно ограничены по сравнению с остальными. Подробнее: ubuntu.com Archive.org

Телеметрию собирают не только операционные системы, но и сами приложения, установленные в вашей системе: браузеры, почтовые клиенты, приложения социальных сетей.

Важно понимать, что эти телеметрические данные можно связать с вашим устройством; они могут помочь деанонимизировать вас и позднее использоваться против вас противником, который получит к ним доступ.

Это не означает, например, что устройства Apple — ужасный выбор для хорошей приватности (хотя это может меняться[116]), но они точно не лучший выбор для относительной анонимности. Они могут защищать вас от того, чтобы третьи стороны знали, что вы делаете, но не от них самих. С высокой вероятностью они точно знают, кто вы.

Позже в этом руководстве мы используем все доступные нам средства, чтобы отключить и заблокировать как можно больше телеметрии и смягчить этот вектор атаки в операционных системах, поддерживаемых этим руководством. Это будет касаться Windows, macOS и в некоторой степени даже Linux.

См. Предупреждение о смартфонах и умных устройствах.

Ваши умные устройства

Вы уже поняли: ваш смартфон — продвинутое устройство слежки и отслеживания, которое:

• записывает всё, что вы говорите в любое время («Hey Siri», «Hey Google»);

• записывает ваше местоположение везде, куда вы ходите;

• постоянно записывает другие устройства вокруг вас (устройства Bluetooth, точки доступа Wi-Fi);

• записывает ваши привычки и данные о здоровье (шаги, экранное время, контакт с заболеваниями, данные подключённых устройств);

• записывает все ваши сетевые местоположения;

• записывает все ваши фотографии и видео, и, скорее всего, где они были сделаны;

• скорее всего, имеет доступ к большинству ваших известных аккаунтов, включая социальные сети, мессенджеры и финансовые аккаунты.

Данные передаются даже если вы отказались от сбора[113], обрабатываются и хранятся бессрочно (скорее всего, без шифрования[117]) разными третьими сторонами[118].

Но это ещё не всё. Этот раздел называется не «Смартфоны», а «Умные устройства», потому что за вами следит не только смартфон. Это также любое другое умное устройство, которое у вас может быть:

• умные часы? (Apple Watch, Android Smartwatch...);

• фитнес-устройства и приложения[119][120]? (Strava[121][122], Fitbit[123], Garmin, Polar[124]...);

• умная колонка? (Amazon Alexa[125], Google Echo, Apple Homepod...);

• умный транспорт? (автомобиль? самокат?);

• умные метки? (Apple AirTag, Galaxy SmartTag, Tile...);

• автомобиль? (Да, у большинства современных автомобилей сегодня есть развитые функции записи и отслеживания[126]);

• любое другое умное устройство? Существуют даже удобные поисковые системы, специально предназначенные для их поиска в интернете:

  • shodan.io

  • censys.io

  • zoomeye.org

См. Предупреждение о смартфонах и умных устройствах.

Вывод: не берите умные устройства с собой, когда выполняете чувствительные действия.

Вы сами

Ваши метаданные

Что такое метаданные? Каждый файл, который вы создаёте или передаёте, несёт метаданные — структурированные данные, встроенные в содержимое или находящиеся рядом с ним, которые описывают, как, когда, где и с помощью чего файл был создан. При обычном использовании эти метаданные невидимы, и о них регулярно забывают. Они уже подставляли журналистские источники, устанавливали информаторов и связывали анонимные документы с их авторами. Инструменты для удаления метаданных существуют, и пользоваться ими несложно. Почти всегда провал происходит из-за незнания, что метаданные вообще были внутри.

Самый часто цитируемый случай — установление в 2013 году источника утечки у подрядчика правительства США по метаданным в документе Word, отправленном в The Intercept[127]. Метаданные печати документа содержали серийный номер, который можно было связать с конкретным принтером, вместе с микроточечными шаблонами отслеживания на самой распечатке; но тот же принцип применим и к цифровым метаданным. Ранее, в 2003 году, в досье правительства Великобритании о возможностях Ирака в области вооружений обнаружили историю правок с именами госслужащих, которые его редактировали. Это вызвало серьёзное политическое смущение[128] и показало, что проблема существовала задолго до широкой осведомлённости о ней.

Ваши метаданные — это вся информация о вашей активности без фактического содержания этой активности. Например, это похоже на знание того, что вам звонил онколог, а после этого вы последовательно звонили семье и друзьям. Вы не знаете, что именно было сказано в разговоре, но по одним метаданным можете догадаться, о чём он был[129].

В эти метаданные часто входит и ваше местоположение, собираемое смартфонами, операционными системами (Android[130]/iOS), браузерами, приложениями и сайтами. Вероятно, несколько компаний точно знают, где вы находитесь в любой момент[131], из-за вашего смартфона[132].

Эти данные о местоположении уже использовались во многих судебных делах[133] в рамках «геозонных ордеров»[134], которые позволяют правоохранительным органам запрашивать у компаний, например Google/Apple, список всех устройств, находившихся в определённом месте в определённое время. Кроме того, такие данные о местоположении частные компании даже продают военным, которые затем могут удобно ими пользоваться[135]. Эти ордера всё шире применяются правоохранительными органами[136][137][138].

Если хотите сами представить, как выглядит «геозонный ордер», вот пример: wigle.net.

Теперь допустим, вы используете VPN, чтобы скрыть свой IP-адрес. Платформа социальной сети знает, что вы были активны в этой учётной записи 4 ноября с 8 утра до 13:00 с IP-адреса этого VPN. VPN якобы не ведёт журналы и не может связать этот VPN-IP с вашим IP-адресом. Однако ваш провайдер знает или по крайней мере может знать, что вы были подключены к тому же VPN-провайдеру 4 ноября с 7:30 до 14:00, но не знает, что вы через него делали.

Вопрос: есть ли где-нибудь кто-то, у кого обе части информации доступны[139] для корреляции в удобной базе данных?

Слышали об Edward Snowden[140]? Сейчас самое время погуглить его и прочитать его книгу[141]. Также почитайте про XKEYSCORE[142][143], MUSCULAR[144], SORM[145], Tempora[146] и PRISM[147].

См. «We kill people based on Metadata»[148] или этот известный твит IDF twitter.com Archive.org Nitter.

См. Смартфоны для предупреждения об использовании смартфонов и других умных устройств. См. Аудит метаданных, чтобы узнать, как избавиться от метаданных; вероятно, именно это и привело вас к этому разделу.

Ваш цифровой след

Это тот раздел, ради которого стоит посмотреть документальный фильм «The Social Dilemma»[149] на Netflix: там эта тема раскрыта лучше, чем у кого-либо ещё.

Сюда входит то, как вы пишете (стилометрия)[150][151], как вы себя ведёте[152][153], как кликаете, как просматриваете сайты, какие шрифты используете в браузере[154]. Распознавание по цифровому отпечатку используется, чтобы угадывать, кто человек, по его поведению. Вы можете использовать определённые педантичные слова или делать конкретные орфографические ошибки, которые выдадут вас через простой поиск Google по похожим признакам, потому что пять лет назад вы писали похожим образом в каком-нибудь посте Reddit с не очень анонимной учётной записи[155]. Одни только слова, которые вы вводите в поисковую систему, могут быть использованы против вас: у властей теперь бывают ордера на поиск людей, использовавших конкретные ключевые слова в поисковиках[156].

Платформы социальных сетей вроде Facebook/Google могут пойти ещё дальше и записывать ваше поведение прямо в браузере. Например, они могут записывать всё, что вы печатаете, даже если вы это не отправляете и не сохраняете. Вспомните черновик письма в Gmail: он сохраняется автоматически по мере набора. Они также могут записывать ваши клики и движения курсора.

В большинстве случаев для этого им достаточно включённого JavaScript в вашем браузере, а он включён по умолчанию в большинстве браузеров, включая Tor Browser. Даже при отключённом JavaScript всё ещё есть способы распознать вас по цифровому отпечатку[157].

Хотя такие методы обычно применяются для маркетинга и рекламы, они также могут быть полезным инструментом для распознавания пользователей. Ваше поведение уникально или достаточно уникально, чтобы со временем вас можно было деанонимизировать.

Вот несколько примеров:

- Специализированные компании продают, например, правоохранительным органам продукты для анализа активности в социальных сетях, такие как mediasonar.com Archive.org
- Например, в качестве основы аутентификации скорость набора пользователя, характер нажатий клавиш, шаблоны ошибок (скажем, случайное нажатие «l» вместо «k» в трёх из каждых семи операций) и движения мыши образуют уникальный поведенческий шаблон этого человека[158]. Некоторые коммерческие сервисы, например TypingDNA (typingdna.com Archive.org), даже предлагают такой анализ как замену двухфакторной аутентификации.
- Эта технология также широко используется в сервисах CAPTCHA[159], чтобы проверять, что вы «человек», и может использоваться для распознавания пользователя по цифровому отпечатку.
- См. Противодействие криминалистической лингвистике.

Затем алгоритмы анализа могут использоваться, чтобы сопоставлять эти шаблоны с другими людьми и связывать вас с другим известным пользователем. Неясно, используются ли такие данные уже сейчас правительствами и правоохранительными органами, но в будущем это возможно. И хотя сейчас это в основном применяется для рекламы, маркетинга и CAPTCHA, в краткосрочной или среднесрочной перспективе это может и, вероятно, будет использоваться в расследованиях для деанонимизации пользователей.

Вот забавный пример, который можно попробовать самому, чтобы увидеть некоторые из этих вещей в действии: clickclickclick.click (извините, архивной ссылки здесь нет). Со временем он становится интереснее (требуется включённый JavaScript).

Вот также свежий пример, просто показывающий, что Google Chrome собирает о вас: web.archive.org

Если вы не можете посмотреть документальный фильм, вот другие ресурсы по теме:

• 2017, Behavior Analysis in Social Networks, link.springer.com Archive.org

• 2017, Social Networks and Positive and Negative Affect sciencedirect.com Archive.today

• 2015, Using Social Networks Data for Behavior and Sentiment Analysis researchgate.net Archive.org

• 2016, A Survey on User Behavior Analysis in Social Networks academia.edu Archive.org

• 2017, презентация DEF CON 25: DEF CON 25 - Svea Eckert, Andreas Dewes - Dark Data Invidious

• 2019, Influence and Behavior Analysis in Social Networks and Social Media sci-hub.se Archive.org

Итак, как это смягчить?

• Это руководство предложит некоторые технические меры с использованием инструментов, устойчивых к распознаванию по цифровому отпечатку, но их может быть недостаточно.

• Нужно применять здравый смысл, искать собственные поведенческие шаблоны и вести себя иначе при использовании анонимных идентичностей. Это включает:

  • то, как вы печатаете (скорость, точность...);

  • слова, которые вы используете (осторожнее с привычными выражениями);

  • тип ответов, который вы используете (если по умолчанию вы саркастичны, попробуйте другой подход в своих идентичностях);

  • то, как вы пользуетесь мышью и кликаете (попробуйте решать CAPTCHA иначе, чем обычно);

  • привычки при использовании некоторых приложений или посещении сайтов (не всегда используйте одни и те же меню, кнопки и ссылки, чтобы добраться до содержимого);

  • ...

Вам нужно действовать и полностью принимать роль, как актёр на сцене. Вам нужно стать другим человеком, думать и действовать как этот человек. Это не техническая мера, а человеческая. Здесь вы можете полагаться только на себя.

В конечном счёте именно от вас в основном зависит, сможете ли вы обмануть эти алгоритмы, выработав новые привычки и не раскрывая реальную информацию при использовании анонимных идентичностей. См. Противодействие криминалистической лингвистике.

Реальная жизнь и OSINT

Это подсказки, которые вы можете со временем дать и которые могут указывать на вашу настоящую личность. Вы можете разговаривать с кем-то или публиковать сообщения на доске, форуме или Reddit. В таких публикациях со временем можно раскрыть информацию о реальной жизни. Это могут быть воспоминания, опыт или подсказки, которыми вы поделились и которые затем позволят мотивированному противнику построить профиль и сузить поиск.

Реальный и хорошо задокументированный пример — арест хакера Jeremy Hammond[160], который со временем раскрыл несколько деталей своего прошлого, а позже был обнаружен.

Есть также несколько случаев, связанных с OSINT в Bellingcat[161]. Посмотрите их очень информативный, хотя немного устаревший, набор инструментов здесь: docs.google.com Archive.org

В нашем сообществе Matrix есть комната для обсуждения OSINT. Можно присоединиться по адресу `#OSINT:matrix.org`.

Также можно посмотреть удобные списки доступных OSINT-инструментов, например чтобы попробовать их на себе:

• github.com Archive.org

• web.archive.org

• osintframework.com

• recontool.org

А также интересный плейлист на YouTube: youtube.com Invidious

И эти интересные подкасты:

inteltechniques.com

Никогда не делитесь через анонимные идентичности реальными индивидуальными переживаниями или деталями, которые позже могут привести к установлению вашей настоящей личности. Подробнее об этом будет в разделе Создание новых идентичностей.

Ваше лицо, голос, биометрия и фотографии

«Ад — это другие люди»: даже если вы обойдёте все перечисленные выше методы, вы ещё не в безопасности из-за повсеместного использования продвинутого распознавания лиц всеми подряд.

Компании вроде Facebook годами использовали продвинутое распознавание лиц[162][163] и применяли другие средства, например спутниковые снимки, чтобы создавать карты «людей» по всему миру[164]. Эта эволюция шла годами, и теперь мы можем сказать: «мы потеряли контроль над своими лицами»[165].

Если вы гуляете в туристическом месте, вы, скорее всего, окажетесь в чьём-то селфи уже через несколько минут, даже не зная об этом. Затем этот человек может загрузить селфи на разные платформы (Twitter, Google Photos, Instagram, Facebook, Snapchat...). Эти платформы применят к снимкам алгоритмы распознавания лиц под предлогом более удобной разметки людей или лучшей организации фототеки. Кроме того, тот же снимок даст точную временную метку и в большинстве случаев геолокацию места, где он был сделан. Даже если человек не предоставит временную метку и геолокацию, их всё равно можно угадать другими средствами[166][167].

Вот несколько ресурсов, чтобы даже попробовать это самостоятельно:

• Bellingcat, Guide To Using Reverse Image Search For Investigations: bellingcat.com Archive.org

• Bellingcat, Using the New Russian Facial Recognition Site SearchFace bellingcat.com Archive.org

• Bellingcat, Dali, Warhol, Boshirov: Determining the Time of an Alleged Photograph from Skripal Suspect Chepiga bellingcat.com Archive.org

• Bellingcat, Advanced Guide on Verifying Video Content bellingcat.com Archive.org

• Bellingcat, Using the Sun and the Shadows for Geolocation bellingcat.com Archive.org

• Bellingcat, Navalny Poison Squad Implicated in Murders of Three Russian Activists bellingcat.com Archive.org

• Bellingcat, Berlin Assassination: New Evidence on Suspected FSB Hitman Passed to German Investigators bellingcat.com Archive.org

• Bellingcat, Digital Research Tutorial: Investigating a Saudi-Led Coalition Bombing of a Yemen Hospital youtube.com Invidious

• Bellingcat, Digital Research Tutorial: Using Facial Recognition in Investigations youtube.com Invidious

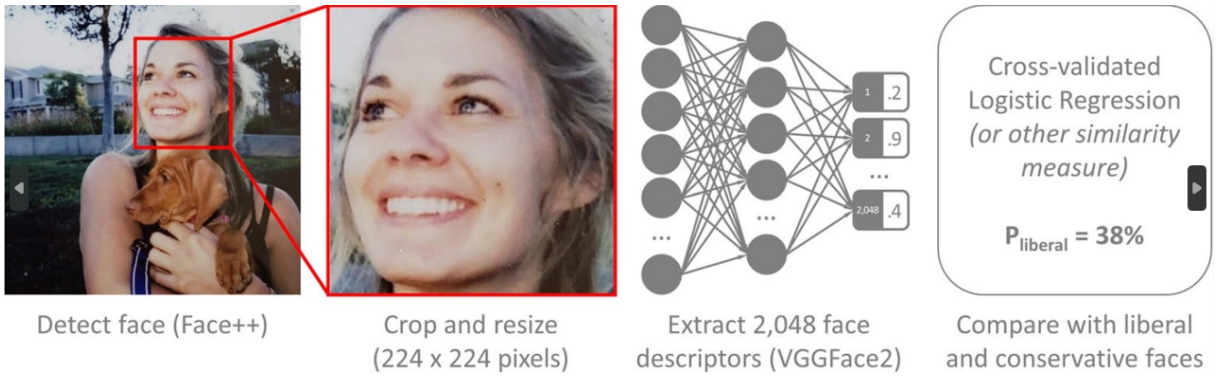
• Bellingcat, Digital Research Tutorial: Geolocating (Allegedly) Corrupt Venezuelan Officials in Europe youtube.com Invidious

Распознавание походки и другая дальнодействующая биометрия

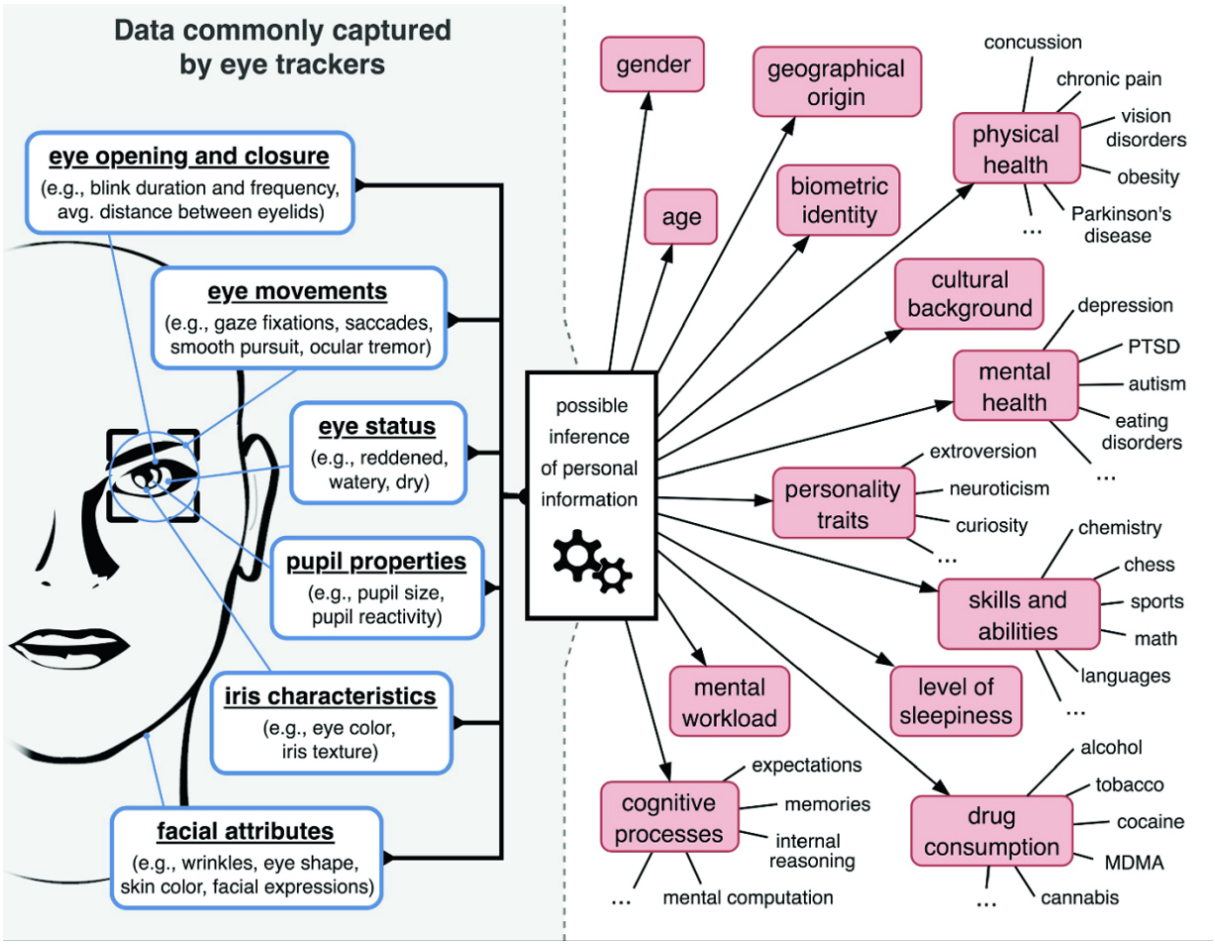
Даже если вы не смотрите в камеру, они всё равно могут выяснить, кто вы[168], распознать ваши эмоции[169], проанализировать походку[170][171][172], прочитать по губам[173], проанализировать поведение глаз[174] и, вероятно, угадать политические взгляды[175][176].

Вопреки массовым представлениям и поп-культуре, современные системы распознавания походки нельзя обмануть простой сменой походки, например положив что-то неудобное в обувь: они анализируют, как мышцы всего тела движутся при выполнении определённых действий. Лучший способ обмануть современное распознавание походки — носить свободную одежду, скрывающую движение мышц при действиях.

Для идентификации могут использоваться и другие признаки, например мочки ушей, которые на самом деле более индивидуальны, чем отпечатки пальцев, или даже форма черепа. Поэтому мягкие головные уборы вроде балаклав не рекомендуются для сокрытия личности: они выглядят крайне подозрительно и при этом повторяют форму черепа.



(Иллюстрация из nature.com Archive.org)



(Иллюстрация из rd.springer.com Archive.org)

Эти платформы (Google/Facebook) уже знают, кто вы, по нескольким причинам:

• потому что у вас есть или был профиль у них, и вы сами себя идентифицировали;

• даже если вы никогда не создавали профиль на этих платформах, он у вас всё равно есть, хотя вы об этом не знаете[177][178][179][180][181];

• потому что другие люди отмечали или идентифицировали вас на своих фотографиях с праздников или вечеринок;

• потому что другие люди добавили вашу фотографию в список контактов, которым затем поделились с платформой.

Вот также показательная демонстрация Microsoft Azure, которую можно попробовать самостоятельно: azure.microsoft.com. Она позволяет распознавать эмоции и сравнивать лица на разных фотографиях.

Правительства уже знают, кто вы, потому что у них есть ваши фотографии из удостоверения личности, паспорта или водительских прав, а часто и добавленная в базу биометрия, например отпечатки пальцев. Эти же правительства интегрируют такие технологии, часто предоставленные частными компаниями вроде израильской Oosto[182], Clearview AI[183][184] или NEC[185], в сети камер наблюдения для поиска «лиц, представляющих интерес»[186]. Некоторые государства с крайне высоким уровнем слежки, например Китай, внедрили широкое использование распознавания лиц для разных целей[187][188], включая, возможно, выявление этнических меньшинств[189]. Простая ошибка алгоритма распознавания лиц может разрушить вашу жизнь[190][191].

Вот несколько ресурсов о техниках, которые сегодня используют правоохранительные органы:

• видео CCC, объясняющее современные возможности слежки правоохранительных органов: media.ccc.de Archive.org

• EFF SLS: eff.org Archive.org

Apple делает FaceID массовым и продвигает его использование для входа во многие сервисы, включая банковские системы.

То же происходит с аутентификацией по отпечатку пальца, которую многие производители смартфонов делают массовой. Простая фотография, на которой видны ваши пальцы, может использоваться для деанонимизации[192][193][194][195].

То же касается вашего голоса, который можно анализировать для разных целей, как показано в недавнем патенте Spotify[196].

Даже радужная оболочка глаза в некоторых местах может использоваться для идентификации[197].

Можно легко представить недалёкое будущее, где вы не сможете создавать учётные записи или входить куда-либо без предоставления уникальной биометрии (подходящее время пересмотреть Gattaca[198], Person of Interest[199] и Minority Report[200]). И можно легко представить, насколько полезны такие большие биометрические базы данных могут быть заинтересованным третьим сторонам.

Кроме того, всю эту информацию можно использовать против вас, если вы уже деанонимизированы, с помощью deepfake[201]: создавая ложную информацию — фотографии, видео, голосовые записи[202]... Это уже применялось для таких целей[203][204]. Для этого даже доступны коммерческие сервисы, например respeecher.com Archive.org и descript.com Archive.org.

См. эту демонстрацию: youtube.com Invidious

На данный момент есть несколько шагов[205], которые можно использовать, чтобы смягчить, и только смягчить, распознавание лиц во время чувствительных действий там, где могут быть камеры наблюдения:

• Носите медицинскую маску: доказано, что она обходит некоторые технологии распознавания лиц[206], но не все[207].

• Носите бейсболку или шляпу, чтобы снизить вероятность идентификации камерами, снимающими сверху, которые могут записать ваше лицо. Помните, что это не поможет против камер, направленных спереди.

• Носите солнцезащитные очки вместе с маской и бейсболкой, чтобы снизить вероятность идентификации по особенностям глаз.

• Рассмотрите специальные солнцезащитные очки (к сожалению, дорогие) под названием Reflectacles: reflectacles.com Archive.org. Небольшое исследование показало их эффективность против распознавания лиц IBM и Amazon[208].

• Всё это всё равно может оказаться бесполезным из-за упомянутого ранее распознавания походки, но здесь есть надежда, если у вас есть 3D-принтер: gitlab.com Archive.org

(см. Распознавание походки и другая дальнодействующая биометрия)

(Обратите внимание: если вы собираетесь использовать эти меры там, где установлены продвинутые системы распознавания лиц, сами эти меры могут пометить вас как подозрительного и вызвать проверку человеком.)

Фишинг и социальная инженерия

Фишинг[209] — это тип атаки социальной инженерии[210], при котором противник пытается вытянуть из вас информацию, притворяясь чем-то или кем-то другим.

Типичный случай — противник использует атаку «человек посередине»[35] или поддельное письмо/звонок, чтобы попросить у вас учётные данные для сервиса. Например, это может происходить по электронной почте или через имитацию финансовых сервисов.

Такие атаки также могут использоваться для деанонимизации человека: его обманом заставляют скачать вредоносное ПО или со временем раскрыть личную информацию. Единственная защита — не попадаться на них и пользоваться здравым смыслом.

Их бесчисленное количество раз применяли с ранних дней интернета; обычный вариант называется «419 scam» (см. en.wikipedia.org Wikiless Archive.org).

Вот хорошее видео, если хотите немного больше узнать о типах фишинга: Black Hat, Ichthyology: Phishing as a Science youtube.com Invidious.

Вредоносное ПО, эксплойты и вирусы

Вредоносное ПО в ваших файлах, документах и письмах

С помощью стеганографии или других техник вредоносное ПО легко встроить в распространённые форматы файлов, такие как документы Office, изображения, видео, PDF-документы...

Это могут быть как простые HTML-ссылки для отслеживания, так и сложное целевое вредоносное ПО.

Это могут быть простые изображения размером в один пиксель[211], спрятанные в ваших письмах, которые обращаются к удалённому серверу, чтобы попытаться получить ваш IP-адрес.

Это может быть эксплуатация уязвимости в устаревшем формате или устаревшей программе чтения[212]. Затем такие эксплойты могут использоваться для компрометации вашей системы.

Вот хорошие видео с дополнительными объяснениями по теме:

• What is a File Format? youtube.com Invidious

• Ange Albertini: Funky File Formats: youtube.com Invidious

Всегда проявляйте крайнюю осторожность. См. Виртуализация, чтобы смягчить утечку любой информации даже в случае открытия такого вредоносного файла.

Если хотите узнать, как пытаться обнаруживать такое вредоносное ПО, см. Проверка файлов на вредоносное ПО.

Вредоносное ПО и эксплойты в ваших приложениях и сервисах

Итак, вы используете Tor Browser или Brave Browser поверх Tor. Возможно, вы используете их поверх VPN для дополнительной безопасности. Но нужно помнить, что существуют эксплойты[213] (взломы), о которых может знать противник, но не знать поставщик приложения или браузера. Такие эксплойты могут использоваться для компрометации вашей системы и раскрытия деталей, позволяющих деанонимизировать вас, например вашего IP-адреса или другой информации.

Реальный пример применения этой техники — дело Freedom Hosting[214] в 2013 году, когда ФБР внедрило вредоносное ПО[215] через эксплойт браузера Firefox на сайте Tor. Этот эксплойт позволил раскрыть данные некоторых пользователей. Более свежий заметный пример — взлом SolarWinds[216], когда несколько учреждений правительства США были скомпрометированы через внедрение вредоносного ПО на официальный сервер обновления программ.

В некоторых странах вредоносное ПО просто обязательно и/или распространяется самим государством. Так, например, происходит в Китае с WeChat[217], который затем можно использовать вместе с другими данными для государственной слежки[218].

За годы было бесчисленное количество примеров вредоносных расширений браузера, приложений для смартфонов и разных приложений, заражённых вредоносным ПО.

Вот несколько шагов для смягчения такого типа атак:

- Никогда не доверяйте используемым приложениям на 100%.
- Перед использованием всегда проверяйте, что вы используете обновлённую версию таких приложений, и в идеале проверяйте каждую загрузку по подписи, если она доступна.
- Не используйте такие приложения напрямую на физической системе; вместо этого используйте виртуальную машину для изоляции.

Чтобы отразить эти рекомендации, далее руководство будет вести вас к использованию виртуализации (см. Виртуализация), чтобы даже если ваш браузер или приложения будут скомпрометированы умелым противником, он оказался заперт в песочнице[219] без возможности получить доступ к идентифицирующей информации или скомпрометировать вашу систему.

Вредоносные USB-устройства

В продаже уже доступны коммерческие и дешёвые устройства «badUSB»[220], которые могут устанавливать вредоносное ПО, записывать то, что вы печатаете, определять ваше местоположение, слушать вас или получать контроль над ноутбуком просто при подключении. Вот примеры, которые уже можно купить самостоятельно:

- Hak5, USB Rubber Ducky shop.hak5.org Archive.org
- Hak5, O.MG Cable youtube.com Invidious
- Keelog keelog.com Archive.org
- AliExpress aliexpress.com Archive.org

Противник может внедрить такие устройства куда угодно: в зарядный кабель, мышь, клавиатуру, USB-накопитель... Их можно использовать, чтобы отслеживать вас или компрометировать компьютер или смартфон. Самый известный пример таких атак, вероятно, Stuxnet[221] в 2005 году.

Хотя USB-накопитель можно физически осмотреть, просканировать разными утилитами и проверить компоненты на подлинность, скорее всего, вы никогда не сможете обнаружить сложное вредоносное ПО, встроенное умелым противником в настоящие компоненты настоящего USB-накопителя, без продвинутого криминалистического оборудования[222].

Чтобы смягчить это, никогда не доверяйте таким устройствам и не подключайте их к чувствительному оборудованию. Если вы используете устройство для зарядки, подумайте об использовании USB-блокиратора данных, который разрешает только зарядку и не допускает передачу данных. Такие блокираторы сейчас легко купить во многих интернет-магазинах. Также стоит рассмотреть полное отключение USB-портов в BIOS компьютера, если они вам не нужны и если это возможно.

Вредоносное ПО и скрытые входы в аппаратной прошивке и операционной системе

Это может звучать знакомо, потому что частично уже обсуждалось ранее в разделе Ваш процессор.

Вредоносное ПО и скрытые входы могут быть встроены прямо в аппаратные компоненты. Иногда такие скрытые входы реализует сам производитель, как IME в случае процессоров Intel. В других случаях их может внедрить третья сторона, которая оказывается между заказом нового оборудования и доставкой клиенту[223].

Такое вредоносное ПО и скрытые входы противник также может развёртывать с помощью программных эксплойтов. Многие из них в технической среде называются руткитами[224]. Обычно такие виды вредоносного ПО труднее обнаружить и смягчить, потому что они работают на более низком уровне, чем пользовательское пространство[225], и часто прямо в прошивке[226] аппаратных компонентов.

Что такое прошивка? Прошивка — это низкоуровневая операционная система для устройств. Вероятно, у каждого компонента вашего компьютера есть прошивка, включая, например, диски. BIOS[227]/UEFI[228] вашей машины — тоже разновидность прошивки.

Такие компоненты могут позволять удалённое управление и способны тихо и скрытно дать полный контроль над целевой системой.

Как уже упоминалось, пользователям труднее обнаруживать такое ПО, но некоторые ограниченные шаги всё же можно предпринять: защищать устройство от вмешательства и применять меры вроде перепрошивки BIOS. К сожалению, если такое вредоносное ПО или скрытый вход реализован самим производителем, обнаружить и отключить его становится чрезвычайно трудно.

Примечание: угрозы, описанные в этом разделе, почти исключительно актуальны для ценных целей противников государственного уровня. Если ваша модель угроз — преследователь, корпоративный конкурент или даже большинство правоохранительных органов, этот раздел можно пропустить. Если вы журналист, диссидент или активист, действующий против противника государственного уровня, читайте.

Большинство руководств по анонимности сосредоточено на программных и сетевых угрозах. Физические атаки и атаки на уровне оборудования встречаются реже, дороже в исполнении и требуют либо физического доступа к устройству, либо вмешательства в цепочку поставок. Такая стоимость означает, что их не применяют случайно. Но против правильной цели они разрушительно эффективны, потому что никакая программная настройка не защищает вас, если скомпрометировано оборудование под ней.

Импланты в прошивке

Импланты в прошивке — это вредоносный код, внедрённый в низкоуровневое программное обеспечение, которое запускается до загрузки операционной системы: в UEFI/BIOS[229], прошивку контроллера накопителя или прошивку сетевой карты. Поскольку они находятся ниже ОС, они переживают переустановку операционной системы, очистку диска и большинство криминалистических проверок.

LoJax[230], обнаруженный ESET в 2018 году, был первым публично задокументированным UEFI-руткитом, реально встреченным в природе; его связывают с группой APT28 (Fancy Bear). Он записывал вредоносный модуль прямо во flash-память SPI прошивки UEFI, сохраняясь после переустановки ОС и даже замены жёсткого диска. MosaicRegressor[231], описанный Kaspersky в 2020 году, был похожим образом внедрён в UEFI и найден на устройствах сотрудников НКО и журналистов, контактировавших с Северной Кореей.

Кому угрожает такая атака? В обоих задокументированных случаях целями были сотрудники НКО, журналисты и дипломатический персонал — люди, чьи устройства проходили через руки государственных участников или на кого были направлены сложные целевые фишинговые атаки, дававшие удалённый доступ к записи прошивки. Это не та угроза, которую можно масштабно применять массово. Её используют хирургически, против конкретных ценных людей.

Меры смягчения ограничены, но их стоит понимать. UEFI Secure Boot[232] проверяет криптографические подписи загрузчика и компонентов ОС перед выполнением, не позволяя неподписанному коду запускаться при загрузке. Однако он не защищает от компрометации самой прошивки: если UEFI уже изменён, Secure Boot можно отключить или обойти изнутри. Это значимая защита против атакующих, которые ещё не получили доступ уровня прошивки, но не корень доверия при наличии импланта в прошивке. Intel Boot Guard и аналог AMD идут дальше: они записывают хэш начальной прошивки в оборудование на этапе производства, делая изменение прошивки обнаруживаемым. Heads[233] — открытая альтернатива прошивки для поддерживаемого оборудования (в основном ThinkPad и некоторых машин System76), которая даёт измеряемую загрузку, аттестацию с TPM и обнаружение вмешательства; это самый практичный вариант для пользователя с высоким риском, которому нужна проверяемая целостность прошивки. См. также: О Secure Boot.

Аппаратные средства USB-атаки

Инструменты атак через USB коммерчески доступны и хорошо изучены. **O.MG Cable** — это USB-кабель со встроенным беспроводным имплантом, визуально и функционально неотличимый от обычного зарядного кабеля; он может выполнять нажатия клавиш, выводить данные и принимать удалённые команды по Wi-Fi. **USB Rubber Ducky** и более широкое семейство продуктов Hak5 представляются целевому компьютеру клавиатурой, выполняя заранее загруженные последовательности нажатий со скоростью, недоступной человеку. См. также: Вредоносные USB-устройства.

Распознать такое трудно. Кабели O.MG специально созданы, чтобы выдерживать визуальный осмотр. Практические меры смягчения: **никогда не использовать кабели или USB-устройства, которые вы не купили сами и не получили запечатанными**, использовать USB-блокиратор данных («USB condom») при зарядке от недоверенных портов и настроить операционную систему так, чтобы она требовала подтверждения перед доверием новым USB-устройствам (USBGuard в Linux[234]; в Windows без сторонних инструментов такой встроенной возможности нет).

Атаки Evil Maid

Подробнее об атаках Evil Maid см.: Атака Evil Maid.

Меры смягчения:

- **Никогда не оставляйте устройство без присмотра в среде высокого риска.** Это единственная полная мера смягчения.
- **Измеряемая загрузка с аттестацией TPM** (как в Heads или корректно настроенной связке UEFI + TPM) обнаружит вмешательство в загрузчик, сравнив измерения с известными хорошими значениями, сохранёнными в TPM.
- **Пломба, показывающая вскрытие**, на корпусе устройства (лак для ногтей, нанесённый поверх винтов и сфотографированный, или коммерческие пломбы-индикаторы вскрытия) даёт низкотехнологичный слой обнаружения, который удивительно эффективен против неопытных противников.

Компрометация цепочки поставок

Атаки на цепочку поставок нацелены на ваше устройство до того, как оно попадёт к вам: на этапе производителя, дистрибьютора или доставки. Каталог ANT АНБ[235], утёкший благодаря Snowden в 2013 году, документировал аппаратные импланты, устанавливаемые в маршрутизаторы Cisco и другое сетевое оборудование во время доставки. Для большинства пользователей такая угроза нереалистична. Для высокопоставленного диссидента, адвоката по правам человека или разведывательного источника в стране, чьё правительство влияет на аппаратные цепочки поставок, её стоит учитывать.

Практические меры смягчения ограничены. Покупка устройств лично в розничном магазине, а не доставка, сокращает окно перехвата. Предпочтение оборудования от поставщиков вне досягаемости цепочки поставок противника и использование оборудования с поддержкой Heads и проверенной прошивкой дают некоторую уверенность. В случаях самого высокого риска следует считать любое устройство, которое выходило из-под вашего контроля даже ненадолго, потенциально скомпрометированным.

Контрольный список физического осмотра

Для людей с высоким риском, которые получают устройство или возвращаются к нему:

- Осмотрите отверстия портов (USB, Thunderbolt, слот SD-карты) на признаки посторонних предметов или следов.
- Проверьте винты на царапины, не похожие на заводскую сборку; после осмотра нанесите пломбу-индикатор вскрытия.
- Сравните кабель, который собираетесь использовать, с заведомо хорошим образцом; если сомневаетесь, выбросьте его.
- При первой загрузке после любого периода доступа без присмотра проверьте измерения прошивки, если ваша платформа это поддерживает (журнал событий TPM в Heads; `tpm2-tools` в Linux).

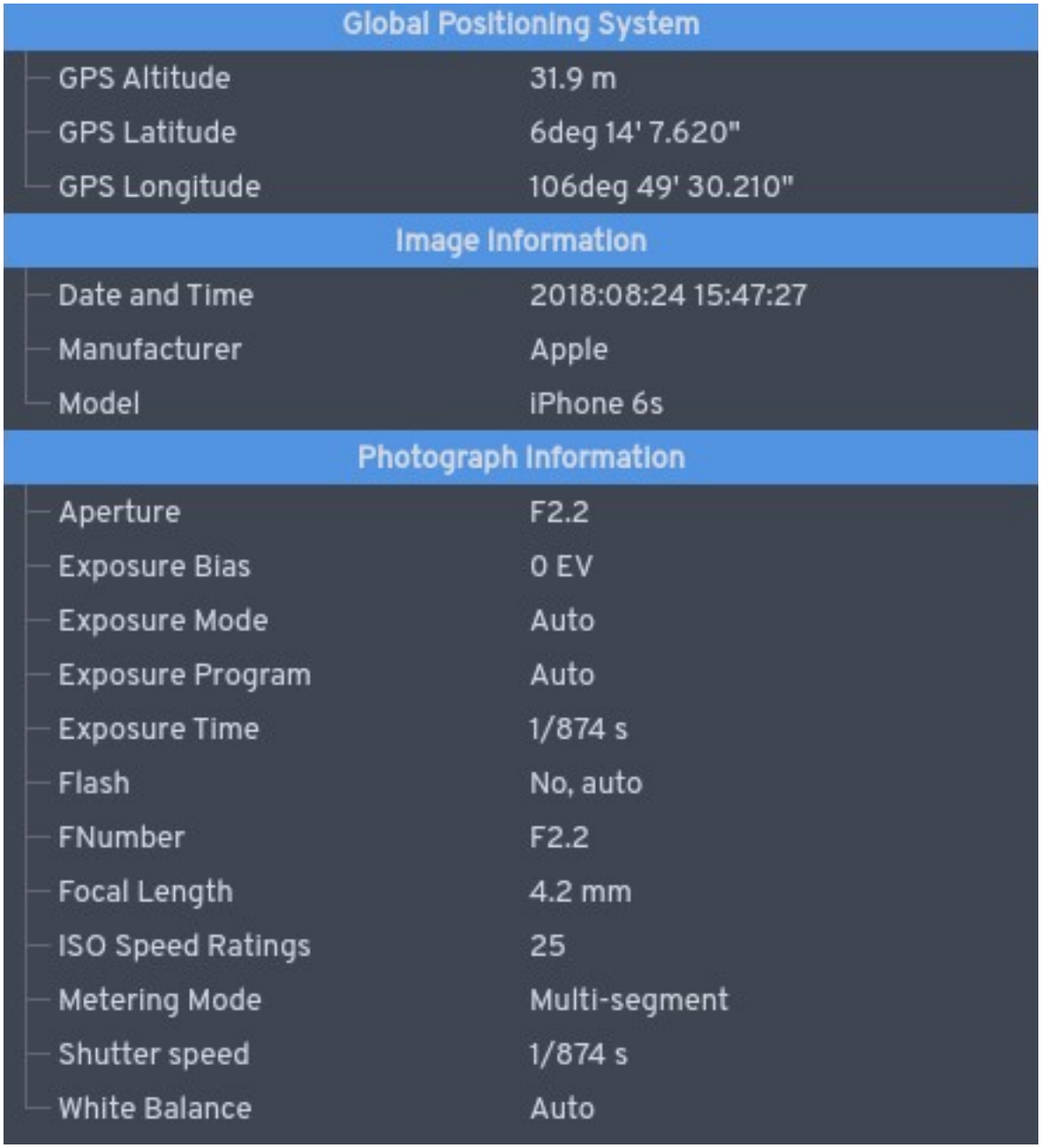
• Если Secure Boot неожиданно отключён в настройках UEFI, считайте устройство скомпрометированным.

Ваши файлы, документы, фотографии и видео

Свойства и метаданные

Для многих это очевидно, но не для всех. У большинства файлов есть прикреплённые метаданные. Хороший пример — фотографии, которые хранят сведения EXIF[236]; они могут содержать много информации, например координаты GPS, модель камеры или телефона, на который был сделан снимок, и точное время съёмки. Хотя эта информация может не раскрывать напрямую, кто вы, она может точно сказать, где вы были в определённый момент, что позволит другим использовать разные источники, чтобы найти вас, например камеры наблюдения или другие записи, сделанные в том же месте и в то же время во время протеста. Вы должны проверять любой файл, который собираетесь размещать на таких платформах, на любые свойства, способные содержать информацию, ведущую обратно к вам.

Вот пример данных EXIF, которые могут быть в фотографии:



(Иллюстрация из Wikipedia)

Это работает и для видео. Да, у видео тоже бывает геотегирование, и многие совершенно об этом не знают. Вот, например, очень удобный инструмент для геолокации видео YouTube: mattw.io Archive.org

По этой причине вы всегда должны быть невероятно осторожны при загрузке файлов через анонимные идентичности и проверять метаданные этих файлов.

Даже если вы публикуете обычный текстовый файл, всегда проверяйте его дважды или трижды на утечки информации перед публикацией. Некоторые рекомендации об этом есть в разделе Дополнительные меры против криминалистики в конце руководства.

Водяные знаки

Фотографии, видео и аудио

Фотографии и видео часто содержат видимые водяные знаки, показывающие, кто владелец или создатель, но в разных продуктах бывают и невидимые водяные знаки, нацеленные на идентификацию самого зрителя.

Поэтому если вы информатор и думаете о том, чтобы передать наружу фотографию, аудио или видео, подумайте дважды. Есть вероятность, что внутри есть невидимый водяной знак, содержащий информацию о вас как о зрителе. Такие водяные знаки можно включить простой настройкой, например в Zoom (видео[237] или аудио[238]), или с помощью расширений[239] для популярных приложений вроде Adobe Premiere Pro. Их могут вставлять разные системы управления содержимым.

Свежий пример, где человека, слившего запись встречи Zoom, поймали из-за водяного знака: theintercept.com Tor Mirror Archive.org

Такие водяные знаки могут вставляться разными продуктами[240][241][242][243] с использованием стеганографии[244] и выдерживать сжатие[245] и повторное кодирование[246][247].

Эти водяные знаки нелегко обнаружить, и они могут позволить установить источник, несмотря на все усилия.

Кроме водяных знаков, камеру, на которую снимали видео, а значит и устройство съёмки, тоже можно идентифицировать разными техниками, например по характеристикам объектива[248], что может привести к деанонимизации.

Будьте крайне осторожны при публикации видео, фотографий или аудиофайлов с известных коммерческих платформ: они могут содержать такие невидимые водяные знаки в дополнение к деталям в самих изображениях. Гарантированной стопроцентной защиты от этого нет. Придётся пользоваться здравым смыслом.

Водяные знаки принтеров

Знаете ли вы, что ваш принтер, скорее всего, тоже за вами следит? Даже если он не подключён ни к какой сети. В ИТ-сообществе это обычно известный факт, но за его пределами знают немногие.

Да... Принтеры тоже можно использовать для вашей деанонимизации, как объясняет EFF здесь: eff.org Archive.org

Вот также старое, но всё ещё актуальное видео EFF, объясняющее как это работает: youtube.com Invidious

Многие принтеры печатают невидимый водяной знак, позволяющий идентифицировать принтер на каждой напечатанной странице. Это называется принтерной стеганографией[249]. Ощутимого способа смягчить это нет, кроме как изучить свой принтер и убедиться, что он не печатает невидимый водяной знак. Это важно, если вы собираетесь печатать анонимно.

Вот старый, но всё ещё актуальный список принтеров и брендов, которые печатают или не печатают такие точки отслеживания, от EFF: eff.org Archive.org

Также вот несколько советов из документации Whonix (Printing and Scanning) Archive.org:

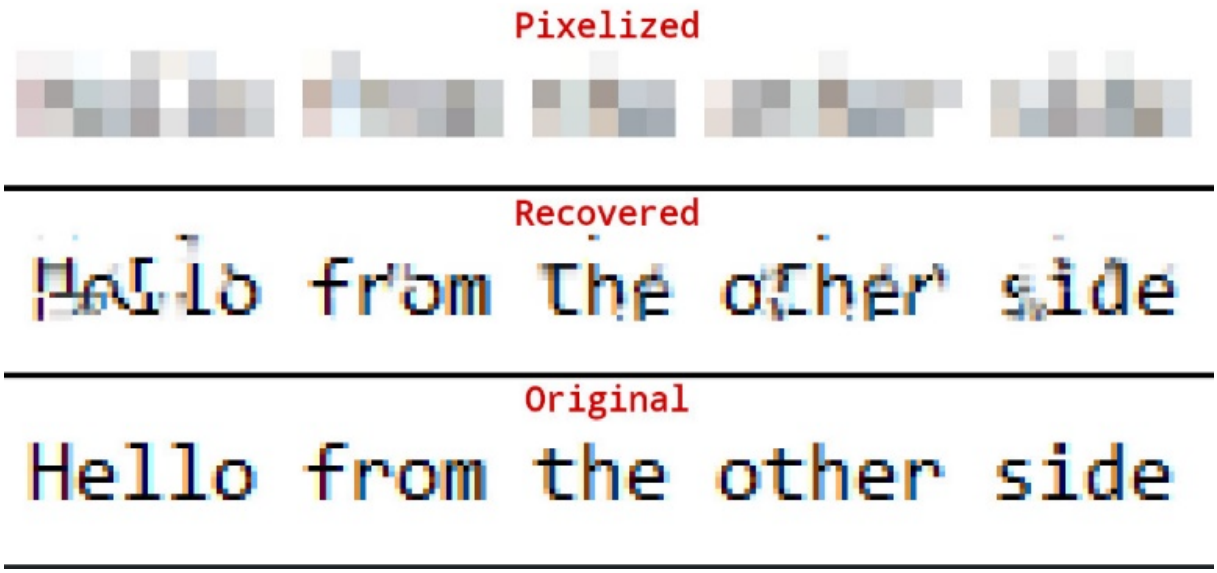
Никогда не печатайте в цвете: обычно водяные знаки отсутствуют без цветных тонеров/картриджей[250].

Пикселизированная или размытая информация

Вы когда-нибудь видели документ с размытым текстом? Вы когда-нибудь смеялись над фильмами или сериалами, где они «улучшают» изображение, чтобы восстановить информацию, которую будто бы невозможно прочитать?

Что ж, существуют техники восстановления информации из таких документов, видео и фотографий.

Вот, например, открытый проект, который можно использовать самому для восстановления текста из некоторых размытых изображений: github.com Archive.org



Конечно, это открытый проект, доступный всем. Но можно представить, что такие техники уже раньше использовались другими противниками. Их можно применять для раскрытия размытой информации в опубликованных документах, а затем использовать это для вашей деанонимизации.

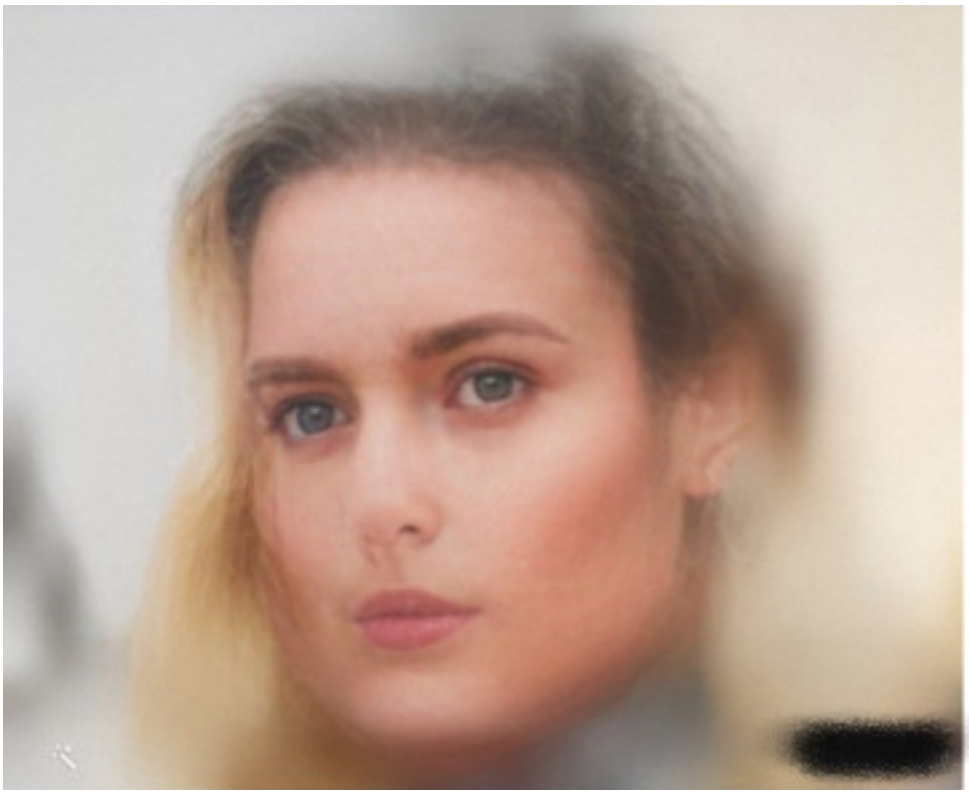
Также есть руководства по использованию таких техник с инструментами редактирования изображений вроде GIMP, например medium.com Archive.org, за которым следует medium.com Scribe.rip Archive.org

Наконец, множество ресурсов по устранению размытия можно найти здесь: github.com Archive.org

Некоторые онлайн-сервисы могут даже в какой-то степени помочь сделать это автоматически, например инструмент улучшения фотографий MyHeritage.com:

myheritage.com Archive.org

Вот результат для изображения выше:



Конечно, на этом этапе этот инструмент скорее «угадывает», чем действительно устраняет размытие, но этого может быть достаточно, чтобы найти вас через разные сервисы обратного поиска изображений.

Существуют также техники устранения размытия и депикселизации фрагментов в видео: см. positive.security Archive.org

По этой причине всегда чрезвычайно важно правильно редактировать и вычищать любой документ, который вы хотите опубликовать. Размытия недостаточно: любые чувствительные данные нужно полностью закрашивать чёрным или удалять, чтобы противник не мог попытаться восстановить данные. Не пикселизируйте, не размывайте — просто ставьте сплошной чёрный прямоугольник для скрытия информации.

Ваши криптовалютные транзакции

Вопреки распространённому мнению, криптовалютные транзакции, например Bitcoin и Ethereum, не анонимны[251]. Большинство криптовалют можно точно отслеживать разными методами[252][253].

Помните, что написано у них на странице: bitcoin.org Archive.org и bitcoin.org Archive.org: «Bitcoin is not anonymous».

Главная проблема не в том, чтобы создать случайный криптовалютный кошелёк для получения средств за VPN/Tor-адресом: на этом этапе кошелёк анонимен. Проблема главным образом возникает, когда вы хотите обменять фиатные деньги (евро, доллары...) на криптовалюту, а затем вывести криптовалюту обратно. Реалистичных вариантов почти нет, кроме перевода средств на биржу, например Coinbase/Kraken/Bitstamp/Binance. У таких бирж известные адреса кошельков, и они ведут подробные журналы из-за финансовых правил KYC[254], а затем могут связать эти криптовалютные транзакции с вами через финансовую систему[255].

Есть криптовалюты, созданные с учётом приватности и анонимности, например Monero, но даже у них есть особенности и предупреждения, которые нужно учитывать[256][257].

Использование «частных» миксеров, tumblers[258] (централизованных сервисов, специализирующихся на «анонимизации» криптовалют через «смешивание») и coinjoin-сервисов рискованно: вы не знаете, что на них происходит[259], а смешивание может быть тривиально разобрано обратно[260]. Их централизованная природа также может создать вам проблемы, поскольку они более уязвимы перед законами о противодействии отмыванию денег[261].

Это не означает, что Bitcoin вообще нельзя использовать анонимно. Bitcoin действительно можно использовать анонимно, если вы не конвертируете его в обычную валюту, используете кошелёк Bitcoin из безопасной анонимной сети и не переиспользуете адреса или не объединяете выходы, которые использовались при оплате у разных продавцов. Иными словами, нужно избегать правил KYC/AML на разных биржах, не пользоваться сетью Bitcoin с какого-либо известного IP-адреса и использовать кошелёк, предоставляющий инструменты сохранения приватности. См. Анонимные криптовалютные платежи.

В целом лучшим вариантом для использования криптовалюты с разумной анонимностью и приватностью остаётся Monero, и в идеале не стоит использовать ничего другого для чувствительных транзакций, если вы не понимаете ограничения и связанные риски. Пожалуйста, прочитайтеПредупреждение о Monero.

Кратко: используйте Monero!

Ваши облачные резервные копии и службы синхронизации

Все компании рекламируют использование сквозного шифрования (E2EE). Это верно почти для каждого мессенджера и сайта (HTTPS). Apple и Google рекламируют использование шифрования на своих Android-устройствах и iPhone.

Но что насчёт резервных копий? Тех автоматических резервных копий iCloud/Google Drive, которые у вас есть?

Что ж, нужно знать, что большинство таких резервных копий не полностью защищено сквозным шифрованием и содержит часть вашей информации, легко доступной третьей стороне. Вы увидите заявления, что данные зашифрованы при хранении и защищены от всех... За исключением того, что обычно они всё же оставляют себе ключ для доступа к части данных. Эти ключи используются для индексации вашего содержимого, восстановления аккаунта и сбора разной аналитики.

Существуют специализированные коммерческие криминалистические решения (Magnet Axiom[262], Cellebrite Cloud[263]), которые помогут противнику легко анализировать ваши облачные данные.

Заметные примеры:

• Apple iCloud: support.apple.com Archive.org: «Сообщения в iCloud также используют сквозное шифрование. Если у вас включена резервная копия iCloud, **она включает копию ключа, защищающего ваши сообщения**. Это гарантирует, что вы сможете восстановить сообщения, если потеряете доступ к iCloud Keychain и доверенным устройствам».

• Google Drive и WhatsApp: faq.whatsapp.com Archive.org: «**Медиа и сообщения, резервную копию которых вы создаёте, не защищены сквозным шифрованием WhatsApp, пока находятся в Google Drive**». Однако обратите внимание, что Facebook/Whatsapp объявили о развёртывании зашифрованных резервных копий 14 октября 2021 года (about.fb.com Archive.org), что должно решить эту проблему.

• Dropbox: dropbox.com Archive.org «Чтобы предоставлять эти и другие функции, **Dropbox получает доступ, хранит и сканирует ваши материалы**. Вы даёте нам разрешение делать это, и это разрешение распространяется на наших аффилированных лиц и доверенные третьи стороны, с которыми мы работаем».

• Microsoft OneDrive: privacy.microsoft.com Archive.org: продукты для продуктивности и коммуникации: «Когда вы используете OneDrive, мы собираем данные об использовании сервиса, а также содержимое, которое вы храните, чтобы предоставлять, улучшать и защищать сервисы. **Например, мы индексируем содержимое ваших документов OneDrive, чтобы вы могли искать их позже, и используем данные о местоположении, чтобы вы могли искать фотографии по месту съёмки**».

Не стоит доверять облачным провайдерам свои чувствительные данные, если они не были заранее и локально зашифрованы. Также стоит скептически относиться к их заявлениям о приватности. В большинстве случаев они могут получить доступ к вашим данным и передать их третьей стороне, если захотят[264].

Единственный способ смягчить это — шифровать данные на своей стороне и только затем загружать их в такие сервисы, **или просто не пользоваться ими вообще.**

Микроархитектурные атаки деанонимизации через побочные каналы

Была опубликована атака, которая может деанонимизировать пользователей, если у них есть известный псевдоним. Например, атакующий, пытающийся отслеживать деятельность журналиста, может использовать публичный Twitter-аккаунт этого журналиста, чтобы связать его анонимные идентичности с публичной. Это нарушает изоляцию идентичностей и может привести к полной деанонимизации даже пользователей, которые соблюдают правильную операционную безопасность.

Атака, опубликованная на leakuidatorplusteam.github.io Archive.org, может быть смягчена известным расширением NoScript, и это будет наша предпочтительная рекомендация.

Одна слабо задокументированная атака может использовать примерно такой подход к распознаванию по цифровому отпечатку: Alice просматривает веб через Firefox. Только что посещённый сайт использует невидимый `iframe`, который создаёт длинные строки, например предложения или хэши, чтобы получить строку, невидимую пользователю. Для этих строк задаётся определённый шрифт, Arial. Отрисовывает ли браузер это на экране, несущественно; важно только, меняется ли шрифт. `iframe` в этом случае нужен исключительно для того, чтобы определить, установлен ли у пользователя определённый шрифт. Если Alice использует шрифт, который этот фрейм пытался отрисовать, это отправляется обратно сайту и человеку, контролирующему сайт.

Шрифт создаёт вокруг себя прямоугольник определённой высоты и ширины, то есть определённую высоту и ширину содержащегося текста. `iframe` повторяет это для каждого установленного шрифта, чтобы создать список шрифтов, установленных у Alice. Из-за стилевых различий между семействами шрифтов одна и та же строка при одном и том же размере шрифта даст другую высоту и ширину, чем Arial. Arial используется как запасной шрифт для отображения текста, который иначе не отобразился бы, если у пользователя нет нужного шрифта на машине и поэтому он недоступен из браузера.

Если шрифт, запрошенный `iframe`, недоступен, для показа текста пользователю будет использован Arial. Каждый раз, когда измерение шрифта, определяемое размерами получившегося прямоугольника, меняется, это означает, что шрифт присутствует в браузере и на машине Alice. Повторив это для сотен шрифтов, сайты могут использовать информацию об установленных шрифтах для отслеживания пользователей между сайтами. Представьте, что сайт затем продаёт эту «анонимизированную» информацию как набор данных рекламным компаниям, чтобы показывать вам рекламу на основе посещаемых сайтов, потому что они знают каждый шрифт, установленный на вашей машине, и теперь могут отслеживать вашу идентичность по всему интернету. Эта атака демонстрируется здесь: Everything you always wanted to know about web-based device fingerprinting (but were afraid to ask) by Dr. Nick Nikiforakis, PhD in Computer Science from KU Leuven. Он объясняет, как его команда исследователей определила, какие сайты используют такие техники среди 10 000 самых популярных сайтов Alexa. Они обнаружили, что 145 из них распознавали браузеры по цифровому отпечатку. Распознавание происходило в 100% случаев: не имело значения, использовали ли пользователи заголовок Do Not Track, популярную настройку приватности и безопасности во многих браузерах.

Атак вроде невидимых iframe и медиэлементов можно избежать, глобально блокируя все скрипты с помощью чего-то вроде uBlock Origin chrome.google.com или NoScript chrome.google.com. Это настоятельно рекомендуется не только тем, кто хочет быть анонимным, но и обычным пользователям веба.

Tor Browser

Примечание: теперь эта атака по умолчанию предотвращается обновлением NoScript (11.4.8 и выше) на всех уровнях безопасности в Tor Browser.

Все остальные

Установка расширения NoScript предотвратит атаку **по умолчанию только в приватных окнах** с помощью новой функции TabGuard. Но в настройках NoScript её можно включить для всех окон. См.:

- Твит о выпуске: twitter.com Archive.org
- Объяснение для пользователей: noscript.net Archive.org
- Пост на форуме Tor Project: forum.torproject.net Archive.org
- Расширение NoScript для Firefox (Firefox и другие браузеры на основе Firefox, кроме Tor Browser): addons.mozilla.org
- Расширение NoScript для браузеров на основе Chromium (Brave, Chrome, Edge и другие браузеры на основе Chromium): chrome.google.com

Альтернатива NoScript для всех остальных браузеров

Исследователи, раскрывшие проблему, также сделали доступным расширение ниже. Повторим: **в Tor Browser ничего не требуется**. Этот путь не является для нас предпочтительным, но он доступен, если вы не хотите использовать NoScript.

- Расширение Leakuidator+ для браузеров на основе Chromium (Brave, Chrome, Edge и другие браузеры на основе Chromium): chrome.google.com
- Расширение Leakuidator+ для Firefox (Firefox и другие браузеры на основе Firefox, кроме Tor Browser): addons.mozilla.org

Разделения идентичностей через отдельные браузеры или даже виртуальные машины недостаточно, чтобы избежать этой атаки. Однако другое решение — убедиться, что, начиная работать с анонимной идентичностью, вы полностью закрываете всю активность, связанную с другими идентичностями. Уязвимость работает только если вы активно вошли в неанонимную идентичность. Проблема в том, что это может мешать эффективной работе, поскольку многозадачность между несколькими идентичностями становится невозможной.

Локальные утечки данных и криминалистика

Большинство из вас, вероятно, видели достаточно криминальных драм на Netflix или телевидении, чтобы знать, что такое криминалистика. Это специалисты, обычно работающие на правоохранительные органы, которые выполняют разный анализ доказательств. Разумеется, это может включать ваш смартфон или ноутбук.

Хотя такие действия могут выполняться противником, когда вы уже «сгорели», они также могут случиться случайно во время обычной проверки или пограничного контроля. Такие несвязанные проверки могут раскрыть противникам секретную информацию, о существовании которой они раньше не знали.

Криминалистические техники теперь очень продвинуты и могут раскрывать ошеломляющее количество информации с ваших устройств, даже если они зашифрованы[265]. Эти техники широко применяются правоохранительными органами по всему миру, и их следует учитывать.

Вот несколько свежих ресурсов, которые стоит прочитать о смартфоне:

• UpTurn, The Widespread Power of U.S. Law Enforcement to Search Mobile Phones upturn.org Archive.org

• New-York Times, The Police Can Probably Break Into Your Phone nytimes.com Archive.org

• Vice, Cops Around the Country Can Now Unlock iPhones, Records Show vice.com Archive.org

Я также настоятельно рекомендую прочитать некоторые документы с точки зрения криминалистического эксперта, например:

• EnCase Forensic User Guide, encase-docs.opentext.com Archive.org

• FTK Forensic Toolkit, accessdata.com Archive.org

• SANS Digital Forensics and Incident Response Videos, youtube.com

И наконец, вот очень поучительная подробная статья о текущем состоянии безопасности iOS/Android от Johns Hopkins University: securephones.io[266].

Когда речь идёт о ноутбуке, криминалистических техник много, и они широко распространены. Многие из этих проблем можно смягчить с помощью полного шифрования диска, виртуализации (см. Виртуализация) и изоляции. Далее руководство подробно разберёт такие угрозы и техники их смягчения.

Плохая криптография

В сообществе информационной безопасности часто повторяют пословицу: «Не изобретайте собственную криптографию!».

И для этого есть причины[267][268][269][270].

Мы не хотим, чтобы из-за этой фразы люди переставали изучать криптографию и создавать в ней новое. Поэтому вместо этого мы рекомендуем осторожно относиться к подходу «сделаю свою криптографию», потому что она не обязательно будет хорошей:

• Хорошая криптография непроста; обычно на её разработку и доводку уходят годы исследований.

• Хорошая криптография прозрачна, не является проприетарной или закрытой, чтобы её могли проверить коллеги.

• Хорошая криптография разрабатывается осторожно, медленно и редко в одиночку.

• Хорошая криптография обычно представляется и обсуждается на конференциях и публикуется в разных журналах.

• Хорошая криптография проходит обширную экспертную проверку до выпуска для использования в реальном мире.

• Даже правильное использование и внедрение уже существующей хорошей криптографии — это вызов.

Тем не менее это не останавливает некоторых людей: они всё равно публикуют разные производственные приложения и сервисы со своей самодельной криптографией или проприетарными закрытыми методами:

• Будьте осторожны при использовании приложений и сервисов с закрытыми или проприетарными методами шифрования. Все хорошие криптографические стандарты публичны и прошли

экспертную проверку; не должно быть проблемы в том, чтобы раскрыть используемый стандарт.

- Скептически относитесь к приложениям и сервисам, использующим «модифицированный» или проприетарный криптографический метод[271].
- По умолчанию не доверяйте никакой «самодельной криптографии», пока она не прошла аудит, экспертную проверку, отбор и принятие криптографическим сообществом[272][273].
- Не существует «криптографии военного уровня»[274][275][276].

Криптография — сложная тема, и плохая криптография легко может привести к вашей деанонимизации.

В контексте этого руководства мы рекомендуем придерживаться приложений и сервисов, которые используют хорошо зарекомендовавшие себя, опубликованные и прошедшие экспертную проверку методы.

Итак, чему отдавать предпочтение и чего избегать по состоянию на 2021 год? Вам придётся самостоятельно искать технические детали каждого приложения и смотреть, использует ли оно «плохую криптографию» или «хорошую криптографию». Получив технические детали, можно свериться с этой страницей, чтобы понять, чего они стоят: latacora.micro.blog Archive.org

Вот несколько примеров:

- Хэши:
  - Предпочтительно: SHA-3 или BLAKE2[277]
  - Всё ещё относительно приемлемо: SHA-2 (например, широко используемые SHA-256 или SHA-512)
  - Избегать: SHA-1, MD5 (к сожалению, всё ещё широко используется), CRC, MD6 (редко используется)
- Шифрование файлов/дисков:
  - Предпочтительно:
    - С аппаратным ускорением[278]: AES (Rijndael) 256 бит с HMAC-SHA-2 или HMAC-SHA-3 (это то, что Veracrypt, Bitlocker, Filevault 2, KeepassXC и LUKS используют по умолчанию). Предпочтительнее SHA-3.
    - Без аппаратного ускорения: то же, что выше, или, если доступно, рассмотрите:
      - ChaCha20[279] или XChaCha20 (ChaCha20 можно использовать с Kryptor kryptor.co.uk; к сожалению, в Veracrypt он недоступен).
      - Serpent[280]
      - TwoFish[281]
  - Избегать: практически всего остального
- Хранение паролей:
  - Предпочтительно: Argon2, scrypt
  - Если этих вариантов нет, используйте bcrypt, а если и это невозможно, хотя бы PBKDF2 (только как крайний вариант)
  - Скептически относитесь к Argon2d, потому что он уязвим к некоторым видам побочных каналов. Предпочитайте Argon2i или Argon2id
  - Избегать: SHA-3, SHA-2, SHA-1, MD5

- Безопасность браузера (HTTPS):
  - Предпочтительно: TLS 1.3 (в идеале TLS 1.3 с поддержкой ECH/eSNI) или хотя бы TLS 1.2 (широко используется)
  - Избегать: всего остального (TLS =<1.1, SSL =<3)
- Подпись сообщений/файлов с помощью GnuPG (GPG):
  - Предпочтительно ECDSA (ed25519)+ECDH (ec25519) или RSA 4096 бит
    - **Рассмотрите более современную[282] альтернативу PGP/GPG: Minisign** **jedisct1.github.io** Archive.org
  - Избегать: RSA 2048 бит
- SSH-ключи:
  - ED25519 (предпочтительно) или RSA 4096 бит
  - Избегать: RSA 2048 бит
- **Предупреждение: RSA и ED25519, к сожалению, не считаются квантово-устойчивыми[283], и хотя они ещё не взломаны, вероятно, однажды в будущем их взломают. Вопрос скорее в том, когда RSA будет взломан, а не в том, случится ли это вообще. Поэтому в этих контекстах они предпочтительны из-за отсутствия лучшей возможности.**

Вот несколько реальных случаев проблем плохой криптографии:

- Telegram: democratic-europe.eu Archive.org
- Telegram: buttondown.email Archive.org
- Cryptocat: web.archive.org
- Другие примеры можно найти здесь: cryptofails.com Archive.org

Далее это руководство не будет рекомендовать «плохую криптографию», и, надеемся, этого будет достаточно, чтобы вас защитить?

Политики отсутствия журналов

Многие думают, что сервисы, ориентированные на приватность, например VPN или поставщики электронной почты, безопасны благодаря политикам отсутствия журналов или схемам шифрования. К сожалению, многие из этих же людей забывают, что все такие поставщики — юридические коммерческие организации, подчиняющиеся законам стран, в которых они работают.

Любого из этих поставщиков могут заставить тайно, без вашего ведома, например по судебному приказу с запретом на разглашение[284] или письму национальной безопасности[285], записывать вашу активность, чтобы деанонимизировать вас. Недавно было несколько таких примеров:

- 2021, Proton: Proton записал IP-адрес французского активиста после распоряжения швейцарских властей (ссылка на источник недоступна).
- 2021, WindScribe: серверы не были зашифрованы как следовало, что позволило властям проводить атаки «человек посередине»[286].
- 2021, серверы DoubleVPN: журналы и сведения об аккаунтах были изъяты правоохранительными органами[287].

• 2021, немецкий почтовый провайдер Tutanota был вынужден отслеживать конкретные аккаунты в течение 3 месяцев[288].

• 2020, немецкий почтовый провайдер Tutanota был вынужден внедрить скрытый вход для перехвата и сохранения копий незашифрованных писем одного пользователя[289] (они не расшифровывали хранимые письма).

• 2017, PureVPN был вынужден раскрыть ФБР информацию об одном пользователе[290].

• 2014, пользователь EarthVPN был арестован на основании журналов, предоставленных нидерландской полиции[291].

• 2013, защищённый поставщик электронной почты Lavabit закрылся после борьбы с секретным запретом на разглашение[292].

• 2011, пользователь HideMyAss был деанонимизирован, а журналы были переданы ФБР[293].

Некоторые поставщики внедрили Warrant Canary[294], который позволил бы пользователям узнать, были ли они скомпрометированы такими приказами, но, насколько нам известно, это ещё не было проверено на практике.

Наконец, сейчас хорошо известно, что некоторые компании могут быть прикрытиями, спонсируемыми государственными противниками (см. историю Crypto AG[295] и историю Omnisec[296]).

По этим причинам нельзя доверять таким поставщикам свою приватность, несмотря на все их заявления. В большинстве случаев вы будете последним, кто узнает, что какие-либо из ваших аккаунтов стали целью таких приказов, а возможно, вообще никогда не узнаете.

Чтобы смягчить это, в случаях, когда вы хотите использовать VPN, мы будем рекомендовать VPN-провайдера, оплаченного наличными или Monero, поверх Tor, чтобы VPN-сервис не знал никакой идентифицирующей информации о вас.

Если VPN-провайдер ничего о вас не знает, это должно смягчить проблему ситуации, когда он заявляет, что не ведёт журналы, но всё равно ведёт их.

Некоторые продвинутые целевые техники

(Иллюстрация: отличный фильм, который мы настоятельно рекомендуем, Das Leben der Anderen[297])

Умелые противники[298] могут использовать множество продвинутых техник для обхода ваших мер безопасности, если они уже знают, где находятся ваши устройства. Многие из этих техник подробно описаны здесь: cyber.bgu.ac.il Archive.org (Air-Gap Research Page, Cyber-Security Research Center, Ben-Gurion University of the Negev, Israel), а также в этом отчёте welivesecurity.com Archive.org (ESET, JUMPING THE AIR GAP: 15 years of nation-state effort). Они включают:

- Атаки, требующие вредоносных имплантов:
  - Вывод данных через заражённый вредоносным ПО маршрутизатор: youtube.com Invidious
  - Вывод данных через наблюдение за изменением света в клавиатуре с подсветкой с помощью скомпрометированной камеры: youtube.com Invidious
    - Вывод данных через скомпрометированную камеру безопасности, которая сначала могла использовать предыдущую атаку: youtube.com Invidious
    - Связь извне со скомпрометированными камерами безопасности через инфракрасные световые сигналы: youtube.com Invidious
  - Вывод данных со скомпрометированного компьютера без сети через акустический анализ шума вентиляторов смартфоном: youtube.com Invidious
  - Вывод данных с заражённого вредоносным ПО компьютера без сети через светодиоды жёсткого диска с помощью дрона: youtube.com Invidious
  - Вывод данных с USB-вредоноса на компьютере без сети через электромагнитные помехи: youtube.com Invidious
  - Вывод данных с заражённого вредоносным ПО жёсткого диска через скрытый акустический шум: youtube.com Invidious
  - Вывод данных через GSM-частоты со скомпрометированного вредоносным ПО компьютера без сети: youtube.com Invidious
  - Вывод данных через электромагнитное излучение скомпрометированного дисплея: youtube.com Invidious
  - Вывод данных через магнитные волны со скомпрометированного компьютера без сети на смартфон, лежащий внутри пакета Фарадея: youtube.com Invidious
  - Связь между двумя скомпрометированными компьютерами без сети с помощью ультразвуковых волн: youtube.com Invidious
  - Вывод кошелька Bitcoin со скомпрометированного компьютера без сети на смартфон: youtube.com Invidious
  - Вывод данных со скомпрометированного компьютера без сети с использованием яркости дисплея: youtube.com Invidious
  - Вывод данных со скомпрометированного компьютера без сети через вибрации: youtube.com Invidious
  - Вывод данных со скомпрометированного компьютера без сети путём превращения RAM в Wi-Fi-излучатель: youtube.com Invidious
  - Вывод данных со скомпрометированного компьютера без сети через линии электропитания: arxiv.org Archive.org
- **Атаки, не требующие вредоносного ПО:**
  - Наблюдение за пустой стеной в комнате с расстояния, чтобы определить, сколько людей находится в комнате и что они делают[299]. Публикация с демонстрацией: wallcamera.csail.mit.edu Archive.org

- Наблюдение за отражающим пакетом снеков в комнате с расстояния, чтобы восстановить всю комнату[300]. Публикация с фотографическими примерами: arxiv.org Archive.org
- Измерение вибраций пола для идентификации людей и определения их состояния здоровья и настроения[301]. Публикация с демонстрацией: engineering.cmu.edu Archive.org
- Наблюдение за лампочкой с расстояния, чтобы слушать звук в комнате[302] без какого-либо вредоносного ПО. Демонстрация: youtube.com Invidious. Следует отметить, что этот тип атаки совсем не новый: статьи о таких техниках появлялись ещё в 2013 году[303], и даже можно купить устройства для самостоятельного выполнения, например здесь: gcomtech.com Archive.org

Вот также хорошее видео тех же авторов, объясняющее эти темы: Black Hat, The Air-Gap Jumpers youtube.com Invidious

Реалистично это руководство мало поможет против таких противников, поскольку такое вредоносное ПО может быть внедрено в устройства производителем, кем-то посередине[304] или кем-либо с физическим доступом к компьютеру без сети. Однако всё же есть некоторые способы смягчить такие техники:

- Не выполняйте чувствительные действия, будучи подключёнными к недоверенной или незащищённой линии электропитания, чтобы предотвратить утечки по питанию.
- Не используйте устройства перед камерой, которая может быть скомпрометирована.
- Используйте устройства в звукоизолированной комнате, чтобы предотвратить утечки звука.
- Используйте устройства в клетке Фарадея, чтобы предотвратить электромагнитные утечки.
- Не обсуждайте чувствительную информацию там, где лампочки могут быть видны снаружи.
- Покупайте устройства в разных, непредсказуемых, офлайн-местах (магазинах), где вероятность их заражения таким вредоносным ПО ниже.
- Не позволяйте никому, кроме доверенных людей, получать доступ к вашим компьютерам без сети.

Некоторые дополнительные ресурсы

- Посмотрите документацию Whonix о техниках сбора данных здесь: Data Collection Techniques Archive.org
- Вам также может понравиться сервис tosdr.org Archive.org (Terms of Services, Didn't Read), который даёт хороший обзор разных условий использования многих сервисов.
- Посмотрите eff.org Archive.org для дополнительных ресурсов.
- Посмотрите en.wikipedia.org Wikiless Archive.org, чтобы получить обзор всех известных проектов массовой слежки, текущих и прошлых.
- Посмотрите gwern.net Archive.org (даже если вы не знаете Death Note).
- Рассмотрите возможность найти и прочитать книгу Michael Bazzell «Open-Source Intelligence Techniques» (на момент написания — восьмое издание, чтобы узнать больше о современных техниках OSINT) inteltechniques.com
- Наконец, проверьте freehaven.net Archive.org для последних академических работ, связанных с онлайн-анонимностью.

Примечания

Если вы всё ещё не думаете, что такая информация может использоваться разными участниками для вашего отслеживания, можно самостоятельно посмотреть статистику по некоторым платформам и помнить, что она учитывает только законные запросы данных и не включает такие вещи, как PRISM, MUSCULAR, SORM или XKEYSCORE, объяснённые ранее:

• Google Transparency Report transparencyreport.google.com Archive.org

• Facebook Transparency Report transparency.facebook.com Archive.org

• Apple Transparency Report apple.com Archive.org

• Cloudflare Transparency Report cloudflare.com Archive.org

• Snapchat Transparency Report snap.com Archive.org

• Telegram Transparency Report t.me Archive.org (требуется установленный Telegram)

• Microsoft Transparency Report microsoft.com Archive.org

• Amazon Transparency Report amazon.com Archive.org

• Dropbox Transparency Report dropbox.com Archive.org

• Discord Transparency Report discord.com Archive.org

• GitHub Transparency Report github.blog Archive.org

• Snapchat Transparency Report snap.com Archive.org

• TikTok Transparency Report tiktok.com Archive.org

• Reddit Transparency Report redditinc.com Archive.org

• Twitter Transparency Report transparency.twitter.com Archive.org

Сноски

[1] [назад] English translation of German Telemedia Act huntonprivacyblog.com Archive.org. Section 13, Article 6, "The service provider must enable the use of Telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable. The recipient of the service is to be informed about this possibility. ".
[2] [назад] Wikipedia, Real-Name System Germany en.wikipedia.org Wikiless Archive.org
[3] [назад] Wikipedia, Don't be evil en.wikipedia.org Wikiless Archive.org
[4] [назад] YouTube, WarGames - "The Only Winning Move" youtube.com Invidious
[5] [назад] Wikipedia, OSINT en.wikipedia.org Wikiless Archive.org
[6] [назад] YouTube Internet Historian Playlist, HWNDU youtube.com Invidious
[7] [назад] Wikipedia, 4chan en.wikipedia.org Wikiless Archive.org
[8] [назад] PIA, See this good article on the matter privateinternetaccess.com Archive.org (disclaimer: this is not an endorsement or recommendation for this commercial service).
[9] [назад] Medium.com, Privacy, Blockchain and Onion Routing medium.com Scribe.rip Archive.org
[10] [назад] This World of Ours, James Mickens scholar.harvard.edu Archive.org
[11] [назад] XKCD, Security xkcd.com Archive.org
[12] [назад] Wikipedia, Threat Model en.wikipedia.org Wikiless Archive.org
[13] [назад] Bellingcat bellingcat.com Archive.org
[14] [назад] YouTube, Internet Historian, The Bikelock Fugitive of Berkeley youtube.com Invidious
[15] [назад] Wikipedia, Doxing en.wikipedia.org Wikiless Archive.org
[16] [назад] BBC News, Tor Mirror bbc.com Archive.org
[17] [назад] GitHub, Real World Onion websites github.com Archive.org (updated extremely often)
[18] [назад] Tor Project, Who Uses Tor 2019.www.torproject.org Archive.org
[19] [назад] Whonix Documentation, The importance of Anonymity whonix.org Archive.org
[20] [назад] Geek Feminism geekfeminism.wikia.org Archive.org
[21] [назад] Tor Project, Tor Users 2019.www.torproject.org Archive.org
[22] [назад] PrivacyHub, Internet Privacy in the Age of Surveillance cyberghostvpn.com Archive.org
[23] [назад] PIA Blog, 50 Key Stats About Freedom of the Internet Around the World privateinternetaccess.com Archive.org
[24] [назад] Wikipedia, IANAL en.wikipedia.org Wikiless Archive.org
[25] [назад] Wikipedia, Trust but verify en.wikipedia.org Wikiless Archive.org
[26] [назад] Wikipedia, Zero-trust Security Model en.wikipedia.org Wikiless Archive.org
[27] [назад] Wikipedia, IP Address en.wikipedia.org Wikiless Archive.org
[28] [назад] Wikipedia; Data Retention en.wikipedia.org Wikiless Archive.org
[29] [назад] Wikipedia, Tor Anonymity Network en.wikipedia.org Wikiless Archive.org
[30] [назад] Wikipedia, VPN en.wikipedia.org Wikiless Archive.org

[31] [назад] Ieee.org, Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency - Choose Two ieeexplore.ieee.org Archive.org
[32] [назад] Wikipedia, DNS en.wikipedia.org Wikiless Archive.org
[33] [назад] Wikipedia, DNS Blocking en.wikipedia.org Wikiless Archive.org
[34] [назад] CensoredPlanet censoredplanet.org Archive.org
[35] [назад] Wikipedia, MITM en.wikipedia.org Wikiless Archive.org
[36] [назад] ArXiv, Characterizing Smart Home IoT Traffic in the Wild arxiv.org Archive.org
[37] [назад] Labzilla.io, Your Smart TV is probably ignoring your Pi-Hole labzilla.io Archive.org
[38] [назад] Wikipedia, DNS over HTTPS: en.wikipedia.org Wikiless Archive.org
[39] [назад] Wikipedia, DNS over TLS, en.wikipedia.org Wikiless Archive.org
[40] [назад] Wikipedia, Pi-Hole en.wikipedia.org Wikiless Archive.org
[41] [назад] Wikipedia, SNI en.wikipedia.org Wikiless Archive.org
[42] [назад] Wikipedia, ECH en.wikipedia.org Wikiless Archive.org
[43] [назад] Wikipedia, eSNI en.wikipedia.org Wikiless Archive.org
[44] [назад] Usenix.org, On the Importance of Encrypted-SNI (ESNI) to Censorship Circumvention usenix.org Archive.org
[45] [назад] Wikipedia, CDN en.wikipedia.org Wikiless Archive.org
[46] [назад] Cloudflare, Good-bye ESNI, hello ECH! blog.cloudflare.com Archive.org
[47] [назад] ZDNET, Russia wants to ban the use of secure protocols such as TLS 1.3, DoH, DoT, ESNI zdnet.com Archive.org
[48] [назад] ZDNET, China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI zdnet.com Archive.org
[49] [назад] Wikipedia, OCSP en.wikipedia.org Wikiless Archive.org
[50] [назад] Madaidans Insecurities, Why encrypted DNS is ineffective madaidans-insecurities.github.io Archive.org
[51] [назад] Wikipedia, OCSP Stapling en.wikipedia.org Wikiless Archive.org
[52] [назад] Chromium Documentation, CRLSets dev.chromium.org Archive.org
[53] [назад] ZDNet, Chrome does certificate revocation better zdnet.com Archive.org
[54] [назад] KUL, Encrypted DNS=>Privacy? A Traffic Analysis Perspective esat.kuleuven.be Archive.org
[55] [назад] ResearchGate, Oblivious DNS: Practical Privacy for DNS Queries researchgate.net Archive.org
[56] [назад] Nymity.ch, The Effect of DNS on Tor's Anonymity nymity.ch Archive.org
[57] [назад] Wikipedia, RFID en.wikipedia.org Wikiless Archive.org
[58] [назад] Wikipedia, NFC en.wikipedia.org Wikiless Archive.org
[59] [назад] Samsonite Online Shop, RFID accessories shop.samsonite.com Archive.org
[60] [назад] Google Android Help, Android Location Services support.google.com Archive.org
[61] [назад] Apple Support, Location Services and Privacy support.apple.com Archive.org
[62] [назад] 2016 International Conference on Indoor Positioning and Indoor Navigation, Wi-Fi probes as digital crumbs for crowd localization fly.isti.cnr.it Archive.org
[63] [назад] Southeast University of Nanjing, Probe Request Based Device Identification Attack and Defense ncbi.nlm.nih.gov Archive.org
[64] [назад] Medium.com, The Perils of Probe Requests medium.com Scribe.rip Archive.org
[65] [назад] State University of New York, Towards 3D Human Pose Construction Using Wi-Fi cse.buffalo.edu Archive.org
[66] [назад] Digi.Ninja, Jasager digi.ninja Archive.org
[67] [назад] Hak5 Shop, Wi-Fi Pineapple shop.hak5.org Archive.org
[68] [назад] Wikipedia, Deautentication Attack en.wikipedia.org Wikiless Archive.org
[69] [назад] Wikipedia, Capture Portal en.wikipedia.org Wikiless Archive.org
[70] [назад] HackerFactor Blog, Deanonymizing Tor Circuits hackerfactor.com Archive.org
[71] [назад] KU Leuven, Website Fingerprinting through Deep Learning distrinet.cs.kuleuven.be Archive.org
[72] [назад] KU Leuven, Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning homes.esat.kuleuven.be Archive.org
[73] [назад] Internet Society, Website Fingerprinting at Internet Scale web.archive.org Archive.org
[74] [назад] KU Leuven, A Critical Evaluation of Website Fingerprinting Attacks esat.kuleuven.be Archive.org
[75] [назад] DailyDot, How Tor helped catch the Harvard bomb threat suspect dailydot.com Archive.org
[76] [назад] ArsTechnica, How the NSA can break trillions of encrypted Web and VPN connections arstechnica.com Archive.org
[77] [назад] Wikipedia, Sybil Attack en.wikipedia.org Wikiless Archive.org
[78] [назад] ArsTechnica, Does Tor provide more benefit or harm? New paper says it depends arstechnica.com Archive.org
[79] [назад] ResearchGate, The potential harms of the Tor anonymity network cluster disproportionately in free countries pnas.org Archive.org
[80] [назад] Tor Project, Tor design paper svn-archive.torproject.org Archive.org
[81] [назад] Murdoch & Danezis, Low-Cost Traffic Analysis of Tor (2005) cl.cam.ac.uk Archive.org
[82] [назад] Sun et al., RAPTOR: Routing Attacks on Privacy in Tor (2015) usenix.org Archive.org
[83] [назад] CryptoEngineering, How does Apple (privately) find your offline devices? blog.cryptographyengineering.com Archive.org
[84] [назад] Apple Support support.apple.com Archive.org
[85] [назад] XDA, Samsung's Find My Mobile app can locate Galaxy devices even when they're offline xda-developers.com Archive.org
[86] [назад] Apple Support, If your Mac is lost or stolen support.apple.com Archive.org
[87] [назад] Wikipedia, BLE en.wikipedia.org Wikiless Archive.org
[88] [назад] Cryptography Engineering Blog, How does Apple (privately) find your offline devices? blog.cryptographyengineering.com Archive.org
[89] [назад] Wikipedia, IMEI en.wikipedia.org Wikiless Archive.org
[90] [назад] Wikipedia, IMSI en.wikipedia.org Wikiless Archive.org
[91] [назад] Android Documentation, Device Identifiers source.android.com Archive.org
[92] [назад] Google Privacy Policy, Look for IMEI policies.google.com Archive.org
[93] [назад] Wikipedia, IMEI and the Law en.wikipedia.org Wikiless Archive.org
[94] [назад] Bellingcat, The GRU Globetrotters: Mission London bellingcat.com Archive.org
[95] [назад] Bellingcat,"V" For "Vympel": FSB's Secretive Department "V" Behind Assassination Of Georgian Asylum Seeker In Germany bellingcat.com Archive.org
[96] [назад] Wikipedia, CCTV en.wikipedia.org Wikiless Archive.org
[97] [назад] Apple, Transparency Report, Device Requests apple.com Archive.org
[98] [назад] The Intercept, How Cops Can Secretly Track Your Phone theintercept.com Tor Mirror Archive.org
[99] [назад] Wikipedia, IMSI Catcher en.wikipedia.org Wikiless Archive.org
[100] [назад] Wikipedia, Stingray en.wikipedia.org Wikiless Archive.org

[101] [назад] Gizmodo, Cops Turn to Canadian Phone-Tracking Firm After Infamous 'Stingrays' Become 'Obsolete' gizmodo.com Archive.org
[102] [назад] Purism, Librem 5 shop.puri.sm Archive.org
[103] [назад] Wikipedia, MAC Address en.wikipedia.org Wikiless Archive.org
[104] [назад] Acyclica Road Trend Product Sheet, web.archive.org Archive.org
[105] [назад] ResearchGate, Tracking Anonymized Bluetooth Devices researchgate.net Archive.org
[106] [назад] Wikipedia, CPU en.wikipedia.org Wikiless Archive.org
[107] [назад] Wikipedia, Intel Management Engine en.wikipedia.org Wikiless Archive.org
[108] [назад] Wikipedia, AMD Platform Security Processor en.wikipedia.org Wikiless Archive.org
[109] [назад] Wikipedia, IME, Security Vulnerabilities en.wikipedia.org Wikiless Archive.org
[110] [назад] Wikipedia, IME, Assertions that ME is a backdoor en.wikipedia.org Wikiless Archive.org
[111] [назад] Wikipedia, IME, Disabling the ME en.wikipedia.org Wikiless Archive.org
[112] [назад] Libreboot, libreboot.org Archive.org / Coreboot, coreboot.org Archive.org
[113] [назад] Trinity College Dublin, Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google scss.tcd.ie Archive.org
[114] [назад] Apple, Differential Privacy White Paper apple.com Archive.org
[115] [назад] Wikipedia, Differential Privacy en.wikipedia.org Wikiless Archive.org
[116] [назад] Continuing Ed, The All-Seeing "i": Apple Just Declared War on Your Privacy edwardsnowden.substack.com Archive.org
[117] [назад] Reuters, Exclusive: Apple dropped plan for encrypting backups after FBI complained -- sources reuters.com Archive.org
[118] [назад] ZDnet, I asked Apple for all my data. Here's what was sent back zdnet.com Archive.org
[119] [назад] De Correspondent, Here's how we found the names and addresses of soldiers and secret agents using a simple fitness app decorrespondent.nl Archive.org
[120] [назад] Website Planet, Report: Fitness Tracker Data Breach Exposed 61 Million Records and User Data Online websiteplanet.com Archive.org
[121] [назад] Wired, The Strava Heat Map and the End of Secrets wired.com Archive.org
[122] [назад] Bellingcat, How to Use and Interpret Data from Strava's Activity Map bellingcat.com Archive.org
[123] [назад] The Guardian, Fitness tracking app Strava gives away location of secret US army bases theguardian.com Archive.org
[124] [назад] Telegraph, Running app reveals locations of secret service agents in MI6 and GCHQ telegraph.co.uk Archive.org
[125] [назад] Washington Post, Alexa has been eavesdropping on you this whole time washingtonpost.com Archive.org
[126] [назад] Washington Post, What does your car know about you? We hacked a Chevy to find out washingtonpost.com Archive.org
[127] [назад] The Intercept, NSA Leaker Reality Winner Identified in Part Through Printer Tracking Dots theintercept.com Archive.org
[128] [назад] BBC News, Downing Street dossier 'was plagiarised' news.bbc.co.uk Archive.org
[129] [назад] Using Metadata to find Paul Revere (kieranhealy.org Archive.org)
[130] [назад] Wikipedia, Google SensorVault, en.wikipedia.org Wikiless Archive.org
[131] [назад] NRKBeta, My Phone Was Spying on Me, so I Tracked Down the Surveillants nrkbeta.no Archive.org
[132] [назад] New York Times nytimes.com Archive.org
[133] [назад] Sophos, Google data puts innocent man at the scene of a crime nakedsecurity.sophos.com Archive.org
[134] [назад] Wikipedia, Geofence Warrant en.wikipedia.org Wikiless Archive.org
[135] [назад] Vice.com, Military Unit That Conducts Drone Strikes Bought Location Data From Ordinary Apps vice.com Archive.org
[136] [назад] TechCrunch, Google says geofence warrants make up one-quarter of all US demands techcrunch.com Archive.org
[137] [назад] TechDirt, Google Report Shows 'Reverse Warrants' Are Swiftly Becoming Law Enforcement's Go-To Investigative Tool techdirt.com Archive.org
[138] [назад] Vice.com, Here's the FBI's Internal Guide for Getting Data from AT&T, T-Mobile, Verizon vice.com Archive.org
[139] [назад] Wikipedia, Room 641A en.wikipedia.org Wikiless Archive.org
[140] [назад] Wikipedia, Edward Snowden en.wikipedia.org Wikiless Archive.org
[141] [назад] Wikipedia, Permanent Record en.wikipedia.org Wikiless Archive.org
[142] [назад] Wikipedia, XKEYSCORE en.wikipedia.org Wikiless Archive.org
[143] [назад] ElectroSpaces, Danish military intelligence uses XKEYSCORE to tap cables in cooperation with the NSA electrospaces.net Archive.org
[144] [назад] Wikipedia, MUSCULAR en.wikipedia.org Archive.org
[145] [назад] Wikipedia, SORM en.wikipedia.org Wikiless Archive.org
[146] [назад] Wikipedia, Tempora en.wikipedia.org Wikiless Archive.org
[147] [назад] Wikipedia, PRISM en.wikipedia.org Wikiless Archive.org
[148] [назад] Justsecurity, General Hayden justsecurity.org Archive.org
[149] [назад] IDMB, The Social Dilemma imdb.com Archive.org
[150] [назад] ArsTechnica, How the way you type can shatter anonymity---even on Tor arstechnica.com Archive.org
[151] [назад] Wikipedia, Stylometry en.wikipedia.org Wikiless Archive.org
[152] [назад] Paul Moore Blog, Behavioral Profiling: The password you can't change. paul.reviews Archive.org
[153] [назад] Wikipedia, Sentiment Analysis en.wikipedia.org Wikiless Archive.org
[154] [назад] EFF, CoverYourTracks coveryourtracks.eff.org Archive.org
[155] [назад] Berkeley.edu, On the Feasibility of Internet-Scale Author Identification people.eecs.berkeley.edu Archive.org
[156] [назад] Forbes, Exclusive: Government Secretly Orders Google To Identify Anyone Who Searched A Sexual Assault Victim's Name, Address And Telephone Number forbes.com Archive.org
[157] [назад] FingerprintJS, Demo: Disabling JavaScript Won't Save You from Fingerprinting fingerprintjs.com Archive.org
[158] [назад] SecuredTouch Blog, Behavioral Biometrics 101: Behavioral Biometrics vs. Behavioral Analytics blog.securedtouch.com Archive.org
[159] [назад] Wikipedia, Captcha en.wikipedia.org Wikiless Archive.org
[160] [назад] ArsTechnica, Stakeout: how the FBI tracked and busted a Chicago Anon arstechnica.com Archive.org
[161] [назад] Bellingcat MH17 - Russian GRU Commander 'Orion' Identified as Oleg Ivannikov bellingcat.com Archive.org
[162] [назад] Facebook Research, Deepface research.fb.com Archive.org
[163] [назад] Privacy News Online, Putting the "face" in Facebook: how Mark Zuckerberg is building a world without public anonymity privateinternetaccess.com Archive.org
[164] [назад] CNBC, "Facebook has mapped populations in 23 countries as it explores satellites to expand internet" cnbc.com Archive.org
[165] [назад] MIT Technology Review, This is how we lost control of our faces, technologyreview.com Archive.org

[166] [назад] Bellingcat, Shadow of a Doubt: Crowdsourcing Time Verification of the MH17 Missile Launch Photo bellingcat.com Archive.org
[167] [назад] Brown Institute, Open-Source Investigation, brown.columbia.edu Archive.org
[168] [назад] NewScientist, Facebook can recognize you in photos even if you're not looking newscientist.com Archive.org
[169] [назад] Google Patent, Techniques for emotion detection and content delivery patentimages.storage.googleapis.com Archive.org
[170] [назад] APNews, Chinese 'gait recognition' tech IDs people by how they walk apnews.com Archive.org
[171] [назад] The Sun, New CCTV technology could now identify you just by the WAY you walk and your body shape thesun.co.uk Archive.org
[172] [назад] City Security Magazine, Gait recognition: a useful identification tool citysecuritymagazine.com Archive.org
[173] [назад] Vice.com, Tech Companies Are Training AI to Read Your Lips vice.com Archive.org
[174] [назад] New Atlas, Eye tracking can reveal an unbelievable amount of information about you newatlas.com Archive.org
[175] [назад] TechCrunch, Facial recognition reveals political party in troubling new research techcrunch.com Archive.org
[176] [назад] Nature.com, Facial recognition technology can expose political orientation from naturalistic facial images nature.com Archive.org
[177] [назад] Slate slate.com Archive.org
[178] [назад] The Conversation theconversation.com Archive.org
[179] [назад] The Verge theverge.com Archive.org
[180] [назад] ZDNET zdnet.com Archive.org
[181] [назад] CNET cnet.com Archive.org
[182] [назад] Oosto oosto.com Archive.org
[183] [назад] BuzzFeed.news, Surveillance Nation buzzfeednews.com Archive.org
[184] [назад] Wired, Clearview AI Has New Tools to Identify You in Photos wired.com Archive.org
[185] [назад] NEC, Neoface nec.com Archive.org
[186] [назад] The Guardian, Met police deploy live facial recognition technology theguardian.com Archive.org
[187] [назад] YouTube, The Economist, China: facial recognition and state control youtube.com Invidious
[188] [назад] CNN, Want your unemployment benefits? You may have to submit to facial recognition first edition.cnn.com Archive.org
[189] [назад] Washington Post, Huawei tested AI software that could recognize Uighur minorities and alert police, report says washingtonpost.com Archive.org
[190] [назад] The Intercept, How a Facial Recognition Mismatch Can Ruin Your Life theintercept.com Tor Mirror Archive.org
[191] [назад] Vice, Facial Recognition Failures Are Locking People Out of Unemployment Systems vice.com Archive.org
[192] [назад] BBC, WhatsApp photo drug dealer caught by 'groundbreaking' work bbc.com Archive.org
[193] [назад] CNN, Drug dealer jailed after sharing a photo of cheese that included his fingerprints edition.cnn.com Archive.org
[194] [назад] Vice.com, Cops Got a Drug Dealer's Fingerprints From Photos of His Hand on WhatsApp vice.com Archive.org
[195] [назад] Kraken Blog, blog.kraken.com Archive.org
[196] [назад] JUSTIA Patent, Identification of taste attributes from an audio signal patents.justia.com Archive.org
[197] [назад] PYMNTS, Iris Scan Serves As Traveler ID At Dubai Airport pymnts.com Archive.org
[198] [назад] IMDB, Gattaca 1997, imdb.com Archive.org
[199] [назад] IMDB, Person of Interest 2011 imdb.com Archive.org
[200] [назад] IMDB, Minority Report 2002, imdb.com Archive.org
[201] [назад] Wikipedia, Deepfake en.wikipedia.org Wikiless Archive.org
[202] [назад] Econotimes, Deepfake Voice Technology: The Good. The Bad. The Future econotimes.com Archive.org
[203] [назад] Wikipedia, Deepfake Events en.wikipedia.org Wikiless Archive.org
[204] [назад] Forbes, A Voice Deepfake Was Used To Scam A CEO Out Of $243,000 forbes.com Archive.org
[205] [назад] Joseph Steinberg, How To Prevent Facial Recognition Technology From Identifying You josephsteinberg.com Archive.org
[206] [назад] NIST, Face recognition accuracy with masks using pre-COVID-19 algorithms nvlpubs.nist.gov Archive.org
[207] [назад] BBC, Facial recognition identifies people wearing masks bbc.com Archive.org
[208] [назад] University of Wisconsin, Exploring Reflectacles As Anti-Surveillance Glasses and for Adversarial Machine Learning in Computer Vision diglib.uwgb.edu Archive.org
[209] [назад] Wikipedia, Phishing en.wikipedia.org Wikiless Archive.org
[210] [назад] Wikipedia, Social Engineering en.wikipedia.org Wikiless Archive.org
[211] [назад] BBC, Spy pixels in emails have become endemic bbc.com Archive.org
[212] [назад] Vice, Facebook Helped the FBI Hack a Child Predator vice.com Archive.org
[213] [назад] Wikipedia, Exploit en.wikipedia.org Wikiless Archive.org
[214] [назад] Wikipedia, Freedom Hosting en.wikipedia.org Wikiless Archive.org
[215] [назад] Wired, 2013 FBI Admits It Controlled Tor Servers Behind Mass Malware Attack wired.com Archive.org
[216] [назад] Wikipedia, 2020 United States federal government data breach en.wikipedia.org Wikiless Archive.org
[217] [назад] BBC, China social media: WeChat and the Surveillance State bbc.com Archive.org
[218] [назад] The Intercept, Revealed: Massive Chinese Police Database theintercept.com Tor Mirror Archive.org
[219] [назад] Wikipedia, Sandbox en.wikipedia.org Wikiless Archive.org
[220] [назад] Wired, Why the Security of USB Is Fundamentally Broken wired.com Archive.org
[221] [назад] Wikipedia, Stuxnet en.wikipedia.org Wikiless Archive.org
[222] [назад] Superuser.com, How do I safely investigate a USB stick found in the parking lot at work? superuser.com Archive.org
[223] [назад] The Guardian, Glenn Greenwald: how the NSA tampers with US-made internet routers theguardian.com Archive.org
[224] [назад] Wikipedia, Rootkit en.wikipedia.org Wikiless Archive.org
[225] [назад] Wikipedia, Userspace en.wikipedia.org Wikiless Archive.org
[226] [назад] Wikipedia, Firmware en.wikipedia.org Wikiless Archive.org
[227] [назад] Wikipedia, BIOS en.wikipedia.org Wikiless Archive.org
[228] [назад] Wikipedia, UEFI en.wikipedia.org Wikiless Archive.org
[229] [назад] Wikipedia, UEFI en.wikipedia.org Wikiless Archive.org
[230] [назад] ESET, LoJax: First UEFI rootkit found in the wild eset.com Archive.org
[231] [назад] Kaspersky, MosaicRegressor: Lurking in the Shadows of UEFI securelist.com Archive.org
[232] [назад] Wikipedia, Secure Boot en.wikipedia.org Wikiless Archive.org
[233] [назад] Heads firmware project osresearch.net Archive.org
[234] [назад] GitHub, USBGuard github.com Archive.org
[235] [назад] Der Spiegel, NSA ANT catalogue spiegel.de Archive.org
[236] [назад] Bellingcat, Joseph Mifsud: Rush for the EXIF bellingcat.com Archive.org

[237] [назад] Zoom Support, Adding a watermark support.zoom.us Archive.org
[238] [назад] Zoom Support, Audio Watermark support.zoom.us Archive.org
[239] [назад] CreativeCloud Extension, IMATAG exchange.adobe.com Archive.org
[240] [назад] NexGuard, dtv.nagra.com Archive.org
[241] [назад] Vobile Solutions, vobilegroup.com Archive.org
[242] [назад] Cinavia, cinavia.com Archive.org
[243] [назад] Imatag, imatag.com Archive.org
[244] [назад] Wikipedia, Steganography en.wikipedia.org Wikiless Archive.org
[245] [назад] IEEExplore, A JPEG compression resistant steganography scheme for raster graphics images ieeexplore.ieee.org Archive.org
[246] [назад] ScienceDirect, Robust audio watermarking using perceptual masking researchgate.net Archive.org
[247] [назад] IEEExplore, Spread-spectrum watermarking of audio signals researchgate.net Archive.org
[248] [назад] Google Scholar, source camera identification scholar.google.com Archive.org
[249] [назад] Wikipedia, Printing Steganography en.wikipedia.org Wikiless Archive.org
[250] [назад] MIT, SeeingYellow, web.archive.org Archive.org
[251] [назад] arXiv, An Analysis of Anonymity in the Bitcoin System arxiv.org Archive.org
[252] [назад] Bellingcat, How To Track Illegal Funding Campaigns Via Cryptocurrency, bellingcat.com Archive.org
[253] [назад] CoinDesk, Leaked Slides Show How Chainalysis Flags Crypto Suspects for Cops coindesk.com Archive.org
[254] [назад] Wikipedia, KYC en.wikipedia.org Wikiless Archive.org
[255] [назад] arXiv.org, Probing the Mystery of Cryptocurrency Theft: An Investigation into Methods for Taint Analysis arxiv.org Archive.org
[256] [назад] YouTube, Breaking Monero youtube.com Invidious
[257] [назад] Monero, Monero vs Princeton Researchers, monero.org Archive.org
[258] [назад] Wikipedia, Cryptocurrency Tumbler en.wikipedia.org Wikiless Archive.org
[259] [назад] Wikipedia, Security Through Obscurity en.wikipedia.org Wikiless Archive.org
[260] [назад] ArXiv, Tracking Mixed Bitcoins arxiv.org Archive.org
[261] [назад] SSRN, The Cryptocurrency Tumblers: Risks, Legality and Oversight researchgate.net Archive.org
[262] [назад] Magnet Forensics, Magnet AXIOM magnetforensics.com Archive.org
[263] [назад] Cellebrite, Unlock cloud-based evidence to solve the case sooner cellebrite.com Archive.org
[264] [назад] Property of the People, Lawful Access to Secure Messaging Apps Data, propertyofthepeople.org Archive.org
[265] [назад] Grayshift, grayshift.com Archive.org
[266] [назад] Securephones.io, Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions securephones.io Archive.org
[267] [назад] Loup-Vaillant.fr, Rolling Your Own Crypto loup-vaillant.fr Archive.org
[268] [назад] Dhole Moments, Crackpot Cryptography and Security Theater soatok.blog Archive.org
[269] [назад] Vice.com, Why You Don't Roll Your Own Crypto vice.com Archive.org
[270] [назад] arXiv, MIT, You Really Shouldn't Roll Your Own Crypto: An Empirical Study of Vulnerabilities in Cryptographic Libraries arxiv.org Archive.org
[271] [назад] YouTube, Great Crypto Failures youtube.com Invidious
[272] [назад] Cryptography Dispatches, The Most Backdoor-Looking Bug I've Ever Seen buttondown.email Archive.org
[273] [назад] Citizenlab.ca, Move Fast and Roll Your Own Crypto citizenlab.ca Archive.org
[274] [назад] Jack Poon, The myth of military grade encryption medium.com Scribe.rip Archive.org
[275] [назад] Congruent Labs, Stop calling it "Military-Grade Encryption" blog.congruentlabs.co Archive.org
[276] [назад] IronCoreLabs Blog, "Military Grade Encryption" blog.ironcorelabs.com Archive.org
[277] [назад] Wikipedia, BLAKE2, en.wikipedia.org Wikiless Archive.org
[278] [назад] Wikipedia, AES Instruction Set, en.wikipedia.org Wikiless Archive.org
[279] [назад] Wikipedia, ChaCha Variants, en.wikipedia.org Wikiless Archive.org
[280] [назад] Wikipedia, Serpent, en.wikipedia.org Wikiless Archive.org
[281] [назад] Wikipedia, TwoFish, en.wikipedia.org Wikiless Archive.org
[282] [назад] Lacatora, The PGP Problem latacora.singles Archive.org
[283] [назад] Wikipedia, Shor's Algorithm, en.wikipedia.org Wikiless Archive.org
[284] [назад] Wikipedia, Gag Order, en.wikipedia.org Wikiless Archive.org
[285] [назад] Wikipedia, National Security Letter en.wikipedia.org Wikiless Archive.org
[286] [назад] ArsTechnica, VPN servers seized by Ukrainian authorities weren't encrypted arstechnica.com Archive.org
[287] [назад] BleepingComputer, DoubleVPN servers, logs, and account info seized by law enforcement bleepingcomputer.com Archive.org
[288] [назад] CyberScoop, Court rules encrypted email provider Tutanota must monitor messages in blackmail case cyberscoop.com Archive.org
[289] [назад] Heise Online (German), heise.de Archive.org
[290] [назад] PCMag, Did PureVPN Cross a Line When It Disclosed User Information? pcmag.com Archive.org
[291] [назад] Internet Archive, Wipeyourdata, "No logs" EarthVPN user arrested after police finds logs archive.is Archive.org
[292] [назад] Wikipedia, Lavabit Suspension and Gag order, en.wikipedia.org Wikiless Archive.org
[293] [назад] Internet Archive, Invisibler, What Everybody Ought to Know About HideMyAss archive.is
[294] [назад] Wikipedia, Warrant Canary en.wikipedia.org Wikiless Archive.org
[295] [назад] Washington Post, The intelligence coup of the century washingtonpost.com Archive.org
[296] [назад] Swissinfo.ch, Second Swiss firm allegedly sold encrypted spying devices swissinfo.ch Archive.org
[297] [назад] Wikipedia, Das Leben der Anderen en.wikipedia.org Wikiless Archive.org
[298] [назад] Wired, Mind the Gap: This Researcher Steals Data With Noise, Light, and Magnets wired.com Archive.org
[299] [назад] Scientific American, A Blank Wall Can Show How Many People Are in a Room and What They're Doing scientificamerican.com Archive.org
[300] [назад] Scientific American, A Shiny Snack Bag's Reflections Can Reconstruct the Room around It scientificamerican.com Archive.org
[301] [назад] Scientific American, Footstep Sensors Identify People by Gait scientificamerican.com Archive.org
[302] [назад] Ben Nassi, Lamphone nassiben.com Archive.org
[303] [назад] The Guardian, Laser spying: is it really practical? theguardian.com Archive.org
[304] [назад] ArsTechnica, Photos of an NSA "upgrade" factory show Cisco router getting implant arstechnica.com Archive.org

Общая подготовка

Лично мне, в контексте этого руководства, также интересно посмотреть на вашу модель безопасности. И в этом контексте мы можем рекомендовать только одну:

Zero-Trust Security[1] («Никогда не доверяй, всегда проверяй»).

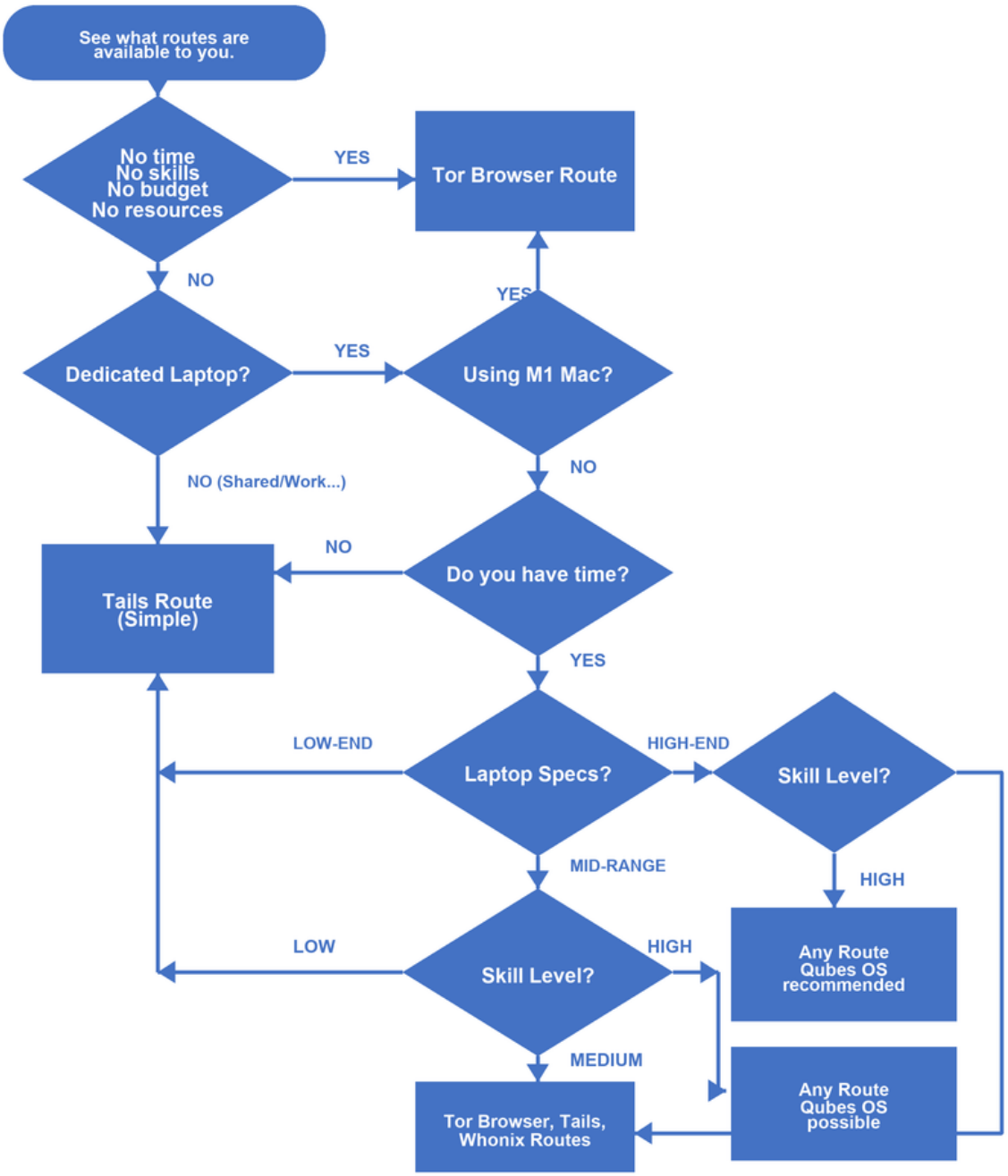
Вот несколько ресурсов о том, что такое Zero-Trust Security:

• DEFCON, Zero Trust a Vision for Securing Cloud, youtube.com Invidious

• От самого NSA, Embracing a Zero Trust Security Model, media.defense.gov Archive.org

Выбор маршрута

Сначала вот небольшая базовая UML-диаграмма, показывающая доступные варианты в зависимости от ваших навыков, бюджета, времени и ресурсов.



Ограничения по времени

• У вас совсем нет времени:

  • **Выбирайте маршрут Tor Browser.**

• У вас крайне мало времени на обучение, и вам нужно быстро работающее решение:

  • **Лучший вариант — выбрать маршрут Tails, без раздела о постоянном правдоподобном отрицании.**

• У вас есть время и, что важнее, мотивация учиться:

  • **Подойдёт любой маршрут.**

Ограничения бюджета и оборудования

- У вас нет бюджета, даже доступ к ноутбуку затруднён, или у вас есть только смартфон:
    - **Выбирайте маршрут Tor Browser.**
- У вас есть только один ноутбук, и вы не можете позволить себе ничего другого. Вы используете этот ноутбук для работы, семьи или личных дел, либо для всего сразу:
    - **Лучший вариант — выбрать маршрут Tails.**
- Вы можете позволить себе отдельный выделенный ноутбук без внешнего контроля и наблюдения для чувствительных действий:
    - Но он старый, медленный и со слабыми характеристиками (меньше 6 ГБ RAM, меньше 250 ГБ дискового пространства, старый или медленный процессор):
        - **Вам следует выбрать маршрут Tails.**
    - Он не такой старый и имеет нормальные характеристики (минимум 8 ГБ RAM, 250 ГБ дискового пространства или больше, нормальный процессор):
        - **Можно выбрать маршруты Tails или Whonix.**
    - Он новый и имеет отличные характеристики (больше 16 ГБ, а в идеале 32 ГБ RAM, больше 250 ГБ дискового пространства, современный быстрый процессор):
        - Можно выбрать любой маршрут, но мы рекомендовали бы Qubes OS, если ваша модель угроз это допускает. Пожалуйста, смотрите требования.[2]
    - Если это Mac на ARM, например M1/M2:
        - **Сейчас это невозможно по следующим причинам:**
            - Виртуализация образов Intel x86 на ARM-хостах (M1/M2) всё ещё ограничена коммерческим ПО, например Parallels или Fusion, которое в основном пока не поддерживается Whonix. Эти варианты очень нестабильны и подходят только продвинутым людям. Пожалуйста, самостоятельно изучите эту информацию.
            - Virtualbox теперь доступен нативно для архитектуры ARM64 в виде пакета по состоянию на октябрь 2022 года. Скачайте "Developer preview for macOS/Arm64 (M1/M2) hosts".
            - Whonix нелегко поддерживает macOS. «You need to build Whonix using the build script to get it running on Apple Silicon.» См. тему на форуме.
            - Tails пока не поддерживается на архитектуре ARM64. См. эту тему для подробностей, учитывая, что страница давно не обновлялась.
            - Qubes OS пока не поддерживается на архитектуре ARM64, хотя ведётся работа над доступностью на aarch64; она может задержаться на неопределённое будущее.

Общий совет этого руководства относительно программ виртуализации: это затратно. Тем не менее вам, вероятно, стоит получить отдельный ноутбук, способный запускать ПО виртуализации, желательно с 64-битной архитектурой, чтобы использовать его для более чувствительных действий и тестирования.

Навыки

• У вас совсем нет ИТ-навыков, и содержимое этого руководства выглядит как язык инопланетян? Рассмотрите:

  • **маршрут Tor Browser, самый простой из всех;**

  • **маршрут Tails, без раздела о постоянном правдоподобном отрицании.**

• У вас есть некоторые ИТ-навыки, и вы в целом понимаете это руководство на данный момент? Рассмотрите:

  • **маршрут Tails, с необязательным разделом о постоянном правдоподобном отрицании;**

  • **маршрут Whonix.**

• У вас средние или высокие ИТ-навыки, и вы уже знакомы с частью содержимого этого руководства? Рассмотрите:

  • **любой маршрут; Qubes OS предпочтительна, если вы можете себе это позволить.**

• Вы l33T-хакер, «there is no spoon», «the cake is a lie», вы годами пользуетесь `doas`, «all your base are belong to us», и у вас сильные мнения о systemd.

  • **Это руководство не предназначено для вас и не поможет с вашим HardenedBSD на защищённом ноутбуке с Libreboot ;-)**

Соображения о противниках

Теперь, когда вы знаете, что возможно, перед выбором подходящего маршрута нужно также учитывать угрозы и противников.

Угрозы

• Если ваша главная забота — криминалистическое исследование ваших устройств, стоит рассмотреть маршрут Tor Browser или маршрут Tails.

• Если ваша главная забота — удалённые противники, которые могут раскрыть вашу онлайн-личность на разных платформах, стоит рассмотреть маршруты Tails, Whonix или Qubes OS, перечисленные по возрастанию сложности.

• Если вы хотите системное правдоподобное отрицание[3][4], несмотря на риски[5][6], рассмотрите маршрут Tails, включая раздел о постоянном правдоподобном отрицании (см. Постоянное правдоподобное отрицание с Whonix и Tails).

• Если вы находитесь во враждебной среде, где одно только использование Tor/VPN невозможно, опасно или подозрительно, рассмотрите маршрут Tails (без фактического использования Tor) или более продвинутые маршруты вроде Whonix или Qubes OS.

Противники

- Низкие навыки:
  - Низкие ресурсы:
    - Любая мотивация: любой маршрут
  - Средние ресурсы:
    - Низкая или средняя мотивация: любой маршрут
    - Высокая мотивация: маршруты Tails, Whonix, Qubes OS
  - Высокие ресурсы:
    - Низкая мотивация: любой маршрут
    - Средняя или высокая мотивация: маршруты Tails, Whonix, Qubes OS
- Средние навыки:
  - Низкие ресурсы:
    - Низкая мотивация: любой маршрут
    - Средняя или высокая мотивация: маршруты Tails, Whonix, Qubes OS
  - Средние ресурсы:
    - Низкая мотивация: любой маршрут
    - Средняя или высокая мотивация: маршруты Tails, Whonix, Qubes OS
  - Высокие ресурсы:
    - Низкая или высокая мотивация: маршруты Tails, Whonix, Qubes OS
- Высокие навыки:
  - Низкие ресурсы:
    - Низкая мотивация: любой маршрут
    - Средняя или высокая мотивация: маршруты Tails, Whonix, Qubes OS
  - Средние ресурсы:
    - Низкая или высокая мотивация: маршруты Tails, Whonix, Qubes OS
  - Высокие ресурсы:
    - Низкая или высокая мотивация: маршруты Tails, Whonix, Qubes OS **(но, вероятно, это выходит за рамки руководства, потому что это, скорее всего, глобальный противник)**

В любом случае вам стоит прочитать эти две страницы документации Whonix, которые подробно объясняют ваши варианты:

- Warning Archive.org
- Dev/Threat Model Archive.org
- Comparison with Others Archive.org

Возможно, вы спрашиваете себя: «Как понять, нахожусь ли я во враждебной онлайн-среде, где активность активно отслеживается и блокируется?»

- Сначала прочитайте об этом у EFF здесь: ssd.eff.org Archive.org

• Проверьте некоторые данные самостоятельно на сайте Tor Project OONI[7] (Open Observatory of Network Interference): explorer.ooni.org

• Посмотрите censoredplanet.org и проверьте, есть ли у них данные о вашей стране.

• Для Китая отдельно посмотрите gfwatch.org и usenix.org Archive.org

• Проверьте самостоятельно с помощью OONI; во враждебной среде это может быть рискованно.

Шаги для всех маршрутов

Привыкнуть использовать более надёжные пароли

См. Рекомендации по паролям и парольным фразам.

Получение анонимного номера телефона

Пропустите этот шаг, если вы не собираетесь создавать анонимные учётные записи на большинстве массовых платформ, а хотите только анонимный просмотр, или если платформы, которыми вы будете пользоваться, разрешают регистрацию без номера телефона.

Физический одноразовый телефон и предоплаченная SIM-карта

Получить одноразовый телефон

Это довольно просто. Оставьте смартфон включённым дома. Возьмите наличные и сходите на случайный блошиный рынок или в небольшой магазин, в идеале без камер наблюдения внутри и снаружи, избегая фотографирования и видеозаписи, и просто купите самый дешёвый телефон, который найдёте, за наличные и без предоставления личной информации. Нужно только, чтобы он был рабочим.

Примечание о вашем текущем телефоне: смысл оставить смартфон включённым — не раскрыть тот факт, что вы не пользуетесь устройством. Если смартфон выключен, это создаёт след метаданных, который можно использовать для сопоставления времени отключения смартфона с включением одноразового телефона. Если возможно, оставьте телефон чем-то занятым, например включите YouTube с автопроигрыванием, чтобы дополнительно замаскировать след метаданных. Это не сделает корреляцию вашей неактивности невозможной, но может усложнить её, если шаблоны использования телефона выглядят убедительно, пока вы покупаете одноразовый телефон.

Мы рекомендовали бы взять старый «глупый телефон» со съёмной батареей, например старую Nokia, если ваши мобильные сети всё ещё позволяют таким телефонам подключаться, потому что некоторые страны полностью вывели из эксплуатации 1G-2G. Это нужно, чтобы избежать автоматической отправки и сбора телеметрии или диагностических данных на самом телефоне. Никогда не подключайте такой телефон к Wi-Fi.

Примечание сайта: будьте осторожны с некоторыми продавцами, как показано здесь therecord.media Archive.org

Также будет критически важно никогда не включать этот одноразовый телефон, даже без SIM-карты, в любом географическом месте, которое может привести к вам, например дома или на работе, и никогда в том же месте, где находится ваш другой известный смартфон, потому что у него есть IMEI/IMSI, которые легко приведут к вам. Это может казаться большой нагрузкой, но на практике нет: такие телефоны используются только во время настройки, регистрации и иногда для проверки.

См. Предупреждение о смартфонах и умных устройствах.

Перед переходом к следующему шагу нужно проверить, что телефон исправен. Но мы повторимся: важно оставить смартфон дома, когда вы идёте за этим, или выключить его перед выходом, если вы обязаны взять его с собой, и проверять телефон в случайном месте, которое нельзя связать с вами. И снова: не делайте это перед камерой наблюдения, избегайте камер, следите за окружением. Wi-Fi в этом месте тоже не нужен.

Когда вы убедились, что телефон исправен, отключите Bluetooth, затем выключите его, выньте батарею, если можете, вернитесь домой и продолжайте обычные дела. Переходите к следующему шагу.

Получение анонимной предоплаченной SIM-карты

Это самая трудная часть всего руководства. Это единая точка отказа (SPOF, Single Point of Failure). Мест, где всё ещё можно купить предоплаченные SIM-карты без регистрации по документу, становится всё меньше из-за разных правил типа KYC[8].

Вот список мест, где их всё ещё можно получить сейчас: prepaid-data-sim-card.fandom.com Archive.org

Вы должны найти место «не слишком далеко» и физически поехать туда, чтобы купить предоплаченные карты и ваучеры пополнения за наличные. Перед поездкой проверьте, не был ли принят закон, делающий регистрацию обязательной, на случай если указанная wiki не обновлена. Старайтесь избегать камер наблюдения и камер вообще, и не забудьте купить ваучер пополнения вместе с SIM-картой, если это не комплект, потому что большинство предоплаченных карт требует пополнения перед использованием.

См. Предупреждение о смартфонах и умных устройствах.

Перед поездкой дважды проверьте, что мобильные операторы, продающие предоплаченные SIM-карты, разрешат активацию SIM и пополнение без какой-либо регистрации по документу. В идеале они должны позволять активацию SIM и пополнение из страны, где вы живёте.

Мы бы рекомендовали GiffGaff в Великобритании: он «доступен по цене», не требует идентификации для активации и пополнения и даже позволяет менять номер до двух раз через сайт. Поэтому одна предоплаченная SIM-карта GiffGaff даст вам три номера для ваших нужд.

Выключите телефон после активации/пополнения и до возвращения домой. Больше никогда не включайте его в месте, которое может раскрыть вашу личность; в идеале перед поездкой в безопасное место с одним только одноразовым телефоном оставьте настоящий телефон включённым, но дома.

Онлайн-номер телефона

ОТКАЗ ОТ ОТВЕТСТВЕННОСТИ: не пытайтесь делать это, пока не закончите настройку безопасной среды по одному из выбранных маршрутов. Этот шаг требует онлайн-доступа и должен выполняться только из анонимной сети. Не делайте это из какой-либо известной или небезопасной среды. Пропустите это, пока не закончите один из маршрутов.

Существует много коммерческих сервисов, предлагающих номера для получения SMS онлайн, но у большинства из них нет анонимности/приватности, и они могут оказаться бесполезны, потому что большинство социальных платформ ограничивает количество регистраций на один телефонный номер.

Есть форумы и сабреддиты, например r/phoneverification/, где пользователи предлагают за небольшую плату получить такие SMS за вас, используя PayPal или какую-нибудь криптовалюту. К сожалению, там полно мошенников, и это очень рискованно с точки зрения анонимности. **Не используйте их ни при каких обстоятельствах.**

На сегодняшний день мы не знаем авторитетного сервиса, который предлагал бы такую услугу и принимал оплату наличными, например по почте, как некоторые VPN-провайдеры. Но несколько сервисов предоставляют онлайн-номера и принимают Monero, что может быть достаточно анонимно, хотя менее рекомендуется, чем физический способ из предыдущего раздела:

• **Рекомендуемые**: не требуют никакой идентификации, даже электронной почты:

  • (Исландия, принимает Monero) crypton.sh Tor Mirror Archive.org

  • (Украина, принимает Monero) virtualsim.net Archive.org

• Требуют идентификацию в виде действительной электронной почты:

  • (США, Калифорния, принимает Monero) mobilesms.io Archive.org

  • (Германия, принимает Monero) sms77.io Archive.org

  • (Россия, принимает Monero) onlinesim.ru Archive.org

Другие возможности перечислены здесь: cryptwerk.com Archive.org. **Используйте на свой риск.**

А что если у вас нет денег? В таком случае придётся попытать удачу с бесплатными сервисами и надеяться на лучшее. Вот несколько примеров, **используйте на свой риск**:

• oksms.org

• smspva.com

• sms24.me

Отказ от ответственности: мы не можем ручаться ни за одного из этих поставщиков. Мы рекомендуем сделать это физически самостоятельно. В таком случае вам придётся полагаться на анонимность Monero, и не следует использовать сервис, требующий какой-либо идентификации вашей настоящей личности. Пожалуйста, прочитайте Предупреждение о Monero.

Удобнее, дешевле и менее рискованно просто получить предоплаченную SIM-карту в одном из физических мест, где их всё ещё продают за наличные без документа.

Получить USB-накопитель

Пропустите этот шаг, если вы не собираетесь создавать анонимные учётные записи на большинстве массовых платформ, но хотите анонимный просмотр; или если платформы, которыми вы будете пользоваться, разрешают регистрацию без номера телефона.

Получите хотя бы один или два обычных USB-накопителя нормального размера: минимум 16 ГБ, но мы рекомендовали бы 32 ГБ.

Пожалуйста, не покупайте и не используйте сомнительные самошифрующиеся устройства вроде этих: syscall.eu Archive.org

Некоторые могут быть очень эффективны[9], но многие — это игрушечные устройства, не дающие реальной защиты[10].

Найти безопасные места с нормальным публичным Wi-Fi

Вам нужно найти безопасные места, где вы сможете выполнять чувствительные действия через публично доступный Wi-Fi без регистрации аккаунта или документа и с избеганием камер наблюдения.

Это может быть любое место, которое не связано с вами напрямую, то есть не дом и не работа, и где можно какое-то время пользоваться Wi-Fi без лишнего внимания. Но это также должно быть место, где вы сможете делать это так, чтобы вас никто не «заметил».

Если вы думаете, что Starbucks — хитрая идея, лучше пересмотрите её:

• В их заведениях, вероятно, есть камеры наблюдения, а записи хранятся неизвестное время.

• В большинстве случаев, чтобы получить код доступа к Wi-Fi, нужно купить кофе. Если вы заплатите за этот кофе электронным способом, они смогут связать ваш Wi-Fi-доступ с вашей личностью.

Осведомлённость об обстановке критически важна: нужно постоянно следить за окружением и избегать туристических мест так, будто они заражены Эболой. Вы хотите избежать попадания на чьи-либо фотографии и видео, пока кто-то делает селфи, снимает TikTok или выкладывает туристические фотографии в Instagram. Если вы туда попадёте, помните: высока вероятность, что эти снимки окажутся в интернете, публично или приватно, с полными метаданными (время/дата/данные о местоположении) и вашим лицом. Помните, что это могут и будут индексировать Facebook/Google/Yandex/Apple и, вероятно, все агентства из трёх букв.

Пока это может быть недоступно местной полиции, но в ближайшем будущем может стать доступным.

В идеале вам понадобится набор из 3-5 отдельных мест такого типа, чтобы не использовать одно и то же место дважды. В течение недель для разных шагов этого руководства потребуется несколько поездок.

Также можно рассмотреть подключение к таким местам с безопасного расстояния для дополнительной безопасности. См. Использование дальнобойной антенны для подключения к публичному Wi-Fi с безопасного расстояния.

Маршрут Tor Browser

Эта часть руководства поможет настроить самый простой и лёгкий способ анонимно просматривать веб. Это не обязательно лучший метод: ниже есть более продвинутые методы с гораздо лучшей безопасностью и гораздо лучшими мерами против разных противников. Но это прямой способ быстро и анонимно получить доступ к ресурсам без бюджета, без времени, без навыков и при ограниченном использовании.

Что такое Tor Browser? Tor Browser (torproject.org Archive.org) — это веб-браузер вроде Safari/Firefox/Chrome/Edge/Brave, созданный с учётом приватности и анонимности.

Этот браузер отличается от других тем, что подключается к интернету через сеть Tor с использованием луковой маршрутизации. Сначала мы рекомендуем посмотреть очень хорошее вводное видео от самого Tor Project: youtube.com Invidious. После этого, вероятно, стоит перейти на их страницу и прочитать краткий обзор здесь: 2019.www.torproject.org Archive.org. Без излишних технических деталей: Tor Browser — простое решение в стиле «запустил и забыл» для анонимного просмотра веба почти с любого устройства. Вероятно, его достаточно для большинства людей, и его можно использовать с любого компьютера или смартфона.

Вот несколько способов настроить его для основных ОС.

Предупреждение: не устанавливайте расширения в Tor Browser: они могут использоваться для распознавания вас по цифровому отпечатку и идентификации.

Windows, Linux и macOS

См. Установка и использование настольного Tor Browser.

Android

Примечание о Tor Browser для Android: разработка Tor Browser для Android отстаёт от настольного комплекта Tor Browser Bundle (TBB). Некоторые функции пока недоступны. Например, настольная версия Tor теперь включает автоматические мосты с помощью Moat:

«**Connection Assist** работает, запрашивая и скачивая актуальный список вариантов для конкретной страны, чтобы попробовать их на основе вашего местоположения (с вашего согласия). Ему удаётся сделать это без предварительного подключения к сети Tor, используя moat — тот же инструмент доменного фронтинга, который Tor Browser использует для запроса моста у torproject.org.»

• Перейдите в:

  • Play Store: play.google.com

  • F-Droid Store: его там пока нет, но можно добавить вручную по инструкциям на support.torproject.org Archive.org

• Установите.

• Запустите Tor Browser.

• После запуска нажмите значок **Settings** в правом верхнем углу.

• Выберите **Settings** > **Privacy and security** > **Tor network**.

• Выберите **Config Bridge**.

• Прочитайте Использование мостов Tor во враждебной среде.

• **Если нужно, после чтения приложения выше**, включите параметр и выберите тип моста:

  • Obfs4

  • Meek-Azure

  • Snowflake

• **Если ваш интернет не цензурируется**, подумайте о запуске одного из типов мостов, чтобы помочь сети.

  • Легко: Obsf4 — собственный Obsf4 можно легко запустить по этим инструкциям: community.torproject.org

  • Средне: Snowflake — подробнее о Snowflake здесь: snowflake.torproject.org

  • Сложно: Meek — документация здесь. Это не так просто: gitlab.torproject.org

Лично я, если вам нужно использовать мост (это не нужно в невраждебной среде), выбрал бы Meek-Azure. Такие мосты, вероятно, будут работать даже если вы в Китае и хотите обойти Great Firewall. Это, вероятно, лучший вариант для маскировки активности Tor при необходимости, а серверы Microsoft обычно не блокируются.

*Доступно только пользователям настольного Tor: недавно Tor Project сделал доступ к мостам невероятно простым с помощью **Connection Assist**, и теперь во враждебных или цензурируемых регионах это делается автоматически. Просто откройте Tor Browser, и соединение будет настроено под ваши нужды в любой враждебной сети. Раньше ниже этого абзаца был список вариантов, необходимых для включения и настройки мостов, но теперь это делается автоматически с помощью moat.* Archive.org

• Вы почти закончили.

Как и в настольной версии, нужно знать, что в Tor Browser есть уровни безопасности. На Android к ним можно перейти так:

• Нажмите меню в правом нижнем углу.

• Нажмите **Settings**.

• Перейдите в раздел **Privacy and security**.

• Нажмите **Security Settings**.

Подробности о каждом уровне есть здесь: tb-manual.torproject.org Archive.org, а вот краткое описание:

• Standard (по умолчанию):

  • Включены все функции, включая JavaScript.

• Safer:

  • JavaScript отключён на сайтах без HTTPS.

    - Некоторые шрифты и символы отключены.
    - Воспроизведение любого медиа работает по нажатию, то есть по умолчанию отключено.
- Safest:
    - JavaScript отключён везде.
    - Некоторые шрифты и символы отключены.
    - Воспроизведение любого медиа работает по нажатию, то есть по умолчанию отключено.

Для большинства случаев мы рекомендовали бы уровень Safer. Уровень Safest стоит включать, если вы считаете, что заходите на подозрительные или опасные сайты, и/или если вы особенно параноидальны.

Если вы особенно параноидальны, используйте Safest по умолчанию и подумайте о снижении до Safer, если сайт непригоден из-за блокировки JavaScript.

Однако уровень Safer следует использовать с дополнительными предосторожностями на некоторых сайтах: см. Дополнительные меры предосторожности в браузере при включённом JavaScript.

Теперь вы действительно закончили и можете анонимно просматривать веб с устройства Android.

Пожалуйста, см. Предупреждение об использовании Orbot на Android.

iOS

Отказ от ответственности: Onion Browser после выпуска на iOS в 2018 году имел утечки IP через WebRTC. Он всё ещё остаётся единственным официально одобренным браузером для сети Tor на iOS. Пользователям следует соблюдать осторожность при использовании браузера и проверять утечки DNS.

Хотя официального Tor Browser для iOS пока нет, есть альтернатива под названием Onion Browser, одобренная Tor Project[11].

- Перейдите на apps.apple.com
- Установите.
- Отключите Wi-Fi и мобильные данные.
- Запустите Onion Browser.
- После запуска нажмите значок настроек в правом верхнем углу. Предварительное отключение Wi-Fi и мобильных данных нужно было, чтобы Onion Browser не подключился автоматически и чтобы вы могли открыть эти параметры.
- Выберите «Bridge Configuration» и прочитайте Использование мостов Tor во враждебной среде.
- **Если нужно, после чтения приложения выше**, включите параметр и выберите тип моста:
    - Obfs4
    - Snowflake
    - Meek-Azure, к сожалению, недоступен в Onion Browser для iOS (см. commit 21bc18428 для подробностей).
- **Если ваш интернет не цензурируется**, подумайте о запуске одного из типов мостов, чтобы помочь сети.

• Легко: Obsf4 — собственный Obsf4 можно легко запустить по этим инструкциям: community.torproject.org

• Средне: Snowflake — подробнее о Snowflake здесь: snowflake.torproject.org

• Сложно: Meek — документация здесь. Это не так просто: gitlab.torproject.org

Лично я, если вам нужно использовать мост (это не нужно в невраждебной среде), выбрал бы Snowflake, поскольку мосты Meek-Azure недоступны. Они, вероятно, будут работать даже если вы в Китае и хотите обойти Great Firewall. Это, вероятно, лучший доступный вариант на iOS.

• Вы почти закончили.

Как и в настольной версии, нужно знать, что в Onion Browser есть уровни безопасности. На iOS к ним можно перейти так:

• Нажмите значок щита в левом верхнем углу.

• У вас будет три уровня на выбор.

Уровень безопасности	**JavaScript**	**WS/XHR/Geo**	**A/V**	**Apps**	**WebRTC**	**HTTP↔HTTPS**	**Реклама/всплывающие окна**
Gold	Отключён	Отключено	Нет	Заблокировано	Заблокировано	Заблокировано	Заблокировано
Silver	Частично разрешён	Отключено	Нет	Заблокировано	Заблокировано	Заблокировано	Заблокировано
Bronze	Разрешён	Включено	Разрешено	Заблокировано	Не заблокировано	Не заблокировано	Заблокировано

Для большинства случаев мы рекомендовали бы уровень Silver. Gold следует включать только если вы считаете, что заходите на подозрительные или опасные сайты, или если вы особенно параноидальны. Режим Gold также, скорее всего, сломает многие сайты, активно зависящие от JavaScript.

Поскольку в режиме Silver JavaScript включён, см. Дополнительные меры предосторожности в браузере при включённом JavaScript.

Теперь вы действительно закончили и можете анонимно просматривать веб с устройства iOS.

Важное предупреждение

Этот маршрут самый простой, но он не рассчитан на сопротивление высококвалифицированным противникам. При этом он пригоден на любом устройстве независимо от конфигурации. Этот маршрут также уязвим к корреляционным атакам (см. Ваш анонимизированный трафик Tor/VPN) и ничего не знает о том, что может находиться на вашем устройстве: это может быть любое вредоносное ПО, эксплойт, вирус, программа удалённого администрирования, родительский контроль... Тем не менее, если ваша модель угроз довольно низкая, этого, вероятно, достаточно для большинства людей.

Если у вас есть время и желание учиться, мы рекомендуем вместо этого выбрать другие маршруты: они дают гораздо лучшую безопасность, смягчают намного больше рисков и значительно уменьшают поверхность атаки.

Маршрут Tails

Эта часть руководства поможет вам настроить Tails, если верно одно из следующего:

• вы не можете позволить себе отдельный ноутбук;

• ваш отдельный ноутбук слишком старый и слишком медленный;

• у вас очень низкие ИТ-навыки;

• вы всё равно решили выбрать Tails.

Tails[12] означает **The Amnesic Incognito Live System**. Это загрузочная Live-операционная система, работающая с USB-накопителя; она создана для того, чтобы не оставлять следов и принудительно пропускать все соединения через сеть Tor.

Вы вставляете USB-накопитель Tails в ноутбук, загружаетесь с него и получаете полноценную операционную систему, созданную с учётом приватности и анонимности. Как только вы выключите компьютер, всё исчезнет, если вы специально не сохранили это где-либо.

Tails — удивительно простой способ быстро начать работу с тем, что у вас уже есть, и без долгого обучения. У него обширная документация и учебные материалы.

ПРЕДУПРЕЖДЕНИЕ: Tails не всегда актуален по встроенному ПО. И он не всегда актуален по обновлениям Tor Browser. Вы всегда должны убедиться, что используете последнюю версию Tails, и проявлять крайнюю осторожность при использовании встроенных приложений Tails, которые могут быть уязвимы к эксплойтам и раскрыть ваше местоположение[13].

Однако у него есть недостатки:

• Tails использует Tor, поэтому вы будете использовать Tor для доступа к любому ресурсу в интернете. Уже одно это сделает вас подозрительным для большинства платформ, где вы хотите создавать анонимные учётные записи; это будет подробнее объяснено позже.

• Ваш провайдер, будь то домашний провайдер или публичный Wi-Fi, тоже увидит, что вы используете Tor, и это само по себе может сделать вас подозрительным.

• Tails не включает изначально часть программ, которые вам могут понадобиться позже, что заметно усложнит ситуацию, если вы захотите запускать какие-то конкретные вещи, например эмуляторы Android.

• Tails использует Tor Browser; он очень безопасен, но большинство платформ его тоже обнаружит, и это помешает созданию анонимных идентичностей на многих платформах.

• Tails не защитит вас сильнее от гаечного ключа за 5 долларов[14].

• Самого Tor может быть недостаточно для защиты от противника с достаточными ресурсами, как объяснялось ранее.

Важное примечание: если ваш ноутбук контролируется/наблюдается и на нём есть локальные ограничения, пожалуйста, прочитайтеКак обойти некоторые локальные ограничения на контролируемых компьютерах.

Перед тем как идти дальше, также прочитайте документацию Tails, предупреждения и ограничения: tails.boum.org Archive.org

С учётом всего этого и того, что их документация отличная, мы просто направим вас к их хорошо сделанному и хорошо поддерживаемому руководству:

tails.boum.org Archive.org; выберите свой вариант и следуйте инструкциям.

Если у вас проблемы с доступом к Tor из-за цензуры или других причин, можно попробовать мосты Tor по этому руководству Tails: tails.boum.org Archive.org, а больше информации о них есть в документации Tor: 2019.www.torproject.org Archive.org

Если вы считаете, что одно только использование Tor опасно или подозрительно, см. Что делать, когда Tor и VPN невозможны?

Настройки Tor Browser в Tails

При использовании Tor Browser нужно нажать маленький значок щита в правом верхнем углу, рядом с адресной строкой, и выбрать уровень безопасности (подробности см. tb-manual.torproject.org Archive.org). В основном их три.

- Standard (по умолчанию):
    - Включены все функции, включая JavaScript.
- Safer:
    - JavaScript отключён на сайтах без HTTPS.
    - Некоторые шрифты и символы отключены.
    - Воспроизведение любого медиа работает по нажатию, то есть по умолчанию отключено.
- Safest:
    - JavaScript отключён везде.
    - Некоторые шрифты и символы отключены.
    - Воспроизведение любого медиа работает по нажатию, то есть по умолчанию отключено.

Для большинства случаев мы рекомендовали бы уровень Safer. Уровень Safest стоит включать, если вы считаете, что заходите на подозрительные или опасные сайты, либо если вы особенно параноидальны. Режим Safest также, скорее всего, сломает многие сайты, активно зависящие от JavaScript.

Если вы особенно параноидальны, используйте Safest по умолчанию и подумайте о снижении до Safer, если сайт непригоден из-за блокировки JavaScript.

Наконец, при использовании Tor Browser в Tails на уровне Safer рассмотрите дополнительные меры предосторожности в браузере при включённом JavaScript.

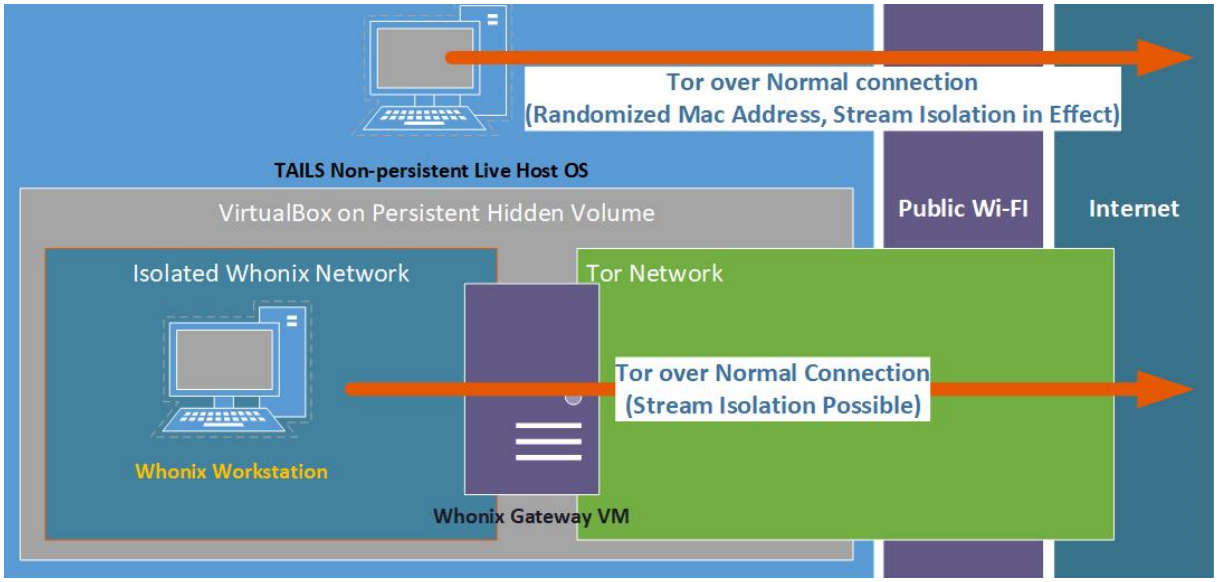
Когда вы закончите и получите рабочий Tails на ноутбуке, переходите к шагу Создание ваших анонимных онлайн-идентичностей гораздо дальше в руководстве; а если вам нужна постоянность и правдоподобное отрицание, продолжайте следующий раздел.

Постоянное правдоподобное отрицание с Whonix и Tails

Рассмотрите проект github.com Archive.org для Tails.

Этот проект — умная идея самодостаточного решения виртуальной машины в один клик, которое можно хранить на зашифрованном диске с использованием правдоподобного отрицания[3] (сначала см. первые разделы маршрута Whonix, а также объяснения правдоподобного отрицания и раздел Как безопасно удалять отдельные файлы/папки/данные на HDD/SSD и USB-накопителях в конце руководства для лучшего понимания).

Это позволит создать гибридную систему, объединяющую Tails с вариантами виртуализации из маршрута Whonix в этом руководстве.



Примечание: см.Выбор способа подключениив маршруте Whonix для дополнительных объяснений изоляции потоков

Кратко:

• Вы можете запускать непостоянный Tails с одного USB-накопителя, следуя их рекомендациям.

• Вы можете хранить постоянные виртуальные машины во втором контейнере, который можно зашифровать обычным способом или с использованием функции правдоподобного отрицания Veracrypt; это могут быть, например, виртуальные машины Whonix или любые другие.

• Вы получаете пользу от дополнительной функции изоляции потоков Tor (подробнее об изоляции потоков см. Tor поверх VPN).

В этом случае, как описывает проект, на вашем компьютере не должно оставаться следов вашей активности, а чувствительная работа может выполняться из виртуальных машин, хранящихся в скрытом контейнере, который мягкому противнику будет нелегко обнаружить.

Этот вариант особенно интересен для «лёгких поездок» и смягчения криминалистических атак при сохранении постоянства вашей работы. Вам нужны только 2 USB-накопителя: один с Tails и один с контейнером Veracrypt, содержащим постоянный Whonix. Первый USB-накопитель будет выглядеть так, будто содержит только Tails, а второй — как случайный мусор, но с внешним ложным томом, который можно показать для правдоподобного отрицания.

Вы также можете задаться вопросом, получится ли в итоге схема «Tor поверх Tor», но нет. Виртуальные машины Whonix будут обращаться к сети напрямую через обычный интернет, а не через луковую маршрутизацию Tails.

В будущем это может также поддерживаться самим проектом Whonix, как объясняется здесь: Whonix-Host Archive.org, но пока это не рекомендуется конечным пользователям.

Помните, что шифрование с правдоподобным отрицанием или без него — не универсальное средство и будет мало полезно в случае пыток. Более того, в зависимости от того, кто ваш противник, то есть от вашей модели угроз, может быть разумно вообще не использовать Veracrypt (ранее TrueCrypt), как показано в этой демонстрации: defuse.ca Archive.org

Правдоподобное отрицание эффективно только против мягких законных противников, которые не прибегают к физическим средствам.

См. en.wikipedia.org Wikiless Archive.org

ОСТОРОЖНО: пожалуйста, см. разделы Соображения по использованию внешних SSD-накопителей и Понимание HDD и SSD, если вы рассматриваете хранение таких скрытых виртуальных машин на внешнем SSD:

- **Не используйте скрытые тома на SSD-накопителях: Veracrypt не поддерживает и не рекомендует это[15].**
- **Вместо зашифрованных томов используйте файловые контейнеры.**
- **Убедитесь, что вы знаете, как правильно очищать данные с внешнего SSD-накопителя.**

Вот моё руководство, как этого добиться:

Первый запуск

- Скачайте последний выпуск HiddenVM с github.com Archive.org
- Скачайте последний выпуск Whonix XFCE с GitHub Releases Archive.org

Примечание: начиная с версии руководства v1.2.5 Whonix был обновлён с версии 17 до 18 (Whonix 18.1.4.x). См. Обновление до Whonix 18 для пути обновления, если сейчас вы используете Whonix 17.x.

- Подготовьте USB-накопитель/диск с Veracrypt:
  - Создайте скрытый том на USB-накопителе/диске; мы рекомендовали бы минимум 16 ГБ для скрытого тома.
  - Во внешний том поместите ложные файлы.
  - В скрытый том поместите файл appimage HiddenVM.
  - В скрытый том поместите файл OVA Whonix XFCE.
- Загрузитесь в Tails.
- Настройте раскладку клавиатуры как вам нужно.
- Выберите Additional Settings и задайте пароль администратора (root), он нужен для установки HiddenVM.
- Запустите Tails.
- Подключитесь к безопасному Wi-Fi; это обязательный шаг для дальнейшей работы.
- Перейдите в Utilities и разблокируйте свой скрытый том Veracrypt; не забудьте отметить флажок hidden volume.
- Запустите appimage HiddenVM.
- Когда будет предложено выбрать папку, выберите корень скрытого тома, где находятся файлы Whonix OVA и HiddenVM appimage.

• Дайте ему сделать своё дело; это установит Virtualbox внутри Tails одним нажатием.

• Когда всё будет готово, Virtualbox Manager должен запуститься автоматически.

• Импортируйте файлы Whonix OVA (см. Виртуальные машины Whonix).

Примечание: если во время импорта возникают проблемы вроде «NS_ERROR_INVALID_ARG (0x80070057)», вероятно, на скрытом томе недостаточно места для Whonix. Сами Whonix рекомендуют 32 ГБ свободного места, но это, вероятно, не обязательно, и 10 ГБ должно хватить для начала. Можно попробовать обойти ошибку, переименовав файл Whonix *.OVA в *.TAR и распаковав его внутри Tails. Когда распаковка закончится, удалите файл OVA и импортируйте остальные файлы через мастер импорта. На этот раз может сработать.

Последующие запуски

• Загрузитесь в Tails.

• Подключитесь к Wi-Fi.

• Разблокируйте скрытый том.

• Запустите приложение HiddenVM.

• Это должно автоматически открыть VirtualBox Manager и показать ваши прежние виртуальные машины с первого запуска.

Шаги для всех остальных маршрутов

Получить отдельный ноутбук

В идеале стоит получить отдельный ноутбук, который нельзя будет легко связать с вами: желательно оплатить его наличными анонимно и с теми же предосторожностями, что ранее упоминались для телефона и SIM-карты. Это рекомендуется, но не обязательно. Это руководство поможет максимально усилить защиту ноутбука, чтобы предотвратить утечки данных разными способами. Между вашими онлайн-идентичностями и вами будет несколько линий обороны, которые должны помешать большинству противников деанонимизировать вас, кроме государственных или глобальных участников. На это потребуются значительные ресурсы.

В идеале этот ноутбук должен быть чистым, только что установленным ноутбуком с Windows, Linux или macOS, без ваших обычных повседневных действий и офлайн, то есть никогда не подключавшимся к домашней сети. В случае ноутбука с Windows, если вы использовали его до такой чистой установки, он также не должен быть активирован. Если он поставлялся предактивированным, просто переустановите без ключа продукта. В случае MacBook особенно важно, чтобы он никогда прежде никак не был связан с вашей личностью. Поэтому покупайте б/у за наличные у неизвестного незнакомца, который не знает вашу личность.

Это нужно, чтобы смягчить будущие проблемы в случае онлайн-утечек, включая телеметрию вашей ОС или приложений, которые могут раскрыть уникальные идентификаторы ноутбука во время использования: MAC-адрес, адрес Bluetooth, ключ продукта... А также чтобы избежать отслеживания обратно к вам, если понадобится избавиться от ноутбука.

Если вы раньше использовали этот ноутбук для других целей, например повседневных дел, все его аппаратные идентификаторы, вероятно, уже известны и зарегистрированы Microsoft или Apple. Если позже любой из этих идентификаторов будет раскрыт, например вредоносным ПО, телеметрией, эксплойтами или человеческими ошибками, они могут привести обратно к вам.

У ноутбука должно быть как минимум 250 ГБ дискового пространства, **не меньше 6 ГБ, а в идеале 8 или 16 ГБ RAM**, и он должен быть способен одновременно запускать пару виртуальных машин. У него должна быть рабочая батарея на несколько часов. По возможности стоит стремиться к большому хранилищу, 1 ТБ и больше, потому что нам понадобится как можно больше места.

В ноутбуке может быть HDD (7200 rpm) или SSD/NVMe-накопитель. У обоих вариантов есть свои преимущества и проблемы, которые будут подробно разобраны позже.

Все будущие онлайн-шаги, выполняемые с этого ноутбука, в идеале должны выполняться из безопасной сети, например публичного Wi-Fi в безопасном месте (см. Найти безопасные места с нормальным публичным Wi-Fi). Но сначала несколько шагов нужно будет выполнить офлайн.

Некоторые рекомендации по ноутбукам

Мы настоятельно рекомендовали бы взять ноутбук «бизнес-класса», то есть не потребительский и не игровой, если можете. Например, какой-нибудь ThinkPad от Lenovo; это мой личный фаворит.

Причина в том, что такие бизнес-ноутбуки обычно предлагают лучшие и более настраиваемые функции безопасности, особенно в настройках BIOS/UEFI, и более долгую поддержку, чем большинство потребительских ноутбуков (Asus, MSI, Gigabyte, Acer...). Интересные функции, на которые стоит смотреть:

- Лучшие пользовательские настройки Secure Boot **(где можно выборочно управлять всеми ключами, а не просто использовать стандартные)**.
- Пароли HDD/SSD в дополнение к паролям BIOS/UEFI.
- Ноутбуки AMD могут быть интереснее, потому что некоторые позволяют отключить AMD PSP (аналог Intel IME у AMD) прямо в настройках BIOS/UEFI по умолчанию. И, насколько мне известно, AMD PSP проходил аудит и, в отличие от IME, в нём не нашли «злых» функций[16]. Однако если вы выбираете маршрут Qubes OS, рассмотрите процессоры Intel, потому что Qubes OS не поддерживает AMD в своей системе anti-evil-maid[17].
- Инструменты безопасной очистки из BIOS, особенно полезные для SSD/NVMe-накопителей; см. варианты BIOS/UEFI для очистки дисков у разных брендов.
- Лучший контроль отключения/включения отдельных периферийных устройств: USB-порты, Wi-Fi, Bluetooth, камера, микрофон...
- Лучшие функции безопасности для виртуализации.
- Встроенные защиты от физического вмешательства.
- Более долгая поддержка обновлениями BIOS/UEFI и последующими обновлениями безопасности BIOS/UEFI.
- Некоторые поддерживаются Libreboot.

Настройки BIOS/UEFI/прошивки ноутбука

PC

Доступ к этим настройкам можно получить через загрузочное меню ноутбука. Вот хорошее руководство от HP, объясняющее разные способы входа в BIOS на разных компьютерах: store.hp.com Archive.org

Обычно для входа нужно нажать конкретную клавишу, например F1, F2 или Del, при загрузке, до запуска ОС.

Оказавшись там, нужно применить несколько рекомендуемых настроек:

• Полностью отключите Bluetooth, если можете.

• Отключите биометрию, например сканеры отпечатка пальца, если она есть и если можете. Однако можно добавить дополнительную биометрическую проверку только для загрузки, до запуска ОС, но не для доступа к настройкам BIOS/UEFI.

• Отключите веб-камеру и микрофон, если можете.

• Включите пароль BIOS/UEFI и используйте длинную парольную фразу вместо короткого пароля, если можете. Убедитесь, что этот пароль требуется для:

  • доступа к самим настройкам BIOS/UEFI;

  • изменения порядка загрузки;

  • запуска/включения устройства.

• Включите пароль HDD/SSD, если функция доступна. Эта функция добавит ещё один пароль на сам HDD/SSD, а не в прошивку BIOS/UEFI, и не позволит использовать этот HDD/SSD в другом компьютере без пароля. Обратите внимание, что эта функция тоже специфична для некоторых производителей и может требовать специального ПО, чтобы разблокировать диск на совершенно другом компьютере.

• Запретите доступ к параметрам загрузки, то есть к порядку загрузки, без ввода пароля BIOS/UEFI, если можете.

• Отключите USB/HDMI или любые другие порты (Ethernet, Firewire, SD-карта...), если можете.

• Отключите Intel ME, если можете; вероятность очень высока, что не сможете.

• Отключите AMD PSP, если можете; это аналог IME у AMD, см. Ваш процессор.

• Отключите Secure Boot, если собираетесь использовать Qubes OS, потому что он не поддерживается из коробки[18]. Оставьте его включённым, если собираетесь использовать Linux/Windows.

• Проверьте, есть ли в BIOS ноутбука вариант безопасного стирания HDD/SSD, который может быть удобен при необходимости.

Включайте такие функции только по необходимости и снова отключайте после использования. Это может смягчить некоторые атаки, если ноутбук изъят в заблокированном, но всё ещё включённом состоянии, или если вам пришлось довольно быстро выключить его, а кто-то получил к нему доступ. Эта тема будет объяснена позже в руководстве.

О Secure Boot

Что такое Secure Boot[19]? Кратко: это функция безопасности UEFI, созданная для предотвращения загрузки компьютера с операционной системы, загрузчик которой не подписан конкретными ключами, сохранёнными в прошивке UEFI вашего ноутбука.

Когда операционная система или загрузчик[20] это поддерживает, можно сохранить ключи вашего загрузчика в прошивке UEFI, и это предотвратит запуск любой неразрешённой операционной системы, например Live OS с USB или чего-то похожего.

Настройки Secure Boot защищены паролем, который вы задали для доступа к BIOS/UEFI. Если у вас есть этот пароль, можно отключить Secure Boot и разрешить неподписанным ОС загружаться на вашей системе. Это может смягчить некоторые атаки Evil Maid, которые будут объяснены позже.

В большинстве случаев Secure Boot по умолчанию отключён или включён в режиме setup, который позволяет загружать любую систему. Чтобы Secure Boot работал, операционная система должна его поддерживать, подписать свой загрузчик и отправить эти ключи подписи в прошивку UEFI. После этого нужно зайти в настройки BIOS/UEFI, сохранить эти ключи, отправленные вашей ОС, и перевести Secure Boot из режима setup в пользовательский режим, либо в custom mode в некоторых случаях.

После этого смогут загружаться только те операционные системы, целостность загрузчика которых прошивка UEFI может проверить.

У большинства ноутбуков в настройках Secure Boot уже хранятся некоторые ключи по умолчанию. Обычно это ключи производителя или компаний вроде Microsoft. Это означает, что по умолчанию даже с Secure Boot часто можно загрузить некоторые USB-диски. В их число входят Windows, Fedora, Ubuntu, Mint, Debian, CentOS, OpenSUSE, Tails, Clonezilla и многие другие. Qubes OS на данный момент Secure Boot вообще не поддерживает.

На некоторых ноутбуках можно управлять этими ключами и удалять ненужные через custom mode, чтобы разрешить только ваш загрузчик, который вы при желании можете подписать сами.

От чего защищает Secure Boot? Он защищает ноутбук от загрузки неподписанных загрузчиков, например загрузчиков с внедрённым вредоносным ПО, если они не подписаны поставщиком ОС.

От чего Secure Boot **не** защищает?

- Secure Boot не шифрует диск, и противник всё равно может просто вынуть диск из ноутбука и извлечь данные на другой машине. Поэтому Secure Boot бесполезен без полного шифрования диска.
- Secure Boot не защищает от подписанного загрузчика, который был скомпрометирован и подписан самим производителем, например Microsoft в случае Windows. Большинство массовых дистрибутивов Linux сегодня подписаны и загружаются с включённым Secure Boot.
- Secure Boot может иметь ошибки и эксплойты, как любая другая система. Если вы используете старый ноутбук, который больше не получает обновления BIOS/UEFI, такие проблемы могут остаться неисправленными.

Кроме того, против Secure Boot возможны разные атаки, подробно объяснённые в этих технических видео:

- Defcon 22, youtube.com Invidious
- BlackHat 2016, youtube.com Invidious

Так что он может быть полезен как дополнительная мера против некоторых противников, но не против всех. Сам по себе Secure Boot не шифрует жёсткий диск. Это дополнительный слой, и только.

Я всё же рекомендую держать его включённым, если можете.

Mac

Уделите минуту настройке пароля прошивки по руководству здесь: support.apple.com Archive.org

Также стоит включить защиту от сброса пароля прошивки (доступна с Catalina) по документации здесь: support.apple.com Archive.org

Эта функция смягчит возможность для некоторых противников использовать аппаратные взломы для отключения или обхода пароля прошивки. Обратите внимание, что это также помешает самой Apple получить доступ к прошивке в случае ремонта.

Физическая защита ноутбука от вмешательства

В какой-то момент вы неизбежно оставите этот ноутбук где-то один. Вы не будете спать с ним и носить его с собой каждый день. Нужно сделать так, чтобы кому-либо было как можно труднее вмешаться в него незаметно для вас. Это в основном полезно против ограниченных противников, которые не применят к вам гаечный ключ за 5 долларов[14].

Важно знать, что для некоторых специалистов тривиально просто установить кейлоггер в ноутбук или просто сделать клон жёсткого диска, который позже позволит им обнаружить наличие зашифрованных данных криминалистическими методами. Подробнее об этом позже.

Вот хороший дешёвый метод защитить ноутбук от вмешательства с помощью лака для ногтей с блёстками: mullvad.net Archive.org [21] (с фотографиями).

Хотя это хороший дешёвый метод, он также может вызвать подозрения, потому что довольно заметен и может просто показать, что вам «есть что скрывать». Поэтому существуют более тонкие способы добиться того же результата. Например, можно сделать макрофотографию крупным планом задних винтов ноутбука или нанести небольшое количество свечного воска внутрь одного из винтов, чтобы это выглядело как обычная грязь. Затем можно проверять вмешательство, сравнивая новые фотографии винтов со старыми. Их положение могло немного измениться, если противник был недостаточно аккуратен и не затянул их точно так же, как раньше. Или воск внутри головки винта мог быть повреждён по сравнению с прежним состоянием.

Те же техники можно использовать с USB-портами: можно поместить крошечное количество свечного воска внутрь разъёма, и оно будет повреждено при вставке USB-накопителя.

В более рискованных средах регулярно проверяйте ноутбук на вмешательство перед использованием.

Маршрут Whonix

Примечание о версии Whonix: Whonix был обновлён с версии 17 до 18 (Whonix 18.1.4.x на момент написания) с поддержкой автоматического обновления релизов. См. Обновление до Whonix 18 для пути обновления, если сейчас вы используете Whonix 17.x или более ранние версии.

Выбор основной ОС

Этот маршрут будет активно использовать виртуальные машины[22]; им понадобится основная ОС, на которой будет запускаться программа виртуализации. В этой части руководства есть три рекомендуемых варианта:

• выбранный вами дистрибутив Linux, кроме Qubes OS;

• Windows 10/11, желательно редакция Home из-за отсутствия Bitlocker;

• macOS, Catalina или выше до Monterey.

Кроме того, велика вероятность, что ваш Mac связан или был связан с Apple Account во время покупки или после входа, и поэтому его уникальные аппаратные идентификаторы могут привести обратно к вам в случае утечки аппаратных идентификаторов.

Linux также не обязательно лучший выбор для анонимности, в зависимости от вашей модели угроз. Причина в том, что Windows позволит нам **удобно** использовать правдоподобное отрицание[3] (оно же отрицаемое шифрование[23]) на уровне ОС. Windows, к сожалению, одновременно является кошмаром для приватности[24], но это единственный простой в настройке вариант для использования правдоподобного отрицания на уровне всей ОС. Телеметрия Windows и блокировка телеметрии также широко документированы, что должно смягчить многие проблемы.

Что такое правдоподобное отрицание? Вы можете сотрудничать с противником, который требует доступ к вашему устройству или данным, не раскрывая настоящий секрет. Всё это с использованием отрицаемого шифрования[6].

Мягкий законный противник может попросить пароль от зашифрованного ноутбука. Сначала можно отказаться сообщать пароль, используя «право хранить молчание» или «право не свидетельствовать против себя», но некоторые страны вводят законы[25][26], исключающие такие случаи из этих прав, потому что террористы и «подумайте о детях». В таком случае вам, возможно, придётся раскрыть пароль или столкнуться с тюремным сроком за неуважение к суду. Вот здесь и вступает в игру правдоподобное отрицание.

Вы можете раскрыть пароль, но этот пароль даст доступ только к «правдоподобным данным», то есть ложной ОС. Криминалисты будут хорошо понимать, что у вас могут быть скрытые данные, но не должны быть способны это доказать **(если вы всё сделали правильно)**. Вы сотрудничали, следователи получили доступ к чему-то, но не к тому, что вы действительно хотите скрыть. Поскольку бремя доказательства должно лежать на их стороне, у них не останется вариантов, кроме как поверить вам, если у них нет доказательства наличия скрытых данных.

Эта функция может использоваться на уровне ОС, где есть правдоподобная ОС и скрытая ОС, или на уровне файлов, где у вас есть зашифрованный файловый контейнер, похожий на zip-файл, в котором разные файлы будут показаны в зависимости от используемого пароля шифрования.

Это также означает, что вы можете настроить собственную продвинутую схему правдоподобного отрицания с любой основной ОС, например храня виртуальные машины в скрытом томе-контейнере Veracrypt. Будьте осторожны со следами в основной ОС: их придётся очищать, если основная ОС постоянная; см. раздел Дополнительные меры против криминалистики позже. Есть проект для реализации этого внутри Tails (github.com Archive.org), который сделает основную ОС непостоянной и позволит использовать правдоподобное отрицание внутри Tails.

В случае Windows правдоподобное отрицание также является причиной, по которой в идеале стоит иметь Windows 10/11 Home, а не Pro. Дело в том, что Windows 10/11 Pro изначально предлагает систему полного шифрования диска Bitlocker[27], а Windows 10/11 Home вообще не предлагает полного шифрования диска. Позже вы будете использовать стороннее открытое ПО для шифрования, которое позволит полное шифрование диска в Windows 10/11 Home. Это даст вам

хорошее правдоподобное объяснение, почему вы используете это ПО. А вот использование такого ПО на Windows 10/11 Pro выглядело бы подозрительно.

Примечание о Linux: что насчёт Linux и правдоподобного отрицания? Да, в Linux тоже можно добиться правдоподобного отрицания. Подробнее будет в разделе основной ОС Linux ниже.

К сожалению, шифрование не магия, и с ним связаны некоторые риски:

Угрозы при шифровании

Атака гаечным ключом за 5 долларов

Помните: шифрование с правдоподобным отрицанием или без него — не универсальное средство и будет мало полезно в случае пыток. Более того, в зависимости от того, кто ваш противник (ваша модель угроз), может быть разумно вообще не использовать Veracrypt (ранее TrueCrypt), как показано в этой демонстрации: defuse.ca Archive.org

Правдоподобное отрицание эффективно только против мягких законных противников, которые не прибегают к физическим средствам. **По возможности избегайте использования ПО с поддержкой правдоподобного отрицания, например Veracrypt, если ваша модель угроз включает жёстких противников. Пользователям Windows в таком случае следует установить Windows Pro как основную ОС и использовать вместо этого Bitlocker.**

См. en.wikipedia.org Wikiless Archive.org

Атака Evil Maid

Атаки Evil Maid[28] выполняются, когда кто-то вмешивается в ваш ноутбук, пока вас нет: устанавливает или клонирует жёсткий диск, ставит вредоносное ПО или кейлоггер. Если противник может клонировать диск, он сможет сравнить образ диска, сделанный в ваше отсутствие, с диском в момент изъятия. Если между этими моментами вы снова использовали ноутбук, криминалисты могут доказать наличие скрытых данных, посмотрев на изменения между двумя образами там, где должно быть пустое или неиспользуемое пространство. Это может стать убедительным доказательством наличия скрытых данных. Если они установят кейлоггер или вредоносное ПО в ноутбук, программно или аппаратно, они смогут просто получить ваш пароль для дальнейшего использования при изъятии. Такие атаки могут выполняться дома, в отеле, на границе или в любом месте, где вы оставляете устройства без присмотра.

Эту атаку можно смягчить следующими действиями, рекомендованными ранее:

- Иметь базовую защиту от вмешательства, как объяснялось выше, чтобы предотвратить физический доступ к внутренностям ноутбука без вашего ведома. Это помешает клонировать диски и установить физический кейлоггер незаметно для вас.
- Отключить все USB-порты, как объяснялось выше, в защищённом паролем BIOS/UEFI. Тогда противник не сможет включить их без физического доступа к материнской плате для сброса BIOS, чтобы загрузить USB-устройство, клонирующее диск, или установить программное вредоносное ПО, работающее как кейлоггер.
- Настроить пароли BIOS/UEFI/прошивки, чтобы предотвратить неразрешённую загрузку с неразрешённого устройства.

• В некоторых ОС и программах шифрования есть защита Anti Evil Maid (AEM), которую можно включить. Это относится к Windows/Veracrypt и Qubes OS, только на процессорах Intel.

Атака Cold Boot

Атаки Cold Boot[29] сложнее, чем Evil Maid, но могут быть частью атаки Evil Maid, потому что требуют, чтобы противник получил ваш ноутбук, пока вы активно используете устройство или вскоре после этого.

Идея довольно проста: как показано в этом видео[30], противник теоретически может быстро загрузить устройство со специального USB-накопителя, который скопирует содержимое RAM, то есть памяти устройства, после выключения. Если USB-порты отключены или если противнику нужно больше времени, он может открыть устройство и «охладить» память спреем или другими химическими веществами, например жидким азотом, чтобы замедлить исчезновение данных из памяти. Затем он сможет скопировать её содержимое для анализа. Такой дамп памяти может содержать ключ для расшифровки устройства. Позже вы примените несколько принципов для смягчения этого.

В случае правдоподобного отрицания были криминалистические исследования[31] о техническом доказательстве наличия скрытых данных простым криминалистическим исследованием, без атаки Cold Boot/Evil Maid, но эти выводы оспаривались другими исследованиями[32] и сопровождающим Veracrypt[33], поэтому пока мы бы не слишком беспокоились об этом.

Для смягчения Cold Boot должны применяться те же меры, что и для Evil Maid, с некоторыми дополнениями:

• Если ваша ОС или программа шифрования позволяет, стоит рассмотреть шифрование ключей внутри RAM. Это возможно с Windows/Veracrypt и будет объяснено позже. См. также sourceforge.net Archive.org

• Включите в Veracrypt опцию очистки ключей из памяти при вставке устройства.

• Нужно ограничить использование режима сна и вместо этого применять выключение или гибернацию, чтобы ключи шифрования не оставались в RAM, когда компьютер уходит в сон. Сон поддерживает питание памяти для более быстрого возобновления работы. Только гибернация и выключение действительно очищают ключ из памяти[34].

См. также Cold Boot Attack Defense Archive.org и Protection Against Physical Attacks Archive.org.

Вот также несколько интересных инструментов для пользователей Linux, которые можно рассмотреть для защиты:

• github.com Archive.org (к сожалению, похоже, не поддерживается)

• github.com Archive.org (тоже, похоже, не поддерживается)

• github.com Archive.org

• askubuntu.com Archive.org

• (Qubes OS, только процессоры Intel) github.com Archive.org

О сне, гибернации и выключении

Если вам нужна лучшая безопасность, полностью выключайте ноутбук каждый раз, когда оставляете его без присмотра или закрываете крышку. Это должно очистить и/или освободить RAM и смягчить атаки Cold Boot. Однако это может быть немного неудобно: придётся полностью перезагружаться и вводить множество паролей в разные приложения, заново запускать виртуальные машины и другие программы. Поэтому вместо этого можно использовать гибернацию (не поддерживается в Qubes OS). Поскольку весь диск зашифрован, сама гибернация не должна создавать большой риск безопасности, но она всё равно выключит ноутбук и очистит память, позволяя затем удобно продолжить работу. **Чего никогда не следует делать, так это использовать обычный сон, который оставляет компьютер включённым, а память под питанием. Это вектор атаки для Evil Maid и Cold Boot, обсуждённых выше. Причина в том, что память под питанием содержит ключи шифрования вашего диска, зашифрованного или нет, и к ним может получить доступ умелый противник.**

Позже руководство объяснит, как включить гибернацию на разных основных ОС, кроме Qubes OS, если вы не хотите каждый раз выключаться.

Локальные утечки данных (следы) и криминалистическое исследование

Как кратко упоминалось ранее, это утечки данных и следы из вашей операционной системы и приложений, возникающие при любой активности на компьютере. Они в большей степени относятся к зашифрованным файловым контейнерам, с правдоподобным отрицанием или без него, чем к шифрованию всей ОС. Такие утечки менее «важны», если вся ОС зашифрована, при условии что вас не принуждают раскрыть пароль.

Допустим, например, у вас есть зашифрованный USB-накопитель Veracrypt с включённым правдоподобным отрицанием. В зависимости от пароля, который вы используете при подключении USB-накопителя, откроется ложная папка или чувствительная папка. В этих папках будут ложные документы/данные в ложной папке и чувствительные документы/данные в чувствительной папке.

В любом случае вы, скорее всего, откроете эти папки через Windows Explorer, macOS Finder или другую утилиту и сделаете то, что планировали. Возможно, вы отредактируете документ в чувствительной папке. Возможно, будете искать документ в папке. Возможно, удалите один файл или посмотрите чувствительное видео через VLC.

Что ж, все эти приложения и ваша операционная система могут хранить журналы и следы такого использования. Это может включать полный путь к папкам/файлам/дискам, время доступа, временные кэши этих файлов, списки «недавнего» в каждом приложении, систему индексации файлов, которая может проиндексировать диск, и даже миниатюры, которые могут быть созданы.

Вот несколько примеров таких утечек:

Windows

• Windows ShellBags, которые хранятся в реестре Windows и тихо сохраняют разные истории доступа к томам/файлам/папкам[35].

• Индексация Windows по умолчанию хранит следы файлов, присутствующих в вашей пользовательской папке[36].

• Списки недавних файлов, также известные как Jump Lists, в Windows и разных приложениях хранят следы недавно открытых документов[37].

• Множество других следов в разных журналах; для более подробного понимания см. этот удобный интересный постер: sans.org Archive.org

macOS

• Gatekeeper[38] и XProtect отслеживают историю загрузок в локальной базе данных и атрибутах файлов.

• Индексация Spotlight.

• Списки недавних файлов в разных приложениях хранят следы недавно открытых документов.

• Временные папки хранят разные следы использования приложений и документов.

• Журналы macOS.

Linux

• Индексация Tracker.

• История Bash.

• Журналы USB.

• Списки недавних файлов в разных приложениях хранят следы недавно открытых документов.

• Журналы Linux.

Криминалисты могут использовать все эти утечки (см. Локальные утечки данных и криминалистика), чтобы доказать наличие скрытых данных, сорвать попытки использовать правдоподобное отрицание и узнать о разных чувствительных действиях.

Поэтому важно применять разные шаги, чтобы помешать криминалистике сделать это: предотвращать и очищать такие утечки/следы, а главное — использовать полное шифрование диска, виртуализацию и изоляцию.

Криминалисты не могут извлечь локальные утечки данных из ОС, к которой не имеют доступа. А вы сможете очистить большинство таких следов, стерев диск или безопасно удалив виртуальные машины; на SSD это не так просто, как кажется.

Некоторые техники очистки всё же будут описаны в части «Заметаем следы» в самом конце руководства.

Онлайн-утечки данных

Используете ли вы простое шифрование или шифрование с правдоподобным отрицанием, даже если вы замели следы на самом компьютере, всё ещё остаётся риск онлайн-утечек данных, которые могут раскрыть наличие скрытых данных.

Телеметрия — ваш враг. Как объяснялось ранее, телеметрия операционных систем, а также приложений, может отправлять в интернет ошеломляющий объём личной информации.

В случае Windows эти данные, например, могут быть использованы для доказательства наличия скрытой ОС/тома на компьютере, и они будут легко доступны Microsoft. Поэтому критически важно отключить и заблокировать телеметрию всеми доступными средствами. Неважно, какую ОС вы используете.

Заключение

Никогда не выполняйте чувствительные действия с незашифрованной системы. И даже если она зашифрована, никогда не выполняйте чувствительные действия прямо из основной ОС. Вместо этого используйте виртуальную машину, чтобы эффективно изолировать и разделять активность и предотвращать локальные утечки данных.

Если у вас почти нет знаний Linux или если вы хотите использовать правдоподобное отрицание на уровне всей ОС, мы рекомендуем ради удобства выбрать Windows или вернуться к маршруту Tails. Это руководство поможет максимально усилить Windows, чтобы предотвратить утечки. Оно также поможет максимально усилить macOS и Linux, чтобы предотвратить похожие утечки.

Если вам неинтересно правдоподобное отрицание на уровне всей ОС и вы хотите научиться пользоваться Linux, мы настоятельно рекомендуем выбрать Linux или маршрут Qubes OS, если оборудование позволяет.

В любом случае основная ОС никогда не должна использоваться для прямого выполнения чувствительных действий. Основная ОС будет использоваться только для подключения к публичной точке доступа Wi-Fi. Она останется неиспользуемой, пока вы выполняете чувствительные действия, и в идеале не должна использоваться для каких-либо повседневных задач.

Также рассмотрите чтение **whonix.org** Archive.org

Основная ОС Linux

Как упоминалось ранее, мы не рекомендуем использовать повседневный ноутбук для чувствительных действий. Или, по крайней мере, не рекомендуем использовать для них уже установленную на нём ОС. Это может привести к нежелательным утечкам данных, которые можно использовать для вашей деанонимизации. Если у вас есть отдельный ноутбук для этого, следует переустановить на нём свежую чистую ОС. Если вы не хотите стирать ноутбук и начинать заново, рассмотрите маршрут Tails или продолжайте на свой риск.

Я также рекомендую выполнять начальную установку полностью офлайн, чтобы избежать утечки данных.

Всегда помните: несмотря на репутацию, массовые дистрибутивы Linux, например Ubuntu, не обязательно лучше по безопасности, чем другие системы вроде macOS и Windows. См. этот материал, чтобы понять почему: madaidans-insecurities.github.io Archive.org.

Полное шифрование диска

Для дистрибутивов на основе Ubuntu или Debian здесь есть два пути:

- Использование LUKS:
  - Без правдоподобного отрицания:
    - Рекомендуемый и простой вариант: зашифровать во время установки: ubuntu.com Archive.org
      - Этот процесс требует полного стирания всего диска, то есть чистой установки.
      - Просто отметьте «Encrypt the new Ubuntu installation for security».
    - Утомительный, но возможный вариант: зашифровать после установки: help.ubuntu.com Archive.org
  - С правдоподобным отрицанием: см. следующий раздел Способ с отделёнными заголовками.
- Использование Veracrypt:
  - С правдоподобным отрицанием или без него: см. следующий раздел Способ Veracrypt.

Для других дистрибутивов придётся самостоятельно изучать документацию, но, скорее всего, всё будет похоже. В контексте этого руководства шифрование во время установки намного проще.

Примечание о правдоподобном отрицании в Linux

Есть несколько способов добиться правдоподобного отрицания в Linux[39], и это возможно. Вот немного больше деталей о некоторых вариантах, которые мы бы рекомендовали. Все эти варианты требуют более высокого уровня навыков работы с Linux.

Способ с отделёнными заголовками

Пока это не поддерживается этим руководством, но в Linux можно добиться формы отрицания с помощью LUKS, используя отделённые заголовки LUKS. Пока мы направим вас на эту страницу для дополнительной информации: wiki.archlinux.org Archive.org

Способ Veracrypt

Технически возможно не только использовать Veracrypt, но и добиться правдоподобного отрицания на основной ОС Linux, применяя Veracrypt для системного полного шифрования диска вместо LUKS. Veracrypt это не поддерживает (системное шифрование поддерживается только в Windows), и для этого нужно возиться с разными командами. Это совершенно не рекомендуется неопытным пользователям и должно использоваться только на ваш риск.

Шаги для этого пока не встроены в руководство, но их можно найти здесь: dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion (это .onion-адрес, нужен Tor Browser).

Отказаться от телеметрии и отключить её

- Во время установки просто убедитесь, что не разрешили сбор данных, если вас об этом спросят.
- Если вы не уверены, убедитесь, что не включили телеметрию, и при необходимости следуйте этому руководству: vitux.com Archive.org
- Любой другой дистрибутив: нужно самостоятельно изучить, как отключить телеметрию.

Отключить всё ненужное

- Отключите Bluetooth, если он включён, по этому руководству: addictivetips.com Archive.org или выполнив команду:
  - `sudo systemctl disable bluetooth.service --force`
- Отключите индексацию, если она включена по умолчанию (Ubuntu >19.04), следуя этому руководству: linuxuprising.com Archive.org или выполнив команды:
  - `sudo systemctl --user mask tracker-store.service tracker-miner-fs.service tracker-miner-rss.service tracker-extract.service tracker-miner-apps.service tracker-writeback.service`
    - Можно спокойно игнорировать ошибки о том, что какой-то службы не существует.
  - `sudo tracker reset -hard`

Гибернация

Как объяснялось ранее, не следует использовать функции сна; лучше выключать или переводить ноутбук в гибернацию, чтобы смягчить некоторые атаки Evil Maid и Cold Boot. К сожалению, эта функция отключена по умолчанию во многих дистрибутивах Linux, включая Ubuntu. Её можно включить, но она может работать не так, как ожидается. Следуйте этой информации на свой риск. Если вы не хотите этого делать, никогда не используйте функцию сна и вместо этого выключайте питание, а поведение закрытия крышки установите на выключение вместо сна.

Следуйте одному из этих руководств, чтобы включить гибернацию:

- how2shout.com Archive.org

• lorenzobettini.it Archive.org

• blog.ivansmirnov.name Archive.org

После включения гибернации измените поведение так, чтобы ноутбук переходил в гибернацию при закрытии крышки, следуя этому руководству для Ubuntu 20.04: ubuntuhandbook.org Archive.org и этому руководству для Ubuntu 18.04: tipsonubuntu.com Archive.org. Для Ubuntu 21.04 или 21.10 руководства пока нет, но вариант для 20.04, вероятно, тоже должен работать.

К сожалению, при гибернации это не очистит ключ из памяти напрямую. Чтобы избежать этого ценой некоторой производительности, можно рассмотреть шифрование swap-файла по этому руководству: help.ubuntu.com Archive.org

Эти настройки должны смягчить атаки Cold Boot, если вы сможете перейти в гибернацию достаточно быстро.

Включить рандомизацию MAC-адреса

• Для Ubuntu следуйте этим шагам: help.ubuntu.com Archive.org.

• Рассмотрите это руководство, которое всё ещё должно работать: josh.works Archive.org

Усиление Linux

Для лёгкого введения новым пользователям Linux рассмотрите youtube.com Invidious

Для более глубоких и продвинутых вариантов обратитесь к:

• этому отличному руководству: madaidans-insecurities.github.io Archive.org

• этому отличному wiki-ресурсу: wiki.archlinux.org Archive.org

• этим отличным скриптам на основе руководства и wiki выше: codeberg.org Archive.org

• этим инструментам, которые помогут усилить ядро Linux:

  • Lynis: github.com

  • Kconfig-hardened-check: github.com

• Рассмотрите установку Safing Portmaster с safing.io Archive.org **(Предупреждение: с некоторыми VPN-клиентами могут быть проблемы. См.: docs.safing.io** Archive.org

• Рассмотрите использование KickSecure при использовании Debian: Kicksecure Archive.org

• Эта интересная статья: 0pointer.net Archive.org

Настройка безопасного браузера

См. Безопасный браузер в основной ОС

Основная ОС macOS

Примечание: чипы Mac M1/M2 теперь поддерживаются нативно; либо можно использовать коммерческие инструменты вроде VMWare Fusion или Parallels Desktop, но они не рассматриваются в этом руководстве. Изучите эту информацию самостоятельно.

Как упоминалось ранее, мы не рекомендуем использовать повседневный ноутбук для чувствительных действий. Или, по крайней мере, не рекомендуем использовать для них уже установленную на нём ОС. Это может привести к нежелательным утечкам данных, которые можно использовать для деанонимизации. Если у вас есть отдельный ноутбук для этого, следует переустановить на нём свежую чистую ОС. Если вы не хотите стирать ноутбук и начинать заново, рассмотрите маршрут Tails или продолжайте на свой риск.

Мы также рекомендуем выполнять начальную установку полностью офлайн, чтобы избежать утечки данных.

Никогда не входите в Apple Account с этого Mac.

Во время установки

• Оставайтесь офлайн.

• Отключите все запросы на передачу данных, когда они появятся, включая службы определения местоположения.

• Не входите в Apple.

• Не включайте Siri.

Усиление macOS

Для лёгкого введения новым пользователям macOS рассмотрите youtube.com Invidious

Чтобы глубже разобраться в защите и усилении macOS, мы рекомендуем прочитать это руководство, которое охватывает многие проблемы: bejarano.io Archive.org

Вот базовые шаги, которые следует выполнить после офлайн-установки:

Включить пароль прошивки с параметром disable-reset-capability

Сначала настройте пароль прошивки по этому руководству Apple: support.apple.com Archive.org

К сожалению, некоторые атаки всё ещё возможны, и противник может отключить этот пароль, поэтому также следует следовать этому руководству, чтобы запретить отключение пароля прошивки кому-либо, включая Apple: support.apple.com Archive.org

Включить гибернацию вместо сна

И снова: это нужно для смягчения некоторых атак Cold Boot и Evil Maid путём отключения питания RAM и очистки ключа шифрования при закрытии крышки. Всегда следует либо использовать гибернацию, либо выключать устройство. В macOS у гибернации даже есть специальная опция для явной очистки ключа шифрования из памяти при переходе в гибернацию, тогда как в других операционных системах иногда приходится ждать исчезновения данных из памяти. И снова: простых настроек для этого нет, поэтому придётся выполнить несколько команд для включения гибернации:

• Откройте Terminal.

• Выполните: `sudo pmset -a destroyfvkeyonstandby 1`

  • Эта команда укажет macOS уничтожать ключ Filevault при Standby (сне).

• Выполните: `sudo pmset -a hibernatemode 25`

  • Эта команда укажет macOS отключать питание памяти во время сна вместо гибридной гибернации, где память остаётся под питанием. Пробуждение станет медленнее, но время работы от батареи увеличится.

Теперь при закрытии крышки MacBook должен переходить в гибернацию вместо сна и смягчать попытки атак Cold Boot.

Кроме того, стоит настроить автоматический сон (Settings > Energy), чтобы MacBook автоматически уходил в гибернацию, если его оставили без присмотра.

Отключить ненужные службы

Отключите некоторые ненужные настройки:

• Отключите Bluetooth.

• Отключите камеру и микрофон.

• Отключите службы определения местоположения.

• Отключите Airdrop.

• Отключите индексацию.

Предотвратить OCSP-запросы Apple

Это печально известные «неблокируемые телеметрические» запросы macOS Big Sur, раскрытые здесь: sneak.berlin Archive.org

Можно заблокировать OCSP-отчётность, выполнив в Terminal команду:

• `sudo sh -c 'echo "127.0.0.1 ocsp.apple.com" >> /etc/hosts'`

Но сначала стоит самостоятельно изучить реальную проблему. Эта страница — хорошее место для начала: blog.jacopo.io Archive.org

Решать вам. Мы бы заблокировали это, потому что не хотим вообще никакой телеметрии от моей ОС к «материнскому кораблю» без моего явного согласия. Никакой.

Включить полное шифрование диска (Filevault)

Следует включить полное шифрование диска на Mac через Filevault по этой части руководства: github.com Archive.org

Будьте осторожны при включении. Не храните ключ восстановления у Apple, если будет предложено; это не должно быть проблемой, поскольку на этом этапе вы должны быть офлайн. Вы не хотите, чтобы третья сторона имела ваш ключ восстановления.

Рандомизация MAC-адреса

К сожалению, macOS не предлагает удобного встроенного способа рандомизации MAC-адреса, поэтому придётся делать это вручную. После каждой перезагрузки всё сбросится, и вам придётся повторять это каждый раз, чтобы не использовать настоящий MAC-адрес при подключении к разным Wi-Fi.

Это можно сделать командами в терминале, без скобок:

• (выключить Wi-Fi) `networksetup -setairportpower en0 off`

• (изменить MAC-адрес) `sudo ifconfig en0 ether 88:63:11:11:11:11`

• (снова включить Wi-Fi) `networksetup -setairportpower en0 on`

Настройка безопасного браузера

См. Безопасный браузер в основной ОС

Основная ОС Windows

Как упоминалось ранее, мы не рекомендуем использовать повседневный ноутбук для чувствительных действий. Или, по крайней мере, не рекомендуем использовать для них уже установленную на нём ОС. Это может привести к нежелательным утечкам данных, которые можно использовать для деанонимизации. Если у вас есть отдельный ноутбук для этого, следует переустановить на нём свежую чистую ОС. Если вы не хотите стирать ноутбук и начинать заново, рассмотрите маршрут Tails или продолжайте на свой риск.

Я также рекомендую выполнять начальную установку полностью офлайн, чтобы избежать утечки данных.

Установка

Следуйте разделу Установка Windows.

Для лёгкого введения можно посмотреть youtube.com Invidious

Включить рандомизацию MAC-адреса

Рандомизируйте MAC-адрес, как объяснялось ранее в руководстве:

Перейдите в Settings > Network & Internet > Wi-Fi > Enable Random hardware addresses.

Либо можно использовать это бесплатное ПО: technitium.com Archive.org

Настройка безопасного браузера

См. Безопасный браузер в основной ОС

Включить дополнительные настройки приватности в основной ОС

См. Дополнительные настройки приватности Windows

Шифрование основной ОС Windows

Если вы собираетесь использовать правдоподобное отрицание на уровне всей системы

Veracrypt[40] — это программа, которую мы будем рекомендовать для полного шифрования диска, шифрования файлов и правдоподобного отрицания. Это ответвление известного, но устаревшего и больше не поддерживаемого TrueCrypt. Его можно использовать для:

- простого полного шифрования диска (жёсткий диск зашифрован одной парольной фразой);
- полного шифрования диска с правдоподобным отрицанием (это означает, что в зависимости от парольной фразы, введённой при загрузке, вы загрузите либо ложную ОС, либо скрытую ОС);
- простого шифрования файлового контейнера (это большой файл, который можно подключить в Veracrypt как внешний диск, чтобы хранить внутри зашифрованные файлы);
- файлового контейнера с правдоподобным отрицанием (это тот же большой файл, но в зависимости от парольной фразы, которую вы используете при подключении, будет подключён либо «скрытый том», либо «ложный том»).

Насколько мне известно, это единственное удобное, пригодное для обычного использования, бесплатное, открытое и открыто прошедшее аудит[41] ПО для шифрования, которое также предоставляет правдоподобное отрицание для широкого применения и работает с Windows Home Edition.

Скачайте и установите Veracrypt отсюда: veracrypt.fr Archive.org

После установки уделите минуту следующим параметрам, которые помогут смягчить некоторые атаки:

- Зашифруйте память параметром Veracrypt[42] (settings > performance/driver options > encrypt RAM) ценой 5-15% производительности. Этот параметр также отключит гибернацию, которая не очищает ключ активно при переходе в гибернацию, и вместо этого зашифрует память целиком, чтобы смягчить некоторые атаки Cold Boot. Подробнее об этой функции здесь: sourceforge.net Archive.org
- Включите параметр Veracrypt для очистки ключей из памяти при вставке нового устройства (system > settings > security > clear keys from memory if a new device is inserted). Это может помочь, если система будет изъята всё ещё включённой, но заблокированной.
- Включите параметр Veracrypt для подключения томов как съёмных (Settings > Preferences > Mount volume as removable media). Это помешает Windows писать некоторые журналы о подключениях в журналы событий[43] и предотвратит часть локальных утечек данных.
- Будьте осторожны и сохраняйте хорошую осведомлённость об обстановке, если чувствуете что-то странное. Выключите ноутбук как можно быстрее.

Если вы не хотите использовать зашифрованную память, потому что производительность может быть проблемой, следует хотя бы включить гибернацию вместо сна. Это не очистит ключи из памяти, и вы всё ещё будете уязвимы к атакам Cold Boot, но по крайней мере должно смягчить их, если у памяти будет достаточно времени, чтобы данные исчезли.

Подробнее позже в Маршрут A и B: простое шифрование с Veracrypt (руководство для Windows).

Если вы не собираетесь использовать правдоподобное отрицание на уровне всей системы

В этом случае для полного шифрования диска мы рекомендуем использовать BitLocker вместо Veracrypt. Причина в том, что BitLocker, в отличие от Veracrypt, не предлагает возможности правдоподобного отрицания. У жёсткого противника тогда нет стимула продолжать «усиленный» допрос, если вы раскрыли парольную фразу.

Обычно в этом случае у вас должна быть установлена Windows Pro, и настройка BitLocker довольно прямолинейна.

В целом можно следовать инструкциям здесь: support.microsoft.com Archive.org

Но вот шаги:

• Нажмите меню Windows.

• Введите «Bitlocker».

• Нажмите «Manage Bitlocker».

• Нажмите «Turn on Bitlocker» на системном диске.

• Следуйте инструкциям:

  • **Не сохраняйте ключ восстановления в Microsoft Account, если будет предложено.**

  • **Сохраняйте ключ восстановления только на внешний зашифрованный диск. Чтобы обойти это, распечатайте ключ восстановления через принтер Microsoft Print to PDF и сохраните ключ в папку Documents. Позже удалите этот файл.**

  • **Шифруйте весь диск, а не только используемое пространство.**

  • **Используйте «New Encryption Mode».**

  • **Запустите проверку BitLocker.**

  • **Перезагрузитесь.**

• Теперь шифрование должно начаться в фоне; проверить это можно, нажав значок Bitlocker в правой нижней части панели задач.

К сожалению, этого недостаточно. При такой настройке ключ Bitlocker может храниться как есть в TPM-чипе компьютера. Это довольно проблемно, потому что в некоторых случаях ключ можно легко извлечь[44][45][46][47].

Чтобы смягчить это, нужно включить ещё несколько параметров согласно рекомендациям Microsoft[48]:

• Нажмите значок Windows.

• Введите Run.

• Введите `gpedit.msc` (это редактор групповой политики).

• Перейдите в Computer Configuration > Administrative Templates > Windows Components > BitLocker > Operating System Drives.

  • Дважды нажмите «Require Additional Authentication at Startup».

    • Нажмите «Configure TPM Startup PIN» и установите «Require Startup PIN with TPM».

  • Дважды нажмите «Allow enhanced PINs for startup».

    • Нажмите «Enable» (это позволит задать пароль, а не PIN).

• Закройте редактор групповой политики.

• Нажмите значок Windows.

• Введите Command, чтобы открыть «Command Prompt».

• Нажмите по нему правой кнопкой и выберите «Run as Administrator».

• Выполните `manage-bde -protectors -delete c:` (это удалит текущую защиту: ключ восстановления, который вам не понадобится).

• Выполните `manage-bde -protectors -add c: -TPMAndPIN` (это запросит пароль до загрузки).

  • Введите выбранный пароль или парольную фразу, хорошую.

• Выполните `manage-bde -status`

  • Теперь для диска C: в разделе «Key Protectors» вы должны увидеть вариант «TPM and PIN».

• Готово.

Теперь при перезагрузке компьютера в идеале должны появляться:

• пароль загрузки BIOS/UEFI;

• пароль разблокировки SSD/HDD, если такая функция доступна в BIOS;

• экран Bitlocker Pre-Boot Pin, где нужно ввести только что настроенный пароль/парольную фразу;

• и наконец экран входа Windows, где можно ввести учётные данные, настроенные ранее.

Включить гибернацию (необязательно)

И снова, как объяснялось ранее: никогда не используйте функцию сна/stand-by, чтобы смягчить некоторые атаки Cold Boot и Evil Maid. Вместо этого следует выключать устройство или переводить его в гибернацию. Поэтому нужно переключить ноутбук со сна на гибернацию при закрытии крышки или при уходе ноутбука в сон.

(**Обратите внимание: если ранее вы включили шифрование RAM в Veracrypt, включить гибернацию нельзя**)

Причина в том, что гибернация действительно полностью выключит ноутбук и очистит память. Сон, напротив, оставит память под питанием, включая ключ расшифровки, и может оставить ноутбук уязвимым к атакам Cold Boot.

По умолчанию Windows 10/11 может не предлагать такую возможность, поэтому её нужно включить по этому руководству Microsoft: docs.microsoft.com Archive.org

• Откройте командную строку администратора: нажмите правой кнопкой по Command Prompt и выберите «Run as Administrator».

• Выполните: `powercfg.exe /hibernate on`

• Теперь выполните дополнительную команду: `powercfg /h /type full`

  • **Эта команда убедится, что режим гибернации полный и полностью очищает память, хотя и не безопасным стиранием.**

После этого перейдите в настройки питания:

• Откройте Control Panel.

• Откройте System & Security.

• Откройте Power Options.

• Откройте «Choose what the power button does».

• Измените всё со сна на гибернацию или выключение.

• Вернитесь в Power Options.

• Выберите Change Plan Settings.

• Выберите Advanced Power Settings.

• Измените все значения Sleep для каждого плана питания на 0 (Never).

• Убедитесь, что Hybrid Sleep отключён для каждого плана питания.

• Включите Hibernate After на нужное вам время.

• Отключите все Wake timers.

Выбор подмаршрута

Теперь нужно выбрать следующий шаг между несколькими вариантами:

• Маршрут A: простое шифрование текущей ОС
    • Плюсы:
        • Не требует стирать ноутбук.
        • Нет проблемы локальных утечек данных.
        • Нормально работает с SSD.
        • Работает с любой ОС.
        • Просто.
    • Минусы:
        • Противник может принудить вас раскрыть пароль и все секреты, и у вас не будет правдоподобного отрицания.
        • Опасность онлайн-утечек данных.
• Маршрут B: простое шифрование текущей ОС с последующим использованием правдоподобного отрицания на уровне самих файлов:
    • Плюсы:
        • Не требует стирать ноутбук.
        • Нормально работает с SSD.
        • Работает с любой ОС.
        • Правдоподобное отрицание возможно против «мягких» противников.
    • Минусы:
        • Опасность онлайн-утечек данных.
        • Опасность локальных утечек данных, из-за которых придётся больше работать над очисткой таких утечек.
• Маршрут C: шифрование операционной системы с правдоподобным отрицанием; у вас будет «скрытая ОС» и «ложная ОС», работающие на ноутбуке:

- Плюсы:
  - Нет проблем с локальными утечками данных.
  - Правдоподобное отрицание возможно против «мягких» противников.
- Минусы:
  - Требуется Windows; эта функция «легко» не поддерживается в Linux.
  - Опасность онлайн-утечек данных.
  - Требует полного стирания ноутбука.
  - Не подходит для SSD из-за необходимости отключать операции Trim[49][50]. Это со временем серьёзно ухудшит производительность и здоровье SSD.

Как видите, маршрут C даёт только два преимущества приватности по сравнению с остальными, и он будет полезен только против мягкого законного противника. Помните en.wikipedia.org Wikiless Archive.org**.**

Решение, какой маршрут выбрать, остаётся за вами. Маршрут A — минимум.

Обязательно часто проверяйте новые версии Veracrypt, чтобы получать последние исправления. Особенно проверяйте это перед применением крупных обновлений Windows, которые могут сломать загрузчик Veracrypt и отправить вас в цикл загрузки.

ОБРАТИТЕ ВНИМАНИЕ: ПО УМОЛЧАНИЮ VERACRYPT ВСЕГДА ПРЕДЛАГАЕТ СИСТЕМНЫЙ ПАРОЛЬ В QWERTY (покажите пароль как тест). Это может вызвать проблемы, если ввод при загрузке использует клавиатуру ноутбука, например AZERTY: пароль был задан в QWERTY, а при загрузке вы вводите его в AZERTY. Поэтому во время тестовой загрузки обязательно проверьте, какую раскладку использует BIOS. Вы можете не войти просто из-за путаницы QWERTY/AZERTY. Если BIOS загружается с AZERTY, пароль в Veracrypt нужно вводить как в QWERTY.

Маршрут A и B: простое шифрование с Veracrypt (руководство для Windows)

Пропустите этот шаг, если ранее использовали BitLocker.

Для этого метода не обязательно иметь HDD, и на этом маршруте не нужно отключать Trim. Утечки Trim будут полезны криминалистике только для обнаружения наличия скрытого тома, но в остальном не дадут большой пользы.

Этот маршрут довольно прямолинеен: он просто зашифрует текущую операционную систему на месте, без потери данных. Обязательно читайте весь текст, который показывает Veracrypt, чтобы полностью понимать происходящее. Шаги:

- Запустите VeraCrypt.
- Перейдите в Settings:
  - Settings > Performance/driver options > Encrypt RAM
  - System > Settings > Security > Clear keys from memory if a new device is inserted
  - System > Settings > Windows > Enable Secure Desktop
- Выберите System.
- Выберите Encrypt System Partition/Drive.

• Выберите Normal (Simple).

• Выберите Single-Boot.

• Выберите AES как алгоритм шифрования; нажмите кнопку test, если хотите сравнить скорости.

• Выберите SHA-512 как хэш-алгоритм, потому что почему бы и нет.

• Введите сильную парольную фразу; чем длиннее, тем лучше, помните Рекомендации по паролям и парольным фразам.

• Соберите немного энтропии, случайно двигая курсор, пока полоса не заполнится.

• Нажмите Next на экране Generated Keys.

• Делать rescue disk[51] или нет — решать вам. Мы рекомендуем сделать его на всякий случай; просто храните его вне зашифрованного диска, например на USB-накопителе, или дождитесь конца руководства с рекомендациями по безопасным резервным копиям. Этот rescue disk не хранит вашу парольную фразу, и она всё равно понадобится для его использования.

• Wipe mode:

  • Если на этом ноутбуке ещё нет чувствительных данных, выберите None.

  • Если чувствительные данные есть на SSD, Trim сам должен с этим справиться[52], но мы бы рекомендовали один проход случайными данными для уверенности.

  • Если чувствительные данные есть на HDD, Trim там нет, и мы бы рекомендовали минимум 1 проход.

• Проверьте настройку. Veracrypt перезагрузит систему для проверки загрузчика перед шифрованием. Этот тест должен пройти, чтобы шифрование продолжилось.

• После перезагрузки и успешного теста Veracrypt предложит начать процесс шифрования.

• Запустите шифрование и дождитесь завершения.

• Готово; пропустите маршрут B и переходите к следующим шагам.

Отдельный раздел о создании зашифрованных файловых контейнеров с правдоподобным отрицанием в Windows будет позже.

Маршрут B: шифрование с правдоподобным отрицанием и скрытой ОС (только Windows)

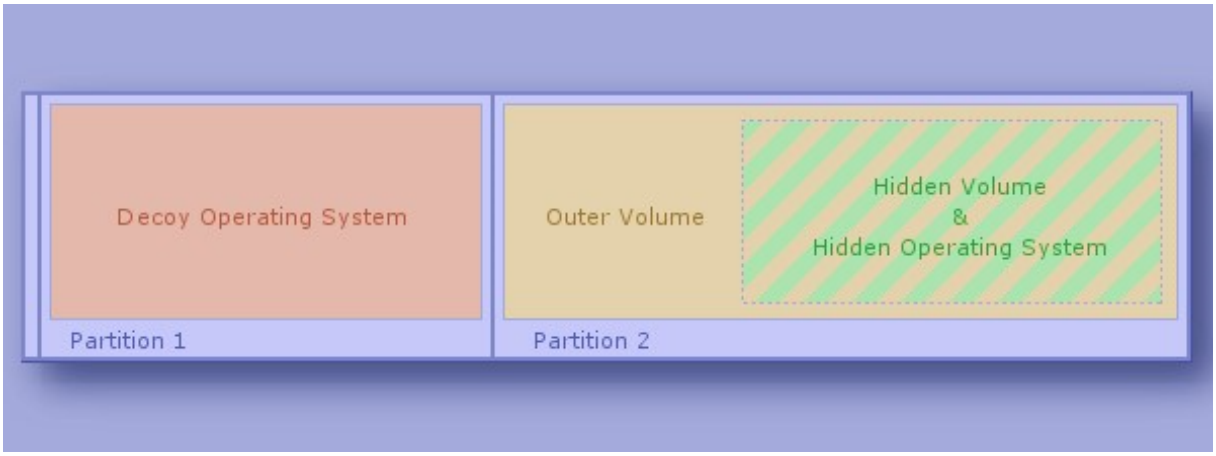
Поддерживается только в Windows.

Рекомендуется только на HDD. На SSD не рекомендуется.

Скрытая ОС не должна быть активирована ключом продукта MS. Поэтому этот маршрут рекомендует и описывает полную чистую установку, которая сотрёт всё на ноутбуке.

Прочитайте документацию Veracrypt veracrypt.fr Archive.org (часть Process of Creation of Hidden Operating System) и veracrypt.fr Archive.org (Security Requirements and Precautions Pertaining to Hidden Volumes).

Вот как будет выглядеть система после завершения процесса:



(Иллюстрация из документации Veracrypt, veracrypt.fr Archive.org)

Как видите, этот процесс требует, чтобы на жёстком диске с самого начала было два раздела.

Этот процесс сделает следующее:

• Зашифрует второй раздел (внешний том), который из ложной ОС будет выглядеть как пустой неформатированный диск.

• Предложит возможность скопировать немного ложного содержимого во внешний том.

  • Именно сюда вы скопируете ложную коллекцию аниме/порно с какого-нибудь внешнего жёсткого диска во внешний том.

• Создаст скрытый том внутри внешнего тома второго раздела. Там будет находиться скрытая ОС.

• Клонирует текущую работающую установку Windows 10/11 в скрытый том.

• Сотрёт текущую работающую Windows 10/11.

• Это означает, что текущая Windows 10/11 станет скрытой Windows 10/11, а вам нужно будет заново установить свежую ложную Windows 10/11.

Обязательно, если у вас SSD и вы всё равно хотите сделать это вопреки рекомендации: отключите SSD Trim в Windows[53] (повторим: это совсем НЕ рекомендуется, потому что само отключение Trim крайне подозрительно). **Кроме того, как упоминалось ранее, отключение Trim сократит срок службы SSD и со временем значительно ухудшит его производительность: ноутбук будет становиться всё медленнее в течение нескольких месяцев использования, пока не станет почти непригодным, после чего придётся очищать диск и переустанавливать всё. Но это нужно сделать, чтобы предотвратить утечки данных[54], которые могут позволить криминалистике сорвать ваше правдоподобное отрицание[55][56]. Единственный обходной путь сейчас — иметь ноутбук с классическим HDD.**

Шаг 1: создать установочный USB-накопитель Windows 10/11

См. Создание установочного носителя Windows и выберите вариант с USB-накопителем.

Шаг 2: загрузиться с USB-накопителя и начать установку Windows 10/11 (скрытая ОС)

• Вставьте USB-накопитель в ноутбук.

• См. Установка Windows и продолжайте установку Windows 10/11 Home.

Шаг 3: настройки приватности (скрытая ОС)

См. Дополнительные настройки приватности Windows

Шаг 4: установка Veracrypt и начало процесса шифрования (скрытая ОС)

Не забудьте прочитать veracrypt.fr Archive.org

Не подключайте эту ОС к известному вам Wi-Fi. Скачайте установщик Veracrypt с другого компьютера и перенесите его сюда с помощью USB-накопителя. Шаги:

• Установите Veracrypt.

• Запустите Veracrypt.

• Перейдите в Settings:

  • Settings > Performance/driver options > Encrypt RAM (**обратите внимание: этот параметр несовместим с гибернацией ноутбука и означает, что придётся полностью выключаться**)

  • System > Settings > Security > Clear keys from memory if a new device is inserted

  • System > Settings > Windows > Enable Secure Desktop

• Перейдите в System и выберите Create Hidden Operating System.

• Внимательно прочитайте все подсказки.

• Выберите Single-Boot, если будет предложено.

• Создайте внешний том, используя AES и SHA-512.

• Используйте всё доступное пространство второго раздела для внешнего тома.

• Используйте сильную парольную фразу (помните Рекомендации по паролям и парольным фразам).

• Выберите yes для Large Files.

• Создайте энтропию, двигая мышь, пока полоса не заполнится, и выберите NTFS. Не выбирайте exFAT: внешний том должен выглядеть «обычно», а NTFS — обычный вариант.

• Отформатируйте внешний том.

• Откройте внешний том:

    - На этом этапе нужно скопировать ложные данные во внешний том. У вас должны быть какие-то чувствительные, но не слишком чувствительные файлы/папки, которые можно туда скопировать на случай, если придётся раскрыть пароль к этому тому**.** Это хорошее место для коллекции аниме/Mp3/фильмов/порно.
    - Мы рекомендуем не заполнять внешний том слишком сильно или слишком слабо: примерно 40%. Помните, что нужно оставить достаточно места для скрытой ОС, которая будет того же размера, что и первый раздел, созданный при установке.
- Используйте сильную парольную фразу для скрытого тома; очевидно, другую, не такую как у внешнего тома.
- Теперь создайте скрытый том, выберите AES и SHA-512.
- Заполните полосу энтропии до конца случайными движениями мыши.
- Отформатируйте скрытый том.
- Продолжайте клонирование.
- Veracrypt перезапустится и клонирует Windows, в которой вы начали этот процесс, в скрытый том. Эта Windows станет вашей скрытой ОС.
- Когда клонирование завершится, Veracrypt перезапустится внутри скрытой системы.
- Veracrypt сообщит, что скрытая система установлена, а затем предложит стереть исходную ОС, то есть ту, которую вы ранее установили с USB-накопителя.
- Используйте 1-Pass Wipe и продолжайте.
- Теперь скрытая ОС будет установлена; переходите к следующему шагу.

Шаг 5: перезагрузиться, загрузиться с USB-накопителя и снова начать установку Windows 10/11 (ложная ОС)

Теперь, когда скрытая ОС полностью установлена, нужно установить ложную ОС:

- Вставьте USB-накопитель в ноутбук.
- См. Установка Windows и снова продолжайте установку Windows 10/11 Home; не устанавливайте другую версию, придерживайтесь Home.

Шаг 6: настройки приватности (ложная ОС)

См. Дополнительные настройки приватности Windows

Шаг 7: установка Veracrypt и начало процесса шифрования (ложная ОС)

Теперь вы зашифруете ложную ОС:

• Установите Veracrypt.

• Запустите VeraCrypt.

• Выберите System.

• Выберите Encrypt System Partition/Drive.

• Выберите Normal (Simple).

• Выберите Single-Boot.

• Выберите AES как алгоритм шифрования; нажмите кнопку test, если хотите сравнить скорости.

• Выберите SHA-512 как хэш-алгоритм, потому что почему бы и нет.

• Введите короткий слабый пароль (да, это серьёзно, сделайте так; позже будет объяснено).

• Соберите энтропию, случайно двигая курсор, пока полоса не заполнится.

• Нажмите Next на экране Generated Keys.

• Делать rescue disk[57] или нет — решать вам. Мы рекомендуем сделать его на всякий случай; просто храните его вне зашифрованного диска, например на USB-накопителе, или дождитесь конца руководства с рекомендациями по безопасным резервным копиям. Этот rescue disk не хранит вашу парольную фразу, и она всё равно понадобится для его использования.

• Wipe mode: выберите 1-Pass на всякий случай.

• Предварительно проверьте настройку. Veracrypt перезагрузит систему для проверки загрузчика перед шифрованием. Этот тест должен пройти, чтобы шифрование продолжилось.

• После перезагрузки и успешного теста Veracrypt предложит начать процесс шифрования.

• Запустите шифрование и дождитесь завершения.

• Ложная ОС теперь готова к использованию.

Шаг 8: проверить настройку (загрузка в обе ОС)

Время проверить настройку:

• Перезагрузитесь и введите парольную фразу скрытой ОС; вы должны загрузиться в скрытую ОС.

• Перезагрузитесь и введите парольную фразу ложной ОС; вы должны загрузиться в ложную ОС.

• Запустите Veracrypt в ложной ОС и подключите второй раздел с парольной фразой внешнего тома. Подключайте его только для чтения: перейдите в Mount Options и выберите Read-Only. Он должен подключить второй раздел как доступный только для чтения и показать ложные данные, то есть вашу коллекцию аниме/порно. Сейчас вы подключаете его только для чтения, потому что если записать туда данные, можно перезаписать содержимое скрытой ОС.

Шаг 9: безопасное изменение ложных данных во внешнем томе

Перед переходом к следующему шагу нужно научиться безопасно подключать внешний том для записи. Это также объяснено в официальной документации Veracrypt veracrypt.fr Archive.org

Делайте это из безопасного, доверенного пространства.

В общих чертах вы подключаете внешний том, одновременно указывая парольную фразу скрытого тома в Mount Options, чтобы защитить скрытый том от перезаписи:

• Откройте Veracrypt.

• Выберите второй раздел.

• Нажмите Mount.

• Нажмите Mount Options.

• Отметьте параметр «Protect the Hidden volume...».

• Введите парольную фразу скрытой ОС.

• Нажмите OK.

• Введите парольную фразу внешнего тома.

• Нажмите OK.

• Теперь вы сможете открыть внешний том и писать в него, меняя содержимое: копировать, перемещать, удалять, редактировать...

Эта операция фактически не подключает скрытый том и должна предотвратить создание криминалистических доказательств, которые могли бы привести к обнаружению скрытой ОС. Однако пока вы выполняете эту операцию, оба пароля будут храниться в RAM. Вы всё ещё можете быть уязвимы к атаке Cold Boot. Чтобы смягчить это, убедитесь, что включили шифрование RAM, как было указано ранее.

Шаг 10: оставить криминалистические доказательства внешнего тома (с ложными данными) внутри ложной ОС

Нужно сделать ложную ОС как можно более правдоподобной. Мы также хотим, чтобы противник недооценил ваш интеллект.

Важно добровольно оставить некоторые криминалистические доказательства ложного содержимого внутри ложной ОС. Эти доказательства позволят криминалистам увидеть, что вы часто подключали внешний том для доступа к его содержимому.

Полезные советы, чтобы оставить такие доказательства:

• Воспроизводите содержимое внешнего тома из ложной ОС, например через VLC. Убедитесь, что история сохраняется.

• Редактируйте документы и работайте с ними.

• Снова включите индексацию файлов в ложной ОС и включите подключённый внешний том.

• Отключайте и часто подключайте его, чтобы смотреть содержимое или перемещать файлы.

• Скопируйте часть содержимого из внешнего тома в ложную ОС, а затем удалите небезопасно. Просто положите в Recycle Bin, как сделал бы наивный человек, думающий, что файл удалён.

• Установите Torrent Client в ложной ОС; время от времени используйте его, чтобы скачивать похожие материалы, которые вы оставите в ложной ОС.

• Можно установить VPN-клиент в ложной ОС с известным вам VPN, не оплаченным наличными.

Не кладите ничего подозрительного в ложную ОС, например:

• это руководство;

• любые ссылки на это руководство;

• любое подозрительное ПО для анонимности, например Tor Browser;

• любые тома Veracrypt;

• любые документы об анонимности или безопасности.

Замысел в том, чтобы заставить противника поверить, что вы не так умны, как он думал, и отбить желание копать глубже.

Примечания

Помните, что для работы сценария правдоподобного отрицания вам нужны убедительные объяснения:

• **Вы используете Veracrypt, потому что у вас Windows 10/11 Home, где нет Bitlocker, но вы всё равно хотели разумную приватность.**

• **У вас два раздела, потому что вы хотели отделить систему от данных для удобной организации, и потому что какой-то технически подкованный друг сказал, что так лучше для производительности.**

• **Вы использовали слабый пароль для удобной быстрой загрузки системы и сильную длинную парольную фразу для внешнего тома. Вам было лень вводить сильную парольную фразу при каждой загрузке.**

• **Вы зашифровали второй раздел другим паролем, отличным от системного, потому что не хотите, чтобы кто-либо в вашей группе/домене видел ваши вещи. Вы не хотели, чтобы эти данные были доступны кому-либо.**

Уделите время и снова прочитайте раздел «Possible Explanations for Existence of Two Veracrypt Partitions on Single Drive» в документации Veracrypt здесь: veracrypt.fr Archive.org

Будьте осторожны:

• **Никогда не подключайте скрытый том из ложной ОС (НИКОГДА). Если вы это сделаете, внутри ложной ОС появятся криминалистические доказательства скрытого тома, что может поставить под угрозу попытку правдоподобного отрицания**. Если вы всё же сделали это намеренно или по ошибке из ложной ОС, есть способы стереть криминалистические доказательства; они будут объяснены позже в конце руководства, так что сама по себе эта ошибка не катастрофа, если вы выполните шаги из Дополнительных мер против криминалистики.

• **Никогда не используйте ложную ОС из той же сети, например публичного Wi-Fi, что и скрытую ОС.**

• **Когда вы подключаете внешний том из ложной ОС, не записывайте данные во внешний том. Это может перезаписать то, что выглядит как пустое пространство, но на самом деле является скрытой ОС. Всегда подключайте его только для чтения.**

- **Если вы хотите изменить ложное содержимое внешнего тома, следует использовать USB-накопитель с Live OS, на котором будет запускаться Veracrypt.**
- **Обратите внимание: вы не будете использовать скрытую ОС для выполнения чувствительных действий; позже это будет делаться из виртуальной машины внутри скрытой ОС. Скрытая ОС предназначена только для защиты от мягких законных противников, которые могут получить доступ к ноутбуку и принудить вас раскрыть пароль.**
- **Будьте осторожны с любым вмешательством в ноутбук. Атаки Evil Maid могут раскрыть скрытую ОС.**

Virtualbox в основной ОС

Помните Виртуализация.

Этот шаг и следующие шаги должны выполняться внутри основной ОС. Это может быть ваша основная ОС с простым шифрованием (Windows/Linux/macOS) или скрытая ОС с правдоподобным отрицанием (только Windows).

В этом маршруте вы будете активно использовать бесплатное ПО Oracle Virtualbox[58]. Это программа виртуализации, в которой можно создавать виртуальные машины, имитирующие компьютер с определённой ОС. Если хотите использовать что-то другое, например Xen, Qemu, KVM или VMWARE, можете, но для удобства эта часть руководства рассматривает только Virtualbox.

Следует понимать, что у Virtualbox не лучшая история с точки зрения безопасности среди программ виртуализации. Некоторые из сообщённых проблем[59] до сих пор не полностью исправлены[60]. Если вы используете Linux и обладаете чуть большими техническими навыками, стоит рассмотреть KVM, следуя руководству Whonix здесь whonix.org Archive.org

В любом случае нужно выполнить некоторые шаги:

Все чувствительные действия будут выполняться внутри гостевой виртуальной машины с Windows 10/11 Pro (на этот раз не Home), Linux или macOS.

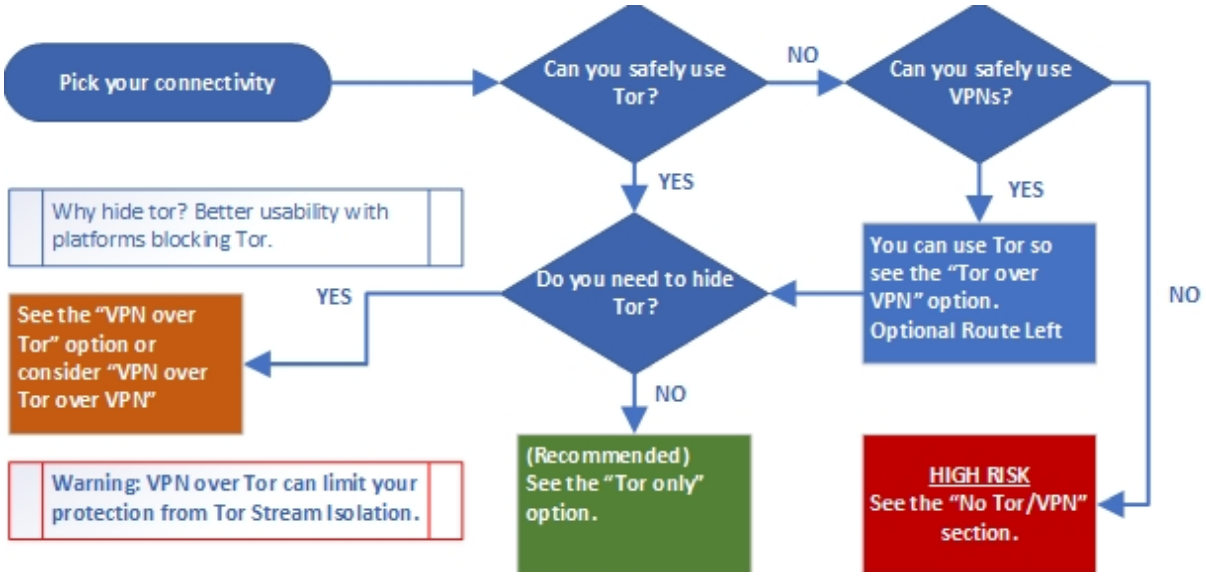
У этого есть несколько преимуществ, которые помогут оставаться анонимным:

- Это должно помешать гостевой ОС виртуальной машины (Windows/Linux/macOS), приложениям и любой телеметрии внутри виртуальных машин напрямую получать доступ к вашему оборудованию. Даже если виртуальная машина будет скомпрометирована вредоносным ПО, оно не должно получить доступ к основной ОС и скомпрометировать реальную машину.
- Это позволит принудительно направить весь сетевой трафик виртуальной машины через другую шлюзовую виртуальную машину, которая направит весь трафик через сеть Tor. Это сетевой «аварийный выключатель». Ваша виртуальная машина полностью потеряет сетевое подключение и уйдёт офлайн, если целевая сетевая виртуальная машина потеряет соединение с сетью Tor.
- Сама виртуальная машина, имеющая интернет-доступ только через шлюз сети Tor, будет подключаться к вашему VPN-сервису, оплаченному наличными, через Tor.
- Утечки DNS будут невозможны, потому что виртуальная машина находится в изолированной сети, которая при любых условиях должна проходить через Tor.

Выбор способа подключения

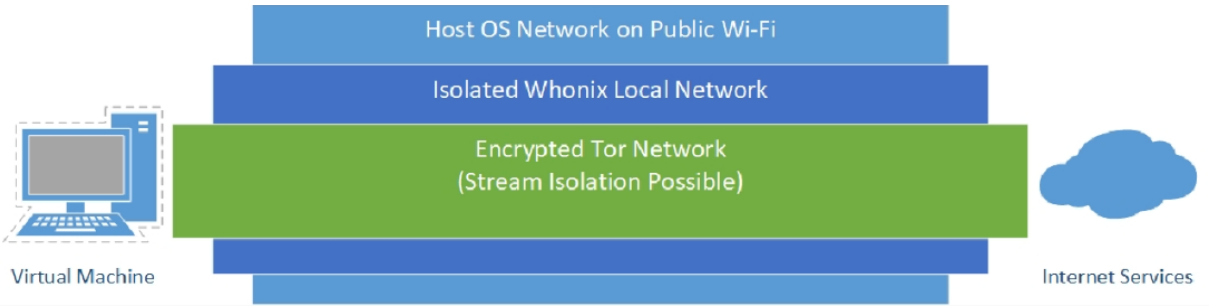
В этом маршруте есть семь возможностей:

- **Рекомендуемые и предпочтительные:**
  - **Использовать только Tor (пользователь > Tor > интернет)**
  - **Использовать VPN поверх Tor (пользователь > Tor > VPN > интернет) в отдельных случаях**
  - **Использовать VPS с самостоятельно размещённым VPN/прокси поверх Tor (пользователь > Tor > собственный VPN/прокси > интернет) в отдельных случаях**
- Возможны, если этого требует контекст:
  - Использовать VPN поверх Tor поверх VPN (пользователь > VPN > Tor > VPN > интернет)
  - Использовать Tor поверх VPN (пользователь > VPN > Tor > интернет)
- Не рекомендуется и рискованно:
  - Использовать только VPN (пользователь > VPN > интернет)
  - Использовать VPN поверх VPN (пользователь > VPN > VPN > интернет)
- **Не рекомендуется и крайне рискованно, но возможно**
  - Без VPN и без Tor (пользователь > интернет)



Только Tor

Это предпочтительное и наиболее рекомендуемое решение.



С этим решением вся ваша сеть проходит через Tor, и в большинстве случаев этого должно быть достаточно для гарантии анонимности.

Однако есть один главный недостаток: **некоторые сервисы напрямую блокируют/запрещают выходные узлы Tor и не позволяют создавать учётные записи с них.**

Чтобы смягчить это, возможно, придётся рассмотреть следующий вариант: VPN поверх Tor, но учитывайте связанные с ним риски, объяснённые в следующем разделе.

VPN/прокси поверх Tor

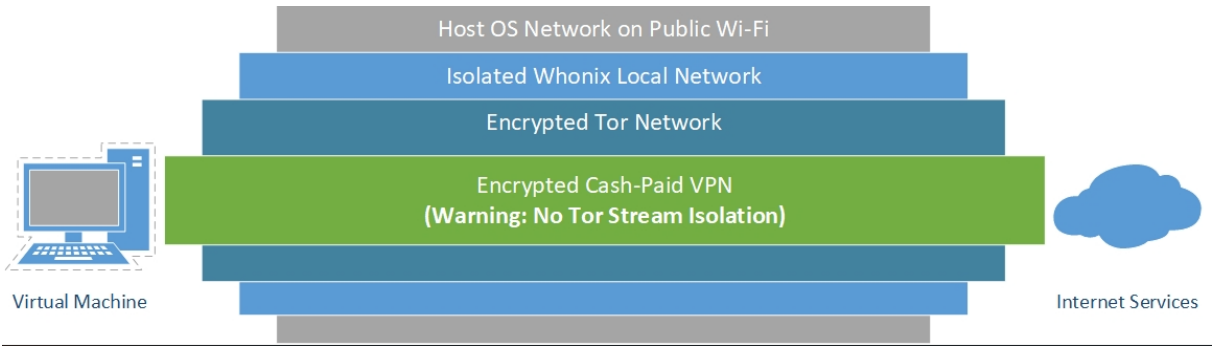
Это решение может дать преимущества в некоторых конкретных случаях по сравнению с использованием только Tor, когда доступ к целевому сервису с выходного узла Tor невозможен. Причина в том, что многие сервисы прямо запрещают, затрудняют или блокируют выходные узлы Tor (см. gitlab.torproject.org Archive.org).

Этого решения можно добиться двумя способами:

• платный VPN поверх Tor (самый простой);

• платный самостоятельно размещённый VPS, настроенный как VPN/прокси (самый эффективный для обхода онлайн-препятствий вроде CAPTCHA, но требует больше навыков Linux).

Как видно на этой иллюстрации, если ваш VPN/прокси, оплаченный наличными (предпочтительно) или Monero, скомпрометирован противником, несмотря на заявления о приватности и политики отсутствия журналов, он увидит только анонимный аккаунт VPN/прокси, оплаченный наличными/Monero, который подключается к его сервисам с выходного узла Tor.

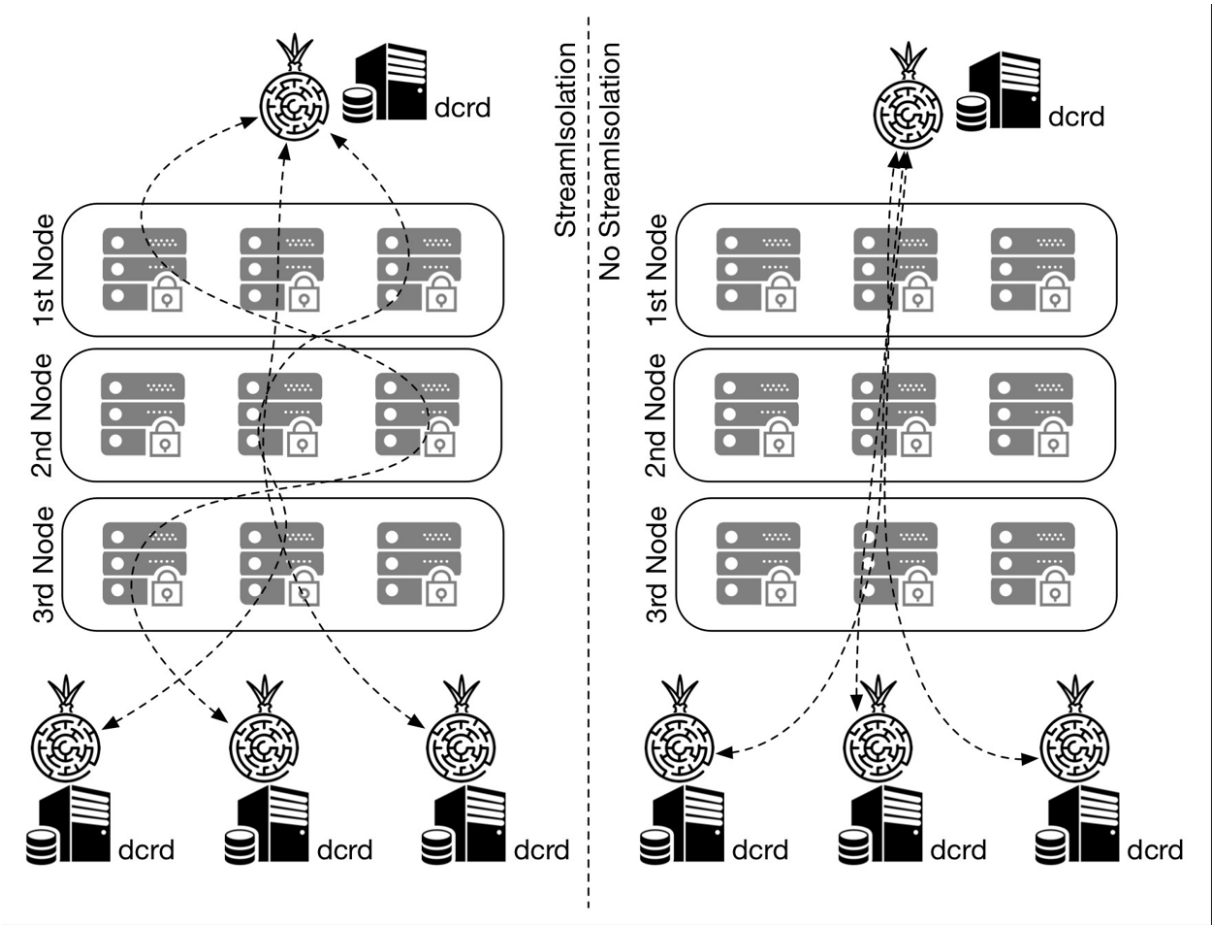


Если противнику каким-то образом удастся скомпрометировать и сеть Tor, он раскроет только IP случайного публичного Wi-Fi, не связанного с вашей личностью.

Если противник каким-то образом скомпрометирует ОС вашей виртуальной машины, например вредоносным ПО или эксплойтом, он будет заперт во внутренней сети Whonix и не должен суметь раскрыть IP публичного Wi-Fi.

Однако у этого решения есть один главный недостаток: вмешательство в изоляцию потоков Tor[61].

Изоляция потоков — это техника смягчения некоторых корреляционных атак, при которой для каждого приложения используются разные цепочки Tor. Вот иллюстрация, показывающая, что такое изоляция потоков:



(Иллюстрация Marcelo Martins, stakey.club Archive.org)

VPN/прокси поверх Tor относится к правой стороне[62], то есть использование VPN/прокси поверх Tor принуждает Tor использовать одну цепочку для всех действий вместо нескольких цепочек для каждого действия. Это означает, что VPN/прокси поверх Tor может в некоторых случаях снизить эффективность Tor, и поэтому его следует использовать только в отдельных случаях:

• когда целевой сервис не разрешает выходные узлы Tor;

• когда вас не смущает использование общей цепочки Tor для разных сервисов, например при использовании разных сервисов с входом в аккаунт.

Однако не стоит использовать этот метод, если ваша цель — просто просматривать разные случайные сайты без входа в аккаунт: вы не получите преимуществ изоляции потоков, и это может со временем упростить противнику корреляционные атаки между вашими сессиями (см. Ваш анонимизированный трафик Tor/VPN). Если же ваша цель — использовать одну и ту же идентичность в каждой сессии на одних и тех же сервисах с входом в аккаунт, ценность изоляции потоков ниже, потому что вас можно коррелировать другими средствами.

Также нужно знать, что изоляция потоков не обязательно настроена по умолчанию в Whonix Workstation. Она предварительно настроена только для некоторых приложений, включая Tor Browser.

Также обратите внимание, что изоляция потоков не обязательно меняет все узлы вашей цепочки Tor. Иногда она меняет только один или два. Во многих случаях изоляция потоков, например внутри Tor Browser, меняет только ретранслятор (средний) узел и выходной узел, сохраняя тот же сторожевой (входной) узел.

Подробнее:

• whonix.org Archive.org

• tails.boum.org Archive.org

• whonix.org Archive.org

Tor поверх VPN

Вы можете спросить: а что насчёт Tor поверх VPN вместо VPN поверх Tor? Мы бы не обязательно рекомендовали это:

• Недостатки:

  • Ваш VPN-провайдер — просто ещё один провайдер интернета, который будет знать ваш исходный IP и сможет деанонимизировать вас при необходимости. Мы им не доверяем. Мы предпочитаем ситуацию, где VPN-провайдер не знает, кто вы. Это мало добавляет с точки зрения анонимности.

  • В результате вы будете подключаться к разным сервисам с IP выходного узла Tor, который во многих местах заблокирован/помечен. Это не помогает с точки зрения удобства.

• Преимущества:

  • **Главное преимущество: если вы во враждебной среде, где доступ к Tor невозможен/опасен/подозрителен, но VPN допустим.**

  • Этот метод также не ломает изоляцию потоков Tor.

  • Он также скрывает активность Tor от основного провайдера.

Если у вас проблемы с доступом к сети Tor из-за блокировок/цензуры, можно попробовать мосты Tor. См. Использование мостов Tor во враждебной среде.

Также можно рассмотреть **VPN поверх Tor поверх VPN (пользователь > VPN > Tor > VPN > интернет)** с двумя VPN, оплаченными наличными/Monero. Это означает, что основная ОС подключится к первому VPN из публичного Wi-Fi, затем Whonix подключится к Tor, а наконец ваша виртуальная машина подключится ко второму VPN поверх Tor поверх VPN (см. whonix.org Archive.org).

Конечно, это сильно ударит по производительности и может быть довольно медленным, но Tor где-то необходим для достижения разумной анонимности.

Технически добиться этого в этом маршруте легко: нужны два отдельных анонимных VPN-аккаунта, и нужно подключиться к первому VPN из основной ОС, а затем следовать маршруту.

Вывод: делайте это только если считаете, что использование одного Tor рискованно/невозможно, но VPN допустимы. Или просто потому что можете и почему бы нет. Этот метод не снизит вашу безопасность/приватность/анонимность.

Только VPN

Этот маршрут не будет объясняться и не рекомендуется.

Если вы можете использовать VPN, вы должны суметь добавить поверх него слой Tor. А если можете использовать Tor, то можете добавить анонимный VPN поверх Tor и получить предпочтительное решение.

Простое использование VPN или даже VPN поверх VPN не имеет смысла, потому что со временем это можно связать с вами. Один из VPN-провайдеров будет знать ваш реальный исходный IP, даже если это безопасное публичное место, а если добавить поверх него ещё один, второй всё равно будет знать, что вы использовали первый VPN-сервис. Это лишь немного задержит деанонимизацию. Да, это дополнительный слой... но постоянный централизованный слой, и вас можно деанонимизировать со временем. Это просто цепочка из трёх провайдеров, каждый из которых подчиняется законным запросам.

Подробнее см. следующие источники:

• whonix.org Archive.org

• whonix.org Archive.org

• researchgate.net Archive.org

• gist.github.com Archive.org

• schub.wtf Archive.org

В контексте этого руководства Tor где-то необходим для разумной и безопасной анонимности, и вам следует использовать его, если можете.

Без VPN/Tor

Если там, где вы находитесь, нельзя использовать ни VPN, ни Tor, вы, вероятно, в очень враждебной среде, где слежка и контроль крайне высоки.

Просто не делайте этого: оно не стоит риска. Вас почти мгновенно может деанонимизировать любой мотивированный противник, который способен добраться до вашего физического местоположения за считанные минуты.

Не забудьте вернуться к противникам (угрозам) и проверке сети на слежку/цензуру с помощью OONI.

Если у вас совсем нет другого варианта и вы всё равно хотите что-то сделать, см. Что делать, когда Tor и VPN невозможны? **(на свой риск) и рассмотрите маршрут Tails вместо этого.**

Тип подключения	Анонимность	Простота доступа к онлайн-ресурсам	Изоляция потоков Tor	Безопаснее там, где Tor подозрителен/опасен	Скорость	Стоимость	Рекомендуется
Только Tor	**Хорошая**	**Средняя**	**Возможна**	**Нет**	**Средняя**	**Бесплатно**	**Да**
Tor поверх VPN	**Хорошая+**	**Средняя**	**Возможна**	**Да**	**Средняя**	**Около 50€/год**	**Если нужно (Tor недоступен)**

Тип подключения	Анонимность	Простота доступа к онлайн-ресурсам	Изоляция потоков Tor	Безопаснее там, где Tor подозрителен/опасен	Скорость	Стоимость	Рекомендуется
Tor поверх VPN поверх Tor	**Лучшая**	**Средняя**	**Возможна**	**Да**	**Плохая**	**Около 50€/год**	**Да**
VPN поверх Tor	**Хорошая-**	**Хорошая**	**Нет**	**Нет**	**Средняя**	**Около 50€/год**	**Если нужно (удобство)**
Собственный VPS VPN/прокси поверх Tor	**Хорошая-**	**Очень хорошая**	**Нет**	**Да**	**Средняя**	**Около 50€/год**	**Если нужно (удобство)**
VPN/прокси поверх Tor поверх VPN	**Хорошая-**	**Хорошая**	**Нет**	**Да**	**Плохая**	**Около 100€/год**	**Если нужно (удобство и Tor недоступен)**
Только VPN/прокси	**Плохая**	**Хорошая**	**Н/Д**	**Да**	**Хорошая**	**Около 50€/год**	**Нет.**
Без Tor и VPN	**Плохая**	**Неизвестно**	**Н/Д**	**Нет**	**Хорошая**	**Около 100€ (антенна)**	**Нет.**

К сожалению, использование одного Tor вызовет подозрение у многих целевых платформ. Если использовать только Tor, вы столкнётесь со множеством препятствий: CAPTCHA, ошибки, трудности регистрации. Кроме того, само использование Tor там, где вы находитесь, может создать вам проблемы. Но Tor всё ещё остаётся лучшим решением для анонимности и должен где-то присутствовать.

- Если вы собираетесь создавать постоянные общие идентичности с входом в аккаунт на разных сервисах, где доступ из Tor затруднён, мы рекомендуем варианты **VPN поверх Tor** и **VPS VPN/прокси поверх Tor** (или VPN поверх Tor поверх VPN, если нужно). Это может быть немного менее безопасно против корреляционных атак из-за нарушения изоляции потоков Tor, но даёт гораздо больше удобства при доступе к онлайн-ресурсам, чем один Tor. Это «приемлемый» компромисс, если вы достаточно осторожны со своей идентичностью.
  - **Примечание: становится всё более обычным, что массовые сервисы и CDN также блокируют или затрудняют жизнь пользователям VPN через CAPTCHA и другие препятствия. В таком случае собственный VPS с VPN/прокси поверх Tor — лучшее решение, потому что выделенный VPS гарантирует, что вы единственный пользователь своего IP и почти не встретите препятствий.** Рассмотрите самостоятельно размещённый VPN/прокси на VPS, оплаченном Monero/наличными (для пользователей, лучше знакомых с Linux), если хотите минимум проблем; это будет подробнее объяснено в следующем разделе.
- Если же ваша цель — просто анонимно просматривать случайные сервисы без создания конкретных общих идентичностей, используя сервисы, дружественные Tor, или если вы не хотите принимать компромисс из предыдущего варианта, **мы рекомендуем маршрут только Tor, чтобы сохранить все преимущества изоляции потоков (или Tor поверх VPN, если нужно).**
- Если проблема в стоимости, по возможности рекомендуем вариант только Tor.
- Если доступ и к Tor, и к VPN невозможен или опасен, у вас нет выбора, кроме как безопасно полагаться на публичный Wi-Fi. См. Что делать, когда Tor и VPN невозможны?

Дополнительные обсуждения, которые помогут решить самостоятельно:

- Tor Project: gitlab.torproject.org Archive.org
- Документация Tails:
  - gitlab.tails.boum.org Archive.org
  - tails.boum.org Archive.org
- Документация Whonix (в этом порядке):
  - whonix.org Archive.org
  - whonix.org Archive.org
  - whonix.org Archive.org
- Некоторые работы по теме:
  - researchgate.net Archive.org

Получение анонимного VPN/прокси

Пропустите этот шаг, если хотите использовать только Tor.

См. Получение анонимного VPN/прокси

Whonix

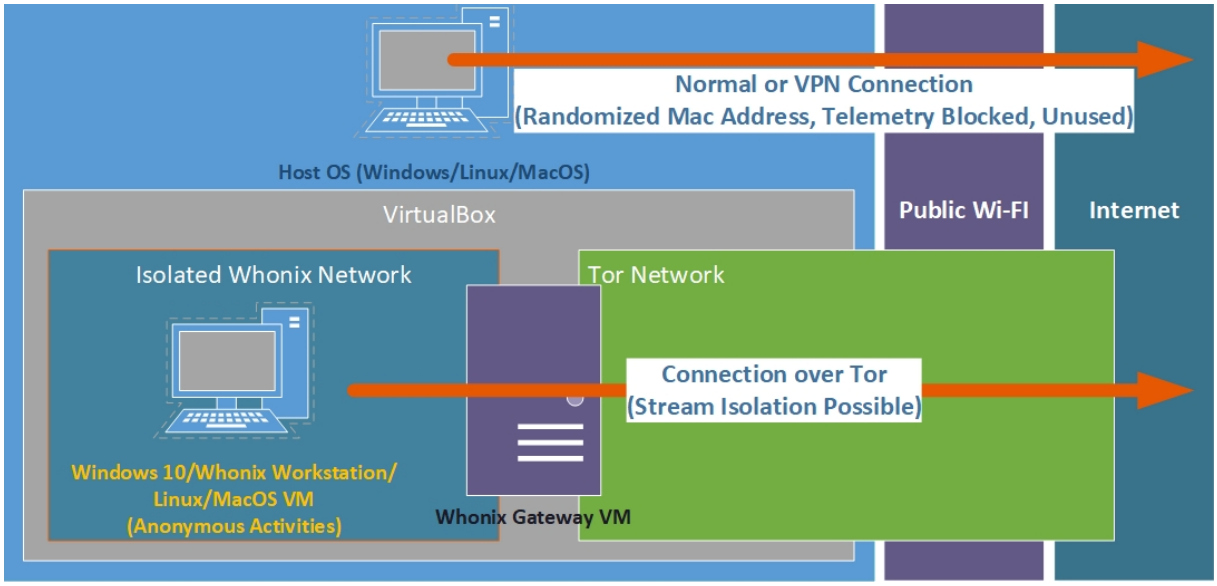
Пропустите этот шаг, если не можете использовать Tor.

Этот маршрут будет использовать виртуализацию и Whonix[63] как часть процесса анонимизации. Whonix — это дистрибутив Linux, состоящий из двух виртуальных машин:

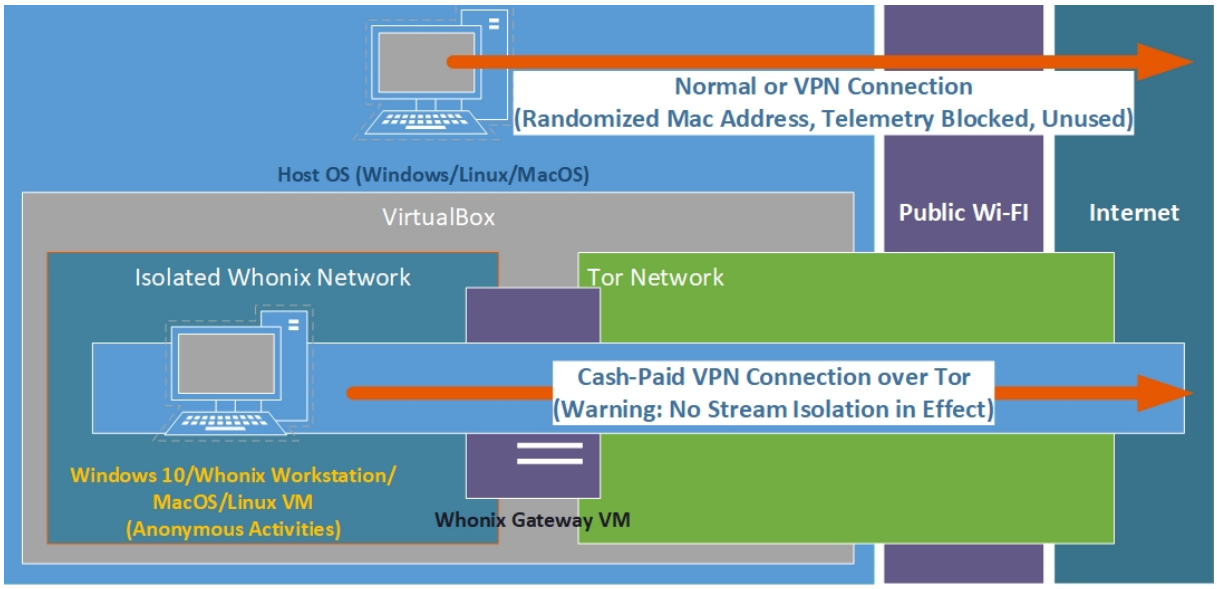
- Whonix Workstation (виртуальная машина, где можно выполнять чувствительные действия)
- Whonix Gateway (эта виртуальная машина устанавливает соединение с сетью Tor и направляет весь сетевой трафик Workstation через сеть Tor).

Поэтому руководство предложит два варианта этого маршрута:

- Маршрут только Whonix, где весь трафик направляется через сеть Tor (только Tor или Tor поверх VPN).



• Гибридный маршрут Whonix, где весь трафик направляется через VPN, оплаченный наличными (предпочтительно) или Monero, поверх сети Tor (VPN поверх Tor или VPN поверх Tor поверх VPN).



Вы сможете решить, какой вариант использовать, на основе моих рекомендаций. Мы рекомендуем второй, как объяснялось выше.

Whonix хорошо поддерживается и имеет обширную, невероятно подробную документацию.

Примечание о снимках Virtualbox

Позже вы создадите и запустите несколько виртуальных машин в Virtualbox для чувствительных действий. Virtualbox предоставляет функцию «Snapshots»[64], которая позволяет сохранить состояние виртуальной машины в любой момент времени. Если позже по какой-либо причине вы захотите вернуться к этому состоянию, снимок можно восстановить в любой момент.

Я настоятельно рекомендую пользоваться этой функцией, создавая снимок после начальной установки/обновления каждой виртуальной машины. Этот снимок следует делать до любого использования виртуальной машины для чувствительной или анонимной активности.

Это позволит превратить виртуальные машины в своего рода одноразовые Live-операционные системы, похожие на Tails, который обсуждался ранее. То есть вы сможете стереть все следы своей активности внутри виртуальной машины, восстановив снимок до более раннего состояния. Разумеется, это не будет «так же хорошо», как Tails, где всё хранится в памяти, потому что следы этой активности могут остаться на жёстком диске. Криминалистические исследования показали возможность восстановления данных из откатанной виртуальной машины[65]. К счастью, после удаления или возврата к раннему снимку будут способы убрать такие следы. Эти техники будут обсуждаться в разделе Дополнительные меры против криминалистики.

Скачать Virtualbox и утилиты Whonix

В основной ОС нужно скачать несколько вещей:

• Последнюю версию установщика Virtualbox для вашей основной ОС: virtualbox.org Archive.org

• (Пропустите, если не можете использовать Tor напрямую или через VPN) последнюю стабильную OVA **Whonix 18.x** из:
  • GitHub Releases Archive.org
  • Или официального зеркала загрузки: download.whonix.org (XFCE Desktop рекомендуется новичкам)

• (Необязательно) Whonix Text Client Archive.org доступен для продвинутых пользователей, предпочитающих минимальную настройку.

Примечание о Whonix 18.x: начиная с версии руководства v1.2.5 Whonix был обновлён с версии 17 до 18 (Whonix 18.1.4.x). См. Обновление до Whonix 18 для пути обновления, если сейчас вы используете Whonix 17.x.

На этом подготовка завершится, и теперь вы должны быть готовы начать настройку финальной среды, которая будет защищать вашу анонимность в интернете.

Усиление Virtualbox (Whonix 17.x и 18.x)

Для идеальной безопасности следуйте руководству Whonix по усилению Archive.org с этими дополнительными примечаниями:

Рекомендуемые настройки (применяются ко всем виртуальным машинам):
• Отключить Audio.
• Не включать Shared Folders.
• Отключить 2D-ускорение: `VBoxManage modifyvm "vm-name" --accelerate2dvideo off`
• Отключить 3D-ускорение.
• Отключить Serial Port.
• Убрать Floppy и CD/DVD drives или сделать их нефункциональными.
• Отключить Remote Display server.
• Включить PAE/NX для функций безопасности.
• Отключить ACPI.

Рассинхронизация сетевого времени:
Рассинхронизируйте часы виртуальных машин, чтобы предотвратить атаки синхронизации (см. Whonix Documentation - Network Time Synchronization Archive.org):

```
# Example offsets (choose different values for each VM)
VBoxManage modifyvm "Whonix-Gateway-XFCE" --biossystemtimeoffset -35017
VBoxManage modifyvm "Whonix-Workstation-XFCE" --biossystemtimeoffset +27931
```

Меры против Spectre/Meltdown: (необязательно, может повлиять на производительность)
Для подробного усиления против Spectre/Meltdown см. whonix.org Archive.org.

Дополнительная безопасность: (Whonix 18.x+)
• Рассмотрите включение AppArmor в Whonix Workstation: whonix.org Archive.org
• Изучите рекомендации DoNot Archive.org

• Отключите USB-контроллер, который включён по умолчанию. Установите Pointing Device в «PS/2 Mouse», иначе изменения будут откатываться.

Наконец, также следуйте этой рекомендации, чтобы рассинхронизировать часы виртуальной машины по сравнению с основной ОС: whonix.org Archive.org

Смещение должно быть в пределах 60000 миллисекунд и должно отличаться для каждой виртуальной машины. Вот несколько примеров, которые позже можно применить к любой виртуальной машине:

• `VBoxManage modifyvm "Whonix-Gateway-XFCE" --biossystemtimeoffset -35017`

• `VBoxManage modifyvm "Whonix-Gateway-XFCE" --biossystemtimeoffset +27931`

• `VBoxManage modifyvm "Whonix-Workstation-XFCE" --biossystemtimeoffset -35017`

• `VBoxManage modifyvm "Whonix-Workstation-XFCE" --biossystemtimeoffset +27931`

Также рассмотрите применение этих мер VirtualBox для смягчения уязвимостей Spectre[66]/Meltdown[67], запустив эту команду из каталога программы VirtualBox. Всё это описано здесь: whonix.org Archive.org (учтите, это может серьёзно повлиять на производительность виртуальных машин, но для лучшей безопасности это следует сделать).

Наконец, рассмотрите советы безопасности от самих Virtualbox здесь: virtualbox.org Archive.org

Tor поверх VPN

Пропустите этот шаг, если вы не собираетесь использовать Tor поверх VPN и хотите использовать только Tor или не можете использовать Tor.

Если по какой-либо причине вы собираетесь использовать Tor поверх VPN, сначала нужно настроить VPN-сервис в основной ОС.

Помните, что в этом случае мы рекомендуем иметь два VPN-аккаунта. Оба должны быть оплачены наличными/Monero (см. Получение анонимного VPN/прокси). Один будет использоваться в основной ОС для первого VPN-соединения. Другой можно использовать в виртуальной машине, чтобы получить VPN поверх Tor поверх VPN (пользователь > VPN > Tor > VPN).

Если вы собираетесь использовать только Tor поверх VPN, нужен только один VPN-аккаунт.

Инструкции см. в Установка VPN на виртуальную машину или основную ОС.

Виртуальные машины Whonix

Пропустите этот шаг, если не можете использовать Tor.

• Запустите Virtualbox в основной ОС.

• Импортируйте Whonix OVA в Virtualbox: см. VirtualBox/XFCE Archive.org
  • Для продвинутых пользователей также можно использовать версию Text Client.

• Запустите виртуальные машины Whonix.

Помните: если на этом этапе у вас проблемы с подключением к Tor из-за цензуры или блокировок, стоит подключиться с помощью мостов, как объяснено в Bridges Archive.org.

• Обновите виртуальные машины Whonix по инструкциям на Operating System Software and Updates Archive.org

Примечание: пользователям Qubes OS следует смотреть раздел Обновление до Whonix 18 с примечаниями по миграции.

• Выключите виртуальные машины Whonix.

• Сделайте снимок обновлённых виртуальных машин Whonix в Virtualbox: выберите виртуальную машину и нажмите кнопку Take Snapshot. Подробнее об этом позже.

• Переходите к следующему шагу.

Важное примечание: также прочитайте эти очень хорошие рекомендации здесь whonix.orgArchive.orgпоскольку большинство этих принципов применимо и к этому руководству. Также прочитайте их общую документацию здесь whonix.orgArchive.org; там тоже есть множество советов, похожих на это руководство.

Улучшения и лучшие практики Whonix 18.x

Ключевые изменения в Whonix 18.x:
• Автоматизированный процесс обновления релизов для плавного перехода с Whonix 17.x.
• Улучшенная интеграция AppArmor для более сильной изоляции приложений в системах на основе Debian.
• Улучшенная конфигурация сети с более хорошими вариантами подключения к Tor.
• Обновлённые руководства по усилению безопасности с современными лучшими практиками.
• Лучшая интеграция и совместимость с Qubes OS.

Лучшие практики для пользователей Whonix 18.x:

1. **Всегда делайте снимок** перед применением любых системных обновлений или изменений конфигурации.
2. **Проверяйте целостность системы** после обновлений с помощью команд `sudo checkvm`.
3. **Регулярно пересматривайте страницу DoNot**, чтобы оставаться в курсе лучших практик безопасности.
4. **Поддерживайте виртуальные машины Whonix обновлёнными**, используя автоматизированный процесс обновления, когда он доступен.
5. **Рассмотрите KVM вместо VirtualBox**.

Для пользователей Qubes OS:
Поддерживается Qubes R4.2+ с Whonix 18. Всегда проверяйте целостность системы после обновления с помощью `systemcheck`. Подробные инструкции по миграции см. в разделе Обновление до Whonix 18.

Выбор гостевой рабочей виртуальной машины

Использование Whonix/Linux потребует от вас больше навыков, поскольку это дистрибутивы Linux. Вы также столкнётесь с большими трудностями, если собираетесь использовать специфическое ПО, с которым сложнее работать в Whonix/Linux. Настройка VPN поверх Tor в Whonix тоже будет сложнее, чем в Windows.

Если вы можете использовать Tor

Можно решить, предпочитаете ли вы выполнять чувствительные действия из Whonix Workstation, предоставленной в предыдущем разделе **(настоятельно рекомендуется)**, или из собственной виртуальной машины, которая будет использовать Whonix Gateway так же, как Whonix Workstation (менее безопасно, но может потребоваться в зависимости от того, что вы собираетесь делать).

Если вы не можете использовать Tor

Если вы не можете использовать Tor, можно использовать собственную виртуальную машину на ваш выбор, которая в идеале будет использовать анонимный VPN, если возможно, чтобы затем подключиться к сети Tor. Или можно выбрать рискованный маршрут: см. Что делать, когда Tor и VPN невозможны?

Виртуальная машина Linux (Whonix или Linux)

Whonix Workstation (рекомендуется и предпочтительно)

Пропустите этот шаг, если не можете использовать Tor.

Просто используйте предоставленную виртуальную машину Whonix Workstation. **Это самый безопасный и защищённый вариант для этого маршрута.**

Это также единственная виртуальная машина, где для большинства приложений по умолчанию заранее настроена изоляция потоков[68].

Если вам нужно дополнительное ПО в Workstation (например, другой браузер), следуйте их руководству здесь: whonix.org Archive.org

Для дополнительной защиты от вредоносного ПО рассмотрите запуск Whonix в режиме Live Mode. См. whonix.org Archive.org

Не забудьте применить рекомендации по усилению виртуальной машины здесь: Virtualbox Hardening recommendations.

Рассмотрите использование AppArmor на ваших Whonix Workstation, следуя этому руководству: whonix.org Archive.org

Linux (любой дистрибутив)

Будьте осторожны: любые настройки, которые вы сделаете в гостевых виртуальных машинах не на Whonix (раскладка клавиатуры, язык, часовой пояс, разрешение экрана и другие), позднее могут использоваться для создания цифрового отпечатка ваших виртуальных машин. См. whonix.org Archive.org

Если вы можете использовать Tor (напрямую или поверх VPN)

Используйте выбранный вами дистрибутив Linux. Для удобства мы рекомендуем Ubuntu или Fedora, но подойдёт и любой другой. Убедитесь, что не включаете телеметрию.

Подробные инструкции см. в этом руководстве: whonix.org Archive.org

Рассмотрите усиление виртуальной машины, как рекомендовано в Hardening Linux.

Если вы не можете использовать Tor

Используйте выбранный вами дистрибутив Linux. Для удобства мы рекомендуем Ubuntu или Fedora, но подойдёт и любой другой. Убедитесь, что не включаете телеметрию. Можно выбрать рискованный маршрут: см. Что делать, когда Tor и VPN невозможны?

Выберите браузер внутри виртуальной машины

В этот раз мы рекомендуем браузер Brave.

Почему именно его, см. здесь: Какой браузер использовать в гостевой/одноразовой виртуальной машине

Также см. Усиление браузеров.

Виртуальная машина Windows 10/11

Будьте осторожны: любые настройки, которые вы сделаете в гостевых виртуальных машинах не на Whonix (раскладка клавиатуры, язык, часовой пояс, разрешение экрана и другие), позднее могут использоваться для создания цифрового отпечатка ваших виртуальных машин. См. whonix.org Archive.org

Скачивание ISO Windows 10 и 11

Используйте официальную виртуальную машину Windows 10/11 Pro и усиливайте её самостоятельно: см. Windows Installation Media Creation и выбирайте вариант с ISO.

Если вы можете использовать Tor (напрямую или поверх VPN)

Подробные инструкции см. в этом руководстве: whonix.org Archive.org

Установка

- Выключите виртуальную машину Whonix Gateway (это не даст Windows отправлять телеметрию и позволит создать локальную учётную запись).
- Откройте Virtualbox.
- Выберите Machine > New > Select Windows 10 or Windows 11 64bit.
- Выделите минимум 2 ГБ для Windows 10 и 4 ГБ для Windows 11.
- Создайте виртуальный диск в формате VDI и выберите Dynamically Allocated.
- Оставьте размер диска 50 ГБ для Windows 10 и 80 ГБ для Windows 11 (это максимум; фактически он не должен столько занять).
- Убедитесь, что PAE/NX включён в System > Processor.
- Выберите виртуальную машину, нажмите Settings и перейдите на вкладку Network.
- Выберите "Internal Network" в поле "Attached to" и выберите Whonix.
- Перейдите на вкладку Storage, выберите пустой CD и нажмите значок рядом с SATA Port 1.
- Нажмите "Choose a disk file" и выберите ранее скачанный ISO Windows.
- Нажмите OK и запустите виртуальную машину.
- Virtualbox предложит нажать кнопку для загрузки с ISO или спросит, с чего загружаться; выберите ISO или нажмите кнопку.
- Следуйте шагам из Windows Installation.
- Запустите виртуальную машину Whonix Gateway.

Сетевые настройки

- Вернитесь в Windows.
- Windows 10: снова откройте Settings, затем Network & Internet. Windows 11: откройте Settings, нажмите верхнее левое меню и выберите "Network and Internet".
- Windows 10: нажмите Properties (под Ethernet). Windows 11: нажмите Ethernet.
- Windows 10: Edit IP settings. Windows 11: Edit IP assignment.
- Windows 10: включите IPv4 и задайте следующее; Windows 11: переключитесь с DHCP на Manual и задайте следующее:
  - IP address `10.152.152.50` (увеличивайте этот IP на единицу для каждой следующей виртуальной машины)
  - Subnet prefix length `18` (`255.255.192.0`)
  - Gateway `10.152.152.10` (это Whonix Gateway)
  - (Windows 10) DNS `10.152.152.10` (это снова Whonix Gateway)

    - (Windows 11) выйдите из IP assignment, выберите DNS server assignment и задайте `10.152.152.10` (это снова Whonix Gateway)
    - Save
- Windows может спросить, хотите ли вы быть "discoverable" в этой сети. Нажмите NO. Если появится запрос, всегда оставайтесь в "public network".

Каждый раз, когда вы в будущем будете включать эту виртуальную машину, перед каждой загрузкой нужно менять её Ethernet MAC Address. Это можно сделать в Virtualbox > Settings > Network > Advanced > нажать кнопку обновления рядом с MAC address. Это можно сделать только когда виртуальная машина выключена.

Если вы не можете использовать Tor

См. Что делать, когда Tor и VPN невозможны?

Установка

- Откройте Virtualbox.
- Выберите Machine > New > Select Windows 10 or 11 64bit.
- Выделите минимум 4 ГБ ОЗУ для Windows 11 и 2 ГБ ОЗУ для Windows 10.
- Создайте виртуальный диск в формате VDI и выберите Dynamically Allocated.
- На вкладке System/Processor убедитесь, что PAE/NX включён.
- Оставьте размер диска 80 ГБ для Windows 11 и 50 ГБ для Windows 10 (это максимум; фактически он не должен столько занять).
- Перейдите на вкладку Storage, выберите пустой CD и нажмите значок рядом с SATA Port 1.
- Нажмите "Choose a disk file" и выберите ранее скачанный ISO Windows.
- Нажмите OK и запустите виртуальную машину.
- Virtualbox предложит нажать кнопку для загрузки с ISO или спросит, с чего загружаться; выберите ISO или нажмите кнопку.
- Следуйте шагам из Windows Installation.

Сетевые настройки

• Windows спросит, хотите ли вы быть обнаруживаемым в этой сети. Нажмите NO.

Каждый раз, когда вы в будущем будете включать эту виртуальную машину, перед каждой загрузкой нужно менять её Ethernet MAC Address. Это можно сделать в Virtualbox > Settings > Network > Advanced > нажать кнопку обновления рядом с MAC address. Это можно сделать только когда виртуальная машина выключена.

Выберите браузер внутри виртуальной машины

В этот раз мы рекомендуем браузер Brave.

Почему именно его, см. здесь: Какой браузер использовать в гостевой/одноразовой виртуальной машине

Также см. Усиление браузеров.

Дополнительные настройки приватности в Windows 10/11

См. Windows Additional Privacy Settings

Виртуальная машина Android

Потому что иногда нужно анонимно запускать и мобильные приложения. Для этой цели можно настроить виртуальную машину Android. Как и в других случаях, в идеале эта виртуальная машина тоже будет находиться за Whonix Gateway для подключения к сети Tor. Но её также можно настроить как VPN поверх Tor поверх VPN.

Если вы можете использовать Tor (напрямую или поверх VPN)

Позднее, во время создания виртуальной машины, перейдите в сетевые настройки и выберите Internal Network, Whonix.

Затем в самом Android:

• Выберите Wi-Fi.

• Выберите VirtWifi для подключения.

• Перейдите в расширенные свойства Wi-Fi.

• Переключитесь с DHCP на Static.

  • IP address `10.152.152.50` (увеличивайте этот IP на единицу для каждой следующей виртуальной машины)

  • Subnet prefix length `18` (`255.255.192.0`)

  • Gateway `10.152.152.10` (это Whonix Gateway)

- DNS `10.152.152.10` (это снова Whonix Gateway)

Если вы не можете использовать Tor

Просто используйте руководства как есть и см. Что делать, когда Tor и VPN невозможны?

Установка

Две возможности: AnBox или Android-x86.

Лично мы рекомендуем AnBox вместо Android-x86, но для него нужен Linux.

AnBox

В целом следуйте руководству по установке AnBox на Whonix Workstation здесь: whonix.org Archive.org, чтобы запускать Android-приложения внутри виртуальной машины AnBox.

Или следуйте инструкциям здесь: anbox.io, чтобы установить его на любую другую виртуальную машину **(только Linux)**.

Android-x86

В целом следуйте этому руководству: android-x86.org Archive.org

- Скачайте ISO-файл по своему выбору.
- Создайте новую виртуальную машину.
- Выберите Linux и Linux 2.6 / 3.x / 4.x 64 Bit.
- В System:
  - Выделите не меньше 2048 МБ (2 ГБ) памяти.
  - Снимите флажок Floppy drive.
  - На вкладке Processor выберите как минимум 1 ЦП или больше.
  - Включите PAE/NX.
- В Display Settings измените адаптер на VBoxVGA.
- В Audio Settings измените на Intel HD Audio.
- Запустите виртуальную машину.
- Выберите Advanced, если нужна сохраняемость, или Live, если нужна одноразовая загрузка (и пропустите следующие шаги).
- Выберите Auto Install on Selected Hard Disk.
- Выберите Run Android.

• Настройте как хотите (отключите все запросы на сбор данных). **Я рекомендую использовать TaskBar Home.**

• Перейдите в Settings, Android-x86 Options и отключите весь сбор данных.

• Подключитесь к сети Wi-Fi VirtWifi **(см. раздел выше, если вы находитесь за Whonix и хотите использовать Tor)**.

Теперь всё готово, и вы можете установить любое приложение Android.

Виртуальная машина macOS

Да, при желании вы действительно можете запускать macOS внутри Virtualbox (на основных системах Windows/Linux/macOS). Можно запускать любую нужную версию macOS.

Если вы можете использовать Tor (напрямую или поверх VPN)

Во время следующих руководств, перед запуском виртуальной машины macOS, убедитесь, что поместили виртуальные машины macOS в сеть Whonix.

• Выберите виртуальную машину, нажмите Settings и перейдите на вкладку Network.

• Выберите "Internal Network" в поле "Attached to" и выберите Whonix.

После этого, во время установки, нужно будет вручную ввести IP-адрес для подключения через Whonix Gateway.

Используйте эти настройки, когда появится запрос в процессе установки macOS:

• IP address `10.152.152.50` (увеличивайте этот IP на единицу для каждой следующей виртуальной машины)

• Subnet prefix length `18` (`255.255.192.0`)

• Gateway `10.152.152.10` (это Whonix Gateway)

• DNS `10.152.152.10` (это снова Whonix Gateway)

Если вы не можете использовать Tor

Просто используйте руководства как есть и см. Что делать, когда Tor и VPN невозможны?

Установка

- Основная ОС Windows:
  - Руководство Virtualbox Catalina: wikigain.com Archive.org
  - Руководство Virtualbox Big Sur: wikigain.com Archive.org
  - Руководство Virtualbox Monterey: wikigain.com Archive.org
- Основная ОС macOS:
  - Просто используйте те же руководства, что выше, но выполняйте разные команды в терминале. Это должно работать без проблем.
- Основная ОС Linux:
  - Просто используйте те же руководства, что выше, но выполняйте разные команды в терминале. Это должно работать без проблем.

У запуска macOS в виртуальных машинах есть некоторые недостатки. Главный из них: у них нет серийного номера (по умолчанию 0), и вы не сможете войти ни в один сервис Apple (iCloud, iMessage...) без подлинного идентификатора. Такие идентификаторы можно задать с помощью этого скрипта: github.com Archive.org, но помните, что случайно созданные идентификаторы работать не будут, а использование чужого идентификатора нарушит их Условия обслуживания и может считаться выдачей себя за другого человека (и, следовательно, может быть незаконным).

Примечание: у нас также возникало несколько проблем с запуском этих систем на процессорах AMD. Это можно исправить; ниже конфигурация, которую мы использовали и которая нормально работала с Catalina, Big Sur и Monterey. Она заставляет Virtualbox имитировать процессор Intel:

- `VBoxManage modifyvm "macOSCatalina" ---cpuidset 00000001 000106e5 00100800 0098e3fd bfebfbff`
- `VBoxManage setextradata "macOSCatalina" "VBoxInternal/Devices/efi/0/Config/DmiSystemProduct" "MacBookPro15,1"`
- `VBoxManage setextradata "macOSCatalina" "VBoxInternal/Devices/efi/0/Config/DmiBoardProduct" "Mac-551B86E5744E2388"`
- `VBoxManage setextradata "macOSCatalina" "VBoxInternal/Devices/smc/0/Config/DeviceKey" "ourhardworkbythesewordsguardedpleasedontsteal(c)AppleComputerInc"`
- `VBoxManage setextradata "macOSCatalina" "VBoxInternal/Devices/smc/0/Config/GetKeyFromRealSMC" 1`
- `VBoxManage modifyvm "macOSCatalina" --cpu-profile "Intel Core i7-6700K"`
- `VBoxManage setextradata "macOSCatalina" VBoxInternal2/EfiGraphicsResolution 1920x1080`

Усиление macOS

См. Hardening macOS.

Выберите браузер внутри виртуальной машины

В этот раз мы рекомендуем браузер Brave.

Почему именно его, см. здесь: Какой браузер использовать в гостевой/одноразовой виртуальной машине

Также см. Усиление браузеров.

KeepassXC

Вам понадобится что-то для хранения ваших данных (логинов/паролей, личностей и данных TOTP[69]).

Для этой цели мы настоятельно рекомендуем KeePassXC из-за встроенной функции TOTP. Это возможность создавать записи для аутентификации 2FA[70] с помощью функции аутентификатора.

Помните: в идеале это должно быть установлено в гостевой виртуальной машине, а не в основной ОС. Никогда не выполняйте чувствительные действия из основной ОС.

Руководства:

• Tails: KeePassXC встроен по умолчанию.

• Whonix: whonix.org Archive.org

• Linux:

  • Скачать с keepassxc.org Archive.org

  • Следуйте руководству здесь: keepassxc.org Archive.org

• Windows:

  • Скачать с keepassxc.org Archive.org

  • Следуйте руководству здесь: keepassxc.org Archive.org

• macOS:

  • Скачать с keepassxc.org Archive.org

  • Следуйте руководству здесь: keepassxc.org Archive.org

Проверьте, что KeePassXC работает, прежде чем переходить к следующему шагу.

Установка VPN-клиента (оплата наличными/Monero)

Если вы решили не использовать VPN, оплаченный наличными, и хотите использовать только Tor, пропустите этот шаг.

Если во враждебной среде вы вообще не можете использовать VPN, пропустите этот шаг.

В остальных случаях см. Установка VPN на виртуальную машину или основную ОС, чтобы установить VPN-клиент в клиентскую виртуальную машину.

На этом маршрут должен завершиться, и теперь вы должны быть готовы.

О сборе данных и утечках VPN-клиентов

Возможно, вы спрашиваете себя, можно ли доверять таким VPN-клиентам и не утекут ли через них сведения о вашей локальной среде VPN-провайдеру при использовании в схеме "VPN поверх Tor".

Это обоснованное опасение, но его стоит воспринимать с долей осторожности.

Помните, что вся VPN-активность происходит из изолированной виртуальной машины во внутренней сети за сетевым шлюзом (Whonix Gateway). Не так важно, если VPN-клиент оставит какие-то идентификаторы в вашей гостевой виртуальной машине. Гостевая виртуальная машина всё равно изолирована и отделена от основной ОС. Поверхность атаки мала, особенно при использовании авторитетных и рекомендуемых VPN-провайдеров из руководств (iVPN, Mullvad, Proton VPN и, возможно, Safing.io).

В лучшем случае VPN-клиент узнает ваш локальный IP (внутренний IP) и некоторые случайно созданные идентификаторы, но не должен суметь получить что-либо из основной ОС. И теоретически VPN-клиент не должен отправлять телеметрию VPN-провайдеру. Если ваш VPN-клиент делает это или просит разрешение на это, стоит подумать о смене провайдера.

(Необязательно) Аварийное отключение сети для виртуальных машин

Этот шаг позволит настроить основную ОС так, чтобы доступ в интернет был только у виртуальной машины Whonix Gateway. Тем самым он предотвратит любые "утечки" из основной ОС, при этом позволив Whonix Gateway установить подключение к Tor. Другие виртуальные машины (Whonix Workstation или любые другие, установленные за ним) не будут затронуты.

Есть три способа сделать это:

- Ленивый способ (не особо рекомендуется): не поддерживается Whonix и может иметь последствия для безопасности, потому что вы выставите виртуальную машину Whonix Gateway в публичную сеть Wi-Fi. Мы не рекомендуем это, если только вы не спешите или не готовы мириться с худшим вариантом.
  - **Этот способ не будет работать с Wi-Fi-сетями, где для подключения нужен портал авторизации или регистрация.**
- Лучший способ (см. ниже): также не поддерживается Whonix, но он не выставляет виртуальную машину Whonix Gateway в публичную сеть Wi-Fi. С точки зрения безопасности это должно держать ситуацию под контролем.

• Наилучший способ: использовать внешний USB-адаптер Wi-Fi и просто отключить Wi-Fi в основной ОС/на компьютере.

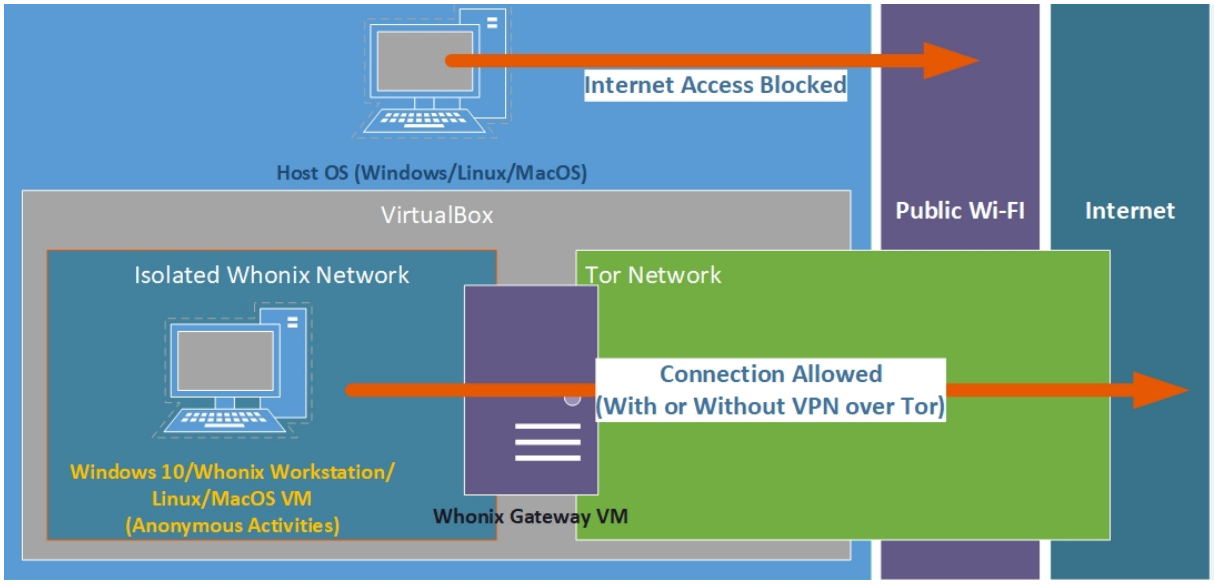
Ленивый способ

> Не поддерживается Whonix

Этот способ не поддерживается проектом Whonix[71], но я всё равно приведу этот вариант. Он помогает не дать основной ОС утечь какими-либо сведениями, пока вы используете виртуальные машины Whonix.

Учтите, что в таком виде этот вариант будет работать только в Wi-Fi-сетях без портала авторизации (где не нужно вводить какие-либо сведения для разблокировки доступа).

На иллюстрации ниже показан результат этого шага:



Конфигурация виртуальной машины Whonix Gateway

Чтобы это работало, нужно изменить некоторые настройки виртуальной машины Whonix Gateway. Нам нужно добавить DHCP-клиент в Whonix Gateway, чтобы получать IP-адреса от сети. Для этих изменений у основной ОС пока всё ещё должен быть разрешён доступ в интернет.

Вот как это сделать:

• Убедитесь, что основная ОС подключена к безопасной Wi-Fi-сети.

• Через VirtualBox запустите виртуальную машину Whonix Gateway.

• Запустите терминал в виртуальной машине.

• Установите DHCP-клиент в виртуальную машину Whonix Gateway с помощью следующей команды:

  • `sudo apt install dhcpcd5`

- Теперь измените сетевую конфигурацию виртуальной машины Whonix Gateway с помощью следующей команды:
  - `sudo nano /etc/network/interfaces.d/30_non-qubes-whonix`
- Внутри файла измените следующие строки:
  - `# auto eth0` на `auto eth0`
  - `# iface eth0 inet dhcp` на `iface eth0 inet dhcp`
  - `iface eth0 inet static` на `# iface eth0 inet static`
  - `address 10.0.2.15` на `# address 10.0.2.15`
  - `netmask 255.255.255.0` на `# netmask 255.255.255.0`
  - `gateway 10.0.2.2` на `# gateway 10.0.2.2`
- Сохраните (Ctrl+X и подтвердите Y) и выключите виртуальную машину через меню в левом верхнем углу.
- Откройте приложение VirtualBox и выберите виртуальную машину Whonix Gateway.
- Нажмите Settings.
- Перейдите на вкладку Network.
- Для Adapter 1 измените значение "Attached To" с "NAT" на "Bridged Adapter".
- В поле "Name" выберите ваш сетевой адаптер Wi-Fi.
- Нажмите OK; часть настройки виртуальной машины завершена.

Конфигурация основной ОС

Теперь нужно заблокировать доступ основной ОС в интернет, при этом позволив виртуальной машине подключаться. Это делается подключением основной ОС к Wi-Fi без назначения ей IP-адреса. Виртуальная машина затем использует вашу связь с Wi-Fi, чтобы получить IP-адрес.

Основная ОС Windows

Цель здесь — подключиться к Wi-Fi-сети без интернет-соединения. Для этого после подключения нужно удалить шлюз из соединения:

- Сначала подключитесь к выбранной безопасной Wi-Fi-сети.
- Откройте командную строку с правами администратора (правый щелчок по Command Prompt и Run as Administrator).
- Выполните команду: `route delete 0.0.0.0` (она удаляет шлюз из вашей IP-конфигурации).
- Готово: основная ОС теперь не сможет выходить в интернет, оставаясь подключённой к Wi-Fi.
  - Учтите, что это сбрасывается при каждом отключении/повторном подключении к сети, и маршрут придётся удалять снова. Это не постоянная настройка.
- Теперь можно запустить виртуальную машину Whonix Gateway, которая должна автоматически получить IP от Wi-Fi-сети и предоставить сеть другим виртуальным машинам за ней (Whonix Workstation или другим).

• Наконец, после этого можно запустить виртуальную машину Whonix Workstation (или любую другую виртуальную машину, которую вы настроили за Whonix Gateway), и она должна подключиться к интернету через Tor.

Основная ОС Linux

Цель здесь — подключиться к Wi-Fi-сети без интернет-соединения. Для этого после подключения нужно удалить шлюз из соединения:

• Сначала подключитесь к выбранной безопасной Wi-Fi-сети.

• Откройте терминал.

• Выполните команду: `sudo ip route del default` (она удаляет шлюз из вашей IP-конфигурации).

• Готово: основная ОС теперь не сможет выходить в интернет, оставаясь подключённой к Wi-Fi.

  • Учтите, что это сбрасывается при каждом отключении/повторном подключении к сети, и маршрут придётся удалять снова. Это не постоянная настройка.

• Теперь можно запустить виртуальную машину Whonix Gateway, которая должна автоматически получить IP от Wi-Fi-сети и предоставить сеть другим виртуальным машинам за ней (Whonix Workstation или другим).

• Наконец, после этого можно запустить виртуальную машину Whonix Workstation (или любую другую виртуальную машину, которую вы настроили за Whonix Gateway), и она должна подключиться к интернету через Tor.

Основная ОС macOS

Цель здесь — подключиться к Wi-Fi-сети без интернет-соединения. Для этого после подключения нужно удалить шлюз из соединения:

• Сначала подключитесь к выбранной безопасной Wi-Fi-сети.

• Откройте терминал.

• Выполните команду: `sudo route delete default` (она удаляет шлюз из вашей IP-конфигурации).

• Готово: основная ОС теперь не сможет выходить в интернет, оставаясь подключённой к Wi-Fi.

  • Учтите, что это сбрасывается при каждом отключении/повторном подключении к сети, и маршрут придётся удалять снова. Это не постоянная настройка.

• Теперь можно запустить виртуальную машину Whonix Gateway, которая должна автоматически получить IP от Wi-Fi-сети и предоставить сеть другим виртуальным машинам за ней (Whonix Workstation или другим).

• Наконец, после этого можно запустить виртуальную машину Whonix Workstation (или любую другую виртуальную машину, которую вы настроили за Whonix Gateway), и она должна подключиться к интернету через Tor.

Лучший способ (рекомендуется)

Этот способ не противоречит рекомендациям Whonix (поскольку не выставляет Whonix Gateway в сеть основной ОС) и имеет преимущество: он позволяет подключаться не только к открытым Wi-Fi-сетям, но и к сетям с порталом авторизации, где нужно ввести сведения для доступа в интернет.

При этом проект Whonix всё равно не поддерживает такой вариант, но это нормально: главная проблема более раннего ленивого способа в том, что Whonix Gateway выставляется в сеть основной ОС, а здесь этого не происходит.

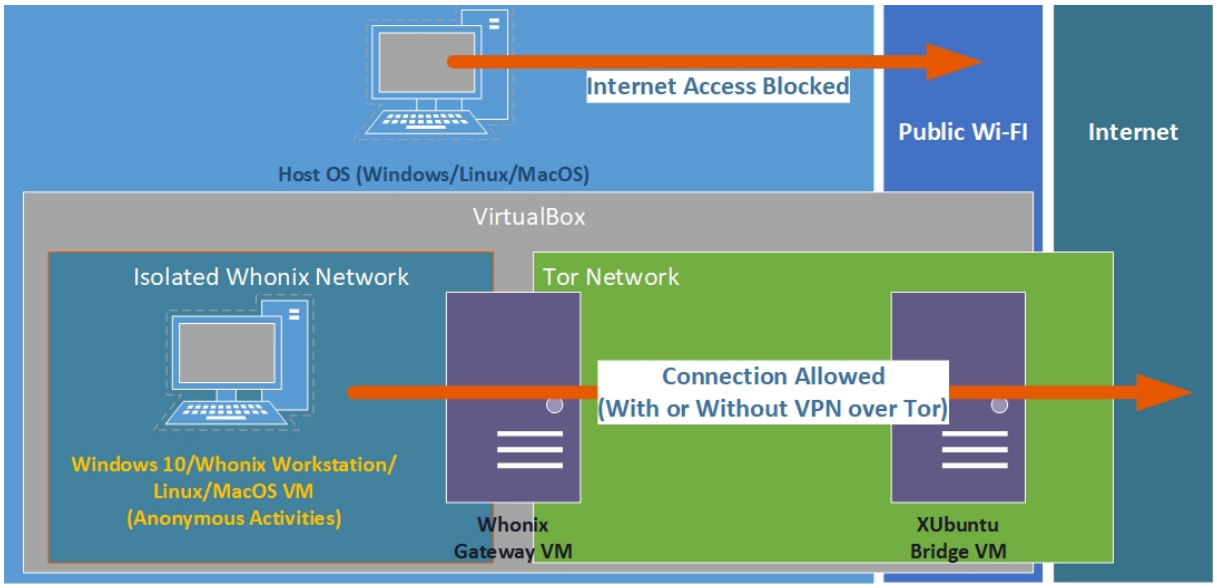
Для этого варианта понадобится дополнительная виртуальная машина между основной ОС и Whonix Gateway, которая будет работать как сетевой мост.

Для этой цели я рекомендую использовать лёгкий дистрибутив Linux. Подойдёт любой, но проще всего будет дистрибутив на основе Ubuntu; я рекомендую лёгкий XUbuntu, потому что такую схему на нём настроить очень просто.

Почему XUbuntu, а не Ubuntu или KUbuntu? Потому что XUbuntu использует лёгкую среду рабочего стола XFCE, а эта виртуальная машина будет служить только посредником и ничем больше.

Конечно, можно сделать то же самое с любым другим дистрибутивом Linux, если вы решите, что XUbuntu вам не нравится.

Итоговая схема будет выглядеть так:



Установка виртуальной машины XUbuntu

XUbuntu выбран из-за производительности XFCE.

Убедитесь, что для этой операции вы подключены к безопасной Wi-Fi-сети.

Сначала нужно скачать последний стабильный ISO-выпуск XUbuntu с xubuntu.org

Когда скачивание завершено, пора создать новую виртуальную машину:

• Запустите VirtualBox Manager.

• Создайте новую виртуальную машину и назовите её как хотите, например "XUbuntu Bridge".

• Выберите тип "Linux".

• Выберите версию "Ubuntu (64-bit)".

• Оставьте остальные параметры по умолчанию и нажмите Create.

• На следующем экране оставьте параметры по умолчанию и нажмите Create.

• Выберите новую виртуальную машину и нажмите Settings.

• Выберите Network.

• Для Adapter 1 переключитесь в Bridged Mode и выберите ваш Wi-Fi-адаптер в поле Name.

• Выберите Adapter 2 и включите его.

• Подключите его к "Internal Network" и назовите "XUbuntu Bridge".

• Выберите Storage.

• Выберите пустой CD-дисковод.

• Справа нажмите значок CD и выберите "Choose a disk file".

• Выберите ранее скачанный ISO XUbuntu и нажмите OK.

• Запустите виртуальную машину.

• Выберите Start XUbuntu.

• Выберите Install XUbuntu.

• Выберите раскладку клавиатуры и нажмите Continue.

• Выберите Minimal Installation и Download Updates while installing XUbuntu.

• Выберите Erase Disk and install XUbuntu и нажмите Install Now.

• Выберите нужный часовой пояс и нажмите Continue.

• Выберите случайные имена, не связанные с вами (моё любимое имя пользователя — "NoSuchAccount").

• Выберите пароль и потребуйте пароль для входа.

• Нажмите Continue и дождитесь завершения установки и перезагрузки.

• После перезагрузки войдите в систему.

• Нажмите значок подключения в правом верхнем углу (он выглядит как две вращающиеся сферы).

• Нажмите Edit Connections.

• Выберите Wired Connection 2 (Adapter 2, ранее настроенный в параметрах VirtualBox).

• Выберите вкладку IPv4.

• Измените Method на "Shared to other computers" и нажмите Save.

• Настройка виртуальной машины XUbuntu Bridge завершена.

Конфигурация виртуальной машины Whonix Gateway

По умолчанию в Whonix Gateway нет DHCP-клиента, а он понадобится, чтобы получить IP из общей сети, которую вы настроили ранее:

• Через VirtualBox запустите виртуальную машину Whonix Gateway.

• Запустите терминал в виртуальной машине.

• Установите DHCP-клиент в виртуальную машину Whonix Gateway с помощью следующей команды:

  • `sudo apt install dhcpcd5`

• Теперь измените сетевую конфигурацию виртуальной машины Whonix Gateway с помощью следующей команды:

  • `sudo nano /etc/network/interfaces.d/30_non-qubes-whonix`

• Внутри файла измените следующие строки:

  • `# auto eth0` на `auto eth0`

  • `# iface eth0 inet dhcp` на `iface eth0 inet dhcp`

  • `iface eth0 inet static` на `# iface eth0 inet static`

  • `address 10.0.2.15` на `# address 10.0.2.15`

  • `netmask 255.255.255.0` на `# netmask 255.255.255.0`

  • `gateway 10.0.2.2` на `# gateway 10.0.2.2`

• Сохраните (Ctrl+X и подтвердите Y) и выключите виртуальную машину через меню в левом верхнем углу.

• Откройте приложение VirtualBox и выберите виртуальную машину Whonix Gateway.

• Нажмите Settings.

• Перейдите на вкладку Network.

• Для Adapter 1 измените значение "Attached To" с "NAT" на "Internal Network".

• В поле "Name" выберите внутреннюю сеть "XUbuntu Bridge", которую создали ранее, и нажмите OK.

• Перезагрузите виртуальную машину Whonix Gateway.

• В меню слева сверху выберите System, Tor Control Panel и проверьте, что подключение установлено (так и должно быть).

• Конфигурация виртуальной машины Whonix Gateway завершена.

Конфигурация основной ОС

Теперь нужно заблокировать доступ основной ОС в интернет, при этом позволив виртуальной машине XUbuntu Bridge подключаться. Это делается подключением основной ОС к Wi-Fi без назначения ей адреса шлюза. Виртуальная машина затем использует вашу связь с Wi-Fi, чтобы получить IP-адрес.

При необходимости из виртуальной машины XUbuntu Bridge вы сможете запустить браузер и ввести данные в портал авторизации/регистрации Wi-Fi-сети.

Только виртуальная машина XUbuntu Bridge должна иметь доступ в интернет. Основная ОС будет ограничена только локальным трафиком.

Основная ОС Windows

Цель здесь — подключиться к Wi-Fi-сети без интернет-соединения. Для этого после подключения нужно удалить шлюз из соединения:

- Сначала подключитесь к выбранной безопасной Wi-Fi-сети.
- Откройте командную строку с правами администратора (правый щелчок по Command Prompt и Run as Administrator).
- Выполните команду: `route delete 0.0.0.0` (она удаляет шлюз из вашей IP-конфигурации).
- Готово: основная ОС теперь не сможет выходить в интернет, оставаясь подключённой к Wi-Fi.
    - Учтите, что это сбрасывается при каждом отключении/повторном подключении к сети, и маршрут придётся удалять снова. Это не постоянная настройка.
- Теперь можно запустить виртуальную машину XUbuntu Bridge, которая должна автоматически получить IP от Wi-Fi-сети и предоставить сеть другим виртуальным машинам за ней (Whonix Workstation или другим).
- При необходимости можно использовать браузер в виртуальной машине XUbuntu Bridge, чтобы заполнить любые сведения на портале авторизации/регистрации для доступа к Wi-Fi.
- После этого можно запустить виртуальную машину Whonix Gateway, которая должна получить интернет-соединение от виртуальной машины XUbuntu Bridge.
- Наконец, после этого можно запустить виртуальную машину Whonix Workstation (или любую другую виртуальную машину, которую вы настроили за Whonix Gateway), и она должна подключиться к интернету через Tor.

Основная ОС Linux

Цель здесь — подключиться к Wi-Fi-сети без интернет-соединения. Для этого после подключения нужно удалить шлюз из соединения:

- Сначала подключитесь к выбранной безопасной Wi-Fi-сети.
- Откройте терминал.
- Выполните команду: `sudo ip route del default` (она удаляет шлюз из вашей IP-конфигурации).
- Готово: основная ОС теперь не сможет выходить в интернет, оставаясь подключённой к Wi-Fi.
    - Учтите, что это сбрасывается при каждом отключении/повторном подключении к сети, и маршрут придётся удалять снова. Это не постоянная настройка.
- Теперь можно запустить виртуальную машину XUbuntu Bridge, которая должна автоматически получить IP от Wi-Fi-сети и предоставить сеть другим виртуальным машинам за ней (Whonix Workstation или другим).
- При необходимости можно использовать браузер в виртуальной машине XUbuntu Bridge, чтобы заполнить любые сведения на портале авторизации/регистрации для доступа к Wi-Fi.
- После этого можно запустить виртуальную машину Whonix Gateway, которая должна получить интернет-соединение от виртуальной машины XUbuntu Bridge.
- Наконец, после этого можно запустить виртуальную машину Whonix Workstation (или любую другую виртуальную машину, которую вы настроили за Whonix Gateway), и она должна подключиться к интернету через Tor.

Основная ОС macOS

Цель здесь — подключиться к Wi-Fi-сети без интернет-соединения. Для этого после подключения нужно удалить шлюз из соединения:

- Сначала подключитесь к выбранной безопасной Wi-Fi-сети.
- Откройте терминал.
- Выполните команду: `sudo route delete default` (она удаляет шлюз из вашей IP-конфигурации).
- Готово: основная ОС теперь не сможет выходить в интернет, оставаясь подключённой к Wi-Fi.
    - Учтите, что это сбрасывается при каждом отключении/повторном подключении к сети, и маршрут придётся удалять снова. Это не постоянная настройка.
- Теперь можно запустить виртуальную машину XUbuntu Bridge, которая должна автоматически получить IP от Wi-Fi-сети и предоставить сеть другим виртуальным машинам за ней (Whonix Workstation или другим).
- При необходимости можно использовать браузер в виртуальной машине XUbuntu Bridge, чтобы заполнить любые сведения на портале авторизации/регистрации для доступа к Wi-Fi.
- После этого можно запустить виртуальную машину Whonix Gateway, которая должна получить интернет-соединение от виртуальной машины XUbuntu Bridge.
- Наконец, после этого можно запустить виртуальную машину Whonix Workstation (или любую другую виртуальную машину, которую вы настроили за Whonix Gateway), и она должна подключиться к интернету через Tor.

Наилучший способ

Этот способ не противоречит рекомендациям Whonix (поскольку не выставляет Whonix Gateway в сеть основной ОС) и имеет преимущество: он позволяет подключаться не только к открытым Wi-Fi-сетям, но и к сетям с порталом авторизации, где нужно ввести сведения для доступа в интернет. При этом проект Whonix всё равно не поддерживает такой вариант, но это нормально: главная проблема более раннего ленивого способа в том, что Whonix Gateway выставляется в сеть основной ОС, а здесь этого не происходит. Этот вариант лучший, потому что сеть на основной ОС будет полностью отключена с момента загрузки.

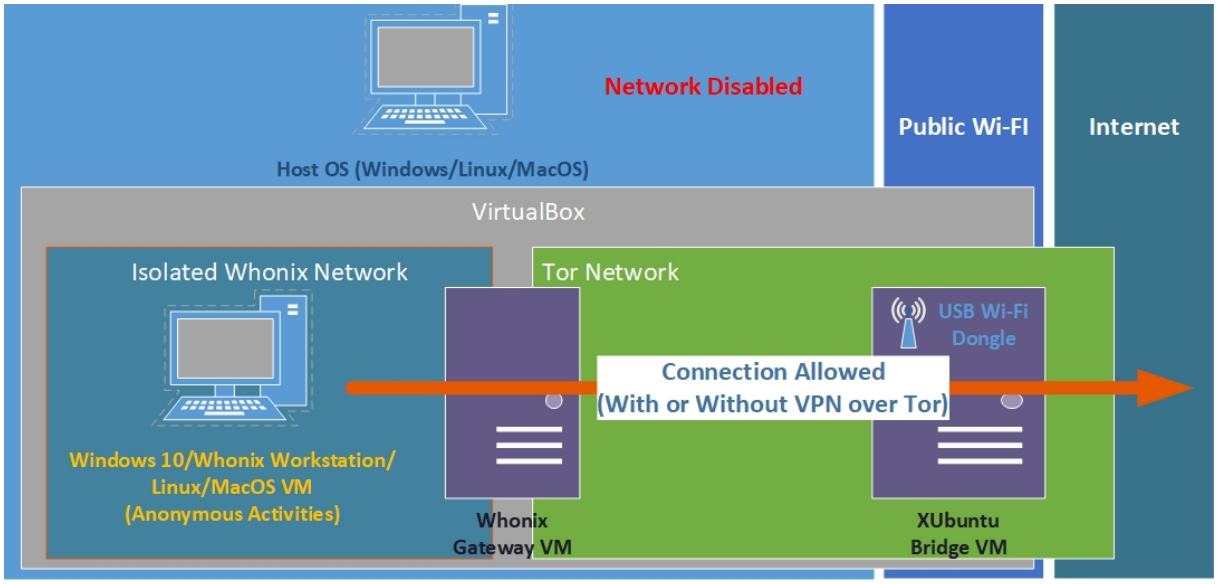
Для этого варианта понадобится дополнительная виртуальная машина между основной ОС и Whonix Gateway, которая будет работать как сетевой мост и подключаться к Wi-Fi-сети. **Для этого варианта нужен рабочий USB-адаптер Wi-Fi, который будет передан в мостовую виртуальную машину.**

Для этой цели я рекомендую использовать лёгкий дистрибутив Linux. Подойдёт любой, но проще всего будет дистрибутив на основе Ubuntu; я рекомендую лёгкий XUbuntu, потому что такую схему на нём настроить очень просто.

Почему XUbuntu, а не Ubuntu или KUbuntu? Потому что XUbuntu использует лёгкую среду рабочего стола XFCE, а эта виртуальная машина будет служить только посредником и ничем больше.

Конечно, можно сделать то же самое с любым другим дистрибутивом Linux, если вы решите, что XUbuntu вам не нравится.

Итоговая схема будет выглядеть так:



Конфигурация основной ОС

- Полностью отключите сеть в основной ОС (полностью выключите встроенный Wi-Fi).
- Подключите и установите USB-адаптер Wi-Fi. Подключите его к безопасной публичной Wi-Fi-сети. Это должно быть просто и должно установиться автоматически в любой современной ОС (Windows 10/11, macOS, Linux).

Конфигурация виртуальной машины Whonix Gateway

По умолчанию в Whonix Gateway нет DHCP-клиента, а он понадобится, чтобы получить IP из общей сети, которую вы позже настроите в мостовой виртуальной машине:

- Через VirtualBox запустите виртуальную машину Whonix Gateway.
- Запустите терминал в виртуальной машине.
- Установите DHCP-клиент в виртуальную машину Whonix Gateway с помощью следующей команды:
  - `sudo apt install dhcpcd5`
- Теперь измените сетевую конфигурацию виртуальной машины Whonix Gateway с помощью следующей команды:
  - `sudo nano /etc/network/interfaces.d/30_non-qubes-whonix`
- Внутри файла измените следующие строки:
  - `# auto eth0` на `auto eth0`
  - `# iface eth0 inet dhcp` на `iface eth0 inet dhcp`
  - `iface eth0 inet static` на `# iface eth0 inet static`
  - `address 10.0.2.15` на `# address 10.0.2.15`
  - `netmask 255.255.255.0` на `# netmask 255.255.255.0`
  - `gateway 10.0.2.2` на `# gateway 10.0.2.2`
- Сохраните (Ctrl+X и подтвердите Y) и выключите виртуальную машину через меню в левом верхнем углу.

Установка виртуальной машины XUbuntu

Убедитесь, что для этой операции вы подключены к безопасной Wi-Fi-сети.

Сначала нужно скачать последний стабильный ISO-выпуск XUbuntu с xubuntu.org

Когда скачивание завершено, пора создать новую виртуальную машину:

- Отключите основную ОС от Wi-Fi, к которой ранее подключались через адаптер, и забудьте эту сеть.
- Запустите VirtualBox Manager.
- Создайте новую виртуальную машину и назовите её как хотите, например "XUbuntu Bridge".
- Выберите тип "Linux".

• Выберите версию "Ubuntu (64-bit)".

• Оставьте остальные параметры по умолчанию и нажмите Create.

• На следующем экране оставьте параметры по умолчанию и нажмите Create.

• Выберите новую виртуальную машину и нажмите Settings.

• Выберите Network.

• Для Adapter 1 подключите его к "Internal Network" и назовите "XUbuntu Bridge".

• Выберите Storage.

• Выберите пустой CD-дисковод.

• Справа нажмите значок CD и выберите "Choose a disk file".

• Выберите ранее скачанный ISO XUbuntu и нажмите OK.

• Выберите вкладку USB.

• Справа нажмите значок USB со знаком + (второй сверху).

• Выберите USB-адаптер Wi-Fi из списка и убедитесь, что он отмечен (оставьте параметры USB по умолчанию).

• Запустите виртуальную машину.

• Выберите Start XUbuntu.

• Выберите Install XUbuntu.

• Выберите раскладку клавиатуры и нажмите Continue.

• Выберите Minimal Installation и не отмечайте вариант Download Updates during the install.

• Выберите Erase Disk and install XUbuntu и нажмите Install Now.

• Выберите нужный часовой пояс и нажмите Continue.

• Выберите случайные имена, не связанные с вами (моё любимое имя пользователя — "NoSuchAccount").

• Выберите пароль и потребуйте пароль для входа.

• Нажмите Continue и дождитесь завершения установки и перезагрузки.

• После перезагрузки войдите в систему.

• Нажмите значок подключения в правом верхнем углу (он выглядит как две вращающиеся сферы).

• Нажмите Edit Connections.

• Выберите Wired Connection 1 (обычно он должен быть только один).

• Выберите вкладку IPv4.

• Измените Method на "Shared to other computers" и нажмите Save.

• Снова нажмите значок подключения в правом верхнем углу.

• Подключитесь к выбранной безопасной Wi-Fi-сети и при необходимости введите нужные сведения в портал авторизации.

• Настройка виртуальной машины XUbuntu Bridge завершена.

На этом этапе у основной ОС вообще не должно быть сети, а виртуальная машина XUbuntu должна иметь полностью рабочее Wi-Fi-подключение; это подключение будет раздаваться во внутреннюю сеть "XUbuntu Bridge".

Дополнительная конфигурация виртуальной машины Whonix Gateway

Теперь пора настроить виртуальную машину Whonix Gateway, чтобы она получила доступ из общей сети мостовой виртуальной машины, которую вы только что создали на предыдущем шаге:

• Откройте приложение VirtualBox и выберите виртуальную машину Whonix Gateway.

• Нажмите Settings.

• Перейдите на вкладку Network.

• Для Adapter 1 измените значение "Attached To" с "NAT" на "Internal Network".

• В поле "Name" выберите внутреннюю сеть "XUbuntu Bridge", которую создали ранее, и нажмите OK.

• Перезагрузите виртуальную машину Whonix Gateway.

• В меню слева сверху выберите System, Tor Control Panel и проверьте, что подключение установлено (так и должно быть).

• Конфигурация виртуальной машины Whonix Gateway завершена.

На этом этапе виртуальная машина Whonix Gateway должна получать доступ в интернет от виртуальной машины XUbuntu Bridge, которая, в свою очередь, получает доступ в интернет через USB-адаптер Wi-Fi и раздаёт его. У основной ОС вообще не должно быть сетевого подключения.

Все виртуальные машины за Whonix Gateway теперь должны работать нормально без дополнительной настройки.

Сделайте снимок VirtualBox ваших виртуальных машин после установки.

Готово; теперь можно пропустить остаток и перейти к части Выход в сеть.

Маршрут Qubes

Учтите, что руководство обновлено до Qubes OS 4.1

Как они говорят на своём сайте, Qubes OS — достаточно безопасная, свободная, открытая и ориентированная на безопасность операционная система для однопользовательских настольных компьютеров. Qubes OS использует виртуализацию на основе Xen и широко опирается на неё, позволяя создавать и управлять изолированными отсеками, называемыми Qubes.

Qubes OS — не дистрибутив Linux[72], а дистрибутив Xen. Он отличается от дистрибутивов Linux тем, что широко использует виртуализацию и разделение на отсеки, так что каждое приложение запускается в отдельной виртуальной машине (Qube). Дополнительный плюс: Qubes OS по умолчанию интегрирует Whonix и позволяет повысить приватность и анонимность. Перед выбором этого маршрута настоятельно рекомендуется изучить принципы Qubes OS. Вот несколько рекомендуемых материалов:

• Qubes OS Introduction, qubes-os.org Archive.org

• Qubes OS Video Tours, qubes-os.org Archive.org

• Qubes OS Getting Started, qubes-os.org Archive.org

• YouTube, Life Behind the Tinfoil: A Look at Qubes and Copperhead - Konstantin Ryabitsev, The Linux Foundation youtube.com Invidious

• YouTube, We used the reasonably-secure Qubes OS for 6 months and survived - Matty McFatty @themattymcfatty youtube.com Invidious

• YouTube, Qubes OS: How it works, and a demo of this VM-centric OS youtube.com Invidious

Эту ОС рекомендуют заметные фигуры, такие как Edward Snowden и PrivacyGuides.org.

Qubes — лучший вариант в этом руководстве для людей, которым комфортнее с Linux и технологиями в целом. Но у него есть недостатки: отсутствие правдоподобного отрицания на уровне всей ОС, требования к оборудованию и совместимость с оборудованием. Хотя по их требованиям его можно запустить на 4 ГБ ОЗУ Archive.org, рекомендуемый объём — 16 ГБ. Мы не рекомендуем использовать Qubes OS, если у вас меньше 8 ГБ ОЗУ. Для комфортной работы стоит иметь 16 ГБ; для особенно приятной — 24 или 32 ГБ.

Причина такого требования к ОЗУ в том, что каждое приложение будет запускаться в отдельной виртуальной машине, и каждая такая виртуальная машина будет требовать и выделять некоторый объём памяти, недоступный другим приложениям. Если вы запускаете родные приложения Windows внутри Qubes в Qubes OS, расход ОЗУ будет значительным.

Перед продолжением также проверьте совместимость оборудования здесь: qubes-os.org Archive.org. Результаты могут отличаться, и у вас могут возникнуть разные проблемы совместимости оборудования, которые придётся диагностировать и решать самостоятельно.

Я считаю, что если вы можете себе это позволить и вам комфортна идея использования Linux, стоит выбрать этот маршрут, поскольку он, вероятно, лучший с точки зрения безопасности и приватности. Единственный недостаток этого маршрута в том, что он, в отличие от маршрута Whonix, не даёт способа включить правдоподобное отрицание en.wikipedia.org Wikiless на уровне всей ОС.

Выбор способа подключения

В этом маршруте есть семь возможностей:

• **Рекомендуемые и предпочтительные:**

  • **Использовать только Tor (пользователь > Tor > интернет)**

  • **Использовать VPN поверх Tor (пользователь > Tor > VPN > интернет) в отдельных случаях**

  • **Использовать VPS с самостоятельно размещённым VPN/прокси поверх Tor (пользователь > Tor > самостоятельно размещённый VPN/прокси > интернет) в отдельных случаях**

• Возможные, если этого требует контекст:

  • Использовать VPN поверх Tor поверх VPN (пользователь > VPN > Tor > VPN > интернет)

  • Использовать Tor поверх VPN (пользователь > VPN > Tor > интернет)

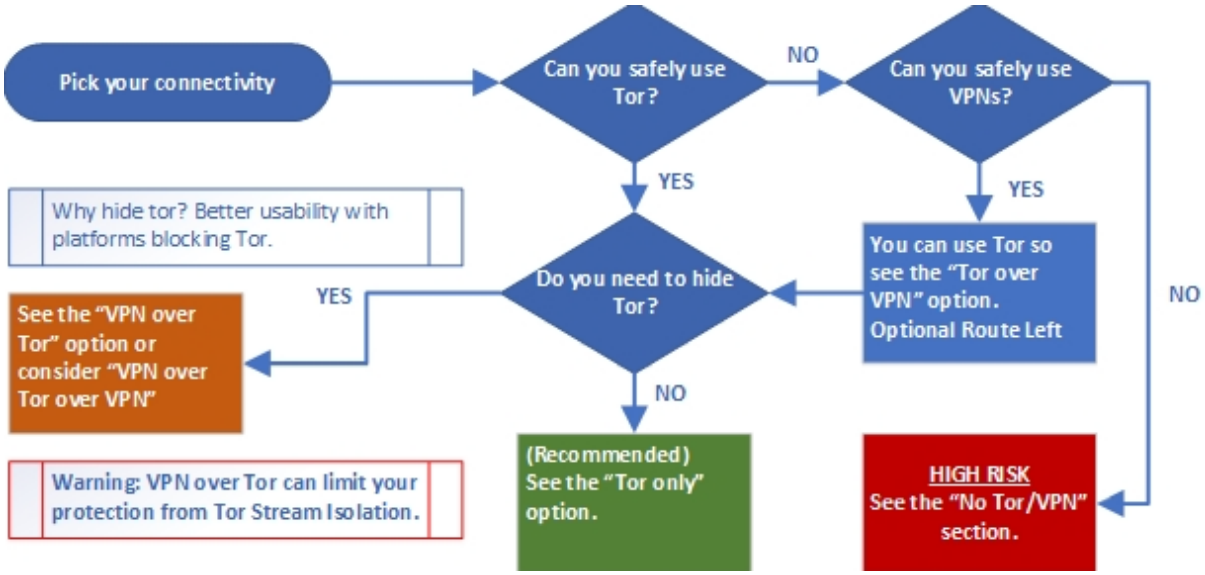
• Не рекомендуемые и рискованные:

  • Использовать только VPN (пользователь > VPN > интернет)

  • Использовать VPN поверх VPN (пользователь > VPN > VPN > интернет)

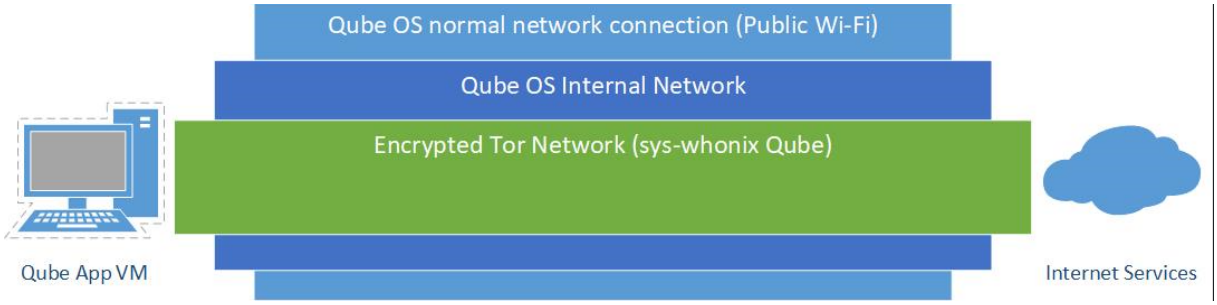
• **Не рекомендуется и крайне рискованно (но возможно)**

  • Без VPN и без Tor (пользователь > интернет)



Только Tor

Это предпочтительное и наиболее рекомендуемое решение.



При таком решении вся ваша сеть проходит через Tor, и этого должно быть достаточно для гарантии вашей анонимности в большинстве случаев.

Однако есть один главный недостаток: **некоторые сервисы прямо блокируют/запрещают выходные узлы Tor и не позволяют создавать с них учётные записи.**

Чтобы смягчить это, возможно, придётся рассмотреть следующий вариант: VPN поверх Tor, но с учётом рисков, объяснённых в следующем разделе.

VPN/прокси поверх Tor

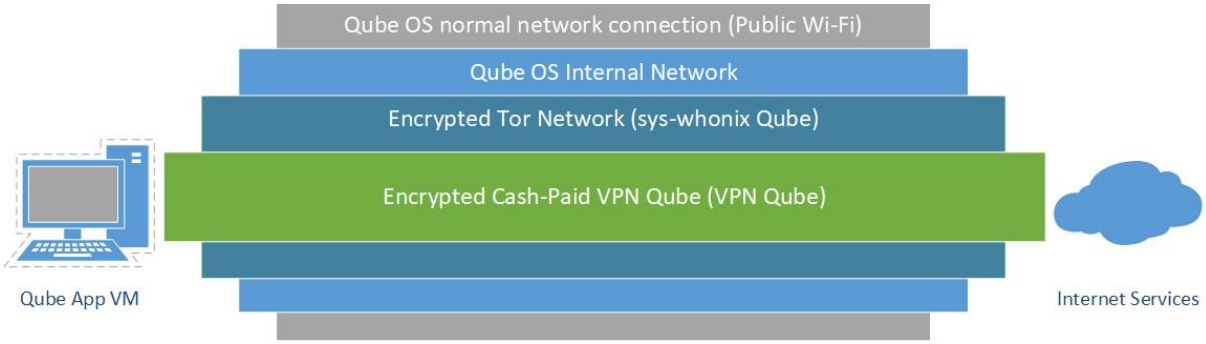
Это решение может дать преимущества в некоторых конкретных случаях по сравнению с использованием только Tor, когда доступ к целевому сервису с выходного узла Tor невозможен. Причина в том, что многие сервисы прямо запрещают, затрудняют или блокируют выходные узлы Tor (см. gitlab.torproject.org Archive.org).

Это решение можно реализовать двумя способами:

• Платный VPN поверх Tor (самый простой)

• Платный самостоятельно размещённый VPS, настроенный как VPN/прокси (самый эффективный для обхода онлайн-препятствий вроде CAPTCHA, но требует больше навыков Linux)

Как видно на этой иллюстрации, если ваш VPN/прокси, оплаченный наличными (предпочтительно)/Monero, будет скомпрометирован противником (несмотря на заявления о приватности и политики отсутствия журналов), он найдёт только анонимную учётную запись VPN, оплаченную наличными/Monero, которая подключается к их сервисам с выходного узла Tor.

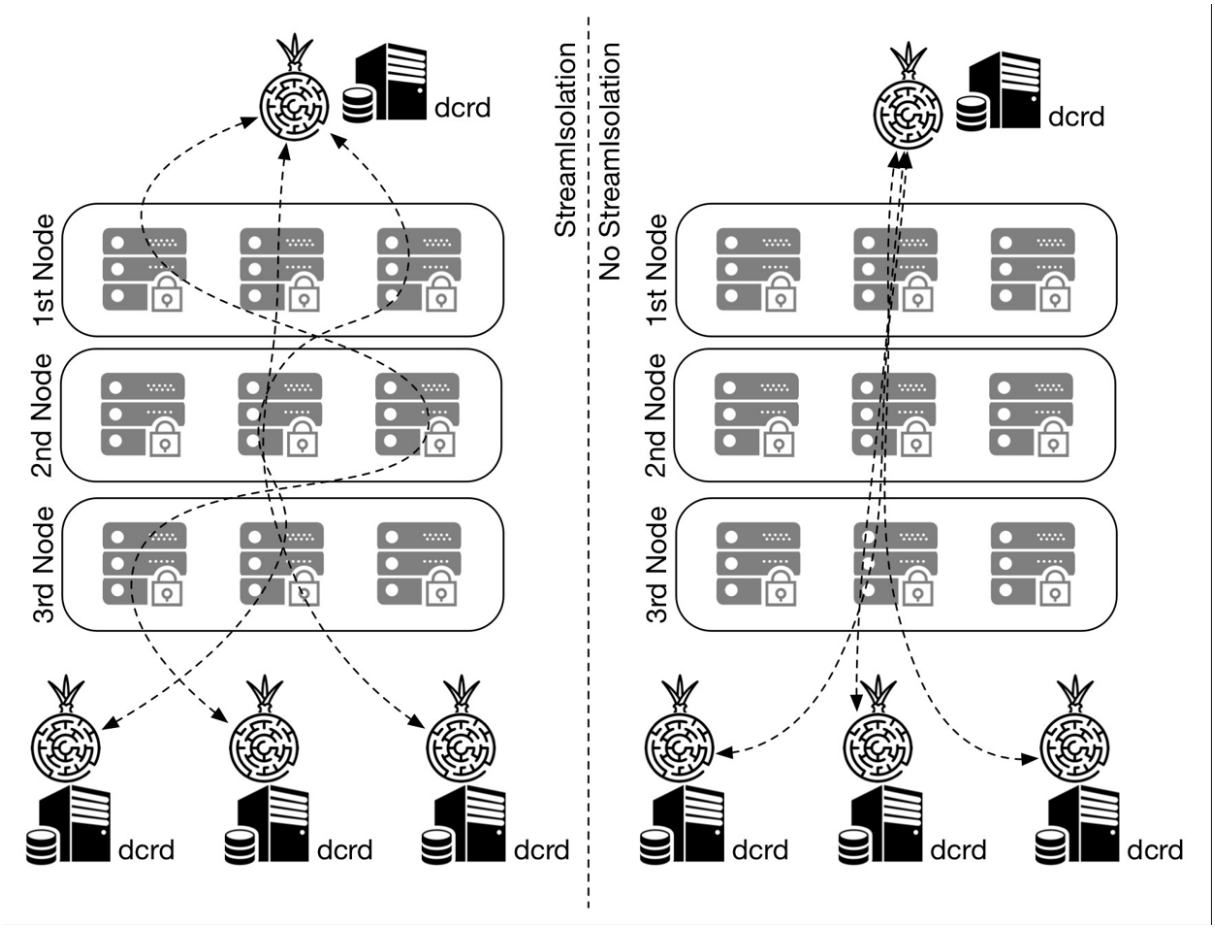


Если противнику каким-то образом удастся скомпрометировать и сеть Tor, он увидит только IP случайной публичной Wi-Fi-сети, не связанной с вашей личностью.

Если противник каким-то образом скомпрометирует ОС вашей виртуальной машины (например, вредоносным ПО или уязвимостью), он останется заперт во внутренней сети Whonix и не должен суметь раскрыть IP публичной Wi-Fi-сети.

Однако у этого решения есть один важный недостаток, который нужно учитывать: вмешательство в изоляцию потоков Tor[73].

Изоляция потоков — это метод смягчения рисков, который помогает предотвращать некоторые корреляционные атаки, создавая разные цепочки Tor для разных приложений. Вот иллюстрация, показывающая, что такое изоляция потоков:



(Иллюстрация Marcelo Martins, stakey.club Archive.org)

VPN/прокси поверх Tor попадает на правую сторону[74], то есть использование VPN/прокси поверх Tor заставляет Tor использовать одну цепочку для всей активности вместо нескольких цепочек для каждой. Это значит, что использование VPN/прокси поверх Tor в некоторых случаях может снизить эффективность Tor, и поэтому его следует применять только в отдельных ситуациях:

• Когда целевой сервис не допускает выходные узлы Tor.

• Когда вас устраивает общая цепочка Tor для разных сервисов. Например, для использования разных сервисов с входом в учётную запись.

Однако стоит не использовать этот метод, если ваша цель — просто просматривать разные случайные сайты без входа в учётные записи: вы не получите преимуществ изоляции потоков, и это может облегчить противнику корреляционные атаки между вашими сеансами (см. Ваш анонимизированный Tor/VPN-трафик).

Дополнительная информация:

• whonix.org Archive.org

• tails.boum.org Archive.org

• whonix.org Archive.org

Tor поверх VPN

Возможно, вы задаётесь вопросом: а что насчёт Tor поверх VPN вместо VPN поверх Tor?

• Недостатки

  • Ваш VPN-провайдер — просто ещё один интернет-провайдер, который будет знать ваш исходный IP и при необходимости сможет вас деанонимизировать. Мы им не доверяем. Лучше ситуация, где VPN-провайдер не знает, кто вы. Это мало что добавляет к анонимности.

  • В результате вы будете подключаться к разным сервисам с IP выходного узла Tor, который во многих местах запрещён или помечен. Это не помогает удобству.

• Преимущества:

  • **Главное преимущество: если вы во враждебной среде, где доступ к Tor невозможен/опасен/подозрителен, но VPN допустим.**

  • Этот метод также не ломает изоляцию потоков Tor.

Учтите: если у вас проблемы с доступом к сети Tor из-за блокировок/цензуры, можно попробовать мосты Tor (см. документацию Tor 2019.www.torproject.org Archive.org и документацию Whonix whonix.org Archive.org).

Также можно рассмотреть **VPN поверх Tor поверх VPN (пользователь > VPN > Tor > VPN > интернет)** с двумя VPN, оплаченными наличными/Monero. Это означает, что вы подключите основную ОС к первому VPN из публичной Wi-Fi-сети, затем Whonix подключится к Tor, а наконец ваша виртуальная машина подключится ко второму VPN поверх Tor поверх VPN (см. whonix.org Archive.org).

Конечно, это серьёзно ударит по производительности и может быть довольно медленным, но для достижения разумной анонимности Tor где-то в цепочке необходим.

Технически добиться этого в этом маршруте просто: нужны две отдельные анонимные учётные записи VPN; к первому VPN нужно подключиться из основной ОС, а затем следовать маршруту.

Итог: делайте это только если считаете, что использовать один Tor рискованно/невозможно, но VPN допустимы. Или просто потому что можете, почему бы и нет. Этот метод не снизит вашу безопасность/приватность/анонимность.

Только VPN

Этот маршрут не будет объясняться и не рекомендуется.

Если вы можете использовать VPN, значит, вы должны быть способны добавить поверх него слой Tor. А если вы можете использовать Tor, значит, вы можете добавить анонимный VPN поверх Tor, чтобы получить предпочтительное решение.

Использовать только VPN или даже VPN поверх VPN бессмысленно, потому что со временем это можно отследить до вас. Один из VPN-провайдеров будет знать ваш настоящий исходный IP (даже если это безопасное публичное место), а если вы добавите второй поверх него, второй всё равно будет знать, что вы использовали первый VPN-сервис. Это лишь немного задержит вашу деанонимизацию. Да, это дополнительный слой... но это постоянный централизованный дополнительный слой, и со временем вас можно деанонимизировать. По сути, это цепочка из трёх интернет-провайдеров, каждый из которых подчиняется законным запросам.

Дополнительные сведения см. в следующих источниках:

• whonix.org Archive.org

• whonix.org Archive.org

• researchgate.net Archive.org

• gist.github.com Archive.org

• schub.wtf Archive.org

В контексте этого руководства Tor где-то необходим для разумной и безопасной анонимности, и вам следует использовать его, если можете.

Без VPN/Tor

Если там, где вы находитесь, нельзя использовать ни VPN, ни Tor, вероятно, вы в очень враждебной среде, где слежка и контроль чрезвычайно высоки.

Просто не делайте этого: оно того не стоит и слишком рискованно. Любой мотивированный противник, способный добраться до вашего физического местоположения за считанные минуты, сможет почти мгновенно вас деанонимизировать.

Не забудьте снова посмотреть Противники (угрозы) и Проверка сети на слежку/цензуру с помощью OONI.

Если у вас совсем нет другого варианта и вы всё равно хотите что-то сделать, см. Что делать, когда Tor и VPN невозможны? **(на свой риск)**.

Тип подключения	Анонимность	Удобство доступа к онлайн-ресурсам	Изоляция потоков Tor	Безопаснее там, где Tor подозрителен/опасен	Скорость	Стоимость	Рекомендуется
Только Tor	**Хорошая**	**Среднее**	**Возможна**	**Нет**	**Средняя**	**Бесплатно**	**Да**
Tor поверх VPN	**Хорошая+**	**Среднее**	**Возможна**	**Да**	**Средняя**	**Около 50 евро/год**	**Если нужно (Tor недоступен)**
Tor поверх VPN поверх Tor	**Лучшая**	**Среднее**	**Возможна**	**Да**	**Плохая**	**Около 50 евро/год**	**Да**
VPN поверх Tor	**Хорошая-**	**Хорошее**	**Нет**	**Нет**	**Средняя**	**Около 50 евро/год**	**Если нужно (удобство)**
Самостоятельно размещённый VPS VPN/прокси поверх Tor	**Хорошая-**	**Очень хорошее**	**Нет**	**Нет**	**Средняя**	**Около 50 евро/год**	**Если нужно (удобство)**
VPN/прокси поверх Tor поверх VPN	**Хорошая-**	**Хорошее**	**Нет**	**Да**	**Плохая**	**Около 100 евро/год**	**Если нужно (удобство и Tor недоступен)**
Только VPN/прокси	**Плохая**	**Хорошее**	**Н/П**	**Да**	**Хорошая**	**Около 50 евро/год**	**Нет**

Тип подключения	Анонимность	Удобство доступа к онлайн-ресурсам	Изоляция потоков Tor	Безопаснее там, где Tor подозрителен/опасен	Скорость	Стоимость	Рекомендуется
Без Tor и VPN	**Плохая**	**Неизвестно**	**Н/П**	**Нет**	**Хорошая**	**Около 100 евро (антенна)**	**Нет. На свой риск.**

К сожалению, использование только Tor вызывает подозрения у многих целевых платформ. Если использовать только Tor, вы столкнётесь со множеством препятствий (CAPTCHA, ошибки, сложности с регистрацией). Кроме того, само использование Tor там, где вы находитесь, может создать вам проблемы. Но Tor остаётся лучшим решением для анонимности и должен где-то присутствовать в цепочке.

- Если вы собираетесь создавать постоянные общие и аутентифицированные личности на разных сервисах, где доступ из Tor затруднён, мы рекомендуем варианты **VPN поверх Tor** и **VPS VPN/прокси поверх Tor** (или VPN поверх Tor поверх VPN, если нужно). Это может быть немного менее безопасно против корреляционных атак из-за нарушения изоляции потоков Tor, но даёт намного больше удобства при доступе к онлайн-ресурсам, чем один Tor. Это "приемлемый" компромисс, на мой взгляд, если вы достаточно осторожны со своей личностью.
  - **Примечание: становится всё более распространённым, что массовые сервисы и CDN также блокируют или затрудняют доступ пользователям VPN с помощью CAPTCHA и разных других препятствий**. **В таком случае самостоятельно размещённый VPS с VPN/прокси поверх Tor — лучшее решение: собственный выделенный VPS гарантирует, что вы единственный пользователь своего IP, и препятствий будет мало или не будет вовсе.** Рассмотрите самостоятельно размещённый VPN/прокси на VPS, оплаченном Monero/наличными (для пользователей, лучше знакомых с Linux), если хотите наименьшее количество проблем (это будет подробнее объяснено в следующем разделе).
- Если же ваша цель — просто анонимно просматривать случайные сервисы без создания конкретных общих личностей, использовать дружелюбные к Tor сервисы; или если вы не хотите принимать компромисс из предыдущего варианта. **Тогда мы рекомендуем маршрут только через Tor, чтобы сохранить все преимущества изоляции потоков (или Tor поверх VPN, если нужно).**
- Если вопрос в стоимости, мы рекомендуем вариант только Tor, если он возможен.
- Если доступ и к Tor, и к VPN невозможен или опасен, тогда у вас нет выбора, кроме как безопасно полагаться на публичный Wi-Fi. См. Что делать, когда Tor и VPN невозможны?

Дополнительно можно посмотреть обсуждения здесь; они помогут принять решение самостоятельно:

- Tor Project: gitlab.torproject.org Archive.org
- Документация Tails:
  - gitlab.tails.boum.org Archive.org
  - tails.boum.org Archive.org
- Документация Whonix (в этом порядке):
  - whonix.org Archive.org
  - whonix.org Archive.org
  - whonix.org Archive.org

• Некоторые статьи по теме:

  • researchgate.net Archive.org

Получение анонимного VPN/прокси

Пропустите этот шаг, если хотите использовать только Tor или VPN невозможен.

См. Получение анонимного VPN/прокси

Примечание о правдоподобном отрицании

Qubes OS использует LUKS для полного шифрования диска, и технически возможно добиться формы отрицания с помощью отделённых заголовков LUKS. Это пока не интегрировано в это руководство, но развивающееся руководство о том, как этого добиться, можно найти здесь: forum.qubes-os.org, а дополнительный контекст есть в разделе основной ОС Linux (см. Примечание о правдоподобном отрицании в Linux).

Установка

Вы будете следовать инструкциям из их собственного руководства qubes-os.org Archive.org:

(Secure Boot не поддерживается согласно их FAQ: qubes-os.org Archive.org, поэтому его следует отключить в настройках BIOS/UEFI.)

• Скачайте последний установочный ISO Qubes OS 4.1.x в соответствии с их списком совместимости оборудования.

• Получите и проверьте главный подписывающий ключ Qubes OS: keys.qubes-os.org

• Подготовьте USB-накопитель с ISO-файлом Qubes OS.

• Установите Qubes OS согласно руководству по установке:

  • **Если вы хотите использовать Tor или VPN поверх Tor: на последнем шаге отметьте “Enabling system and template updates over the Tor anonymity network using Whonix”. Это заставит все обновления Qubes OS проходить через Tor. Хотя это заметно снизит скорость обновления, это повысит вашу анонимность с самого начала.** (Если у вас проблемы с подключением к Tor из-за цензуры или блокировок, рассмотрите использование мостов Tor, как рекомендовалось ранее. Просто следуйте руководству здесь: whonix.org Archive.org)

  • Если вы хотите использовать Tor поверх VPN или не можете использовать ни Tor, ни VPN, оставьте этот пункт неотмеченным.

  • Обязательно убедитесь, что проверяете подпись ISO; она находится на этой странице: qubes-os.org Archive.org. Проверьте цифровой отпечаток, получив его из нескольких независимых источников разными способами, как рекомендовано. Это нужно, чтобы убедиться, что образ не был изменён. Не пропускайте этот важнейший шаг, даже если

знаете, что получаете ISO из доверенного источника: сайт Qubes тоже теоретически может быть скомпрометирован.

- Если вам запрещено использовать Tor, нет смысла устанавливать шаблоны виртуальных машин Whonix. Вы можете отключить установку Whonix во время первичной настройки после установки.

Чтобы убедиться, что ISO Qubes не был изменён, нужно получить цифровой отпечаток главного ключа Qubes из нескольких разных источников. Это руководство можно использовать как один из таких источников.

Цифровой отпечаток главного подписывающего ключа Qubes должен совпадать с `427F 11FD 0FAA 4B08 0123 F01C DDFA 1A3E 3687 9494`.

Не забудьте прочитать руководство по проверке подписей на сайте Qubes: qubes-os.org Archive.org.

Поведение при закрытии крышки

К сожалению, Qubes OS не поддерживает гибернацию[75], что создаёт проблему с точки зрения атак холодной загрузки. Чтобы смягчить эти риски, я настоятельно рекомендую настроить Qubes OS на выключение при любом действии питания (кнопка питания, закрытие крышки). Это можно сделать через XFCE Power Manager. Не используйте функции сна.

Anti Evil Maid (AEM)

Предупреждение: этот шаг работает только с процессорами Intel, legacy BIOS и TPM 1.2. Если вы не соответствуете этим требованиям, пропустите этот шаг.

Anti Evil Maid — это реализация статической доверенной загрузки на основе TPM, основная цель которой — предотвращать атаки Evil Maid. Для установки и использования AEM нужно подключить USB-накопитель напрямую к dom0. Поэтому пользователь должен выбрать между защитой dom0 от потенциально вредоносного USB-накопителя и защитой системы от атак Evil Maid. Учтите, что AEM совместим только с процессорами Intel и legacy-вариантами загрузки.

Предпочтительный способ смягчения любой атаки evil maid — постоянно сохранять физический контроль над устройством. Если это невозможно, этот механизм может быть актуален для вашей модели угроз.

Перед тем как решить использовать эту систему, пожалуйста, прочитайте Важные примечания об evil-maid и вмешательстве

Подробнее и инструкции по установке:

- qubes-os.org Archive.org
- blog.invisiblethings.org Archive.org
- github.com Archive.org

Подключение к публичному Wi-Fi

Помните: это следует делать из безопасного места (см. Найдите безопасные места с приличным публичным Wi-Fi и Использование дальнобойной антенны для подключения к публичным Wi-Fi с безопасного расстояния):

- В правом верхнем углу щёлкните левой кнопкой по значку сети и запишите SSID Wi-Fi, к которому хотите подключиться.
- Теперь щёлкните правой кнопкой по значку сети и выберите Edit Connections.
- Добавьте подключение с помощью знака +.
- Выберите Wi-Fi.
- Введите SSID нужной сети, который записали ранее (если нужно).
- Выберите Cloned Mac Address.
- Выберите Random, чтобы случайным образом изменить ваш MAC Address.
    - **Предупреждение: эта настройка должна работать в большинстве случаев, но на некоторых сетевых адаптерах может быть ненадёжной. Если хотите быть уверены, обратитесь к этой документации: github.com** Archive.org
- Save.
- Теперь снова щёлкните левой кнопкой по учётной записи подключения и подключитесь к нужной Wi-Fi-сети.
- Если это открытая Wi-Fi-сеть, требующая регистрации, нужно запустить браузер для регистрации:
    - После подключения запустите Disposable Fedora Firefox Browser.
    - Перейдите в верхнее левое меню.
    - Выберите Disposable, Fedora, Firefox.
    - Откройте Firefox и зарегистрируйтесь в Wi-Fi (анонимно).

Обновление Qubes OS с 4.0.x до 4.1.x (это стоит сделать)

Лично мы не стали бы делать это поверх установленной системы и предпочли бы свежую установку.

Но если вы действительно хотите, это технически возможно по этому руководству: qubes-os.org Archive.org

Обновление Qubes OS

После подключения к Wi-Fi нужно обновить Qubes OS и Whonix. Перед выполнением любых чувствительных действий Qubes OS всегда нужно держать обновлённой. Особенно ваши браузерные виртуальные машины. Обычно Qubes OS предупреждает об обновлениях в правом верхнем углу значком шестерёнки. Поскольку в этом случае процесс может занять время из-за использования Tor, его можно запустить принудительно:

• Нажмите значок Applications в левом верхнем углу.

• Выберите Qubes Tools.

• Выберите Qubes Update.

• Отметьте "Enable updates for Qubes without known available updates".

• Выберите все Qubes.

• Нажмите Next и дождитесь завершения обновлений.

• Если при установке вы отметили вариант Tor, будьте терпеливы: через Tor это может занять время.

Обновление до Whonix 18

Обзор улучшений Whonix 18.x:

• Автоматизированный процесс обновления релизов (ручное вмешательство не требуется)
• Улучшенная интеграция AppArmor для лучшей изоляции приложений
• Улучшенная конфигурация сети и подключения к Tor
• Обновлённая документация во всех разделах
• Лучшая совместимость с Qubes OS (теперь официально поддерживается на R4.3+)

Чтобы обновить Whonix 17 до Whonix 18:

1. **Сделайте резервную копию всех данных** — перед обновлением клонируйте виртуальные машины с помощью снимков Virtualbox или предпочитаемым вами способом.

1. **Сначала обновите основную систему Qubes:**
   • Убедитесь, что используете как минимум Qubes R4.2 (для совместимости с Whonix 17)
   • По возможности обновитесь до Qubes R4.3+ (рекомендуется для поддержки Whonix 18)

1. **Выполните стандартные обновления в ваших шаблонах согласно инструкциям ОС:**

```
sudo unattended-upgrade --auto-run
```

1. **Запустите автоматизированное обновление:**

```
sudo release-upgrade
```

   • Оно выполнит обновление автоматически без необходимости пользовательского ввода.

1. **Перезагрузите виртуальные машины и выполните `systemcheck` для проверки целостности системы после обновления:**

```
sudo checkvm --all
sudo tor --verify
```

1. **Для Qubes обновите источники репозиториев APT после обновления (необязательно, можно позже).**

Важные примечания:

- **Qubes R4.2+ с Whonix 18 теперь официально поддерживается**. Подробные инструкции см. whonix.org Archive.org.
- Всегда проверяйте целостность системы после обновления с помощью `systemcheck` и инструментов проверки Tor.
- Если вы не используете Qubes OS, следуйте общему руководству по обновлению Whonix Archive.org.

Усиление Qubes OS

Отказ от ответственности: этот раздел находится в разработке и будет значительно дорабатываться в следующих выпусках. Этот раздел предназначен для более продвинутых пользователей.

Изоляция приложений

Хотя Qubes OS уже изолирует всё по своей архитектуре, также полезно рассмотреть изоляцию самих приложений с помощью AppArmor или SELinux.

AppArmor

"AppArmor is a Mandatory Access Control framework. When enabled, AppArmor confines programs according to a set of rules that specify what files a given program can access. This initiative-taking approach helps protect the system against both known and unknown vulnerabilities" (Debian.org).

По сути, AppArmor[76] — система изоляции приложений. По умолчанию она не включена, но поддерживается Qubes OS.

- О виртуальных машинах Fedora:
  - Fedora использует не AppArmor, а SELinux, поэтому смотрите следующий раздел.
- О виртуальных машинах Debian:
  - Перейдите и прочитайте wiki.debian.org Archive.org
- О любой другой виртуальной машине Linux:
  - Перейдите и прочитайте:
    - wiki.archlinux.org Archive.org
    - wiki.debian.org Archive.org

- О виртуальных машинах Whonix: стоит рассмотреть включение и использование AppArmor, особенно на виртуальных машинах Whonix в Qubes OS:
  - Сначала стоит перейти и прочитать whonix.org Archive.org
  - Затем стоит снова перейти и прочитать whonix.org Archive.org

SELinux

SELinux[77] похож на AppArmor. Различия между SELinux и AppArmor — технические детали, в которые мы не будем углубляться.

Хорошее объяснение того, что это такое: youtube.com Invidious

В этом руководстве и в контексте Qubes OS важно упомянуть SELinux, поскольку это рекомендуемый Fedora метод, а Fedora — одна из систем по умолчанию в Qubes OS.

Поэтому перейдите и прочитайте docs.fedoraproject.org Archive.org

Можно использовать SELinux в шаблонах Fedora. Но решать вам. Повторю: это для продвинутых пользователей.

Настройка VPN ProxyVM

Пропустите этот шаг, если вы не хотите использовать VPN и будете использовать только Tor, либо если VPN тоже невозможен.

Это руководство также должно работать с любым OpenVPN-провайдером (например, Mullvad, IVPN, Safing.io или Proton VPN).

Оно основано на руководстве, предоставленном самими Qubes OS (github.com Archive.org). Если вы знакомы с этим процессом, можно следовать их руководству.

Кроме того, у Mullvad есть справочная статья, которая проводит через настройку Proxy VM: mullvad.net Archive.org.

Создание ProxyVM

- Нажмите значок Applications (левый верхний угол).
- Нажмите Create Qubes VM.
- Задайте имя и метку по желанию: я предлагаю "VPNGatewayVM".
- Выберите Type: Standalone Qube copied from a template.
- Выберите Template: Debian-11 (по умолчанию).
- Выберите Networking:
  - Выберите sys-whonix, если хотите использовать VPN поверх Tor / только Tor (рекомендуется)
  - Выберите sys-firewall, если хотите использовать Tor поверх VPN / без Tor или VPN / только VPN

• Advanced: отметьте provides network.

• Отметьте "Start Qube automatically on boot".

• Создайте виртуальную машину.

  • Если вы выбираете VPN поверх Tor, нужно перейти в настройки созданной ProxyVM и выбрать "sys-vpn" для сети.
    • Более простой способ настроить ProxyVM — просто запустить VPN-клиент в ProxyVM.
    • Обычно при подключении к сайту вашего VPN-провайдера он сообщает, правильно ли ваш трафик маршрутизируется через VPN.

  • Если вы выбираете Tor поверх VPN, нужно сделать обратное: у ProxyVM сеть должна быть настроена как "sys-tor", а у виртуальной машины "sys-tor" сетью должна быть "sys-vpn".
    • Проверьте подключение виртуальной машины к интернету, запустив браузер внутри ProxyVM. Откройте check.torproject.org Archive.org (должно быть написано, что вы подключены к Tor)

Скачивание VPN-конфигурации от вашего VPN-провайдера, оплаченного наличными/Monero

Если вы можете использовать Tor

Используя Tor Browser (будьте осторожны и не используйте для этого обычный браузер открытого интернета), скачайте у вашего VPN-провайдера необходимые файлы конфигурации OpenVPN для Linux.

Это можно сделать с помощью встроенного в Qubes OS Tor Browser: откройте значок Applications (левый верхний угол) и выберите приложение Disposable Tor Browser.

Если вы не можете использовать Tor

Запустите браузер из DisposableVM и скачайте у вашего VPN-провайдера необходимые файлы конфигурации OpenVPN для Linux. См. Что делать, когда Tor и VPN невозможны?

Когда вы закончите скачивать файлы конфигурации в Disposable Browser (обычно это zip-файл), скопируйте их в вашу ProxyVM VPN Gateway (правый щелчок по файлу и отправка в другую AppVM).

Конфигурация ProxyVM

Пропустите этот шаг, если не собираетесь использовать VPN

• Нажмите левый верхний угол.

• Выберите только что созданную VPN VM.

• Откройте Files этой VPN VM.

• Перейдите в "Qubesincoming" > dispXXXX (это была ваша Disposable Browser VM).

• Дважды щёлкните скачанный zip-файл с файлами конфигурации OpenVPN, чтобы распаковать его.

• Теперь снова выберите VPN VM и запустите терминал.

• Установите OpenVPN следующей командой: `sudo apt-get install openvpn`

• Скопируйте все файлы конфигурации OpenVPN, предоставленные вашим VPN-провайдером, в /etc/openvpn/.

• Для всех файлов конфигурации OpenVPN (для каждого местоположения):

  • Измените каждый файл с помощью `sudo nano configfile` (не забудьте sudo, чтобы редактировать файл внутри /etc).

  • Измените протокол с "udp" на "tcp" (Tor не поддерживает UDP).

  • Измените порт на поддерживаемый вашим VPN-провайдером TCP-порт (например, 80 или 443).

  • Сохраните и выйдите из каждого файла.

• Измените файл конфигурации OpenVPN (/etc/default/openvpn), набрав `sudo nano /etc/default/openvpn`

  • Измените `#AUTOSTART="all"` на `AUTOSTART="all"` (другими словами, удалите "#")

  • Сохраните и выйдите.

• Измените файл правил брандмауэра Qubes (/rw/config/qubes-firewall-user-script), набрав "sudo nano /rw/config/qubes-firewall-user-script"

  • Добавьте следующие строки (без кавычек и примечаний в скобках)

    • `virtualif=10.137.0.17`

(Это IP ProxyVM; он не динамический, и вам может понадобиться изменить его после перезагрузки)

• `vpndns1=10.8.0.1`

(Это первый DNS-сервер вашего VPN-провайдера; он не должен меняться)

• `vpndns2=10.14.0.1`

(Это второй DNS-сервер вашего VPN-провайдера; он не должен меняться)

• `iptables -F OUTPUT`

• `iptables -I FORWARD -o eth0 -j DROP`

• `iptables -I FORWARD -i eth0 -j DROP`

• `ip6tables -I FORWARD -o eth0 -j DROP`

- `ip6tables -I FORWARD -i eth0 -j DROP`

  (Это заблокирует исходящий трафик, когда VPN не работает; это аварийное отключение сети. Подробнее здесь: linuxconfig.org Archive.org)

- `iptables -A OUTPUT -d 10.8.0.1 -j ACCEPT`
- `iptables -A OUTPUT -d 10.14.0.1 -j ACCEPT`

  (Это разрешит DNS-запросы к DNS вашего VPN-провайдера, чтобы разрешать имена VPN-серверов в файлах конфигурации OpenVPN)

- `iptables -F PR-QBS -t nat`
- `iptables -A PR-QBS -t nat -d $virtualif -p udp --dport 53 -j DNAT --to $vpndns1`
- `iptables -A PR-QBS -t nat -d $virtualif -p tcp --dport 53 -j DNAT --to $vpndns1`
- `iptables -A PR-QBS -t nat -d $virtualif -p udp --dport 53 -j DNAT --to $vpndns2`
- `iptables -A PR-QBS -t nat -d $virtualif -p tcp --dport 53 -j DNAT --to $vpndns2`

  (Это перенаправит все DNS-запросы из ProxyVM на DNS-серверы VPN-провайдера)

- Перезапустите ProxyVM, набрав "sudo reboot".
- Проверьте VPN-подключение ProxyVM, запустив внутри неё браузер и перейдя на страницу проверки вашего VPN-провайдера. Теперь там должно быть написано, что вы подключены к VPN:
  - Mullvad: mullvad.net Archive.org
  - IVPN: ivpn.net Archive.org (проверьте верхний баннер)
  - Proton VPN: следуйте их инструкциям здесь: protonvpn.com Archive.org

VPN поверх Tor

Настройка одноразового браузерного Qube для использования VPN поверх Tor

- В Applications Menu (левый верхний угол) выберите Disposable Fedora VM.
- Перейдите в Qube Settings.
- Нажмите Clone Qube и назовите его, например, "sys-VPNoverTor".
- Снова в Application Menu выберите только что созданный клон.
- Перейдите в Qube Settings.
- Измените Networking на созданный ранее ProxyVPN.
- Нажмите OK.
- Запустите браузер внутри Whonix Workstation.
- Проверьте, что у вас есть VPN-подключение; оно должно работать.

Теперь у вас должна быть Disposable Browser VM, работающая с вашим VPN, оплаченным наличными/Monero, поверх Tor.

Tor поверх VPN

Перенастройте виртуальную машину Whonix Gateway так, чтобы она использовала вашу ProxyVM как NetVM вместо sys-firewall:

• В Applications Menu (левый верхний угол) выберите виртуальную машину sys-whonix.

• Перейдите в Qube Settings.

• Измените Networking NetVM на созданный ранее ProxyVPN вместо sys-firewall.

• Нажмите OK.

• Создайте Whonix Workstation Disposable VM (следуйте этому руководству whonix.org Archive.org)

• Запустите браузер из этой виртуальной машины и проверьте, что VPN-подключение есть и работает.

Кроме того, можно создать любой другой тип одноразовой виртуальной машины (но это менее безопасно, чем вариант Whonix):

• В Applications Menu (левый верхний угол) выберите Disposable Fedora VM.

• Перейдите в Qube Settings.

• Нажмите Clone Qube и назовите его, например, "sys-TorOverVPN".

• Снова в Application Menu выберите только что созданный клон.

• Перейдите в Qube Settings.

• Измените Networking на созданный ранее sys-whonix.

• Нажмите OK.

• Запустите браузер внутри виртуальной машины.

• Проверьте, что у вас есть VPN-подключение; оно должно работать.

Теперь у вас должна быть Disposable Browser VM, работающая с Tor поверх VPN, оплаченного наличными/Monero.

Любая другая комбинация?

Например, VPN поверх Tor поверх VPN

К этому моменту вы должны понимать, насколько легко в Qubes маршрутизировать трафик из одной виртуальной машины в другую.

Можно создать несколько ProxyVM для VPN-доступа и оставить Whonix для Tor. Нужно лишь менять настройки NetVM у разных виртуальных машин, чтобы изменить схему.

У вас может быть:

• Одна VPN ProxyVM для базового подключения Qubes OS.

• Виртуальная машина sys-whonix (Whonix Gateway), получающая сеть от первой ProxyVM.

• Вторая VPN ProxyVM, получающая сеть от sys-whonix.

• Одноразовые виртуальные машины, получающие свою NetVM от второй ProxyVM.

В результате получится пользователь > VPN > Tor > VPN > интернет (VPN поверх Tor поверх VPN). Экспериментируйте сами. Qubes OS прекрасно подходит для таких вещей.

Настройка безопасного браузера в Qubes OS

См.: Какой браузер использовать в гостевой/одноразовой виртуальной машине

Fedora Disposable VM

В Applications Menu (слева сверху) выберите шаблон Fedora-36:

• Перейдите в Qube Settings.

• Клонируйте виртуальную машину и назовите её "fedora-36-brave" (в этом шаблоне виртуальной машины будет Brave).

• Снова перейдите в Applications Menu и выберите только что созданный клон.

• Перейдите в Qube Settings.

• Измените её сеть на ProxyVPN и нажмите Apply.

• Запустите терминал из виртуальной машины.

Если хотите использовать Brave: примените инструкции из их документации Archive.org и выполните следующие команды:

```
sudo dnf install dnf-plugins-core
```

```
sudo dnf config-manager --add-repo
https://brave-browser-rpm-release.s3.brave.com/x86_64/
```

```
sudo rpm --import https://brave-browser-rpm-release.s3.brave.com/brave-core.asc
```

```
sudo dnf install brave-browser
```

Также стоит рассмотреть усиление браузера, см. Усиление браузеров

Whonix Disposable VM

Измените шаблон Whonix Disposable VM и следуйте инструкциям здесь: whonix.org Archive.org

Дополнительные меры предосторожности для браузера

• См.: Усиление браузеров

• См.: Дополнительные меры предосторожности для браузера с включённым JavaScript

Настройка виртуальной машины Android

Потому что иногда нужно анонимно запускать и мобильные приложения. Для этой цели можно настроить виртуальную машину Android. Как и в других случаях, в идеале эта виртуальная машина тоже будет находиться за Whonix Gateway для подключения к сети Tor. Но её также можно настроить как VPN поверх Tor поверх VPN.

Поскольку Android-x86 не работает "хорошо" с Qubes OS (по моему опыту), вместо него мы рекомендуем AnBox (anbox.io Archive.org), который работает с Qubes OS "достаточно хорошо". Дополнительную информацию также можно найти здесь: whonix.org Archive.org

Если вы можете использовать Tor

Позднее в настройках Qubes во время создания:

• Выберите Networking.

• Измените на sys-whonix, чтобы поместить её за Whonix Gateway (поверх Tor).

Если вы не можете использовать Tor

Просто используйте руководства как есть. См. Что делать, когда Tor и VPN невозможны?.

Установка

В целом следуйте этому руководству:

• Нажмите значок Applications (левый верхний угол).

• Нажмите Create Qubes VM.

• Задайте имя и метку по желанию: мы предлагаем "Android".

• Выберите Type: Standalone Qube copied from a template.

• Выберите Template: Debian-11.

• Выберите Networking:

  • Выберите sys-whonix, если хотите использовать VPN поверх Tor / только Tor (рекомендуется)

  • Выберите sys-firewall, если хотите использовать Tor поверх VPN / без Tor или VPN / только VPN

• Запустите Qube и откройте терминал.

Теперь нужно следовать инструкциям отсюда: github.com Archive.org:

• Начните с клонирования репозитория AnBox Modules:

    - `git clone https://github.com/anbox/anbox-modules.git`
    - Перейдите в клонированный каталог.
    - Выполните `./INSTALL.sh` (или следуйте ручным инструкциям в руководстве).
- Перезагрузите машину.
- Откройте новый терминал.
- Установите Snap:
    - `sudo apt install snapd`

Теперь следуйте другому их руководству отсюда: github.com Archive.org:

- Установите AnBox:
    - `snap install --devmode --beta anbox`
- Чтобы позже обновить AnBox, выполните:
    - `snap refresh --beta --devmode anbox`
- Перезагрузите машину.
- Снова откройте терминал и запустите эмулятор:
    - `anbox.appmgr`

Должен появиться интерфейс Android. Иногда он падает, и вам может понадобиться запустить его дважды, чтобы он заработал.

Если хотите установить приложения в этот эмулятор:

- Установите ADB:
    - `sudo apt install android-tools-adb`
- Сначала запустите Anbox (выполните `anbox.appmgr`)
- Получите APK любого приложения, которое хотите установить.
- Теперь установите любой APK:
    - `adb install my-app.apk`

Вот и всё: теперь у вас должен быть Android Qube поверх Tor (или чего угодно ещё), способный запускать почти любое приложение, которое можно загрузить через ADB. На данный момент это самый простой способ получить эмуляцию Android в Qubes OS.

KeePassXC

Вам понадобится место для хранения ваших данных (логинов/паролей, личностей и сведений TOTP[78]).

Для этой цели рекомендуется KeePassXC из-за встроенной функции TOTP. Это возможность создавать записи для аутентификации 2FA[79] с помощью функции аутентификатора.

В контексте Qubes OS чувствительную информацию следует хранить внутри vault Qube:

- Сначала нажмите значок Applications (слева сверху) и выберите vault Qube.
- Нажмите Qubes Settings.

• Выберите вкладку Applications.

• Из списка доступных приложений добавьте KeePassXC в список выбранных приложений.

Готово; теперь можно пропустить остаток и перейти к части "Создание ваших анонимных онлайн-личностей".

Руководство по установке виртуальных машин на основе Windows в Qubes OS

См. их руководство здесь: github.com Archive.org

Сноски

[1] [назад] Wikipedia, Zero-trust Security Model en.wikipedia.org Wikiless Archive.org
[2] [назад] Qubes OS, System Requirements qubes-os.org Archive.org
[3] [назад] Wikipedia, Plausible Deniability en.wikipedia.org Wikiless Archive.org
[4] [назад] Wikipedia, Rubber-hose Cryptanalysis en.wikipedia.org Archive.org
[5] [назад] Defuse.ca, TrueCrypt's Plausible Deniability is Theoretically Useless defuse.ca Archive.org
[6] [назад] Wikipedia, Deniable Encryption en.wikipedia.org Wikiless Archive.org
[7] [назад] Wikipedia, OONI, en.wikipedia.org Wikiless Archive.org
[8] [назад] Privacy International, Timeline of SIM Card Registration Laws privacyinternational.org Archive.org
[9] [назад] NYTimes, Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes nytimes.com Archive.org
[10] [назад] Usenix.org, Shedding too much Light on a Microcontroller's Firmware Protection usenix.org Archive.org
[11] [назад] TorProject.org, Can I run Tor Browser on an iOS device? support.torproject.org Archive.org
[12] [назад] Wikipedia, Tails en.wikipedia.org Wikiless Archive.org
[13] [назад] Vice.com, Facebook Helped the FBI Hack a Child Predator vice.com Archive.org
[14] [назад] XKCD, Security xkcd.com Archive.org
[15] [назад] Veracrypt Documentation, Trim Operations veracrypt.fr Archive.org
[16] [назад] YouTube, 36C3 - Uncover, Understand, Own - Regaining Control Over Your AMD CPU youtube.com Invidious
[17] [назад] Qubes OS, Anti-Evil Maid, github.com Archive.org
[18] [назад] QubesOS FAQ, qubes-os.org Archive.org
[19] [назад] Wikipedia, Secure Boot en.wikipedia.org Wikiless Archive.org
[20] [назад] Wikipedia, Booting en.wikipedia.org Wikiless Archive.org
[21] [назад] Wired, Don't Want Your Laptop Tampered With? Just Add Glitter Nail Polish wired.com Archive.org
[22] [назад] Wikipedia, Virtual Machine en.wikipedia.org Wikiless Archive.org
[23] [назад] Wikipedia, Deniable Encryption en.wikipedia.org Wikiless Archive.org
[24] [назад] PrivacyGuides.org, Don't use Windows 10 - It's a privacy nightmare web.archive.org Archive.org
[25] [назад] Wikipedia, Key Disclosure Laws en.wikipedia.org Wikiless Archive.org
[26] [назад] GP Digital, World map of encryption laws and policies gp-digital.org Archive.org
[27] [назад] Wikipedia, Bitlocker en.wikipedia.org Wikiless Archive.org
[28] [назад] Wikipedia, Evil Maid Attack en.wikipedia.org Wikiless Archive.org
[29] [назад] Wikipedia, Cold Boot Attack en.wikipedia.org Wikiless Archive.org
[30] [назад] CITP 2008 (youtube.com) Invidious
[31] [назад] ResearchGate, Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems researchgate.net Archive.org
[32] [назад] SANS.org, Mission Implausible: Defeating Plausible Deniability with Digital Forensics sans.org Archive.org
[33] [назад] SourceForge, Veracrypt Forum sourceforge.net Archive.org
[34] [назад] Microsoft, BitLocker Countermeasures docs.microsoft.com Archive.org
[35] [назад] SANS, Windows ShellBag Forensics in-depth sans.org Archive.org
[36] [назад] University of York, Forensic data recovery from the Windows Search Database eprints.whiterose.ac.uk Archive.org
[37] [назад] A forensic insight into Windows 10 Jump Lists web.archive.org Archive.org
[38] [назад] Wikipedia, Gatekeeper en.wikipedia.org Wikiless Archive.org
[39] [назад] Alpine Linux Wiki, Setting up a laptop wiki.alpinelinux.org Archive.org
[40] [назад] Wikipedia Veracrypt en.wikipedia.org Wikiless Archive.org
[41] [назад] OSTIF Veracrypt Audit, 2016 web.archive.org
[42] [назад] Veracrypt Documentation, Unencrypted Data in RAM veracrypt.fr Archive.org
[43] [назад] Veracrypt Documentation, Data Leaks veracrypt.fr Archive.org
[44] [назад] Dolos Group, From Stolen Laptop to Inside the Company Network dolosgroup.io Archive.org
[45] [назад] Trammell Hudson's Projects, Understanding TPM Sniffing Attacks trmm.net Archive.org
[46] [назад] Jon Aubrey, attacking laptops that are protected by Microsoft Bitlocker drive encryption twitter.com Nitter
[47] [назад] F-Secure Labs, Sniff, there leaks my BitLocker key labs.f-secure.com Archive.org
[48] [назад] Microsoft, BitLocker Countermeasures, Attacker countermeasures docs.microsoft.com Archive.org
[49] [назад] Wikipedia, Trim en.wikipedia.org Wikiless Archive.org
[50] [назад] Veracrypt Documentation, Trim Operations veracrypt.fr Archive.org
[51] [назад] Veracrypt Documentation, Rescue Disk veracrypt.fr Archive.org
[52] [назад] St Cloud State University, Forensic Research on Solid State Drives using Trim Analysis web.archive.org Archive.org
[53] [назад] WindowsCentral, Trim Tutorial windowscentral.com Archive.org
[54] [назад] Veracrypt Documentation, Trim Operation veracrypt.eu Archive.org
[55] [назад] Black Hat 2018, Perfectly Deniable Steganographic Disk Encryption i.blackhat.com Archive.org

[56] [назад] Milan Broz's Blog, TRIM & dm-crypt ... problems? asalor.blogspot.com Archive.org
[57] [назад] Veracrypt Documentation, Rescue Disk veracrypt.fr Archive.org
[58] [назад] Wikipedia, Virtualbox en.wikipedia.org Wikiless Archive.org
[59] [назад] VirtualBox Ticket 17987 virtualbox.org Archive.org
[60] [назад] Whonix Documentation, Spectre Meltdown whonix.org Archive.org
[61] [назад] Whonix Documentation, Stream Isolation whonix.org Archive.org
[62] [назад] Whonix Documentation, Tunnels Comparison Table whonix.org Archive.org
[63] [назад] Wikipedia, Whonix en.wikipedia.org Wikiless Archive.org
[64] [назад] Oracle Virtualbox Manual, Snapshots docs.oracle.com Archive.org
[65] [назад] Utica College, Forensic Recovery Of Evidence From Deleted Oracle Virtualbox Virtual Machines web.archive.org
[66] [назад] Wikipedia, Spectre en.wikipedia.org Wikiless Archive.org
[67] [назад] Wikipedia, Meltdown en.wikipedia.org Wikiless Archive.org
[68] [назад] Whonix Documentation, Stream Isolation, By Settings whonix.org Archive.org
[69] [назад] Wikipedia, TOTP en.wikipedia.org Wikiless Archive.org
[70] [назад] Wikipedia, Multi-Factor Authentication en.wikipedia.org Wikiless Archive.org
[71] [назад] Whonix Documentation, Bridged Adapters Warning whonix.org Archive.org
[72] [назад] Qubes OS, FAQ, qubes-os.org Archive.org
[73] [назад] Whonix Documentation, Stream Isolation whonix.org Archive.org
[74] [назад] Whonix Documentation, Tunnels Comparison Table whonix.org Archive.org
[75] [назад] Qubes OS Issues, Simulate Hibernation / Suspend-To-Disk (Issue #2414) github.com Archive.org
[76] [назад] Wikipedia, AppArmor en.wikipedia.org Wikiless Archive.org
[77] [назад] Wikipedia, SELinux en.wikipedia.org Wikiless Archive.org
[78] [назад] Wikipedia, TOTP en.wikipedia.org Wikiless Archive.org
[79] [назад] Wikipedia, Multi-Factor Authentication en.wikipedia.org Wikiless Archive.org

Краткое примечание: корреляция и атрибуция

Корреляция — это связь между двумя или несколькими переменными или атрибутами. Как определяется атрибуция? Во время цифровой криминалистики и реагирования на инциденты (DFIR) аналитики обычно ищут индикаторы компрометации (IoC) после событий, требующих их действий. Такие индикаторы обычно состоят из IP-адресов, имён, баз данных; всё это может назначить отдельному человеку или группе определённую поведенческую "метку". Это называется атрибуцией. Один из принципов статистики гласит: "корреляция не подразумевает причинно-следственную связь". Это означает, что, хотя вы можете оставить определённые следы в определённых областях устройства или сети, они показывают только наличие действия, то есть не обязательно именно ваше присутствие. Они не показывают, кто вы; они лишь устанавливают, что что-то произошло и *кто-то* что-то сделал.

Атрибуция нужна, чтобы доказать вину или ответственность, и это главная причина, по которой пользователи сети Tor, заходившие в даркнет, оказывались скомпрометированы: они оставляли следы, которые связывались с их реальными личностями. Ваш IP может быть, но обычно не является, достаточно сильным индикатором для установления вины. Это видно на примере печально известных кибератак NotPetya против США, которые позднее также обрушились на Украину. Хотя Белый дом никогда прямо не *сказал*, что это сделала Россия, атаку приписали российскому (ГРУ), то есть прямому ведомству, в котором размещены российские подразделения кибероперацій с возможностью отрицания причастности[1], в разведывательном сообществе (IC) нечасто называемые "spy makers".

В чём смысл, спросите вы? Если говорить прямо, это отличный пример: NotPetya, которая теперь несомненно считается работой российских кибероперацій против иностранных государств и правительств, всё ещё никогда формально не была приписана России, а только известной группе внутри России (разговорно называемой Cozy Bear), что невозможно ни подтвердить, ни опровергнуть из-за высокой степени разделения внутри структуры российских вооружённых сил. И частично это также связано с усилиями по маскировке под обычное вымогательское ПО, а также с тем, что регулярно использовались серверы взломанных зарубежных ресурсов, не связанных ни с Россией, ни с её внутренними сетями.

Всё это показывает, на какие меры готовы идти государственные акторы. Возможно, вы этого не осознаёте, но иностранные правительства используют техники сокрытия, подобные тем, что обсуждаются в разделах этого руководства. Они регулярно используют Tor и VPN для сокрытия трафика; каждый день применяют взломанные устройства и доступ к украденному оборудованию для кибершпионажа, и с точки зрения судебного эксперта это делает атрибуцию невероятно сложной, если не почти невозможной. Проблема корреляции тривиальна, и её можно решить, просто используя инструменты сокрытия IP, такие как VPN и сеть Tor, но при этом всё равно быть связанным с вашим реальным именем и IP через утечки данных или другие факторы. Если вы внимательно следуете приведённым ниже техникам и навыкам и применяете их, ваши действия будет трудно атрибутировать вам.

[1] [назад] Wikipedia, Plausible Deniability en.wikipedia.org Wikiless Archive.org

Создание ваших анонимных онлайн-личностей

Методология предотвращения анонимности

Если вы часто используете VPN или Tor, вы быстро столкнётесь со множеством CAPTCHA почти повсюду. Довольно часто при использовании Tor или VPN, даже если вам удастся решить все задания (иногда десятки подряд), после решения вам всё равно откажут.

См. gitlab.torproject.org Archive.org

Хотя большинство людей думает, что такие задания сводятся только к решению небольшой головоломки, важно понимать, что всё намного сложнее: современные CAPTCHA используют продвинутое машинное обучение ("Large Language Model" или "LLM", часто ошибочно называемое ИИ) и алгоритмы анализа риска, чтобы проверить, "человек" ли вы; и это часто работает с ошибками. Они могут проверять файлы cookie вашего браузера и историю просмотра с помощью интеллектуальных тактик создания цифрового отпечатка. Они могут отслеживать движения курсора (например, скорость и точность) и использовать алгоритмы, чтобы решить, выглядят ли они "человеческими/органичными". Они могут отслеживать ваше поведение до, во время и после тестов, чтобы убедиться, что вы "человек". Также весьма вероятно, что эти платформы уже могут надёжно идентифицировать вас по уникальному способу взаимодействия с такими заданиями. Это может работать несмотря на сокрытие вашего IP-адреса/браузера и очистку всех cookie.

Посмотрите, например, это выступление DEF CON 25: DEF CON 25 - Svea Eckert, Andreas Dewes - Dark Data Invidious

Вы часто будете получать несколько заданий подряд (иногда бесконечно), а иногда и чрезвычайно сложные задания с чтением неразборчивых символов или определением разных объектов в бесконечных наборах картинок. Их также будет больше, если вы используете систему блокировки рекламы (например, uBlock Origin) или если ваша учётная запись по какой-либо причине уже была помечена за прежнее использование VPN или Tor.

По моему опыту, у вас также будет больше CAPTCHA (Google reCAPTCHA), если вы не используете браузер на основе Chromium. Это можно смягчить, используя браузер на основе Chromium, например Brave. Также есть расширение браузера Buster, которое может помочь с такими заданиями: github.com Archive.org.

Что касается Cloudflare (hCaptcha), можно использовать их решение для доступности здесь (hcaptcha.com Archive.org), которое позволит зарегистрироваться (с анонимной личностью, созданной позже) и установить cookie в вашем браузере, чтобы обходить их CAPTCHA. Другой способ смягчить hCaptcha — использовать их собственное решение "Privacy Pass" privacypass.github.io Archive.org в виде расширения браузера, которое можно установить в браузер вашей виртуальной машины. Это менее рекомендуется, как мы объясним дальше в руководстве, из-за атак по побочным каналам.

Поэтому с такими заданиями следует обращаться осторожно и заставлять себя менять способ их решения (скорость/движения/точность), чтобы предотвратить создание цифрового отпечатка по CAPTCHA.

К счастью, насколько нам известно, пока это официально/публично не используется для деанонимизации людей в интересах третьих сторон.

Чтобы избежать этих проблем, стоит рассмотреть использование VPN поверх Tor. А лучший способ избежать их, вероятно, — использовать самостоятельно размещённый VPN/прокси поверх Tor на VPS-сервере, оплаченном наличными/Monero.

(Иллюстрации Randall Munroe, xkcd.com, лицензия CC BY-NC 2.5)

Captcha[1] означает "Completely Automated Public Turing test to tell Computers and Humans Apart" — это тесты Тьюринга[2], задания, которые нужно выполнить перед доступом к форме/сайту. Чаще всего вы будете встречать их от Google (сервис reCAPTCHA[3]) и Cloudflare (hCaptcha[4]). По их собственным метрикам hCaptcha используется на 15% интернета[5].

Они разработаны, чтобы отделять ботов от людей, но также явно используются для отпугивания анонимных и приватных пользователей от доступа к сервисам.

Если вы часто используете VPN или Tor, вы быстро столкнётесь со множеством CAPTCHA почти повсюду[6]. Довольно часто при использовании Tor, даже если вам удастся решить все задания (иногда десятки подряд), после решения вам всё равно откажут.

См. gitlab.torproject.org Archive.org

Хотя большинство людей думает, что такие задания сводятся только к решению небольшой головоломки, важно понимать, что всё намного сложнее: современные CAPTCHA используют продвинутое машинное обучение и алгоритмы анализа риска, чтобы проверить, человек ли вы[7]:

- Они проверяют ваш браузер, cookie и историю просмотра с помощью создания цифрового отпечатка браузера[8].
- Они отслеживают движения курсора (скорость, точность) и используют алгоритмы, чтобы решить, выглядят ли они "человеческими/органичными".
- Они отслеживают ваше поведение до, во время и после тестов, чтобы убедиться, что вы "человек"[9].

Также весьма вероятно, что эти платформы уже могут надёжно идентифицировать вас по уникальному способу взаимодействия с такими заданиями. Это может работать несмотря на сокрытие вашего IP-адреса/браузера и очистку всех cookie.

Посмотрите, например, это выступление DEF CON 25: DEF CON 25 - Svea Eckert, Andreas Dewes - Dark Data Invidious

Вы часто будете получать несколько заданий подряд (иногда бесконечно), а иногда и чрезвычайно сложные задания с чтением неразборчивых символов или определением разных объектов в бесконечных наборах картинок. CAPTCHA также будет больше, если вы используете систему блокировки рекламы (например, uBlock) или если ваша учётная запись по какой-либо причине уже была помечена за прежнее использование VPN или Tor.

По моему опыту, у вас также будет больше CAPTCHA (Google reCAPTCHA), если вы не используете браузер на основе Chromium. Но это можно смягчить, используя браузеры на основе Chromium, например Brave. Также есть расширение браузера Buster, которое может помочь с этим: github.com Archive.org.

Что касается Cloudflare (hCaptcha), можно использовать их решение Accessibility здесь (hcaptcha.com Archive.org), которое позволит зарегистрироваться (с анонимной личностью, созданной позже) и установить cookie в вашем браузере, чтобы обходить их CAPTCHA. Другой способ смягчить hCaptcha — использовать их собственное решение "Privacy Pass"[10] privacypass.github.io Archive.org в виде расширения браузера, которое можно установить в браузер вашей виртуальной машины.

Поэтому с такими заданиями следует обращаться осторожно и заставлять себя менять способ их решения (скорость/движения/точность/...), чтобы предотвратить "цифровой отпечаток CAPTCHA".

К счастью, насколько нам известно, пока это официально/публично не используется для деанонимизации людей в интересах третьих сторон.

Чтобы избежать этих проблем, стоит рассмотреть использование VPN поверх Tor. А лучший способ избежать их, вероятно, — использовать самостоятельно размещённый VPN/прокси поверх Tor на VPS-сервере, оплаченном наличными/Monero.

Проверка по телефону

Большинство платформ рекламируют проверку по телефону как способ убедиться, что вы человек. Но не обманывайтесь: главная причина проверки по телефону не только в проверке, что вы человек, но и в возможности деанонимизировать вас при необходимости.

Большинство платформ (включая ориентированные на приватность, такие как Signal/Telegram/Proton) потребуют номер телефона для регистрации, а большинство стран теперь обязывают предъявлять удостоверение личности для регистрации[11].

К счастью, это руководство ранее объясняло, как получить номер для таких случаев: Получение анонимного телефонного номера.

Проверка по электронной почте

Проверки по электронной почте раньше было достаточно, но теперь в большинстве случаев этого уже мало. Важно знать, что открытые почтовые провайдеры (например, провайдеры одноразовой почты) помечаются почти так же, как открытые прокси (например, Tor).

Большинство платформ не позволят вам зарегистрироваться с использованием "анонимной" или одноразовой почты. Так же как они не позволят зарегистрироваться с IP-адреса из сети Tor.

Ключевой момент в том, что становится всё сложнее зарегистрировать бесплатную почтовую учётную запись где-либо без предоставления, как вы уже догадались... номера мобильного телефона. Тот же номер мобильного телефона можно удобно использовать, чтобы найти вас в большинстве мест.

Возможно, такие сервисы (например, Proton) потребуют предоставить адрес электронной почты для регистрации. В таком случае мы рекомендуем создать адрес электронной почты у этих провайдеров:

• MailFence: mailfence.com

• Disroot: disroot.org

• Autistici: autistici.org

• Envs.net: envs.net

Имейте в виду, что они не предоставляют архитектуру нулевого доступа (архитектура нулевого доступа — это когда только вы можете получить доступ к своей почте, и даже администраторы сервиса не могут читать ваши сообщения). Это значит, что они могут получить доступ к вашей почте в состоянии хранения в своей базе данных.

> **Примечание о Riseup:** гарантийная канарейка RiseUp была обновлена с опозданием, а в их Twitter появилось загадочное сообщение, будто бы говорящее не доверять им. Из-за подозрительного характера этого твита это руководство больше не может их рекомендовать.

Также см.: forums.whonix.org

Для riseup.net Tor Mirror (до моего сведения дошло, что теперь сайт, к сожалению, требует приглашение от уже зарегистрированного пользователя)

Сервисы почтовых псевдонимов

Если вы хотите не сообщать свои анонимные адреса электронной почты разным сторонам, мы настоятельно предлагаем рассмотреть сервисы почтовых псевдонимов, такие как:

- simplelogin.io (предпочтительный первый выбор из-за большего числа возможностей на бесплатном уровне)
- anonaddy.com

Эти сервисы позволяют создавать случайные псевдонимы для вашей анонимной почты (например, на Proton) и могут повысить вашу общую приватность, если вы не хотите раскрывать эту почту ни для каких целей. Оба рекомендованы Privacyguides.org и Privacytools.io. Я тоже их рекомендую.

Проверка сведений пользователя

Очевидно, Reddit этого (пока) не делает, но Facebook, скорее всего, делает и будет искать "подозрительные" вещи в ваших сведениях (что может включать распознавание лица).

Некоторые примеры:

- IP-адрес из страны, отличной от страны в вашем профиле.
- Возраст в профиле не соответствует возрасту на фотографии.
- Этническая принадлежность в профиле не соответствует этнической принадлежности на фотографии.
- Язык не соответствует языку страны.
- Неизвестность в чужих контактах (то есть никто другой вас не знает).
- Закрытие настроек приватности сразу после регистрации.
- Имя не соответствует правильной этнической принадлежности/языку/стране?

Проверка удостоверения личности

В большинстве случаев это решающий барьер. Насколько нам известно, только Facebook и LinkedIn (за пределами финансовых сервисов) запрашивали такие проверки, включающие отправку фотографий какого-либо удостоверения личности (паспорт, национальная ID-карта, водительское удостоверение...). Единственный способ сделать это потребовал бы создания поддельных официальных документов (подделка) с использованием приличных навыков Photoshop, и во многих местах это может быть незаконно.

Поэтому это черта, которую мы не будем помогать вам пересекать в этом руководстве. Некоторые сервисы предлагают такие услуги в интернете, но мы считаем их *недобросовестными участниками* и полагаем, что они переходят границы.

Во многих странах только правоохранительные органы, некоторые специальные процедуры (например, запросы GDPR) и некоторые хорошо регулируемые финансовые сервисы могут запрашивать подтверждение личности. Поэтому законность требования таких документов спорна, и мы считаем, что таким платформам не должно быть разрешено требовать их.

В некоторых странах (например, в Германии) такая практика незаконна, и онлайн-платформы вроде Facebook или LinkedIn юридически обязаны позволять вам использовать псевдоним и оставаться анонимным.

IP-фильтры

Как уже говорилось ранее в этом руководстве, многие платформы применяют фильтрацию по IP. Выходные узлы Tor публично перечислены, а выходные серверы VPN "хорошо известны". Существует множество коммерческих и бесплатных сервисов, позволяющих легко блокировать такие IP (привет, Cloudflare).

Операторы и администраторы многих платформ не хотят трафика с этих IP, поскольку он часто приносит на их платформы много незаконного/вредоносного/невыгодного трафика. Обычно эти платформы используют один из следующих аргументов:

- "Подумайте о детях!";
- "Терроризм!";
- "Российская тролльская пропаганда!";
- "Ну, это шум в данных, которые мы продаём рекламодателям!" (например, AdSense или Facebook Ads).

"Но мы всё равно платим за их трафик, так что давайте просто запретим их всех."

К счастью, эти системы несовершенны, и вы всё ещё сможете обходить такие ограничения, меняя личности (в случае Tor) и каждый раз пытаясь открыть сайт, пока не найдёте выходной узел, который ещё не внесён в чёрный список.

Некоторые платформы позволят войти с IP Tor, но не зарегистрироваться (см. gitlab.torproject.org Archive.org). Такие платформы будут хранить удобный постоянный журнал IP, который вы использовали при регистрации, а некоторые будут хранить такие журналы бессрочно, например все IP, с которых вы входили (привет, Facebook).

Терпимость к VPN намного выше, поскольку они не считаются "открытыми прокси", но это не помешает многим платформам усложнять их использование, заставляя большинство пользователей VPN проходить всё более трудные CAPTCHA.

По этой причине это руководство в определённых случаях рекомендует использовать VPN поверх Tor (а не Tor поверх VPN). **Помните, что лучший способ избежать таких проблем — использовать самостоятельно размещённый VPN/прокси поверх Tor на VPS, оплаченном наличными/Monero**.

Цифровые отпечатки браузера и устройства

Цифровые отпечатки вашего браузера и устройства[12] — это набор свойств/возможностей вашей системы/браузера. Они используются на большинстве сайтов для невидимого отслеживания пользователей, а также для адаптации пользовательского опыта сайта под их браузер. Например, сайты смогут предоставить "мобильный опыт", если вы используете мобильный браузер, или предложить конкретную языковую/географическую версию в зависимости от вашего цифрового отпечатка. Большинство таких техник работает с современными браузерами, например браузерами на основе Chromium[13] (Chrome/Edge) или Firefox[14], если не принять специальные меры. Создание цифровых отпечатков браузера и устройства[12] обычно встроено в сервисы CAPTCHA, но также встречается в разных других сервисах.

Многие платформы (например, Google[15]) будут проверять ваш браузер на разные возможности и настройки и блокировать браузеры, которые им не нравятся. Это одна из причин, по которой мы рекомендуем использовать в этой виртуальной машине браузеры на основе Chromium, например Brave Browser, а не Tor Browser.

Также стоит отметить, что, хотя некоторые браузеры и расширения предлагают сопротивление созданию цифровых отпечатков, само это сопротивление тоже может использоваться для создания вашего цифрового отпечатка, как объяснено здесь: palant.info Archive.org

Это руководство будет смягчать эти проблемы, случайным образом меняя или скрывая многие такие идентификаторы цифрового отпечатка с помощью:

• Использования виртуализации (см. Виртуализация);

• Использования конкретных рекомендаций (см. Дополнительные меры предосторожности для браузера с включённым JavaScript);

• Использования усиления Усиление браузеров;

• и использования браузеров, устойчивых к созданию цифровых отпечатков (например, Brave или Tor Browser).

Вот некоторые вещи, которые они проверяют в современных браузерах:

• User-Agent: имя и версия вашего браузера.

• HTTP_ACCEPT Headers: тип содержимого, который ваш браузер может обрабатывать.

• Time Zone and Time Zone Offset: ваш часовой пояс.

• Screen Size and Color Depth: разрешение вашего экрана.

• System Fonts: шрифты, установленные в вашей системе.

• Cookies support: поддерживает ли ваш браузер cookie.

• Hash of Canvas fingerprint and Hash of WebGL fingerprint: уникальные идентификаторы, создаваемые на основе возможностей графического отображения.

• WebGL Vendor & Renderer: название вашей видеокарты.

• Do-Not-Track enabled or not: да, они могут использовать сведения DNT, чтобы отслеживать вас.

• Language: язык вашего браузера.

• Platform: операционная система, которую вы используете.

• Touch Support: поддерживает ли ваша система сенсорный ввод (например, телефон/планшет или ноутбук с сенсорным экраном).

• Ad Blocking use: блокирует ли ваш браузер рекламу.

• AudioContext fingerprint: подобно Canvas и WebGL, это создаёт цифровой отпечаток ваших звуковых возможностей.

• CPU: какой у вас процессор и сколько их.

• Memory: сколько памяти в вашей системе.

• Browser Permissions: разрешает ли ваш браузер некоторые вещи, например доступ к данным о местоположении или к микрофону/веб-камере.

К сожалению, чаще всего эти цифровые отпечатки будут уникальны или почти уникальны для вашего браузера/системы. Это означает, что даже если вы выйдете с сайта, а затем войдёте снова под другим именем пользователя, ваш цифровой отпечаток может остаться тем же, если вы не приняли меры предосторожности. Противник может использовать такие цифровые отпечатки, чтобы отслеживать вас на разных сервисах, даже если у вас нет учётной записи ни на одном из них и вы используете блокировку рекламы. Эти цифровые отпечатки, в свою очередь, могут использоваться для деанонимизации, если вы сохраняете один и тот же отпечаток между сервисами.

Вот сервисы, с помощью которых можно проверить цифровые отпечатки браузера:

• abrahamjuliot.github.io (вероятно, лучший в целом)

• coveryourtracks.eff.org

• amiunique.org

• browserleaks.com

• deviceinfo.me

• (только браузеры на основе Chromium) z0ccc.github.io

Скорее всего, вы обнаружите, что цифровой отпечаток вашего браузера уникален, что бы вы ни делали.

Взаимодействие с человеком

Некоторые платформы добавляют это как дополнительный шаг и требуют реального взаимодействия с представителем службы поддержки. Обычно по электронной почте, но иногда через чат/телефон. Они захотят проверить, что вы существуете, попросив вас ответить на письмо/сообщение/звонок.

Это раздражает, но в нашем случае с этим довольно легко справиться. Мы не создаём ботов. Это руководство для людей, создающих человеческие учётные записи.

Модерация пользователями

Многие платформы делегируют модерацию других пользователей и их содержимого самим пользователям и полагаются на них. Это функции "report", которые вы найдёте на большинстве платформ.

Тысячи жалоб не имеют значения, если вы Donald Trump или Kim Kardashian, но если на вас, одиночного "без друзей" анонимного пользователя, пожалуются хотя бы один раз, вас могут мгновенно приостановить/пометить/заблокировать.

Поведенческий анализ

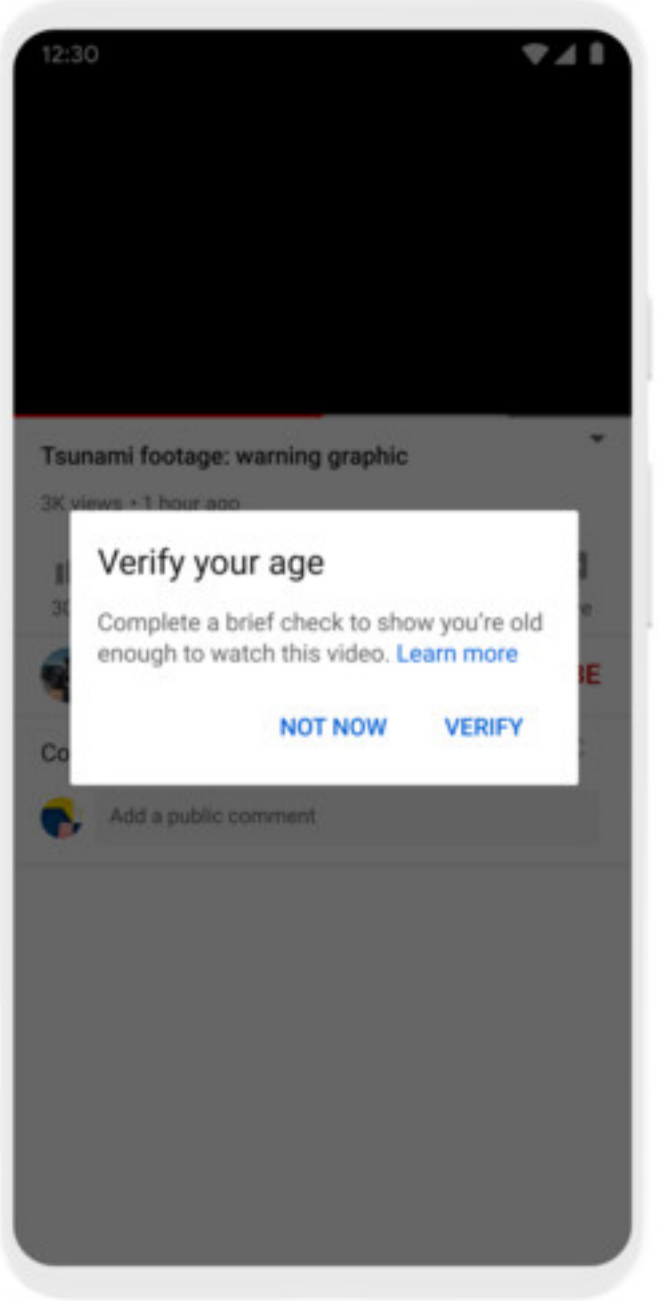
См. Ваш цифровой след.

Финансовые транзакции

Просто и эффективно: некоторые платформы требуют выполнить финансовую транзакцию для проверки учётной записи, иногда под предлогом проверки возраста. Это может быть проверка кредитной карты или чрезвычайно небольшой банковский перевод. Некоторые примут пожертвование в основной криптовалюте вроде Bitcoin или Ethereum.

Хотя это может казаться безобидным, очевидно, что это метод проверки личности и деанонимизации. Он просто косвенно опирается на сторонние финансовые правила KYC[16].

Например, теперь это относится к YouTube для некоторых европейских пользователей[17], но также используется сервисами вроде Amazon, где для создания учётной записи нужен действительный способ оплаты.


12:30
Tsunami footage: warning graphic
Verify your age
Complete a brief check to show you're old enough to watch this video. Learn more
NOT NOW
VERIFY
Add a public comment

Вход через другую платформу

"Зачем самим проверять этого пользователя, если можно попросить других разобраться с этим?"

Вы это заметите и, вероятно, уже сталкивались с этим. Некоторые приложения/платформы попросят или потребуют войти через известную и широко используемую авторитетную платформу вместо собственной системы (Sign-in with Google/Facebook/Apple/Twitter).

Этот вариант часто представлен как "вариант по умолчанию", а "Sign-in with e-mail and password" спрятан с помощью хитрых тёмных паттернов[18] и, к сожалению, иногда необходим.

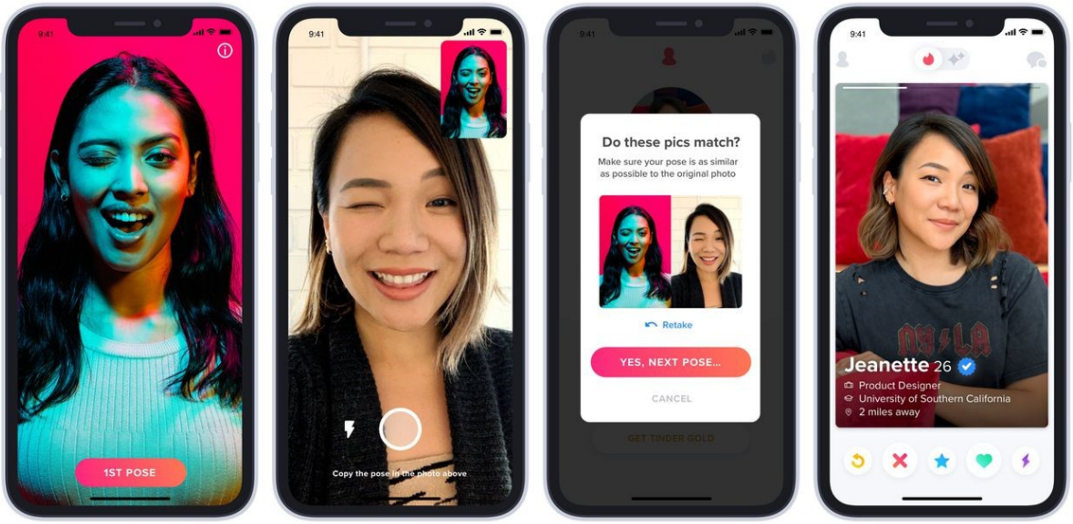
Этот метод делегирует процесс проверки таким платформам вместо предположения, что вам не удастся легко создать анонимную учётную запись Google/Facebook/Apple/Twitter.

К счастью, на сегодняшний день это всё ещё возможно.

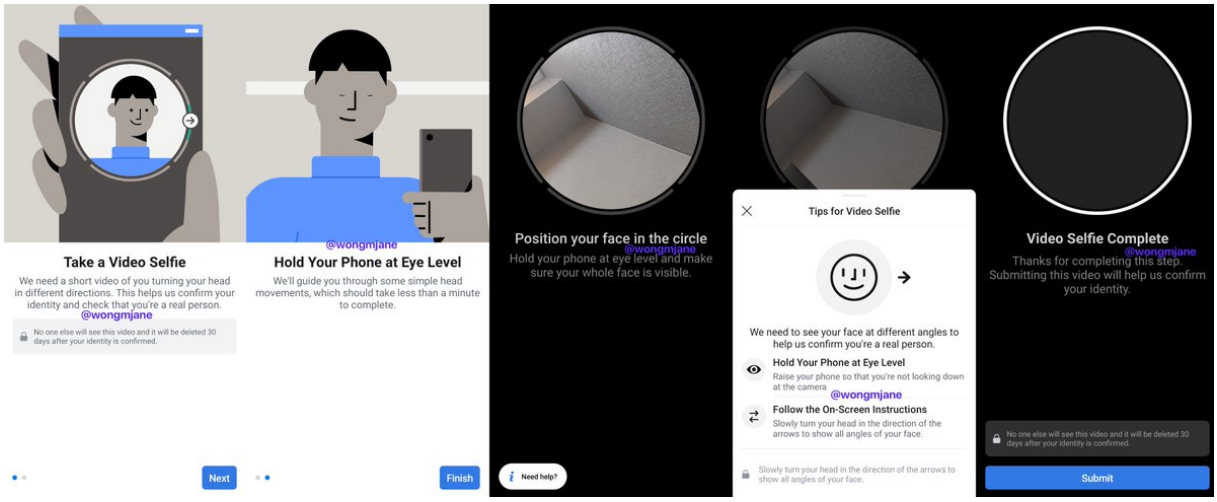
Распознавание лица и биометрия

Это распространённый метод на некоторых криптовалютных торговых платформах и в некоторых приложениях для знакомств.

Некоторые платформы/приложения потребуют сделать живую фотографию себя либо за каким-то действием (подмигивание, поднятая рука...), либо с показом специальной информации (рукописный текст, паспорт или удостоверение личности) на фотографии. Иногда платформа/приложение потребует несколько фотографий, чтобы повысить уверенность.



Это руководство (пока) не рассматривает этот способ, поскольку он в основном используется на финансовых платформах (которые всё равно смогут идентифицировать вас другими средствами) и в некоторых приложениях для знакомств вроде Tinder[19]. К сожалению, этот метод теперь также иногда используется Facebook[20] и Instagram как часть их методов проверки (хотя пока мы с ним ещё не сталкивались).



В некоторых случаях эти проверки нужно проходить со смартфона и с помощью камеры "внутри приложения", чтобы вы не могли отправить ранее сохранённое (отредактированное) изображение.

Недавно даже такие платформы, как PornHub, решили внедрить похожие меры в будущем[21].

Эту проверку чрезвычайно трудно обойти, но возможно. Один из способов потенциально обойти её — использовать технологию "deep fake", например открытое ПО FaceSwap github.com Archive.org, чтобы создать необходимые проверочные фотографии с помощью случайно сгенерированного компьютером лица, наложенного на фотографию согласившейся модели (или стоковое фото).

К сожалению, некоторые приложения требуют прямой доступ к камере смартфона для обработки проверки. В таком случае вам нужно найти способ выполнять такие "замены лица" на лету с помощью фильтра и каким-то образом подать результат в камеру, используемую приложением. Возможный подход похож на этот впечатляющий проект: github.com Archive.org.

Ручные проверки

Они могут быть вызваны любым из перечисленного выше и просто означают, что кто-то (обычно специализированные сотрудники) вручную проверит ваш профиль и решит, настоящий он или нет, исходя из своего субъективного мнения.

В некоторых странах даже разработаны горячие линии, куда можно сообщать о любом подрывном содержимом[22].

Плюсы: обычно такой вердикт "окончательный", и вы, вероятно, избежите дальнейших проблем, если всё хорошо.

Минусы: обычно такой вердикт "окончательный", и вас, вероятно, заблокируют без возможности апелляции, если всё плохо. Иногда такие проверки заканчиваются тем, что платформа просто игнорирует вас и отменяет без какой-либо причины. Любая апелляция останется без ответа, будет проигнорирована или приведёт к случайной ошибке тёмного паттерна при попытке обжаловать именно эту личность (например, это происходит в Instagram: если вашу учётную запись "приостанавливают", очевидно после ручной проверки, попытка заполнить форму апелляции просто выдаёт ошибку и просит попробовать позже; мы пытаемся подать одну и ту же апелляцию для этой личности уже как минимум последние 6 месяцев).

Выход в сеть

Теперь, когда у вас есть базовое понимание всех способов, которыми вас могут деанонимизировать, отслеживать и проверять, начнём обходить их, оставаясь анонимными. Помните:

• Нельзя доверять интернет-провайдерам.

• Нельзя доверять VPS-провайдерам.

• Нельзя доверять провайдерам публичного Wi-Fi.

• Нельзя доверять операторам мобильной связи.

• Нельзя доверять VPN-провайдерам.

• Нельзя доверять никакой онлайн-платформе.

• Нельзя доверять Tor.

• Нельзя доверять вашей операционной системе.

• Нельзя доверять вашему ноутбуку.

• Нельзя доверять вашему смартфону (особенно Android).

• Нельзя доверять вашим умным устройствам.

• Прежде всего, нельзя доверять людям.

И что теперь? Вместо того чтобы не доверять никому и ничему, мы советуем "доверяй, но проверяй"[23] (или "никогда не доверяй, всегда проверяй", если вы настроены жёстче и хотите применять безопасность с нулевым доверием[24]).

Не начинайте этот процесс, если:

- **Вы не сверились с местными законами на предмет соблюдения требований и законности ваших действий.**
- **Вы не понимаете свою модель угроз.**
- **Вы не находитесь в безопасном месте с публичным Wi-Fi, без смартфона или другого умного устройства при себе. И желательно в месте, где вас не снимают камеры видеонаблюдения (помните о поиске безопасных мест с приличным публичным Wi-Fi и использовании дальнобойной антенны для подключения к публичным Wi-Fi с безопасного расстояния)**
- **Вы не завершили полностью подготовку одного из маршрутов.**
- **Ещё раз: крайне важно понимать, что вы не сможете создать большинство учётных записей без действительного номера телефона. Поэтому большая часть вашей анонимности на массовых платформах зависит от анонимности вашего онлайн-номера телефона и/или одноразового телефона с предоплаченной SIM-картой (если вы используете такой вариант). Если ваш номер телефона не анонимен или ваш одноразовый телефон можно связать с вами, вас можно деанонимизировать. Если вы не можете получить такой анонимный номер телефона и/или физическую SIM с одноразовым телефоном, вам придётся ограничиться платформами, которые не требуют проверки по номеру телефона.**

Не забудьте посмотреть Предупреждение о смартфонах и умных устройствах

Создание новых личностей

Это самая увлекательная часть: теперь вы будете создавать свои личности из воздуха. Эти личности не существуют, но должны быть правдоподобными и выглядеть "органично". В идеале у них должна быть история, "легенда" (да, это настоящий термин[25]).

Что такое легенда? Это полная предыстория вашего персонажа:

• Возраст

• Пол

• Гендер

• Этническая принадлежность

• Место и дата рождения

• Место проживания

• Страна происхождения

• Посещённые страны (например, для путешествий)

• Интересы и хобби

• История образования

• Опыт работы

• Сведения о здоровье

• Религия, если есть

• Цели

• Семейная история

• Состав семьи, если есть (дети? супруга? супруг?)

• Семейное положение, если есть (в браке? одиноки?)

• Языки, на которых говорит

• Черты личности (интроверт, экстраверт...)

• ...

Всё это нужно тщательно продумывать для каждой отдельной личности, и вы должны невероятно аккуратно придерживаться деталей каждой легенды при использовании этих личностей. Не должно утечь ничего, что может привести к вашей настоящей личности. Не должно утечь ничего, что может нарушить согласованность вашей легенды. Всё всегда должно быть согласованным.

Инструменты, которые могут с этим помочь:

• fakenamegenerator.com

• thispersondoesnotexist.com

• generated.photos (**сгенерированные этим инструментом изображения имеют водяной знак, который может понадобиться удалить с помощью редактора изображений, например Gimp**)
  • **Предупреждение:** для работы этому инструменту нужен JavaScript, и он активно создаёт цифровые отпечатки. Большая часть этого отправляется в Microsoft Clarity. Даже с установленным uBlock и на более безопасном уровне Tor Browser неэффективно блокировал создание цифровых отпечатков. На самом безопасном уровне это, очевидно, не

работает. В наших тестах только Brave с агрессивной защитой от цифровых отпечатков/рекламы не отправлял аналитику.

Сейчас также тот момент, когда можно наконец рассмотреть получение онлайн-номера телефона, как объяснено в разделе Онлайн-номер телефона.

Мы немного поможем вам, перечислив несколько советов, которые усвоили за годы исследований **(отказ от ответственности: это основано только на моём личном опыте)**:

• "Некоторые животные равнее других".

  • Этническая принадлежность важна, и у вас будет меньше проблем и меньше внимания со стороны алгоритмов проверки, если ваша личность кавказская/восточноазиатская, чем если она арабская/чёрная (да, мы тщательно это тестировали, и это определённо проблема).

  • Возраст важен, и у вас будет меньше проблем, если вы молоды (18-22), чем если вы среднего возраста или старше. Платформы, похоже, мягче относятся к новым молодым аудиториям и реже накладывают ограничения.

  • Пол/гендер важен, и у вас будет меньше проблем, если вы женщина, чем если вы мужчина.

  • Страна происхождения важна, и у вас будет меньше проблем, если ваша личность норвежская, чем если она украинская, нигерийская или мексиканская.

  • Страна проживания важна, и у вас будет меньше проблем, если ваша личность живёт в Осло или Париже, чем если вы решите поселить её в Киеве или Каире.

  • Язык важен, и у вас будет меньше проблем, если вы говорите по-английски или на языке вашей личности, чем если используете несвязанный язык. Не создавайте 20-летнюю женщину арабского происхождения, родившуюся в Норвегии, которая говорит по-украински или по-арабски.

• Личности, являющиеся "резидентами ЕС" с "IP ЕС" (выходной IP VPN/Tor), на многих платформах получат преимущества защиты GDPR. Остальные нет. GDPR в большинстве случаев ваш друг, и это следует учитывать.

• Аналогично, географическое положение исходного IP (ваш IP/местоположение при заходе на "whatsmyipaddress.com") должно как можно лучше соответствовать местоположению вашей личности. При использовании VPN поверх Tor это можно выбрать в VPN-клиенте, если вы используете подход VPN поверх Tor, либо просто создать новую личность в Tor Browser или Brave Tor Tab, пока не получите подходящий выходной узел, либо настроить Tor на ограничение выходных узлов. Рассмотрите исключение любых выходных IP, расположенных не в Западной Европе/США/Канаде/Японии/Южной Корее/Австралии/Новой Зеландии, поскольку с ними у вас будет меньше проблем. В идеале стоит получить IP Европейского союза для дополнительной защиты GDPR и, если возможно, немецкий выходной IP из-за их правовой позиции по использованию анонимных учётных записей на онлайн-платформах.

• Brave Browser (на основе Chromium) с Private Tor Tab имеет более высокий уровень принятия, чем Tor Browser (на основе Firefox). У вас будет меньше проблем с CAPTCHA и онлайн-платформами[15], если вы используете Brave, а не Tor Browser (можете проверить это сами).

• Для каждой личности нужно иметь соответствующую фотографию профиля. Для этой цели мы рекомендуем просто зайти на thispersondoesnotexist.com или generated.photos и сгенерировать компьютерную фотографию профиля (учтите, что уже разработаны алгоритмы[26][27] для обнаружения таких изображений, и это может работать не в 100% случаев). Также можно сгенерировать такие изображения самостоятельно на своём компьютере, если хотите, используя открытый проект StyleGan здесь: github.com Archive.org. Просто обновляйте

страницу, пока не найдёте изображение, которое соответствует вашей личности по всем параметрам (возраст, пол и этническая принадлежность), и сохраните его. Было бы ещё лучше иметь несколько фотографий, связанных с этой личностью, но пока у нас нет "простого способа" сделать это.

Предупреждение: generated.photos требует JavaScript для работы и активно создаёт цифровые отпечатки. Большая часть этого отправляется в Microsoft Clarity. Даже с установленным uBlock и на более безопасном уровне Tor Browser неэффективно блокировал создание цифровых отпечатков. На самом безопасном уровне это, очевидно, не работает. В наших тестах только Brave с агрессивной защитой от цифровых отпечатков/рекламы не отправлял аналитику.

• **Бонус:** можно сделать изображение более реалистичным, используя этот сервис (с анонимной личностью) myheritage.com Archive.org. Вот пример:

• Оригинал:

• Результат (смотрите онлайн, потому что PDF плохо работает со встроенными медиа):

Небольшая проблема: **MyHeritage.com блокирует выходные узлы Tor, так что для этого вам снова может понадобиться VPN поверх Tor.**

Того же результата можно добиться без MyHeritage, сделав это самостоятельно, например с помощью github.com Archive.org, но это потребует больше ручных действий (**и требует NVIDIA GPU**). Скоро появятся и другие коммерческие продукты, например d-id.com Archive.org, с примерами здесь: youtube.com Invidious.

Примечание: если вы делаете несколько изображений одной и той же личности с помощью некоторых инструментов выше, обязательно сравните сходство с помощью инструмента Microsoft Azure Face Verification: azure.microsoft.com.

- Заранее создайте и сохраните в KeePassXC сведения каждой личности, включая специально продуманные детали, упомянутые ранее.
- Не выбирайте должность в известной частной корпорации/компании, поскольку в их HR-отделах есть люди, отслеживающие активность на платформах вроде LinkedIn, и они сообщат о вашем профиле как о поддельном, если он не соответствует их базе данных. Вместо этого выберите работу фрилансером или в крупном публичном учреждении, где из-за децентрализованной природы будет меньше внимания.

• Отслеживайте (записывайте) предыстории ваших личностей. Везде нужно использовать одни и те же даты и ответы. Всё всегда должно совпадать. Даже истории, которые вы рассказываете о своей воображаемой жизни, всегда должны совпадать. Если однажды вы скажете, что работаете стажёром в Department of Health, а позже на другой платформе скажете, что работаете стажёром в Department of Transportation, люди могут усомниться в вашей личности. Будьте последовательны.

• Используйте отдельный номер телефона для каждой личности. Онлайн-платформы отслеживают использование номеров телефонов, и если одна личность/номер будет помечена за нарушение Community Guidelines или Terms of Services, другие личности, использующие тот же номер, тоже могут быть помечены/заблокированы.

• Адаптируйте язык/письмо под личность, чтобы не вызывать подозрений и снизить вероятность создания вашего цифрового отпечатка онлайн-платформами. Будьте особенно осторожны с педантичными словами, оборотами речи и цитатами, по которым кто-то может догадаться, что ваш стиль письма очень похож на человека с таким-то именем в Twitter или пользователя Reddit. См. Противодействие судебной лингвистике.

• **Всегда используйте TOTP 2FA (не SMS, чтобы предотвратить атаки подмены SIM[28] и сохранить работоспособность личности после истечения срока вашей предоплаченной карты), используя KeePassXC, когда это доступно, чтобы защитить входы на разные платформы.**

• Помните Рекомендации по паролям и парольным фразам.

Вот также хорошее руководство по этой конкретной теме: gendersec.tacticaltech.org Archive.org

Примечание: если у вас проблемы с поиском выходного узла в нужной стране, можно принудительно использовать определённые страны для выходных узлов (и, следовательно, выходные страны) в Tor, изменив файл torrc на Whonix Gateway или даже в Tor Browser:

• Whonix/Tails: создайте/измените файл `/usr/local/etc/torrc.d/50_user.conf`[29].

• В Tor Browser: измените файл torrc, расположенный в `Browser/TorBrowser/Data/Tor`[30].

Оказавшись в файле, можно сделать следующее:

• Указать выходные узлы, добавив эти две строки (это потребует выходной узел в Китае/России/Украине):

  • `ExitNodes {CH},{RU},{UA}`

  • `StrictNodes 1`

• Исключить определённые выходные узлы, добавив эту строку (она исключит все выходные узлы из Франции/Германии/США/Великобритании):

  • `ExcludeNodes {FR},{DE},{US},{UK}`

Всегда используйте прописные буквы для любых настроек.

Учтите, что это ограничивает луковую маршрутизацию и может снизить вашу анонимность, если ограничения слишком жёсткие. Визуализированный список доступных выходных узлов можно посмотреть здесь: bigdatacloud.com Archive.org

Вот список возможностей (это общий список, и во многих из этих стран выходных узлов может не быть вообще): web.archive.org

Проверка, насколько плох ваш выходной узел Tor

Пропустите это, если используете VPN/прокси поверх Tor (хотя при желании можно выполнить те же проверки с выходным узлом VPN).

Не все выходные узлы Tor одинаковы. В основном это зависит от того, какую "exit policy" применяет их оператор. Некоторые выходные узлы Tor считаются более или менее "чистыми" и будут появляться только в списках выходных узлов Tor. Другие выходные узлы Tor считаются "грязными" и будут появляться в десятках разных чёрных списков. Как понять, на чистом вы узле или на плохом? Это не так просто.

Этот процесс очень лёгкий.

Он работает независимо от того, используете ли вы Tor Browser в основной ОС, в виртуальной машине, с Whonix или Qubes OS.

• Откройте в одной вкладке целевой сайт, на котором хотите зарегистрироваться.

• Нажмите значок Tor Circuit слева от значка "замка" в верхнем левом углу, чтобы увидеть ваш маршрут через сеть Tor.

• Посмотрите третий IP (Exit IP), который вы используете в этой вкладке для этого сайта. (IP-адрес нельзя скопировать, но при необходимости можно набрать его в адресной строке браузера.)

• Откройте новую вкладку и перейдите на MX Toolbox: mxtoolbox.com

• Введите Exit IP из первой вкладки в поле поиска. Скорее всего, вы увидите: "We notice you are on a blacklist."

• Проверьте, в скольких чёрных списках находится выходной узел Tor. В идеале он должен быть только в двух. Если он есть в других списках, например Spamhaus ZEN, у вас могут возникнуть проблемы:

  • DAN TOR

  • DAN TOREXIT

Если выходной узел "чистый" (в небольшом числе списков), вернитесь к первой вкладке и откройте сайт, который хотите использовать для регистрации.

Система настоящих имён

К сожалению, неиспользование вашей настоящей личности противоречит Условиям обслуживания ("TOS") многих сервисов, особенно принадлежащих Microsoft и Facebook. Но не отчаивайтесь: как объяснено в Требованиях, это всё ещё законно в Германии, где суды подтвердили законность неиспользования настоящих имён на онлайн-платформах (§13 VI German Telemedia Act of 2007[31][32]). **К счастью, ToS не могут отменять законы (пока)**.

Это не значит, что в других местах это незаконно; это значит, что если закон не на вашей стороне, это может быть нарушением их TOS. **Помните: это руководство одобряет такой подход только для немцев, проживающих в Германии.**

Со своей стороны мы решительно осуждаем такой тип политики настоящих имён. См., например, эту статью Wikipedia с некоторыми примерами: en.wikipedia.org Wikiless Archive.org

Вот ещё несколько источников по немецкому случаю:

• slate.com Archive.org

• theverge.com Archive.org

• pcmag.com Archive.org

• vzbv.de Archive.org

• pcmag.com Archive.org

• reuters.com Archive.org

Или вы можете быть совершеннолетним жителем любой другой страны, где можете самостоятельно подтвердить и проверить законность этого. Повторим: это не юридическая консультация, и мы не юристы. **Делайте это на свой риск.**

Другие страны, где это было признано незаконным:

• Южная Корея (см. en.wikipedia.org Wikiless Archive.org)

• Если вы знаете другие, пожалуйста, сообщите нам со ссылками в GitHub issues.

Некоторые платформы полностью обходят это требование, вместо этого требуя действительный способ оплаты (см. Финансовые транзакции). Хотя формально через ToS это напрямую не требует настоящего имени, результат тот же, поскольку они обычно принимают только массовые (не Monero/наличные) способы оплаты (например, Visa/MasterCard/Maestro или PayPal), которые юридически требуют настоящего имени в рамках правил KYC[16]. Результат тот же и даже эффективнее, чем простая политика настоящих имён, которую в некоторых странах, например Германии, можно было бы игнорировать.

О платных сервисах

Если вы собираетесь использовать платные сервисы, отдавайте предпочтение тем, которые принимают оплату наличными или Monero, что можно сделать напрямую и безопасно, сохраняя анонимность.

Если сервис, который вы собираетесь купить, не принимает их, но принимает Bitcoin (BTC), рассмотрите следующее приложение: Анонимная онлайн-оплата BTC (или любой другой криптовалютой).

Этот раздел покажет обзор текущих разных требований на некоторых платформах:

- **Рассмотрите использование рекомендуемых инструментов на privacyguides.orgArchive.orgдля лучшей приватности вместо обычных массовых инструментов.**
- **Также рассмотрите использование рекомендуемых инструментов на whonix.orgArchive.orgвместо обычных массовых инструментов, например почтовых провайдеров: whonix.orgArchive.orgСледующий обзор не описывает практики приватности этих платформ, а только их требования для регистрации учётной записи. Если хотите использовать инструменты и платформы, учитывающие приватность, перейдите на privacyguides.orgArchive.org.**

Легенда:

• "Unclear": неясно из-за нехватки информации или противоречивых сведений.

• "Maybe": это случалось в меньшинстве моих тестов.

• "Likely": это случалось в большинстве моих тестов.

• "Yes" или "No": это либо происходило, либо систематически не происходило во всех моих тестах.

• "Easy": общий опыт был прямолинейным, с минимальными препятствиями или без них.

• "Medium": общий опыт включает некоторые препятствия, но всё ещё осуществим без слишком больших трудностей.

• "Hard": общий опыт — болезненная борьба со множеством препятствий.

• "N/A": неприменимо, потому что это невозможно было протестировать в контексте этого руководства.

• "Indirectly": это означает, что что-то требуется, но косвенно через стороннюю систему (например, финансовый KYC).

• **См. Система настоящих имён для важной информации. Подробности ниже.**

Ниже приведён список "проблемных сервисов". Если сервиса нет ниже, значит, с ним вообще нет проблем ни по одному пункту (например, Briar).

Amazon

• Противоречит ли это их ToS? Нет, но да amazon.com Archive.org

"1. Amazon Services, Amazon Software

A. Use of Amazon Services on a Product. To use certain Amazon Services on a Product, you must have your own Amazon.com account, be logged in to your account on the Product, **and have a valid payment method associated with your account.** "

Хотя технически это не требует настоящего имени, это требует действительный способ оплаты. К сожалению, они не принимают "наличные" или "Monero" как способ оплаты. Поэтому вместо этого они опираются на финансовый KYC (где политика настоящего имени практически везде принудительна).

• Потребуют ли они номер телефона? Да, но см. ниже

• Можно ли создать учётную запись через Tor? Да, но см. ниже

Из-за требования действительного способа оплаты мы не смогли это протестировать. Хотя, похоже, это не противоречит их ToS, в контексте этого руководства это невозможно, если только вам не удастся анонимно получить действительный платёжный метод с KYC, что, насколько мне известно, почти невозможно или крайне трудно.

Так что, насколько мне известно, создать анонимную учётную запись Amazon невозможно.

Apple

• Противоречит ли это их ToS? Да apple.com Archive.org

"IV. Your Use of the Service

A. Your Account

In order to use the Service, you must enter your Apple ID and password to authenticate your Account**. You agree to provide accurate and complete information when you register with, and as you use, the Service ("Service Registration Data"), and you agree to update your Service Registration Data to keep it accurate and complete".**

• Потребуют ли они номер телефона? Да

• Можно ли создать учётную запись через Tor? Да

Учтите, что эта учётная запись не позволит настроить почтовую учётную запись Apple. Для этого понадобится устройство Apple.

Binance

• Противоречит ли это их ToS? Да binance.com Archive.org

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта

• Можно ли создать учётную запись через Tor? Нет

Discord

• Противоречит ли это их ToS? Нет discord.com Archive.org

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта

• Можно ли создать учётную запись через Tor? Пока у нас не было с этим проблем при использовании настольного клиента

При использовании веб-клиента у вас может быть больше проблем (CAPTCHA). Особенно с Tor Browser.

Я предлагаю использовать приложение Discord Client в виртуальной машине через Tor или, в идеале, через VPN/прокси поверх Tor, чтобы смягчить такие проблемы.

Element

• Противоречит ли это их ToS? Нет element.io Archive.org

• Потребуют ли они номер телефона? Нет, им даже не нужна электронная почта

• Можно ли создать учётную запись через Tor? Да

Ожидайте несколько CAPTCHA при создании учётной записи на некоторых homeserver.

Facebook

• Противоречит ли это их ToS? Да facebook.com Archive.org

"1. Who can use Facebook

When people stand behind their opinions and actions, our community is safer and more accountable. For this reason, you must:

• Use the same name that you use in everyday life.

• Provide accurate information about yourself.

• Потребуют ли они номер телефона? Да, и, вероятно, позже потребуют больше

• Можно ли создать учётную запись через Tor? Да, но это очень трудно, и их onion-адрес[33] не поможет. В большинстве случаев вы просто получите случайную ошибку при регистрации, а после входа учётную запись приостановят."

Но этот пункт их ToS незаконен в Германии (см. Требования).

Facebook — одна из самых агрессивных платформ в отношении проверки личности, и она активно продвигает свою "политику настоящих имён". Именно поэтому это руководство рекомендуется только жителям Германии.

Однако в наших тестах мы смогли выделить несколько советов:

• Будет проще, если сначала у вас есть учётная запись Instagram.

• Регистрация через Tor почти невозможна (даже через их .onion-адрес, который выглядит как шутка) и удастся только если вам "очень повезёт" (я предполагаю, если вы используете выходной узел, ещё не известный системам проверки Facebook). В большинстве случаев он вообще не позволит зарегистрироваться и просто завершится ошибкой "An error has occurred during registration".

• Регистрация через VPN с большей вероятностью завершится успешно, но всё ещё может привести к той же ошибке. Поэтому здесь нужно быть готовым к множеству проб и ошибок.

• Регистрация через самостоятельно размещённый VPN/прокси — лучший вариант, но убедитесь, что ваш профиль/личность соответствует данным о местоположении IP.

• Моя более ранняя запись в руководстве про оруэлловскую цитату из Animal Farm полностью проявляется на Facebook. Вы столкнётесь с огромной разницей в принятии в зависимости от возраста/пола/этнической принадлежности/национальности/... Именно здесь у вас будет намного меньше проблем, если вы создаёте учётную запись молодой европейской белой женщины. Вы почти наверняка потерпите неудачу, если попытаетесь создать мужчину среднего возраста, тогда как мои другие учётные записи до сих пор не приостановлены и не заблокированы.

• Вход (после регистрации) при этом нормально работает через VPN и Tor, но всё ещё может вызвать приостановку учётной записи за нарушение Community Guidelines или Terms of Services (несмотря на то, что вы не использовали учётную запись ни для чего, кроме регистрации/входа). В идеале стоит снова входить с того же IP самостоятельно размещённого VPN/прокси.

Также на основании моих тестов я сильно подозреваю, что следующие пункты влияют на вероятность приостановки со временем:

• Отсутствие друзей

• Отсутствие интересов и "органичной активности"

• Отсутствие вас в контактах у других пользователей

• Отсутствие на других платформах (например, Instagram/WhatsApp)

• Слишком раннее ограничение настроек приватности профиля после регистрации

Если вашу учётную запись приостановят, нужно будет обжаловать решение через довольно простую форму, где потребуется отправить "удостоверение личности". Однако эта система проверки удостоверения личности мягче, чем у LinkedIn, и позволит отправить разные документы, требующие гораздо меньших навыков Photoshop.

Также возможно, что они попросят снять селфи-видео или фотографию с определёнными жестами, чтобы доказать вашу личность. Если так произойдёт, боимся, пока это тупик, если только вы не используете технику замены лица с deepfake.

Если вы подадите апелляцию, вам придётся ждать, пока Facebook её рассмотрит (я не знаю, автоматический это процесс или человеческий), и ждать в надежде, что они снимут приостановку с вашей учётной записи.

GitHub

• Противоречит ли это их ToS? Нет docs.github.com Archive.org

• Потребуют ли они номер телефона? Нет, всё хорошо

• Можно ли создать учётную запись через Tor? Да, но ожидайте CAPTCHA

GitHub прост и не требует номера телефона.

Обязательно зайдите в Settings > E-Mail и сделайте вашу электронную почту приватной, а также заблокируйте любые push-операции, которые раскрыли бы вашу электронную почту.

GitLab

• Противоречит ли это их ToS? Нет about.gitlab.com Archive.org

• Потребуют ли они номер телефона? Нет, всё хорошо

• Можно ли создать учётную запись через Tor? Да, но ожидайте CAPTCHA

GitLab прост и не требует номера телефона.

Google

• Противоречит ли это их ToS? Нет policies.google.com Archive.org

• Потребуют ли они номер телефона? Да, потребуют. Здесь нет обходного пути.

• Можно ли создать учётную запись через Tor? Да, но ожидайте несколько CAPTCHA, и номер телефона будет необходим

Proton хорош... но чтобы выглядеть менее подозрительно, просто лучше иметь также массовую учётную запись Google Mail.

Как и Proton, Google, скорее всего, потребует номер телефона при регистрации как часть процесса проверки. Однако, в отличие от Proton, Google сохранит этот номер телефона во время регистрации и также ограничит число учётных записей, которые можно создать при регистрации[34][35].

По моему опыту исследований, это число ограничено тремя учётными записями/номерами телефона. Если вам не повезло с номером (если его раньше использовал другой мобильный пользователь), лимит может быть меньше.

Поэтому снова используйте ваш онлайн-номер телефона ИЛИ одноразовый телефон с предоплаченной SIM-картой, чтобы создать учётную запись. Не забудьте использовать сведения личности, которые придумали ранее (дата рождения). Когда учётная запись создана, пожалуйста, уделите время следующим действиям:

• **(Приём)** Войдите в Google Mail на настольном компьютере и перейдите в Gmail Quick Settings > See all Setting > Forwarding and POP/IMAP > Add a forwarding address > Verify (using Proton) > вернитесь в Gmail и настройте пересылку с удалением копии Google > Save. Этот шаг позволит проверять вашу Google Mail через Proton и поможет избежать срабатывания проверок безопасности Google при будущих входах с разных выходных IP VPN/Tor, при этом чувствительная почта будет храниться в Proton. Этот приём позволит получать все письма с ваших Gmail-адресов на адрес Proton (или другой), не входя в учётные записи Google (уменьшая риск их приостановки, особенно если вы используете Tor).

• Включите 2FA в настройках учётной записи Google. Сначала придётся включить 2FA с использованием номера телефона. Затем появится возможность включить 2FA с помощью приложения-аутентификатора. Используйте этот вариант и настройте его с новой записью KeePassXC TOTP. Когда закончите, удалите телефонную 2FA из учётной записи Google. Это не даст кому-то использовать этот номер телефона в будущем (когда у вас его уже не будет) для восстановления/получения доступа к этой учётной записи.

• Добавьте Proton как резервный адрес электронной почты для учётной записи.

• Удалите номер телефона из сведений учётной записи как вариант восстановления.

• Загрузите изображение профиля Google, которое сделали ранее на шаге создания личности.

• Просмотрите настройки приватности Google и отключите как можно больше:

  • Activity logging

  • YouTube

• Выйдите и не трогайте учётную запись без необходимости (как уже сказано, для проверки Gmail вы будете использовать Proton).

Помните, что существуют разные алгоритмы для поиска странной активности. Если вы получите письмо (в Proton) с предупреждением Google Security Warning, нажмите на него и нажмите кнопку, чтобы сказать: "Yes it was me". Это помогает.

Не используйте эту учётную запись для "sign-up with Google" где-либо без необходимости.

Будьте крайне осторожны, если решите использовать учётную запись для активности Google (например, отзывы в Google Maps или комментарии на YouTube), поскольку это легко может вызвать проверки (негативные отзывы, комментарии, нарушающие Community Guidelines на YouTube).

Если вашу учётную запись приостановят[36] (это может случиться при регистрации, после регистрации или после использования в некоторых сервисах Google), её всё ещё можно восстановить, отправив[37] апелляцию/проверку (где снова потребуется ваш номер телефона и, возможно, переписка с поддержкой Google с объяснением причины). **Приостановка учётной записи не отключает пересылку почты, но приостановленная учётная запись через некоторое время будет удалена.**

Если после приостановки учётная запись Google будет восстановлена, всё должно быть нормально.

Если учётную запись заблокируют окончательно, апелляции не будет, и пересылка отключится. Ваш номер телефона будет помечен, и вы не сможете использовать его для регистрации другой учётной записи. Будьте осторожны при использовании таких учётных записей, чтобы не потерять их. Они ценны.

Также возможно, что Google потребует проверку удостоверения личности через косвенный финансовый KYC или проверку фотографии документа, если вы попытаетесь получить доступ к взрослому содержимому на их платформе или опубликовать его[38].

Instagram

• Противоречит ли это их ToS? **Может быть?** Мы не уверены help.instagram.com Archive.org

"**You can't impersonate others or provide inaccurate information. You do not have to disclose your identity on Instagram, but you must provide us with accurate and up-to-date information (including registration information)**. **Also, you may not impersonate someone you are not, and you can't create an account for someone else unless you have their express permission".**

Немного оксюморон, не правда ли? Поэтому мы не уверены, разрешено это или нет.

• Потребуют ли они номер телефона? Возможно, но менее вероятно через VPN и очень вероятно через Tor

• Можно ли создать учётную запись через Tor? Да, но ожидайте несколько CAPTCHA, и номер телефона будет необходим

Также возможно, что они попросят снять селфи-видео или фотографию с определёнными жестами, чтобы доказать вашу личность (внутри приложения или через запрос по электронной почте). Если так произойдёт, боимся, пока это тупик.

Не секрет, что Instagram является частью Facebook, однако он мягче, чем Facebook, когда речь идёт о проверке пользователей. Маловероятно, что вас приостановят или заблокируют после регистрации. Но это может помочь.

Например, мы заметили, что при создании учётной записи Facebook у вас будет меньше проблем, если у вас уже есть действительная учётная запись Instagram. Всегда следует создавать Instagram-учётную запись перед попыткой создать Facebook.

К сожалению, при использовании веб-версии Instagram есть некоторые ограничения. Например, вы не сможете включить Authenticator 2FA из веба по неизвестной нам причине.

После регистрации сделайте следующее:

• Загрузите изображение вашей сгенерированной личности, если хотите.

• Перейдите в Settings.

• Сделайте учётную запись приватной (по крайней мере сначала).

• Не показывайте статус активности.

• Не разрешайте sharing.

Jami

• Противоречит ли это их ToS? Нет jami.net Archive.org

• Потребуют ли они номер телефона? Нет, им даже не нужна электронная почта

• Можно ли создать учётную запись через Tor? Нет, по какой-то технической причине это не работает

Kraken

• Противоречит ли это их ToS? Да kraken.com Archive.org

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта

• Можно ли создать учётную запись через Tor? Да

LinkedIn

• Противоречит ли это их ToS? Да linkedin.com Archive.org

"To use the Services, you agree that: (1) you must be the "*Minimum Age*" (described below) or older; (2) **you will only have one LinkedIn account, which must be in your real name**; and (3) you are not already restricted by LinkedIn from using the Services. **Creating an account with false information is a violation of our terms**, including accounts registered on behalf of others or persons under the age of sixteen. "

Но этот пункт их ToS незаконен в Германии (см. Требования).

• Потребуют ли они номер телефона? Да, потребуют.

• Можно ли создать учётную запись через Tor? Да, но ожидайте несколько CAPTCHA, и номер телефона будет необходим

LinkedIn гораздо менее агрессивен, чем Twitter, но тем не менее в большинстве случаев потребует действительную электронную почту (желательно снова Gmail) и номер телефона (хотя не всегда).

Однако LinkedIn сильно полагается на жалобы и модерацию пользователями/клиентами. Не стоит создавать профиль с должностью внутри частной корпорации или небольшой стартап-компании. Сотрудники компании отслеживают активность LinkedIn и получают уведомления, когда присоединяются новые люди. Затем они могут сообщить о вашем профиле как о поддельном, и ваш профиль будет приостановлен или заблокирован до апелляции.

Затем LinkedIn потребует пройти процесс проверки, который, к сожалению, потребует отправить удостоверение личности (ID-карта, паспорт, водительское удостоверение). Эту проверку удостоверения личности обрабатывает компания Jumio[39], специализирующаяся на проверке документов. Скорее всего, это тупик, поскольку заставит вас развивать серьёзные навыки Photoshop.

Вместо этого гораздо менее вероятно, что на вас пожалуются, если вы останетесь расплывчатым (скажете, что вы студент/стажёр/фрилансер) или сделаете вид, что работаете в крупном публичном учреждении, слишком большом, чтобы кто-то беспокоился или проверял.

Как и с Twitter и Google, после регистрации следует сделать следующее:

• Отключить рекламу.

• Отключить уведомления.

• Отключить поиск по телефону/электронной почте.

• Загрузить изображение вашей личности.

MailFence

• Противоречит ли это их ToS? Нет

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта

• Можно ли создать учётную запись через Tor? Возможно. По моим тестам, письма для подтверждения регистрации не отправляются при регистрации через Tor. При использовании VPN поверх Tor или прокси поверх Tor проблем нет.

Medium

• Противоречит ли это их ToS? Нет, если речь не о криптовалютах policy.medium.com Archive.org

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта

• Можно ли создать учётную запись через Tor? Пока с этим не было проблем

Для входа каждый раз нужна электронная почта.

Microsoft

• Противоречит ли это их ToS? Да microsoft.com Archive.org

"i. Creating an Account. You can create a Microsoft account by signing up online. **You agree not to use any false, inaccurate, or misleading information when signing up for your Microsoft account".**

Но этот пункт их ToS незаконен в Германии (см. Требования).

• Потребуют ли они номер телефона? Вероятно, но не всегда. В зависимости от удачи с вашим выходным узлом Tor они могут потребовать только проверку по электронной почте. Если использовать VPN поверх Tor, скорее всего, они попросят только электронную почту.

• Можно ли создать учётную запись через Tor? Да, можно, но ожидайте CAPTCHA, как минимум проверку по электронной почте, **и, вероятно, проверку по телефону.**

Так что да, всё ещё возможно создать учётную запись MS без номера телефона и с использованием Tor или VPN, но для этого может понадобиться перебрать несколько выходных узлов.

После регистрации следует настроить аутентификацию 2FA в параметрах безопасности с использованием KeePassXC TOTP.

OnlyFans

• Противоречит ли это их ToS? Нет, выглядит нормально onlyfans.com Archive.org

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта

• Можно ли создать учётную запись через Tor? Да, можно

К сожалению, такая учётная запись будет крайне ограниченной, и чтобы что-либо делать, нужно будет пройти их процесс проверки, требующий проверки финансовой транзакции типа KYC. Так что это не очень полезно.

Proton

• Противоречит ли это их ToS? Нет proton.me Archive.org

• Потребуют ли они номер телефона? Возможно. Это зависит от IP, с которого вы приходите. Если из Tor — вероятно. Из VPN — менее вероятно.

• Можно ли создать учётную запись через Tor? Да, но очень вероятно, что потребуется номер телефона, тогда как через VPN может потребоваться только электронная почта или CAPTCHA. У них даже есть ".onion"-адрес: protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion.

Очевидно, вам нужна электронная почта для вашей онлайн-личности, а одноразовая почта почти везде заблокирована.

Proton — бесплатный провайдер электронной почты из Швейцарии, выступающий за безопасность и приватность.

Они рекомендованы Privacyguides.org[40]. Их единственная заметная проблема в том, что они (в большинстве случаев) требуют номер телефона или другой адрес электронной почты для регистрации (по крайней мере при попытке зарегистрироваться из VPN или Tor).

Они утверждают, что не хранят/не связывают телефон/электронную почту, связанную с регистрацией, а сохраняют только хэш, не связанный с учётной записью[41]. Если их утверждение верно, хэш не связан с вашей учётной записью, и вы следовали моему руководству по телефонному номеру, вы должны быть достаточно защищены от отслеживания.

Эту почтовую учётную запись можно использовать для создания учётной записи Google/Gmail.

Reddit

• Противоречит ли это их ToS? Нет redditinc.com Archive.org

• Потребуют ли они номер телефона? Нет, не потребуют.

• Можно ли создать учётную запись через Tor? Да

Reddit прост. Для регистрации нужны только действительное имя пользователя и пароль. Обычно они даже не требуют электронную почту (при регистрации можно пропустить поле электронной почты, оставив его пустым).

Никаких проблем с регистрацией через Tor или VPN, кроме редких CAPTCHA.

Рассмотрите чтение этого поста Reddit: old.reddit.com Archive.org

Slashdot

• Противоречит ли это их ToS? Да slashdotmedia.com Archive.org

"8. Registration; Use of Secure Areas and Passwords

Some areas of the Sites may require you to register with us. When and if you register, you agree to (a) provide accurate, current, and complete information about yourself as prompted by our registration form (including your e-mail address) and (b) to maintain and update your information (including your e-mail address) to keep it accurate, current, and complete. You acknowledge that should any information provided by you be found to be untrue, inaccurate, not current, or incomplete, we reserve the right to terminate this Agreement with you and your current or future use of the Sites (or any portion thereof)".

• Потребуют ли они номер телефона? Нет

• Можно ли создать учётную запись через Tor? Да

Telegram

• Противоречит ли это их ToS? Нет telegram.org Archive.org

• Потребуют ли они номер телефона? К сожалению, да

• Можно ли создать учётную запись через Tor? Да, но иногда вас случайно блокируют без какой-либо причины

Telegram довольно прямолинеен, и можно скачать их переносимое приложение Windows для регистрации и входа.

Потребуется номер телефона (который можно использовать только один раз) и больше ничего.

В большинстве случаев у нас не было проблем ни через Tor, ни через VPN, но было несколько случаев, когда нашу учётную запись Telegram просто блокировали за нарушение условий обслуживания (неясно, каких именно). И это снова несмотря на то, что мы ни для чего их не использовали.

У них есть процесс апелляции по электронной почте, но нам не удалось получить ни одного ответа.

Их процесс апелляции — это просто отправка письма на recover@telegram.org Archive.org с указанием вашего номера телефона и проблемы, после чего остаётся надеяться на ответ.

После регистрации следует сделать следующее:

• Перейдите в Edit profile.

• Задайте Username.

• Перейдите в Settings (Desktop App).

• Установите видимость Phone Number в Nobody.

• Установите Last Seen & Online в Nobody.

• Установите Forwarded Messages в Nobody.

• Установите Profile photos в Contacts.

• Установите Calls в Contacts.

• Установите Group & Channels в Contacts.

Tutanota

• Противоречит ли это их ToS? Нет tutanota.com Archive.org

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта.

• Можно ли создать учётную запись через Tor? Не совсем; насколько мне известно, почти все выходные узлы Tor заблокированы

Twitter

• Противоречит ли это их ToS? Нет twitter.com

• Потребуют ли они номер телефона? Крайне вероятно, возможно, теперь это требование во всех случаях.

• Можно ли создать учётную запись через Tor? Да, но ожидайте несколько CAPTCHA, и через некоторое время потребуется номер телефона.

Twitter крайне агрессивен в предотвращении анонимности в своей сети. Регистрироваться следует с электронной почтой и паролем (не телефоном) и не использовать "Sign-in with Google". Используйте ваш Gmail как адрес электронной почты.

С большой вероятностью ваша учётная запись будет немедленно приостановлена во время регистрации и потребует пройти серию автоматических тестов для разблокировки. Это будет включать серию CAPTCHA, подтверждение электронной почты и имени в Twitter или другие сведения. В некоторых случаях также потребуется ваш номер телефона.

В некоторых случаях, несмотря на выбор текстовой проверки, система проверки Twitter всё равно звонит на телефон. В таком случае придётся ответить и услышать проверочный код. Мы подозреваем, что это ещё один способ предотвращать автоматизированные системы и недобросовестные компании или сущности, продающие услуги приёма SMS через интернет.

Twitter сохранит всю эту информацию и свяжет её с вашей учётной записью, включая ваш IP, электронную почту и номер телефона. Вы не сможете использовать этот номер телефона для создания другой учётной записи.

После восстановления учётной записи стоит уделить время следующему:

• Загрузите изображение профиля личности.

• Включите 2FA в настройках безопасности, используя новую запись KeePassXC TOTP; также сохраните коды безопасности в KeePassXC.

• Отключите Photo tagging.

• Отключите E-mail lookup.

• Отключите Phone lookup.

• Отключите все настройки персонализированной рекламы.

• Отключите данные о местоположении в твитах.

• **Осторожно:** удалите номер телефона из учётной записи (на свой риск; это часто приводит к приостановке учётной записи)

• Подпишитесь на нескольких людей по теме.

• Выйдите и оставьте учётную запись в покое.

Примерно через неделю стоит снова проверить Twitter, и вероятность довольно высока, что учётная запись снова будет приостановлена за "suspicious activity" или "violating community guidelines", несмотря на то, что вы вообще её не использовали (ни одного твита/подписки/лайка/ретвита или личного сообщения), но на этот раз другой системой. Мы называем это "Double-tap".

На этот раз нужно подать апелляцию через форму[42], указать хорошую причину и дождаться обработки апелляции Twitter. Во время этого процесса вы можете получить письмо (в Proton) с просьбой ответить на обращение в поддержку, чтобы доказать, что у вас есть доступ к электронной почте и что это вы. Оно будет направлено на ваш Gmail-адрес, но придёт в Proton.

Не отвечайте из Proton, поскольку это вызовет подозрения; нужно войти в Gmail (к сожалению) и составить новое письмо оттуда, скопировав E-Mail, Subject и Content из Proton, а также ответ с подтверждением, что у вас есть доступ к этой электронной почте.

Через несколько дней учётную запись должны восстановить "окончательно". После этого проблем быть не должно, но помните: они всё ещё могут заблокировать вашу учётную запись по любой причине, если вы нарушите правила сообщества. Тогда номер телефона и электронная почта будут помечены, и у вас не останется варианта, кроме как получить новую личность с новым номером для повторной регистрации. Не используйте эту учётную запись для троллинга.

Twitch

• Противоречит ли это их ToS? Нет twitch.tv Archive.org

• Потребуют ли они номер телефона? Нет, но им нужна электронная почта.

• Можно ли создать учётную запись через Tor? Да

Учтите, что вы не сможете включить 2FA на Twitch, используя только электронную почту. Для включения этой функции нужен номер телефона.

WhatsApp

• Противоречит ли это их ToS? **Да** whatsapp.com Archive.org

"**Registration**. You must register for our Services **using accurate information**, provide your current mobile phone number, and, if you change it, update your mobile phone number using our in-app change number feature. You agree to receive text messages and phone calls (from us or our third-party providers) with codes to register for our Services".

• Потребуют ли они номер телефона? Да, потребуют.

• Можно ли создать учётную запись через Tor? Пока с этим не было проблем.

4chan

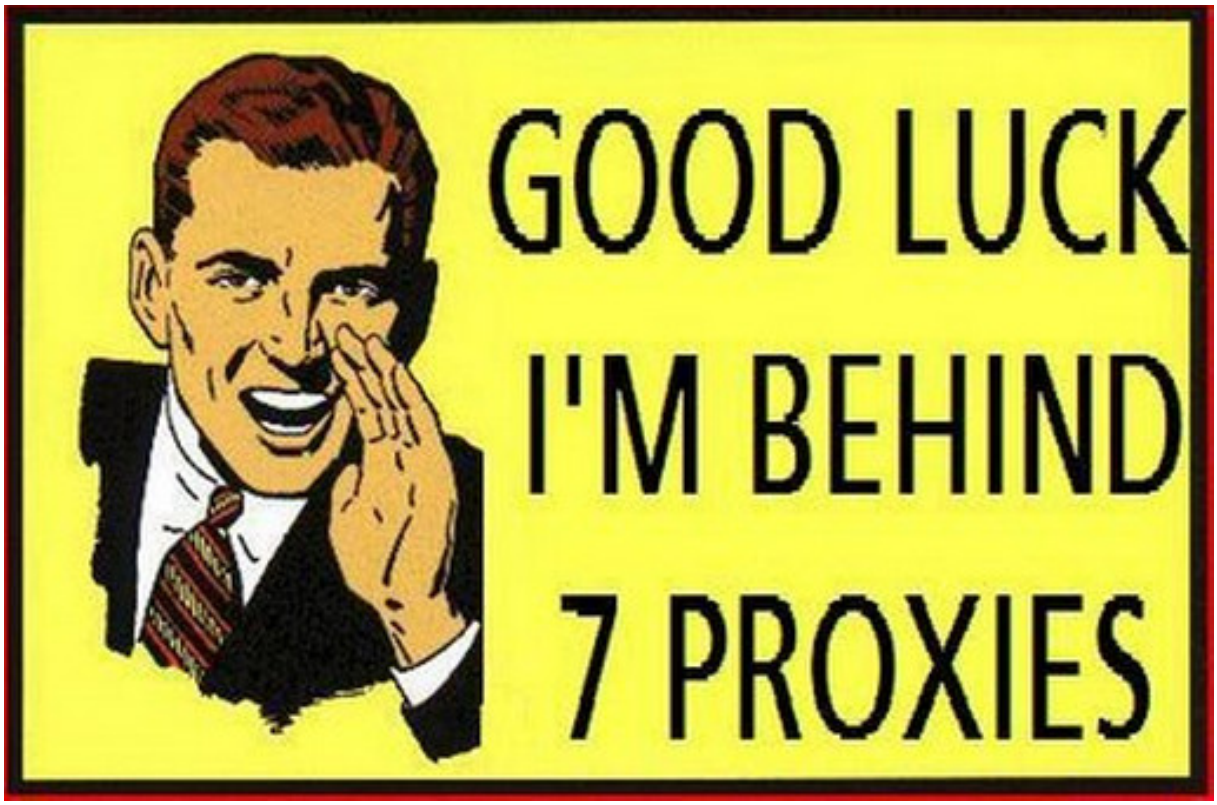
• Противоречит ли это их ToS? Нет

• Потребуют ли они номер телефона? Нет, не потребуют.

• Можно ли там публиковать через Tor или VPN? Маловероятно.

4chan — это 4chan... Это руководство не будет объяснять вам 4chan. Они блокируют выходные узлы Tor и известные диапазоны IP VPN.

Вам придётся найти отдельный способ публиковать там хотя бы через семь прокси[43], неизвестных системе блокировки 4chan (подсказка: анонимный VPS, оплаченный Monero, вероятно, лучший вариант).



Криптокошельки

Используйте любое приложение криптокошелька внутри виртуальной машины Windows. Но будьте осторожны и не переводите ничего на биржу или известный кошелёк. Криптовалюта в большинстве случаев НЕ анонимна и может быть отслежена до вас, когда вы покупаете/продаёте её (помните раздел Ваши криптовалютные транзакции).

Если вы действительно хотите использовать криптовалюту, используйте Monero — единственную с разумной приватностью/анонимностью.

В идеале нужно найти способ покупать/продавать криптовалюту за наличные у неизвестного человека.

Что насчёт приложений только для мобильных устройств (WhatsApp/Signal)

Есть только три способа безопасно использовать их анонимно (из тех, что мы рекомендуем). Использование VPN на телефоне не входит в их число. Все они, к сожалению, как минимум "утомительны".

- Используйте эмулятор Android внутри виртуальной машины Windows и запускайте приложение через ваш многослойный Tor/VPN. Недостаток в том, что такие эмуляторы обычно довольно требовательны к ресурсам, будут замедлять виртуальную машину и расходовать больше батареи. Вот также (устаревшее) руководство по этой теме: bellingcat.com Archive.org. От себя мы рекомендуем использовать:
  - Android-x86 в Virtualbox (см. android-x86.org Archive.org), который тоже можно легко настроить.
  - AnBox (anbox.io Archive.org), который также довольно легко настроить, в том числе на Whonix Workstation; см. whonix.org Archive.org
- **Не рекомендуется:** использовать неофициальное приложение (например, Wassapp для WhatsApp), чтобы подключаться из виртуальной машины Windows к приложению. Используйте на свой риск: вас могут заблокировать за нарушение условий обслуживания из-за использования неофициального приложения.
- **Не рекомендуется и наиболее сложно:** иметь одноразовый смартфон, который вы подключите к многослойной сети виртуальной машины через tethering/раздачу подключения по Wi-Fi. Мы не будем подробно описывать это здесь, но такой вариант существует.

Нет способа надёжно и легко настроить приличный многослойный подход к подключению на телефоне Android (на IOS, насколько нам известно, это вообще невозможно). Под надёжностью мы понимаем уверенность, что смартфон не утечёт ничем, например данными о местоположении или чем-либо ещё, от загрузки до выключения.

Что-либо ещё

Используйте ту же логику и безопасность для любой другой платформы.

Это должно работать в большинстве случаев с большинством платформ. **Самая трудная платформа для использования с полной анонимностью — Facebook.**

Очевидно, это не будет работать с банками и большинством финансовых платформ (например, PayPal или криптовалютными биржами), требующих настоящую официальную и существующую идентификацию. Это руководство там не поможет, поскольку во многих местах это было бы незаконно.

Как анонимно общаться и обмениваться файлами

Приложений для обмена сообщениями повсюду очень много. У некоторых отличный UI и UX, но ужасная безопасность/приватность. У некоторых отличная безопасность/приватность, но ужасный UI и UX. Нелегко выбрать те, которые стоит использовать для чувствительных действий. Поэтому этот раздел поможет вам сделать выбор.

Прежде чем идти дальше, есть несколько ключевых базовых понятий, которые нужно понять:

Сквозное шифрование

Сквозное шифрование[44] (также e2ee) — довольно простое понятие. Оно просто означает, что только вы и адресат знаете публичные ключи шифрования друг друга, и никто посередине, кто мог бы подслушивать, не сможет расшифровать коммуникацию.

Однако этот термин часто используется по-разному в зависимости от провайдера:

- Некоторые провайдеры заявляют e2ee, но забывают упомянуть, что именно покрыто их протоколами. Например, защищены ли метаданные внутри их протокола e2ee? Или только содержимое сообщений?
- Некоторые провайдеры предоставляют e2ee, но только как дополнительную опцию (отключено по умолчанию).
- Некоторые провайдеры предлагают e2ee для общения один-на-один, но не для группового общения.
- Некоторые провайдеры заявляют использование e2ee, но их проприетарные приложения закрыты, и никто не может проверить это утверждение и стойкость используемого шифрования.

По этим причинам всегда важно проверять заявления разных приложений. Открытые приложения всегда предпочтительнее: они позволяют проверить, какое шифрование используется и верны ли заявления. Если приложение не открытое, у него должен быть публично доступный независимый отчёт (сделанный авторитетной третьей стороной), подтверждающий его заявления.

Собственная криптография

См. раздел Плохая криптография в начале этого руководства.

Всегда осторожно относитесь к приложениям, которые придумывают собственную криптографию, пока она не была проверена многими людьми в криптографическом сообществе (или, ещё лучше, опубликована и прошла академическое рецензирование). Опять же, это труднее проверить у закрытых проприетарных приложений.

Проблема не в том, что собственная криптография плоха сама по себе, а в том, что хорошей криптографии нужны настоящее рецензирование, аудит, тестирование... И поскольку вы, вероятно, не криптоаналитик (и мы тоже), велика вероятность, что мы некомпетентны оценивать криптографию некоторых приложений.

Прямая секретность

Прямая секретность[45] (FS, также PFS для Perfect Forward Secrecy) — свойство протокола согласования ключей в некоторых таких приложениях для обмена сообщениями и сопутствующая функция e2ee. Это происходит до установления связи с адресатом. "Forward" относится к будущему времени и означает, что каждый раз при установлении новой e2ee-коммуникации создаётся новый набор ключей для конкретного сеанса. Цель прямой секретности — сохранить секретность прошлых коммуникаций (сеансов), даже если текущая скомпрометирована. Если противник получит ваши текущие ключи e2ee, он будет ограничен содержимым одного сеанса и не сможет легко расшифровать прошлые.

У этого есть некоторые недостатки для удобства пользователя: например, новое устройство может не иметь удобного доступа к удалённо сохранённой истории чата без дополнительных шагов.

Итак, коротко: прямая секретность защищает прошлые сеансы от будущей компрометации ключей или паролей.

Подробнее об этом в этом видео YouTube: youtube.com Invidious

Некоторые провайдеры и приложения, заявляющие e2ee, иногда не предлагают FS/PFS по причинам удобства использования (например, групповое общение сложнее с PFS). Поэтому важно предпочитать открытые приложения, предоставляющие прямую секретность, тем, которые её не предоставляют.

Шифрование данных в состоянии хранения с нулевым доступом

Шифрование с нулевым доступом[46] в состоянии хранения используется, когда вы храните данные у какого-то провайдера (например, историю чатов или резервные копии чатов), но эта история или резервная копия зашифрована на вашей стороне и не может быть прочитана или расшифрована провайдером, который её размещает.

Шифрование с нулевым доступом — дополнительная/сопутствующая функция к e2ee, но она применяется главным образом к данным в состоянии хранения, а не к коммуникациям.

Примерами этой проблемы могут быть iMessage и WhatsApp; см. Ваши облачные резервные копии и службы синхронизации в начале этого руководства.

Так что, опять же, лучше предпочитать приложения/провайдеров, которые предлагают шифрование с нулевым доступом в состоянии хранения и не могут читать/получать доступ ни к вашим данным, ни к метаданным даже в состоянии хранения, а не только ограничиваются коммуникациями.

Такая функция предотвратила бы крупные взломы, например скандал Cambridge Analytica[47], если бы была реализована.

Защита метаданных

Помните раздел Ваши метаданные (включая данные о местоположении). Сквозное шифрование — это одно, но оно не обязательно защищает ваши метаданные.

Например, WhatsApp может не знать, что вы говорите, но может знать, с кем вы разговариваете, как долго и когда вы с кем-то говорили, кто ещё состоит с вами в группах и передавали ли вы им данные (например, большие файлы).

Сквозное шифрование само по себе не защищает от сбора ваших метаданных подслушивающей стороной.

Эти данные также могут защищаться/запутываться некоторыми протоколами, чтобы значительно усложнить сбор метаданных для подслушивающих. Так, например, Signal Protocol предлагает некоторую дополнительную защиту с такими функциями, как:

• Опция Sealed Sender[48].

• Private Contact Discovery[49].

• Private Group System[50].

Другие приложения, например Briar или OnionShare, защищают метаданные, используя сеть Tor как щит и храня всё локально на устройстве. Ничего не хранится удалённо, а все коммуникации либо прямые, через близкое Wi-Fi/Bluetooth-соединение, либо удалённые через сеть Tor.

Однако большинство приложений, особенно закрытые проприетарные коммерческие приложения, будут собирать и хранить ваши метаданные для разных целей. Одних таких метаданных достаточно, чтобы выяснить много о ваших коммуникациях.

Снова важно предпочитать открытые приложения, учитывающие приватность и имеющие разные методы защиты не только содержимого коммуникаций, но и всех связанных метаданных.

Открытый исходный код

Наконец, приложения с открытым исходным кодом всегда предпочтительнее, потому что они позволяют третьим сторонам проверять реальные возможности и слабости по сравнению с заявлениями отделов маркетинга. Открытый исходный код не означает, что приложение должно быть бесплатным или некоммерческим. Это просто означает прозрачность.

Приложение0	Сквозное шифрование 1	Собственная криптография	Прямая секретность	Шифрование с нулевым доступом в состоянии хранения 5	Защита метаданных (запутывание, шифрование...)	Открытый исходный код	Настройки приватности по умолчанию	Родная анонимная регистрация (без электронной почты или телефона)	Возможно через Tor	История приватности и безопасности	Децентрализовано	Дополнительные примечания
Berty (избегать)	Да	Нет	Да	Да	Да	Да 13	Хорошие	Да	Да	Хорошая	Да (peer-to-peer)	Недостаточно проверено этим проектом, рекомендовать нельзя
Briar (предпочтительно)	Да	Нет 1	Да	Да	Да (сильная)	Да	Хорошие	Да	Родная поддержка3	Хорошая	Да (peer-to-peer)	
Cwtch (предпочтительно)	Да	Нет	Да	Да	Да (сильная)	Да	Хорошие	Да	Родная поддержка	Хорошая	Да (peer-to-peer)	
Discord (избегать)	Нет	Закрытый исходный код7	Нет	Нет	Нет	Нет	Плохие	Нужна электронная почта	Виртуализация	Плохая	Нет	
Element / Matrix.org (предпочтительно)	Да (дополнительно включается)	Нет	Да	Да	Слабая2	Да	Хорошие	Да	Через прокси3 или виртуализацию	Хорошая	Частично (федеративные серверы)	
Facebook Messenger (избегать)	Частично (только 1 к 1 / дополнительно включается)	Закрытый исходный код7	Да	Нет	Нет	Нет	Плохие	Нужны электронная почта и телефон	Виртуализация	Плохая	Нет	
OnionShare (предпочтительно)	Да	Нет	Уточняется8	Уточняется 8	Да (сильная)	Да	Хорошие	Да	Родная поддержка	Хорошая	Да (peer-to-peer)	
Apple Messages (iMessage)	Да	Закрытый исходный код7	Нет	Частично	Нет	Нет	Хорошие	Нужно устройство Apple	Возможно через виртуализацию с настоящим ID устройства Apple	Плохая	Нет	

Приложение0	Сквозное шифрование 1	Собственная криптография	Прямая секретность	Шифрование с нулевым доступом в состоянии хранения 5	Защита метаданных (запутывание, шифрование...)	Открытый исходный код	Настройки приватности по умолчанию	Родная анонимная регистрация (без электронной почты или телефона)	Возможно через Tor	История приватности и безопасности	Децентрализовано	Дополнительные примечания
IRC	Да (плагины OTR)	Нет	Нет	Нет	Нет	Да	Плохие	Да	Через прокси3 или виртуализацию	Хорошая	Нет	
Jami (предпочтительно)	Да	Нет3	Да	Да	Частично	Да	Хорошие	Да	Через прокси3 или виртуализацию9	Хорошая	Частично	Tor ломает некоторые функции
KakaoTalk (избегать)	Да	Закрытый исходный код7	Нет4	Нет	Нет	Нет	Плохие	Нет (но возможно)	Виртуализация	Плохая	Нет	
Keybase	Да	Нет	Частично (исчезающие сообщения)	Нет	Нет	Да	Хорошие	Нужна электронная почта			Нет	
Kik (избегать)	Нет	Закрытый исходный код7	Нет	Нет	Нет	Нет	Плохие	Нет (но возможно)	Виртуализация	Плохая	Нет	
Line (избегать)	Частично (дополнительно включается)	Закрытый исходный код7	Нет	Нет	Нет	Нет	Плохие	Нет (но возможно)	Виртуализация	Плохая	Нет	
Pidgin with OTR (избегать)	Да (OTR5)	Нет	Да	Нет	Нет	Да	Плохие	Да	Через прокси3 или виртуализацию	Плохая6	Нет	
Tox (избегать)	Да	Нет	Нет	Нет	Нет	Да	Хорошие	Да	Через прокси3 или виртуализацию	Средняя7	Да	Известные криптографические слабости14
Session (предпочтительно только на iOS)	Да	Нет	Нет	Да	Да	Да	Хорошие	Да	Через прокси3 или виртуализацию10	Хорошая	Да	Не хватает PFS и возможности отрицания

Приложение0	Сквозное шифрование 1	Собственная криптография	Прямая секретность	Шифрование с нулевым доступом в состоянии хранения 5	Защита метаданных (запутывание, шифрование...)	Открытый исходный код	Настройки приватности по умолчанию	Родная анонимная регистрация (без электронной почты или телефона)	Возможно через Tor	История приватности и безопасности	Децентрализовано	Дополнительные примечания
Signal	Да	Нет	Да	Да	Да (умеренная)	Да	Хорошие	Нужен телефон	Виртуализация	Хорошая	Нет	Для анонимного использования нужен одноразовый или анонимный VOIP-номер
Skype (избегать)	Частично (только 1 к 1 / дополнительно включается)	Закрытый исходный код7	Нет	Нет	Нет	Нет	Плохие	Нет (но возможно)	Виртуализация	Плохая	Нет	
SnapChat (избегать)	Нет	Закрытый исходный код7	Нет	Нет	Нет	Нет	Плохие	Нет (но возможно)	Виртуализация	Плохая	Нет	Удалённые/истёкшие сообщения легко восстановить15,16
Teams (избегать)	Да	Закрытый исходный код7	Нет	Нет	Нет	Нет	Плохие	Нет (но возможно)	Виртуализация	Плохая	Нет	
Telegram	Частично (только 1 к 1 / дополнительно включается)	Да (MTProto 8)	Частично (только секретные чаты)	Да	Нет	Частичноо5	Средние (e2ee по умолчанию выключено)	Нужен телефон	Через прокси3 или виртуализацию	Средняя9	Нет	
Viber (избегать)	Частично (только 1 к 1)	Закрытый исходный код7	Да	Нет	Нет	Нет	Плохие	Нет (но возможно)	Виртуализация	Плохая	Нет	
WeChat (избегать)	Нет	Закрытый исходный код7	Нет	Нет	Нет	Нет	Плохие	Нет	Виртуализация	Плохая	Нет	
WhatsApp (избегать)	Да	Закрытый исходный код7	Да	Нет	Нет	Нет	Плохие	Нужен телефон	Виртуализация	Плохая	Нет	

Приложение0	Сквозное шифрование 1	Собственная криптография	Прямая секретность	Шифрование с нулевым доступом в состоянии хранения 5	Защита метаданных (запутывание, шифрование...)	Открытый исходный код	Настройки приватности по умолчанию	Родная анонимная регистрация (без электронной почты или телефона)	Возможно через Tor	История приватности и безопасности	Децентрализовано	Дополнительные примечания
Wickr Me	Частично (только 1 к 1)	Нет	Да	Нет	Да (умеренная)	Нет	Хорошие	Да	Виртуализация	Хорошая	Нет	
Gajim (XMPP) (предпочтительно)	Да	Нет	Да	Нет	Нет	Да	Хорошие	Да	Через прокси3 или виртуализацию	Хорошая	Частично	
Zoom (избегать 10)	Спорно11	Нет	Уточняется8	Нет	Нет	Нет	Плохие	Нужна электронная почта	Виртуализация	Плохая12	Нет	Риск вредоносного ПО17
Molly	Да	Нет	Да	Да	Да (умеренная)	Да	Хорошие	Нужен телефон	Виртуализация	Хорошая	Нет	Нужен номер телефона. Усиленная по безопасности ветка клиента Signal. Обновления безопасности могут задерживаться до недели

Легенда:

1. Пометка "предпочтительно" или "избегать" относится к использованию этих приложений для чувствительных коммуникаций. Это только моё мнение, и вы можете составить своё, используя материалы выше и другие источники. Помните: "доверяй, но проверяй".
2. e2ee означает "сквозное шифрование".
3. Для защиты подключения через Tor могут потребоваться дополнительные шаги.
4. Их способность и готовность бороться за приватность и не сотрудничать с разными противниками.
5. Открыты только клиентские приложения, но не серверные.
6. Это означает, что данные полностью зашифрованы в состоянии хранения (а не только при передаче) и нечитабельны для любой третьей стороны без ключа, который знаете только вы (включая резервные копии).

7. Невозможно проверить, потому что это проприетарный закрытый исходный код.

8. "Предстоит определить", неизвестно на момент написания.

9. Для работы Jami потребуется включить DHTProxy в параметрах, и он будет ограничен только текстом.

10. Session также использует собственное решение луковой маршрутизации под названием LokiNet.

Некоторые приложения, например Threema и Wire, были исключены из сравнения, потому что они не бесплатны и не принимают анонимные способы оплаты, такие как наличные/Monero.

Заключение

Помните: контрольный список того, что нужно проверить перед публикацией информации.

Мы рекомендуем эти варианты в таком порядке (как также рекомендуют PrivacyGuides.org[51][52], кроме Session и Cwtch):

- macOS:
  - Родная поддержка луковой маршрутизации через Tor (**предпочтительно**):
    - OnionShare версии >2.3 (onionshare.org Tor Mirror Archive.org)
    - Cwtch (cwtch.im Archive.org; **предупреждение: проект находится на стадии альфа/бета**)
  - Без родной поддержки Tor (для идеальной анонимности нужны дополнительные шаги: пропускать трафик через Tor при помощи виртуализации или прокси):
    - Element/Matrix.org (element.io Archive.org)
    - Jami (jami.net Archive.org)
    - Gajim/XMPP (gajim.org Archive.org)
- Windows:
  - Родная поддержка луковой маршрутизации через Tor (**предпочтительно**):
    - OnionShare версии >2.3 (onionshare.org Tor Mirror Archive.org)
    - Cwtch (cwtch.im Archive.org; **предупреждение: проект находится на стадии альфа/бета**)
  - Без родной поддержки Tor (для идеальной анонимности нужны дополнительные шаги: пропускать трафик через Tor при помощи виртуализации или прокси):
    - Element/Matrix.org (element.io Archive.org)
    - Jami (jami.net Archive.org)
    - Gajim/XMPP (gajim.org Archive.org)
- Linux:
  - Родная поддержка луковой маршрутизации через Tor (**предпочтительно**):
    - Briar (briarproject.org Archive.org)
    - OnionShare версии >2.3 (onionshare.org Tor Mirror Archive.org)
    - Cwtch (cwtch.im Archive.org; **предупреждение: проект находится на стадии альфа/бета**)

    - Без родной поддержки Tor (для идеальной анонимности нужны дополнительные шаги: пропускать трафик через Tor при помощи виртуализации или прокси):
        - Element/Matrix.org (element.io Archive.org)
        - Jami (jami.net Archive.org)
        - Gajim/XMPP (gajim.org Archive.org)
- Обратите внимание: чтобы Jami работал через Tor, нужно включить локальный параметр DHTProxy в настройках Jami. Это будет работать только для текстовых сообщений, но не для звонков и видео.

Обратите внимание: эти варианты (Briar, Cwtch и OnionShare) пока не поддерживают несколько устройств. Ваша информация строго хранится на том устройстве и в той операционной системе, где вы всё настраиваете. Не используйте их в непостоянной операционной системе, если только вам не нужен именно временный сеанс.

Есть ли безопасные варианты для мобильных устройств? **Да, но мы их не одобряем и не рекомендуем, кроме Briar на Android. Помните также, что это руководство в целом не советует использовать смартфоны для чувствительных действий.**

- Android:
    - Briar (briarproject.org Archive.org)
    - Cwtch (cwtch.im Archive.org **предупреждение: проект находится на стадии альфа/бета**)
- iOS:
    - За неимением лучшего варианта и при том, что он **обычно не рекомендуется**: Session Messenger: getsession.org Archive.org. Почему в сообществе приватности его сейчас не рекомендуют? **См. Предостережение о Session messenger, чтобы понять, почему мы осторожно относимся к Session Messenger**.

Обратите внимание: все варианты без родной поддержки Tor ради безопасности нужно использовать через Tor (из Tails или гостевой ОС, работающей за Whonix Gateway, например Whonix Workstation или виртуальной машины Android-x86).

Хотя мы не рекомендуем большинство платформ для обмена сообщениями по различным причинам, описанным выше (требования номера телефона и электронной почты), это не значит, что их невозможно использовать анонимно, если вы понимаете, что делаете. Даже Facebook Messenger можно использовать анонимно, если принять необходимые меры предосторожности, описанные в этом руководстве: виртуализация за Tor Gateway в непостоянной операционной системе.

Предпочтительные варианты рекомендуются из-за их позиции в отношении приватности, настроек по умолчанию, выбранной криптографии, а также потому, что они позволяют удобно регистрироваться анонимно без множества трудностей с подтверждением номера телефона или электронной почты и имеют открытый исходный код. В большинстве случаев им стоит отдавать предпочтение.

Вы также можете свериться со следующими внешними материалами для дополнительных сравнений (**мы не обязательно разделяем их мнения**):

- SecuChart, bkil.gitlab.io Archive.org Repository (поддерживаемый проект с открытым исходным кодом)
- Wikipedia, en.wikipedia.org Wikiless Archive.org
    - Wikipedia, en.wikipedia.org Wikiless Archive.org

- Whonix Documentation, Instant Messenger Chat whonix.org Archive.org (устаревший, не поддерживается, но содержит полезную информацию)
- **Устаревшие, неподдерживаемые или заброшенные материалы, запланированные к удалению из нашего руководства в следующем выпуске:**
  - Secure Messaging Apps securemessagingapps.com Archive.org
  - Proton Blog, proton.me Archive.org
  - SecureChart.org, securechatguide.org Archive.org
  - Messenger-Matrix.de at messenger-matrix.de Archive.org

Мы не одобряем и не рекомендуем для анонимности некоторые массовые платформы, включая широко хвалёный Signal, который на сегодняшний день всё ещё требует номер телефона для регистрации и связи с другими людьми. В контексте этого руководства мы настоятельно рекомендуем по возможности не использовать Signal. Та же рекомендация относится к популярным ответвлениям Signal, таким как Molly (molly.imArchive.org)

Как публично делиться файлами

Предупреждение: прежде чем публиковать что-либо открыто, убедитесь, что ваши файлы очищены от любой информации, которая может раскрыть вашу личность. См. контрольный список того, что нужно проверить перед публикацией информации.

Рассмотрите следующие платформы:

- Cryptpad.fr (cryptpad.fr): бесплатный тариф ограничен 1 ГБ суммарно; сервис рекомендован PrivacyGuides.org на privacyguides.org Archive.org
- Proton Drive (proton.me): платный. Требует наличия "Proton Unlimited" или "Mail Plus". Proton Drive использует сквозное шифрование и рекомендован PrivacyGuides.org
  - Как и в случае с Proton и Proton VPN, анонимно зарегистрироваться там непросто. При попытке регистрации через Tor они просят подтверждение либо по номеру телефона, либо через пожертвование
- Filen (filen.io): бесплатный тариф ограничен 10 ГБ суммарно

Рассмотрите использование IPFS[53]:

- Pinata (pinata.cloud): бесплатный тариф ограничен 1 ГБ суммарно

Безопасная редактура документов

Возможно, вы захотите безопасно и анонимно самостоятельно публиковать какую-либо информацию в виде текстов, изображений, видео и так далее.

Для всех этих целей есть несколько рекомендаций:

- В идеале не следует использовать проприетарное программное обеспечение вроде Adobe Photoshop, Microsoft Office и так далее.
- Лучше использовать программное обеспечение с открытым исходным кодом, например LibreOffice, Gimp и так далее.

Хотя коммерческие альтернативы богаты возможностями, они также являются проприетарными и закрытыми и часто имеют разные проблемы, например:

• Отправляют телеметрию обратно компании.

• Добавляют в документы ненужные метаданные, а иногда и водяные знаки.

• Эти приложения не бесплатны, и любая утечка метаданных может быть связана с вами, поскольку вы где-то их покупали.

Коммерческое программное обеспечение можно использовать для создания чувствительных документов, но нужно быть особенно внимательным ко всем параметрам в разных приложениях (коммерческих или бесплатных), чтобы никакая утечка данных не раскрыла сведения о вас.

Ниже приведена сравнительная таблица рекомендуемого и включённого программного обеспечения, собранная из разных источников (PrivacyGuides.org, Whonix, Tails, Prism-Break.org и я). Имейте в виду, что моя рекомендация учитывает контекст этого руководства: лишь эпизодическое присутствие в сети по мере необходимости.

Тип	**Whonix**	**Prism-Break.org**	**PrivacyGuides.org**	**Tails**	**Это руководство**
Офлайн-редактирование документов	LibreOffice	N/A	LibreOffice*	LibreOffice	LibreOffice,; Notepad++
Онлайн-редактирование документов (совместная работа)	N/A	Cryptpad.fr	Cryptpad.fr,; Etherpad.org,; Privatebin.net	N/A	Cryptpad.fr,; Etherpad.org,; Privatebin.net
Редактирование изображений	Flameshot (L)	N/A	N/A	GIMP	GIMP
Редактирование аудио	Audacity	N/A	N/A	Audacity	Audacity
Редактирование видео	Flowblade (L)	N/A	N/A	N/A	Flowblade (L); Olive (?); OpenShot (?); ShotCut (?)
Запись экрана	Vokoscreen	N/A	N/A	N/A	Vokoscreen
Медиапроигрыватель	VLC	N/A	N/A	VLC	VLC
Просмотр PDF	Ristretto (L)	N/A	N/A	N/A	Браузер
Редактура PDF	PDF-Redact Tools (L)	N/A	N/A	PDF-Redact Tools (L)	LibreOffice,; PDF-Redact Tools (L)

Легенда: * Не рекомендуется, но упоминается. N/A = не включено или нет рекомендации для этого типа программ. (L)= только Linux, но, возможно, можно использовать на Windows/macOS другими способами (HomeBrew, виртуализация, Cygwin). (?)= не проверено, но имеет открытый исходный код и может быть рассмотрено.

Во всех случаях мы настоятельно рекомендуем использовать такие приложения только внутри виртуальной машины или Tails, чтобы максимально снизить риск утечек. Если вы этого не делаете, вам придётся тщательно очищать эти документы перед публикацией (см. аудит метаданных).

Передача чувствительной информации

Возможно, вы захотите анонимно передать информацию какой-либо организации, например прессе.

Если вам нужно это сделать, следует принять определённые меры, потому что нельзя доверять ни одной организации защиту вашей анонимности[54]. См. контрольный список того, что нужно проверить перед публикацией информации.

Для этого мы настоятельно рекомендуем использовать SecureDrop[55] (securedrop.org Archive.org) — проект с открытым исходным кодом от Freedom of the Press Foundation.

- Обязательно уделите время их "руководству для источников": docs.securedrop.org Archive.org
- В идеале SecureDrop нужно использовать через Tor; подготовленный список таких адресов можно найти здесь: github.com Archive.org

Если SecureDrop недоступен, можно рассмотреть другие способы связи, но предпочтение следует отдавать тем, где используется сквозное шифрование. **Никогда не делайте этого из-под вашей реальной личности; используйте только безопасную среду и анонимную личность.**

Без SecureDrop можно рассмотреть:

- Использование электронной почты с шифрованием GPG, если получатель где-то опубликовал свой ключ GPG. Его можно поискать здесь:
  - В проверенных аккаунтах получателя в социальных сетях (Twitter), если он его там указал.
  - На keybase.io (Tor-адрес keybase5wmilwokqirssclfnsqrjdsi7jdir5wy7y7iu3tanwmtp6oid.onion)
  - В каталогах OpenPGP, таких как: **(будьте осторожны: это публичные каталоги, и любой может загрузить любой ключ для любого адреса электронной почты; нужно сверить подпись с другими платформами, чтобы убедиться, что это действительно их ключ).**
    - pgp.mit.edu
    - keyserver.ubuntu.com
    - keys.openpgp.org
- Использование любой другой платформы (даже личных сообщений в Twitter), но опять же с шифрованием сообщения для получателя через GPG.

Чего следует избегать:

- Не отправляйте физические материалы почтой из-за риска оставить ДНК, отпечатки пальцев или другую отслеживаемую информацию (см. VPN, оплаченный наличными (предпочтительно)).
- Не используйте способы, привязанные к номеру телефона (даже одноразовому), например Signal/WhatsApp/Telegram.
- Не используйте голосовую или видеосвязь любого вида.
- Не раскрывайте никаких намёков на вашу реальную личность при обмене сообщениями.
- Не встречайтесь с людьми в реальной жизни, если только у вас нет абсолютно никакого другого варианта (это крайняя мера).

Если вы намерены раскрыть свою анонимность, чтобы защитить свою безопасность:

- Сначала очень тщательно оцените риски.
- Внимательно разберитесь в законности и безопасности вашего намерения, а также в последствиях для вас и других людей. Хорошо всё обдумайте.

• Возможно, перед этим стоит обратиться к **доверенному** юристу.

Задачи по поддержанию аккаунтов

• Время от времени следует аккуратно входить в свои аккаунты, чтобы они оставались активными.

• Регулярно проверяйте электронную почту на предмет проверок безопасности и любых других уведомлений по аккаунту.

• Регулярно проверяйте возможное появление признаков компрометации любой из ваших личностей через haveibeenpwned.com Archive.org (разумеется, из безопасной среды).

Сноски

[1] [назад] Wikipedia, Captcha en.wikipedia.org Wikiless Archive.org
[2] [назад] Wikipedia, Turing Test en.wikipedia.org Wikiless Archive.org
[3] [назад] Google reCAPTCHA google.com Archive.org
[4] [назад] hCaptcha hcaptcha.com Archive.org
[5] [назад] hCaptcha, hCaptcha Is Now the Largest Independent CAPTCHA Service, Runs on 15% Of The Internet hcaptcha.com Archive.org
[6] [назад] Nearcyan.com, You (probably) don't need ReCAPTCHA nearcyan.com Archive.org
[7] [назад] ArsTechnica, "Google's reCAPTCHA turns "invisible," will separate bots from people without challenges" arstechnica.com Archive.org
[8] [назад] BlackHat Asia 2016, "I'm not a human: Breaking the Google reCAPTCHA" blackhat.com Archive.org
[9] [назад] Google Blog security.googleblog.com Archive.org
[10] [назад] Cloudflare Blog, Cloudflare supports Privacy Pass blog.cloudflare.com Archive.org
[11] [назад] Privacy International, Timeline of SIM Card Registration Laws privacyinternational.org Archive.org
[12] [назад] Wikipedia, Device Fingerprinting en.wikipedia.org Wikiless Archive.org
[13] [назад] Chromium Documentation, Technical analysis of client identification mechanisms sites.google.com Archive.org
[14] [назад] Mozilla Wiki, Fingerprinting wiki.mozilla.org Archive.org
[15] [назад] Developers Google Blog, Guidance to developers affected by our effort to block less secure browsers and applications developers.googleblog.com Archive.org
[16] [назад] Wikipedia, KYC en.wikipedia.org Wikiless Archive.org
[17] [назад] Google Help, Access age-restricted content & features support.google.com Archive.org
[18] [назад] Wikipedia, Dark Pattern en.wikipedia.org Wikiless Archive.org
[19] [назад] The Verge, Tinder will give you a verified blue check mark if you pass its catfishing test theverge.com Archive.org
[20] [назад] DigitalInformationWorld, Facebook will now require you to Create a Video Selfie for Identity Verification digitalinformationworld.com Archive.org
[21] [назад] Vice.com, PornHub Announces 'Biometric Technology' to Verify Users vice.com Archive.org
[22] [назад] Variety, China Launches Hotline to Report Online Comments That 'Distort' History or 'Deny' Its Cultural Excellence variety.com Archive.org
[23] [назад] Wikipedia, Trust but verify en.wikipedia.org Wikiless Archive.org
[24] [назад] Wikipedia, Zero-trust Security Model en.wikipedia.org Wikiless Archive.org
[25] [назад] Wikipedia, Espionage, Organization en.wikipedia.org Wikiless Archive.org
[26] [назад] Medium.com, Kyle McDonald, How to recognize fake AI-generated images kcimc.medium.comScribe.rip Archive.org
[27] [назад] Jayway Blog, Using ML to detect fake face images created by AI blog.jayway.com Archive.org
[28] [назад] Wikipedia, Sim Swapping en.wikipedia.org Wikiless Archive.org
[29] [назад] Whonix Documentation, Tor Configuration whonix.org Archive.org
[30] [назад] Tor Browser Documentation, Editing Torrc support.torproject.org Archive.org
[31] [назад] English translation of German Telemedia Act huntonprivacyblog.com Archive.org. Section 13, Article 6, "The service provider must enable the use of Telemedia and payment for them to occur anonymously or via a pseudonym where this is technically possible and reasonable. The recipient of the service is to be informed about this possibility. ".
[32] [назад] Wikipedia, Real-Name System Germany en.wikipedia.org Wikiless Archive.org
[33] [назад] Facebook Onion Website facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion
[34] [назад] Google Help support.google.com Archive.org
[35] [назад] Google Help, Customer Matching Process support.google.com Archive.org
[36] [назад] Google, Your account is disabled support.google.com Archive.org
[37] [назад] Google, Request to restore the account support.google.com Archive.org
[38] [назад] Google Help, Update your account to meet age requirements support.google.com Archive.org
[39] [назад] Jumio, ID verification features jumio.com Archive.org
[40] [назад] Privacyguides.org recommended E-mail Providers privacyguides.org Archive.org
[41] [назад] Proton Registration Human Verification proton.me Archive.org
[42] [назад] Twitter Appeal Form help.twitter.com
[43] [назад] KnowYourMeme, Good Luck, I'm Behind 7 Proxies knowyourmeme.com Archive.org
[44] [назад] Wikipedia, end-to-end encryption en.wikipedia.org Wikiless Archive.org
[45] [назад] Wikipedia, Forward Secrecy en.wikipedia.org Wikiless Archive.org
[46] [назад] Proton Blog, What is zero-access encryption? proton.me Archive.org
[47] [назад] Wikipedia, Cambridge Analytica Scandal en.wikipedia.org Wikiless Archive.org
[48] [назад] Signal Blog, Technology preview: Sealed sender for Signal signal.org Archive.org
[49] [назад] Signal Blog, Private Contact Discovery signal.org Archive.org
[50] [назад] Signal Blog, Private Group System signal.org Archive.org
[51] [назад] Privacyguides.org, File-Sharing privacyguides.org Archive.org
[52] [назад] Privacyguides.org, Real-Time Communication privacyguides.org Archive.org
[53] [назад] Wikipedia, IPFS en.wikipedia.org Wikiless Archive.org

[54] [назад] Praxis Films, Open Letter from Laura Poitras praxisfilms.org Archive.org
[55] [назад] Wikipedia, SecureDrop en.wikipedia.org Wikiless Archive.org

Безопасное резервное копирование вашей работы

Никогда не загружайте зашифрованные файловые контейнеры с правдоподобным отрицанием (со скрытыми контейнерами внутри) в большинство облачных сервисов (iCloud, Google Drive, OneDrive, Dropbox) без мер предосторожности. Причина в том, что большинство облачных сервисов хранят резервные копии и версии ваших файлов, а такие резервные копии и версии зашифрованных контейнеров можно использовать для дифференциального анализа, чтобы доказать существование скрытого контейнера.

Вместо этого руководство рекомендует другие способы безопасного резервного копирования ваших данных.

Офлайн-резервные копии

Такие резервные копии можно делать на внешний жёсткий диск или USB-накопитель. Возможны разные варианты.

Резервные копии выбранных файлов

Требования

Для таких резервных копий вам понадобится USB-накопитель или внешний жёсткий диск с достаточным объёмом, чтобы вместить файлы, которые вы хотите сохранить.

Veracrypt

Для этой цели мы рекомендуем использовать Veracrypt на всех платформах (Linux/Windows/macOS) из-за удобства, безопасности и переносимости.

Обычные файловые контейнеры

Процесс довольно простой: достаточно следовать руководству Veracrypt здесь: veracrypt.fr Archive.org

В таком контейнере можно вручную хранить чувствительные данные или использовать любую утилиту резервного копирования, чтобы копировать файлы из операционной системы в этот контейнер.

Затем этот контейнер можно безопасно хранить где угодно.

Скрытые файловые контейнеры с правдоподобным отрицанием

Процесс тоже довольно простой и похож на предыдущее руководство, только в этот раз вы используете мастер Veracrypt, чтобы создать скрытый том Veracrypt вместо стандартного тома Veracrypt.

Можно создать скрытый том внутри существующего стандартного тома или просто использовать мастер для создания нового.

Допустим, вам нужен контейнер на 8 ГБ. Мастер сначала создаст "внешний том", где при запросе можно будет хранить отвлекающую информацию. В отвлекающий том следует положить несколько отвлекающих файлов: в чём-то чувствительных и правдоподобных, но не тех, которые вы хотите скрыть.

Затем Veracrypt попросит создать меньший скрытый контейнер (например, 2 ГБ или 4 ГБ) внутри внешнего тома; там можно хранить настоящие скрытые файлы.

Когда вы выбираете файл для монтирования в Veracrypt, в зависимости от введённого пароля будет смонтирован либо внешний отвлекающий том, либо скрытый том.

Затем можно смонтировать скрытый том и обычным образом использовать его для хранения чувствительных файлов.

Будьте осторожны при монтировании внешнего отвлекающего тома для обновления его содержимого. В этот момент нужно защитить скрытый том от перезаписи, потому что работа в отвлекающем томе может перезаписать данные в скрытом томе.

Для этого при монтировании отвлекающего тома выберите параметры монтирования, отметьте "Protect hidden volume" и на том же экране введите пароль скрытого тома. Затем смонтируйте отвлекающий том. Это защитит скрытый том от перезаписи при изменении отвлекающих файлов. Это также объясняется в документации Veracrypt: veracrypt.fr Archive.org

Будьте крайне осторожны с такими файловыми контейнерами:

- **Не храните несколько их версий и не держите их там, где выполняется версионирование (файловой системой или системой хранения). Эти файловые контейнеры должны быть одинаковыми везде, где вы их храните. Если где-то есть резервная копия таких контейнеров, она должна быть абсолютно идентична той, которой вы пользуетесь. Если не принять эту меру предосторожности, противник сможет сравнить две разные версии контейнера и доказать существование скрытых данных. Внимательно следуйте рекомендациям здесь: veracrypt.frArchive.org. Помните раздел Локальные утечки данных и криминалистика.**
- Мы настоятельно рекомендуем хранить такие контейнеры на внешних USB-накопителях, которые вы будете монтировать только из гостевых виртуальных машин и никогда из основной операционной системы. **После каждого изменения файлов следует очистить свободное пространство на USB-диске и убедиться, что любая резервная копия таких контейнеров абсолютно идентична на каждом накопителе и на вашем компьютере. См. раздел Как безопасно удалять отдельные файлы/папки/данные на HDD/SSD и USB-накопителях, чтобы узнать, как это сделать.**
- Если у вас есть время, **мы даже рекомендуем полностью стирать USB-накопители перед любыми изменениями таких контейнеров на компьютере (если вы не работаете напрямую с USB-накопителя).** Это нужно, чтобы противник, который изымет ваши устройства до того, как вы успеете обновить накопители, не получил несколько версий контейнеров, по которым можно криминалистическими методами доказать существование скрытых данных.

- **Никогда не храните такие контейнеры в облачных хранилищах, где есть резервные копии и где у вас нет прямого контроля над окончательным удалением. Они могут сохранять "старые версии" ваших файлов, которые затем также можно использовать в криминалистике, чтобы доказать существование скрытых данных.**
- Если вы монтируете скрытый том из основной операционной системы (**не рекомендуется**), после использования следует стереть все следы этого скрытого тома везде. Следы могут оставаться в разных местах: системных журналах, журналировании файловых систем, недавних документах в приложениях, индексировании, записях реестра и так далее. Чтобы удалить такие артефакты, обратитесь к разделу Некоторые дополнительные меры против криминалистики этого руководства. Особенно это важно в Windows. Лучше монтировать такие тома в гостевых виртуальных машинах. Например, в VirtualBox можно сделать снимок виртуальной машины перед открытием или работой со скрытым томом, а после использования восстановить снимок перед следующим открытием или работой с ним. Это должно стереть следы его присутствия и смягчить проблему. Основная операционная система может сохранить журналы подключения USB-накопителя, но не использования скрытого тома. Поэтому мы не рекомендуем использовать их из основной операционной системы.
- Не храните такие контейнеры на внешних SSD, если вы не уверены, что можете использовать на них Trim (см. раздел Понимание HDD и SSD).

Резервные копии всего диска/системы

Короткая версия: просто используйте Clonezilla, потому что в моих тестах она работала надёжно и стабильно на всех операционных системах, кроме Mac, где, вероятно, стоит использовать родные утилиты (Time Machine/Дисковую утилиту), чтобы избежать проблем совместимости, тем более что вы используете родное шифрование macOS. При использовании Windows не делайте резервную копию раздела со скрытой ОС, если используете правдоподобное отрицание (как объяснялось раньше, такая резервная копия может позволить противнику доказать существование скрытой ОС, сравнив последнюю резервную копию с текущей системой, где данные изменились, и тем самым разрушить правдоподобное отрицание; вместо этого используйте файловые контейнеры).

Здесь есть два варианта:

- (Не рекомендуется) Делать резервную копию из работающей операционной системы при помощи утилиты резервного копирования (коммерческие утилиты вроде EaseUS Todo Free, Macrium Reflect и так далее) или родных утилит вроде macOS Time Machine, QubesOS Backup, Ubuntu Deja Dup или Windows Backup.
  - Такая резервная копия может выполняться, пока операционная система работает.
  - Такая резервная копия будет зашифрована не дисковым шифрованием, а алгоритмом шифрования утилиты резервного копирования (которому придётся доверять и который в большинстве случаев нельзя по-настоящему контролировать). В качестве альтернативы можно отдельно зашифровать носитель резервной копии самостоятельно, например Veracrypt. Нам не известно ни одной бесплатной или платной утилиты, которая изначально поддерживает Veracrypt.
  - Некоторые утилиты позволяют делать дифференциальные или инкрементные резервные копии вместо полных.

    - Эти утилиты резервного копирования не смогут восстановить ваш зашифрованный диск "как есть", потому что они не поддерживают такие зашифрованные файловые системы изначально. Поэтому для восстановления системы в зашифрованном состоянии потребуется больше работы: повторное шифрование после восстановления.
- (Рекомендуется) Делать это офлайн с загрузочного накопителя, например с бесплатной Clonezilla с открытым исходным кодом.
    - Такую резервную копию можно делать только тогда, когда операционная система не запущена.
    - Такая резервная копия сохранит зашифрованный диск "как есть", а значит, будет по умолчанию зашифрована тем же механизмом. Это больше похоже на решение "запустил и забыл". Восстановление также восстановит шифрование "как есть", и система сразу будет готова к использованию после восстановления.
    - Этот метод не позволяет делать инкрементные или дифференциальные резервные копии, то есть каждый раз придётся заново делать полную резервную копию.
    - Этот метод проще всего сопровождать.

Мы много тестировали утилиты резервного копирования из работающей системы (Macrium Reflect, EaseUS Todo Reflect, Deja Dup и так далее) и лично считаем, что оно того не стоит. Вместо этого мы рекомендуем периодически создавать образ системы с помощью простой Clonezilla. Это намного проще выполнить, намного проще восстановить, и обычно это надёжно работает без проблем во всех случаях. И вопреки распространённому мнению, это не так уж медленно: большинство резервных копий занимает около часа, в зависимости от скорости целевого носителя.

Для резервного копирования отдельных файлов во время работы мы рекомендуем использовать файловые контейнеры или зашифрованные носители напрямую и вручную, как объяснялось в предыдущем разделе.

Требования

Вам понадобится отдельный внешний диск, где свободного места не меньше, чем на исходном диске, а лучше больше. Если в ноутбуке диск на 250 ГБ, для полного образа резервной копии понадобится минимум 250 ГБ свободного места. Иногда утилита резервного копирования существенно уменьшит объём за счёт сжатия, но как правило безопасности на резервном диске следует иметь не меньше места, чем на исходном, а лучше больше.

Некоторые общие предупреждения и соображения

- Если вы используете Secure Boot, вам понадобится утилита резервного копирования с поддержкой Secure Boot; к ним относятся AMD64-версии Clonezilla.
- Рассмотрите exFAT как файловую систему для дисков с резервными копиями: она обеспечивает лучшую совместимость между разными ОС (macOS, Linux и Windows), чем NTFS/HFS/ext4 и так далее.

Linux

Ubuntu

Мы рекомендуем использовать утилиту Clonezilla с открытым исходным кодом из-за удобства и надёжности, но есть много других родных утилит и методов Linux, которые можно использовать для этой цели.

Поэтому следуйте шагам из раздела Clonezilla.

QubesOS

Qubes OS рекомендует использовать собственную утилиту для резервного копирования, как описано здесь: qubes-os.org Archive.org. Но это просто хлопотно и даёт ограниченную добавленную ценность, если только вы не хотите сделать резервную копию одного отдельного Qube. Поэтому вместо этого мы также рекомендуем просто сделать полный образ с Clonezilla: это снимет все лишние сложности и вернёт вас к рабочей системе за несколько простых шагов.

Поэтому следуйте шагам из раздела Clonezilla.

Windows

Для этой цели мы рекомендуем только бесплатную утилиту Clonezilla с открытым исходным кодом. Есть коммерческие утилиты с той же функциональностью, но мы не видим у них преимуществ по сравнению с Clonezilla.

Несколько предупреждений:

- Если вы используете шифрование BitLocker с включённым TPM[1], возможно, вам также нужно будет где-то безопасно сохранить ключ BitLocker, потому что он может понадобиться для восстановления диска, если HDD/SSD или другие аппаратные компоненты изменились. Другой вариант — использовать BitLocker без TPM; тогда такая опция не понадобится. Но, опять же, мы вообще не рекомендуем использовать BitLocker.
- У вас всегда должна быть где-то под рукой резервная копия аварийного диска Veracrypt, чтобы можно было решить некоторые проблемы, которые всё ещё могут появиться после восстановления. Помните: этот аварийный диск не содержит вашу парольную фразу или какие-либо чувствительные сведения. Его можно хранить как есть.
- Если после сбоя вы заменили HDD/SSD, Windows 10/11 может отказаться загружаться, если изменился идентификатор жёсткого диска. Перед резервным копированием следует также сохранить этот идентификатор, потому что может понадобиться изменить идентификатор нового диска: Windows 10/11 может требовать совпадающий идентификатор перед загрузкой. См. Diskpart.
- **Если вы используете правдоподобное отрицание в Windows, НЕ делайте резервную копию раздела со скрытой ОС, потому что этот образ может быть использован криминалистами для доказательства существования скрытого тома, как объяснялось раньше. Резервную**

копию раздела с отвлекающей ОС можно делать без проблем, но раздел со скрытой ОС копировать нельзя.

Следуйте шагам из раздела Clonezilla.

macOS

Мы рекомендуем просто использовать родное резервное копирование Time Machine с шифрованием (и сильной парольной фразой, которая может совпадать с парольной фразой вашей ОС), согласно руководствам Apple: support.apple.com Archive.org и support.apple.com Archive.org.

Подключите внешний диск, и система должна предложить использовать его как резервную копию Time Machine.

Тем не менее стоит рассмотреть форматирование этого диска в exFAT, чтобы его также было удобно использовать в других ОС (Windows/Linux) без дополнительного программного обеспечения, по этому руководству: support.apple.com Archive.org

Это просто проще, и оно будет работать онлайн, пока вы работаете. Вы сможете восстановить данные на любом другом Mac из параметров восстановления, а также использовать этот диск для резервного копирования других устройств.

Также можно использовать Clonezilla, чтобы клонировать жёсткий диск Mac, но это может вызвать проблемы совместимости оборудования и, вероятно, почти ничего не добавит с точки зрения безопасности. Поэтому для macOS мы специально не рекомендуем Clonezilla.

Онлайн-резервные копии

Файлы

Это непростой вопрос. Проблема в том, что ответ зависит от вашей модели угроз.

- **Коротко: не храните файловые контейнеры с правдоподобным отрицанием (Veracrypt) онлайн.** Если вы используете контейнеры с правдоподобным отрицанием, их нельзя хранить ни на какой платформе, где у вас нет полного контроля над процессом удаления, потому что платформа, скорее всего, какое-то время хранит резервные копии предыдущих версий. И снова: эти предыдущие версии могут позволить криминалистам доказать существование скрытых данных и разрушить правдоподобное отрицание. Это относится к платформам вроде Dropbox, Google Drive, OneDrive и другим. Единственным допустимым онлайн-хранением таких файлов может быть "холодное хранение", то есть вы больше никогда не изменяете эти файлы и просто держите их отдельно, неизменными по сравнению с любой локальной версией.
- Если вы используете обычные зашифрованные резервные копии без правдоподобного отрицания, их можно хранить почти где угодно, если они правильно зашифрованы локально перед загрузкой (например, Veracrypt, с сильными парольными фразами и шифрованием). **Никогда не доверяйте шифрованию любого онлайн-провайдера. Доверяйте только собственному локальному шифрованию, например с помощью Veracrypt.** В таких случаях резервные копии можно хранить почти где угодно в аккаунтах ваших онлайн-личностей (iCloud, Google

Drive, Dropbox и так далее), если они сильно зашифрованы локально перед загрузкой. Но можно предпочесть и сервисы, заботящиеся о приватности, например Cryptpad.fr (1 ГБ).

Очевидно, что нельзя делать такие резервные копии или обращаться к ним с незащищённых/небезопасных устройств; используйте только выбранные ранее безопасные среды.

Самостоятельное размещение

Самостоятельное размещение, например с использованием Nextcloud, тоже возможно, если у вас есть анонимный хостинг.

См. Рекомендуемые VPS-провайдеры(#vps-hosting-providers).

Также примите во внимание предупреждение о Monero.

Облачное размещение

Для небольших файлов рассмотрите:

• Cryptpad.fr (cryptpad.fr): бесплатный тариф ограничен 1 ГБ суммарно; сервис рекомендован PrivacyGuides.org на privacyguides.org Archive.org

• Filen (filen.io): бесплатный тариф ограничен 10 ГБ суммарно

Сейчас нам не известно ни одной платформы онлайн-хранения или хостинга, принимающей оплату наличными, в отличие от провайдеров, упомянутых ранее.

Если вы всё же намерены хранить чувствительные данные на "массовых платформах" (Dropbox, Google Drive, OneDrive и так далее), **помните, что там никогда нельзя хранить контейнеры с правдоподобным отрицанием, и помните, что всё нужно шифровать и проверять локально (в том числе метаданные) перед загрузкой туда**. Это можно делать программным обеспечением вроде Veracrypt или Cryptomator (cryptomator.org). Никогда не загружайте на такие платформы незашифрованные файлы и, повторюсь, обращайтесь к ним только из безопасной изолированной виртуальной машины.

Информация

Если вы просто хотите сохранить информацию (текст), мы рекомендуем использовать безопасные и приватные сервисы для публикации текстовых фрагментов[2]. В основном мы будем придерживаться тех, которые рекомендует PrivacyGuides.org (privacyguides.org Archive.org):

• privatebin.info

• cryptpad.fr

На этих сервисах можно просто создать защищённый паролем документ с информацией, которую вы хотите сохранить.

Просто создайте документ, защитите его паролем и запишите в него информацию. Запомните адрес документа.

Синхронизация файлов между устройствами онлайн

Ответ на это очень простой, и по нему есть ясный консенсус для всех: syncthing.net Archive.org

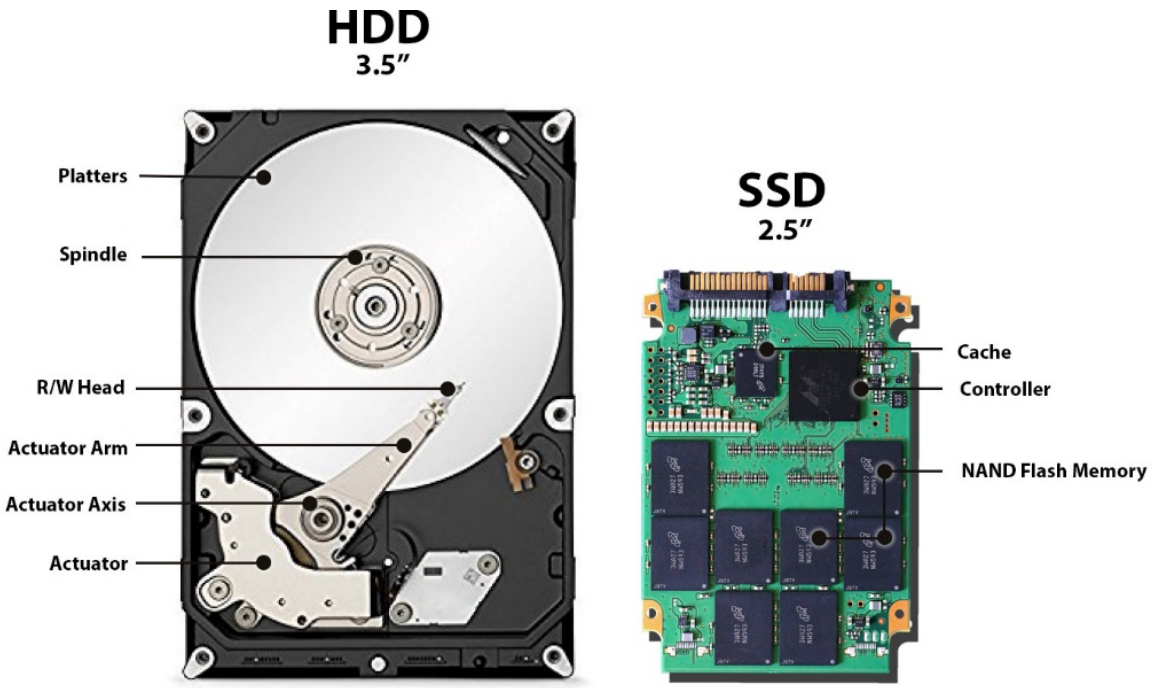
Просто используйте SyncThing: это самый безопасный и защищённый способ синхронизации между устройствами, он бесплатен, имеет открытый исходный код и может легко использоваться переносным способом без установки из контейнера, который нужно синхронизировать.

Сноски

[1] [назад] Wikipedia, TPM en.wikipedia.org Wikiless Archive.org
[2] [назад] Wikipedia, Pastebin en.wikipedia.org Wikiless Archive.org

Заметание следов

Понимание HDD и SSD



Если вы собираетесь стереть весь HDD в ноутбуке, процесс довольно прямолинеен. Данные записываются в точное место на магнитной (жёсткой) пластине (поэтому такой диск и называют жёстким диском), и ваша ОС точно знает, где они находятся на пластине, где их удалить и где перезаписать для безопасного удаления простыми способами (например, снова и снова перезаписывая это место, пока не останется следов).

С другой стороны, если вы используете SSD, процесс не так прост: накопитель использует несколько внутренних механизмов, чтобы продлить срок службы и повысить производительность. Три таких процесса особенно важны для нас в этом руководстве. SSD делятся на две основные категории:

• ATA-накопители (обычно SATA и обычно в формате 2,5 дюйма, как на изображении выше).

• NVMe-накопители (обычно формата M.2, как на иллюстрации ниже).

Вот примеры самых распространённых форматов:

Все они продаются как внутренние и внешние накопители в корпусах.

Методы и утилиты для управления ими и их стирания будут различаться в зависимости от типа накопителя, который вы используете. Поэтому важно знать, какой именно накопитель находится внутри вашего ноутбука.

В большинстве современных ноутбуков с высокой вероятностью будет один из средних вариантов (M.2 SATA или M.2 NVMe).

Выравнивание износа

Эти накопители используют технику под названием выравнивание износа[1]. На высоком уровне выравнивание износа работает так. Пространство на каждом диске делится на блоки, а блоки, в свою очередь, делятся на страницы, примерно как главы в книге состоят из страниц. Когда файл записывается на диск, ему назначается определённый набор страниц и блоков. Если бы вы хотели перезаписать файл на HDD, было бы достаточно сказать диску перезаписать эти блоки. Но в SSD и USB-накопителях стирание и повторная запись одного и того же блока изнашивают его. Каждый блок можно стереть и перезаписать только ограниченное число раз, прежде чем он просто перестанет работать (примерно как если постоянно писать и стирать карандашом на бумаге: в какой-то момент бумага может порваться и стать непригодной). Чтобы противодействовать этому, SSD и USB-накопители стараются сделать так, чтобы каждый блок стирался и перезаписывался примерно одинаковое число раз, и накопитель прослужил как можно дольше (отсюда и термин "выравнивание износа"). Побочный эффект состоит в том, что иногда вместо стирания и записи блока, где изначально хранился файл, накопитель оставляет этот блок нетронутым, помечает его как недействительный и просто записывает изменённый файл в другой блок. Это похоже на то, как если бы глава в книге осталась без изменений, изменённый файл был записан на другой странице, а оглавление книги просто обновилось и стало указывать на новое место. Всё это происходит на очень низком уровне в электронике диска, поэтому операционная система даже не понимает, что это произошло. Но это также означает, что даже если вы пытаетесь перезаписать файл, нет гарантии, что накопитель действительно его перезапишет; именно поэтому безопасное удаление на SSD намного сложнее.

Само по себе выравнивание износа может быть недостатком для безопасности и преимуществом для противников, например криминалистических экспертов. Эта функция делает классическое "безопасное удаление" контрпродуктивным и бесполезным, поэтому она была удалена из некоторых операционных систем, например macOS (начиная с версии 10.11 El Capitan), где раньше её можно было включить для корзины.

Большинство старых утилит безопасного удаления были написаны с расчётом на HDD, не контролируют выравнивание износа и совершенно бессмысленны при использовании SSD. Избегайте их на SSD.

Операции Trim

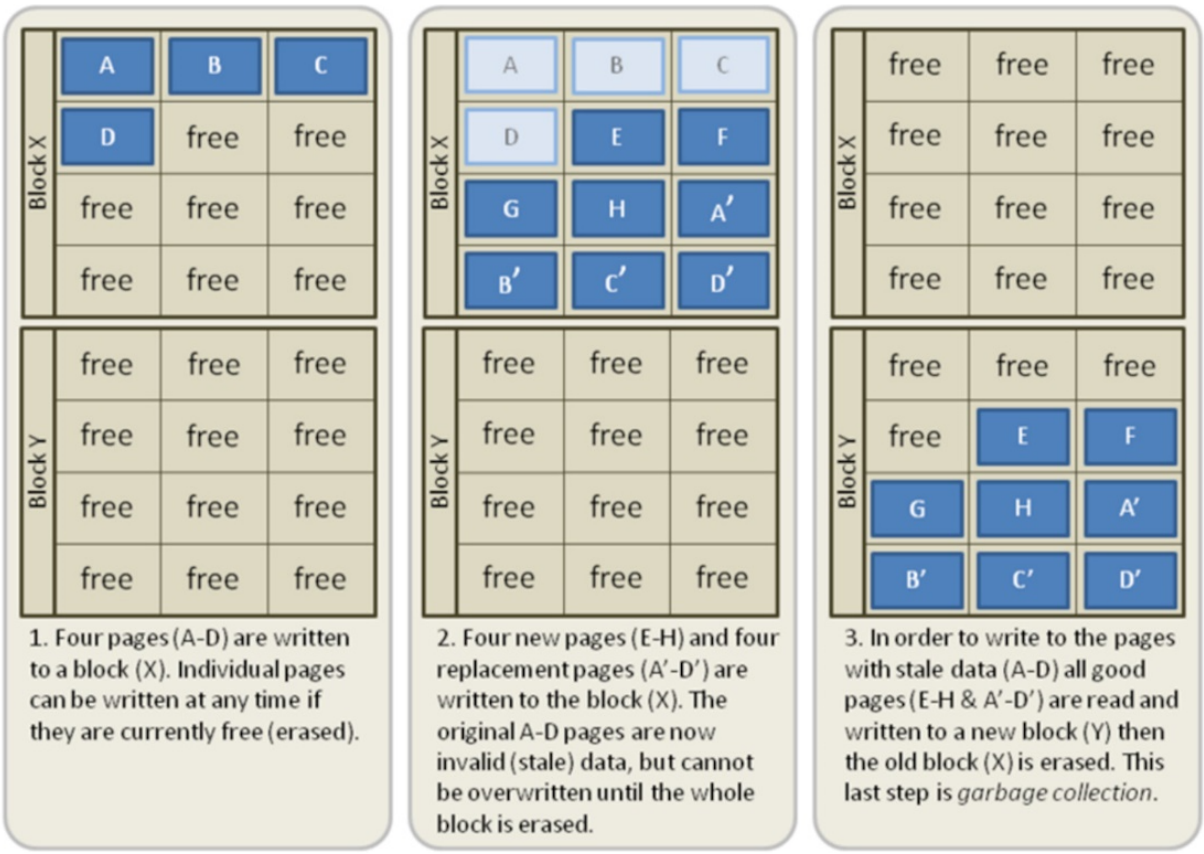
Что же теперь? Здесь появляется операция Trim[2]. Когда вы удаляете данные на SSD, ваша ОС должна поддерживать так называемую команду операции Trim и **может (и должна)** периодически отправлять эту команду SSD (ежедневно, еженедельно, ежемесячно и так далее). Эта команда сообщает контроллеру SSD, что в блоках есть страницы с данными, которые теперь свободны и могут быть действительно удалены, но сама ничего не удаляет.

Trim должен быть включён по умолчанию во всех современных операционных системах, которые обнаруживают SSD и рассматриваются в этом руководстве (macOS, Windows 10/11, Ubuntu, Qubes OS 4.1.x и так далее).

Если операции Trim не выполняются регулярно (или вообще не выполняются), данные заранее не удаляются, и в какой-то момент все блоки и страницы будут заняты данными. Ваша ОС этого не увидит и будет считать место свободным по мере удаления файлов, но контроллер SSD этого не увидит (это называется усилением записи[3]). Тогда контроллер SSD будет вынужден стирать эти страницы и блоки на лету, что снизит скорость записи. Причина в том, что, хотя ОС/SSD может записывать данные на любую свободную страницу в любом блоке, стирание возможно только целыми блоками; из-за этого SSD приходится выполнять много операций для записи новых данных. Перезапись просто невозможна. Это нарушит систему выравнивания износа и со временем приведёт к ухудшению производительности SSD. Каждый раз, когда вы удаляете файл на SSD, ОС должна отправлять команду Trim вместе с удалением, чтобы сообщить контроллеру SSD: страницы с данными файла теперь свободны для удаления.

Итак, сам Trim не удаляет данные, а только помечает их для удаления. Данные, удалённые без использования Trim (например, если Trim отключён, заблокирован или задержан), всё равно будут когда-нибудь удалены сборкой мусора SSD или когда вы захотите перезаписать то, что ОС считает свободным пространством. Но они могут сохраняться немного дольше, чем при использовании Trim.

Вот иллюстрация из Wikipedia, показывающая, как это работает на SSD:



Как видно на иллюстрации выше, данные (из файла) будут записаны на первые четыре страницы блока X. Позже новые данные будут записаны на оставшиеся страницы, а данные первых файлов будут помечены как недействительные (например, операцией Trim при удалении файла). Как объясняется на en.wikipedia.org Wikiless Archive.org, операция стирания может выполняться только целыми блоками (а не отдельными страницами).

Помимо пометки файлов для удаления (на надёжных SSD), Trim обычно делает их нечитаемыми с помощью метода под названием "Deterministic Read After Trim" или "Deterministic Zeroes After Trim". Это означает, что если противник попытается прочитать данные из страницы/блока после Trim и каким-то образом сумеет отключить сборку мусора, контроллер не вернёт никаких осмысленных данных.

Trim — ваш союзник, и при использовании SSD он должен быть всегда включён; он должен давать достаточную разумную защиту. По этой же причине не следует использовать правдоподобное отрицание Veracrypt на SSD с включённым Trim: эта функция несовместима с Trim[4].

Сборка мусора

Сборка мусора[5] — это внутренний процесс внутри SSD, который ищет данные, помеченные для стирания. Этот процесс выполняется контроллером SSD, и вы его не контролируете. Если вернуться к иллюстрации выше, вы увидите, что сборка мусора — последний шаг: она замечает, что в определённом блоке некоторые страницы помечены для удаления, затем копирует действительные страницы (не помеченные для удаления) в другой свободный целевой блок и после этого может стереть исходный блок целиком.

Сама по себе сборка мусора НЕ требует Trim для работы, но она будет намного быстрее и эффективнее, если Trim выполняется. Сборка мусора — один из процессов, который действительно окончательно стирает данные с SSD.

Заключение

Итак, факт в том, что криминалистическому эксперту очень маловероятно[6][7] и трудно восстановить данные с SSD после Trim, но это не полностью невозможно[8][9][10], если он действует достаточно быстро и имеет доступ к серьёзному оборудованию, навыкам и мотивации[11].

В контексте этого руководства, где также используется полное шифрование диска, удаление и Trim должны быть достаточно безопасны на любом SSD и будут рекомендованы как стандартный метод удаления.

Как безопасно стереть весь ноутбук/накопители

Итак, вы хотите быть уверены. Чтобы добиться стопроцентно безопасного удаления на SSD, нужно использовать специальные приёмы для SSD (если вы используете HDD, пропустите эту часть и переходите к вашей операционной системе):

- Простые варианты для менее опытных людей:
  - Если доступно, просто используйте параметр Secure Erase из BIOS/UEFI (ATA/NVME Secure Erase или Sanitize).
    - Стоит отметить, что это зависит от встроенного ПО накопителя. Некоторые производители накопителей ошибались в реализации, из-за чего данные всё ещё можно было восстановить.
  - Просто переустановите свежую операционную систему (удалите/быстро отформатируйте диск) и заново зашифруйте его. Процесс полного шифрования диска должен стереть все предыдущие данные с диска.
  - Купите PartedMagic[12] за 11 долларов и используйте его для стирания любого диска.
- Технические варианты для более продвинутых людей:
  - Перезаписать всё содержимое накопителя
    - HDD:
      - Перезапишите содержимое накопителя с помощью инструмента вроде srm, wipe, shred и так далее. В идеале стоит использовать метод Гутмана, созданный для максимально эффективного стирания данных на всех дисках. Этот метод работает и на SSD, хотя для них он чрезмерен.
      - Простого перезаписывания содержимого накопителя не всегда достаточно. Специализированные инструменты безопасного удаления рассчитаны на несколько проходов, чтобы эффективнее стирать данные. Это особенно важно на старых накопителях. Мы рекомендуем использовать либо `wipe`, либо `srm`.
        - Если используете `wipe`, просто применяйте параметры по умолчанию (`wipe /dev/sdX`), поскольку они настроены для наиболее эффективного стирания данных на HDD.
        - Если используете `srm`, обязательно вручную укажите стирание по Гутману (`srm -G /dev/sdX`).
    - SSD:
      - Перезапишите содержимое накопителя. Инструменты вроде wipe или shred часто чрезмерны, поскольку выполняют до 35 проходов. Они работают, но большинству SSD достаточно пары проходов.
      - Используйте `wipe` всего с парой проходов: `wipe -qQ2 /dev/sdX`.
        - `-qQ2` означает 2 прохода. Замените `2` на нужное число проходов.
      - Используйте `srm` с перезаписью в 3 прохода: `srm -P /dev/sdX`.
      - Используйте `dd`: `dd if=/dev/urandom of=/dev/sdX bs=8M status=progress conv=fsync`. Эта команда перезапишет накопитель случайными данными. Чтобы выполнить несколько проходов (я рекомендую минимум 2), просто запускайте команду снова, пока не будете удовлетворены.
        - Причина повторного запуска в том, что у SSD есть скрытое ("избыточно зарезервированное") пространство, где могут оставаться фрагменты удалённых данных. Двойное стирание заставляет накопитель стереть это зарезервированное пространство. Это гарантированно работает только если каждый проход записывает разные данные (поэтому в каждом проходе мы стираем случайными данными).

        - `bs=8M` записывает блоками по 8 МиБ за раз. Это не влияет на качество удаления данных, но изменение параметра может повлиять на длительность стирания.
    - ATA/NVMe Secure Erase: этот метод удалит таблицу сопоставления, которая отслеживает выделенные данные в блоках хранения, но не уничтожит сами данные.
    - ATA/NVMe Sanitize Crypto Scramble (он же Instant Secure Erase, Crypto Erase), применимый к самошифрующимся SSD: этот метод изменит ключ шифрования самошифрующегося SSD и сделает все хранящиеся на нём данные нечитаемыми.
    - ATA/NVMe Sanitize Block Erase: этот метод выполняет настоящее стирание каждого блока хранения, уничтожает данные и меняет ключ шифрования, если он есть.
    - ATA/NVMe Sanitize Overwrite **(ужасно медленно, может быть опасно и не рекомендуется)**: этот метод выполняет стирание блока, а затем перезаписывает каждый блок хранения (это то же самое, что Block Erase, но с дополнительной перезаписью данных). Этот метод чрезмерен и не нужен.
- Физическое уничтожение:
    - HDD:
        1. Откройте накопитель (отвёрткой, обычно Torx T8)
        2. Извлеките пластины (отвёрткой, обычно Torx T6)
        3. Потрите пластины редкоземельным магнитом
        4. Сломайте/деформируйте/раздавите пластины
        5. Сожгите пластины или прокалите их в духовке (**не** пропускайте этот шаг)
        6. Разделите обломки
        7. Выбросьте их в разных местах
    - SSD:
        - В идеале сначала следует стереть накопитель другими средствами, поскольку неизвестно, защищает ли один только этот метод от всех нападающих.
        1. Откройте накопитель
        2. Сломайте/раздавите плату и ячейки памяти
        3. Сожгите их
        4. Разделите обломки
        5. Выбросьте их в разных местах
    - Бонус: см. youtube.com Invidious

Для максимальной, даже чрезмерно параноидальной безопасности стоит предпочесть вариант Sanitize Block Erase, но Secure Erase, вероятно, более чем достаточно, учитывая, что ваш накопитель уже зашифрован. К сожалению, нет **бесплатных** простых универсальных инструментов (загрузочных, с графическим меню), поэтому придётся либо использовать инструменты производителей накопителей, либо бесплатные ручные утилиты hdparm[13] и nvme-cli[14], либо коммерческий инструмент вроде PartedMagic.

Поэтому это руководство рекомендует бесплатные утилиты hdparm и nvme-cli с использованием Live-системы System Rescue.

Если можете себе позволить, просто купите Parted Magic за 11 долларов: он предоставляет удобный графический инструмент для стирания SSD выбранным вами способом[15][16].

Примечание: Ещё раз: перед продолжением проверьте BIOS, потому что некоторые системы предлагают встроенный инструмент безопасного стирания накопителя (ATA/NVMe Secure Erase или ATA/NVMe Sanitize). Если он доступен, используйте его, и следующие шаги не понадобятся. Проверьте это заранее, чтобы избежать лишних хлопот; см. параметры BIOS/UEFI для стирания дисков у разных брендов.

Linux (все версии, включая Qubes OS)

Системный/внутренний SSD

- Вариант A: проверьте, есть ли в BIOS/UEFI встроенный параметр для этого, и если есть, используйте правильный вариант ("ATA/NVMe Secure Erase" или "ATA/NVMe Sanitize"). Не используйте стирание с проходами на SSD.
- Вариант B: см. Использование System Rescue для безопасного стирания SSD
- Вариант C: сотрите диск и переустановите Linux с новым полным шифрованием диска, чтобы перезаписать все секторы новыми зашифрованными данными. **Этот метод будет ужасно медленным по сравнению с вариантами A и B, потому что он будет медленно перезаписывать весь SSD. Также учтите, что при использовании LUKS это может быть не поведением по умолчанию. Возможно, придётся проверить параметр, который также шифрует пустое пространство, чтобы это действительно стёрло накопитель.**

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внешний SSD

Сначала см. Соображения по использованию внешних SSD

В большинстве случаев Trim должен быть достаточен, и можно просто использовать команду `blkdiscard`, чтобы принудительно выполнить Trim всего устройства, как объясняется здесь: wiki.archlinux.org Archive.org

Если ваш USB-контроллер и USB SSD поддерживают Trim и ATA/NVMe secure erase, можно осторожно стереть их через hdparm тем же методом, что и системный диск выше, только Linux на него вы, очевидно, устанавливать не будете. Но помните, что это не рекомендуется (см. соображения выше).

Если он не поддерживает Trim и/или ATA secure erase, можно (небезопасно) стереть накопитель обычным образом (без проходов, как HDD), а затем полностью заново зашифровать его выбранной утилитой (например, LUKS или Veracrypt). Процесс полного расшифрования и повторного шифрования диска перезапишет весь SSD и должен обеспечить безопасное стирание.

В качестве альтернативы можно также (небезопасно) стереть диск обычным способом, а затем полностью заполнить его псевдослучайными данными, что тоже должно обеспечить безопасное удаление (это можно сделать через BleachBit bleachbit.org Archive.org или из командной строки с помощью secure-delete по этому руководству: superuser.com Archive.org).

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внутренний/системный HDD

- Вариант A: проверьте, есть ли в BIOS/UEFI встроенный параметр, и если есть, используйте правильный вариант (Wipe + Passes в случае HDD).
- Вариант B: см. Использование ShredOS для безопасного стирания HDD
- Вариант C: сотрите диск и переустановите Linux с новым полным шифрованием диска, чтобы перезаписать все секторы новыми зашифрованными данными. **Этот метод будет ужасно медленным по сравнению с вариантами A и B, потому что он будет медленно перезаписывать весь HDD.**

Внешний/вторичный HDD и USB-накопители

- Вариант A: следуйте одному из этих руководств:
  - linuxhint.com Archive.org
  - linoxide.com Archive.org
  - wiki.archlinux.org Archive.org

Я рекомендую использовать для этой цели `dd` или `shred`.

- Вариант B: установите и используйте BleachBit bleachbit.org Archive.org или следуйте этому руководству EFF: ssd.eff.org Archive.org
- Вариант C: см. Использование ShredOS для безопасного стирания HDD

Windows

К сожалению, вы не сможете стереть основную ОС встроенными средствами Microsoft из настроек. Причина в том, что загрузчик был изменён Veracrypt, и операция завершится ошибкой. Кроме того, этот метод не был бы эффективен на SSD.

Системный/внутренний SSD

- Вариант A: проверьте, есть ли в BIOS/UEFI встроенный параметр для этого, и если есть, используйте правильный вариант ("ATA/NVMe Secure Erase" или "ATA/NVMe Sanitize"). Не используйте стирание с проходами на SSD.
- Вариант B: см. Инструменты производителей для стирания HDD и SSD
- Вариант C: см. Использование System Rescue для безопасного стирания SSD
- Вариант D: сотрите диск и переустановите Windows перед выполнением нового полного шифрования диска (с помощью Veracrypt или BitLocker), чтобы перезаписать все секторы новыми зашифрованными данными. **Этот метод будет медленнее вариантов A и B, потому что он перезапишет весь SSD.**

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внешний SSD

Сначала см. Соображения по использованию внешних SSD

Если возможно, используйте инструменты производителя. Такие инструменты должны поддерживать безопасное стирание или sanitize через USB и доступны для большинства брендов: см. Инструменты производителей для стирания HDD и SSD.

Если вы не уверены в поддержке Trim на вашем USB-диске, можно (небезопасно) стереть его обычным образом (достаточно простого быстрого форматирования), а затем снова зашифровать диск с помощью Veracrypt или BitLocker. Процесс полного расшифрования и повторного шифрования диска перезапишет весь SSD и должен обеспечить безопасное стирание.

В качестве альтернативы можно также (небезопасно) стереть диск обычным способом, а затем полностью заполнить его псевдослучайными данными, что тоже должно обеспечить безопасное удаление (это можно сделать через параметры стирания свободного места в BleachBit или PrivaZer). См. Очистка дополнительными инструментами.

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внутренний/системный HDD

• Вариант A: проверьте, есть ли в BIOS/UEFI встроенный параметр для этого, и если есть, используйте правильный вариант (Wipe + Passes).

• Вариант B: см. Инструменты производителей для стирания HDD и SSD

• Вариант C: см. Использование ShredOS для безопасного стирания HDD

Внешний/вторичный HDD и USB-накопители

• Вариант A: см. Инструменты производителей для стирания HDD и SSD

• Вариант B: используйте внешние инструменты, например:

  • Eraser (с открытым исходным кодом): eraser.heidi.ie Archive.org

  • KillDisk Free: killdisk.com Archive.org

• Вариант C: см. Использование ShredOS для безопасного стирания HDD

macOS

Системный/внутренний SSD

К сожалению, дисковая утилита восстановления macOS не сможет выполнить безопасное стирание SSD, как указано в документации Apple: support.apple.com Archive.org.

В большинстве случаев, если ваш диск был зашифрован FileVault и вы просто выполняете обычное стирание, по их мнению, этого должно быть "достаточно". По моему мнению, это не так, поэтому у вас нет другого варианта, кроме как переустановить macOS и после переустановки снова зашифровать её FileVault. Это должно выполнить "криптографическое стирание" за счёт перезаписи прежней установки и шифрования. К сожалению, этот метод будет довольно медленным.

Если вы хотите выполнить более быстрое безопасное стирание (или у вас нет времени на переустановку и повторное шифрование), можно попробовать метод, описанный в Использование System Rescue для безопасного стирания SSD **(это не сработает на Mac с M1)**. **Но будьте осторожны: это также сотрёт раздел восстановления, который нужен для переустановки macOS.**

Внешний SSD

Сначала см. Соображения по использованию внешних SSD

Если ваш USB-контроллер и USB SSD поддерживают Trim и ATA secure erase, и если Trim включён для диска в macOS, можно просто стереть весь диск обычным образом, и на современных дисках данные не должны быть восстановимы.

Если вы не уверены в поддержке Trim или хотите больше определённости, можно (небезопасно) стереть его с помощью дисковой утилиты macOS перед полным повторным шифрованием по двум руководствам Apple:

• support.apple.com Archive.org

• support.apple.com Archive.org или с помощью полного шифрования диска Veracrypt.

Процесс полного повторного шифрования диска перезапишет весь SSD и должен обеспечить безопасное стирание.

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внешний HDD и USB-накопители

Следуйте этому руководству: support.apple.com Archive.org и используйте параметр безопасного стирания в Дисковой утилите; он должен нормально работать на HDD и USB-накопителях.

Как безопасно удалять отдельные файлы/папки/данные на HDD/SSD и USB-накопителях

Здесь применяются те же принципы, что и в предыдущих главах. Возникают и те же проблемы.

На HDD можно безопасно удалить файлы, просто удалив их, а затем применив один или несколько "проходов" для перезаписи соответствующих данных. Это можно сделать многими утилитами во всех ОС.

На SSD, однако, всё снова становится немного сложнее, потому что из-за выравнивания износа, зависимости от операции Trim и сборки мусора накопителя вы никогда не можете быть уверены, что что-либо действительно удалено. Противник, у которого есть ключ расшифрования вашего SSD (будь то LUKS, FileVault 2, Veracrypt или BitLocker), может разблокировать накопитель и попытаться восстановить данные классическими утилитами восстановления[17]; если данные не были правильно обработаны Trim, это может получиться. Но, опять же, это крайне маловероятно.

Поскольку операция Trim на большинстве современных накопителей выполняется не непрерывно, а по расписанию, простого принудительного Trim должно быть достаточно. Но, опять же, единственный способ быть на 100% уверенным, что файл безопасно удалён с разблокированного зашифрованного SSD, — снова перезаписать всё свободное пространство после удаления нужных файлов или расшифровать и заново зашифровать накопитель. Но это чрезмерно и не нужно. Простого Trim всего диска должно быть достаточно.

Помните, что независимо от метода удаления любого файла на любом носителе (HDD, SSD, USB-накопителе), в системе, вероятно, останутся другие следы (журналы, индексирование, shellbags и так далее), и эти следы тоже придётся очищать. Также помните, что ваши накопители должны быть полностью зашифрованы, поэтому это, скорее всего, дополнительная мера. Подробнее об этом позже в разделе Некоторые дополнительные меры против криминалистики.

Windows

Помните: если вы вопреки всем рекомендациям используете правдоподобное отрицание на SSD, Trim использовать вообще нельзя.

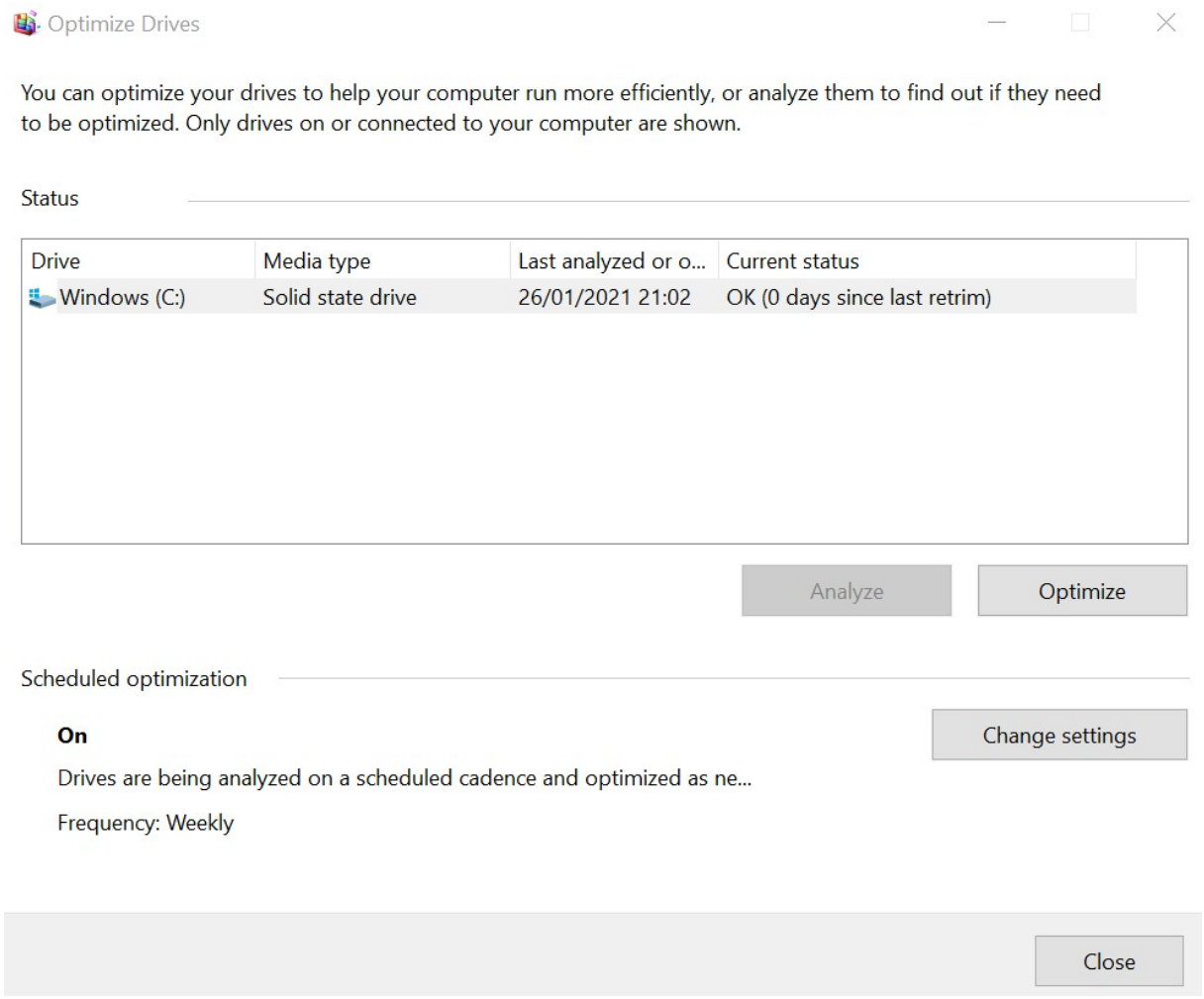
Системный/внутренний SSD

На этом этапе просто удалите файл окончательно (очистите корзину), а Trim и сборка мусора сделают остальное. Этого должно быть достаточно.

Если вы не хотите ждать периодического Trim (в Windows 10/11 по умолчанию он настроен еженедельно), можно также принудительно выполнить Trim всего диска с помощью родного инструмента Windows "Оптимизация" (см. Инструменты очистки Windows).

Если данные были удалены какой-либо утилитой (например, VirtualBox при откате снимка), можно также выполнить Trim всего диска тем же инструментом "Оптимизация", чтобы очистить всё оставшееся.

Просто откройте Проводник Windows, щёлкните правой кнопкой мыши системный диск и выберите "Свойства". Перейдите на вкладку "Сервис". Нажмите "Оптимизировать", затем снова "Оптимизировать", чтобы принудительно выполнить Trim. Готово. По моему мнению, этого, вероятно, достаточно.



Если вам нужна большая безопасность и вы не доверяете операции Trim, у вас останутся только такие варианты:

- Расшифровать и заново зашифровать весь накопитель (с помощью Veracrypt или BitLocker), чтобы перезаписать всё свободное пространство после удаления данных. Это обеспечит перезапись всего свободного пространства.
- Выполнить Trim, а затем заполнить всё свободное пространство диска утилитой вроде BleachBit или PrivaZer.

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внутренний/внешний HDD или USB-накопитель

Перед продолжением обратитесь к Инструментам очистки Windows и выберите утилиту.

Процесс довольно прост и зависит от выбранного инструмента из приложения:

• Щёлкните правой кнопкой мыши файл/папку:

  • PrivaZer: Delete without a trace

  • BleachBit: Shred with BleachBit (или см. это руководство EFF: ssd.eff.org Archive.org)

В случае USB-накопителей рассмотрите стирание свободного пространства одной из указанных выше утилит после удаления файлов или полное стирание накопителя через Eraser / KillDisk, как было описано ранее.

Внешний SSD

Сначала см. Соображения по использованию внешних SSD

Если Trim поддерживается и включён Windows для вашего внешнего SSD, проблем с безопасным удалением данных обычными командами удаления быть не должно. Дополнительно можно принудительно выполнить Trim с помощью родного инструмента Windows "Оптимизация" (см. Инструменты очистки Windows):

Просто откройте Проводник Windows, щёлкните правой кнопкой мыши системный диск и выберите "Свойства". Перейдите на вкладку "Сервис". Нажмите "Оптимизировать", затем снова "Оптимизировать", чтобы принудительно выполнить Trim. Готово. По моему мнению, этого, вероятно, достаточно.

Если Trim не поддерживается или вы не уверены, возможно, придётся обеспечить безопасное удаление данных так:

• Заполнить всё свободное пространство после любого удаления (например, с помощью BleachBit или PrivaZer).

• Расшифровывать и заново шифровать диск другим ключом после каждого удаления (с помощью Veracrypt или BitLocker).

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Linux (не Qubes OS)

Системный/внутренний SSD

Просто окончательно удалите файл (и очистите корзину), и он должен стать невосстановимым благодаря операциям Trim и сборке мусора.

Если вы не хотите ждать периодического Trim (в Ubuntu по умолчанию он настроен еженедельно), можно также принудительно выполнить Trim всего диска, запустив `fstrim --all` из терминала. Это немедленно отправит Trim и должно обеспечить достаточную безопасность. Эта утилита входит в пакет `util-linux` в Debian/Ubuntu и должна быть установлена по умолчанию в Fedora.

Если вам нужна большая безопасность и вы не доверяете операции Trim, у вас останутся только такие варианты:

- Расшифровать и заново зашифровать весь накопитель (например, через LUKS по этому руководству: wiki.archlinux.org Archive.org), чтобы перезаписать всё свободное пространство после удаления данных. Это обеспечит перезапись всего свободного пространства.
- Выполнить Trim через `fstrim --all`, а затем заполнить всё свободное пространство диска утилитой, например:
  - BleachBit bleachbit.org Archive.org
  - Установить пакет secure-delete и использовать `sfill` в корне накопителя:
    - Например, `sudo sfill -l -l /` должно сработать (это займёт значительное время)
  - Использовать старый метод через `dd` (взят из этого ответа: superuser.com Archive.org), запустив эти команды на накопителе, который нужно заполнить:
    - `dd if=/dev/zero of=zero.small.file bs=1024 count=102400`
    - `dd if=/dev/zero of=zero.file bs=1024`
    - `sync ; sleep 60 ; sync`
    - `rm zero.small.file`
    - `rm zero.file`

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внутренний/внешний HDD или USB-накопитель

- Можно сделать это графическим способом через BleachBit, следуя этому руководству EFF: ssd.eff.org Archive.org
- Или можно сделать это из командной строки по этому руководству: linuxhint.com Archive.org (для этой цели мы рекомендуем `wipe` и `shred`).

Внешний SSD

Сначала см. Соображения по использованию внешних SSD

Если Trim поддерживается и включён вашим дистрибутивом Linux для внешнего SSD, проблем с безопасным удалением данных быть не должно; просто выполните `fstrim --all` из терминала, чтобы применить Trim к накопителю. Эта утилита входит в пакет "util-linux" в Debian/Ubuntu и должна быть установлена по умолчанию в Fedora.

Если Trim не поддерживается или вы хотите быть уверены, возможно, придётся обеспечить безопасное удаление данных, заполнив всё свободное пространство диска одной из утилит:

- Расшифровать и заново зашифровать весь накопитель (например, через LUKS по этому руководству: wiki.archlinux.org Archive.org или через графический интерфейс Veracrypt), чтобы перезаписать всё свободное пространство после удаления данных. Это обеспечит перезапись всего свободного пространства.
- Заполнить свободное пространство одним из этих методов:
  - BleachBit bleachbit.org Archive.org
  - Установить пакет secure-delete и использовать `sfill` в корне накопителя:
    - Например, `sudo sfill -l -l /` должно сработать (это займёт значительное время)
  - Использовать старый метод через `dd` (взят из этого ответа: superuser.com Archive.org), запустив эти команды:
    - `dd if=/dev/zero of=zero.small.file bs=1024 count=102400`
    - `dd if=/dev/zero of=zero.file bs=1024`
    - `sync ; sleep 60 ; sync`
    - `rm zero.small.file`
    - `rm zero.file`

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Linux (Qubes OS)

Системный/внутренний SSD

Как и в других дистрибутивах Linux, обычного удаления и Trim должно быть достаточно на большинстве SSD. Поэтому просто окончательно удалите файл (и очистите любую корзину), и он должен стать невосстановимым благодаря периодическим операциям Trim и сборке мусора.

Чтобы выполнить Trim в Qubes OS, следуйте этой документации: github.com Archive.org

Как и в других системах Linux, если вам нужна большая безопасность и вы не доверяете операции Trim, у вас останутся только такие варианты:

- Расшифровать и заново зашифровать весь накопитель, чтобы перезаписать всё свободное пространство после удаления данных. Это обеспечит перезапись всего свободного пространства. Мы не нашли надёжного руководства о том, как безопасно сделать это в Qubes OS, но возможно, это руководство сработает: wiki.archlinux.org Archive.org (на ваш риск, это пока не проверено).
- Обратиться к этой документации (github.com Archive.org), затем выполнить Trim через `fstrim --all`, а после этого заполнить всё свободное пространство диска утилитой, например:
  - BleachBit bleachbit.org Archive.org
  - Установить пакет secure-delete и использовать `sfill` в корне накопителя:
    - Например, `sudo sfill -l -l /` должно сработать (это займёт значительное время)
  - Использовать старый метод через `dd` (взят из этого ответа: superuser.com Archive.org), запустив эти команды на накопителе, который нужно заполнить:
    - `dd if=/dev/zero of=zero.small.file bs=1024 count=102400`
    - `dd if=/dev/zero of=zero.file bs=1024`
    - `sync ; sleep 60 ; sync`
    - `rm zero.small.file`
    - `rm zero.file`

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

Внутренний/внешний HDD или USB-накопитель

Используйте тот же метод, что и в Linux, из Qube, подключённого к конкретному USB-устройству.

- Можно сделать это графическим способом через BleachBit, следуя этому руководству EFF: ssd.eff.org Archive.org
- Или можно сделать это из командной строки по этому руководству: linuxhint.com Archive.org (для этой цели мы рекомендуем `wipe` и `shred`).

Внешний SSD

Сначала см. Соображения по использованию внешних SSD

Если Trim поддерживается и включён вашим дистрибутивом Linux для внешнего SSD, проблем с безопасным удалением данных быть не должно; просто выполните `fstrim --all` из терминала, чтобы применить Trim к накопителю. Чтобы включить Trim на накопителе, обратитесь к этой документации (github.com Archive.org).

Если Trim не поддерживается или вы хотите быть уверены, возможно, придётся обеспечить безопасное удаление данных, заполнив всё свободное пространство диска утилитой из Qube, подключённого к соответствующему USB-устройству:

- Расшифровать и заново зашифровать весь накопитель (например, через LUKS по этому руководству: wiki.archlinux.org Archive.org или через графический интерфейс Veracrypt), чтобы перезаписать всё свободное пространство после удаления данных. Это обеспечит перезапись всего свободного пространства.
- Заполнить свободное пространство одним из этих методов:
  - BleachBit bleachbit.org Archive.org
  - Установить пакет secure-delete и использовать `sfill` в корне накопителя:
    - Например, `sudo sfill -l -l /` должно сработать (это займёт значительное время)
  - Использовать старый метод через `dd` (взят из этого ответа: superuser.com Archive.org), запустив эти команды:
    - `dd if=/dev/zero of=zero.small.file bs=1024 count=102400`
    - `dd if=/dev/zero of=zero.file bs=1024`

Повторите эти шаги на любом другом разделе, если на том же SSD есть отдельные разделы, перед удалением файлов.

- `sync ; sleep 60 ; sync`
- `rm zero.small.file`
- `rm zero.file`

Повторите эти шаги на любом другом разделе, если на том же SSD есть отдельные разделы.

Помните: все эти варианты нужно применять ко всему физическому накопителю, а не к отдельному разделу/тому. Иначе механизмы выравнивания износа могут помешать этому сработать правильно.

macOS

Системный/внутренний SSD

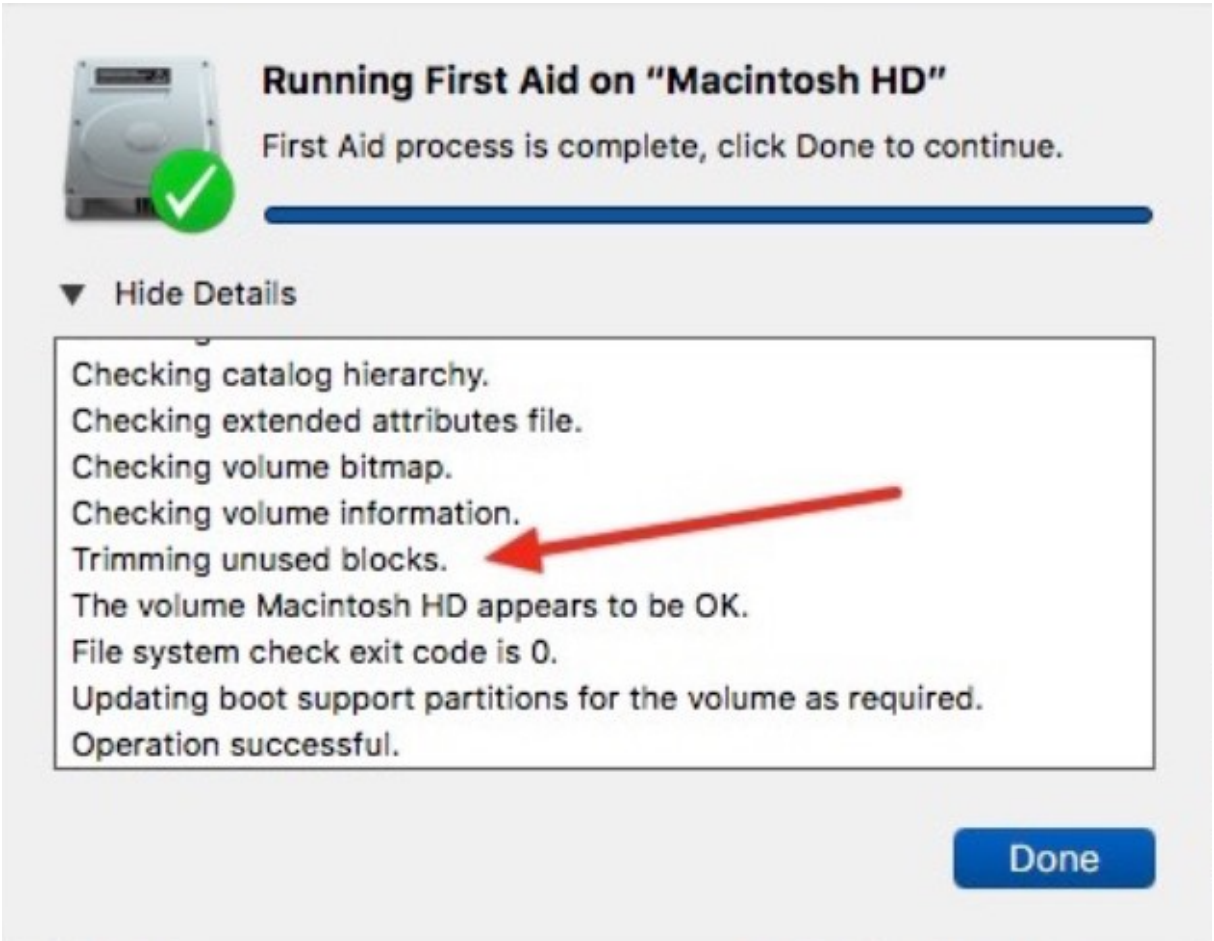
Просто окончательно удалите файл (и очистите корзину), и он должен стать невосстановимым благодаря операциям Trim и сборке мусора.

• Если ваша файловая система APFS, о Trim можно не беспокоиться: согласно документации Apple, он выполняется асинхронно, когда ОС записывает данные[18].

«Поддерживает ли Apple File System операции TRIM?

Да. Операции TRIM выдаются асинхронно после удаления файлов или освобождения свободного пространства; это гарантирует, что такие операции выполняются только после сохранения изменений метаданных в постоянном хранилище».

• Если ваша файловая система HFS+, можно запустить First Aid для системного диска из Дисковой утилиты; это должно выполнить операцию Trim, что будет видно в подробностях (support.apple.com Archive.org)



Системный/внутренний, внешний HDD или USB-накопитель

К сожалению, Apple удалила параметры безопасного стирания из корзины даже для HDD[19]. Поэтому остаётся использовать другие инструменты:

• Permanent Eraser edenwaith.com Archive.org

• Из терминала можно использовать команду `rm --P filename`, которая должна стереть файл и перезаписать его, как объясняется в этом руководстве EFF: ssd.eff.org Archive.org.

В случае USB-накопителей рассмотрите их полное стирание с помощью Дисковой утилиты, как было описано ранее.

Внешний SSD

Сначала см. Соображения по использованию внешних SSD

Если Trim поддерживается и включён macOS для вашего внешнего SSD, проблем с безопасным удалением данных быть не должно.

Если Trim не поддерживается, возможно, придётся обеспечить безопасное удаление данных так:

• Заполнить всё свободное пространство после любого удаления методом Linux выше (`dd`).

• Расшифровывать и заново шифровать диск другим ключом после каждого удаления (с помощью Дисковой утилиты или Veracrypt).

Некоторые дополнительные меры против криминалистики

Обратите внимание: здесь возникает та же проблема SSD, которая обсуждалась в предыдущем разделе. Вы никогда не можете быть на 100% уверены, что данные SSD удалены, когда вы просите накопитель это сделать, если только не стираете весь накопитель специальными методами выше.

Нам не известен ни один на 100% надёжный способ выборочно и безопасно удалять отдельные файлы на SSD, кроме перезаписи ВСЕГО свободного пространства (что может сократить срок службы SSD) после удаления этих файлов и Trim. Если этого не делать, придётся доверять операции Trim SSD, **что, по моему мнению, достаточно**. **Разумно считать, что криминалисты, опять же, с очень малой вероятностью смогут восстановить ваши файлы после удаления с Trim.**

Кроме того, большинство этих мер не должно быть нужно, поскольку весь ваш накопитель должен быть зашифрован, и поэтому ваши данные в любом случае не должны быть доступны для криминалистического анализа через исследование SSD/HDD. Так что это просто "бонусные меры" против слабых/неквалифицированных противников.

Также рассмотрите эту документацию, если используете Whonix: whonix.org Archive.org, а также их общее руководство по усилению защиты для всех платформ здесь: whonix.org Archive.org

Аудит метаданных

Преобразование формата не удаляет метаданные надёжно. Преобразование DOCX в PDF через Word встраивает метаданные документа Word в PDF. Печать в PDF несколько чище, но всё равно сохраняет сведения о программе-создателе. Безопасный путь — использовать специализированный инструмент.

Тип файла	Инструмент	Что проверить и удалить
JPEG / TIFF / HEIC	`exiftool -all= file.jpg`	EXIF, XMP, IPTC — все контейнеры
PNG	`exiftool -all= file.png`	фрагменты tEXt/iTXt, XMP
DOCX / XLSX / PPTX	MAT2 или Document Inspector в Word	Автор, история правок, отслеживаемые изменения, путь к шаблону, комментарии
PDF	`exiftool -all= file.pdf` или MAT2	пакет XMP, строка producer, автор, ключевые слова
Любой недоверенный файл	Dangerzone[20]	Преобразовать в безопасный PDF через изолированный контейнер, удалив все метаданные
Видео (MP4 / MOV)	`exiftool -all= file.mp4`	GPS, данные об устройстве, время создания, версия кодировщика

Самый безопасный рабочий процесс для публикации чувствительных документов: открыть оригинал в Dangerzone, который отрисует его в изолированном контейнере и экспортирует чистый PDF с удалёнными метаданными. Для изображений запустите `exiftool -all= -overwrite_original filename` и перед публикацией проверьте через `exiftool filename`, что результат чистый.

Изображения и видео

EXIF[21] (Exchangeable Image File Format) — это стандарт метаданных, используемый цифровыми камерами и смартфонами. Типичная фотография со смартфона содержит: координаты GPS в момент съёмки (широту, долготу, высоту и иногда направление); производителя, модель и серийный номер камеры; фокусное расстояние объектива; отметку времени, включая смещение часового пояса; и версию программы, использованной для обработки изображения.

Одних данных GPS часто достаточно, чтобы определить конкретную комнату в конкретном здании. В нескольких громких случаях установления источника ключевую роль сыграли геоданные EXIF в изображениях, отправленных журналистам или опубликованных в сети.

Почему удалить EXIF не всегда достаточно: EXIF — это один контейнер метаданных. Файлы JPEG и TIFF также поддерживают **XMP** (Extensible Metadata Platform)[22], формат метаданных, разработанный Adobe и встроенный в файл как XML-пакет. Инструменты, удаляющие EXIF, не обязательно удаляют XMP. XMP может содержать те же геоданные, авторство и данные об устройстве, а иногда и больше. ExifTool читает и записывает оба формата; многие более простые "удалители EXIF" вообще не трогают XMP. Кроме того, некоторые производители камер встраивают собственные метаданные в своё пространство имён внутри XMP, и они сохраняются даже после стандартного удаления EXIF.

Ещё одна тонкость: некоторые платформы (особенно старые версии Twitter и Facebook) удаляют EXIF на стороне сервера перед показом изображений, но хранят оригинал. Не полагайтесь на очистку платформой как на механизм приватности.

На Windows, macOS и Linux мы рекомендуем ExifTool (exiftool.org Archive.org) и/или ExifCleaner (exifcleaner.com Archive.org), которые позволяют просматривать и/или удалять эти свойства.

ExifTool изначально доступен в Tails и Whonix Workstation.

Метаданные PDF

PDF несут собственный слой метаданных. **Пакет XMP** в PDF может содержать автора, приложение-создатель (включая номер версии), производителя (программу, создавшую PDF, например "Microsoft Word 16.0.1" или конкретную версию LibreOffice), отметки времени создания и изменения, а также название документа. **Строка producer** особенно полезна следователям, потому что конкретные версии программ связаны с конкретными временными окнами и установками.

Менее очевидно, что **встраивание шрифтов** в PDF может создать цифровой отпечаток документа, указывающий на конкретную установку. Подмножества шрифтов — конкретные контуры символов, встроенные в PDF, — слегка различаются в зависимости от установленных шрифтов, используемого средства отрисовки и версии программы, создавшей файл. Сравнение встроенных данных шрифтов в нескольких документах может связать их с одним автором даже без каких-либо других идентифицирующих метаданных.[23]

PDFParanoia (Linux/Windows/macOS/QubesOS)

Рассмотрите github.com Archive.org, который удаляет метаданные и водяные знаки из любых PDF.

ExifCleaner (Linux/Windows/macOS/QubesOS)

Просто установите его с exifcleaner.com Archive.org, запустите и перетащите файлы в графический интерфейс.

ExifTool (Linux/Windows/macOS/QubesOS)

На самом деле всё просто: установите exiftool и запустите:

• Чтобы показать метаданные: `exiftool filename.pdf`

• Чтобы удалить все метаданные: `exiftool -All= filename.pdf`

ExifCleaner

Просто установите его с exifcleaner.com Archive.org, запустите и перетащите файлы в графический интерфейс.

ExifTool

На самом деле всё просто: установите exiftool и запустите:

• Чтобы показать метаданные: `exiftool filename.jpg`

• Чтобы удалить все метаданные: `exiftool -All= filename.jpg`

Помните, что ExifTool изначально доступен в Tails и Whonix Workstation.

Родной инструмент Windows

Вот руководство по удалению метаданных из изображения средствами ОС: purevpn.com Archive.org

Маскировка/запутывание для предотвращения распознавания изображений

Рассмотрите использование Fawkes sandlab.cs.uchicago.edu Archive.org (github.com Archive.org), чтобы замаскировать изображения от технологий распознавания на разных платформах.

Если нужны онлайн-версии, рассмотрите:

• lowkey.umiacs.umd.edu Archive.org

• adversarial.io Archive.org

DOCX и документы Office

Документы Microsoft Office — это ZIP-архивы с XML-файлами, а эти XML-файлы содержат обширные метаданные. Сюда входят: имя и инициалы автора (из профиля Office на момент создания); имя последнего изменившего; отметки времени создания и изменения; число правок; общее время редактирования; название компании из установки Office; путь к шаблону документа, использованному при создании (он может включать имя пользователя или сетевой путь); и, что критически важно, **история правок и отслеживаемые изменения** — удаления и правки, которые автор считал удалёнными, могут храниться в документе и быть восстановимы любым, кто откроет его достаточно способным средством просмотра.

Несколько случаев утечки документов журналистам привели к установлению источника, потому что имя автора или сетевое имя пользователя было встроено в XML. Метаданные John Doe указывали на реальных людей. Исправление — перед публикацией использовать **File → Inspect Document** в Word (он покажет скрытые данные и предложит удалить их) или использовать MAT2[20], чтобы полностью удалить метаданные. Преобразование в PDF не удаляет эти сведения надёжно; см. ниже.

В качестве альтернативы на Windows, macOS, Qubes OS и Linux мы рекомендуем ExifTool (exiftool.org Archive.org) и/или ExifCleaner (exifcleaner.com Archive.org), которые позволяют просматривать и/или удалять эти свойства.

ExifCleaner

Просто установите его с exifcleaner.com Archive.org, запустите и перетащите файлы в графический интерфейс.

ExifTool

На самом деле всё просто: установите exiftool и запустите:

• Чтобы показать метаданные: `exiftool filename.docx`

• Чтобы удалить все метаданные: `exiftool -All= filename.docx`

Документы LibreOffice

• Select Files in the upper menu
    • Select Properties
    • Uncheck "Apply User Data"
    • Uncheck "Save Preview image with the Document"
    • Click "Reset Properties"
    • Make sure there is nothing on the Description and Custom Properties tabs
• Select Tools in the upper menu
    • Select Options
    • Select Security
    • Click "Security Options and Warning"
    • Check:
        • "When printing"
        • "When saving or sending"
        • "When creating PDF files"
        • "Remove personal information on saving"

Кроме того, на Windows, macOS, Qubes OS и Linux мы рекомендуем ExifTool (exiftool.org Archive.org) и/или ExifCleaner (exifcleaner.com Archive.org), которые позволяют просматривать и/или удалять дополнительные свойства.

ExifCleaner

Просто установите его с exifcleaner.com Archive.org, запустите и перетащите файлы в графический интерфейс.

ExifTool

На самом деле всё просто: установите exiftool и запустите:

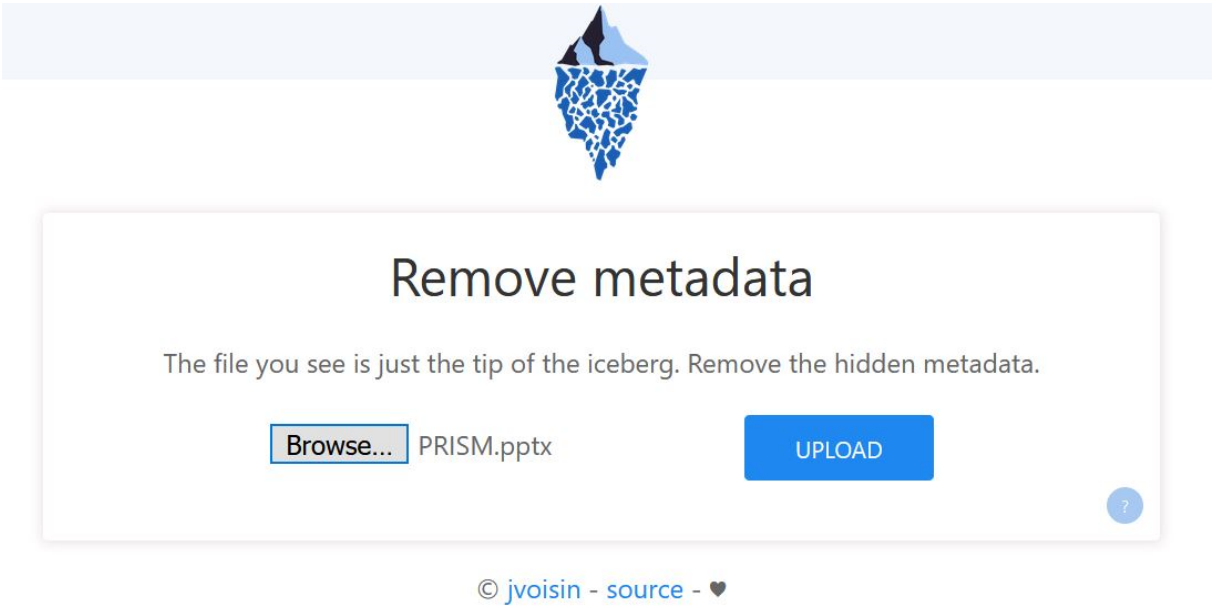
• Чтобы показать метаданные: `exiftool filename.odt`

• Чтобы удалить все метаданные: `exiftool -All= filename.odt`

Универсальный инструмент

Ещё один хороший инструмент для удаления метаданных из разных документов — mat2 с открытым исходным кодом, рекомендованный privacyguides.org[24] (0xacab.org Archive.org), который довольно легко использовать в Linux. Мне так и не удалось заставить его нормально работать в Windows из-за разных проблем с зависимостями, несмотря на предоставленные инструкции. Зато в Linux его очень просто установить и использовать.

Поэтому мы предлагаем создать небольшую виртуальную машину Debian в VirtualBox (за вашим Whonix Gateway), которую затем можно использовать из других виртуальных машин для анализа разных файлов через удобный веб-интерфейс. Для этого см. Создание гостевой ВМ mat2-web для удаления метаданных из файлов



Mat2 также предустановлен в ВМ Whonix Workstation[20] и доступен в Tails по умолчанию[25].

Tails

Tails отлично подходит для этого; вам не о чем беспокоиться, даже если вы используете SSD. Выключите его, и всё исчезнет, как только память потеряет содержимое.

Whonix

Обратите внимание: Whonix можно запускать в Live-режиме, не оставляя следов при выключении виртуальных машин. Подробнее см. их VM Live Mode Archive.org и Warning Archive.org.

macOS

Гостевая ОС

Вернитесь к более раннему снимку в VirtualBox (или в любой другой программе виртуализации, которую вы используете) и выполните команду Trim на Mac через Дисковую утилиту, снова запустив First Aid в основной ОС, как объяснено в конце следующего раздела.

Основная ОС

Большую часть сведений из этого раздела также можно найти в хорошем руководстве github.com Archive.org

База карантина (используется Gatekeeper и XProtect)

macOS (до Big Sur включительно) хранит SQL-базу карантина со всеми файлами, которые вы когда-либо загружали из браузера. Эта база находится в `~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2`.

Вы можете самостоятельно запросить её, выполнив в терминале команду: `sqlite3 ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2 "select * from LSQuarantineEvent"`

Для криминалистики это настоящая золотая жила, и её следует отключить:

- Выполните следующую команду, чтобы полностью очистить базу:
  `:>~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2`
- Выполните следующую команду, чтобы заблокировать файл и не дать записывать туда дальнейшую историю загрузок: `sudo chflags schg ~/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2`

Наконец, можно также полностью отключить Gatekeeper, выполнив в терминале следующую команду[26]:

• `sudo spctl --master-disable`

Подробнее см. этот раздел руководства: github.com Archive.org

Помимо этой удобной базы, каждый сохранённый файл также будет нести подробные атрибуты файловой системы HFS+/APFS, показывающие, например, когда он был загружен, чем и откуда.

Их можно увидеть, просто открыв терминал и набрав `mdls filename` и `xattr -l filename` для любого файла, загруженного из любого браузера.

Чтобы удалить такие атрибуты, придётся сделать это вручную из терминала:

• Выполните `xattr -d com.apple.metadata:kMDItemWhereFroms filename`, чтобы удалить источник

  • Также можно использовать `-dr`, чтобы сделать это рекурсивно для целой папки/диска

• Выполните `xattr -d com.apple.quarantine filename`, чтобы удалить ссылку на карантин

  • Также можно использовать `-dr`, чтобы сделать это рекурсивно для целой папки/диска

• Проверьте через `xattr --l filename`; вывода быть не должно

(Обратите внимание, что Apple удалила удобный параметр `xattr --c`, который раньше просто удалял все атрибуты сразу, поэтому теперь придётся делать это для каждого атрибута каждого файла)

Эти атрибуты и записи сохранятся даже если вы очистите историю браузера, и это, очевидно, плохо для приватности (правда?), а удобного инструмента, который сейчас справлялся бы с этим, нам не известно.

К счастью, есть способы смягчить проблему заранее, поскольку эти атрибуты и записи задаются браузерами. Поэтому мы протестировали разные браузеры (на macOS Catalina, Big Sur и Monterey), и вот результаты на дату этого руководства:

Браузер	Запись в базе карантина	Файловый атрибут карантина	Файловый атрибут источника
Safari (обычный режим)	Да	Да	Да
Safari (приватное окно)	Нет	Нет	Нет
Firefox (обычный режим)	Да	Да	Да
Firefox (приватное окно)	Нет	Нет	Нет
Chrome (обычный режим)	Да	Да	Да
Chrome (приватное окно)	Частично (только отметка времени)	Нет	Нет
Brave (обычный режим)	Частично (только отметка времени)	Нет	Нет
Brave (приватное окно)	Частично (только отметка времени)	Нет	Нет
Brave (окно Tor)	Частично (только отметка времени)	Нет	Нет
Tor Browser	Нет	Нет	Нет

Как вы сами видите, самый простой способ смягчить проблему — просто использовать приватные окна. Они не записывают эти атрибуты источника/карантина и не сохраняют записи в базе QuarantineEventsV2.

Очистить QuarantineEventsV2 легко, как объяснено выше. Удаление атрибутов требует некоторой работы. **Brave — единственный протестированный браузер, который по умолчанию не сохраняет эти атрибуты при обычной работе.**

Разные артефакты

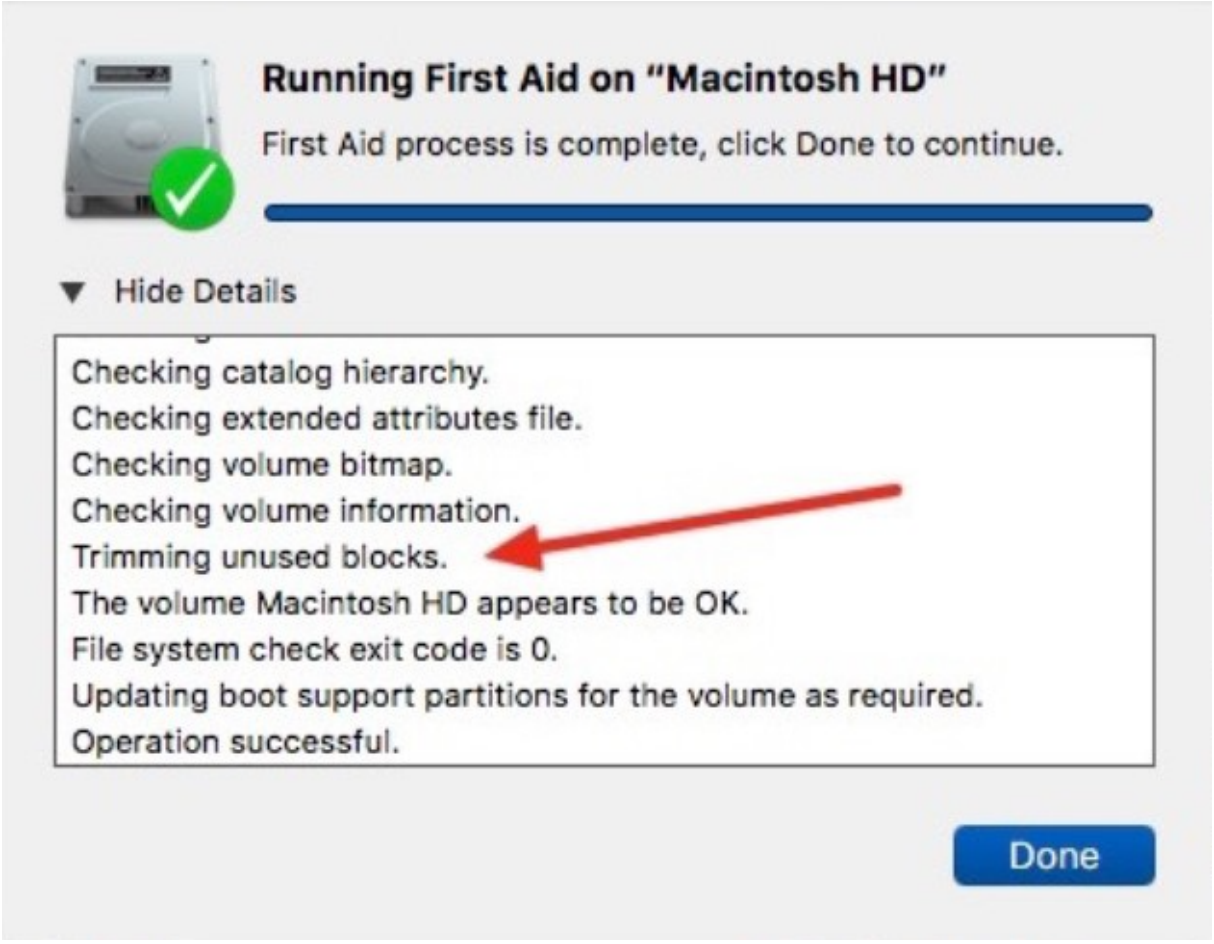
Кроме того, macOS хранит разные журналы смонтированных устройств, подключённых устройств, известных сетей, аналитики, правок документов и так далее.

См. этот раздел руководства, чтобы узнать, где искать и как удалять такие артефакты: github.com Archive.org

Многие из них можно удалить разными коммерческими сторонними инструментами, но лично мы рекомендуем использовать бесплатный и хорошо известный Onyx, который можно найти здесь: titanium-software.fr Archive.org. К сожалению, у него закрытый исходный код, но он нотариально заверен, подписан и пользуется доверием много лет.

Принудительное выполнение Trim после очистки

- Если ваша файловая система APFS, о Trim можно не беспокоиться: он выполняется асинхронно, когда ОС записывает данные.
- Если ваша файловая система HFS+ (или любая другая, кроме APFS), можно запустить First Aid для системного диска из Дисковой утилиты; это должно выполнить операцию Trim, что будет видно в подробностях (support.apple.com Archive.org).



Linux (Qubes OS)

Рассмотрите их рекомендации: github.com Archive.org

Если вы используете Whonix на Qubes OS, рассмотрите выполнение некоторых их руководств:

• Руководство Whonix System Hardening whonix.org Archive.org

• Включение App Armor в Qubes whonix.org Archive.org

• Также рассмотрите использование Linux Kernel Guard whonix.org Archive.org

Linux (не Qubes)

Гостевая ОС

Вернитесь к более раннему снимку гостевой ВМ в VirtualBox (или любой другой программе виртуализации, которую вы используете) и выполните команду Trim на ноутбуке через `fstrim --all`. Эта утилита входит в пакет `util-linux` в Debian/Ubuntu и должна быть установлена по умолчанию в Fedora. Затем переходите к следующему разделу.

Основная ОС

Обычно в основной ОС у вас не должно быть следов для очистки, поскольку, если вы следуете этому руководству, всё делается из ВМ.

Тем не менее, возможно, вы захотите очистить некоторые журналы. Рассмотрите этот удобный (но, к сожалению, неподдерживаемый) инструмент: github.com Archive.org

После очистки убедитесь, что утилита `fstrim` установлена (в Fedora должна быть по умолчанию) и входит в пакет `util-linux` в Debian/Ubuntu. Затем просто выполните `fstrim --all` в основной ОС. На SSD этого должно быть достаточно, как объяснялось ранее.

Рассмотрите Linux Kernel Guard как дополнительную меру: whonix.org Archive.org

Windows

Гостевая ОС

Вернитесь к более раннему снимку в VirtualBox (или любой другой программе виртуализации, которую вы используете) и выполните команду Trim в Windows с помощью "Optimize", как объясняется в конце следующего раздела.

Основная ОС

Теперь, когда у вас было много действий с ВМ или основной ОС, стоит уделить время заметанию следов. **Большинство этих шагов не следует выполнять в отвлекающей ОС при использовании правдоподобного отрицания. Причина в том, что вы хотите сохранить для противника отвлекающие/правдоподобные следы чувствительной, но не секретной активности. Если всё будет чисто, это может вызвать подозрения.**

Диагностические данные и телеметрия

Сначала избавимся от диагностических данных, которые ещё могли остаться:

• После каждого использования устройств Windows перейдите в Settings, Privacy, Diagnostic & Feedback и нажмите Delete.

Затем заново рандомизируем MAC-адреса виртуальных машин и Bluetooth-адрес основной ОС.

• После каждого выключения ВМ Windows изменяйте её MAC-адрес для следующего запуска: VirtualBox > выберите ВМ > Settings > Network > Advanced > Refresh the MAC address.

• После каждого использования основной ОС Windows (у ВМ вообще не должно быть Bluetooth) откройте Device Manager, выберите Bluetooth, отключите устройство и включите его снова (это принудительно рандомизирует Bluetooth-адрес).

Журналы событий

Журналы событий Windows будут хранить множество разных сведений, которые могут содержать следы ваших действий: какие устройства монтировались (включая, например, тома Veracrypt NTFS[27]), сетевые подключения, сведения о сбоях приложений и разные ошибки. Лучше регулярно очищать их. Не делайте этого в отвлекающей ОС.

• Откройте Start, найдите Event Viewer и запустите Event Viewer:

  • Перейдите в Windows logs.

  • Выберите и очистите все пять журналов через правый щелчок.

История Veracrypt

По умолчанию Veracrypt сохраняет историю недавно смонтированных томов и файлов. Нужно убедиться, что Veracrypt никогда не сохраняет историю. Опять же, не делайте этого в отвлекающей ОС, если используете правдоподобное отрицание для ОС. Нам нужно сохранить историю монтирования отвлекающего тома как часть правдоподобного отрицания:

• Запустите Veracrypt

• Убедитесь, что флажок "Never saves history" установлен (в отвлекающей ОС он не должен быть установлен)

Теперь следует очистить историю в любых приложениях, которыми вы пользовались, включая историю браузера, cookies, сохранённые пароли, сеансы и историю форм.

История браузера

• Brave (если вы не включили очистку при выходе)
    • Перейдите в Settings
    • Перейдите в Shields
    • Перейдите в Clear Browsing Data
    • Выберите Advanced
    • Выберите "All Time"
    • Отметьте все параметры
    • Clear Data
• Tor Browser
    • Просто закройте браузер, и всё будет очищено

История Wi-Fi

Теперь пора очистить историю Wi-Fi, к которым вы подключались. К сожалению, Windows продолжает хранить список прошлых сетей в реестре даже если вы "забыли" их в настройках Wi-Fi. Насколько нам известно, утилиты пока это не очищают (например, BleachBit или PrivaZer), поэтому придётся сделать это вручную:

• Запустите Regedit по этому руководству: support.microsoft.com Archive.org

• В Regedit введите это в адресную строку:
`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles`

• Там справа вы увидите множество папок. Каждая такая папка — это "ключ". Каждый ключ будет содержать сведения о текущих известных Wi-Fi или прошлых сетях, которые вы использовали. Можно просмотреть их по одному и увидеть описание справа.

• Удалите все эти ключи.

Shellbags

Как объяснялось ранее, Shellbags — это, по сути, история доступных томов/файлов на вашем компьютере. Помните, что shellbags — исключительно полезные источники информации для криминалистики[28], и их нужно очищать. Особенно если вы где-либо монтировали "скрытый том". Опять же, не делайте этого в отвлекающей ОС:

• Загрузите Shellbag Analyzer & Cleaner с privazer.com Archive.org
    • Запустите его
    • Analyze
    • Нажмите Clean и выберите:

    - Deleted Folders
    - Folders on Network / External devices
    - Search Results
- Select advanced
    - Отметьте всё, кроме двух параметров резервного копирования (не делать резервную копию)
    - Select SSD cleanup (если у вас SSD)
    - Select one pass (All zero)
    - Clean

Очистка дополнительными инструментами

После очистки предыдущих следов следует также использовать сторонние утилиты, которые могут очищать разные следы. В том числе следы файлов/папок, которые вы удалили.

Перед продолжением обратитесь к Инструментам очистки Windows.

PrivaZer

Шаги для PrivaZer:

- Загрузите и установите PrivaZer с privazer.com Archive.org
    - Запустите PrivaZer после установки
    - Не используйте их мастер
    - Выберите Advanced User
    - Выберите Scan in Depth и укажите цель
    - Выберите всё, что хотите просканировать, и нажмите Scan
    - Выберите, что хотите очистить (пропустите часть shellbag, поскольку для неё вы уже использовали другую утилиту)
        - **При использовании SSD следует просто пропустить очистку свободного пространства и вместо этого использовать родную функцию Windows Optimize (см. ниже), которой должно быть более чем достаточно. Мы использовали бы это только на HDD.**
    - (Если вы выбрали Free Space cleaning) Выберите Clean Options и убедитесь, что тип хранилища правильно определён (HDD или SSD).
    - (Если вы выбрали Free Space cleaning) В Clean Options **(будьте осторожны с этим параметром: он сотрёт всё свободное пространство на выбранном разделе, особенно если вы работаете в отвлекающей ОС. Не стирайте свободное пространство или что-либо ещё на втором разделе, иначе рискуете уничтожить скрытую ОС)**
        - Если у вас SSD:

        - Secure Overwriting Tab: мы бы просто выбрали Normal Deletion + Trim (самого Trim должно быть достаточно[29]). Secure Deletion with Trim[30] (1 проход) может быть избыточным и чрезмерным, если вы всё равно собираетесь перезаписывать свободное пространство.
        - Free Space Tab: лично мы, опять же "для уверенности", выбрали бы Normal Cleanup, который заполнит всё свободное пространство данными. Мы не очень доверяем Smart Cleanup, поскольку он фактически не заполняет всё свободное пространство SSD данными. Но, опять же, в большинстве случаев это, вероятно, не нужно и чрезмерно.
    - Если у вас HDD:
        - Secure Overwriting Tab: мы бы просто выбрали Secure Deletion (1 проход).
        - Free Space: мы бы просто выбрали Smart Cleanup, поскольку нет причин перезаписывать секторы без данных на HDD.
- Выберите Clean и нужный режим:
    - Turbo Cleanup выполнит только обычное удаление (на HDD/SSD) и не очистит свободное пространство. Это небезопасно ни на HDD, ни на SSD.
    - Quick Cleanup выполнит безопасное удаление (на HDD) и обычное удаление + Trim (на SSD), но не очистит свободное пространство. Для SSD это достаточно безопасно, но для HDD — нет.
    - Normal Cleanup выполнит безопасное удаление (на HDD) и обычное удаление + Trim (на SSD), а затем очистит всё свободное пространство (Smart Cleanup на HDD и Full Cleanup на SSD) и должен быть безопасным. Этот вариант лучший для HDD, но совершенно чрезмерен для SSD.
- Нажмите Clean и дождитесь завершения очистки. Это может занять время и заполнит всё свободное пространство данными.

BleachBit

Шаги для BleachBit:

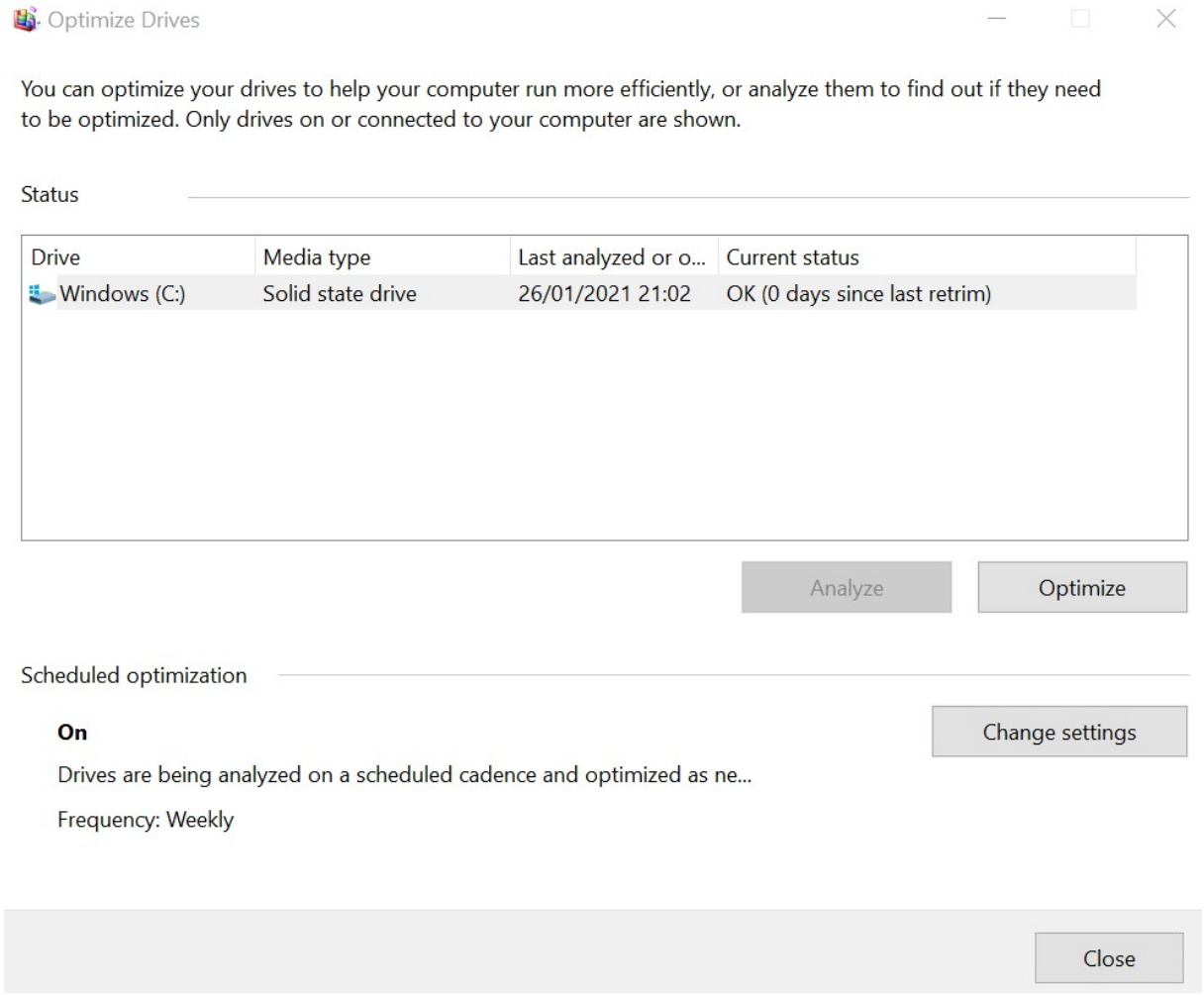
- Получите и установите последнюю версию BleachBit отсюда: bleachbit.org Archive.org
- Запустите BleachBit
- Очистите как минимум всё в этих разделах:
    - Deep Scan
    - Windows Defender
    - Windows Explorer (including Shellbags)
    - System
    - Выберите любые другие следы, которые хотите удалить из списка
        - Опять же, как и с предыдущей утилитой, мы не стали бы очищать свободное пространство на SSD, потому что считаем, что родной инструмент Windows "Optimize" достаточен (см. ниже), а заполнение свободного пространства на SSD с включённым Trim — совершенно чрезмерно и не нужно.

• Нажмите Clean и ждите. Это займёт время и заполнит всё свободное пространство данными как на HDD, так и на SSD.

Принудительное выполнение Trim через Windows Optimize (для SSD)

С помощью этой родной утилиты Windows 10/11 можно просто запустить Trim на SSD; этого должно быть более чем достаточно, чтобы безопасно очистить все удалённые файлы, которые каким-то образом могли избежать Trim при удалении.

Просто откройте Проводник Windows, щёлкните правой кнопкой мыши системный диск и выберите Properties. Выберите Tools. Нажмите Optimize and Defragment. Готово: это не выполнит дефрагментацию, а только оптимизацию, то есть запустит операцию Trim (en.wikipedia.org Wikiless Archive.org).



Удаление ваших личностей из поисковых систем и других платформ

Скорее всего, ваши действия (например, публикации на разных платформах и ваши профили) будут проиндексированы (и закэшированы) многими поисковыми системами.

Вопреки распространённому мнению, часть этой информации, хотя и не всю, можно удалить, выполнив несколько шагов. Даже если это не удалит информацию с самих сайтов, людям станет сложнее найти её через поисковые системы:

- Сначала нужно удалить ваши личности с самих платформ, если это возможно. Большинство позволит это сделать, но не все. Для некоторых придётся связаться с поддержкой/модераторами, а для других будут готовые формы.
- Если они не позволяют удалить профили, возможно, вы сможете переименовать свою личность. Измените имя пользователя, если можете, и все сведения аккаунта на фиктивные, включая электронную почту.
- Если разрешено, иногда можно также отредактировать старые публикации и удалить из них информацию.

Полезные сведения о том, как удалять разные аккаунты, можно посмотреть на этих сайтах:

- justdeleteme.xyz Archive.org
- justgetmydata.com Archive.org

Когда вы закончите с этой частью, следует заняться поисковыми системами. Хотя, возможно, вы не сможете удалить информацию, можно попросить их обновить/удалить устаревшие сведения, что может убрать часть кэшированной информации.

Google

К сожалению, для запроса обновления/удаления потребуется аккаунт Google (однако это можно сделать с любого аккаунта Google любого человека). Обойти это нельзя, кроме как ждать.

Перейдите на их страницу "Remove outdated content from Google Search": search.google.com Archive.org и отправьте соответствующий запрос.

Если ваш профиль/имя пользователя были удалены/изменены, они должны заново проиндексировать содержимое, обновить его и удалить эти следы.

Обработка таких запросов может занять несколько дней. Будьте терпеливы.

Bing

К сожалению, для запроса обновления/удаления потребуется аккаунт Microsoft (однако это можно сделать с любого аккаунта Microsoft любой личности). Обойти это нельзя, кроме как ждать.

Перейдите на их страницу "Content Removal": bing.com Archive.org и отправьте соответствующий запрос.

Если ваш профиль/имя пользователя были удалены/изменены, они должны заново проиндексировать содержимое, обновить его и удалить эти следы.

Обработка может занять несколько дней. Будьте терпеливы.

DuckDuckGo

DuckDuckGo не хранит кэшированную версию страниц[31], а вместо этого перенаправляет вас к кэшированной версии Google/Bing, если она доступна.

Кроме того, DuckDuckGo получает большую часть результатов поиска из Bing (а не Google)[32], поэтому удаление содержимого из Bing со временем должно убрать его и из DuckDuckGo.

Yandex

К сожалению, для запросов на удаление потребуется аккаунт Yandex (однако это можно сделать с любого аккаунта Yandex любой личности). Обойти это нельзя, кроме как ждать.

Когда у вас будет аккаунт Yandex, перейдите в Yandex Webmaster tools webmaster.yandex.com Archive.org, затем выберите Tools и Delete URL webmaster.yandex.com Archive.org

Там можно ввести URL, который больше не существует, если вы его удалили.

Это сработает только со страницами, которые были удалены, и поэтому не поможет удалить кэш существующих записей. Для этого, к сожалению, нет инструмента, который принудительно обновляет кэш, но можно попробовать их инструмент обратной связи:

Найдите изменённую страницу (где ваш профиль был удалён/изменён) и нажмите стрелку рядом с результатом. Выберите Complain. Отправьте жалобу о том, что страница не соответствует поисковому результату. Есть надежда, что это заставит Yandex через некоторое время снова обойти страницу и заново её проиндексировать. Это может занять дни или недели.

Qwant

Насколько нам известно, готового инструмента для принудительного обновления нет, и вам придётся ждать обновления результатов, если оно вообще произойдёт. Если вы знаете способ, сообщите нам об этом через GitHub issues.

Yahoo Search

Да, Yahoo Search всё ещё существует, но согласно их справочной странице help.yahoo.com Archive.org, кроме ожидания, нет способа удалить или обновить информацию. Это может занять 6-8 недель.

Baidu

Насколько нам известно, готового инструмента для принудительного обновления нет, если только вы не контролируете сайт (и не делаете это через их инструменты для веб-мастеров). Поэтому вам придётся ждать обновления результатов, если оно вообще произойдёт. Если вы знаете способ, сообщите мне об этом через GitHub issues.

Wikipedia

Насколько нам известно, удалить информацию из самих статей Wikipedia нельзя, но если вы просто хотите удалить следы вашего имени пользователя (как участника, который делал правки), это можно сделать, выполнив эти шаги: en.wikipedia.org Wikiless Archive.org

Это не удалит сведения о ваших онлайн-личностях, которые могут встречаться в других статьях, а только вашу собственную личность в Wikipedia как пользователя.

Archive.today

Некоторую информацию иногда можно удалить по запросу (например, чувствительную информацию), как видно по многочисленным примерам здесь: blog.archive.today

Это делается через их страницу "ask": blog.archive.today

Internet Archive

Вы можете удалить страницы из интернет-архивов, но **только если владеете соответствующим сайтом** и свяжетесь с ними по этому поводу. Скорее всего, вы не сможете удалить архивы, например, "публикаций Reddit" или чего-то похожего. Но можно всё равно спросить и посмотреть, что они ответят.

Согласно их справочной странице help.archive.org, можно отправить запрос на info@archive.org с URL в тексте сообщения, чтобы они рассмотрели исключение или удаление страниц из Wayback Machine.

Другие

Посмотрите эти сайты:

• justdeleteme.xyz

• inteltechniques.com Archive.org

Сноски

[1] [назад] Wikipedia, Wear Leveling en.wikipedia.org Wikiless Archive.org
[2] [назад] Wikipedia, Trim en.wikipedia.org Wikiless Archive.org
[3] [назад] Wikipedia, Write Amplification en.wikipedia.org Wikiless Archive.org
[4] [назад] Wikipedia, Trim Disadvantages en.wikipedia.org Wikiless Archive.org
[5] [назад] Wikipedia, Garbage Collection en.wikipedia.org Wikiless Archive.org
[6] [назад] Techgage, Too TRIM? When SSD Data Recovery is Impossible techgage.com Archive.org
[7] [назад] ResearchGate, Live forensics method for acquisition on the Solid-State Drive (SSD) NVMe TRIM function researchgate.net Archive.org
[8] [назад] ElcomSoft, Life after Trim: Using Factory Access Mode for Imaging SSD Drives blog.elcomsoft.com Archive.org
[9] [назад] Forensic Focus, Forensic Acquisition Of Solid State Drives With Open Source Tools forensicfocus.com Archive.org
[10] [назад] ResearchGate, Solid State Drive Forensics: Where Do We Stand? researchgate.net Archive.org
[11] [назад] BleepingComputer, Firmware attack can drop persistent malware in hidden SSD area bleepingcomputer.com Archive.org
[12] [назад] Wikipedia, Parted Magic en.wikipedia.org Wikiless Archive.org
[13] [назад] Wikipedia, hdparm en.wikipedia.org Wikiless Archive.org
[14] [назад] GitHub, nvme-cli github.com Archive.org
[15] [назад] PartedMagic Secure Erase partedmagic.com Archive.org
[16] [назад] Partedmagic NVMe Secure Erase partedmagic.com Archive.org
[17] [назад] UFSExplorer, Can I recover data from an encrypted storage? ufsexplorer.com Archive.org
[18] [назад] Apple Developer Documentation developer.apple.com Archive.org
[19] [назад] EFF, How to: Delete Your Data Securely on macOS ssd.eff.org Archive.org
[20] [назад] Whonix Documentation, Scrubbing Metadata whonix.org Archive.org
[21] [назад] Bellingcat, Joseph Mifsud: Rush for the EXIF bellingcat.com Archive.org
[22] [назад] Adobe, XMP Specification adobe.com Archive.org
[23] [назад] Proceedings on Privacy Enhancing Technologies, Linking Documents via Font Metadata (2019) petsymposium.org Archive.org
[24] [назад] Privacyguides.org, Productivity tools privacyguides.org Archive.org
[25] [назад] Tails documentation, MAT gitlab.tails.boum.org Archive.org
[26] [назад] GitHub, Disable Gatekeeper on macOS Big Sur (11.x) disable-gatekeeper.github.io Archive.org
[27] [назад] Veracrypt Documentation, Data Leaks veracrypt.fr Archive.org
[28] [назад] SANS, Windows ShellBag Forensics in-depth sans.org Archive.org
[29] [назад] St Cloud State University, Forensic Research on Solid State Drives using Trim Analysis web.archive.org Archive.org
[30] [назад] Wikipedia, Trim en.wikipedia.org Wikiless Archive.org
[31] [назад] DuckDuckGo help, Cache help.duckduckgo.com Archive.org
[32] [назад] DuckDuckGo help, Sources help.duckduckgo.com Archive.org

Низкотехнологичные старые приёмы

Спрятать коммуникацию на виду

Вы должны помнить, что использование всех этих мер безопасности (шифрование, правдоподобное отрицание, VPN, Tor, безопасные операционные системы и так далее) само по себе может сделать вас подозрительным. Для наблюдателя их использование может быть равносильно открытому заявлению "мне есть что скрывать", а это может побудить некоторых противников расследовать вас или наблюдать за вами дальше.

Поэтому есть и другие способы обмениваться сообщениями в сети или отправлять их другим людям при необходимости, не раскрывая свою личность и не устанавливая с ними прямую связь. Разные организации используют такие способы десятилетиями; они могут помочь, если вы не хотите привлекать внимание использованием безопасных технологий, но всё равно хотите передать чувствительную информацию незаметно.

Одна распространённая техника сочетает идею тайника[1] и запутывания защищённой коммуникации[2] через стеганографию[3] и/или клептографию[4]. У неё много названий, например Koalang[5], "Talking Around" или даже "социальная стеганография". Эта техника очень старая и до сих пор широко используется подростками для обхода родительского контроля. Это сокрытие на виду.

Вот пример: что если вы хотите дать кому-то понять, что что-то пошло не так и ему нужно уйти в тень? Что ему нужно немедленно стереть все данные, избавиться от одноразовых телефонов и чувствительной информации?

Что если вы хотите дать доверенному человеку (друзьям, семье, юристам, журналистам и так далее) знать, что у вас неприятности и за вами нужно присмотреть?

И всё это без раскрытия личности человека, которому вы отправляете сообщение, без раскрытия содержания сообщения третьим сторонам, без вызова подозрений и без использования каких-либо безопасных методов, упомянутых выше.

Можно просто использовать для этого любую публичную онлайн-платформу (Instagram, Twitter, Reddit, любой форум, YouTube и так далее), применяя кодовые сообщения, согласованные заранее между вами и вашим контактом и вписанные в контекст выбранной платформы/медиа. Понять их должен только ваш контакт.

Это может быть набор конкретных эмодзи или обычный на вид комментарий с особой формулировкой. Или даже просто лайк на конкретной публикации известного автора, которого вы обычно смотрите и лайкаете. Для всех остальных это будет выглядеть совершенно нормально, но для осведомлённого читателя может означать многое и запустить заранее согласованные действия. Можно также скрыть сообщение с помощью стеганографии, например через stegcloak.surge.sh.

Можно даже не заходить так далеко. Простого времени "Last seen" в конкретном аккаунте может быть достаточно, чтобы запустить заранее согласованное сообщение. Если ваш собеседник видит, что этот аккаунт был онлайн, это может означать, что возникла проблема.

Как заметить, что кто-то обыскивал ваши вещи

Есть несколько старых приёмов, которые помогут заметить, что кто-то трогал ваши вещи, пока вас не было.

Один приём, например, очень прост и требует только провода/кабеля. Просто разложите предметы на столе/тумбочке или в ящиках по прямой линии. Можно использовать простой USB-кабель как инструмент для выравнивания.

Сделайте линию кабелем и расположите предметы вдоль неё. Когда вернётесь, просто проверьте эти места и посмотрите, остаются ли предметы на линии. Так вам не нужно точно помнить, где лежали вещи, и не нужно фотографировать.

К счастью, современные технологии сделали это ещё проще. Если вы подозреваете, что кто-то может рыться в ваших вещах, пока вас нет, можно просто сфотографировать область телефоном перед уходом. Когда вернётесь, сравните места с фотографиями, и всё должно быть ровно там, где вы оставили. Если что-то сдвинулось, значит, кто-то там был.

Противнику будет чрезвычайно трудно и долго обыскать ваши вещи, а затем с полной точностью вернуть всё именно так, как было.

А если это распечатанный документ или книга, и вы хотите узнать, читал ли его кто-то? Ещё проще. Аккуратно сделайте в документе пометку карандашом. Затем сотрите её любым ластиком так, будто хотели исправить. Суть в том, чтобы осторожно оставить следы/крошки ластика на месте, где вы стирали или писали карандашом, и закрыть документ. Можно также сфотографировать крошки перед закрытием документа.

Скорее всего, если кто-то откроет ваш документ, чтобы прочитать его, а потом аккуратно положит обратно, эти крошки упадут или заметно сдвинутся. Это простой старый приём, который может показать, что кто-то обыскивал ваш документ.

Сноски

[1] [назад] Wikipedia, Dead Drop en.wikipedia.org Wikiless Archive.org
[2] [назад] Wikipedia, Secure Communication Obfuscation en.wikipedia.org Wikiless Archive.org
[3] [назад] Wikipedia, Steganography en.wikipedia.org Wikiless Archive.org
[4] [назад] Wikipedia, Kleptography en.wikipedia.org Wikiless Archive.org
[5] [назад] Wikipedia, Koalang en.wikipedia.org Wikiless Archive.org

Последние мысли об OPSEC

Подождите, что такое OPSEC? OPSEC означает Operations Security[1], то есть операционная безопасность. Базовое определение такое: OPSEC — это процесс защиты отдельных фрагментов данных, которые можно собрать вместе и получить более полную картину.

Важный шаг здесь, и, вероятно, самый простой, — урок из фильма Fight Club: первое правило в том, что вы **не** говорите о Fight Club. Это относится ко многим аспектам вашей операционной безопасности в сети, или OPSEC. Время, потраченное на это руководство, даст вам инструменты и знания для более полноценного и безопасного опыта в интернете. Будьте уверены: это руководство покажет вам вещи, которые расстроят вашего противника. Вы узнаете, как защищать операционные системы, блокировать критически важную информацию и обеспечивать успех миссии. Но единственное, чего вы должны придерживаться, — это правило: не говорите о деталях операции. Самая большая враждебная угроза для вас — OSINT (обсуждается ниже и по всему документу). Противник будет собирать информацию о вас по тому, что наблюдает в ваших действиях в сети и в реальной жизни.

Противники бывают разными. Для одних это представители иностранного государства, для других — просто сотрудник конкурирующей компании, который ищет недовольных работников, чтобы затем давить на них. В общем смысле задача OPSEC такова: это ваш корабль, и вы не должны делать или говорить ничего, что потопит ваш собственный корабль. Простого выражения недовольства начальником, условиями работы или оборудованием может хватить, чтобы создать не только поведенческий профиль, но и вектор атаки. В этом примере недовольный сотрудник обычно даёт достаточно информации, чтобы оправдать давление на него ради дальнейших сведений, а возможно, и вымогательство, шантаж или что-то хуже. Невыполнение базового OPSEC может привести к провалу в разных точках. Это может привести к серьёзной травме или даже смерти, если ваша модель угроз включает решительного нападающего, иностранного субъекта и так далее.

Вы должны жить по простому правилу: "болтливость топит корабли", но помнить, что обычно топят их именно ваши губы. OPSEC часто сводится к здравому смыслу и осторожности в ваших действиях, включая физический мир:

Цифровой и сетевой OPSEC

- **Помните: используйте парольные фразы или наборы слов вместо коротких паролей и используйте разные для каждого сервиса. См. Рекомендации по паролям и парольным фразам.**
- Убедитесь, что после этого вы не храните копию этого руководства в небезопасном месте. Одно только наличие этого руководства, скорее всего, разрушит все ваши возможности правдоподобного отрицания.
- Время от времени проводите OSINT по себе и своим личностям: ищите их в сети через разные поисковые системы, чтобы отслеживать свои онлайн-личности. Этот процесс можно даже частично автоматизировать разными инструментами, например Google Alerts google.com Archive.org.

- Никогда не используйте одну только биометрию для защиты ваших секретов. Биометрию можно использовать без вашего согласия.
- Проверяйте подписи и хэши программ и документов, которые вы скачиваете, перед установкой/просмотром.
- Не ведите себя одинаково: например, не посещайте одни и те же ссылки в обычном интернете, а затем те же ссылки под вашей анонимной онлайн-личностью. Посмотрите это выступление DEF CON 25, если ещё не смотрели: DEF CON 25 - Svea Eckert, Andreas Dewes - Dark Data Invidious.
- Шифруйте всё, но не считайте это полной гарантией. Помните про гаечный ключ за 5 долларов.

Физический OPSEC и реальная жизнь

- Помните о "Физической защите ноутбука от вмешательства".
- См. Важные замечания об evil-maid и вмешательстве.
- Посмотрите Как заметить, что кто-то обыскивал ваши вещи.
- Рассмотрите использование Haven guardianproject.github.io Archive.org на старом телефоне Android, чтобы следить за домом/комнатой, пока вас нет.
- Помните Предупреждение о смартфонах и умных устройствах. Не забывайте, что умные устройства могут скомпрометировать вашу анонимность.
- Никогда не путешествуйте с такими устройствами, если вам нужно проходить строгий пограничный контроль и там они могут быть незаконны или вызвать подозрения.
- Не подключайте к этому ноутбуку никакое оборудование, если вы ему не доверяете. Для зарядки используйте USB-блокиратор данных.
- Помните первое правило Fight Club и не говорите ни с кем о ваших чувствительных действиях под вашей реальной личностью.
- Ведите нормальную жизнь и не выглядите странно. Если всё ваше время в сети проходит через Tor, а аккаунтов в социальных сетях у вас нет вообще, вы уже выглядите подозрительно и привлекаете ненужное внимание.
- Держите правдоподобное отрицание как вариант, но помните, что против гаечного ключа за 5 долларов оно тоже не поможет.
- Никогда, вообще никогда не оставляйте ноутбук без присмотра/включённым/разблокированным где-либо, когда занимаетесь чувствительными действиями. Помните историю Росса Ульбрихта и его ареста: en.wikipedia.org Wikiless Archive.org.
- Регулярно проверяйте признаки вмешательства (не только устройства, но и дом/комнату).
- Если можете, не разговаривайте с полицией/властями (по крайней мере если вы в США) youtube.com Invidious без юриста. Храните молчание.
- Знайте и всегда держите под рукой данные юриста, который сможет помочь вам как крайняя мера, если всё пойдёт плохо.
- Поддерживайте высокую ситуационную осведомлённость, но не настолько высокую, чтобы выглядеть подозрительно.

- Рассмотрите использование физического ключа безопасности (например, YubiCo YubiKey) для разной защиты от компрометации аккаунтов. **(Это не рассматривается в этой версии руководства, но находится в работе для будущих версий.)**
- Прочитайте советы здесь: whonix.org Archive.org
- **Используйте здравый смысл, не будьте глупы, смотрите на ошибки других и учитесь; посмотрите/прочитайте это:**
  - Medium.com, Darkweb Vendors and the Basic Opsec Mistakes They Keep Making medium.com Scribe.rip Archive.org
  - 2020, Sinwindie, OSINT, and Dark Web Markets, Why OPSEC Still Matters youtube.com Invidious
  - 2020, RSA Conference 2020, When Cybercriminals with Good OpSec Attack youtube.com Invidious
  - 2015, DEF CON 22, Adrian Crenshaw, Dropping Docs on Darknets: How People Got Caught youtube.com Invidious (Slides Archive.org)
  - 2017, Ochko123 - How the Feds Caught Russian Mega-Carder Roman Seleznev youtube.com Invidious
  - 2017, DEF CON 25 - Svea Eckert, Andreas Dewes - Dark Data Invidious
  - 2015, DEF CON 22, Zoz, Don't Fuck It Up! youtube.com Invidious
  - 2020, Bad Opsec, How Tor Users Got Caught, youtube.com Invidious
  - 2022, Master of OpSec Masters: A View Through the Prism of Time, officercia.mirror.xyz Archive.org
  - 2022, How can you become a one-man-army OSINT specialist? officercia.mirror.xyz Archive.org

Рекомендуется изучить распространённые способы, которыми люди портят OPSEC: dan-kir.github.io Archive.org. Что бы вы ни делали, относитесь к OPSEC серьёзно и Don't Fuck It Up!

ФИНАЛЬНОЕ ПРЕДУПРЕЖДЕНИЕ ОБ OPSEC: ДЕРЖИТЕ ВАШИ АНОНИМНЫЕ ЛИЧНОСТИ ПОЛНОСТЬЮ ИЗОЛИРОВАННЫМИ ОТ ОБЫЧНОЙ СРЕДЫ И РЕАЛЬНОЙ ЛИЧНОСТИ. НЕ ПЕРЕДАВАЙТЕ НИЧЕГО МЕЖДУ АНОНИМНЫМИ СРЕДАМИ И СРЕДОЙ РЕАЛЬНОЙ ЛИЧНОСТИ. ДЕРЖИТЕ ИХ ПОЛНОСТЬЮ РАЗДЕЛЁННЫМИ НА ВСЕХ УРОВНЯХ. БОЛЬШИНСТВО ПРОВАЛОВ OPSEC ПРОИСХОДИТ ИЗ-ЗА СЛУЧАЙНОЙ УТЕЧКИ ИНФОРМАЦИИ ЧЕЛОВЕКОМ, А НЕ ИЗ-ЗА ТЕХНИЧЕСКИХ СБОЕВ.

[1] [назад] Wikipedia, OPSEC en.wikipedia.org Wikiless Archive.org

Что делать, если вы обнаружили вмешательство или обыск

- В случае ноутбука, вероятно, туда установили клавиатурный перехватчик и, возможно, сетевые и GPS-возможности. Мы рекомендуем открыть ноутбук, вынуть накопитель (он должен быть полностью зашифрован), уйти в безопасное место и бросить ноутбук. Не пытайтесь снять "жучок", потому что это может подвергнуть вас физической опасности.
- Если вы обнаружили обыск комнаты, дома и так далее, мы снова рекомендуем уйти в безопасное место, оставив всё в комнате, что тоже может быть с "жучком".
- Сделайте всё возможное, чтобы противник не заподозрил и не узнал, что вы обнаружили обыск и/или вмешательство. Будьте изобретательны. Например, позвоните другу просто сказать, что собираетесь в супермаркет купить еды.

Если вы думаете, что вас раскрыли

Если у вас есть немного времени

• Не паникуйте.

• Удалите из интернета всё, что можете, связанное с этой конкретной личностью (аккаунты, комментарии и так далее).

• Удалите всё офлайн, что связано с этой личностью, включая резервные копии.

• (Если используется физическая SIM-карта) Уничтожьте SIM-карту и выбросьте её в случайную мусорную урну где-нибудь.

• (Если используется физический одноразовый телефон) Сотрите одноразовый телефон, затем уничтожьте его и выбросьте в случайную мусорную урну где-нибудь.

• Безопасно сотрите жёсткий диск ноутбука, а затем в идеале физически уничтожьте HDD/SSD/ноутбук и выбросьте где-нибудь.

• Сделайте то же самое с резервными копиями.

• Держите данные вашего юриста рядом или, если нужно, заранее позвоните ему, чтобы подготовить дело.

• Вернитесь к обычным занятиям и надейтесь на лучшее.

Если у вас нет времени

• Не паникуйте.

• Постарайтесь как можно быстрее выключить ноутбук или перевести его в спящий режим и надейтесь на лучшее. Если вы достаточно быстры, память должна потерять содержимое или очиститься, а ваши данные на данный момент должны быть в основном в безопасности.

• По возможности свяжитесь с юристом и надейтесь на лучшее. Если пока связаться с ним нельзя, **постарайтесь хранить молчание (если ваша страна это позволяет), пока у вас не будет юриста, который поможет вам, и если закон разрешает вам хранить молчание.**

Имейте в виду, что во многих странах есть специальные законы, которые могут заставить вас раскрыть пароли и перекрыть ваше "право хранить молчание". См. эту статью Wikipedia: en.wikipedia.org Wikiless Archive.org и другой визуальный ресурс со ссылками на законы: gp-digital.org Archive.org. В Австралии, в частности, действуют широкие законы о приватности[1], а также был принят Surveillance Legislation Amendment (Identify and Disrupt) Act 2021[2], который даёт властям полномочия изменять, добавлять, копировать и удалять данные на устройствах и в аккаунтах подозреваемого.

Небольшая заключительная редакторская заметка

После прочтения всего руководства мы надеемся, что вы получили дополнительные полезные представления о приватности и анонимности. Теперь ясно, по моему скромному мнению, что в мире, где мы живём, осталось лишь несколько безопасных гаваней, где можно разумно ожидать приватности, и ещё меньше — анонимности. Многие часто говорят, что роман "1984" Джорджа Оруэлла не должен был быть инструкцией. И всё же сегодня это руководство и множество его ссылок, надеемся, покажут вам, насколько глубоко мы уже в этой норе.

Вы также должны знать, что большую часть цифровой информации, подробно описанной в этом руководстве, мотивированный противник может подделать или изменить для любой цели. Даже если вам удастся сохранить секреты от посторонних глаз, кто угодно может сфабриковать что угодно под свою историю:

- Журналы IP, DNS, геоданных и подключений можно подделать или изменить простым текстовым редактором без следов.
- Файлы и их свойства можно создать, изменить и снабдить временными метками простыми утилитами без следов.
- Данные EXIF изображений и видео можно изменить простыми утилитами без следов.
- Цифровые доказательства (изображения, видео, голосовые записи, электронные письма, документы и так далее) можно легко создать, разместить, удалить или уничтожить без следов.

Не стесняйтесь подвергать сомнению такую информацию из любого источника в эту эпоху дезинформации.

"Ложь успевает пройти полмира, пока правда надевает ботинки"[3]

Пожалуйста, продолжайте думать самостоятельно, используйте критическое мышление и сохраняйте открытый ум. "Sapere Aude" (осмелься знать!).

"В конце концов Партия объявит, что дважды два — пять, и вам придётся в это поверить" — Джордж Оруэлл, "1984", часть первая, глава седьмая.

Рассмотрите возможность помочь другим (см. Помощь другим оставаться анонимными)

Сноски

[1] [назад] Wikipedia, Privacy in Australian Law en.wikipedia.org Wikiless Archive.org
[2] [назад] Parliament of Autralia, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021, aph.gov.au Archive.org
[3] [назад] Quote Investigator, A Lie Can Travel Halfway Around the World While the Truth Is Putting On Its Shoes quoteinvestigator.com Archive.org

Пожертвования

У этого проекта нет финансирования или спонсоров, и пожертвования более чем приветствуются.

См.: Contribute в верхней части сайта.

(Пожалуйста, проверьте контрольную сумму и GPG-подпись этого файла для подтверждения подлинности; если вы не знаете, как это сделать, это объясняется в README репозитория).

Помощь другим оставаться анонимными

Если вы хотите помочь пользователям, сталкивающимся с цензурой и угнетением, рассмотрите помощь им через помощь сети Tor. Это можно сделать несколькими способами:

- Самый простой:
  - Использовать дополнение Snowflake в браузере (snowflake.torproject.org Archive.org)
- Немного больше работы:
  - Запустить ретрансляционный узел Tor (community.torproject.org Archive.org)
    - См. Рекомендуемые VPS-провайдеры
    - Дополнительное руководство: torrelay.ca Archive.org

Если хотите задачу чуть сложнее, можно также анонимно запустить выходной узел Tor, используя рекомендованных выше VPS-провайдеров.

Для этого см. blog.torproject.org Archive.org

Этот проект, например, запускает несколько выходных узлов Tor на пожертвования. Их можно увидеть здесь: metrics.torproject.org

Благодарности

- **Особая благодарность Эдварду Сноудену, который вдохновил нас написать это руководство (пожалуйста, купите и прочитайте его книгу en.wikipedia.org Wikiless Archive.org)**
- **Огромная благодарность людям, которые анонимно пожертвовали этому проекту**
- **Особая благодарность LiJu09 за помощь со светлой темой сайта (github.com)**
- **Особая благодарность людям из Simplelogin.io за предоставление бесплатного пожизненного премиум-доступа к их сервису**
- Спасибо GitHub за хостинг этого проекта и множеству людей, которые поставили ему звезду
- Спасибо Njal.la за анонимное предоставление доменного имени и VPS-хостинга
- Спасибо 1984.is за анонимное предоставление VPS-хостинга
- Спасибо всем людям, которые внесли вклад и поделились этим руководством с другими
- Спасибо людям из проектов Internet Archive и Archive.today
- Спасибо людям из проекта Monero
- Спасибо людям из проекта Zcash
- Спасибо людям из проекта Wikipedia
- Спасибо людям из проекта Tails
- Спасибо людям из проекта HiddenVM
- Спасибо людям из проекта Whonix
- Спасибо людям из проекта Qubes OS
- Спасибо людям из проекта Veracrypt
- Спасибо людям из проектов Tor и OONI
- Спасибо людям из проекта Briar
- Спасибо людям из проекта OnionShare
- Спасибо людям из проекта Element/Matrix
- Спасибо людям из проекта Jami
- Спасибо людям из проектов KeePass и KeePassXC
- Спасибо людям из проекта Fawkes
- Спасибо людям из проекта VirtualBox
- Спасибо людям из проектов ExifCleaner, Mat2 и ExifTool
- Спасибо людям из проекта Go Incognito от Techlore
- Спасибо Didier Stevens за его pdf-tools
- Спасибо людям из EFF
- Спасибо людям из SANS
- Спасибо людям из проекта OWASP

- Спасибо людям из проекта Privacyguides.org
- Спасибо людям из BlackHat, DEF CON и CCC
- Спасибо людям из Bellingcat и другим исследователям OSINT/криминалистики **(и простите, что этим руководством мы усложняем им жизнь)**
- Спасибо создателям документального фильма Social Dilemma **(посмотрите его, если ещё не смотрели)**
- Спасибо Michael Bazzell и его отличным книгам по OSINT, которые мы рекомендуем **купить** на inteltechniques.com
- Спасибо Randall Munroe из XKCD за его отличные и глубокие веб-комиксы.
- Спасибо людям из тех немногих коммерческих организаций, которые действительно серьёзно относятся к приватности
- Спасибо всему сообществу открытого исходного кода и особенно сообществу Linux
- Спасибо многим исследователям, журналистам, юристам и отдельным людям, упомянутым в этом руководстве, за их различные исследования и проекты
- Спасибо следующим людям за их вклад и помощь:
  - NobodySpecial, git.envs.net
  - Mahanihaka

Установка Windows

Это процесс установки Windows 10/11, который должен быть применим к любой установке Windows 10/11 в рамках этого руководства.

Windows 10 (Windows 11 см. ниже)

Установка

НЕ ПОДКЛЮЧАЙТЕ WINDOWS НИ К КАКОЙ СЕТИ ВО ВРЕМЯ УСТАНОВКИ (это позволит создать локальный аккаунт, а не использовать аккаунт Microsoft, и также предотвратит отправку телеметрии во время установки).

- (Только для установки ВМ VirtualBox) Перейдите в меню VirtualBox Machine Settings. Выберите network. Отключите кабель.
- Нажмите "Install Now"
- Выберите "I don't have a product key"
- Выберите нужную редакцию:
    - Основная ОС: используйте
        - Если вы собираетесь использовать правдоподобное отрицание: Windows Home
        - Если вы не собираетесь использовать правдоподобное отрицание: Windows Pro
    - ОС ВМ: используйте Windows Pro или Windows Pro N
- Выберите Custom
- Хранилище:
    - Если это простая установка ОС (основная ОС с простым шифрованием) или ВМ без шифрования, **выберите весь диск** и продолжайте установку (пропустите следующий шаг).
    - Если это часть настройки шифрования с правдоподобным отрицанием на основной ОС:
        - Если вы устанавливаете Windows в первый раз (скрытая ОС):
            - Удалите текущие разделы
            - Создайте первый раздел минимум на 50 ГБ дискового пространства (примерно треть общего дискового пространства).
            - Создайте второй раздел из оставшихся двух третей общего дискового пространства.
        - Если вы устанавливаете Windows во второй раз (отвлекающая ОС):
            - Не удаляйте текущие разделы
            - Установите Windows на первый раздел, который вы создали при первой установке.

    - Продолжайте установку в первый раздел
- Запустите процесс установки
- Выберите регион "United States"
- Пропустите дополнительную раскладку клавиатуры
- Выберите "I don't have internet"
- Выберите "Continue with limited setup"
- Создайте имя пользователя на свой выбор.
- Используйте пароль на свой выбор.
- Выберите все три контрольных вопроса и ответьте как угодно (не реальными данными).
- Не используйте Online Speech Recognition
- Не разрешайте приложению использовать ваше местоположение
- Не включайте "find my device"
- Отправляйте только "required diagnostic data"
- Не улучшайте Inking and Typing
- Не включайте улучшенный tailored experience.
- Не разрешайте приложениям использовать Advertising ID
- Выберите "Now" в запросе Cortana

Настройки приватности

- Когда установка закончится, перейдите в Settings > через значок меню вверху слева выберите Privacy and Security
    - Когда установка закончится, перейдите в Settings > Privacy и сделайте следующее:
    - General: всё Off
    - Speech: Off
    - Inking and Typing: Off
    - Diagnostic: Required level выключен, параметры OFF, **Delete your data**, частота Never
    - Activity History: всё Off и очистить историю
    - Location: всё Off (кнопка change) и очистить
    - Camera: отключить (кнопка change)
    - Microphone: отключить (кнопка change)
    - Voice Activation: всё Off
    - Notification: отключить (кнопка change)
    - Account info: отключить (кнопка change)
    - Contact info: отключить (кнопка change)

- Calendar access: отключить (кнопка change)
- Phone calls: отключить (кнопка change)
- Call History: отключить (кнопка change)
- E-mail: отключить (кнопка change)
- Tasks: отключить (кнопка change)
- Messaging: отключить (кнопка change)
- Radios: отключить (кнопка change)
- Other devices: установить Off
- Background Apps: отключить (кнопка change)
- App Diagnostics: отключить (кнопка change)
- Automatic file download disabled
- Documents: отключить (кнопка change)
- Pictures: отключить (кнопка change)
- Videos: отключить (кнопка change) и установить Off
- File system: отключить (кнопка change)
- Отключите индексирование файлов через "Indexing Options" (перейдите в Windows 11 Control Panel, переключите вид на "Large Icons" и выберите Indexing Options).
- Измените список и удалите все расположения.
- Перейдите в Advanced и нажмите Rebuild.
- (Только основная ОС) Отключите Bluetooth в настройках:
- Перейдите в Settings
- Перейдите в Devices
- Выберите Bluetooth и отключите его

• (Только основная ОС) Всё равно заклейте веб-камеру и микрофон, ради дополнительной паранойи.

• (Только основная ОС) Перейдите в Settings > Network & Internet > Wi-Fi и включите Random Hardware Address.

Windows 11

Установка

НЕ ПОДКЛЮЧАЙТЕ WINDOWS НИ К КАКОЙ СЕТИ ВО ВРЕМЯ УСТАНОВКИ (это позволит создать локальный аккаунт, а не использовать аккаунт Microsoft, и также предотвратит отправку телеметрии во время установки).

- (Только для установки ВМ VirtualBox) Перейдите в меню VirtualBox Machine Settings. Выберите network. Отключите кабель. Для этой задачи также можно следовать отличному руководству Oracle: blogs.oracle.com Archive.org
- Выберите язык, валюту и раскладку клавиатуры
- Нажмите "Install Now"
- (Только для установки ВМ VirtualBox) Нажмите Shift и F10 одновременно
- (Только для установки ВМ VirtualBox) Запустите "regedit" в командной строке
- (Только для установки ВМ VirtualBox) Когда откроется Registry Editor, перейдите к `HKEY_LOCAL_MACHINE\SYSTEM\Setup`, щёлкните правой кнопкой по ключу "Setup" и выберите "New => Key". Когда будет предложено назвать ключ, введите "LabConfig" и нажмите Enter.
- (Только для установки ВМ VirtualBox) Теперь щёлкните правой кнопкой по ключу "LabConfig", выберите значение "New => DWORD (32-bit)" и создайте значение с именем "BypassTPMCheck", затем установите его данные в "1". Теми же шагами создайте "BypassRAMCheck" и "BypassSecureBootCheck"
- Выберите "I don't have a product key"
- Примите соглашение
- Выберите нужную редакцию:
  - Основная ОС: используйте
    - Если вы собираетесь использовать правдоподобное отрицание: Windows Home
    - Если вы не собираетесь использовать правдоподобное отрицание: Windows Pro
  - ОС ВМ: используйте Windows Pro или Windows Pro N
- Выберите Custom Install
- Хранилище:
  - Если это простая установка ОС (основная ОС с простым шифрованием) или ВМ без шифрования, **выберите весь диск** и продолжайте установку (пропустите следующий шаг).
  - Если это часть настройки шифрования с правдоподобным отрицанием на основной ОС:
    - Если вы устанавливаете Windows в первый раз (скрытая ОС):
      - Удалите текущие разделы
      - Создайте первый раздел минимум на 50 ГБ дискового пространства (примерно треть общего дискового пространства).
      - Создайте второй раздел из оставшихся двух третей общего дискового пространства.
    - Если вы устанавливаете Windows во второй раз (отвлекающая ОС):
      - Не удаляйте текущие разделы
      - Установите Windows на первый раздел, который вы создали при первой установке.

    • Продолжайте установку в первый раздел
• Запустите процесс установки
• Выберите регион "United States"
• Выберите раскладку клавиатуры и пропустите вторую раскладку
• Выберите "I don't have internet"
• Выберите "Continue with limited setup"
• Создайте имя пользователя на свой выбор.
• Используйте пароль на свой выбор.
• Выберите все три контрольных вопроса и ответьте как угодно (не реальными данными).
• Отключите Location
• Отключите find my device
• Отключите optional diagnostic data
• Отправляйте только "required diagnostic data"
• Не улучшайте Inking and Typing
• Отключите tailored experience.
• Отключите Advertising ID
• Нажмите Accept

Настройки приватности

• Когда установка закончится, перейдите в Settings > Privacy и сделайте следующее:
    • General: всё Off
    • Speech: Off
    • Inking and Typing: Off
    • Diagnostic: Required level выключен, параметры OFF, **Delete your data**, частота Never
    • Activity History: всё Off и очистить историю
    • Location: всё Off (кнопка change) и очистить
    • Camera: отключить (кнопка change)
    • Microphone: отключить (кнопка change)
    • Voice Activation: всё Off
    • Notification: отключить (кнопка change)
    • Account info: отключить (кнопка change)
    • Contact info: отключить (кнопка change)
    • Calendar access: отключить (кнопка change)
    • Phone calls: отключить (кнопка change)

  - Call History: отключить (кнопка change)
  - E-mail: отключить (кнопка change)
  - Tasks: отключить (кнопка change)
  - Messaging: отключить (кнопка change)
  - Radios: отключить (кнопка change)
  - Other devices: установить Off
  - Background Apps: отключить (кнопка change)
  - App Diagnostics: отключить (кнопка change)
  - Automatic file download disabled
  - Documents: отключить (кнопка change)
  - Music Library: отключить (кнопка change)
  - Pictures: отключить (кнопка change)
  - Videos: отключить (кнопка change) и установить Off
  - File system: отключить (кнопка change)
  - Отключите индексирование файлов через "Indexing Options" (перейдите в Windows 11 Control Panel, переключите вид на "Large Icons" и выберите Indexing Options).
  - Измените список и удалите все расположения.
  - Перейдите в Advanced и нажмите Rebuild.
  - (Только основная ОС) Отключите Bluetooth в настройках:
  - Перейдите в Settings
  - Перейдите в Devices
  - Выберите Bluetooth и отключите его
- (Только основная ОС) Всё равно заклейте веб-камеру и микрофон, ради дополнительной паранойи.
- (Только основная ОС) Перейдите в Settings > Network & Internet > Wi-Fi и включите Random Hardware Address.

Дополнительные настройки приватности Windows

Как уже было написано ранее в этом руководстве и как отмечает PrivacyGuides.org (privacyguides.org Archive.org), Windows 10/11 — кошмар для приватности. Отключить всё во время и после установки через доступные вам настройки недостаточно. Объём телеметрии, которую собирает Microsoft, ошеломляет и может разрушить ваши попытки сохранить секреты. Вам нужно скачать и использовать несколько утилит, чтобы (надеемся) заставить Windows 10/11 не отправлять данные обратно Microsoft.

Подробные шаги:

- **НИКОГДА НЕ ИСПОЛЬЗУЙТЕ АККАУНТ MICROSOFT ДЛЯ ВХОДА: если вы его используете, следует переустановить эту Windows-машину без подключения к сети и вместо этого использовать локальный аккаунт.**
- Выполняйте эти шаги с другого компьютера. Не подключайте Windows 10/11 к интернету до применения этих настроек. Можно скачать утилиты и скопировать их на USB-накопитель (для переноса на свежую установку Windows 10/11), а если это ВМ, можно перенести их в ВМ через VirtualBox (VM Settings > General > Advanced > Drag n Drop > Enable Host to Guest).
- (Для более опытных пользователей) Скачайте и установите W10Privacy с w10privacy.de Archive.org
  - Откройте приложение как администратор (правый щелчок > more > run as administrator)
  - Отметьте все рекомендуемые (зелёные) настройки и сохраните.
  - Необязательно, но рекомендуется (может что-то сломать, используйте на свой риск): также отметьте оранжевые/красные настройки и сохраните.
  - Перезагрузитесь
- Скачайте и запустите WindowsSpyBlocker с crazymax.dev Archive.org
  - Введите 1 и перейдите в Telemetry
  - Введите 1 и перейдите в Firewall
  - Введите 2 и добавьте Spy Rules
  - Перезагрузитесь
- Также рассмотрите ShutUp10++ с oo-software.com Archive.org
  - Включите как минимум все рекомендуемые настройки
- Наконец, опять же для пользователей со средними навыками, рассмотрите установку Safing Portmaster с safing.io Archive.org **(Предупреждение: с некоторыми VPN-клиентами могут быть проблемы. См.: docs.safing.io** Archive.org
- Вернитесь в настройки в последний раз, чтобы удалить Diagnostic и Delete all Data.

Эти меры вместе с настройками во время установки, будем надеяться, должны быть достаточны, чтобы Microsoft не шпионила за вашей ОС.

Вам придётся часто обновлять и повторно запускать эти утилиты, а также делать это после любого крупного обновления Windows, потому что такие обновления обычно тихо включают телеметрию обратно.

В качестве бонуса может быть интересно немного усилить защиту основной ОС Windows. См. github.com Archive.org (это руководство по безопасности, а не по приватности. Если вы используете это руководство, не включайте Hyper-V, потому что он плохо работает с VirtualBox, и не включайте функции, которые ранее были специально отключены по причинам приватности, например SmartScreen, облачную защиту и так далее.)

Создание установочного носителя Windows

Windows 10

Это шаги для создания установочного носителя Windows 10 (21H1) с помощью этого инструмента и инструкций:

microsoft.com Archive.org

• Скачайте инструмент и запустите его из папки Download.

• Согласитесь с условиями

• Выберите процесс Create an installation Media.

• Выберите редакцию Windows 10 64 Bits с нужным вам языком.

• Выберите нужный процесс:

  • Если устанавливаете на физический компьютер: выберите USB Flash Drive.

  • Если устанавливаете на виртуальную машину: выберите ISO file и сохраните его.

• Продолжайте

Windows 11

• Перейдите на microsoft.com и скачайте ISO.

Безопасное стирание SSD с помощью System Rescue

Эти инструкции действительны для всех операционных систем:

- System Rescue:
  - Создайте USB-диск System Rescue по этим инструкциям: system-rescue.org Archive.org (скачайте ISO и запишите на USB-накопитель с помощью Rufus).
  - Отключите Secure Boot в настройках BIOS/UEFI и измените порядок загрузки на USB-диск (загрузчик System Rescue не подписан и не загрузится с включённым Secure Boot).
  - Следуйте инструкциям для смены раскладки клавиатуры, набрав "stkmap".
  - (Необязательно) После этого запустите `startx`, чтобы открыть графическую среду.
- SATA SSD:
  - (Если вы запускали `startx`) Откройте терминал
  - ATA Secure Erase:
    - Следуйте одному из этих руководств
      - wiki.archlinux.org Archive.org
      - ata.wiki.kernel.org Archive.org
      - tinyapps.org Archive.org
  - ATA Sanitize:
    - Следуйте этому руководству: tinyapps.org Archive.org
- NVMe SSD:
  - (Если вы запускали `startx`) Откройте терминал
  - Следуйте одному из этих руководств:
    - wiki.archlinux.org Archive.org
    - tinyapps.org Archive.org
    - tinyapps.org Archive.org

Clonezilla

- Получите Clonezilla, следуя этим инструкциям: clonezilla.org Archive.org (я рекомендую Alternative version AMD64, которая должна работать с большинством современных ноутбуков)
- Загрузитесь с Clonezilla
- Следуйте этим шагам для создания резервной копии: clonezilla.org Archive.org
  - **Если вы создаёте резервную копию диска с простым шифрованием, шифрование резервной копии не требуется, потому что вы копируете уже зашифрованный диск; но при желании вы всё равно можете зашифровать резервную копию для дополнительной безопасности (и более медленного резервного копирования).**
  - **Если вы собираетесь делать резервную копию устройства с шифрованием и правдоподобным отрицанием, мы настоятельно не рекомендуем это делать, потому что такой образ резервной копии может использоваться для доказательства существования скрытого тома криминалистическими методами, как объяснялось ранее. Не создавайте образ раздела, содержащего скрытую ОС.**
- Готово. Если нужно восстановить, следуйте этим инструкциям: clonezilla.org Archive.org

Каждая резервная копия может занять некоторое время в зависимости от скорости ноутбука и скорости внешнего диска. По моему опыту, ожидайте около 1 часа на резервную копию в зависимости от размера диска и скорости записи носителя резервной копии (мои тесты выполнялись при резервном копировании SSD на 256 ГБ на USB 3.0 HDD 7200 rpm).

Diskpart

Diskpart — это утилита Windows, которую можно использовать для разных операций с жёстким диском. В данном случае вы будете использовать Diskpart, чтобы показать идентификатор диска, а также изменить его при необходимости.

Это может понадобиться, если вы восстанавливаете резервную копию на новый HDD/SSD с идентификатором, отличающимся от сохранённого в резервной копии, и Windows из-за этого отказывается загружаться.

Diskpart можно запустить из любой среды Windows через командную строку. Сюда входят диски восстановления, созданные утилитами вроде Macrium Reflect, любой установочный носитель Windows, аварийные диски EaseUS Todo Free.

- **Показ идентификатора диска**
  - Запустите Diskpart, чтобы войти в утилиту Diskpart
  - Выполните команду `list disk`, чтобы вывести список дисков
  - Выполните `sel disk x` (замените x на ваш системный диск), чтобы выбрать системный диск
  - Выполните `detail disk`, чтобы показать сведения об этом диске
  - Запишите идентификатор диска (это нужно сделать ДО резервного копирования дисков).
- **Изменение идентификатора диска**
  - Этот шаг следует выполнять только если после восстановления полной резервной копии диска на новый жёсткий диск Windows отказывается загружаться
  - Выполните те же команды, что выше, на новом целевом диске
  - Дополнительно выполните команду `uniqueid disk id=02345678` (где id нужно заменить на идентификатор, который вы записали ранее)

Безопасный браузер в основной ОС

Если вы можете использовать Tor

Это руководство будет **рекомендовать только** Tor Browser в основной ОС, потому что он по умолчанию даёт лучшую защиту. Единственный другой приемлемый вариант, по моему мнению, — использовать Brave Browser с вкладкой Tor, **но помните, что сами Brave рекомендуют использовать Tor Browser, если ваша безопасность зависит от анонимностиArchive.org: "If your personal safety depends on remaining anonymous, we highly recommend using Tor Browser instead of Brave Tor windows."**

Этот браузер в основной ОС будет использоваться только для скачивания разных утилит и никогда — для настоящих чувствительных действий.

См. Установка и использование настольного Tor Browser.

Если у вас проблемы с подключением к Tor из-за цензуры или блокировки, можно рассмотреть мосты Tor, как объясняется здесь: bridges.torproject.org Archive.org

Используйте этот браузер для всех следующих шагов внутри основной ОС, если не указано иное.

Если вы не можете использовать Tor

Потому что это слишком опасно/рискованно/подозрительно. В качестве крайней меры мы бы пока рекомендовали Firefox или Brave только в приватных окнах.

Перед продолжением см. Что делать, когда Tor и VPN невозможны?.

Каждый раз делайте это только из другой безопасной публичной Wi-Fi-сети (см. Найти безопасные места с приличным публичным Wi-Fi) и используя дальнобойное соединение (см. Использование дальнобойной антенны для подключения к публичным Wi-Fi с безопасного расстояния).

Очищайте все данные браузера после каждого использования.

Используйте этот метод для всех следующих шагов внутри основной ОС, если не указано иное.

Инструменты очистки Windows

В этом руководстве мы рекомендуем два родных инструмента и два сторонних инструмента:

• Родные инструменты:

  • Windows 10/11 Disk Cleanup Utility: support.microsoft.com Archive.org

    Этот инструмент штатно очищает множество вещей. Этого недостаточно, и вместо него мы рекомендуем использовать сторонние инструменты ниже, чтобы очистить больше. Например, PrivaZer будет напрямую использовать саму утилиту очистки диска, а BleachBit будет использовать собственные механизмы.

• Windows 10/11 Optimize Utility (Defrag on HDD Drives): support.microsoft.com Archive.org (да, руководство для Windows 10, но должно работать и в 11)

    Для безопасности этот инструмент особенно полезен на SSD, потому что функция "Optimize" фактически принудительно запускает Trim для всего диска. Этого, скорее всего, будет более чем достаточно, чтобы любые удалённые данные, которые по какой-либо причине раньше не были обработаны Trim, были обработаны теперь. Данные, удалённые с Trim, восстановить крайне маловероятно, как уже объяснялось в этом руководстве.

• Сторонние инструменты:

  • Утилита BleachBit с открытым исходным кодом bleachbit.org Archive.org

  • Утилита PrivaZer с закрытым исходным кодом privazer.com Archive.org

Я предпочитаю PrivaZer, потому что у него больше настроек и более умные функции, но мы поймём, если вы не доверяете им и предпочитаете программное обеспечение с открытым исходным кодом; в таком случае мы рекомендуем BleachBit, у которого чуть меньше настроек, но похожая функциональность.

Оба инструмента можно использовать для очистки многих вещей, например:

• Журнал Windows USN, который хранит много информации.

• Windows System Resource Usage Monitor (SRUM)[1].

• Разные истории разных программ (например, списки недавнего).

• Разные журналы

• Свободное (нераспределённое) пространство жёсткого диска[2].

• Безопасное удаление файлов

• Безопасное стирание USB-накопителей

Обе эти утилиты могут удалять файлы и перезаписывать свободное пространство после удаления, чтобы улучшить безопасное удаление даже на SSD. Помните, что это может немного сократить срок службы SSD.

Сноски

[1] [назад] Medium.com, Digging into the System Resource Usage Monitor (SRUM) medium.com Scribe.rip Archive.org
[2] [назад] SANS, Timestamped Registry & NTFS Artifacts from Unallocated Space sans.org Archive.org

Безопасное стирание HDD с помощью ShredOS

Для этого рекомендуются несколько утилит (например, старый неподдерживаемый DBAN[1] или System Rescue CD (system-rescue.org Archive.org)), но мы рекомендуем использовать ShredOS.

Если хотите, можете вместо этого использовать DBAN (по этому руководству: lifewire.com Archive.org); процесс в целом такой же, но он не будет работать из коробки с ноутбуками UEFI.

Если хотите использовать System-Rescue, просто перейдите на их сайт и следуйте инструкциям.

Windows

- Скачайте ShredOS с github.com Archive.org
- Распакуйте ISO-файл
- Скачайте Rufus с rufus.ie Archive.org
- Запустите Rufus
- Выберите IMG-файл ShredOS
- Запишите его на USB-накопитель
- Когда закончите, перезагрузитесь и загрузитесь с USB-накопителя (возможно, для этого придётся зайти в настройки BIOS и изменить порядок загрузки).
- Следуйте инструкциям на экране

Linux

- Следуйте инструкциям на github.com Archive.org
- Перезагрузитесь и загрузитесь с USB-накопителя
- Следуйте инструкциям на экране

[1] [назад] DBAN, dban.org Archive.org

Инструменты производителей для стирания HDD и SSD

Всегда сначала проверяйте BIOS/UEFI ноутбука на наличие родных утилит.

Обязательно используйте правильный режим стирания для правильного диска. Wipe и Passes предназначены для HDD. Для SSD есть специальные параметры (например, ATA Secure Erase или Sanitize).

К сожалению, большинство этих инструментов работает только в Windows.

Инструменты, предоставляющие загрузочный диск для стирания при загрузке

- SanDisk DashBoard: kb.sandisk.com Archive.org
- Seagate SeaTools: seagate.com Archive.org
- Samsung Magican: samsung.com Archive.org
- Kingston SSD Manager: kingston.com Archive.org
- Lenovo:
  - Скорее всего, родная утилита доступна в BIOS/UEFI, пожалуйста, проверьте
  - Drive Erase Utility: support.lenovo.com Archive.org
- Crucial Storage Executive: crucial.com Archive.org
- Western Digital Dashboard: support.wdc.com Archive.org
- HP: следуйте инструкциям на store.hp.com Archive.org
- Transcend SSD Scope: transcend-info.com Archive.org
- Dell:
  - Скорее всего, родная утилита доступна в BIOS/UEFI, пожалуйста, проверьте dell.com Archive.org

Инструменты, поддерживающие только запуск из работающей ОС (для внешних дисков)

- Toshiba Storage Tools: toshiba-storage.com Archive.org

Соображения по внешним SSD

Я не рекомендую использовать внешние SSD из-за неопределённости с поддержкой Trim, ATA Secure Erase и параметров Sanitize через USB-контроллеры. Вместо этого мы рекомендуем использовать внешние HDD, которые можно безопасно и надёжно очищать/стирать без лишних сложностей (хотя и намного медленнее, чем SSD).

Пожалуйста, не покупайте и не используйте сомнительные самошифрующиеся устройства вроде этих: syscall.eu Archive.org

Некоторые могут быть очень эффективными[1], но многие — просто сомнительные гаджеты.

Если вы хотите использовать внешний SSD для чувствительного хранения:

- Учитывайте поддержку:
  - Операций Trim и ATA/NVMe secure erase со стороны USB-контроллера ноутбука.
  - Операций Trim и ATA/NVMe secure erase со стороны самого USB SSD.
- Всегда используйте полное шифрование диска на таких дисках
- **По возможности используйте инструменты производителя для их безопасного стирания (см. Соображения по использованию внешних SSD).**
- Рассмотрите ручное стирание данных после использования через полное расшифрование/шифрование или полное заполнение случайными данными.

Так как проверить, поддерживает ли ваш внешний USB SSD Trim и другие операции ATA/NVMe из основной ОС?

Windows

Поддержка Trim

Возможно, Windows правильно обнаружит ваш внешний SSD и включит Trim по умолчанию. Проверьте, работает ли Optimize через родную дисковую утилиту Windows, как объяснялось в разделе Windows для внутреннего SSD.

Операции ATA/NVMe (Secure Erase/Sanitize)

Используйте инструменты производителя, чтобы проверять и выполнять эти операции ... Это практически единственный способ убедиться, что они не только поддерживаются, но и действительно работают. Некоторые утилиты, например CrystalDiskInfo Archive.org, могут сказать, поддерживается ли это, но не проверят, работает ли оно на деле. См. Инструменты производителей для стирания HDD и SSD.

Если это не работает, просто расшифруйте и заново зашифруйте весь накопитель или заполните свободное пространство, как указано в руководстве. Насколько мне известно, другого способа нет. Разве что загрузить System Rescue Linux CD и посмотреть следующий раздел.

Linux

Поддержка Trim

Следуйте этому хорошему руководству: glump.net Archive.org

Операции ATA/NVMe (Secure Erase/Sanitize)

Это не "рекомендуется". Пожалуйста, прочитайте предупреждения здесь ata.wiki.kernel.orgArchive.orgи здесь wiki.archlinux.org Archive.org

Но, похоже, это основано на отдельных практических случаях. Поэтому, если вы уверены, что ваш внешний SSD поддерживает Trim (см. документацию производителя), можно просто **попробовать на свой риск** использовать nvme-cli или hdparm для отправки команд secure erase.

См. также это руководство: code.mendhak.com Archive.org

Результаты могут отличаться. Используйте на свой риск.

macOS

Поддержка Trim

Согласно документации Apple[2], Trim поддерживается на APFS (асинхронно) и HFS+ (через периодический Trim или First Aid).

Поэтому, если он поддерживается (и включён на вашем внешнем SSD), вы должны иметь возможность выполнить Trim на диске не-APFS с помощью Disk Utility и First Aid, что должно отправить Trim.

Если диск поддерживает Trim, но он не включён в macOS, можно попробовать выполнить команду `sudo trimforce enable` из терминала и посмотреть, включит ли она Trim для внешнего SSD. Затем снова проверьте команду First Aid, если это не APFS (подробнее см. это руководство: lifewire.com Archive.org)

Если это не работает, нам не известен надёжный метод включения TRIM, кроме коммерческой утилиты Trim Enabler здесь: cindori.org Archive.org, которая заявляет поддержку внешних дисков.

Операции ATA/NVMe (Secure Erase/Sanitize)

Нам не известно ни одного способа сделать это надёжно и безопасно в macOS. Поэтому придётся попробовать один из вариантов:

• Использовать загрузочный USB System Rescue Linux, чтобы сделать это

• Просто расшифровать и заново зашифровать накопитель через Disk Utility или Veracrypt

• Заполнить свободное пространство диска методом Linux (`dd`)

Сноски

[1] [назад] NYTimes, Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes nytimes.com Archive.org
[2] [назад] Wikipedia, Koalang en.wikipedia.org Wikiless Archive.org

Удаление метаданных с помощью mat2-web

Скачайте последний Debian testing amd64 netinst ISO с debian.org Archive.org

(Берите testing, чтобы получить последний выпуск mat2; stable отстаёт на несколько версий.)

Это очень лёгкая установка, и мы рекомендуем делать её из виртуальной машины (ВМ внутри ВМ), чтобы пользоваться Whonix Tor Gateway. Хотя такую ВМ можно поставить напрямую за Whonix Gateway, по умолчанию Whonix не позволит ВМ в своей сети легко общаться друг с другом. Также можно оставить её в открытом интернете на время установки, а затем перевести в сеть Host-only, либо установить её из ВМ внутри ВМ и потом перенести на основную ОС для использования в режиме Host-only, как показано ниже:

1. Создайте новую машину с любым именем, например **Mat2**.
2. В поле Type выберите **Linux**.
3. В поле Version выберите **Debian (64-bit)**.
4. Оставьте параметры по умолчанию и нажмите **Create**.
5. Выберите ВМ и нажмите **Settings**.
6. Выберите **System** и отключите **Floppy disk** на вкладке Motherboard.
7. Откройте вкладку Processor и **включите PAE/NX**.
8. Выберите **Audio** и **отключите Audio**.
9. Выберите **USB** и **отключите USB controller**.
10. Выберите **Storage** и выберите CD-привод, чтобы подключить Debian Netinst ISO.
11. Выберите **Network** и **Attach to NAT**.
12. Запустите ВМ.
13. Выберите **Install** (не Graphical install).
14. Выберите **Language**, **Location** и **Keyboard layout** по своему усмотрению.
15. Подождите, пока сеть настроится (автоматический DHCP). Это занимает несколько секунд.
16. Задайте имя, например **Mat2**.
17. Оставьте поле **domain** пустым.
18. Задайте пароль **root** по своему усмотрению (желательно надёжный).
19. Создайте нового **user** и **password** по своему усмотрению (желательно надёжный).
20. Выберите нужный **Time Zone**.
21. Выберите **Guided - Use the entire disk**.
22. Выберите единственный доступный диск (в нашем случае **/dev/sda**).
23. Выберите **All files in one partition**.
24. Подтвердите запись изменений на диск.
25. Выберите **No**, чтобы не сканировать другой CD или DVD.
26. Выберите любой регион и любое зеркало по своему усмотрению, а поле **proxy** оставьте пустым.
27. Выберите **No**, чтобы не участвовать в опросе.
28. Выберите **только System Standard Utilities**. Снимите все остальные пункты клавишей **space**.
29. Выберите **Yes**, чтобы установить загрузчик GRUB.
30. Выберите **/dev/sda** и продолжите.
31. Завершите установку и перезагрузитесь.
32. Войдите под своим **user** или **root**. Обычно напрямую использовать root не следует, но в данном случае это допустимо.
33. Обновите установку командой `apt upgrade`. Она уже должна быть обновлена, поскольку это сетевая установка, но мы дополнительно проверяем.

34. Установите нужные пакеты для mat2 командой `apt install ffmpeg uwsgi python3-pip uwsgi-plugin-python3 lib35rsvg2-dev git mat2 apache2 libapache2-mod-proxy-uwsgi`.
35. Перейдите в каталог **/var/www** командой `cd /var/www/`.
36. **Клонируйте mat2-web** из репозитория mat2-web командой `git clone https://0xacab.org/jvoisin/mat2-web.git`.
37. **Создайте каталог для загрузок** командой `mkdir ./mat2-web/uploads/`.
38. **Дайте Apache2 права** на чтение файлов командой `chown -R www-data:www-data ./mat2-web`.
39. **Включите прокси uwsgi для apache2** командой `/usr/sbin/a2enmod proxy_uwsgi`.
40. **Обновите pip** командой `python3 -m pip install pip --upgrade`.
41. **Установите эти модули Python** командой `python3 -m pip install flasgger pyyaml flask-restful flask cerberus flask-cors jinja2`.
42. **Перейдите в каталог настроек** mat2 командой `cd /var/www/mat2-web/config/`.
43. **Скопируйте файл настроек apache2** в **/etc** командой `cp apache2.config /etc/apache2/sites-enabled/apache2.conf`.
44. **Удалите файл настроек по умолчанию** командой `rm /etc/apache2/sites-enabled/000-default.conf`.
45. **Отредактируйте файл настроек apache2**, предоставленный mat2-web, командой `nano /etc/apache2/sites-enabled/apache2.conf`.
46. **Удалите первую строку** `Listen 80`, нажав **Ctrl+K**, чтобы вырезать строку.
47. **Измените путь uwsgi** с `/var/www/mat2-web/mat2-web.sock` на `/run/uwsgi/uwsgi.sock`, затем нажмите **Ctrl+X** для выхода, затем **Y** и **Enter**.
48. **Скопируйте файл настроек uwsgi** в **/etc** командой `cp uwsgi.config /etc/uwsgi/apps-enabled/uwsgi.ini`.
49. **Отредактируйте файл настроек uwsgi** командой `nano /etc/uwsgi/apps-enabled/uwsgi.ini` и измените **uid** и **guid** на `nobody` и `nogroup` соответственно. Сохраните и выйдите через **Ctrl+X**, затем **Y**, затем **Enter**.
50. Выполните `chown -R 777 /var/www/mat2-web`, чтобы изменить владельца на **mat2-web**.
51. **Перезапустите uwsgi** командой `systemctl restart uwsgi`. Ошибок быть не должно.
52. **Перезапустите apache2** командой `systemctl restart apache2`. Ошибок быть не должно.
53. Теперь перейдите в **Settings** > **Network** > **Attached to** и **выберите Host-only Adapter**. Нажмите **OK**, чтобы сохранить.
54. Перезагрузите ВМ через **Machine** > **Reset**. Подтвердите перезагрузку.
55. Войдите в ВМ под **user** из **шага 19** и введите `ip a`. Запишите назначенный ей IP-адрес в разделе link/ether, тот, который имеет вид **192.168.*.***.
56. Из основной ОС, где запущена ВМ, **откройте браузер** и перейдите по IP-адресу вашей Debian ВМ. Он будет выглядеть примерно так: 192.168.1.55.
57. Теперь вы должны увидеть нормально работающий сайт Mat2-Web.
58. **Выключите гостевую ВМ Mat2** командой `shutdown -h now`, чтобы остановить машину.
59. **Создайте снимок ВМ** в VirtualBox, пока гостевая ВМ выключена.

Перезапустите ВМ Mat2, и всё готово: можно использовать Mat2-web для удаления метаданных из большинства файлов!

После использования выключите ВМ и откатитесь к снимку, чтобы удалить следы загруженных файлов. Этой ВМ не нужен доступ в интернет, если только вы не хотите её обновить; в таком случае нужно временно вернуть её в **сеть NAT** и выполнить следующие шаги.

Для обновления Debian **запустите ВМ** и выполните `apt update`, затем `apt upgrade`.

Для обновления mat2-web введите `cd /var/www/mat2-web` и выполните `git pull`.

После обновлений выключите ВМ, переключите её на **Host-only Adapter**, создайте новый снимок и удалите старый.

Готово.

Теперь можно просто запускать эту небольшую ВМ Mat2 по необходимости. Открывайте её из своей гостевой ВМ и используйте интерфейс, чтобы удалять метаданные из большинства файлов. После каждого использования этой ВМ следует откатываться к снимку, чтобы стереть все следы.

Никогда не открывайте эту ВМ ни для какой сети, кроме временного доступа ради обновлений. Этот веб-интерфейс не подходит для прямого внешнего доступа.

Варианты очистки диска через BIOS/UEFI по брендам

Вот несколько ссылок о том, как безопасно очистить диск (HDD/SSD) через BIOS у разных производителей:

• Lenovo ThinkPads: support.lenovo.com Archive.org

• HP (все модели): support.hp.com Archive.org

• Dell (все модели): dell.com Archive.org

• Acer (только Travelmate): us.answers.acer.com Archive.org

• Asus: насколько мне известно, такого варианта нет, кроме, возможно, некоторых моделей ROG.

• Gigabyte: насколько мне известно, такого варианта нет.

• Honor: насколько мне известно, такого варианта нет.

• Huawei: насколько мне известно, такого варианта нет.

Предупреждение о смартфонах и умных устройствах

При выполнении чувствительных действий помните:

- **Не берите с собой настоящий смартфон или умные устройства (даже выключенные).** В сотовых сетях возможны корреляционные атаки, позволяющие увидеть, какой телефон «выключился» перед тем, как одноразовый телефон «включился». С первого раза это может не сработать, но после нескольких повторений круг сузится, и вас могут раскрыть. Лучше оставить основной смартфон дома подключённым к сети (см. эту статью на русском: biboroda.livejournal.com Google Translate Archive.org**).**
- **Ещё раз: не берите их с собой без крайней необходимости. Если всё-таки нужно,** можно рассмотреть выключение и извлечение аккумулятора, а если это невозможно, хранение устройств в клетке Фарадея[1] или специальном экранирующем чехле. В продаже есть много таких чехлов, «блокирующих сигнал», и эффективность некоторых из них изучалась[2]. Если вы не можете позволить себе такой чехол, вероятно, можно добиться «приемлемого результата» одним или несколькими листами алюминиевой фольги (как показано в ранее упомянутом исследовании).
  - Предупреждение: учитывайте, что сами данные датчиков тоже могут надёжно использоваться для отслеживания[3][4].
  - Подумайте о том, чтобы оставить умные устройства дома подключёнными к сети и делать на них что-нибудь вместо того, чтобы брать их с собой выключенными, например смотреть YouTube/Netflix или что-то похожее. Это снизит усилия по отслеживанию, но также создаст цифровые следы, которые могут указывать, что вы были дома.
  - **Сюда может относиться и ваш автомобиль, если в нём, например, есть устройство сотовой связи (как минимум с IMEI) и функция вызова экстренных служб.**

Кроме того, если вы используете смартфон как одноразовый, знайте, что по умолчанию он отправляет много диагностических данных. Этого может быть достаточно, чтобы потенциально идентифицировать вас по шаблонам использования устройства (метод, известный как биометрическое профилирование). Следует использовать одноразовый телефон только при реальной необходимости, чтобы минимизировать объём сведений, которые могут собрать и применить для вашей идентификации.

Наконец, стоит также учитывать эту полезную памятку NSA о безопасности смартфонов: web.archive.org.

Примечание: пожалуйста, не рассматривайте коммерческие «всё-в-одном» устройства для анонимности. Единственный способ добиться правильной операционной безопасности - делать всё самостоятельно. Посмотрите эти примеры, чтобы понять, почему это неудачная идея:

- **AN0M: theguardian.com** Archive.org
- **Encrochat: en.wikipedia.org** Wikiless Archive.org
- **Sky ECC: en.wikipedia.org** Wikiless Archive.org

Никогда не полагайтесь на внешний коммерческий сервис как на первую линию вашей анонимности. Но дальше вы увидите, что платные сервисы всё ещё можно использовать из уже анонимной личности, если купить их анонимно и соблюдать хорошую операционную безопасность.

Сноски

[1] [назад] Wikipedia, Faraday Cage, en.wikipedia.org Wikiless Archive.org
[2] [назад] Edith Cowan University, A forensic examination of several mobile device Faraday bags & materials to test their effectiveness materials to test their effectiveness web.archive.org Archive.org
[3] [назад] arXiv, Deep-Spying: Spying using Smartwatch and Deep Learning arxiv.org Archive.org
[4] [назад] Acm.org, Privacy Implications of Accelerometer Data: A Review of Possible Inferences dl.acm.org Archive.org

Получение анонимного VPN или прокси

Если вы следуете нашим рекомендациям, вам также понадобится подписка на VPN, но на этот раз нужна анонимная подписка, которую нельзя связать с вами через финансовую систему. То есть VPN нужно оплатить наличными или достаточно приватной криптовалютой, например Monero. Позже вы сможете использовать этот VPN для анонимного подключения к разным сервисам, но **никогда напрямую со своего IP-адреса**. Этот VPN нельзя использовать в каком-либо другом, неанонимном контексте, иначе вы поставите под угрозу свою анонимность.

Есть два рабочих варианта:

VPN, оплаченный наличными или Monero

Есть три VPN-компании, рекомендованные PrivacyGuides.org (privacyguides.org Archive.org), которые принимают оплату наличными: Mullvad, iVPN и Proton VPN.

Вот их политики ведения журналов:

• Mullvad: mullvad.net Archive.org
• iVPN: ivpn.net Archive.org
• ProtonVPN: protonvpn.com Archive.org

Кроме того, упомянем нового игрока, за которым стоит следить: Safing SPN safing.io Archive.org). На момент написания он всё ещё находился на стадии alpha, но тоже принимает наличные и предлагает очень отличающуюся концепцию VPN, дающую преимущества, похожие на изоляцию потоков Tor в их «SPN». Обратите внимание, что сейчас Safing SPN недоступен на macOS. Этот вариант предварительный и используется на ваш риск, но мы считаем, что его стоит упомянуть.

Лично мы пока рекомендовали бы Mullvad, исходя из собственного опыта.

Мы не стали бы так же уверенно рекомендовать Proton VPN, потому что для регистрации ему требуется адрес электронной почты, в отличие от Mullvad, iVPN и Safing. Кроме того, Proton склонен требовать подтверждение по номеру телефона у пользователей, которые регистрируются через Tor.

Как это работает?

• Откройте сайт VPN через безопасный браузер (см. Безопасный браузер.

• Перейдите на сайт iVPN, Mullvad или Safing и создайте новый Account ID (на странице входа).

• Эта страница выдаст вам идентификатор учётной записи, идентификатор токена для платежа и сведения о том, куда отправлять деньги по почте.

• Отправьте нужную сумму наличными за выбранную подписку в запечатанном почтовом конверте в их офис, вложив бумагу с Token ID и не указывая обратный адрес, либо оплатите Monero, если такая возможность есть. Если Monero не принимается, но принимается BTC, рассмотрите вариант анонимной онлайн-оплаты с помощью BTC.

• Дождитесь, пока они получат оплату и активируют вашу учётную запись (это может занять время).

• Откройте Tor Browser.

• Проверьте состояние учётной записи и продолжайте, когда она станет активной.

Для дополнительной безопасности рассмотрите следующие меры:

• Надевайте перчатки при работе с любыми предметами, чтобы не оставлять отпечатки пальцев[1] и контактную ДНК[2].
• Менее очевидной альтернативой может быть нанесение суперклея на кончики пальцев, чтобы не было заметно, что вы носите перчатки. Однако это может помешать нормальному использованию сенсорных экранов и хуже защищать от оставления контактной ДНК. Кроме того, если это заметят, суперклей на пальцах может выглядеть очень подозрительно.

• Не используйте материалы или купюры, с которыми работал кто-то, кого можно каким-либо образом связать с вами.

• Не используйте наличные, которые вы только что получили в банкомате: он мог записать серийные номера выданных купюр.

• Если что-то печатаете, убедитесь, что принтер не оставляет водяных меток (см. водяные метки принтеров).

• Не облизывайте конверт или марки[3], если используете их, чтобы не оставить следы ДНК.

• Убедитесь, что внутри материалов и на них нет очевидных следов ДНК, например волос.

• Рассмотрите возможность провести всю операцию на улице, чтобы снизить риск остаточных следов ДНК из вашей среды или загрязнения материалов с вашей стороны.
• Чем больше людей бывает в месте, тем ниже риск: ваша ДНК будет смешиваться с ДНК других людей, которые проходят через это пространство.

• Камеры наблюдения могут быть риском. Постарайтесь закрыть лицо. Кроме того, проблемой может быть распознавание по походке. См. распознавание по походке и другую дальнодействующую биометрию

Ни при каких обстоятельствах не используйте эту новую учётную запись VPN, пока не будет указано иначе, и не подключайтесь к ней через известные вам подключения. Этот VPN будет использоваться позже безопасным способом, поскольку мы не доверяем заявлениям VPN-провайдеров о «политике без журналов». В идеале VPN-провайдер никогда не должен узнать ваш настоящий исходный IP-адрес, например домашний или рабочий.

Самостоятельно размещённый VPN/прокси на VPS, оплаченном Monero или наличными (для пользователей, лучше знакомых с Linux)

Другой вариант - настроить собственный VPN/прокси с помощью VPS (Virtual Private Server) на хостинговой платформе, которая принимает Monero (рекомендуется).

Это даёт некоторые преимущества, поскольку вероятность того, что ваш IP-адрес где-то окажется в списке блокировки, ниже, чем у известных VPN-провайдеров.

У этого варианта есть и недостатки, поскольку Monero не идеален, как объяснялось ранее в этом руководстве, и некоторые глобальные противники, возможно, всё ещё смогут вас отследить. Вам нужно будет получить Monero на бирже через обычную финансовую систему, а затем выбрать хостинг (список здесь: getmonero.org Archive.org) или купить Monero у местного продавца за наличные через localmonero.co.

Ни при каких обстоятельствах не используйте этот новый VPS/VPN/прокси через известные вам подключения. Подключайтесь к нему только через Tor, например с помощью Whonix Workstation (это объясняется далее). Этот VPN будет использоваться позже внутри виртуальной машины через сеть Tor безопасным способом, поскольку мы не доверяем заявлениям VPN-провайдеров о «политике без журналов». VPN-провайдер никогда не должен узнать ваш настоящий исходный IP-адрес.

См. рекомендуемых провайдеров VPS-хостинга

VPN на VPS

Существует много инструкций о том, как это сделать, например эта: proprivacy.com Archive.org

SOCKS-прокси на VPS

Это тоже очевидный вариант, если вы предпочитаете пропустить часть с VPN.

Скорее всего, это проще всего настроить: вы просто используете SSH-подключение к своему VPS, а дополнительная настройка, кроме указания нужного прокси в браузере гостевой ВМ, обычно не требуется.

Вот несколько инструкций, как сделать это очень быстро:

• (Windows/Linux/macOS) linuxize.com Archive.org

• (Windows/Linux/macOS) digitalocean.com Archive.org

• (Windows) forwardproxy.com Archive.org

• (Linux/macOS) ma.ttias.be Archive.org

Вот моя базовая инструкция:

Linux/macOS

Шаги:

• Настройте анонимный VPS.

• Из терминала подключитесь к серверу по SSH командой: `ssh -i ~/.ssh/id_rsa -D 8080 -f -C -q -N username@ip_of_your_server`

• Настройте браузер на использование localhost:8080 как SOCKS-прокси для просмотра сайтов.

• Готово!

Пояснение аргументов:

• -i: путь к SSH-ключу, который будет использоваться для подключения к узлу.

• -D: сообщает SSH, что нужен SOCKS-туннель на указанном номере порта (можно выбрать число от 1025 до 65536).

• -f: отправляет процесс в фон.

• -C: сжимает данные перед отправкой.

• -q: использует тихий режим.

• -N: сообщает SSH, что после поднятия туннеля команда отправляться не будет.

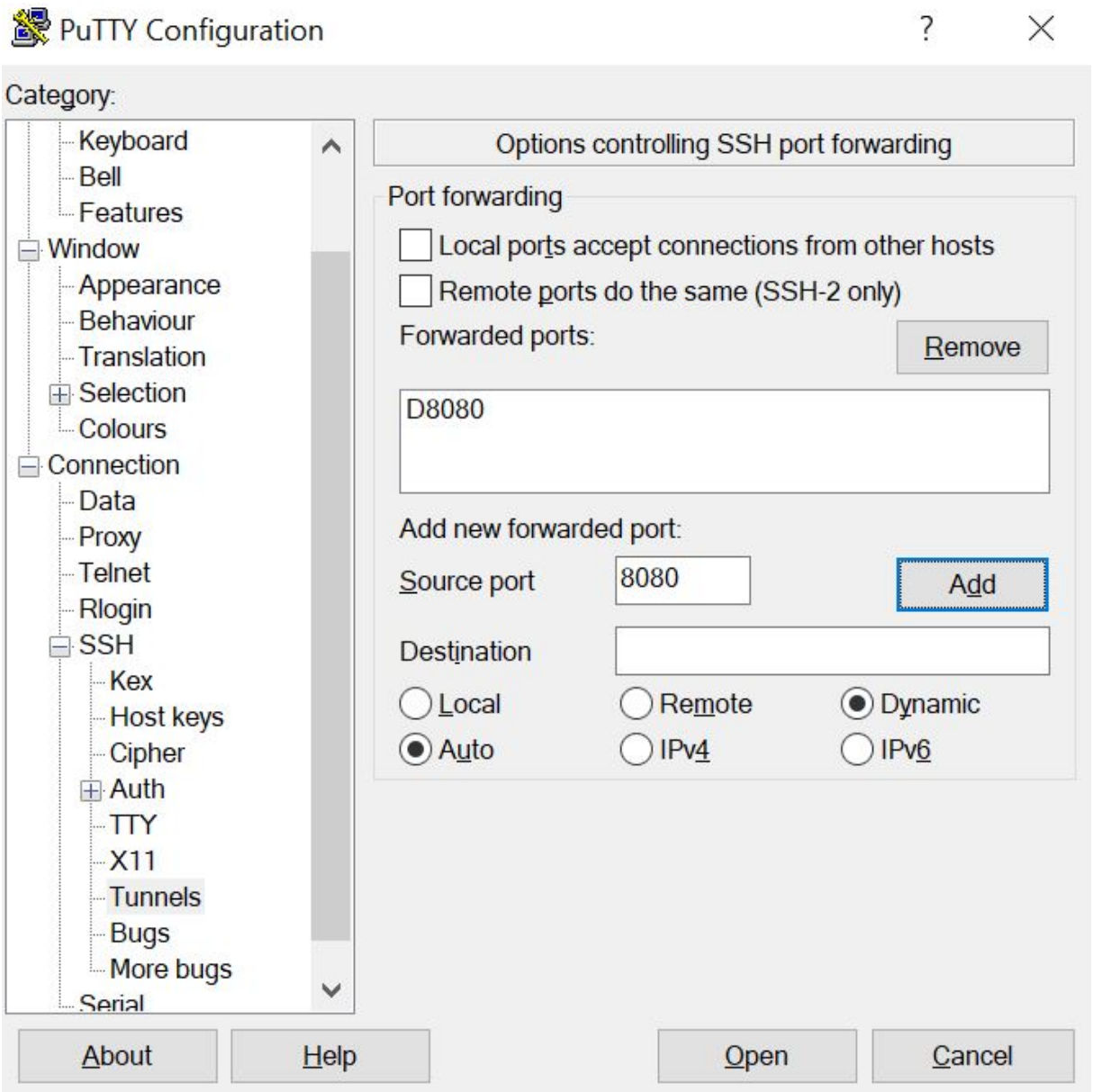
Windows

Шаги:

• Настройте анонимный VPS.

• Скачайте и установите Putty с putty.org Archive.org

• Установите следующие параметры в Putty и подключитесь к серверу.



• Подключитесь к VPS с этими настройками.

• Настройте браузер на использование localhost:8080 как SOCKS-прокси.

• Готово!

Сноски

[1] [назад] YouTube, Fingerprinting Paper - Forensic Education youtube.com Invidious
[2] [назад] Wikipedia, Touch DNA, en.wikipedia.org Wikiless Archive.org
[3] [назад] TheDNAGuide, DNA from Postage Stamps or Hair Samples? Yeeesssss..... yourdnaguide.com Archive.org

Когда Tor и VPN невозможны

БУДЬТЕ КРАЙНЕ ОСТОРОЖНЫ: ЭТО ОЧЕНЬ РИСКОВАННО.

В худших случаях Tor и VPN могут быть недоступны из-за масштабной активной цензуры или блокировки. Даже при использовании мостов Tor (см. Использование мостов Tor во враждебных средах)

Также возможны ситуации, где само использование Tor или одного только VPN может выглядеть подозрительно и быть опасным для вашей безопасности. Если это так, вы можете находиться в очень враждебной среде с высоким уровнем наблюдения и контроля.

Но вам всё равно нужно сделать что-то анонимно, не раскрывая и не утекая никаких сведений.

В таком случае моя рекомендация последней надежды - безопасно подключиться **с расстояния** к публичному Wi-Fi (см. найдите несколько безопасных мест с нормальным публичным Wi-Fi) с помощью ноутбука и «unsafe browser» в Tails. См. tails.boum.org Archive.org.

Если само использование Tor подозрительно или рискованно, НЕ позволяйте Tails пытаться установить Tor-соединение при запуске. Сделайте следующее:

• При запуске откройте Additional Settings.

• Включите Unsafe Browser.

• Измените Connection с Direct на «Configure a Tor Bridge or Local Proxy».

• После запуска подключитесь к безопасной сети.

• Когда появится запрос, просто закройте Tor Connection Wizard, чтобы не устанавливать Tor-соединение.

• Запустите и используйте Unsafe Browser.

Мы настоятельно рекомендуем использовать направленную антенну большого радиуса действия типа «Yagi» с подходящим USB Wi-Fi-адаптером. По крайней мере это позволит подключаться к публичным Wi-Fi с «безопасного расстояния», но помните, что мотивированный противник с подходящим оборудованием всё ещё может выполнить триангуляцию. Поэтому этот вариант не следует использовать длительное время (в лучшем случае минуты). См. использование антенны большого радиуса действия для подключения к публичным Wi-Fi с безопасного расстояния.

Использование Tails должно предотвратить локальные утечки данных, например MAC-адресов или телеметрии, и позволит воспользоваться браузером, чтобы получить нужное (утилиты, учётную запись VPN), а затем как можно быстрее уйти из этого места.

В таких враждебных средах можно также использовать другие маршруты, например Whonix и Qubes OS без Tor/VPN, вместо Tails, если вам нужна сохраняемость данных, но это может быть рискованнее. Лично мы не стали бы так рисковать без абсолютной необходимости. Если вы выберете этот вариант, выполняйте чувствительные действия только из откатываемой или одноразовой ВМ. Никогда не делайте этого из основной ОС.

Если вы прибегаете к этому варианту, держите время онлайн как можно короче: минуты, а не часы.

Берегите себя и будьте предельно осторожны. Всё это полностью на ваш риск.

Рассмотрите возможность прочитать это старое, но всё ещё актуальное руководство: archive.flossmanuals.net Archive.org

Подключение к публичному Wi-Fi с безопасного расстояния

К удалённым публичным Wi-Fi можно подключаться с расстояния с помощью недорогой направленной антенны, которая выглядит примерно так:

Такие антенны широко продаются в разных интернет-магазинах по низкой цене (Amazon, AliExpress, Banggood и т. п.). Единственная проблема в том, что они заметны, и вам, возможно, придётся придумать, как её спрятать, например в картонном тубусе для плакатов в рюкзаке или в достаточно большой сумке. При желании, но с большим риском, можно даже рассмотреть использование из дома, если из окна хорошо видны разные места, где есть публичный Wi-Fi.

Такие антенны нужно сочетать со специальными USB-адаптерами, у которых есть разъём для внешней антенны и достаточно высокая мощность для её использования.

Мы рекомендуем серию AWUS036 среди адаптеров Alfa (см. alfa.com.twArchive.org). Но можно выбрать и другие бренды, например TP-Link TL-WN722 (см. tp-link.com Archive.org).

См. этот пост со сравнением разных адаптеров: wirelesshack.org Archive.org (обычно такие антенны используют специалисты по тестированию на проникновение для проверки Wi-Fi с расстояния, и их часто обсуждают в контексте дистрибутива Kali Linux).

Процесс простой:

• Подключите и установите USB-адаптер в основной ОС.

• **Не забудьте рандомизировать MAC-адрес, если вы купили этот адаптер онлайн, чтобы снизить отслеживаемость (в Tails это включено по умолчанию).**

• Подключите антенну большого радиуса действия к USB-адаптеру вместо штатной.

• Найдите удобное место, откуда видна точка с доступным публичным Wi-Fi на расстоянии, например крышу; также можно представить вариант, где антенна спрятана в сумке, а вы просто сидите где-нибудь на скамейке.

• Направьте антенну в сторону публичного Wi-Fi.

• Подключитесь к выбранному Wi-Fi.

Не забывайте, что это лишь задержит мотивированного противника. Ваш сигнал можно довольно быстро триангулировать, если мотивированный противник доберётся до физического места, где находится Wi-Fi, к которому вы подключаетесь, например с помощью устройства вроде AirCheck youtube.comInvidious, также см. другие продукты здесь: netally.comArchive.org). Такие продукты легко разворачиваются на мобильных платформах, например в автомобиле, и могут определить ваше местоположение за считанные минуты.

В идеале это «не должно быть проблемой», поскольку в этом руководстве предложено несколько способов скрывать исходный IP-адрес с помощью VPN и Tor. Но если вы находитесь в ситуации, где VPN и Tor невозможны, это может быть вашей единственной защитой.

Установка VPN на вашу ВМ или основную ОС

Скачайте установщик клиента VPN для сервиса, оплаченного наличными, и установите его на основную ОС (Tor over VPN, VPN over Tor over VPN) или на выбранную ВМ (VPN over Tor):

- Инструкция Whonix (должна работать с любым VPN-провайдером): whonix.org Archive.org (используйте приведённые ниже настройки Linux, чтобы получить нужные файлы конфигурации)
- Инструкции для Windows:
  - Mullvad: mullvad.net Archive.org
  - iVPN: ivpn.net Archive.org
  - Safing: docs.safing.io Archive.org
  - Proton VPN: protonvpn.com Archive.org
- macOS:
  - Mullvad: mullvad.net Archive.org
  - IVPN: ivpn.net Archive.org
  - Safing: недоступен на macOS.
  - Proton VPN: protonvpn.com Archive.org
- Linux:
  - Mullvad: mullvad.net Archive.org
  - iVPN: ivpn.net Archive.org
  - Safing: docs.safing.io Archive.org
  - Proton VPN: protonvpn.com Archive.org

Важное примечание: Tor не поддерживает UDP, поэтому в сценариях Tor over VPN на ВМ следует использовать TCP в клиенте VPN.

Во всех случаях стоит настроить запуск VPN при загрузке и включить аварийное отключение соединения («kill switch»), если это возможно. Это дополнительный шаг, поскольку решения в этом руководстве при сбое VPN всё равно возвращаются к сети Tor.

Вот несколько инструкций от VPN-провайдеров, рекомендованных в этом руководстве:

- Windows:
  - iVPN: ivpn.net Archive.org
  - Proton VPN: protonvpn.com Archive.org
  - Mullvad: mullvad.net Archive.org
- Whonix Workstation: скоро появится. Это, безусловно, возможно, но мы пока не нашли подходящую и простую инструкцию. Также стоит помнить, что если VPN остановится в Whonix, вы всё равно останетесь за сетью Tor.
- macOS:
  - Mullvad: так же, как в Windows; параметр должен быть в поставляемом VPN-клиенте.
  - iVPN: так же, как в Windows; параметр должен быть в поставляемом VPN-клиенте.

    - Proton VPN: так же, как в Windows, через клиент; параметр должен быть в поставляемом VPN-клиенте protonvpn.com Archive.org
- Linux:
    - Mullvad:
        - mullvad.net Archive.org
        - mullvad.net Archive.org
    - Proton VPN: github.com Archive.org
    - iVPN:
        - ivpn.net Archive.org
        - ivpn.net Archive.org

Обнаружение сетевого наблюдения и цензуры с помощью OONI

Итак, что такое OONI? OONI означает Open Observatory of Network Interference и является подпроектом Tor Project[1].

Во-первых, OONI позволит проверить онлайн наличие наблюдения или цензуры в вашей стране, просто посмотрев их Explorer, где представлены результаты тестов других людей. Это можно сделать здесь: explorer.ooni.org

Но такие тесты ограничены и могут не отражать вашу личную ситуацию. Если это так, можно рассмотреть самостоятельный запуск OONI Probe и самостоятельное выполнение тестов.

Проблема в том, что ваши сетевые провайдеры смогут видеть эти тесты и ваши попытки подключаться к различным сервисам, если сеть отслеживается. Другая проблема в том, что существуют решения, мешающие OONI работать правильно[2].

В обычной среде это может быть неважно, но во враждебной среде это может подвергнуть вас риску. **Поэтому запуск этих тестов может быть опасен.**

Если вы находитесь в такой враждебной среде, где подозреваете активное наблюдение за сетевой активностью, а сам факт попытки доступа к некоторым ресурсам может подвергнуть вас риску, перед любой попыткой следует принять меры предосторожности:

- **Не запускайте тесты из домашней или рабочей сети.**
- **Не запускайте эти тесты с известного устройства или смартфона; используйте только защищённую ОС, в идеале на отдельном ноутбуке.**
  - **Из Tails вы не сможете сделать это, поскольку Tails по умолчанию попытается подключиться к Tor.**
  - **Делайте это только по маршруту Qubes OS или маршруту Whonix из этого руководства после завершения одного из маршрутов.**
- **Рассматривайте запуск этих тестов только быстро, из публичного Wi-Fi с безопасного расстояния (см. что делать, когда Tor и VPN невозможны?).**

OONI Probe для разных платформ (iOS, Android, Windows, macOS и Linux) можно найти здесь: ooni.org Archive.org.

Сноски

[1] [назад] Wikipedia, OONI, en.wikipedia.org Wikiless Archive.org
[2] [назад] GitHub, Mhinkie, OONI-Detection github.com Archive.org

Проверка файлов на вредоносное ПО

Целостность (если доступна)

Обычно проверки целостности[1] выполняются с помощью хешей файлов, которые обычно хранятся в файлах контрольных сумм. Старые файлы могли использовать CRC[2], более новые - MD5[3], но у них есть несколько слабостей (CRC, MD5[4]), из-за которых они ненадёжны для проверки целостности файлов. Это не означает, что они всё ещё не используются широко в других контекстах.

Причина в том, что они недостаточно хорошо предотвращают коллизии[5] и могут позволить противнику создать похожий, но вредоносный файл, который всё равно даст тот же хеш CRC или MD5, несмотря на другое содержимое.

Поэтому обычно рекомендуется использовать хеши на основе SHA[6], а самым распространённым для проверки целостности файлов, вероятно, является SHA-256 на основе SHA-2[7]. SHA гораздо устойчивее к коллизиям[8], чем CRC и MD5. Коллизии с SHA-256 или SHA-512 редки и трудны для вычисления противником.

Если источник файла предоставляет контрольную сумму SHA-256, не стоит стесняться использовать её для подтверждения целостности файла. Обратите внимание, что SHA-1 не рекомендуется, но он лучше, чем отсутствие хеша для сравнения.

Сама контрольная сумма должна быть подтверждённой и доверенной, а также должна поступать из подтверждённого и доверенного источника. Очевидно, не следует доверять файлу только потому, что к нему приложена контрольная сумма.

В случае этого руководства контрольные суммы SHA-256 доступны для каждого файла, включая PDF, и также подтверждаются GPG-подписью, что позволяет проверить подлинность контрольной суммы. Это подводит нас к следующему разделу о подлинности.

Как проверить контрольные суммы? В этом случае используется SHA-256, но можно заменить его на SHA-512.

- Windows[9]:
  - Откройте Command Prompt.
  - Выполните `certutil -hashfile filename.txt sha256` (замените sha256 на sha1, sha512 или md5).
  - Сравните результат с контрольной суммой из источника, которому вы доверяете для этого файла.
- macOS:
  - Откройте Terminal.
  - SHA: выполните `shasum -a 256 /full/path/to/your/file` (замените 256 на 512 или 1 для SHA-1).
  - MD5: выполните `md5 /full/path/to/your/file`.

    - Сравните результат с контрольной суммой из источника, которому вы доверяете для этого файла.
- Linux:
    - Откройте Terminal.
    - Выполните `shasum /full/path/to/your/file` (замените shasum на sha256sum, sha512sum или md5sum).
    - Сравните результат с контрольной суммой из источника, которому вы доверяете для этого файла.

Помните: контрольные суммы - это всего лишь контрольные суммы. Совпадающая контрольная сумма не означает, что файл безопасен.

Подлинность (если доступна)

Целостность - это одно. Подлинность - другое. Это процесс, при котором можно проверить, что сведения подлинны и поступили из ожидаемого источника. Обычно это делается путём подписи сведений, например с помощью GPG[10], с использованием криптографии с открытым ключом[11].

Подпись может служить обеим целям и позволяет проверить и целостность, и подлинность.

Если подписи файлов доступны, всегда следует проверять их, чтобы подтвердить подлинность файлов.

В общих чертах:

- Установите GPG для своей ОС:
    - Windows: gpg4win (gpg4win.org Archive.org)
    - macOS: GPGTools (gpgtools.org Archive.org)
    - Linux: в большинстве дистрибутивов он должен быть предустановлен.
- Скачайте ключ подписи из доверенного источника. Если кто-то не передаёт вам ключ напрямую, следует проверить несколько версий на других сайтах, чтобы убедиться, что вы используете правильный ключ (GitHub, GitLab, Twitter, Keybase, серверы открытых ключей и т. п.).
- Импортируйте доверенный ключ (замените keyfile.asc на имя файла доверенного ключа):
    - Windows:
        - Из Command Prompt выполните `gpg --import keyfile.asc`.
    - macOS:
        - Из Terminal выполните `gpg --import keyfile.asc`.
    - Linux:
        - Из Terminal выполните `gpg --import keyfile.asc`.
- Проверьте подпись файла по импортированной доверенной подписи (замените filetoverify.asc на файл подписи, связанный с файлом, а filetoverify.txt - на реальный файл для проверки):
    - Windows:
        - Выполните `gpg --verify-options show-notations --verify filetoverify.asc filetoverify.txt`.

    - Результат должен показать, что подпись корректна и совпадает с доверенной подписью, импортированной ранее.
- macOS:
    - Выполните `gpg --verify-options show-notations --verify filetoverify.asc filetoverify.txt`.
    - Результат должен показать, что подпись корректна и совпадает с доверенной подписью, импортированной ранее.
- Linux:
    - Выполните `gpg --verify-options show-notations --verify filetoverify.asc filetoverify.txt`.
    - Результат должен показать, что подпись корректна и совпадает с доверенной подписью, импортированной ранее.

Другие инструкции:

- support.torproject.org Archive.org
- tails.boum.org Archive.org (см. Basic OpenPGP verification).
- whonix.org Archive.org

Все эти руководства также должны подходить для любого другого файла с любым другим ключом.

Безопасность (проверка на реальное вредоносное ПО)

В идеале каждая проверка должна выполняться в изолированных и усиленных виртуальных машинах. Это нужно, чтобы снизить вероятность доступа вредоносного ПО к вашему основному компьютеру.

Антивирусное программное обеспечение

Вы можете спросить: а как насчёт антивирусных решений? Ну, нет... это не идеальные решения против многих современных вредоносных программ и вирусов, использующих полиморфный код[12]. Но это не означает, что они не могут помочь против менее сложных и известных атак. Всё зависит от того, как их использовать, поскольку само антивирусное программное обеспечение может стать вектором атаки.

Опять же, всё упирается в моделирование угроз. Поможет ли антивирусное программное обеспечение против NSA? Вероятно, нет. Может ли оно помочь против менее обеспеченных ресурсами противников, использующих известное вредоносное ПО? Вероятно, да.

Некоторые, например Whonix[13], в целом выступают против них, но эта тема обсуждается и оспаривается даже в Whonix[14] другими участниками сообщества.

Вопреки распространённым мифам, поддерживающим идею, что вредоносное ПО бывает только под Windows, а инструменты обнаружения бесполезны в Linux и macOS:

- Да, для Linux существуют вирусы и вредоносное ПО[15][16][17][18][19]

• Да, для macOS существуют вирусы и вредоносное ПО[20][21][22][23][24]

Моя позиция в этом вопросе прагматична. Для некоторого выборочного и ограниченного использования антивирусному программному обеспечению всё ещё есть место. Но это зависит от того, какое именно средство вы используете и как:

• Не используйте антивирусное программное обеспечение с защитой в реальном времени, поскольку оно часто работает с правами администратора и само может стать вектором атаки.

• Не используйте коммерческое антивирусное программное обеспечение, которое применяет какую-либо «облачную защиту» или отправляет обширную телеметрию и образцы файлов компании-разработчику.

• Используйте открытые автономные антивирусные и противовредоносные инструменты без защиты в реальном времени как дополнительную меру для сканирования отдельных файлов, например:

  • Windows/Linux/macOS/Qubes OS: ClamAV (clamav.net Archive.org)

  • Linux/Qubes OS: RFXN Linux Malware Detect (github.com Archive.org)

  • Linux/Qubes OS: Chkrootkit (chkrootkit.org Archive.org)

• Для **нечувствительных файлов** можно также использовать онлайн-сервисы, такие как VirusTotal (virustotal.com) или Hybrid-analysis (hybrid-analysis.com).

  • Если вы не хотите отправлять файл, можно просто проверить базу VirusTotal по хешу файла (см. developers.virustotal.com Archive.org; снова см. раздел Целостность (если доступна), где объясняется, как создавать хеши).

  • Для нечувствительных файлов доступны и другие инструменты; удобный список находится здесь: github.com Archive.org

• **Учтите, что VirusTotal может казаться очень практичным для сканирования разных файлов, но его «политика конфиденциальности» проблематична (см. support.virustotal.comArchive.org) и утверждает:**

«Когда вы отправляете образцы в сервисы, если вы отправляете образцы в сервисы, вы собираете все сведения в самом образце и сведения о факте его отправки».

Поэтому помните: любой документ, который вы им отправляете, будет сохранён, передан другим и использован коммерчески, включая содержимое. Не делайте этого с чувствительной информацией и полагайтесь на разные локальные антивирусные сканеры, которые не отправляют образцы онлайн.

Итак, если сомневаетесь:

• Для нечувствительных файлов мы рекомендуем проверять любые документы, изображения, видео, архивы и программы, которые вы собираетесь открыть, через VirusTotal или похожие инструменты. Почему бы и нет? Можно загрузить файл или проверить хеш.

• Для чувствительных файлов мы рекомендуем как минимум автономную проверку ClamAV без повышенных привилегий.

Например, PDF-файлы этого руководства были отправлены в VirusTotal, поскольку они предназначены для публичного знания, и мы не видим веских причин против этого. Это не гарантирует отсутствия вредоносного ПО, но добавить такую проверку не вредно.

Ручная проверка

Можно также попытаться проверить разные файлы на вредоносное ПО с помощью разных инструментов. Это можно делать как дополнительную меру; особенно полезно для документов, а не приложений и разных исполняемых файлов.

Эти методы требуют больше возни, но могут быть полезны, если вы хотите проверить всё особенно тщательно.

PDF-файлы

Снова о PDF этого руководства: как объясняется в README моего репозитория, можно проверить их на аномалии с помощью PDFID, который можно скачать по адресу blog.didierstevens.com Archive.org:

• Установите Python 3 (на Windows/Linux/macOS/Qubes OS).

• Скачайте PDFID и распакуйте файлы.

• Выполните `python pdfid.py file-to-check.pdf`; для PDF-файлов в этом репозитории вы должны увидеть нули в этих строках:

```
/JS 0 #Это указывает на наличие Javascript
/JavaScript 0 #Это указывает на наличие Javascript
/AA 0 #Это указывает на наличие автоматического действия при открытии
/OpenAction 0 #Это указывает на наличие автоматического действия при открытии
/AcroForm 0 #Это указывает на наличие AcroForm, которая может содержать JavaScript
/JBIG2Decode 0 #Это указывает на использование сжатия JBIG2, которое может применяться для сокрытия
    содержимого
/RichMedia 0 #Это указывает на наличие мультимедийного содержимого в PDF, например Flash
/Launch 0 #Это считает действия запуска
/EmbeddedFile 0 #Это указывает на наличие встроенных файлов в PDF
/XFA 0 #Это указывает на наличие XML Forms в PDF
```

А что, если PDF всё равно кажется подозрительным? Не бойтесь... есть дополнительные меры, чтобы убедиться, что он не вредоносный:

• **Qubes OS:** рассмотрите использование github.com Archive.org, который преобразует PDF в плоский файл изображения. Теоретически это должно удалить любой вредоносный код внутри. Обратите внимание, что это также сделает бесполезным форматирование PDF, например ссылки, заголовки, закладки и ссылки на источники.

• **(Устарело) Linux/Qubes OS** (или, возможно, macOS через Homebrew либо Windows через Cygwin): это *теоретически* должно удалить любой вредоносный код внутри, но также сделает бесполезным форматирование PDF, например ссылки, заголовки, закладки и ссылки на источники. Это похоже на то, как растеризация этого сайта в PDF работает при переключении в тёмный режим. **Обратите внимание, что этот инструмент устарел и зависит от библиотеки ImageMagick, известной несколькими проблемами безопасности[25]. Не следует использовать этот инструмент, даже если он рекомендован в некоторых других руководствах.**

Другие типы файлов

Вот несколько разных ресурсов для этой цели, где можно найти, какой инструмент использовать для какого типа файлов:

- **Для документов и изображений:** рассмотрите использование github.com Archive.org, вдохновлённого Qubes PDF Converter выше; он делает то же самое, но хорошо поддерживается и работает во всех ОС. Этот инструмент также работает с изображениями, файлами ODF и Office (предупреждение: в Windows этому инструменту нужен установленный Docker Desktop, и это может, а точнее будет, мешать VirtualBox и другому программному обеспечению виртуализации, потому что требует включения Hyper-V. VirtualBox и Hyper-V плохо уживаются друг с другом[26]. Для удобства рассмотрите установку внутри Linux ВМ вместо Windows).
- **Для видео:** будьте крайне осторожны, используйте актуальный проигрыватель в изолированной среде. Помните vice.com Archive.org
- Эта практичная шпаргалка SANS: digital-forensics.sans.org Archive.org (предупреждение: многие из этих инструментов может быть сложнее использовать в Windows, и стоит рассмотреть их запуск из Linux ОС, например Tails, Whonix Workstation или выбранного вами дистрибутива Linux, как объясняется далее в этом руководстве. Также существуют другие руководства[20], которые могут быть полезны).
- Этот GitHub-репозиторий с разными ресурсами по анализу вредоносного ПО: github.com Archive.org
- Этот интересный PDF с описанием, какой инструмент использовать для какого типа файлов: winitor.com Archive.org

Даже со всеми этими ресурсами помните: вы всё равно можете столкнуться с продвинутым вредоносным ПО, если оно не обнаруживается этими инструментами. Будьте осторожны и по возможности обрабатывайте такие файлы в изолированных виртуальных машинах, чтобы ограничить поверхность и векторы атаки.

Сноски

[1] [назад] Wikipedia, File Verification en.wikipedia.org Wikiless Archive.org
[2] [назад] Wikipedia, CRC en.wikipedia.org Wikiless Archive.org
[3] [назад] Wikipedia, MD5 en.wikipedia.org Wikiless Archive.org
[4] [назад] Wikipedia, MD5 Security en.wikipedia.org Wikiless Archive.org
[5] [назад] Wikipedia, Collisions en.wikipedia.org Wikiless Archive.org
[6] [назад] Wikipedia, SHA en.wikipedia.org Wikiless Archive.org
[7] [назад] Wikipedia, SHA-2 en.wikipedia.org Wikiless Archive.org
[8] [назад] Wikipedia, Collision Resistance en.wikipedia.org Wikiless Archive.org
[9] [назад] GnuPG Gpg4win Wiki, Check integrity of Gpg4win packages wiki.gnupg.org Archive.org
[10] [назад] Wikipedia, GPG en.wikipedia.org Wikiless Archive.org
[11] [назад] Wikipedia, Public-Key Cryptography en.wikipedia.org Wikiless Archive.org
[12] [назад] Wikipedia, Polymorphic Code en.wikipedia.org Wikiless Archive.org
[13] [назад] Whonix Documentation, Use of AV, whonix.org Archive.org
[14] [назад] Whonix Forums, forums.whonix.org Archive.org
[15] [назад] AV-Test Security Report 2018-2019, av-test.org Archive.org
[16] [назад] ZDNet, ESET discovers 21 new Linux malware families zdnet.com Archive.org
[17] [назад] NakeSecurity, EvilGnome -- Linux malware aimed at your desktop, not your servers nakedsecurity.sophos.com Archive.org
[18] [назад] Immunify, HiddenWasp: How to detect malware hidden on Linux & IoT blog.imunify360.com Archive.org
[19] [назад] Wikipedia, Linux Malware en.wikipedia.org Wikiless Archive.org
[20] [назад] Lenny Zeltser, Analyzing Malicious Documents Cheat Sheet zeltser.com Archive.org
[21] [назад] Wikipedia, macOS Malware en.wikipedia.org Wikiless Archive.org
[22] [назад] MacWorld, List of Mac viruses, malware and security flaws macworld.co.uk Archive.org
[23] [назад] JAMF, The Mac Malware of 2020 resources.jamf.com Archive.org
[24] [назад] macOS Security and Privacy Guide, github.com Archive.org
[25] [назад] ImageTragick.com, imagetragick.com Archive.org
[26] [назад] Oracle Virtualbox Documentation, docs.oracle.com Archive.org

Обход локальных ограничений на контролируемых компьютерах

Бывают ситуации, когда единственное доступное вам устройство на самом деле вам не принадлежит, например:

• Рабочий компьютер с ограничениями на то, что можно делать или запускать.

• Злоупотребление функциями родительского контроля для наблюдения за использованием вашего компьютера, несмотря на то что вы взрослый человек и не давали согласия.

• Злоупотребление разными приложениями наблюдения для отслеживания использования вашего компьютера против вашей воли.

Ситуация может выглядеть безнадёжной, но это не обязательно так: существуют безопасные способы обойти такие ограничения, в зависимости от того, насколько хорошо ваши противники защитили компьютер.

Портативные приложения

Есть много методов, с помощью которых можно локально обойти такие ограничения. Один из них - использовать портативные приложения[1]. Такие приложения не требуют установки в систему и могут запускаться с USB-накопителя или из любого другого места.

Но мы не рекомендуем этот метод.

Причина в том, что портативные приложения не обязательно скрывают себя и не обязательно способны скрыться от отчётов об использовании и криминалистического анализа. Этот метод слишком рискован и, вероятно, вызовет проблемы, если будет замечен в такой враждебной среде.

Даже самые базовые средства контроля, надзорные или родительские, будут отправлять вашему противнику подробные сведения об использовании приложений.

Загрузочные live-системы

Именно этот метод мы рекомендовали бы в таких случаях.

Вашему противнику сравнительно легко предотвратить это, настроив средства контроля в прошивке BIOS/UEFI (см. настройки BIOS/UEFI/прошивки вашего ноутбука), но обычно большинство противников упускают такую возможность, потому что она требует больше технических знаний, чем простая опора на программное обеспечение.

Этот метод может даже снизить подозрения и повысить правдоподобное отрицание: ваши противники думают, что всё под контролем, а в их отчётах всё выглядит нормально.

Этот метод зависит только от одной функции безопасности, которую они, вероятно, в большинстве случаев не включили: защиты загрузки.

Защита загрузки делится на несколько типов:

• Простой пароль BIOS/UEFI, не позволяющий изменить порядок загрузки. Это означает, что вы не сможете запустить такую live-систему вместо контролируемой ОС без ввода пароля BIOS/UEFI.

• Secure Boot. Это «стандартная» функция, которая не позволяет запускать неподписанные системы с вашего компьютера. Хотя её можно настроить так, чтобы разрешалась только ваша контролируемая система, обычно по умолчанию она разрешает запуск целого ряда подписанных систем, например подписанных Microsoft или производителем.

Secure Boot сравнительно легко обойти, поскольку сейчас есть много live-систем, совместимых с Secure Boot, то есть подписанных, и ноутбук разрешит их запуск.

Пароль BIOS/UEFI, напротив, гораздо сложнее обойти без риска. В таком случае остаются два варианта:

• Угадать или знать пароль, чтобы изменить порядок загрузки ноутбука, не вызывая подозрений.

• Сбросить пароль разными методами. **Мы не рекомендуем это делать, потому что если ваши противники приложили дополнительные усилия и включили эту функцию безопасности, они, вероятно, заподозрят неладное, если она окажется отключена; это может существенно усилить подозрения и снизить ваше правдоподобное отрицание.**

Опять же, большинство неопытных или ленивых противников обычно упускают эту функцию и, по моему опыту, оставляют её отключённой.

Это ваш лучший шанс обойти локальные средства контроля без следов.

Причина в том, что большинство средств контроля находятся внутри программного обеспечения вашей основной операционной системы и отслеживают только то, что происходит внутри неё. Эти меры не смогут отследить, что происходило на уровне оборудования или прошивки до загрузки операционной системы.

Меры предосторожности

Хотя вы можете легко обойти локальные ограничения с помощью live-системы, такой как Tails, помните, что ваша сеть тоже может отслеживаться на предмет необычной активности.

Необычная сетевая активность с компьютера в тот момент, когда ваш компьютер якобы выключен, может вызвать подозрения.

Если вы прибегаете к этому варианту, никогда не делайте этого из отслеживаемой или известной сети; используйте только другую безопасную сеть. В идеале - безопасный публичный Wi-Fi (см. найдите несколько безопасных мест с нормальным публичным Wi-Fi).

Не используйте live-систему на устройстве, контролируемом или отслеживаемом программным обеспечением, в известной сети.

Чтобы добиться этого, обратитесь к маршруту Tails. См. разделы маршрут Tails и что делать, когда Tor и VPN невозможны?.

[1] [назад] Wikipedia, Portable Applications en.wikipedia.org Wikiless Archive.org

Выбор браузера для гостевой ВМ

Временное важное предупреждение: для всех браузеров, кроме Tor Browser, см. атаки деанонимизации по микроархитектурным побочным каналам.

Есть 6 вариантов браузера для использования в гостевой или одноразовой ВМ:

• Brave (на основе Chromium)

• Edge (на основе Chromium, только Windows)

• Firefox

• Safari (только ВМ macOS)

• Tor Browser

Ниже приведена сравнительная таблица одного теста цифрового отпечатка разных браузеров с их исходными настройками (**но с включённым Javascript для удобства, кроме режима Tor Safest**).

Отказ от ответственности: эти тесты полезны, но не являются окончательным доказательством реальной устойчивости к цифровым отпечаткам. Однако они помогают сравнить браузеры между собой.

Браузер	**coveryourtracks.eff.org Тест цифрового отпечатка с настоящей рекламой**
Safari (Normal, только macOS)	Провал (уникальный)
Safari (Private Window, только macOS)	Провал (уникальный)
Edge (Normal)	Провал (уникальный)
Edge (Private Window)	Провал (уникальный)
Firefox (Normal)	Провал (уникальный)
Firefox (Private Window)	Провал (уникальный)
Chrome (Normal)	Провал (уникальный)
Chrome (Private Window)	Провал (уникальный)
Brave (Normal)	Пройден (рандомизированный)
Brave (Private Window)	Пройден (рандомизированный)
Brave (Tor Window)	Пройден (рандомизированный)
Tor Browser (Normal mode)	Частично
Tor Browser (Safer mode)	Частично
Tor Browser (Safest mode)	Неизвестно (результат не загрузился)

Ещё один полезный ресурс для сравнения браузеров: privacytests.org Archive.org

Brave

Это мой рекомендованный и предпочтительный выбор браузера внутри гостевых ВМ. Это не мой рекомендованный выбор браузера в основной ОС: там мы строго рекомендуем Tor Browser, как рекомендуют и они сами[1].

Почему Brave, несмотря на споры[2]?

• Позже у вас будет меньше проблем при создании учётных записей, например с капчами. Это основано на нашем опыте создания множества онлайн-личностей с разными браузерами. Здесь вам придётся поверить нам на слово.

• Вы получите встроенную блокировку рекламы, которой в других браузерах по умолчанию нет без установки расширений[3].

• Производительность, вероятно, лучше, чем у Firefox[4].

• Brave, вероятно, лучше сопротивляется цифровым отпечаткам, чем другие браузеры[5].

• Безопасность браузера на основе Chromium, вероятно, выше, чем у Firefox[6][7]. В контексте этого руководства безопасности следует отдавать приоритет, чтобы не дать уязвимости или эксплойту получить доступ к ВМ.

• Сравнение обоих браузеров от Mozilla: mozilla.org Archive.org

• Сравнение обоих браузеров от Techlore: youtube.com Invidious

• Весь трафик всё равно будет маршрутизироваться через VPN поверх Tor. Поэтому даже если вы по ошибке согласитесь на какую-то телеметрию, это не так важно. Помните: в этой модели угроз для анонимности нас в основном интересуют анонимность и безопасность. Приватность наших онлайн-личностей не так важна, если только проблема приватности одновременно не является проблемой безопасности, способной помочь вас деанонимизировать.

• Было установлено, что Brave не отправляет идентифицируемую телеметрию по сравнению с другими браузерами[8].

Ungoogled-Chromium

Этот браузер считается риском безопасности из-за систематического отставания с исправлениями безопасности[9].

Настоятельно не рекомендуется использовать Ungoogled-Chromium.

Edge

Это только для пользователей Windows. Edge тоже хороший выбор.

• Позже у вас будет меньше проблем при создании учётных записей, например с капчами. Это основано на нашем опыте создания множества онлайн-личностей с разными браузерами. Здесь вам придётся поверить нам на слово.

• Безопасность лучше, чем у Firefox, поскольку он основан на Chromium[10][11].

• Производительность лучше, чем у Firefox.

• Весь трафик всё равно будет маршрутизироваться через Tor.

• Можно получить дополнительную защиту с помощью Microsoft Defender Application Guard (MDAG)[12]. Обратите внимание, что эту функцию, к сожалению, нельзя включить в ВМ VirtualBox.

• Встроенная блокировка трекеров, похожая на Brave Shields.

Минусы:

• Вам придётся отключить часть телеметрии внутри браузера.

Safari

Браузер macOS по умолчанию.

Плюсы:

• Это браузер с приличными возможностями безопасности и изоляции.

Минусы:

• Он только для macOS (очевидно).

• Для установки расширений он требует входа в App Store, что невозможно в рамках этого руководства, поскольку это ВМ.

• Даже если бы это было возможно, ему не хватает лучших расширений, доступных для Firefox и Chrome.

В целом мы не рекомендуем использовать Safari в ВМ macOS; лучше выбрать другой браузер, например Brave или Firefox.

Firefox

И, конечно, наконец можно выбрать Firefox.

Плюсы:

• Он вне мира Chromium и не участвует в расширении рыночной доли Chromium.

• Помимо выхода за пределы мира Chromium, он также полностью вне мира Google, несмотря на то что Mozilla Foundation почти полностью финансируется Google[13].

• Впечатляющий объём настройки через расширения почти под любую потребность.

• Firefox можно серьёзно усилить, почти до уровня безопасности браузеров на основе Chromium.

Минусы:

• Более слабая производительность по сравнению с Chromium.

Безопасность Firefox, особенно изоляция, вероятно, слабее, чем у браузеров на основе Chromium[14].

• Вы столкнётесь с большим количеством капч (это основано на моих тестах).

Tor Browser

Если вы сверхпараноидальны и хотите использовать Tor Browser, получив «Tor over VPN over Tor», можно использовать Tor Browser и внутри ВМ. Это совершенно бессмысленно и бесполезно.

Мы не рекомендуем этот вариант. Это просто глупо.

Сноски

[1] [назад] Brave Help, What is a Private Window with Tor Connectivity? support.brave.com Archive.org
[2] [назад] BlackGNU, Brave, the false sensation of privacy blackgnu.net Archive.org
[3] [назад] Brave Help Center, What is "Shields"? support.brave.com Archive.org
[4] [назад] VentureBeat, Browser benchmark battle January 2020: Chrome vs. Firefox vs. Edge vs. Brave venturebeat.com Archive.org
[5] [назад] Brave.com, Brave, Fingerprinting, and Privacy Budgets brave.com Archive.org
[6] [назад] Madaidan's Insecurities, Firefox and Chromium madaidans-insecurities.github.io Archive.org
[7] [назад] GrapheneOS, Web Browsing grapheneos.org Archive.org
[8] [назад] ResearchGate, Web Browser Privacy: What Do Browsers Say When They Phone Home? researchgate.net Archive.org
[9] [назад] Duck's pond, Ungoogled-Chromium qua3k.github.io Archive.org
[10] [назад] Madaidan's Insecurities, Firefox and Chromium madaidans-insecurities.github.io Archive.org
[11] [назад] GrapheneOS, Web Browsing grapheneos.org Archive.org
[12] [назад] Microsoft.com, Microsoft Edge support for Microsoft Defender Application Guard docs.microsoft.com Archive.org
[13] [назад] PcMag, Mozilla Signs Lucrative 3-Year Google Search Deal for Firefox pcmag.com Archive.org
[14] [назад] Madaidan's Insecurities, Firefox and Chromium madaidans-insecurities.github.io Archive.org

Усиление браузеров

В этом разделе мы обсудим усиление браузеров. Основной акцент здесь на разнице между снижением отслеживания и уклонением от отслеживания, а также на плюсах и минусах каждого подхода. Сначала определим их так, как это описывает Rohan Kumar:

- Снижение отслеживания (TR)
  - TR стремится уменьшить объём данных, собираемых об открытом пользователе. Оно снижает распространение следа в основном за счёт блокировки трекеров. Иногда это может увеличить размер следа.
- Уклонение от отслеживания (TE)
  - TE уменьшает объём данных, раскрываемых пользователем. Вместо устранения самого сбора данных TE изначально не даёт предоставить полезные данные. Иными словами, оно уменьшает размер следа.

Браузеры, обеспечивающие снижение отслеживания, используются для более повседневной модели угроз, тогда как уклонение от отслеживания сложнее. Но рассмотреть нужно оба подхода. Снижение отслеживания сосредоточено на просмотре сайтов с меньшим объёмом отслеживания. Сюда входят блокировка содержимого, межсетевые экраны, отказы от участия, отключение телеметрии и т. п. Если вы дошли до этого места руководства, вы, вероятно, уже хорошо это понимаете. Уклонение от отслеживания, однако, включает такие методы, как использование переносимого Tor Browser Bundle для анонимизации вашего следа и онлайн-личности, избегание идентифицируемых расширений и использование случайных задержек нажатий клавиш. Оно больше про минимизацию вашего онлайн-следа, чтобы среда просмотра и использование интернета оставались менее пригодными для снятия цифрового отпечатка.

Кратко упомянуть это нужно, чтобы определить операционные потребности для обоих подходов. Для хороших стандартов и выработки лучших привычек просмотра нужен определённый уровень понимания обоих. В целом это может дать более жизнеспособное решение против публичных трекеров, государственных организаций, пытающихся связать ваши привычки просмотра с вами, и даже обычных людей, пытающихся вас доксить.

Ниже приведены рекомендуемые самые безопасные маршруты для каждого браузера с учётом текущих версий соответствующего программного обеспечения и способности каждого браузера стать безопаснее. В руководстве мы дадим и снижение отслеживания, и уклонение от отслеживания; вам не придётся написать ни одной строки кода.

Brave

- Скачайте и установите Brave Browser с brave.com Archive.org
- **Откройте** Brave Browser.
- Перейдите в **Settings** > **Appearances** (`brave://settings/appearance`)
  - **Отключите** "Show Top Sites".
  - **Отключите** "Show Brave Suggested Sites".
  - **Отключите** "Show Brave Rewards icon in address bar".

    - **Включите** "Always show full URLs".
- Перейдите в **Settings** > **Shields** (`brave://settings/shields`)
    - Установите Shields в **Advanced**.
    - Установите "Trackers and Ads blocking" в **Aggressive**.
    - Установите Upgrade connections to HTTPS в **Enabled**.
    - Установите Cookie blocking в **Only cross-site**.
    - Установите Fingerprinting blocking в **Standard** или **Strict**.
- Перейдите в **Settings** > **Social media blocking** (`brave://settings/socialBlocking`)
    - **Снимите галочки** со всего, что не нужно.
- Перейдите в **Settings** > **Search engine** (`brave://settings/search`)
    - См. поисковые системы
- Перейдите в **Settings** > **Extensions** (`brave://settings/extensions`)
    - **Отключите** всё, кроме "Private Window with Tor".
    - Установите оба метода **Resolve** в "Ask".
- Перейдите в **Settings** > **Wallet** (`brave://settings/wallet`)
    - **Отключите** "Show Brave Wallet icon on toolbar".
    - Установите **Default Ethereum wallet** в "None".
    - Установите **Default Solana wallet** в "None".
- Перейдите в **Settings** > **Privacy and Security** (`brave://settings/privacy`)
    - Оставьте **WebRTC** в "Default".
    - **Отключите** "Allow privacy-preserving product analytics (P3A)".
    - **Отключите** "Automatically send daily usage ping to Brave".
    - Перейдите в "Clear Browsing Data".
        - Выберите **On Exit**.
        - Отметьте все варианты.
        - **Нажмите** "Save".
- Откройте новую вкладку.
- **Нажмите** "Customize" в правом нижнем углу.
    - **Отключите** в Customize Dashboard всё, кроме, возможно, часов.
- Перейдите в **Settings** > **Shields** > **Content filters** (`brave://settings/shields/filters`)
    - Выберите любые дополнительные фильтры блокировки рекламы, которые хотите.
        - Рекомендуются: **CJX's Annoyance List**, **Easylist-Cookie List**, **Fanboy Annoyances List**, **Fanboy Social List**, **Fanboy's Mobile Notifications List** и **uBlock Annoyances List**.
    - Добавьте пользовательские списки фильтров.
        - Добавьте Actually Legitimate URL Shortener Tool, который использует правила из ClearURLs ниже.

    - Добавьте AdGuard URL Tracking Protection, который включает общие правила `$removeparam`.
  - Чтобы сохранить все применённые фильтры, **нажмите** "Save".
- Никогда не включайте Brave Rewards (кнопка должна быть скрыта на всех сайтах).

Дополнения для Brave, которые можно рассмотреть, если нужны дополнительные меры защиты:

- LocalCDN (chrome.google.com)
  - Альтернатива: DecentralEyes (chrome.google.com)
- PrivacyBadger (chrome.google.com)
- NoScript (chrome.google.com)
- Либо ClearURLs (chrome.google.com), **ЛИБО** пользовательский список выше.
- LibRedirect (libredirect.github.io)

На этом всё, и вы должны быть в целом прикрыты. Для полной паранойи можно также просто "Block Scripts", чтобы отключить Javascript. Обратите внимание, что даже отключение Javascript может не защитить вас полностью[1].

Ungoogled-Chromium

Этот браузер считается риском безопасности из-за систематического отставания с исправлениями безопасности[2].

Настоятельно не рекомендуется использовать Ungoogled-Chromium.

Edge

Только Windows:

- Откройте Edge.
- Перейдите в Settings.
- Перейдите в Profiles и убедитесь, что во всех разделах всё отключено (Personal Info, Passwords, Payment info, Profile preferences).
- Перейдите в Privacy, search, and services:
  - Перейдите в Tracking Prevention:
    - Установите Strict или хотя бы Balanced.
    - Настройте постоянное использование Strict в InPrivate Windows.
  - Перейдите в Privacy:
    - Включите отправку Do Not Track.
    - Отключите параметры, позволяющие сайту проверять ваши способы оплаты.
  - Перейдите в Optional Diagnostic Data:

        - Отключите это.
    - Перейдите в Personalize your Web Experience:
        - Отключите это.
    - Перейдите в Security.
        - Отключите всё.
    - Перейдите в Services.
        - Отключите всё.
        - В Address Bar and Search:
            - Отключите всё и смените поисковую систему (см. поисковые системы).
    - Перейдите в Cookies and Sites Permissions:
        - В All Permissions:
            - В Cookies убедитесь, что "Block Third-Party Cookies" отмечено.
            - Заблокируйте всё, кроме:
                - Javascript
                - Images

Включите Application Guard для Edge (только в основной ОС, невозможно внутри ВМ VirtualBox):

Пропустите, если это ВМ.

- Откройте Control Panel.
- Нажмите Programs.
- Нажмите ссылку Turn Windows features on or off.
- Отметьте Windows Defender Application Guard.
- Нажмите OK.
- Нажмите Restart.
- Теперь можно открыть Edge и открыть новое окно "Application Guard".

Для Edge это примерно всё, но вы также можете добавить расширения из Chrome Store, например:

- uBlock Origin (chrome.google.com)
- LocalCDN (chrome.google.com)
    - Альтернатива: DecentralEyes (chrome.google.com)
- PrivacyBadger (chrome.google.com)
- HTTPS Everywhere (chrome.google.com)
- NoScript (chrome.google.com)
- ClearURLs (chrome.google.com)
- LibRedirect (libredirect.github.io)

Safari

Только macOS:

• Откройте Safari.

• Нажмите меню Safari в левом верхнем углу.

• Нажмите Preferences.

  • На вкладке General:

    • Измените New Windows на "Empty Page".

    • Измените New Tabs на "Empty page".

    • Измените Remove History after на "1 day".

    • Измените Remove Download list items на "When Safari Quits" или "When Successful Download".

    • Снимите галочку "Open Safe Files After Downloading".

  • На вкладке Security:

    • Отключите "Warn when visiting a Fraudulent Website" (это отправляет посещаемые вами URL в Google для проверки).

  • На вкладке Privacy:

    • Снимите галочку "Web Advertising".

  • На вкладке Advanced:

    • Отметьте "Show full website address".

Рассмотрите дополнительные меры предосторожности для браузера с включённым JavaScript

На этом всё. К сожалению, вы не сможете добавить расширения, поскольку для них потребуется войти в App Store, чего нельзя делать из ВМ macOS. Опять же, мы не рекомендуем оставаться на Safari в ВМ macOS; лучше перейти на Brave или Firefox.

Firefox

Обычные настройки

• Откройте Firefox.

• На домашней странице Firefox:

  • Нажмите Personalize.

  • Снимите галочки или отключите всё.

• Откройте Settings:

  • Перейдите в Search.

    • Смените поисковую систему (см. поисковые системы).

- Перейдите в Privacy & Security.
    - Установите Custom.
        - Cookies: выберите All Third-Party Cookies.
        - Tracking Content: In all Windows.
        - Отметьте Cryptominers.
        - Отметьте Fingerprinters.
    - Установите постоянную отправку "Do Not Track".
- Перейдите в Logins and Passwords.
    - Снимите галочку "Ask to save logins and passwords for websites".
- Перейдите в Permissions.
    - Location: отметьте блокировку новых запросов.
    - Camera: отметьте блокировку новых запросов.
    - Microphone: отметьте блокировку новых запросов.
    - Notifications: отметьте блокировку новых запросов.
    - Autoplay: выберите Disable Audio and Video.
    - Virtual Reality: отметьте блокировку новых запросов.
    - Отметьте Block Pop-ups.
    - Отметьте Warn when websites try to install add-ons.
- Перейдите в Firefox Data Collection and Use.
    - Отключите всё.
- Перейдите в HTTPS-Only Mode.
    - Включите его во всех окнах.

Расширенные настройки

Рассмотрите Arkenfox/user.js - активно поддерживаемую и очень простую в использовании конфигурацию браузера, которая с помощью "user.js" задаёт все параметры приватности и значения, уменьшающие запись на диск. Ниже мы рекомендуем, если вы не устанавливаете конфигурацию Arkenfox, как минимум задать значения **about:config**. Arkenfox применяет много других настроек, но эти - минимум для вашей защиты при просмотре сайтов. Помните: если ничего не делать и использовать браузер с настройками по умолчанию, он уже будет раскрывать множество идентифицируемых и отслеживаемых характеристик, уникальных для вас. Подробнее о том, почему настройки браузеров по умолчанию небезопасны, см. цифровые отпечатки браузера и устройства.

Эти настройки объясняются в следующих ресурсах в порядке рекомендации, если вы хотите подробнее узнать, что делает каждая настройка:

1. wiki.archlinux.org Archive.org **(наиболее рекомендуется)**

2. proprivacy.com Archive.org

Вот большинство шагов, объединённых из источников выше (некоторые опущены из-за расширений, рекомендованных ниже):

• Перейдите к "about:config" в адресной строке.

• Нажмите Accept the Risk and Continue.

• Безопасные настройки (не должны ничего сломать)

• Отключите Firefox Pocket.

• Установите "extensions.pocket.enabled" в false.

• Отключите всю телеметрию.

• Установите "browser.newtabpage.activity-stream.feeds.telemetry" в false.

• Установите "browser.ping-centre.telemetry" в false.

• Установите "browser.tabs.crashReporting.sendReport" в false.

• Установите "devtools.onboarding.telemetry.logged" в false.

• Установите "toolkit.telemetry.enabled" в false.

• Найдите "toolkit.telemetry.server" и очистите значение.

• Установите "toolkit.telemetry.unified" в false.

• Установите "beacon.enabled" в false.

• Отключите предварительную выборку.

• Установите "network.dns.disablePrefetch" в true.

• Установите "network.dns.disablePrefetchFromHTTPS" в true.

• Установите "network.predictor.enabled" в false.

• Установите "network.predictor.enable-prefetch" в false.

• Установите "network.prefetch-next" в false.

• Установите "browser.urlbar.speculativeConnect.enabled" в false.

• Отключите Javascript в PDF.

• Установите "pdfjs.enableScripting" в false.

• Отключите устаревшее шифрование SSL.

• Установите "security.ssl3.rsa_des_ede3_sha" в false.

• Установите "security.ssl.require_safe_negotiation" в true.

• Отключите Firefox Accounts.

• Установите "identity.fxaccounts.enabled" в false.

• Отключите геолокацию.

• Установите "geo.enabled" в false.

• Отключите веб-уведомления.

• Установите "dom.webnotifications.enabled" в false.

• Отключите уведомления копирования/вставки.

• Установите "dom.event.clipboardevents.enabled" в false.

• Отключите получение состояния микрофона/камеры.

        - Установите "media.navigator.enabled" в false.
    - Включите "Do Not Track".
        - Установите "privacy.donottrackheader.enabled" в true.
    - Отключите SafeBrowsing.
        - Установите "browser.safebrowsing.malware.enabled" в false.
        - Установите "browser.safebrowsing.phishing.enabled" в false.
        - Установите "browser.safebrowsing.downloads.remote.enabled" в false.
- Умеренные настройки (могут сломать некоторые сайты)
    - Отключите WebRTC (это сломает все сайты с видео- или аудиосвязью).
        - Установите "media.peerconnection.enabled" в false.
        - Установите "media.navigator.enabled" в false.
    - Отключите WebGL (это сломает некоторые сайты, активно использующие медиа).
        - Установите "webgl.disabled" в true.
    - Отключите DRM.
        - Установите "media.eme.enabled" в false.
        - Установите "media.gmp-widevinecdm.enabled" в false.
    - Настройте поведение cookie.
        - Установите "network.cookie.cookieBehavior" в 1.
        - Установите "network.http.referer.XOriginPolicy" в 2.
    - Измените политику referer.
        - Установите "network.http.referer.XOriginTrimmingPolicy" в 2.
    - Измените поведение Session Storage.
        - Установите "browser.sessionstore.privacy_level" в 2.
    - Отключите проверки подключения для captive portal.
        - Установите "network.captive-portal-service.enabled" в false.
    - Отключите "Trusted Recursive Resolver".
        - Установите или создайте "network.trr.mode" и задайте значение 5.
- Расширенные настройки (это сломает некоторые сайты)
    - Установите "privacy.resistFingerprinting" в true.
    - Установите "privacy.trackingprotection.fingerprinting.enabled" в true.
    - Установите "privacy.trackingprotection.cryptomining.enabled" в true.
    - Установите "privacy.trackingprotection.enabled" в true.
    - Установите "browser.send_pings" в false.
    - Установите "change privacy.firstparty.isolate" в true.
    - Установите "network.http.referer.XOriginPolicy" в "2" или используйте **Smart Referer** ниже.

    - Установите "change network.cookie.lifetimePolicy" в 2 (это удаляет все cookie после каждой сессии).

Дополнения для установки или рассмотрения

- uBlock Origin (addons.mozilla.org)
- Smart Referer (addons.mozilla.org)
    - Измените значение "network.http.referer.XOriginPolicy" с "2" на "0", чтобы расширение работало. **Отключите** белый список (снимите галочку **Use default whitelist**) и установите **Domain name matching** в **Strict**.
- NoScript (addons.mozilla.org)
    - По умолчанию блокирует **все** скрипты без исключений. Нужно в обычном браузере, если вы хотите блокировать всё выполнение скриптов. Не нужно в Tor Browser.
    - В настройках измените параметры **Default**, отметив всё, кроме "ping", "unrestricted CSS" и "LAN". Это снова включит JavaScript и другие веб-функции, чтобы многие сайты не ломались.
- LibRedirect (libredirect.github.io)
    - Перенаправляет менее приватные сайты, такие как YouTube и Wikipedia, на более приватные открытые альтернативы.
- Skip Redirect (github.com)

Дополнительные ресурсы

Вот ещё два недавних руководства по усилению Firefox:

- chrisx.xyz Archive.org
- ebin.city Archive.org

Сноски

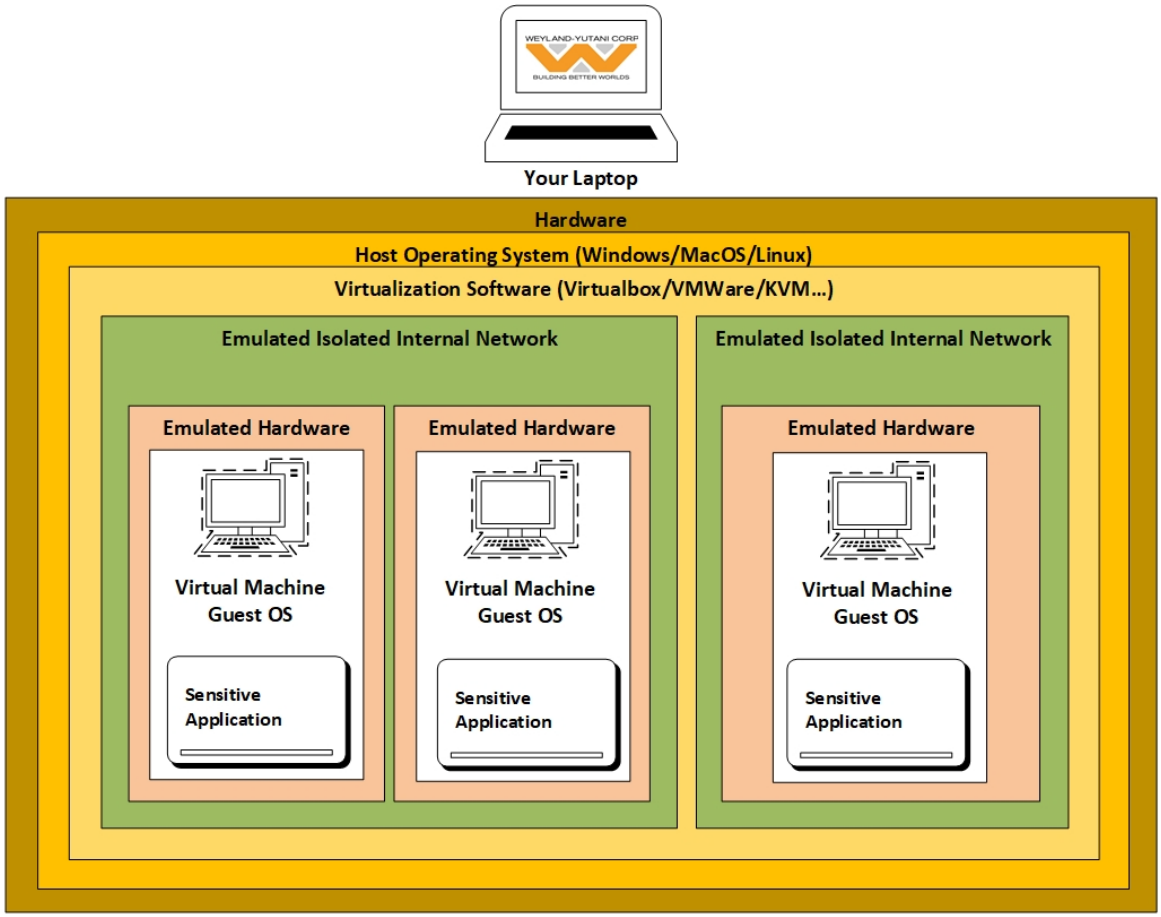
[1] [назад] FingerprintJS, Demo: Disabling JavaScript Won't Save You from Fingerprinting fingerprintjs.com Archive.org
[2] [назад] Duck's pond, Ungoogled-Chromium qua3k.github.io Archive.org

Виртуализация

Итак, вы можете спросить: что такое виртуализация[1]?

В основном это как фильм «Начало», только с компьютерами. На физическом компьютере работают эмулируемые программные компьютеры, называемые виртуальными машинами. При желании можно даже запускать виртуальные машины внутри виртуальных машин, хотя в некоторых случаях для этого понадобится более мощный ноутбук.

Вот небольшая базовая иллюстрация того, что такое виртуализация:



Каждая виртуальная машина - это песочница. Помните: причины их использования в том, чтобы предотвращать следующие риски:

• Снижать локальные утечки данных и упрощать очистку, если что-то пойдёт не так или появится подозрение на компрометацию.

• Уменьшать поверхность атаки вредоносного ПО и эксплойтов: если ваша ВМ скомпрометирована, противнику всё ещё нужно понять, что он находится в ВМ, а затем получить доступ к основной ОС, что не так просто.

• Снижать сетевые утечки данных за счёт возможности принудительно задавать строгие сетевые правила для виртуальных машин при доступе к сети, например пропускать трафик через сеть Tor.

Риски вложенной виртуализации

При вложенной виртуализации поверхность атаки неизбежно больше.

Вот часть сведений об основной системе, которые могут утечь через виртуальную машину:

- Организационно уникальный идентификатор, или OUI, - уникальный идентификатор, назначенный гостевым ВМ VMWare.
- Виртуальные ключи реестра Windows, такие как `ProductID`, могут показывать среду основной машины:
  `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ProductId`
  `XXXXX-123-1234567-12345`
- Драйверы HDD, GPU и мыши могут быть раскрыты через:
  `HKEY_LOCAL_MACHINE\System\CurrentControlSet\`
- Записи реестра покажут, что это виртуальная мышь: `%WINDIR%\system32\drivers\vmmouse.sys`
- Регистры таблиц дескрипторов: stackoverflow.com
  - Поскольку это виртуальная машина, использующая те же ядра CPU, значения дескрипторов смещаются: на CPU есть место только для одного значения каждого идентификатора. Это явный признак, который используется продвинутым вредоносным ПО для обнаружения. Архитекторы вредоносного ПО применяют его, чтобы понять, когда программа запущена в криминалистической среде, например Remnux или Flare VM, популярных инструментах и ОС, которые эксперты используют для анализа вредоносного ПО.
- Гостевые ВМ также косвенно обращаются к тому же оборудованию, что и основная ОС.

См. malwarebytes.com о других методах, которые вредоносное ПО использует для обнаружения виртуализации. Большая часть таких методов предотвращается добавлением некоторых параметров в файл конфигурации ВМ (.vmx). blog.talosintelligence.com

[1] [назад] Wikipedia, Virtualization en.wikipedia.org Wikiless Archive.org

Использование мостов Tor во враждебных средах

В некоторых средах ваши интернет-провайдеры могут пытаться не дать вам получить доступ к Tor. Либо открытый доступ к Tor может быть риском для безопасности.

В таких случаях может понадобиться использовать мосты Tor для подключения к сети Tor (см. документацию Tor 2019.www.torproject.org Archive.org и документацию Whonix whonix.org Archive.org). При возможности также стоит серьёзно рассмотреть запуск собственного моста blog.torproject.org Archive.org, поскольку это сильно помогает уменьшать объём цензуры в мире.

Мосты - это специальные входные узлы Tor, которые не перечислены в публичном каталоге Tor. Некоторые из них работают у людей, запустивших браузерное расширение Snowflake[1], другие - на разных серверах по всему миру. Большинство таких мостов используют тот или иной метод маскировки, называемый obfs4[2].

*Доступно только пользователям настольного Tor: недавно Tor Project сделал доступ к мостам невероятно простым с помощью **Connection Assist**, и теперь во враждебных или цензурируемых регионах это делается автоматически. Просто откройте Tor Browser, и подключение будет настроено под ваши потребности в любой враждебной сети. Раньше под этим абзацем был список вариантов, необходимых для включения и настройки мостов, но теперь это делается автоматически с помощью moat.* Archive.org

Вот определение из руководства Tor Browser[3]: «obfs4 делает трафик Tor похожим на случайный и не даёт цензорам находить мосты сканированием интернета. Мосты obfs4 реже блокируются, чем их предшественники obfs3».

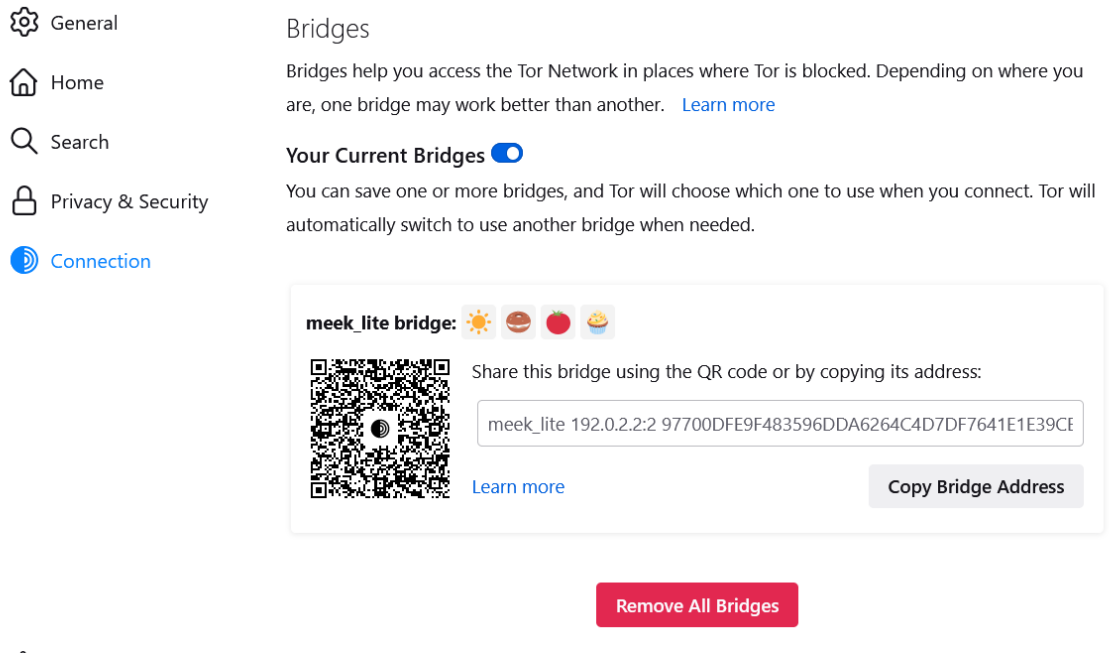
Некоторые мосты называются "Meek" и используют технику "Domain Fronting", при которой ваш клиент Tor (Tails, Tor Browser, Whonix Gateway) подключается к обычному CDN, используемому другими сервисами. Для цензора это будет выглядеть как подключение к обычному сайту, например Microsoft.com. Подробнее см. gitlab.torproject.org.

Согласно определению из их руководства: «транспорты meek создают впечатление, что вы просматриваете крупный сайт, а не используете Tor. meek-azure создаёт впечатление, что вы используете сайт Microsoft». Мосты Snowflake выглядят так, будто ваши соединения - это звонки случайным пользователям интернета. Это разновидность доменного фронтинга ("domain fronting")[4]. Подробное объяснение таких секретных «мостов» см. "domain fronting" по ссылке в предыдущем абзаце.

Наконец, существуют также мосты Snowflake, которые полагаются на пользователей, запускающих расширение snowflake в своём браузере и тем самым становящихся входными узлами. См. snowflake.torproject.org Archive.org.

Сначала следует пройти следующий контрольный список, чтобы убедиться, что вы не можете обойти блокировку Tor (перепроверьте это), и попытаться использовать мосты Tor (bridges.torproject.org Archive.org):

- (Рекомендуется, если заблокировано, но **безопасно**) Попробуйте получить мост obfs4 в параметрах подключения Tor.
- (Рекомендуется, если заблокировано, но **безопасно**) Попробуйте получить мост snowflake в параметрах подключения Tor.
- **(Рекомендуется во враждебной или рискованной среде)** Попробуйте получить мост meek в параметрах подключения Tor; это может быть единственным вариантом, например если вы находитесь в Китае.



(Иллюстрация из настройки мостов Tor Browser)

Если ни один из встроенных методов не работает, можно попробовать получить мост вручную:

• bridges.torproject.org (для моста meek)

• bridges.torproject.org (для моста obfs4)

Этот сайт, очевидно, тоже может быть заблокирован или отслеживаться, поэтому вместо этого, если у вас есть такая возможность, можно попросить кого-то сделать это за вас, если у вас есть доверенный контакт и приложение со сквозным шифрованием.

Наконец, можно также запросить мост по электронной почте на bridges@torproject.org с пустой темой и текстом письма: "get transport obfs4" или "get transport meek". У этого метода есть ограничения: он доступен только с адреса Gmail или Riseup.

• См.: примечание о Riseup Riseup потенциально был скомпрометирован. Используйте его на свой риск.

Будем надеяться, этих мостов хватит, чтобы подключиться даже во враждебной среде.

Если нет, рассмотрите что делать, когда Tor и VPN невозможны?

Сноски

[1] [назад] Tor Project, Project Snowflake snowflake.torproject.org Archive.org
[2] [назад] GitHub, Obfs4 Repository github.com Archive.org
[3] [назад] Tor Browser Manual, Pluggable Transport tb-manual.torproject.org Archive.org
[4] [назад] Wikipedia, Domain Fronting en.wikipedia.org Wikiless Archive.org

Установка и использование настольного Tor Browser

Установка

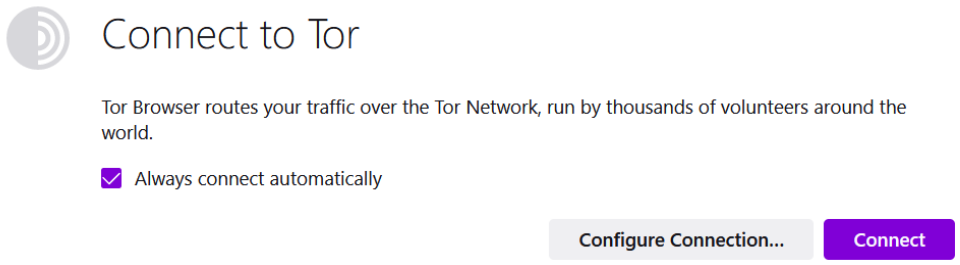
Это применимо к Windows, Linux и macOS.

• Скачайте и установите Tor Browser по инструкциям с torproject.org Archive.org

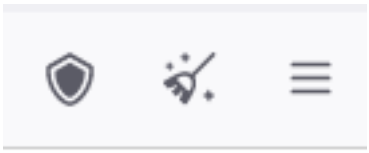
• Откройте Tor Browser.

Использование и меры предосторожности

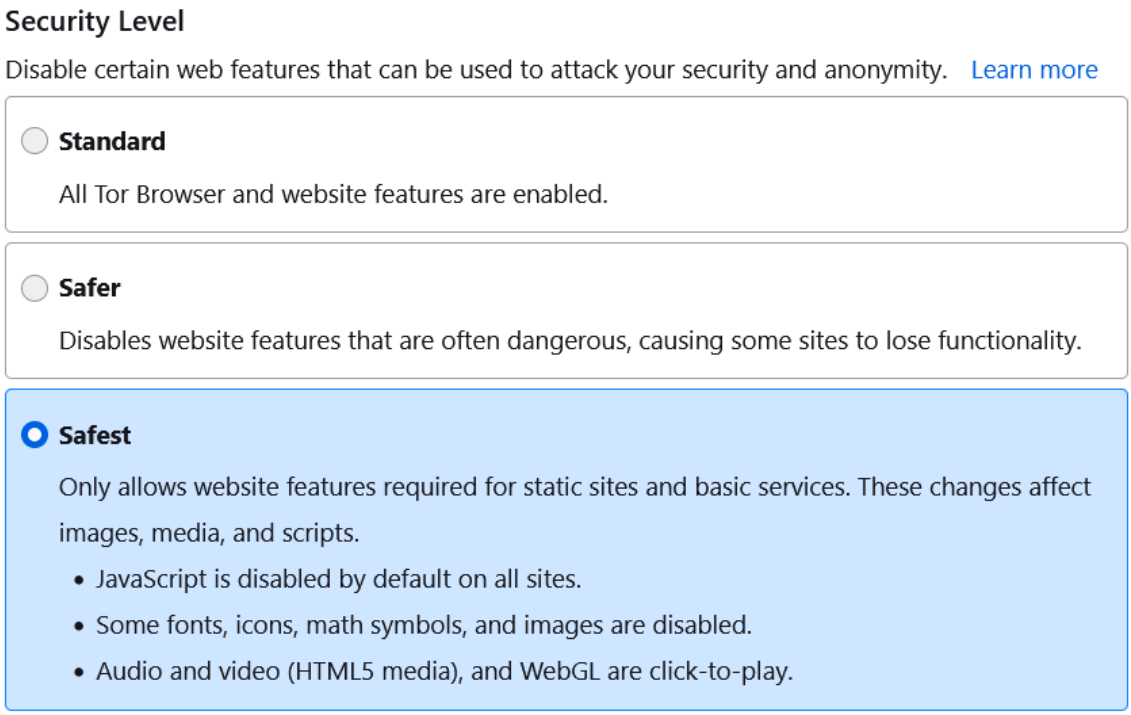
• После открытия Tor Browser вы увидите вариант **Connect**, флажок **Always connect automatically** и кнопку **Configure connection**. Настройки сети Tor находятся там на случай, если вам понадобится настроить мосты для подключения к Tor при проблемах с подключением из-за цензуры или блокировки. Как объясняется здесь: использование мостов Tor во враждебных средах, теперь настольный Tor Browser делает это автоматически.



• Лично мы в случае цензуры или блокировки рекомендовали бы при необходимости использовать мосты Meek-Azure. Мосты Snowflake - как второй вариант.



На этом этапе, ещё до подключения, следует нажать маленький значок щита в правом верхнем углу рядом с адресной строкой и выбрать уровень безопасности (подробности см. tb-manual.torproject.org Archive.org). В основном их три.



• Standard (по умолчанию):
  • Все функции включены, включая JavaScript.
• Safer:
  • JavaScript отключён на сайтах без HTTPS.
  • Некоторые шрифты и символы отключены.
  • Любое воспроизведение медиа работает по принципу "click to play" и по умолчанию отключено.
• Safest:
  • Javascript отключён везде.
  • Некоторые шрифты и символы отключены.
  • Любое воспроизведение медиа работает по принципу "click to play" и по умолчанию отключено.

Мы рекомендуем уровень "Safest" по умолчанию. Уровень "Safer" следует включать, если вы считаете, что вам нужен доступ к сайту, который не работает без JavaScript. Режим Safest, скорее всего, сломает многие сайты, активно полагающиеся на JavaScript.

Если вы особенно параноидальны, используйте уровень "Safest" по умолчанию и рассматривайте понижение до Safer, если сайт непригоден для использования из-за блокировки Javascript.

Необязательно и не рекомендуется Tor Project: если вы не используете уровень "Safest", мы отойдём от некоторых рекомендаций, но согласимся с другими, например с проектом Tails и другими[1], и фактически порекомендуем два расширения к стандартному Tor Browser:

• uBlock Origin (как в Tails), оставив расширение с настройками по умолчанию:
  • Перейдите на addons.mozilla.org внутри Tor Browser и установите расширение.

- LibRedirect: это очень практично, если вы используете режим "Safest", поскольку экземплярам Invidious не нужен JavaScript.
    - Перейдите на libredirect.github.io внутри Tor Browser и установите расширение.

Стоит помнить, что даже агентства из трёх букв рекомендуют своим внутренним пользователям блокировать рекламу для повышения безопасности[2].

Если вы не выбрали указанные выше **личные и официально не рекомендованные варианты**, уровень Safer всё равно следует использовать с некоторыми дополнительными мерами предосторожности при работе с отдельными сайтами: см. дополнительные меры предосторожности для браузера с включённым JavaScript.

Теперь вы действительно закончили и можете анонимно просматривать интернет со своего настольного устройства.

Сноски

[1] [назад] GitLab, Tor Browser Issues, Add uBlock Origin to the Tor Browser gitlab.torproject.org Archive.org
[2] [назад] Vice, The NSA and CIA Use Ad Blockers Because Online Advertising Is So Dangerous vice.com Archive.org

Анонимные платежи криптовалютой

Есть много сервисов, которыми вы можете захотеть пользоваться (VPS-хостинг, почтовый хостинг, доменные имена...), но которые требуют какой-либо оплаты.

Как уже неоднократно упоминалось в этом руководстве, мы настоятельно рекомендуем использовать сервисы, принимающие наличные, которые можно анонимно отправить почтой, или Monero, который можно купить и использовать напрямую и безопасно.

• Но что, если нужный вам сервис не принимает Monero, зато принимает более массовую криптовалюту, например Bitcoin (BTC) или Ethereum (ETH)?

Bitcoin и другие «массовые криптовалюты» совсем не анонимны (помните ваши криптовалютные транзакции), и вам никогда не следует, например, покупать Bitcoin на бирже, а затем напрямую использовать его для анонимной покупки сервисов. Это не сработает, и транзакцию легко отследить.

• **Держитесь подальше от так называемых «приватных» миксеров, тумблеров и coinjoin-сервисов.** Вам может казаться, что это хорошая идея, но они не только бесполезны с криптовалютами вроде BTC/ETH/LTC, но и опасны. Они получают контроль над вашими монетами. Используйте Monero, чтобы анонимизировать криптовалюту. Не используйте обычную биржу с KYC для покупки или продажи Monero, например Kraken, поскольку сведения о ваших покупках и выводах, то есть о предполагаемом использовании, сохраняются на бирже. Вместо этого используйте P2P-биржу без требования KYC, например из списка на kycnot.me.

• **См. предупреждение о специальных тумблерах, миксерах, coinjoin-кошельках и сервисах для приватности.**

Вариант анонимного использования Bitcoin

Несмотря на это, Bitcoin можно безопасно анонимизировать с помощью совместных транзакций без передачи хранения третьей стороне и инструментов трат, сохраняющих приватность. Это возможно благодаря протоколу ZeroLink и реализации Whirlpool, у которой есть два клиента, использующие его и предоставляющие необходимые инструменты трат, описанные ниже. Итак, как это сделать? На самом деле довольно просто:

1. Купите Bitcoin на бирже без KYC, например найденной на kycnot.me.
2. Создайте кошелёк в Samourai Wallet (Android) или Sparrow Wallet (настольный компьютер). Оба используют протокол Whirlpool, чтобы дать пользователю приватность будущих действий в цепочке Bitcoin.
3. Внесите монеты в кошелёк и следуйте соответствующим инструкциям (Samourai, Sparrow), чтобы убрать их исторические связи.
4. Средства следует тратить только из учётной записи Postmix, поскольку именно в ней находятся монеты, получившие анонимность через Whirlpool.

• **При использовании Bitcoin следует запускать собственный узел и всегда подключать к нему свой кошелёк. Для этого не нужно покупать отдельное оборудование; это также просто сделать через сеть Tor.**

Вариант анонимного использования Monero

1. Купите Monero на бирже без KYC, например найденной на kycnot.me.
2. Создайте кошелёк Monero на одной из своих анонимизированных ВМ, например в Whonix Workstation, где графический кошелёк Monero уже включён, или используйте Monero GUI wallet с getmonero.org в других ОС.
3. Переведите Monero из кошелька, где вы его купили, в кошелёк на своей ВМ. Мы не можем достаточно подчеркнуть, насколько важно иметь два отдельных кошелька для этого процесса, даже при работе с Monero.
4. На той же ВМ, например снова в Whonix Workstation, создайте Bitcoin-кошелёк; он тоже нативно предоставляется в Whonix Workstation.
5. Из анонимизированного браузера, например Tor Browser, используйте сервис обмена без KYC (Know Your Customer) (см. сервисы обмена криптовалюты без регистрации и KYC), конвертируйте Monero в BTC и переведите их на BTC-кошелёк, который находится на вашей анонимизированной ВМ.
6. Теперь у вас должен быть анонимизированный Bitcoin-кошелёк, который можно использовать для покупки сервисов, не принимающих Monero.

Никогда не обращайтесь к этому кошельку из неанонимизированной среды. Всегда используйте хорошо продуманную операционную безопасность при BTC-транзакциях. Помните, что их можно отследить обратно к вам.

Происхождение этих BTC нельзя связать с вашей реальной личностью благодаря использованию Monero, **если только Monero не будет сломан**, либо если вы не объединяете выходы после трат у разных продавцов. Рекомендуется использовать кошельки, сохраняющие приватность, из раздела Bitcoin. Пожалуйста, прочитайте предупреждение о Monero.

О Zcash: раньше этот раздел включал использование Zcash, но оно было удалено с учётом более новой и точной информации.

Предупреждение о специальных тумблерах, миксерах, coinjoin-кошельках и сервисах для приватности

Централизованные «приватные» тумблеры, миксеры и coinjoin-сервисы не рекомендуются, поскольку они не обеспечивают анонимность таким способом, который действительно отвязывает выход от его истории. Вот несколько источников по этой проблеме:

• Mixing detection on Bitcoin transactions using statistical patterns. Archive.org
• An Analysis Of Bitcoin Laundry Services Archive.org
• Mixing Strategies in Cryptocurrencies and An Alternative Implementation Archive.org

Такое смешивание BTC должно предотвратить анализ цепочки для будущих транзакций. Однако оно *не* скроет прошлые транзакции или сам факт покупки BTC на бирже с KYC. Вместо этого мы рекомендуем использовать Bitcoin-кошельки с Whirlpool или Monero (предпочтительно).

При конвертации из BTC в Monero

Теперь, как часть любого процесса выше, если вы хотите конвертировать BTC обратно в Monero, мы рекомендуем не использовать сервис обмена, а вместо этого использовать новый инструмент Monero Atomic Swap Tool: unstoppableswap.net. Это позволит избежать лишних комиссий и посредников при использовании коммерческого сервиса обмена. Сайт самодостаточен и содержит подробные инструкции для всех ОС.

Рекомендуемые VPS-хостинг-провайдеры

Мы будем рекомендовать только провайдеров, принимающих Monero в качестве оплаты; вот мой личный короткий список:

• **Njalla njal.la (мой личный фаворит, но довольно дорогой; рекомендуется PrivacyGuides.org).**

• **1984.is (мой второй фаворит, значительно дешевле) 1984.is.**

• Можно рассмотреть на свой риск (не проверено):

  • cryptoho.st (предупреждение: это может нарушать их условия обслуживания, поскольку при регистрации они требуют личную идентификацию)

  • privex.io

  • cockbox.org (предупреждение: этот провайдер довольно провокационный и может кого-то оскорбить)

Также рассмотрите эти списки:

• Tor Project: community.torproject.org Archive.org

• PrivacyGuides.org: privacyguides.org Archive.org

Наконец, можно выбрать один вариант на свой риск из списка здесь, где принимают Monero: getmonero.org Archive.org

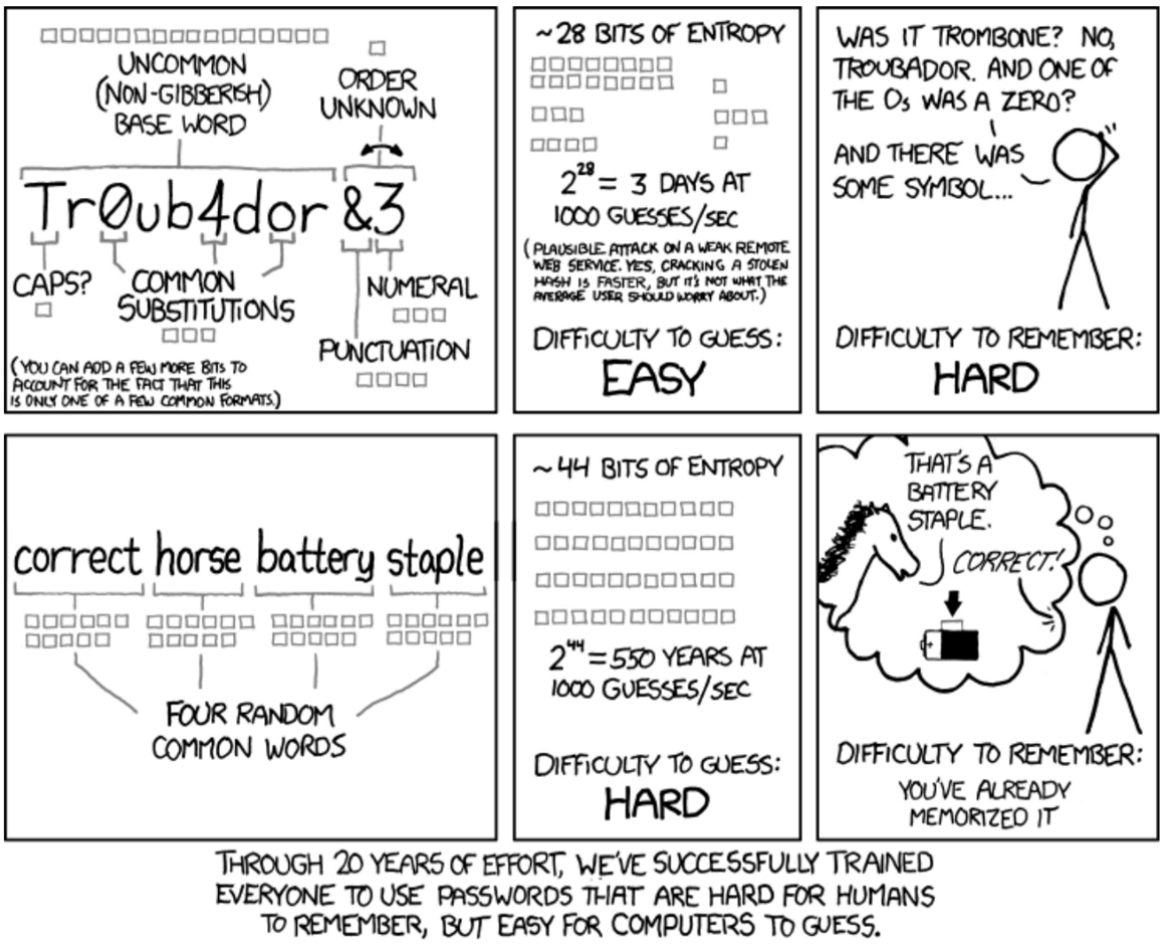
Пожалуйста, прочитайте предупреждение о Monero.

Если сервис не принимает Monero, но принимает BTC, рассмотрите следующее приложение: анонимная онлайн-оплата с помощью BTC.

Рекомендации по паролям и парольным фразам

Моё мнение, совпадающее с мнением многих[1][2][3][4][5][6], состоит в том, что парольные фразы в целом лучше паролей. Поэтому вместо размышлений о более хороших паролях лучше вообще забыть о них и использовать парольные фразы, когда это возможно. Либо просто используйте менеджер паролей с очень длинными паролями, например KeePassXC, предпочтительный менеджер паролей в этом руководстве.

Хорошо известный XKCD ниже xkcd.com Archive.org всё ещё актуален, несмотря на споры (см. explainxkcd.com Archive.org). Да, он уже довольно старый, немного устарел и может быть неверно истолкован. Но в целом он всё ещё верен и остаётся хорошим аргументом в пользу парольных фраз вместо паролей.



(Иллюстрация Randall Munroe, xkcd.com, лицензия CC BY-NC 2.5)

Вот несколько рекомендаций на основе Wikipedia[7]:

• Достаточная длина, чтобы фразу было трудно угадать: обычно четыре слова - минимум, пять или больше лучше.

• Не известная цитата из литературы, священных книг и т. п.

• Трудно угадываемая интуитивно даже человеком, хорошо знающим пользователя.

• Лёгкая для запоминания и точного ввода.

• Для лучшей безопасности можно применить любое легко запоминаемое кодирование на уровне самого пользователя.

• Не используется повторно между сайтами, приложениями и другими источниками.

• Не используйте только «обычные слова», например "horse" или "correct".

Вот хороший сайт с примерами и рекомендациями: useapassphrase.com

Посмотрите это содержательное видео Computerphile: youtube.com Invidious

По возможности используйте разные парольные фразы для каждого сервиса или устройства. Не упрощайте противнику доступ ко всем вашим сведениям только потому, что вы использовали одну и ту же парольную фразу везде.

Вы можете спросить: как? Просто: используйте менеджер паролей, например рекомендуемый KeePassXC. Помните только парольную фразу для разблокировки базы данных, а всё остальное храните в базе KeePassXC. В KeePassXC можно создавать крайне длинные пароли (30+ случайных символов) для каждого отдельного сервиса.

Поисковые системы

Какую поисковую систему выбрать в ваших ВМ?

Мы не будем уходить в подробности. Просто выберите одну из PrivacyGuides.org (privacyguides.org Archive.org).

Лично мои фавориты:

• duckduckgo.com (потому что можно легко использовать операторы вроде "!g" для Google или "!b" для Bing)

• startpage.com

• Экземпляры SearX (searx.me), перечисленные здесь: searx.space

Обратите внимание, что у некоторых из них есть удобный адрес ".onion":

• DuckDuckGo: duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

В итоге мы часто оставались недовольны результатами обеих этих поисковых систем и всё равно оказывались в Bing или Google.

Противодействие криминалистической лингвистике

Обратите внимание: эта информация взята и адаптирована из поста на Dread, доступного здесь: dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion

Плагиат не предполагается; были внесены важные адаптации и изменения, чтобы улучшить исходный пост разными способами.

Введение

Стилометрия - это наш личный и уникальный стиль письма. Кем бы вы ни были, у вас есть уникальный, пригодный для снятия цифрового отпечатка и отслеживаемый стиль письма. Это известно уже давно, и на этом принципе построена отрасль криминалистики: криминалистическая лингвистика. В этой области конкретное название криминалистической лингвистики, применяемой к интернет-преступлениям, - «письменный отпечаток» ("Writeprint"). Письменный отпечаток в первую очередь стремится установить авторство в интернете, сравнивая текст подозреваемого с известным набором инвариантных для автора, обычно написанных текстов; даже без текстов для сравнения этот криминалистический метод может дать личные сведения об авторе, например пол, возраст и черты личности.

Что ищет противник, изучая ваше письмо?

1. Лексические признаки: анализ выбора слов.
2. Синтаксические признаки: анализ стиля письма, структуры предложений, пунктуации и расстановки дефисов.
3. Структурные признаки: анализ структуры и организации письма.
4. Контекстно-значимые слова: анализ значимой для контекста лексики, например сокращений.
5. Идиосинкратические признаки: анализ грамматических ошибок; это самый важный фактор, поскольку он даёт сравнительно высокую точность при установлении автора.

Примеры

Вы можете думать, что противник не обращает на это внимания. Подумайте ещё раз. Было несколько случаев, где противники, например правоохранительные органы, использовали методы письменного отпечатка, чтобы помочь поймать и осудить людей. Вот несколько примеров:

• Дело OxyMonster (arstechnica.com Archive.org):

  • Открытые данные показали, что у Vallerius (он же OxyMonster) есть аккаунты Instagram и Twitter. Агенты сравнили стиль письма "OxyMonster" на форуме Dream Market, где он был старшим модератором, со стилем Vallerius в его публичных аккаунтах Instagram и Twitter. Они обнаружили много сходств в использовании слов и пунктуации, включая слово "cheers"; двойные восклицательные знаки; частое использование кавычек; и периодические публикации на французском.

Не используйте для чувствительных действий тот же стиль письма, что и для обычных действий. В частности, внимательно следите за использованием привычных фраз и пунктуации. Также, как дополнительное замечание: ограничьте объём материалов, которые противник может использовать как текст для сравнения. Вы ведь не хотите попасть в неприятности из-за политического поста в Twitter или поста на Reddit, сделанного много лет назад?

• Вот ещё один пример из книги American Kingpin о том, как агент DEA исследовал стиль письма DPR (Dread Pirate Roberts, он же Ross Ulbricht, основатель darknet-рынка Silk Road) с необычной стороны. Во-первых, Ross Ulbricht часто использовал слово "epic", что указывало на вероятную молодость. Он также использовал в письме улыбающиеся смайлики, но никогда не ставил дефис в качестве носа, записывая их как ":)", а не старомодное ":-)". Однако больше всего выделялось то, что вместо "yes" или "yeah" на форумах сайта Ulbricht всегда писал "yea".

Обращайте внимание на мелочи, которые могут сложиться в картину. Если обычно вы отвечаете людям "ok", возможно, для чувствительных действий стоит отвечать "okay". НИКОГДА не используйте слова или фразы из чувствительных действий (даже если они не в публичном посте) в обычных целях, и наоборот. Ross Ulbricht использовал "frosty" как имя серверов Silk Road и для своего аккаунта YouTube, что помогло убедить правоохранителей, что Dread Pirate Roberts действительно был Ross Ulbricht.

Как противодействовать усилиям противника

1. Сократите объём текста для сравнения, который противники могут сопоставлять с вами. Это связано с небольшим онлайн-следом для обычных действий.
2. Используйте текстовый процессор, например LibreWriter, чтобы исправлять грамматические и орфографические ошибки, которые вы регулярно допускаете.
3. Сократите или измените идиомы, которые используете при чувствительных действиях.
4. Поймите, как ваша личность влияет на стиль письма: ваш псевдоним моложе? Старше? Более образован? Менее образован? Если ваша личность старше, возможно, стоит писать в стиле, более похожем на J. R. R. Tolkien.
5. Обращайте внимание на то, как сленг и орфография могут вас идентифицировать. Если вы из UK, следует говорить "maths", а если из US - "math". Неважно, как вы произносите "maths"; важно, что это можно использовать для профилирования. Это также относится к сленгу, поскольку во многих регионах есть собственный, очень специфичный сленг. Например, не стоит просить человека из USA дать вам "rubber" и ожидать, что он даст "eraser".
6. Обращайте внимание на использование эмотиконов и эмодзи. В предыдущем примере агент DEA смог сделать правильное предположение, что Ulbricht, вероятно, молод, потому что он не использовал дефис в улыбающемся эмотиконе.
7. Обращайте внимание на структуру письма. Ставите ли вы два пробела после точки? Постоянно ли используете скобки? Используете ли оксфордскую запятую?
8. Подумайте, какие символы используете в письме. Используете ли €, £ или $? Пишете ли даты как "dd-mm-yyyy" или "mm-dd-yyyy"? Время как "08:00 pm" или "20:00"?

Что разные лингвистические выборы могут сказать о вас

Эмотиконы

1. Русские, например, используют ")" вместо ":-)" или ":)" для выражения улыбки.
2. Скандинавы используют "=)" вместо ":-)" или ":)" для улыбки.
3. Молодые люди обычно не используют дефис в улыбающихся эмотиконах и просто пишут ":)".

Структурные признаки

1. Два пробела после точки создают впечатление, что вы довольно старше, потому что так учили печатать людей, осваивавших печатные машинки.
2. В США числа записывают с запятыми между разрядами слева от десятичной части и с точками справа от неё. Это отличается от того, как числа записывает остальной мир.

US: 1,000.00$

```
Europe: 1.000,00€
```

Орфография, сленг и символы

1. Очевидно, люди в разных странах используют разный сленг. Это ещё заметнее, когда вы используете сленг, плохо известный в других местах, например человек из UK упоминает "headmaster", тогда как в других странах говорят "principal".
2. Орфография - ещё один важный фактор, похожий на сленг, но контролировать её сложнее. Если вы хотите притвориться, что вы из USA, но на самом деле живёте в Australia, одного написания "colour" как color достаточно, чтобы люди поняли, что что-то не так.
3. Некоторые люди также пишут слова особым образом, не связанным с регионом: например, вы можете писать "ax" как "axe" или наоборот.
4. Конечно, символы на вашей клавиатуре могут выдать много сведений, например £ или $.

Техники предотвращения стилометрического отпечатка

Вот несколько техник в порядке применения:

Проверка орфографии и грамматики

Это помогает предотвратить часть идентификации по вашим орфографическим и грамматическим ошибкам.

Офлайн с помощью текстового процессора

Используйте текстовый процессор, например LibreWriter, и функции проверки орфографии и грамматики, чтобы исправлять набранные ошибки.

Онлайн с помощью онлайн-сервиса

Если у вас нет доступного текстового процессора или вы не хотите им пользоваться, можно использовать онлайн-сервис проверки орфографии и грамматики, например Grammarly; для него требуется электронная почта и создание учётной записи.

Техника перевода

Отказ от ответственности: исследование, архивированное здесь: web.archive.org, похоже, указывает, что техника перевода неэффективна для предотвращения стилометрии. Этот шаг может быть бесполезен.

После исправления орфографии и грамматики используйте сайт или программное обеспечение, например Google Translate (или более приватную версию simplytranslate.org), чтобы перевести текст между несколькими разными языками, прежде чем переводить обратно на исходный язык. Такие переводы туда и обратно изменят ваши сообщения и усложнят снятие цифрового отпечатка.

Поиск и замена

Наконец, по желанию добавьте немного шума, намеренно внося в сообщения некоторые ошибки.

Сначала определите список слов, которые вы часто не пишете неправильно, например "grammatical", "symbol" и "pronounced" (этот список должен включать больше слов). **Не используйте для этого автоматическую замену AutoCorrect, поскольку она может исправить там, где это не имеет смысла.** Вместо этого используйте Search and Replace и делайте это вручную для каждого слова. **Не используйте "Replace All" и проверяйте каждое изменение.** Это лишь первый шаг для создания дезинформации против лингвистического цифрового отпечатка.

Затем найдите список слов, которые вы часто используете в письме. Допустим, мы любим использовать сокращения, когда пишем, и часто используем слова вроде "can't", "don't", "shouldn't", "won't" или "let's". Тогда можно открыть LibreWriter и использовать "Search and Replace", чтобы заменить все сокращения полными формами ("can't" > "cannot", "don't" > "do not", "shouldn't" > "should not", "won't" > "will not", "let's" > "let us"). Это может заметно изменить ваше письмо и то, как люди, а главное ваши противники, воспринимают вас. Можно менять большинство слов на другие; например, "huge" на "large". Главное - убедиться, что эти слова подходят вашей личности.

Теперь подумайте об изменении выбора слов под географическое место. Возможно, вы живёте в US, но хотите создать впечатление, что ваша личность из UK. Например, можно использовать орфографию и лексику, привязанную к месту. Это рискованно, и одна ошибка может всё выдать.

Сначала нужно решить, какое местоположение вы хотите создать для своей личности. Вот пример, как создать впечатление, что вы из US или UK. Для начала нужно понять кое-что о том, «откуда» ваша личность; не притворяйтесь, что вы из UK, если не знаете о нём ничего, кроме факта его существования.

После выбора хорошего местоположения для личности изучите различия в языке между двумя вариантами, в данном случае между британским и американским английским. Благодаря интернету это довольно легко: можно найти страницы Wikipedia, удобно показывающие региональные различия языка между двумя странами. Обратите внимание, как пишутся отдельные слова ("metre" > "meter") и какие слова заменяются друг другом ("boot" > "trunk"). Теперь, когда у вас есть список взаимозаменяемых слов и список различий в написании, используйте "Search and Replace" в редакторе и меняйте слова вроде "colour" на "color", а "lorry" на "truck". **Ещё раз: не используйте AutoCorrect или "Replace All", поскольку некоторые изменения могут не иметь смысла. Проверяйте каждую предложенную замену. Например, если использовать AutoCorrect или "Replace all" для слова "boot" и заменить его на "trunk", это будет совершенно логично в контексте автомобилей, но бессмысленно в контексте обуви.**

Финальный совет

Понимайте, что при чувствительных действиях вам нужно постоянно думать о том, что и как вы набираете.

Понимайте, что изменение стиля письма для таких целей в конечном счёте может изменить ваш базовый стиль письма, иронично сделав ваше письмо отслеживаемым на более длинных промежутках времени.

После написания чего-либо вычитывайте себя хотя бы один раз, чтобы убедиться, что в процессе не допустили ошибок. Доверяй себе, но всё равно проверяй.

Можно также рассмотреть использование чего-то вроде AnonyMouth web.archive.org Archive.org - инструмента для анонимизации документов, разработанного PSAL, Privacy, Security, and Automation Laboratory Университета Drexel psal.cs.drexel.edu Archive.org. Такие инструменты могут оказаться бесценными.

Дополнительные ссылки

- seirdy.one Archive.org: Stylometric fingerprinting redux
- whonix.org Archive.org: документация Whonix о стилометрии.
- wikipedia.org Wikiless Archive.org: даёт краткое изложение основ криминалистической лингвистики, не слишком информативное.
- wikipedia.org Wikiless Archive.org: даёт краткое и информативное изложение криминалистической лингвистики применительно к интернет-расследованиям.
- wikipedia.org Wikiless Archive.org: даёт краткий обзор стилометрии.
- wikipedia.org Wikiless Archive.org: рекомендуем прочитать, довольно информативно.
- wikipedia.org Wikiless Archive.org: тоже прочитайте, если вам интересна эта тема.

- wikipedia.org Wikiless Archive.org: это менее важно, если вы используете переводчик, но если не используете переводчик для общения на форумах не на родном языке, стоит быстро ознакомиться.
- wikipedia.org Wikiless Archive.org: читайте только если тема вам интересна.
- regmedia.co.uk Archive.org: объясняет, как власти использовали криминалистическую лингвистику, чтобы помочь арестовать OxyMonster (страницы 13-14).
- wikipedia.org Wikiless Archive.org: возможно, его IQ был 167, но поймали его в основном благодаря криминалистической лингвистике.
- i.blackhat.com Archive.org: объясняет, как стиль письма может использоваться для отслеживания; мы очень рекомендуем прочитать эти слайды или посмотреть сопутствующую презентацию на YouTube.
- media.defcon.org Archive.org: объясняет, как стиль письма может использоваться для отслеживания; мы очень рекомендуем прочитать эти слайды или посмотреть сопутствующую презентацию на YouTube, это довольно похоже на предыдущую презентацию.
- i.blackhat.com Archive.org: рассматривает, как потенциально распознавать обман через интернет, и предлагает контрольный список для оценки доверия к человеку. Мы советуем прочитать слайды или посмотреть презентацию на YouTube.

Дополнительные меры предосторожности для браузера с включённым JavaScript

Чтобы избегать цифровых отпечатков браузера и пользователя через JavaScript, но при этом оставить JavaScript включённым, следует соблюдать дополнительные меры безопасности хотя бы на некоторых сайтах:

Эти рекомендации похожи на рекомендации в начале руководства и особенно применимы для отдельных сайтов. В основном рекомендация состоит в использовании приватных фронтенд-экземпляров и альтернативных сервисов для разных служб:

- Для ссылок YouTube используйте экземпляр Invidious (github.com Archive.org)
    - Мы рекомендуем yewtu.be
- Для ссылок Twitter используйте экземпляр Nitter (github.com Archive.org)
    - Мы рекомендуем nitter.net
- Для ссылок Wikipedia используйте экземпляр Wikiless (codeberg.org Archive.org)
- Для Reddit используйте экземпляр LibReddit (github.com Archive.org)
- Для карт рассмотрите openstreetmap.org
- Для перевода рассмотрите SimplyTranslate на simplytranslate.org
- Для поисковых систем используйте поисковые системы с упором на приватность, например:
    - StartPage: startpage.com
    - DuckDuckGo: duckduckgo.com
    - Экземпляры SearX (searx.me): список доступен здесь: searx.space

(Необязательно) Рассмотрите использование расширения libredirect.github.io Archive.org, чтобы автоматизировать использование перечисленных выше сервисов.

Сравнение версий руководства

Если вы хотите сравнить более старую версию PDF с более новой, рассмотрите эти онлайн-инструменты. Обратите внимание, что мы не одобряем эти инструменты с точки зрения их политик конфиденциальности, но это не должно иметь значения, поскольку эти PDF публичны:

• tools.pdf24.org

• products.aspose.app

• draftable.com

Обмен криптовалюты без регистрации и KYC

Обычный обмен криптовалюты

Для BTC в Monero переходите к следующему разделу. Не используйте сервисы обмена для BTC в Monero.

Вот небольшой список сервисов обмена криптовалюты без KYC; помните, что у всех есть стоимость и комиссии:

• sideshift.ai

• bisq.network

• Kilo Swap (скрытый onion-сервис):
mlyusr6htlxsyc7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion

Рассмотрите kycnot.me - открытый проект со списком бирж и сервисов обмена без KYC (репозиторий: codeberg.org).

Только BTC в Monero

Не используйте никакой сервис обмена, используйте их функцию Atomic Swap. См. этот инструмент Monero Atomic Swap Tool: unstoppableswap.net.

Это позволит избежать лишних комиссий и посредников при использовании коммерческого сервиса обмена. Сайт самодостаточен и содержит подробные инструкции для всех ОС.

Установка кошелька Zcash

Помните: это следует делать только в безопасной среде, например в ВМ за Whonix Gateway.

Debian 11 VM

• Загрузите Debian ВМ.

• Откройте браузер.

• Перейдите на packages.debian.org и скачайте с одного из перечисленных зеркал.

• Перейдите на packages.debian.org и скачайте с одного из перечисленных зеркал.

• Перейдите на сайт ZecWallet Lite, чтобы скачать последний DEB-пакет zecwallet.co (для удобства смените каталог загрузки на /home/user).

• Откройте окно Terminal и выполните следующие команды, при необходимости с обновлённой скачанной версией:

  • `sudo dpkg -i ./libindicator3-7_0.5.0-4_amd64.deb`

  • `sudo dpkg -i ./libappindicator3-1_0.4.92-7_amd64.deb`

  • `sudo dpkg -i ./Zecwallet_Lite_1.7.5_amd64.deb`

• Нажмите меню в левом верхнем углу, найдите и запустите ZecWallet Lite.

Ubuntu 20.04/21.04/21.10 VM

• Загрузите Ubuntu ВМ.

• Откройте браузер.

• Перейдите на сайт ZecWallet Lite, чтобы скачать последний DEB-пакет zecwallet.co

• Откройте окно Terminal.

• Перейдите в каталог загрузок и выполните следующую команду, при необходимости с обновлённой скачанной версией, например: `sudo apt install ./Zecwallet_Lite_1.7.5_amd64.deb`

• Нажмите меню в левом верхнем углу, найдите и запустите ZecWallet Lite.

Windows 10/11 VM

• Загрузите Windows ВМ.

• Откройте браузер.

• Перейдите на zecwallet.co

• Скачайте и установите последний установщик Windows.

• Запустите ZecWallet Lite.

Whonix Workstation 16 VM

• Загрузите Whonix Workstation ВМ.

• Откройте Tor Browser.

• Перейдите на packages.debian.org и скачайте с одного из перечисленных зеркал.

• Перейдите на packages.debian.org и скачайте с одного из перечисленных зеркал.

• Перейдите на сайт ZecWallet Lite, чтобы скачать последний DEB-пакет zecwallet.co (для удобства смените каталог загрузки на /home/user).

• Откройте окно Terminal и выполните следующие команды, при необходимости с обновлённой скачанной версией:

  • `sudo dpkg -i ./libindicator3-7_0.5.0-4_amd64.deb`

  • `sudo dpkg -i ./libappindicator3-1_0.4.92-7_amd64.deb`

  • `sudo dpkg -i ./Zecwallet_Lite_1.7.5_amd64.deb`

• Нажмите меню в левом верхнем углу, перейдите в Development и запустите ZecWallet Lite.

Контрольный список перед передачей сведений

Вот контрольный список того, что нужно проверить перед передачей сведений кому-либо:

• Проверьте файлы на метаданные: см. аудит метаданных

• Проверьте файлы на вредоносное содержимое: см. проверка файлов на вредоносное ПО

• Проверьте файлы на водяные метки: см. водяные метки

• Проверьте любой текст на возможный криминалистический анализ: см. противодействие криминалистической лингвистике

• Посмотрите эту часть документации Whonix: whonix.org Archive.org

• Тщательно оцените потенциальные последствия и риски передачи любых чувствительных сведений для вас и других людей: юридические, этические и моральные. Помните... Не творите зло. Законное не обязательно является хорошим.

После подготовки файлов и удаления всего, что вы не хотите оставлять, перепроверьте их и даже проверьте в третий раз. Затем можно рассмотреть передачу их организации, например прессе или кому-то ещё.

Предупреждение о Monero

Сначала посмотрите это короткое вводное видео о Monero: youtube.com Invidious

Анонимность Monero зависит от его криптографических алгоритмов. Если вы используете Monero с биржи с KYC, сегодня можно быть почти уверенным в безопасности. Но в долгосрочном будущем это может быть не так, если алгоритмы Monero когда-либо будут сломаны[8], например квантовыми вычислениями. Учитывайте, что нормы KYC могут заставлять операторов, например криптовалютные биржи, хранить ваши финансовые записи до 10 лет, а значит вам также нужно, чтобы алгоритмы Monero не были сломаны в следующие 10 лет.

Для дополнительных подробностей можно посмотреть это содержательное видео: youtube.com Invidious

Также рассмотрите чтение: Privacy Limitations in Anonymity Networks with Monero Archive.org

Используйте это на свой риск. Отправка наличных платежей провайдерам через почту всегда является лучшим решением, когда это возможно.

Ресурсы по моделированию угроз

Вот разные ресурсы по моделированию угроз, если вы хотите углубиться в эту тему.

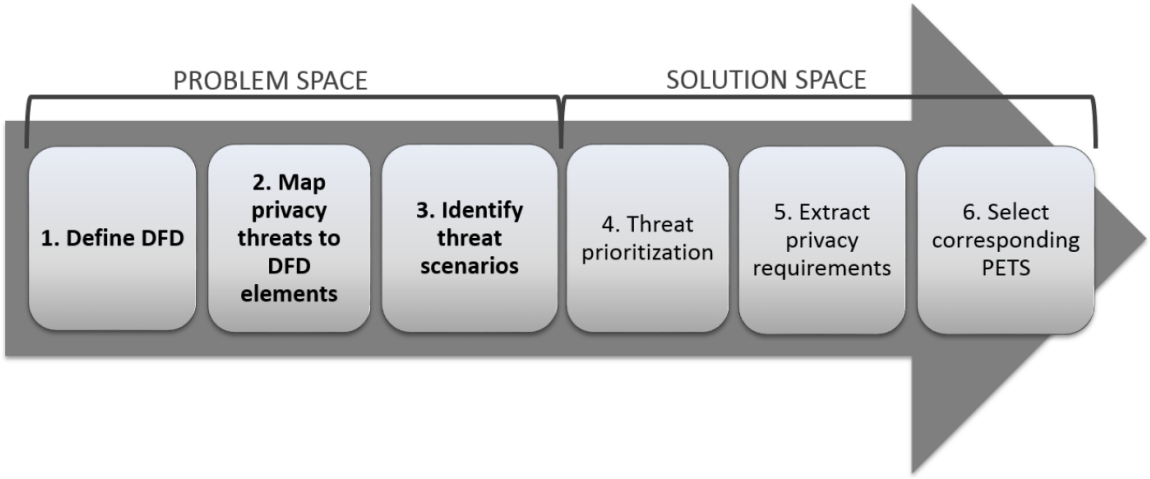
Мы рекомендуем метод моделирования угроз LINDDUN linddun.org Archive.org:

• Исследователи создали онлайн-инструмент, помогающий строить модель угроз: linddun.org Archive.org.
• Он синергичен со STRIDE ниже.
• Он сосредоточен на приватности, но явно отлично подходит и для анонимности.
• Он доступен для любого уровня подготовки, включая начинающих, поскольку даёт много инструкций, но также подходит и для очень подготовленных читателей.
• Он используется при создании Threat Modeling Manifesto: threatmodelingmanifesto.org Archive.org

Инструкции и ресурсы по моделированию угроз LINDDUN:

• **Мы рекомендуем следующее короткое обучающее видео с YouTube-канала "The Hated One", одобренное и проверенное разработчиками LINDDUN: youtube.com** Invidious, чтобы начать.
• Дополнительные ресурсы для более глубокого понимания и использования:
    • Подробнее можно прочитать здесь: A Lightweight Approach to Privacy Threat Modeling
    • Вот два видео Dr. K. Wuyts (imec-DistriNet, KU Leuven), объясняющие процесс:
        • Privacy & prejudice: on privacy threat modeling misconceptions Invidious

• Privacy Threat Model Using LINDDUN Invidious



(Иллюстрация из LINDDUN2015)

Вот альтернативные ресурсы и методологии, если LINDDUN вам не подходит:

• Online Operations Security: github.com (Archive.org)
• STRIDE от Microsoft: en.wikipedia.org Wikiless Archive.org
• PASTA: versprite.com Archive.org
• Threat Modeling: 12 Available Methods: insights.sei.cmu.edu Archive.org
• Threat Modelling: geeksforgeeks.org Archive.org

Заметки об атаке evil-maid и вмешательстве

Нужно учитывать ваш контекст.

Предотвращение атаки evil-maid или вмешательства может привести к плохим последствиям. Ваш противник может тогда прибегнуть к другим средствам, чтобы получить ключ.

С другой стороны, если допустить атаку, но обнаружить её, противник не узнает, что вы осведомлены о вмешательстве. Тогда вы сможете безопасно предпринять шаги, чтобы не раскрыть сведения и, возможно, уйти.

См. раздел несколько последних мыслей об OPSEC с некоторыми советами.

Типы атак на CPU

Отдельные проблемы безопасности поражают многие CPU Intel, например атаки на переходное выполнение, ранее называвшиеся методами побочного канала спекулятивного выполнения. Здесь можно проверить свой CPU на наличие затронутых микропроцессоров с известными ошибками: intel.com Archive.org.

Advanced Programmable Interrupt Controller (APIC) - встроенный компонент CPU, отвечающий за приём, приоритизацию и отправку прерываний логическим процессорам (LP). APIC может работать в режиме xAPIC, также известном как устаревший режим, где регистры конфигурации APIC раскрываются через страницу ввода-вывода с отображением в память (MMIO).

Появляется AEPIC (стилизуется как ÆPIC), первая архитектурная ошибка CPU, которая раскрывает устаревшие данные из микроархитектуры без использования побочного канала. Она архитектурно раскрывает устаревшие данные, ошибочно возвращаемые при чтении неопределённых диапазонов APIC-регистров. Этот новый метод был раскрыт в статье _ÆPIC Leak: Architecturally Leaking Uninitialized Data from the
Microarchitecture_, которую можно прочитать здесь: Borrello2022AEPIC Archive.org

Регистры, специфичные для модели (MSR), и их биты конфигурации также могут автоматически обнаруживаться на CPU Intel и AMD: Kogler2022 Archive.org. Это позволяет атакующему, хорошо знающему устройство CPU, видеть сведения о MSR, которые по сути являются специальными регистрами CPU, позволяющими взаимодействовать с низкоуровневыми функциями CPU и расширенной настройкой поведения CPU. У современных CPU x86 есть сотни таких регистров; обычно они документированы очень слабо, и в последние годы документация становится всё менее подробной.

Предупреждение об Orbot на Android

Хотя это часто понимают неверно, Orbot на Android не заставляет ваши приложения с поддержкой Tor проходить через Tor просто потому, что вы добавили их в список. Orbot действует как VPN для всего устройства, также известный как «прозрачный прокси». Список приложений, использующих Orbot, - это белый список. Он не заставит некоторые приложения магически использовать Tor, а неотмеченные - открытый интернет. Он лишь гарантирует, что VPN для всего устройства использует Tor для маршрутизации трафика. Это означает, что Orbot может контролировать только то, какие приложения имеют доступ к созданному им VPN. Другие приложения потеряют соединение.

Важно знать: если вы запускаете приложение (или Android делает это автоматически), пока Orbot не работает, приложение просто использует обычную сеть без участия Orbot, за исключением некоторых приложений, поддерживающих прокси Orbot.

Кроме того, вас не должно удивлять, что Tor Browser не работает при использовании Orbot в режиме VPN, поскольку архитектура Tor не допускает "Tor over Tor": нельзя повторно войти в сеть Tor из выходного узла Tor.

Это хорошо объясняет Alexander Færøy, основной разработчик Tor Project, в их TorifyHOWTO: Tor over Tor.

«При использовании прозрачного прокси можно запустить Tor-сессию как с клиента, так и с прозрачного прокси (прочитайте предупреждение!), создав сценарий "Tor over Tor". Это приводит к неопределённому и потенциально небезопасному поведению. Теоретически можно получить шесть переходов вместо трёх, но не гарантируется, что это будут три разных перехода: можно получить те же переходы, возможно, в обратном или смешанном порядке. Неясно, безопасно ли это. Это никогда не обсуждалось. Можно выбрать входную/выходную точку, но вы получаете лучшую безопасность, которую Tor может обеспечить, когда оставляете выбор маршрута Tor; переопределение входных/выходных узлов может нарушить вашу анонимность способами, которых мы не понимаем. Поэтому использование Tor over Tor крайне не рекомендуется».

И из поста на Tor Stack Exchange:

«Опасность, помимо потери производительности, из-за которой я не запускаю Tor поверх Tor, связана с измерениями времени и перегрузок. Противники, наблюдающие ваш трафик на выходах ваших цепочек, получают больше шансов связать активность Whonix с активностью Tor Browser Bundle, когда эти общие цепочки замедляются или теряют пакеты одновременно. Это может происходить и без Tor over Tor, если ваши экземпляры используют общий вышестоящий канал. Связь станет плотнее и явнее, если вы пропускаете Tor-трафик Whonix через SOCKS5 Tor-цепочки TBB. Такая более тесная связь повышает риск успешной корреляции».

Предостережение о Session Messenger

- Они используют LokiNet, которому требуется Oxen для запуска узлов, маршрутизирующих трафик Session, а это стоит 15 000 \$OXEN или 3 750 \$OXEN для общего узла[9], что составляет примерно \~\$1 800 или \~\$500 долларов США соответственно. Такая высокая стоимость создаёт барьер входа для запуска узлов, потенциально централизуя сеть и ограничивая её доступность.
  - Цена запуска узлов фактически ставит их сеть за платный барьер, если вы хотите запустить узел, даже просто чтобы внести пропускную способность в сеть, как это можно делать с Tor. Но существует форк Lokinet без стейкинга.
  - Разработчики Session утверждают, что это попытка предотвратить атаки Сивиллы, но многие спорят, что это только поощряет такие атаки: так они гарантируют, что только правительства и другие хорошо финансируемые организации, от которых такие сети обычно пытаются защитить, будут иметь финансовые ресурсы для запуска узлов. Впрочем, всё это спорно. Но $OXEN ориентирован на приватность.
- Они отказались от критически важных функций безопасности протокола (perfect forward secrecy, PFS, и правдоподобное отрицание)[10] в пользу долгосрочных ключей сообщений и самоудаляющихся криптографических подписей, которые дают гораздо более слабые гарантии безопасности[11].
  - Это *могло бы* быть не так плохо, если бы узлы можно было запускать бесплатно, но это не так.
- В апреле 2021 года Session прошёл аудит[12] с удовлетворительными результатами, но этот аудит не упоминает эти изменения. Также сейчас у нас нет достаточной информации о LokiNet, onion-маршрутизируемой сети, используемой Session, чтобы рекомендовать её. Некоторые всё ещё рекомендуют Session, например Techlore[13].
- Их финансирование полностью непрозрачно.

Короче говоря, по нашему мнению, Session Messenger можно использовать на iOS из-за отсутствия лучшей альтернативы, например Briar. Но если Briar или другое приложение, возможно Cwtch в будущем, станет доступным, мы порекомендуем уйти с Session Messenger как можно скорее. Это крайний вариант.

Примеры провалов OPSEC

Следующие случаи взяты из открытых судебных документов, журналистских материалов и разборов после событий. Они включены не для злорадства над пойманными людьми, а потому что каждый показывает конкретный, повторяемый тип провала, напрямую относящийся к рекомендациям в других местах этого руководства. Во всех случаях доступных технических инструментов анонимности было достаточно; провалы были человеческими.

Hector Monsegur (Sabu) - LulzSec, 2011

Контекст: Monsegur был ключевым участником и фактическим лидером LulzSec, известной хакерской группы, ответственной за взломы Sony, FBI и других. Его арестовали в июне 2011 года, после чего он стал информатором FBI, когда ему пригрозили отобрать детей.

Провал: В одном единственном случае Monsegur вошёл в IRC-канал, связанный с Anonymous/LulzSec, не направив соединение через Tor. Его настоящий IP-адрес, выданный домашним интернет-подключением в New York, был записан IRC-сервером. FBI запросило эти журналы повесткой.

Что это показывает: Один сбой в одной сессии достаточен, чтобы деанонимизировать в остальном дисциплинированного оператора. Tor эффективен только если используется *каждый раз* без исключений. На операционном уровне не существует «только в этот раз». Ценность анонимности уничтожается в тот момент, когда она нарушена, даже один раз.

Что ему следовало сделать: Использовать Tor или доверенный VPN для каждого IRC-подключения без исключений, в идеале с оборудования и сети, не связанных с его личностью. Одно выделенное устройство, используемое исключительно для чувствительных действий, предотвратило бы перекрёстное загрязнение.

Ross Ulbricht - Silk Road, 2013

Контекст: Ulbricht управлял Silk Road, псевдонимным darknet-рынком, под именем "Dread Pirate Roberts" примерно два года до ареста в октябре 2013 года.

Провал: Несколько накапливающихся ошибок со временем, а не один инцидент. До существования Silk Road Ulbricht писал на Bitcoin-форуме под именем "altoid", рекламируя сайт, и отдельно использовал то же имя "altoid" для публикации вакансии, где указал личный адрес Gmail. Следователи сопоставили имя пользователя между публикациями. Кроме того, ранние публикации на Stack Overflow были связаны с его реальной личностью. Его ноутбук при задержании был открыт и разблокирован, то есть зашифрованные диски были полностью доступны в момент захвата.

Что это показывает: Повторное использование имени пользователя в разных контекстах - один из самых надёжных векторов деанонимизации, доступных следователям. Псевдоним для чувствительной активности никогда не должен появляться в контексте, связанном с вашей реальной личностью: ни в вакансии, ни в вопросе на форуме, ни в случайном комментарии много лет назад. Разделение должно быть полным и должно предшествовать активности, а не следовать за ней.

Что ему следовало сделать: Использовать полностью отдельные личности, устройства и каналы связи для администрирования Silk Road и личной активности, без общих имён пользователей, адресов электронной почты или контекстов письма. До ареста зашифровать рабочий диск парольной фразой, чтобы захват открытого ноутбука не дал доступ к открытому тексту.

"Defcon" (Blake Benthall) - Silk Road 2.0, 2014

Контекст: Silk Road 2.0 был запущен вскоре после изъятия оригинального Silk Road. Его администратор, действовавший как "Defcon", был арестован в ноябре 2014 года.

Провал: Согласно уголовной жалобе, агент FBI под прикрытием получил позицию внутри персонала сайта. Более технически жалоба описывает использование корреляции времени входа: следователи заметили, что "Defcon" входил на сайт во времена, коррелировавшие с другой идентифицируемой онлайн-активностью. Кроме того, серверная инфраструктура была установлена из-за неверно настроенных конфигураций скрытого сервиса, которые раскрывали реальные IP-адреса; это повторяющийся операционный провал darknet-рынков.

Что это показывает: Два отдельных урока. Во-первых, человеческое внедрение в доверенные круги часто эффективнее технических атак: никакая криптография не защищает от доверенного инсайдера. Во-вторых, операционная безопасность серверной стороны, то есть правильная настройка скрытых сервисов Tor так, чтобы они ни при каких условиях не раскрывали реальный IP, так же важна, как анонимность клиентской стороны. Идеально анонимный администратор не имеет значения, если сам сервер идентифицируем.

Что ему следовало сделать: Проверить все серверные конфигурации на утечки IP до запуска и регулярно после него. Рассматривать весь персонал как потенциальных информаторов на операционном уровне и соответственно разделять сведения.

Jeremy Hammond - AntiSec, 2012

Контекст: Hammond был участником AntiSec, ответвления Anonymous, ответственного за взлом Stratfor. Его арестовали в марте 2012 года.

Провал: Monsegur (Sabu), к этому моменту информатор FBI, направлял Hammond к целям, выбранным FBI, одновременно собирая доказательства против него. Hammond использовал сильные технические практики, но был социально скомпрометирован через доверенные отношения. Он также повторно использовал шаблон пароля, который следователи смогли выявить между аккаунтами.

Что это показывает: Дополнительный урок к делу Monsegur: даже технически дисциплинированные операторы уязвимы к компрометации через доверенные человеческие отношения. Повторное использование паролей или шаблонов паролей между личностями даёт вектор корреляции, даже когда ни один конкретный учётный секрет напрямую не скомпрометирован.

Что ему следовало сделать: Использовать уникальные, случайно сгенерированные учётные данные для каждой личности и каждого сервиса, без общих шаблонов. Более важный урок - операционное доверие к людям нельзя проверить криптографически - не имеет чистого технического решения, но разделение того, что знает каждый соучастник, ограничивает ущерб от любой отдельной компрометации.

Общие закономерности

Если читать эти случаи вместе, повторяются несколько паттернов:

- **Единичные сбои в сессии ломают долгосрочную анонимность.** Последовательность обязательна.
- **Связь личностей между контекстами - самый распространённый следственный вектор.** Имена пользователей, стиль письма, адреса электронной почты и история публикаций доступны для поиска и корреляции.
- **Нужна и серверная, и клиентская безопасность.** Сильная клиентская анонимность не компенсирует протекающий сервер.
- **Человеческие отношения - самая надёжная поверхность атаки.** Внедрение и информаторы встречаются в большинстве значимых закрытий darknet-площадок.
- **Физический захват разблокированного устройства отменяет всё.** Шифрование диска помогает только если устройство заблокировано в момент изъятия.

Постквантовая криптография

Примечание: этот раздел касается угрозы, которая для большинства пользователей не является немедленной. Если ваша модель угроз включает противника уровня государства или коммуникации, чувствительность которых сохраняется на годы вперёд, читайте внимательно. Если вы средний пользователь, сейчас можно просмотреть этот раздел бегло, но стоит вернуться к нему по мере развития технологии.

Большая часть шифрования, защищающего ваши коммуникации сегодня, включая обмен ключами в Signal, HTTPS-соединениях, VPN и PGP, опирается на математические задачи, которые вычислительно нереально решить на любом классическом компьютере. Достаточно мощный квантовый компьютер[14], выполняющий алгоритм Shor[15], эффективно сломал бы эти задачи. Такого компьютера пока нет. Крупнейшие современные машины всё ещё далеки от нужного масштаба. Но это не повод игнорировать проблему.

Угроза называется **«собрать сейчас, расшифровать позже»** (HNDL). Она работает так: противник, реалистично государственное разведывательное агентство, записывает и хранит ваш зашифрованный трафик сегодня, в больших масштабах. Сейчас он не может его прочитать. Но если в следующие 10-20 лет будет построен способный квантовый компьютер, он расшифрует этот архивный трафик задним числом. Для большинства читателей это не срочная проблема. Но для журналиста, защищающего источник, личность которого опасно раскрыть даже в 2035 году, или активиста, живущего при правительстве с очень длинной институциональной памятью, это стоит воспринимать серьёзно.

Хорошая новость в том, что криптографическое сообщество знает об этой проблеме больше десяти лет, и инструменты уже появляются. В 2024 году NIST финализировал первые постквантовые криптографические стандарты[16]:

- **ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism, ранее известный как Kyber[17]) - заменяет классический шаг обмена ключами в протоколах вроде TLS и Signal X3DH. Он основан на сложности задачи Module Learning With Errors (MLWE), которая считается устойчивой как к классическим, так и к квантовым атакам.
- **ML-DSA** (Module-Lattice-Based Digital Signature Algorithm, ранее Dilithium) - постквантовая замена подписей RSA и ECDSA, используемых для аутентификации личностей и подписи программного обеспечения.
- **SPHINCS+** (теперь стандартизирован как SLH-DSA) - схема подписи на основе хешей. Она медленнее и крупнее ML-DSA, но полагается только на безопасность хеш-функций, а не на предположения о решётках, что делает её консервативной запасной опцией на случай ослабления решёточной криптографии.

NIST явно рекомендует развёртывать их в **гибридном режиме** на переходный период, то есть вместе с классическими алгоритмами, а не сразу вместо них. Так атакующему пришлось бы сломать оба компонента одновременно.

PQXDH в Signal

В сентябре 2023 года Signal развернул PQXDH[18] (Post-Quantum Extended Diffie-Hellman), обновив протокол согласования ключей X3DH так, чтобы он сочетал ML-KEM-1024 с классическим обменом Diffie-Hellman X25519. Результат гибридный: безопасность сохраняется, пока хотя бы один компонент остаётся несломленным.

Для пользователей Signal **это произошло автоматически и прозрачно**. Настройка не требуется. Новые разговоры, начатые после развёртывания, по умолчанию используют PQXDH. Это напрямую отвечает на угрозу HNDL для прямой секретности: противник, записавший ваш трафик Signal, не сможет использовать будущий квантовый компьютер для получения ваших сеансовых ключей.

Обратите внимание, что это покрывает только слой обмена ключами. Слой аутентификации, то есть ключи личности, в Signal пока не усилен постквантово, хотя это активная область разработки.

Что делать сейчас

Для большинства моделей угроз практические шаги просты:

- **Используйте Signal.** PQXDH уже развёрнут, действий не требуется.
- **Держите браузер обновлённым.** В Chrome и Firefox гибридный постквантовый обмен ключами (X25519 + ML-KEM) в TLS включён по умолчанию с 2024 года[19]. Это защищает HTTPS-соединения от HNDL на транспортном уровне.
- **Не полагайтесь на PGP/GPG для долгосрочной конфиденциальности очень чувствительных материалов.** Обмены ключами PGP (RSA, ECDH) не усилены постквантово. Сообщения, зашифрованные на PGP-ключ сегодня, могут быть расшифрованы задним числом квантово-способным противником, который их сохранил. Если вам нужно использовать PGP, рассматривайте его только как защиту от современных противников.
- **Проверьте своего VPN-провайдера.** Большинство коммерческих VPN ещё не развернули постквантовый обмен ключами. Некоторые, например Mullvad и ProtonVPN, добавили его. Если HNDL входит в вашу модель угроз, проверьте документацию провайдера или перейдите к тому, кто это поддерживает.

Для людей с действительно высоким риском: коммуникации, раскрытие которых будет опасным через десять или больше лет, требуют внимания уже сейчас. Переход на Signal и установление свежих сессий, а не опора на долгоживущие состояния сессий до развёртывания PQXDH, - самый практичный ближайший шаг.

Примечание о Monero

Криптографические примитивы Monero, в частности использование Ed25519 и Curve25519, уязвимы для алгоритма Shor на достаточно мощном квантовом компьютере. Monero Research Lab изучала эту проблему[8], и постквантовое обновление не развёрнуто. Сообщество считает это среднесрочной, а не немедленной проблемой с учётом текущего состояния квантового оборудования. Для операционной анонимности сегодня Monero остаётся подходящим. Не предполагайте долгосрочную финансовую приватность против квантово-способного противника.

Стилометрический анализ и стиль письма

Примечание: стилометрическая деанонимизация - реальная, но узкая угроза. Она актуальна для людей, которые долго публикуют значительные объёмы текста под псевдонимом, или для подозреваемых источников утечек, которых сравнивают с известным корпусом их письма. Для большинства пользователей этого руководства это не реалистичная угроза. Читайте этот раздел, если вы публично пишете под псевдонимом, многократно общаетесь с одним и тем же противником или являетесь потенциальным информатором, чей стиль письма могут сравнивать с внутренними документами.

Стилометрия[20] - это статистический анализ стиля письма для установления авторства. Главная идея в том, что люди пишут устойчивыми, измеримыми способами, которые сохраняются между темами и контекстами, и эти паттерны трудно сознательно подавить. Автор, который привычно использует оксфордскую запятую, предпочитает "however" слову "but", пишет предложения в среднем по 22 слова и редко использует восклицательные знаки, будет склонен делать это и в посте на форуме, и в электронном письме, и в слитом документе. Даже один раз, когда вы забудете анонимизировать письмо, может стать вашим крахом. В 2026 году Vitalik Buterin, сооснователь Ethereum, пытается заставить ИИ деанонимизировать его самого *намеренно*, чтобы показать, что в ближайшем будущем это весьма вероятно[21].

Какие признаки измеряются

Современные стилометрические системы анализируют десятки и сотни признаков одновременно. Самые различающие - **служебные слова**: артикли, предлоги, союзы. Они используются во многом бессознательно и очень стабильны для каждого автора[22]. Содержательные слова, то есть существительные, глаголы и тематическая лексика, являются плохими стилометрическими признаками, потому что меняются в зависимости от темы; служебные слова нет. Другие признаки включают распределение длины предложений; пунктуационные привычки (частота запятых, использование точки с запятой, предпочтение тире); длину абзацев; богатство словаря (отношение типов к токенам); символьные n-граммы; и синтаксические паттерны, например частоту пассивного залога.

В контролируемых академических оценках современные системы достигают точности установления авторства выше 80% на корпусах из 50 и более кандидатов, когда каждый автор предоставил несколько тысяч слов[23]. Точность заметно падает при более коротких текстах (менее 500 слов), больших наборах кандидатов или когда корпус кандидата и анонимный текст относятся к разным жанрам или контекстам.

Развёрнутые инструменты и реальные случаи

JGAAP (Java Graphical Authorship Attribution Program)[24], разработанная в Duquesne University, - самый широко используемый открытый академический инструмент; его применяли в судебных процессах. **Burner** - более новая система, специально созданная для состязательной деанонимизации онлайн-псевдонимов.

Самый документированный реальный случай - идентификация J.K. Rowling в 2013 году как автора *The Cuckoo's Calling*, опубликованной под псевдонимом Robert Galbraith[25]. Стилометрический анализ Peter Millican и Patrick Juola, сравнивший роман с известными работами Rowling и набором авторов-кандидатов, дал сильное совпадение до того, как идентификация была подтверждена другими средствами. Корпус в этом случае был большим - целые романы, то есть условие, при котором стилометрия работает лучше всего.

В контекстах национальной безопасности стилометрический анализ использовался или предпринимался в расследованиях утечек для сравнения анонимных документов с известным письмом подозреваемых источников, хотя конкретные случаи редко публично подтверждаются.

Что работает, а что нет

Наивные меры противодействия не работают. Замена синонимов, то есть замена слов альтернативами с похожим значением, не влияет на паттерны служебных слов, структуру предложений или пунктуационные привычки, которые являются самыми различающими признаками. Простая попытка «писать иначе» без конкретного метода неэффективна, потому что бессознательные привычки, которые измеряет стилометрия, по определению являются теми, которые автор не замечает.

Что имеет некоторую эффективность: письмо в регистре, действительно непохожем на ваш естественный стиль, например формальная юридическая проза вместо привычного разговорного стиля, снижает точность установления авторства, потому что смена регистра одновременно влияет на несколько классов признаков. Короткие тексты, менее 300-400 слов, заметно снижают уверенность установления авторства. Совместное письмо, где несколько авторов вносят вклад в один документ, существенно ухудшает установление одного автора.

Переписывание ИИ как мера противодействия - активная область исследований со смешанными результатами[26]. Большие языковые модели при переписывании текста действительно меняют распределения служебных слов и структуру предложений, и ранние исследования показывают, что это в некоторой степени снижает точность стилометрического установления авторства. Однако переписывание LLM не удаляет весь стилистический сигнал надёжно: некоторые авторские паттерны переживают перефразирование, и появляется новый сигнал - статистический отпечаток конкретной модели и использованной подсказки. Насколько этот

обмен выгоден, зависит от возможностей противника. Переписывание LLM, вероятно, полезно как один слой в подходе глубокой защиты для авторов с высоким риском, но на него не следует полагаться как на полное решение.

Честная модель угроз

Стилометрии нужен достаточно большой образец текста анонимного автора, в идеале 1 000+ слов, набор известных авторов-кандидатов для сравнения и известный письменный корпус этих кандидатов. Это ограничивает реалистичное применение такими случаями: расследования утечек, где у следователей есть короткий список подозреваемых с известными образцами письма; деанонимизация долго существующих псевдонимных авторов с большим опубликованным объёмом; академические или криминалистические споры об авторстве.

Это не практичная угроза для одноразовых анонимных сообщений; пользователей, у противника которых нет сравнительного корпуса их письма; или коротких сообщений, где образец текста недостаточен для надёжного анализа. Для большинства читателей этого руководства другие угрозы, описанные здесь, - метаданные, идентификация на сетевом уровне, цифровой отпечаток устройства - гораздо более вероятные векторы, чем стилометрия. Сначала разберитесь с ними.

Сноски

[1] [назад] NIST, NIST Has Spoken - Death to Complexity, Long Live the Passphrase! sans.org Archive.org
[2] [назад] ZDnet, FBI recommends passphrases over password complexity zdnet.com Archive.org
[3] [назад] The Intercept, Passphrases That You Can Memorize --- But That Even the NSA Can't Guess theintercept.com Tor Mirror Archive.org
[4] [назад] Proton Blog, Let's settle the password vs. passphrase debate once and for all proton.me Archive.org
[5] [назад] YouTube, Edward Snowden on Passwords: Last Week Tonight with John Oliver (HBO) youtube.com Invidious
[6] [назад] YouTube, How to Choose a Password -- Computerphile youtube.com Invidious
[7] [назад] Wikipedia, Passphrase en.wikipedia.org Wikiless Archive.org
[8] [назад] Monero Research Lab, Evaluating cryptocurrency security and privacy in a post-quantum world github.com Archive.org
[9] [назад] Lokinet Documentation, Service Nodes, loki.network Archive.org
[10] [назад] GetSession.org, The Session Protocol: What's changing --- and why getsession.org Archive.org
[11] [назад] Session Documentation, Session protocol explained, getsession.org Archive.org
[12] [назад] Quarkslab, Audit of Session Secure Messaging Application blog.quarkslab.com Archive.org
[13] [назад] Techlore, Top 5 BEST Messengers For Privacy youtube.com Invidious
[14] [назад] Wikipedia, Quantum computing en.wikipedia.org Wikiless Archive.org
[15] [назад] Wikipedia, Shor's Algorithm, en.wikipedia.org Wikiless Archive.org
[16] [назад] NIST, Post-Quantum Cryptography Standardization csrc.nist.gov Archive.org
[17] [назад] NIST, NIST Releases First 3 Finalized Post-Quantum Encryption Standards nist.gov Archive.org
[18] [назад] Signal Blog, PQXDH Key Agreement Protocol signal.org Archive.org
[19] [назад] Chromium Blog, Protecting Chrome Traffic with Hybrid Kyber KEM blog.chromium.org Archive.org
[20] [назад] Wikipedia, Stylometry en.wikipedia.org Wikiless Archive.org
[21] [назад] Binance Square, Vitalik Buterin Says He Wrote an Anonymous Ethereum Document to Test AI De-Anonymization binance.com Archive.org
[22] [назад] Mosteller & Wallace, Inference and Disputed Authorship: The Federalist (1964) - the foundational study establishing function words as the primary stylometric signal jstor.org Archive.org
[23] [назад] Koppel, Schler & Argamon, Computational Methods in Authorship Attribution, Journal of the American Society for Information Science and Technology, 2009 onlinelibrary.wiley.com Archive.org
[24] [назад] Juola et al., JGAAP: A System for Comparative Authorship Attribution citeseerx.ist.psu.edu Archive.org
[25] [назад] Patrick Juola, How a computer program helped reveal J.K. Rowling as author of A Cuckoo's Calling, Scientific American, 2013 scientificamerican.com Archive.org
[26] [назад] Mahmood et al., This is not my writing: LLMs as Authorship Obfuscation Tools, arXiv 2023 arxiv.org Archive.org