



AnarSec это ресурс который призван помочь анархистам ориентироваться во враждебном мире технологий — подборка пособий по обеспечению цифровой безопасности и анонимности, а также по проведению хакерских атак. Все пособия доступны в виде буклетов, чтобы их можно было распечатать и будут постоянно обновляться.

Защита

Tails

- **Операционная система Tails - для анархистов**
- **Лучшие практики Tails**

Qubes OS

- Qubes OS for Anarchists

Телефоны

- **Избавься от шпиона в твоём кармане**
- GrapheneOS for Anarchists

Общие вопросы

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

Нападение

Скоро ожидается

Эта версия зина была последний раз обновлена 2024-11-25. Зайдите на сайт anarsec.guide/ru и посмотрите, нет ли более поздних редакций.

Символ [†] означает, что этот термин есть в словаре. Ai ferri corti.

Содержание

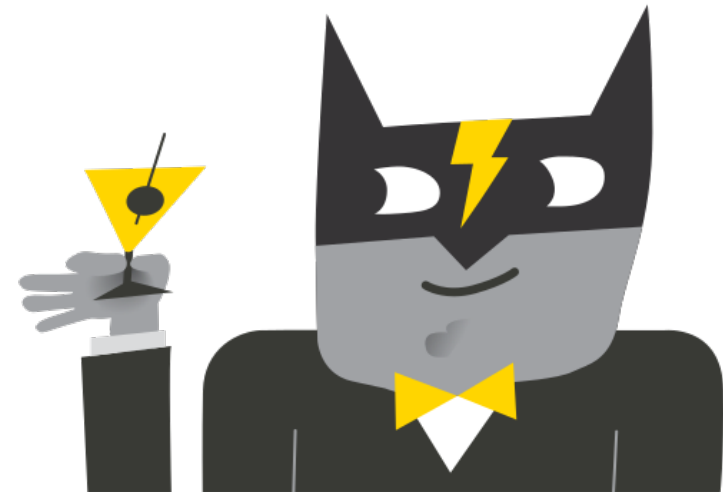
Защита вашей личности при использовании Tails	5
1. Обмен файлами с метаданными	6
2. Использование Tails для более чем одной цели одновре-	
менно	6
Ограничения сети Tor	7
1. Скрытие факта использования Tor и Tails	8
2. Защита от решительных и опытных нападающих	8
Снижение рисков при использовании ненадежных компьютеров.	
16	
1. Установка с зараженного компьютера	16
2. Запуск Tails на компьютере с поврежденным BIOS, про-	
шивкой или оборудованием	17
Использование переключателя защиты от записи	23
Разблокировка переключателя	25
USB-накопители с персональными данными	27
Осведомленность о фишинге	30
Файлы	32
Ссылки	32
Атаки на водопой	34
Шифрование	35
Пароли	35
Зашифрованные тома	38
Зашифрованная связь	40
В заключение	41
Приложение: Объяснение GPG	41
Шаг: Генерация пары ключей	43
Шаг: Проверьте открытый ключ Tails	44
Шаг: Проверьте загруженный файл Tails .img	44
Приложение: Рекомендации	45
Your Phone	46
Your Computer	46
Encrypted Messaging	47

Storing Electronic Devices	47
Приложение: Словарь	47
Asynchronous Communication	47
Command Line Interface (CLI)	47
Correlation Attack	48
Digital Signatures	48
Encryption	49
Forward secrecy	49
GnuPG / OpenPGP	50
LUKS	50
Metadata	50
Open-source	51
Operating system (OS)	51
Passphrase	51
Password	51
Phishing	52
Physical attacks	52
Public-key cryptography	52
Remote attacks	53
Spear phishing	54
Synchronous communication	54
Threat model	54
Tor network	55

Все анархисты должны знать, как использовать Tails — в этом тексте описываются некоторые дополнительные меры предосторожности, которые вы можете предпринять, и которые имеют отношение к модели анархистской угрозы[†]. Не все модели анархистской угрозы одинаковы, и только вы можете решить, какие меры по смягчению последствий стоит применять для вашей деятельности, но мы стремимся предоставить советы, которые подходят для высокорисковых видов деятельности, таких как требование действия. Если вы новичок в Tails, начните с Операционная система Tails - для анархистов¹.

Начнем с рассмотрения трех тем, затронутых на странице предупреждений Tails²: защита вашей личности, ограничения сети Tor и ненадежные компьютеры.

Защита вашей личности при использовании Tails



¹anarsec.guide/ru/posts/tails/

²tails.net/doc/about/warnings/index.ru.html

Tails создан для сокрытия вашей личности. Но некоторые ваши действия могут раскрыть вашу личность:

1. Обмен файлами с метаданными[†], такими как дата, время, местоположение и информация об устройстве
2. Использование Tails для нескольких целей одновременно

1. Обмен файлами с метаданными

Первую проблему можно решить, **очистив метаданные файлов перед их публикацией**:

- Чтобы узнать, как это сделать, см. Remove Identifying Metadata From Files³.

2. Использование Tails для более чем одной цели одновременно

Эту вторую проблему можно смягчить с помощью так называемой **«компарментализации»**:

- Разделение⁴ означает разделение различных видов деятельности или проектов. Если вы используете сеансы Tails для более чем одной цели одновременно, злоумышленник может связать ваши различные виды деятельности вместе. Например, если вы входите в разные учетные записи на одном и том же веб-сайте в одном сеансе Tails, веб-сайт может определить, что учетные записи используются одним и тем же человеком. Это происходит потому, что веб-сайты могут определить, когда два аккаунта используют одну и ту же схему Tor.
- Чтобы не дать злоумышленнику связать ваши действия при использовании Tails, перезапускайте Tails между различными

³anarsec.guide/posts/metadata/

⁴notrace.how/threat-library/mitigations/compartmentalization.html

Tor network

Tor¹⁷⁸ (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet connection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor «the King of high secure, low latency Internet anonymity» with «no contenders for the throne in waiting». The Tor network can be accessed through the Tor Browser on any operating system. The Tails¹⁷⁹ operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists¹⁸⁰ and Privacy Guides¹⁸¹. To understand the limitations of Tor, see the Whonix documentation¹⁸².

¹⁷⁸torproject.org/

¹⁷⁹anarsec.guide/glossary/#tails

¹⁸⁰anarsec.guide/posts/tails/#tor

¹⁸¹privacyguides.org/en/advanced/tor-overview/

¹⁸²whonix.org/wiki/Warning

Spear phishing

Spear phishing is more sophisticated than regular phishing¹⁷⁰, which casts a wide net. In spear phishing, attackers customize their forged messages and send them to a smaller number of potential victims. Spear phishing requires more research on the part of the attacker; however, the success rate of spear phishing attacks is higher than the success rate of regular phishing attacks.

Synchronous communication

Unlike asynchronous communication¹⁷¹, both parties must be online at the same time. This does not require servers for the communication and is often referred to as «peer to peer».

Threat model

Threat modeling is a family of activities for improving security by identifying a set of adversaries, security goals¹⁷², and vulnerabilities¹⁷³, and then defining countermeasures to prevent or mitigate the effects of threats to the system. A threat is a potential or actual undesirable event that can be malicious (such as a DDoS attack¹⁷⁴) or accidental (such as a hard drive failure). Threat modeling is the deliberate activity of identifying and assessing threats and vulnerabilities.

For more information, see the No Trace Project Threat Library¹⁷⁵, Defend Dissent: Digital Threats to Social Movements¹⁷⁶ and Defending against Surveillance and Suppression¹⁷⁷.

¹⁷⁰anarsec.guide/glossary/#phishing

¹⁷¹anarsec.guide/glossary/#asynchronous-communication

¹⁷²anarsec.guide/glossary/#security-goal

¹⁷³anarsec.guide/glossary/#vulnerability

¹⁷⁴anarsec.guide/glossary/#ddos-attack

¹⁷⁵notrace.how/threat-library/

¹⁷⁶open.oregonstate.edu/defenddissent/chapter/digital-threats/

¹⁷⁷open.oregonstate.edu/defenddissent/chapter/surveillance-and-suppression/

действиями. Например, перезапускайте Tails между проверкой писем разных проектов.

- Tails по умолчанию амнезирует, поэтому для сохранения любых данных из сеанса Tails необходимо сохранить их на USB-накопитель. Если сохраняемые файлы могут быть использованы для связывания ваших действий, используйте разные зашифрованные (LUKS⁺) USB-накопители для каждого действия. Например, используйте один USB-накопитель Tails для моделирования веб-сайта, а другой — для исследования действий. В Tails есть функция, называемая Persistent Storage, но мы не рекомендуем использовать ее для хранения данных, о чем мы расскажем ниже⁵.

Ограничения сети Tor



⁵anarsec.guide/ru/posts/tails-best/#ispol-zovanie-perekliuchatelja-zashchity-ot-zapisi

Tails использует сеть Tor[†], поскольку это самая сильная и популярная сеть для защиты от слежки и цензуры. Но у Tor есть ограничения, если вас беспокоят:

1. Скрытие того, что вы используете Tor и Tails
2. Защита ваших онлайн-коммуникаций от решительных и опытных злоумышленников

1. Скрытие факта использования Tor и Tails

Эту первую проблему можно смягчить с помощью **мостов Tor**⁶:

- Tor Bridges — это секретные ретрансляторы Tor, которые скрывают ваше подключение к сети Tor. Однако это необходимо только там, где подключение к Tor заблокировано, например, в странах с жесткой цензурой, некоторыми публичными сетями или некоторыми программами родительского контроля. Это связано с тем, что Tor и Tails защищают вас не тем, что вы выглядите как любой другой пользователь Интернета, а тем, что все пользователи Tor и Tails выглядят одинаково. Становится невозможным определить, кто есть кто среди них.

2. Защита от решительных и опытных нападающих

Сквозная *корреляционная* атака[†] — это теоретический способ, с помощью которого глобальный злоумышленник может нарушить анонимность Tor:

Мощный противник, который может анализировать время и форму трафика, входящего и исходящего из сети Tor, может быть в состоянии деанонимизировать пользователей Tor. Эти атаки называются атаками *сквозной кор-*

decryption; the public key must be made public, and is used for encryption. This is the model used for encrypted communication, since the public key cannot be used for decryption. All other parties must verify that a published public key belongs to its intended owner to avoid man-in-the-middle attacks¹⁶³.

There are several approaches to public-key cryptography. For example, some cryptosystems are based on the algebraic structure of elliptic curves over finite fields (ECC). Others are based on the difficulty of factoring the product of two large prime numbers (RSA). Public-key cryptography can also be used for digital signatures¹⁶⁴.

To learn more, watch this video¹⁶⁵, or for a more detailed look, see Defend Dissent: Public-Key Cryptography¹⁶⁶.

Remote attacks

By remote attack, we mean that an adversary would access the data on your phone or laptop through an Internet or data connection. There are companies that develop and sell the ability to infect your device (usually focusing on smartphones) with malware¹⁶⁷ that would allow their customer (your adversary, be it a corporate or state agent) to remotely access some or all of your information. This is in contrast to a physical attack¹⁶⁸.

For a more detailed look, see Defend Dissent: Protecting Your Devices¹⁶⁹.

⁶tails.net/doc/anonymous_internet/tor/index.en.html#bridges

¹⁶³anarsec.guide/glossary/#man-in-the-middle-attack

¹⁶⁴anarsec.guide/glossary/#digital-signatures

¹⁶⁵youtube.com/watch?v=GSIDS_lvRv4

¹⁶⁶open.oregonstate.edu/defenddissent/chapter/public-key-cryptography/

¹⁶⁷anarsec.guide/glossary/#malware

¹⁶⁸anarsec.guide/glossary/#physical-attacks

¹⁶⁹open.oregonstate.edu/defenddissent/chapter/protecting-your-devices/

Phishing

Phishing is a technique of social engineering¹⁵³. Attackers send SMS messages, emails, chat messages, etc. to their targets to get their personal information. The attackers can then try to impersonate their victims. It can also be used to get the victim to download malware¹⁵⁴ onto a system, which can be used as a starting point for hacking. Spear phishing¹⁵⁵ is a more sophisticated form of phishing. For more information, see the Kicksecure documentation¹⁵⁶.

Physical attacks

A physical attack is a situation where an adversary first gains physical access to your device through loss, theft, or confiscation. For example, your phone may be confiscated when you cross a border or are arrested. This is in contrast to a remote attack¹⁵⁷.

For more information, see Making Your Electronics Tamper-Evident¹⁵⁸, the Threat Library¹⁵⁹, the KickSecure documentation¹⁶⁰, and Defend Dissent: Protecting Your Devices¹⁶¹.

Public-key cryptography

Public-key cryptography (or asymmetric cryptography) is the opposite of symmetric cryptography¹⁶². Each party has two keys (public and private). The private key must be kept secret and is used for

¹⁵³anarsec.guide/glossary/#social-engineering

¹⁵⁴anarsec.guide/glossary/#malware

¹⁵⁵anarsec.guide/glossary/#spear-phishing

¹⁵⁶kicksecure.com/wiki/Social_Engineering

¹⁵⁷anarsec.guide/glossary/#remote-attacks

¹⁵⁸anarsec.guide/posts/tamper

¹⁵⁹notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html

¹⁶⁰kicksecure.com/wiki/Protection_Against_Physical_Attacks

¹⁶¹open.oregonstate.edu/defenddissent/chapter/protecting-your-devices/

¹⁶²anarsec.guide/glossary/#symmetric-cryptography

реляции, потому что злоумышленник должен наблюдать оба конца цепи Тор одновременно. [...] Атаки сквозной корреляции изучались в исследовательских работах, но мы не знаем ни об одном фактическом использовании для деанонимизации пользователей Тор.

Нецелевые и целевые корреляционные атаки

Как описано в приведенной выше цитате, глобальный противник (то есть АНБ) может взломать Тор с помощью корреляционной атаки. Если это произойдет, интернет-адрес, который вы использовали в кофейне без камер видеонаблюдения, будет вести только к вашей общей области (например, к вашему городу), поскольку он не связан с вами. Конечно, это менее верно, если вы используете местоположение регулярно. Корреляционные атаки еще менее осуществимы против подключений к адресу .onion, поскольку вы никогда не покидаете сеть Тор, поэтому нет «конечной точки», с которой можно было бы коррелировать посредством анализа сетевого трафика (если местоположение сервера неизвестно противнику). Стоит подчеркнуть, что «сквозные корреляционные атаки изучались в исследовательских работах, но мы не знаем ни о каком фактическом использовании для деанонимизации пользователей Тор».

То, что мы назовем «целевой» корреляционной атакой, гораздо более вероятно, потому что неглобальный противник (т. е. местные правоохранительные органы) способен на это, если вы уже находитесь в поле их зрения и являетесь целью физического наблюдения⁷ и/или цифрового наблюдения⁸. Это подтип корреляционной атаки, когда предполагаемая цель уже известна, что делает атаку более легкой для достижения, поскольку это значительно сокращает объем данных для фильтрации для корреля-

⁷notrace.how/threat-library/techniques/physical-surveillance/covert.html

⁸notrace.how/threat-library/techniques/targeted-digital-surveillance.html

ции. Нецелевая корреляционная атака, используемая для деанонимизации пользователя Tor, является беспрецедентной в текущих доказательствах, используемых в суде, хотя «целевая» корреляционная атака использовалась в качестве подтверждающего доказательства⁹ — подозреваемый уже был идентифицирован, что позволило следователям сопоставить их наблюдаемый след с определенной онлайн-активностью. В частности, они сопоставили сетевой трафик Tor, исходящий из дома подозреваемого, со временем, когда его анонимный псевдоним был онлайн в чатах.

Чтобы объяснить, как это работает, будет полезно, если у вас есть базовое понимание того, какая информация Tor видна различным третьим лицам — см. интерактивную графику EFF¹⁰. Для нецелевой корреляционной атаки следователю нужно будет *начать с узла выхода Tor*: взять конкретную онлайн-активность, исходящую из узла выхода, и попытаться сопоставить ее с огромным объемом глобальных данных, которые поступают на узлы входа Tor. Однако, если подозреваемый уже идентифицирован, следователь может вместо этого провести «целевую» корреляционную атаку и *начать с узла входа Tor*: взять данные, входящие на узел входа (через *физический или цифровой след* подозреваемого), и попытаться сопоставить их с *конкретной онлайн-активностью*, исходящей из узла выхода.

Для вашего *физического следа* операция по наблюдению может наблюдать, как вы регулярно ходите в кафе, а затем попытаться сопоставить это с онлайн-активностью, в которой они вас подозревают (например, если они подозревают, что вы модератор веб-сайта, они могут попытаться сопоставить эти временные окна с активностью модератора веб-сайта). Для вашего *цифрового следа*, если вы используете Интернет из дома, следователь может наблюдать за всем вашим трафиком Tor, а затем попытаться сопоставить это с онлайн-активностью, в которой они вас подозрева-

create social graphs), and other parties (to target location-based advertising). Whenever you use a computer, you are likely leaving metadata behind.

For more information, see Remove Identifying Metadata From Files¹⁴⁹ and Defend Dissent: Metadata¹⁵⁰.

Open-source

The only software we can trust because the «source code» that it is written in is «open» for anyone to examine.

Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android, and iOS. Linux and some versions of Android are the only open-source options on this list.

Passphrase

A passphrase is similar to a password¹⁵¹, but is made up of words instead of random characters.

Password

A password is a string of characters used for authentication. A strong password consists of randomly chosen characters that all have the same probability of occurrence and can be created with the KeePassXC Password Generator.

For more information, see Defend Dissent: Passwords¹⁵²

⁹medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8

¹⁰eff.org/pages/tor-and-https

¹⁴⁹anarsec.guide/posts/metadata

¹⁵⁰open.oregonstate.education/defenddissent/chapter/metadata/

¹⁵¹anarsec.guide/glossary/#password

¹⁵²open.oregonstate.education/defenddissent/chapter/passwords/

GnuPG / OpenPGP

GnuPG (GPG) is a program that implements the OpenPGP (Pretty Good Privacy) standard. GPG provides cryptographic functions for encrypting, decrypting, and signing text and files. It is a classic example of public-key cryptography¹⁴⁰. When used with email, metadata¹⁴¹ (such as email addresses) remains unencrypted. It does not provide forward secrecy¹⁴².

For more information, see this primer¹⁴³. We don't recommend it for encrypted communications, here's why¹⁴⁴.

LUKS

The Linux Unified Key Setup (LUKS)¹⁴⁵ is a platform-independent specification for disk encryption. It is the standard used in Tails¹⁴⁶, Qubes OS¹⁴⁷, Ubuntu, etc. LUKS encryption is only effective when the device is powered off. LUKS should use Argon2id¹⁴⁸ to make it less vulnerable to brute-force attacks.

Metadata

Metadata is data that provides information about other data. For example, a JPG file contains the actual image (data) but it may also contain metadata such as the date the file was created, the type of camera, GPS coordinates, and so on. Metadata can be valuable to attackers (to find appropriate exploits for outdated software the target is using), government agencies (to collect information about people to

¹⁴⁰anarsec.guide/glossary/#public-key-cryptography

¹⁴¹anarsec.guide/glossary/#metadata

¹⁴²anarsec.guide/glossary/#forward-secrecy

¹⁴³github.com/AnarchoTechNYC/meta/wiki/Pretty-Good-Privacy-%28PGP%29

¹⁴⁴anarsec.guide/posts/e2ee/#pgp-email

¹⁴⁵gitlab.com/cryptsetup/cryptsetup

¹⁴⁶anarsec.guide/glossary/#tails

¹⁴⁷anarsec.guide/glossary/#qubes-os

¹⁴⁸anarsec.guide/posts/tails-best/#passwords

ют. Для вашей *конкретной онлайн-активности* более сложный анализ будет включать регистрацию подключений к серверу для подробного сравнения, а простой анализ будет чем-то, что будет публично видно всем (например, когда ваш псевдоним находится в сети в чате или когда пост публикуется на веб-сайте).

Вы можете смягчить воздействие методов, доступных могущественным противникам, **отдавая приоритет ссылкам .onion, когда они доступны, принимая во внимание возможность целенаправленного наблюдения и используя подключение к Интернету, которое не привязано к вашей личности.**

Интернет-соединение, не привязанное к вашей личности

Использование интернет-соединения, не привязанного к вашей личности, означает, что если атака на сеть Tor будет успешной, она все равно не деанонимизирует вас. У вас есть два варианта: использовать Wi-Fi из общественного места (например, пойти в кафе без камер видеонаблюдения) или использовать антенну Wi-Fi через окно из частного пространства.

Работа в общественном месте

Если вам нужно использовать Интернет нерегулярно, например, чтобы отправить коммюнике или провести исследование действий, вы можете **выполнить обнаружение слежки¹¹ и анти-слежку¹² перед тем, как пойти в кофейню**, точно так же, как вы это делаете перед прямым действием. См. «How to submit an anonymous communiqué and get away with it»¹³ для получения дополнительной информации о том, что включает в себя отправка коммюнике.

¹¹notrace.how/threat-library/mitigations/surveillance-detection.html

¹²notrace.how/threat-library/mitigations/anti-surveillance.html

¹³notrace.how/resources/ru/#how-submit

При использовании Wi-Fi в общественных местах следует учитывать следующие соображения безопасности:

- Время имеет значение. Если вы хотите отправить отчет на следующее утро после беспорядков или коммунике вскоре после акции (время, когда может быть более высокий риск целенаправленного наблюдения), рассмотрите возможность подождать. В 2010 году, на следующее утро после поджога банка в Канаде, полиция следила за подозреваемым, когда он шел из дома в интернет-кафе, и наблюдала, как он размещал коммунике, а затем закапывал ноутбук в лесу. Совсем недавно следователи, осуществлявшие физическое наблюдение за анархистом во Франции¹⁴, установили скрытую камеру для контроля доступа в интернет-кафе недалеко от дома товарища и запросили записи видеонаблюдения за день, когда было отправлено коммунике о поджоге.
- Не входите в привычку посещать одни и те же кафе снова и снова, если можете этого избежать. Чем чаще вы пользуетесь пространством, тем больше Интернет привязан к вашей личности. Кроме того, если слежка знает, куда вы направляетесь, антислежка не будет эффективной.
- Если вам нужно купить кофе, чтобы получить пароль от Wi-Fi, платите наличными!
- Встаньте спиной к стене, чтобы никто не мог «залезть на плечо», чтобы увидеть ваш экран, и в идеале установите на свой ноутбук экран конфиденциальности¹⁵. Если вы пишете коммунике в офлайн-сессии Tails перед походом в общественное пространство, вам понадобится всего несколько минут, чтобы запереться в общественном туалете, чтобы отправить его.
- Если кафе без камер видеонаблюдения встречаются редко, вы можете попробовать получить доступ к Wi-Fi кофейни снаружи, вне зоны действия камер.

¹⁴notrace.how/resources/ru/#ivan

¹⁵anarsec.guide/ru/posts/tails/#ekran-konfidentsial-nosti

To learn more, watch this video¹³¹. For a more detailed look, see *Defend Dissent: Authenticity through Cryptographic Signing*¹³² or our *GPG explanation*¹³³.

Encryption

Encryption is the process of scrambling a message so that it can only be unscrambled (and read) by the intended parties. The method you use to scramble the original message, or *plaintext*, is called the *cipher* or *encryption protocol*. In almost all cases, the cipher is not intended to be kept secret. The scrambled, unreadable, encrypted message is called the ciphertext and can be safely shared. Most ciphers require an additional piece of information, called a *cryptographic key*, to encrypt and decrypt (scramble and unscramble) messages.

For more information, see symmetric cryptography¹³⁴, asymmetric cryptography¹³⁵, or *Defend Dissent: What is Encryption?*¹³⁶

Forward secrecy

Forward secrecy (FS, also known as «Perfect Forward Secrecy») combines a system of long-term keys and session keys to protect encrypted communications from future key compromise. An attacker who can record every encrypted message (man-in-the-middle¹³⁷) won't be able to decrypt those messages if the keys are compromised in the future. Modern encryption protocols such as TLS¹³⁸ 1.3 and the Signal Protocol provide FS. For more information, see *Anonymous Planet*¹³⁹.

¹³¹youtube.com/watch?v=s22eJ1eVLTU&listen=false

¹³²open.oregonstate.edu/defenddissent/chapter/cryptographic-signing/

¹³³anarsec.guide/posts/tails-best/#appendix-gpg-explanation

¹³⁴anarsec.guide/glossary/#symmetric-cryptography

¹³⁵anarsec.guide/glossary/#public-key-cryptography

¹³⁶open.oregonstate.edu/defenddissent/chapter/what-is-encryption/

¹³⁷anarsec.guide/glossary/#man-in-the-middle-attack

¹³⁸anarsec.guide/glossary/#https

¹³⁹anonymousplanet.org/guide.html#forward-secrecy

Line Interface (CLI) allows us to do some things that a Graphical User Interface (GUI) does not. Often, either a GUI or a CLI would work, and which you use is a matter of preference. For example, in Tails¹²¹, you can verify the checksum¹²² of a file using either a GUI (the GtkHash program) or a CLI command (sha256sum).

For more information, see Linux Essentials¹²³. The Tech Learning Collective's «Foundations: Linux Journey» course on the command line¹²⁴ is our recommended introduction to using the CLI/terminal.

Correlation Attack

An end-to-end correlation attack is a theoretical way that a global adversary could break the anonymity of the Tor network¹²⁵. For more information, see Protecting against determined, skilled attackers¹²⁶ and Make Correlation Attacks More Difficult¹²⁷. For research papers on the subject, see Thirteen Years of Tor Attacks¹²⁸ and the design proposal on information leaks in Tor¹²⁹.

Digital Signatures

Digital signatures are based on public-key cryptography¹³⁰. A private key is used to digitally sign data, while the corresponding public key is used by third parties to verify the signature. Before a public key is used to verify a signature, its authenticity should be verified.

¹²¹anarsec.guide/glossary/#tails

¹²²anarsec.guide/glossary/#checksums-fingerprints

¹²³anarsec.guide/posts/linux/#the-command-line-interface

¹²⁴techlearningcollective.com/foundations/linux-journey/the-shell

¹²⁵anarsec.guide/glossary/#tor-network

¹²⁶anarsec.guide/posts/tails-best/#2-protecting-against-determined-skilled-attackers

¹²⁷anarsec.guide/posts/tails/#make-correlation-attacks-more-difficult

¹²⁸github.com/Attacks-on-Tor/Attacks-on-Tor#correlation-attacks

¹²⁹spec.torproject.org/proposals/344-protocol-info-leaks.html

¹³⁰anarsec.guide/glossary/#public-key-cryptography

- Поддерживайте ситуационную осведомленность и будьте готовы вытащить USB-накопитель Tails, чтобы выключить компьютер в любой момент. Очень сложно поддерживать адекватную ситуационную осведомленность, оставаясь сосредоточенным на сеансе Tails — подумайте о том, чтобы попросить близкого друга пообщаться с вами, который может посвятить себя присмотру за вашим окружением. Если USB-накопитель Tails извлечен, Tails выключится и перезапишет оперативную память случайными данными¹⁶. Все USB-накопители LUKS, которые были разблокированы в сеансе Tails, теперь будут снова зашифрованы. Обратите внимание, что Tails предупреждает¹⁷: «Физически извлекайте USB-накопитель только в случае чрезвычайной ситуации, так как это иногда может привести к поломке файловой системы постоянного хранилища».
- У одного человека, отвечающего за рынок даркнета, изъяли компьютер Tails, когда он отвлекся на фальшивую драку рядом с ним. Подобная тактика использовалась и в других полицейских операциях¹⁸. Если бы его USB-накопитель Tails был прикреплен к поясу с помощью короткого куска лески, полиция, скорее всего, потеряла бы все улики, когда USB-накопитель Tails был бы вытащен. Более техническим эквивалентом является BusKill¹⁹ — однако мы рекомендуем покупать его только лично или распечатывать на 3D-принтере²⁰. Это связано с тем, что любое письмо может быть перехвачено²¹ и изменено, что делает оборудование вредоносным²².

¹⁶tails.net/doc/advanced_topics/cold_boot_attacks/index.ru.html

¹⁷tails.net/doc/first_steps/shutdown/index.ru.html

¹⁸dys2p.com/en/2023-05-luks-security.html#attacks

¹⁹buskill.in/tails/

²⁰buskill.in/3d-print-2023-08/

²¹docs.buskill.in/buskill-app/en/stable/faq.html#q-what-about-interdiction

²²ru.wikipedia.org/wiki/BadUSB

Работа из личного пространства

Если вам нужно регулярно пользоваться Интернетом для таких проектов, как модерирование веб-сайта или взлом, то переход на новое место Wi-Fi после принятия контрмер наблюдения может быть нереалистичным на ежедневной основе. Кроме того, главным приоритетом полиции будет изъятие компьютера, пока он не зашифрован, и им гораздо проще этого добиться в общественном месте, особенно если вы одни. В этом сценарии идеальным смягчением является **использование антенны Wi-Fi, расположенной за окном в частном пространстве, для доступа с расстояния в несколько сотен метров** — физическое наблюдение не заметит, как вы входите в кафе, или не сможет легко изъять ваш включенный ноутбук, а цифровое наблюдение не заметит ничего в вашем домашнем Интернете. Чтобы защититься от скрытых камер²³, вам все равно следует быть осторожным с тем, где вы размещаете свой экран.

Если антенна Wi-Fi слишком техническая для вас, вы можете даже захотеть **использовать свой домашний интернет** для некоторых проектов, требующих частого доступа в интернет. Это противоречит предыдущему совету не использовать интернет-соединение, привязанное к вашей личности. Это компромисс: использование Tor из дома позволяет избежать создания физического следа, который так легко наблюдать, за счет создания цифрового следа, который более техничен для наблюдения и из которого может быть сложнее сделать осмысленные выводы. Существует два основных риска деанонимизации, которые следует учитывать при использовании домашнего интернета: что противник деанонимизирует вас с помощью атаки корреляции Tor или что он деанонимизирует вас, взломав вашу систему (например, с помощью фишинга²⁴) что позволяет им обойти Tor²⁵. Что-

²³notrace.how/earsandeyes

²⁴anarsec.guide/ru/posts/tails-best/#osvedomlennost-o-fishinge

²⁵anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists¹¹⁶.

See When to Use Tails vs. Qubes OS¹¹⁷. We do not offer «harm reduction» advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

Encrypted Messaging

See Encrypted Messaging for Anarchists¹¹⁸

Storing Electronic Devices

See Make Your Electronics Tamper-Evident¹¹⁹.

Приложение: Словарь

Asynchronous Communication

Unlike synchronous communication¹²⁰, both parties do not need to be online at the same time. This relies on some sort of server to store messages until the message recipients come online. This is the type of messaging that most people are familiar with (email, Signal, etc.).

Command Line Interface (CLI)

The «command line» is an all-text alternative to the graphical «point and click» tool that most of us are more familiar with; the Command

¹¹⁵anarsec.guide/posts/linux

¹¹⁶anarsec.guide/posts/qubes/

¹¹⁷anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

¹¹⁸anarsec.guide/posts/e2ee/

¹¹⁹anarsec.guide/posts/tamper/

¹²⁰anarsec.guide/glossary/#synchronous-communication

Your Phone

Operating system¹⁰⁷: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists¹⁰⁸. If you decide to have a phone, treat it like an «encrypted landline» and leave it at home when you are out of the house. See Kill the Cop in Your Pocket¹⁰⁹.

Your Computer

Operating system¹¹⁰: **Tails** is unparalleled for sensitive computer use (writing and sending communiques, moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network¹¹¹. See Tails for Anarchists¹¹² and Tails Best Practices¹¹³.

Operating system¹¹⁴: **Qubes OS** has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials¹¹⁵. Qubes OS

¹⁰⁷anarsec.guide/glossary#operating-system-os

¹⁰⁸anarsec.guide/posts/grapheneos/

¹⁰⁹anarsec.guide/posts/nophones/

¹¹⁰anarsec.guide/glossary#operating-system-os

¹¹¹anarsec.guide/glossary#tor-network

¹¹²anarsec.guide/posts/tails/

¹¹³anarsec.guide/posts/tails-best/

¹¹⁴anarsec.guide/glossary#operating-system-os

бы сделать обе эти атаки более сложными, мы рекомендуем подключаться к VPN *перед* подключением к Tor (т.е. Вы → VPN → Tor → Интернет²⁶) при использовании Tails из дома, что требует запуска VPN с вашего сетевого устройства (маршрутизатора или аппаратного брандмауэра). Более подробную информацию об обосновании см. Privacy Guides²⁷.

Подводя итог

Для деликатной и нерегулярной интернет-активности используйте интернет-подключение из случайного кафе, которому предшествует обнаружение слежки и антислежка. Для действий, требующих ежедневного доступа в Интернет, так что принятие мер противодействия слежке и поиск нового кафе нереальны, лучше всего использовать антенну Wi-Fi. Если это слишком технически для вас, то можно использовать домашний Wi-Fi, но для этого нужно доверять устойчивости Tor к корреляционным атакам, мерам, которые вы принимаете против взлома, и вашему VPN-провайдеру.

²⁶gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN#you-vpnssh-tor

²⁷privacyguides.org/ru/advanced/tor-overview/#safely-connecting-to-tor

Снижение рисков при использовании ненадежных компьютеров



Tails может безопасно работать на компьютере, на котором есть вирус. Но Tails не всегда может защитить вас, когда:

1. Установка с зараженного компьютера
2. Запуск Tails на компьютере с неисправной BIOS, прошивкой или оборудованием

1. Установка с зараженного компьютера

Эту первую проблему можно решить, **используя для установки Tails компьютер, которому вы доверяете:**

Теперь, когда мы знаем, что у нас есть подлинная версия файла Tails .img, мы можем приступить к его установке на USB-накопитель.

c tornet.biz¹⁰¹

Приложение: Рекомендации

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance¹⁰² for the purposes of incrimination¹⁰³ and network mapping¹⁰⁴. Our goal is to obscure the State's visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France¹⁰⁵: «So let's be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which "private or confidential words are spoken» and must remain so, even if it's switched off, we become a potential state informer..»

You may also be interested in the Threat Library's «Digital Best Practices»¹⁰⁶.

¹⁰¹tornet.biz/threads/luchshie-praktiki-tails.225/

¹⁰²notrace.how/threat-library/techniques/targeted-digital-surveillance.html

¹⁰³notrace.how/threat-library/tactics/incrimination.html

¹⁰⁴notrace.how/threat-library/techniques/network-mapping.html

¹⁰⁵actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/

¹⁰⁶notrace.how/threat-library/mitigations/digital-best-practices.html

- `gpg --gen-key` запросит у вас некоторые параметры конфигурации, а затем сгенерирует пару ключей.

Шаг: Проверьте открытый ключ Tails

- `gpg --import < tails-signing.key` импортирует открытый ключ Tails в вашу связку ключей, чтобы его можно было использовать.
- `gpg --keyring=/usr/share/keyrings/debian-keyring.gpg --export chris@chris-lamb.co.uk | gpg --import` импортирует открытый ключ разработчика Debian в вашу связку ключей, чтобы его можно было использовать.
- `gpg --keyid-format 0xlong --check-sigs A490D0F4D311A4153E2BB7CADBB802B258ACD84F` позволяет вам проверить открытый ключ Tails с открытым ключом разработчика Debian, проверив вывод в соответствии с инструкциями. Это делается для того, чтобы в случае компрометации источника открытого ключа Tails (tails.net) у вас был внешний источник истины, который вас предупредит.
- `gpg --lsign-key A490D0F4D311A4153E2BB7CADBB802B258ACD84F` сертифицирует открытый ключ Tails с помощью ключа, созданного вами на последнем шаге.

Теперь мы знаем, что у нас есть подлинная версия открытого ключа Tails. `gpg` также знает это, потому что мы решили сертифицировать его.

Шаг: Проверьте загруженный файл Tails .img

- `TZ=UTC gpg --no-options --keyid-format long --verify tails-amd64-6.1.img.sig tails-amd64-6.1.img` позволяет вам проверить, что файл `.img` подписан так, как и должно быть, проверив вывод в соответствии с инструкциями. Номера версий в команде изменятся.

- Согласно нашим рекомендациям (*rec*), в идеале это должна быть система Qubes OS²⁸, так как ее гораздо сложнее заразить, чем обычный компьютер Linux.
- Используйте метод установки «Terminal» «Debian or Ubuntu using the command line and GnuPG»²⁹, так как он более тщательно проверяет целостность загрузки с использованием GPG[†]. Если использование командной строки[†] для вас непонятно, изучите основы командной строки с помощью Linux Essentials³⁰ и см. Приложение ниже³¹.
- После установки не подключайте USB-накопитель Tails (или любые USB-накопители LUKS[†], используемые во время сеансов Tails) к другим компьютерам; если компьютер заражен, инфекция может распространиться на USB-накопитель³².

2. Запуск Tails на компьютере с поврежденным BIOS, прошивкой или оборудованием

Эта вторая проблема требует нескольких смягчений. Давайте начнем с нескольких определений.

- *Программное обеспечение* — это инструкции для компьютера, записанные в «коде».
- *Аппаратное обеспечение* — это физический компьютер, который вы используете.
- *Прошивка* — это низкоуровневое программное обеспечение, встроенное в часть оборудования; вы можете просто думать о нем как о связующем звене между оборудованием и высокоуровневым программным обеспечением операционной системы. Его можно найти в нескольких различных компонентах³³

²⁸anarsec.guide/posts/qubes/

²⁹tails.net/install/expert/index.ru.html

³⁰anarsec.guide/posts/linux/

³¹anarsec.guide/ru/posts/tails-best/#prilozhenie-obiasnenie-gpg

³²ru.wikipedia.org/wiki/BadUSB

(жесткие диски, USB-накопители, графический процессор и т. д.).

- BIOS — это специальная прошивка, встроенная в аппаратную часть «материнской платы» и отвечающая за загрузку компьютера при нажатии кнопки питания.

У наших противников есть две категории векторов атак: физические атаки[†] (через физический доступ) и удаленные атаки[†] (через удаленный доступ к Интернету). Противник с физическим доступом может скомпрометировать программное обеспечение (например, заменив операционную систему вредоносной версией), оборудование (например, добавив кейлоггер) и прошивку (например, заменив BIOS вредоносной версией). Противник с удаленным доступом начинает со взлома вас (компрометация программного обеспечения), а затем может перейти к компрометации прошивки.

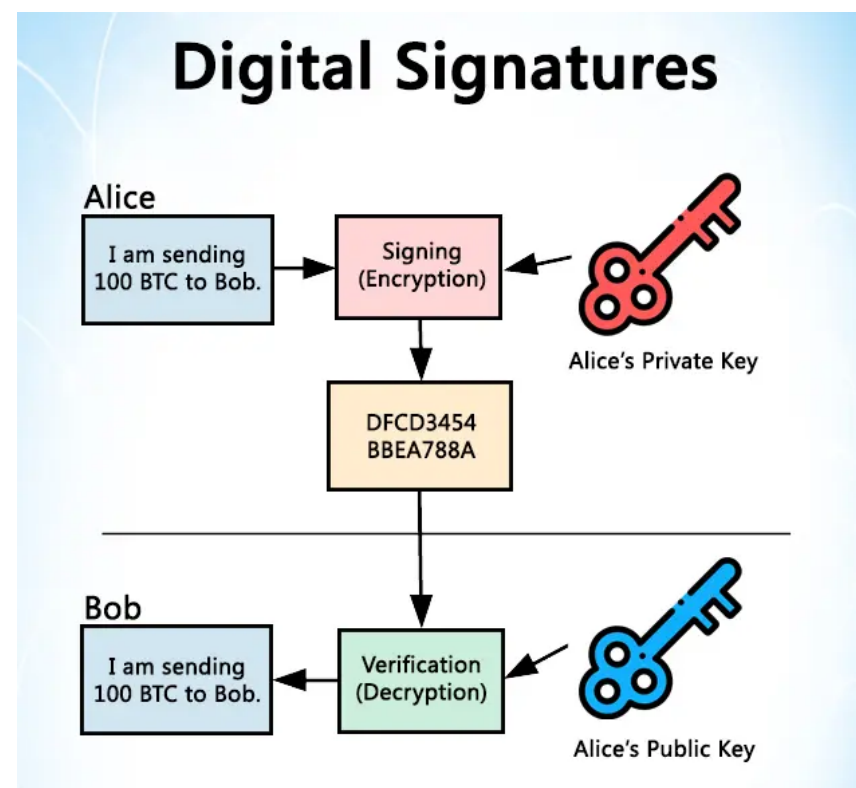
Если злоумышленник взломал аппаратное обеспечение или прошивку ноутбука, это также поставит под угрозу сеанс Tails, поскольку операционная система будет работать на вредоносной основе.

Не всем нужно применять все советы ниже. Например, если вы используете Tails только для анонимного просмотра веб-страниц и письменной переписки, некоторые из них могут оказаться излишними. Однако если вы используете Tails для подачи заявления о действиях, которые в высокой степени криминализированы, более тщательный подход, вероятно, будет уместен.

Для смягчения последствий физических атак:

- Во-первых, **купите новый компьютер**. Ноутбук из случайного восстановленного компьютерного магазина вряд ли уже скомпрометирован³⁴. Покупайте компьютер за наличные, что-

³³kicksecure.com/wiki/Firmware_Security_and_Updates#Firmware_on_Personal_Computers



Tails подписывает свои релизы, и только они могут это сделать, потому что только у них есть их закрытый ключ. Однако я могу проверить, что эта подпись действительна, имея копию их открытого ключа. Теперь я объясню gpgкоманды в инструкциях по проверке Tails⁹⁹.

Шаг: Генерация пары ключей

Tails рекомендует это руководство Riseup¹⁰⁰ для создания собственной пары ключей.

⁹⁹tails.net/install/expert/index.ru.html

¹⁰⁰riseup.net/en/security/message-security/openpgp/gpg-keys#using-the-linux-command-line

Использование `gpg` Tails во время установки будет менее запутанным, если вы поймете, как он работает.

Сначала немного пояснений. PGP и GPG[†] — это термины, которые можно использовать взаимозаменяемо; PGP (Pretty Good Privacy) — это стандарт шифрования, а GPG (GNU Privacy Guard) — это программа, которая его реализует. PGP/GPG также используется для зашифрованной электронной переписки⁹⁷), но мы используем его здесь только для проверки целостности и подлинности файлов.

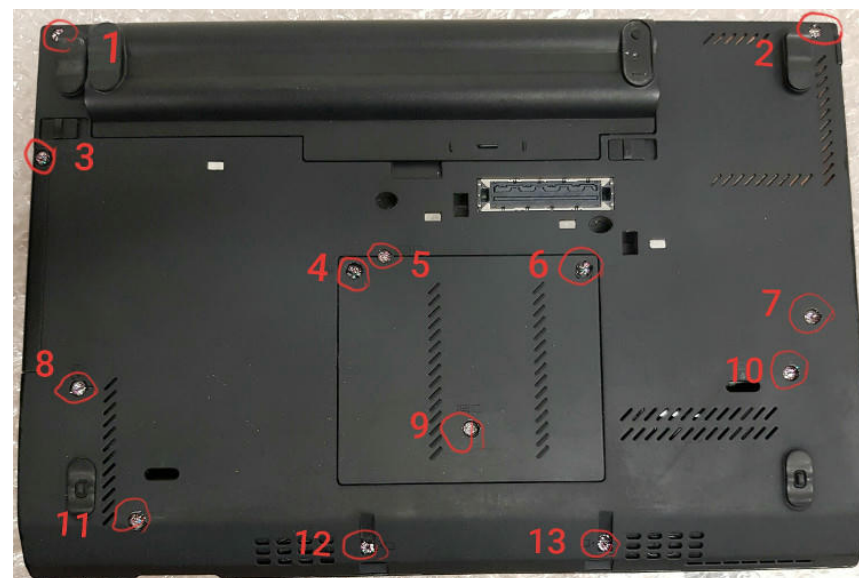
GPG — классический пример криптографии с открытым ключом[†]. GPG предоставляет криптографические функции для шифрования[†], дешифрования и подписи файлов; нас здесь интересует цифровая подпись файлов. Команда Tails подписывает цифровыми[†] подписями свои релизы `.img`. GPG дает нам возможность проверить, что файл действительно был «подписан» разработчиками, что позволяет нам быть уверенными в том, что он не был подделан.

Теперь вам нужно понять основы криптографии с открытым ключом. Это видео Computerphile⁹⁸ содержит отличный обзор с наглядными пособиями. Подводя итог, можно сказать, что для **подписи** сообщений используется **секретный/закрытый** ключ, и только пользователь, у которого есть этот ключ, может это сделать. Каждому **закрытому** ключу соответствует **открытый** ключ — это называется **парой ключей**. Открытый ключ передается всем и используется для проверки подписи.

⁹⁷anarsec.guide/posts/e2ee/#pgp-email

⁹⁸youtube.com/watch?v=GSIDS_lvRv4

бы его нельзя было отследить до вас, и лично, потому что почти можно перехватить — подержанный Thinkpad — дешевый и надежный вариант. Лучше всего использовать Tails с выделенным ноутбуком, что не позволит злоумышленнику нацелиться на прошивку через менее защищенную операционную систему или через ваши обычные неанонимные действия. Еще одна причина иметь выделенный ноутбук заключается в том, что если что-то в Tails сломается, любая информация, которая просочится и раскроет ноутбук, не будет автоматически связана с вами и вашей повседневной деятельностью на компьютере.



- Сделайте винты ноутбука защищенными от несанкционированного доступа, храните его в защищенном от несанкционированного доступа состоянии и следите за взломами. Приняв эти меры предосторожности, вы сможете обнаружить любые будущие физические атаки. Ознакомьтесь с руководством «Make Your Electronics Tamper-Evident»³⁵, чтобы

³⁴arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

адаптировать винты вашего ноутбука, используйте какую-либо форму обнаружения вторжений и храните ноутбук должным образом. Храните все внешние устройства, которые вы будете использовать с ноутбуком, таким же образом (USB, внешний жесткий диск, мышь, клавиатура). Когда физические векторы атак смягчены, злоумышленник может использовать только удаленные атаки.

Для защиты от удаленных атак:

- **Используйте Wi-Fi, не связанный с вашей личностью.** Мы рекомендуем это не только для защиты от деанонимизации, но и для защиты от взлома. Лучше никогда не использовать выделенный ноутбук Tails на вашем домашнем Wi-Fi. Это делает ноутбук гораздо менее доступным для удаленного злоумышленника, чем ноутбук, который регулярно подключен к вашему домашнему Wi-Fi. Злоумышленнику, нацелившемуся на вас, нужна отправная точка, и ваш домашний Wi-Fi — довольно хорошая точка.
- **Извлеките жесткий диск** — это проще, чем кажется. Если вы покупаете ноутбук, вы можете попросить магазин сделать это и потенциально сэкономить немного денег. Если вы ищете на YouTube «извлечь жесткий диск» для вашей конкретной модели ноутбука, вероятно, будет обучающее видео. Убедитесь, что вы извлекли аккумулятор ноутбука и отсоединили шнур питания. Мы извлекаем жесткий диск, чтобы полностью удалить прошивку жесткого диска, которая, как известно, была скомпрометирована хакерами³⁵. Жесткий диск является частью поверхности атаки, и он не нужен в рабочей системе, такой как Tails, которая работает с USB.
- Подумайте о том, **чтобы удалить интерфейс Bluetooth, камеру и микрофон**, хотя это более сложно — вам понадобится руководство пользователя для вашей модели ноутбука. Камеру

³⁵anarsec.guide/posts/tamper/

³⁶wired.com/2015/02/nsa-firmware-hacking/

Для синхронных[†] и асинхронных[†] сообщений мы рекомендуем Cwtch⁹³, если только это не анонимный публичный проект, в этом случае мы все равно рекомендуем PGP. Для получения дополнительной информации см. Encrypted Messaging For Anarchists⁹⁴.

В заключение

Использование Tails без этих советов все равно является огромным улучшением по сравнению со многими другими вариантами. Учитывая, что анархисты регулярно доверяют свою свободу Tails, принятие этих дополнительных мер предосторожности может еще больше укрепить ваше доверие к этой операционной системе.

Приложение: Объяснение GPG

Большинству пользователей Linux редко понадобится интерфейс командной строки⁹⁵. Если вы используете Tails, он вам вообще не понадобится, хотя для более безопасной установки⁹⁶ вам понадобятся следующие команды:

- `wget`: это позволяет загружать файлы из Интернета с помощью командной строки (а не веб-браузера)
- `gpg`: обрабатывает операции шифрования GPG[†]. Используется для проверки целостности и подлинности загрузки Tails.
- `apt`: управляет пакетами в Debian.
- `dd`: копирует файл с одного диска на другой.

⁹³anarsec.guide/posts/e2ee/#cwtch

⁹⁴anarsec.guide/posts/e2ee/

⁹⁵anarsec.guide/posts/linux/#the-command-line-interface

⁹⁶tails.net/install/expert/index.ru.html

- Вам будет предложено ввести пароль. Создайте новую запись в файле KeePassXC и сгенерируйте пароль с помощью функции «Сгенерировать пароль» (значок игральной кости).
- Для параметра «Путь к тому» выберите USB-накопитель «личные данные», который вы только что разблокировали.

Доступ к вашему зашифрованному тому

Когда вы захотите расшифровать том, нажмите «Монтировать том»:

- Это происходит автоматически при создании тома.
- Теперь вы можете добавлять файлы в смонтированный том: щелкните правой кнопкой мыши по тому и выберите «Открыть папку».
 - Вы можете проверить работу SiriKali, создав тестовый файл здесь. Этот файл будет отображаться в зашифрованном виде в каталоге cipher.
- Закончив, щелкните правой кнопкой мыши том и выберите «Отключить».

Прежде чем сохранять важные файлы в томе, следует провести тестирование, чтобы убедиться, что он работает так, как ожидается, особенно если вы используете его впервые.

Зашифрованная связь

Электронная почта PGP — наиболее устоявшаяся форма зашифрованной коммуникации на Tails в анархистском пространстве. К сожалению, PGP не имеет прямой секретности[†] — то есть, один секрет (ваш закрытый ключ) может расшифровать все сообщения, а не только одно сообщение, что является стандартом в зашифрованных сообщениях сегодня. Это противоположность «защите метаданных» и имеет несколько других недостатков⁹².

⁹²anarsec.guide/posts/e2ee/#pgp-email

можно, по крайней мере, «отключить», наклеив на нее наклейку. Микрофон часто подключается к материнской плате через разъем — в этом случае просто отключите его. Если это не очевидно или если разъема нет, так как кабель припаян непосредственно к материнской плате, или если разъем нужен для других целей, отрежьте кабель микрофона плоскогубцами. Тот же метод можно использовать для постоянного отключения камеры. Также можно использовать Tails на выделенном «офлайн» компьютере, удалив также сетевую карту. Некоторые ноутбуки имеют переключатели на корпусе, которые можно использовать для отключения беспроводных интерфейсов, но для «офлайн» компьютера предпочтительнее фактически удалить сетевую карту.

- **Установите целостность загрузки, заменив BIOS на Heads³⁷.** Исследователи безопасности продемонстрировали атаку³⁸ на прошивку BIOS пользователя Tails, что позволило им украсть ключи GPG и электронные письма. К сожалению, BIOS нельзя удалить, как жесткий диск. Он необходим для включения ноутбука, поэтому его необходимо заменить прошивкой с открытым исходным[†] кодом. Это сложный процесс, поскольку он требует открытия компьютера и использования специальных инструментов. Большинство анархистов не смогут сделать это самостоятельно, но, надеюсь, в ваших сетях найдется доверенный человек, который сможет настроить его для вас. Проект называется Heads, потому что это другая сторона Tails — где Tails защищает программное обеспечение, Heads защищает прошивку. Он имеет ту же цель, что и Verified Boot³⁹, найденный в GrapheneOS, который устанавливает полную цепочку доверия от оборудования. Heads имеет ограниченную совместимость⁴⁰, поэтому имейте это в виду при покупке ноутбука, если

³⁷osresearch.net/

³⁸youtube.com/watch?v=sNYsfUNegEA

³⁹privacyguides.org/ru/os/android-overview/#_2

⁴⁰osresearch.net/Prerequisites#supported-devices

вы планируете установить его — мы рекомендуем ThinkPad X230, потому что его установка менее сложна, чем у других моделей. Процессоры этого поколения способны эффективно удалять Intel Management Engine⁴¹ при перепрошивке Heads, но это не относится к более поздним поколениям процессоров на новых компьютерах. Heads можно настроить для проверки целостности и подлинности USB-накопителя Tails — см. документацию⁴², предотвращая его загрузку, если он был подделан. Heads защищает от физических и удаленных классов атак на прошивку BIOS и программное обеспечение операционной системы! Если Heads когда-либо обнаружит подделку, вы должны немедленно рассматривать устройство как ненадежное. Криминалистический анализ⁴³ может выявить, как произошла компрометация, что поможет предотвратить ее повторение. Вы можете связаться со службой, например, с горячая линия по цифровой безопасности Access Now⁴⁴, хотя мы рекомендуем не отправлять им никаких персональных данных.

- **Используйте USB-накопители с защищенной прошивкой**, например Kanguru FlashTrust⁴⁵, чтобы USB-накопитель перестал работать⁴⁶, если прошивка будет скомпрометирована. Kanguru имеет розничных продавцов по всему миру⁴⁷, что позволяет вам покупать их лично, чтобы избежать риска перехвата почты.

⁴¹en.wikipedia.org/wiki/Intel_Management_Engine#Assertions_that_ME_is_a_backdoor

⁴²osresearch.net/InstallingOS/#generic-os-installation

⁴³notrace.how/threat-library/mitigations/computer-and-mobile-forensics.html

⁴⁴accessnow.org/help

⁴⁵kanguru.com/products/kanguru-flashtrust-secure-firmware-usb-3-0-flash-drive

⁴⁶kanguru.com/blogs/gurublog/15235873-prevent-badusb-usb-firmware-protection-from-kanguru

⁴⁷kanguru.com/pages/where-to-buy

аутентификацию⁸⁷, поэтому второй уровень защиты с другой реализацией шифрования может быть полезен для особо конфиденциальных данных.

Установка SiriKali

SiriKali — это программа для зашифрованных томов, которая использует gocryptfs⁸⁸ за кулисами. Она доступна в репозитории Debian⁸⁹ и может быть легко установлена как дополнительное программное обеспечение⁹⁰. В Synaptic установите и sirikali, и gocryptfs (если вы чувствуете себя комфортно в командной строке[†], вы можете использовать gocryptfs напрямую, и вам на самом деле не нужен sirikali). Если вы не хотите переустанавливать SiriKali в каждом сеансе, вам нужно будет настроить Дополнительное программное обеспечение в Постоянном хранилище⁹¹.

Создание зашифрованного тома

При использовании SiriKali для создания тома будут созданы два новых каталога: «зашифрованный» каталог, в котором фактически хранятся зашифрованные файлы (VolumeName/ на вашем USB-накопителе с «персональными данными»), и «обычный» каталог, в котором вы получите доступ к расшифрованному тому после его монтирования (/home/amnesia/.SiriKali/VolumeName).

- Подключите USB-накопитель с «личными данными», на котором вы будете хранить этот зашифрованный том, и введите его парольную фразу LUKS.
- Затем в SiriKali нажмите «Создать том» и выберите опцию «gocryptfs».

⁸⁷notrace.how/threat-library/techniques/targeted-digital-surveillance/authentication-bypass.html

⁸⁸nuetzlich.net/gocryptfs/

⁸⁹packages.debian.org/bookworm/sirikali

⁹⁰anarsec.guide/ru/posts/tails/#ustanovka-dopolnitel-nogo-programmnogo-obespecheniia

⁹¹anarsec.guide/ru/posts/tails-best/#razblokirovka-perekliuchatelja

них нечасто. Чтобы снизить риск того, что вы навсегда забудете пароль Diceware, вы можете использовать Tails для хранения всех «запомненных» паролей на USB-накопителе LUKS, а затем хранить его вне места, где его не смогут найти во время полицейского рейда. Вы должны быть в состоянии восстановить пароль LUKS этого USB-накопителя, если прошло много времени. См. Библиотеку угроз⁸⁶ для двух различных подходов, которые вы можете использовать: один полагается на доверенного товарища, а другой является самодостаточным. Как и в случае со всеми важными резервными копиями, у вас должно быть как минимум два.

Парольные фразы Tails

Для Tails вам необходимо запомнить две парольные фразы:

- 1) Парольная фраза USB- накопителя «персональных данных» LUKS[†], где хранится ваш файл KeePassXC.
- 2) Парольная фраза KeePassXC

Если вы используете постоянное хранилище, это еще одна парольная фраза, которую вам придется ввести на экране приветствия во время загрузки, но она может быть такой же, как пароль LUKS. Выключайте Tails всякий раз, когда вы уходите от компьютера более чем на несколько минут.

Зашифрованные тома

LUKS[†] — это здорово, но глубокая защита не повредит. Если полиция конфискует ваш USB-накопитель во время обыска дома, они попробуют использовать различные тактики, чтобы обойти

⁸⁶notrace.how/threat-library/mitigations/digital-best-practices.html#header-use-strong-passwords



- Запустите Tails с USB-накопителя с физическим переключателем защиты от записи..

Использование переключателя защиты от записи

Что такое переключатель *защиты от записи* ? Когда вы вставляете обычный USB в компьютер, компьютер выполняет операции *чтения* и *записи* с ним, а операция *записи* может изменить данные на USB. Некоторые специ-

альные USB, разработанные для анализа вредоносных программ, имеют физический переключатель, который может заблокировать USB, так что данные могут быть прочитаны с него, но никакие новые данные не могут быть записаны на него.

Если на вашем USB-накопителе Tails есть переключатель защиты от записи, такой как Kanguru FlashTrust⁴⁸, когда переключатель заблокирован, вы защищены от злоумышленника, скомпрометировавшего программное обеспечение Tails, хранящееся на USB-накопителе. Это критически важно. Чтобы скомпрометировать ваш USB-накопитель Tails, злоумышленнику необходимо иметь возможность записывать на него. Это означает, что даже если сеанс Tails заражен вредоносным ПО, ваш USB-накопитель Tails неизменяем, поэтому компрометация не может быть перенесена на последующие сеансы Tails («устойчивость вредоносного ПО») путем изменения файлов операционной системы. Единственный другой способ установить «устойчивость вредоносного ПО» — это компрометация прошивки, которую вы уже смягчили.

Обратите внимание, что прошивка Heads делает переключатель защиты от записи ненужным, поскольку его можно настроить на проверку целостности и подлинности USB-накопителя Tails перед загрузкой⁴⁹.

Если вы не используете Heads и не можете приобрести USB-накопитель с переключателем защиты от записи, у вас есть три варианта.

- 1) Установите Tails на SD-карту и используйте адаптер USB 3.0 для SD-карты, поскольку SD-карты оснащены переключателем защиты от записи.

⁴⁸kanguru.com/products/kanguru-flashttrust-secure-firmware-usb-3-0-flash-drive

⁴⁹osresearch.net/InstallingOS/#generic-os-installation

Что такое парольная фраза Diceware? Как отмечает Privacy Guides⁸⁴, «парольные фразы Diceware являются отличным вариантом, когда вам нужно запомнить или вручную ввести свои учетные данные, например, главный пароль вашего менеджера паролей или пароль шифрования вашего устройства. Примером парольной фразы Diceware является viewable fastness reluctant squishy seventeen shown pencil». Функция генератора паролей в KeePassXC может генерировать парольные фразы Diceware и случайные пароли. Если вы предпочитаете генерировать парольные фразы Diceware с использованием настоящих игральные костей, см. Privacy Guides⁸⁵.

Общие рекомендации

- Запомните парольные фразы Diceware из 7–10 слов для всего, что вам нужно будет ввести, прежде чем вы получите доступ к разблокированной базе данных KeePassXC (другими словами, парольную фразу для полного шифрования диска и главную парольную фразу KeePassXC).
- Сгенерируйте пароли из 21 случайного символа для всего, что может храниться в базе данных KeePassXC. Сохраняйте резервную копию вашей базы данных KeePassXC вне офиса на случай, если она будет повреждена или изъята.

Кончик

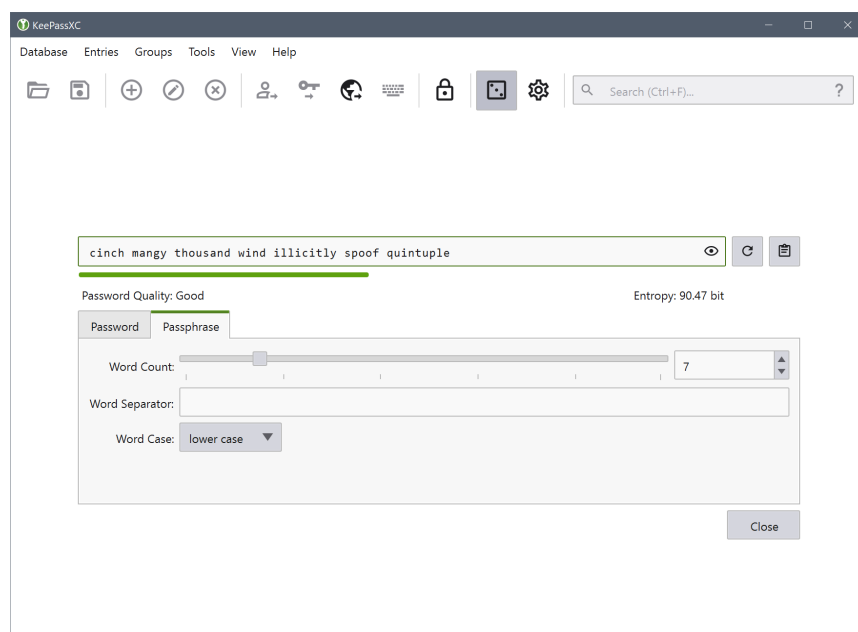
Ваши запомненные пароли Diceware могут легко забыться, если у вас есть несколько, за которыми нужно следить, особенно если вы используете какие-либо из

⁸⁴privacyguides.org/ru/basics/passwords-overview/#_7

⁸⁵privacyguides.org/ru/basics/passwords-overview/#_7

объемов облачных вычислений⁷⁹. Новая версия LUKS (LUKS2 с использованием Argon2id) менее уязвима для атак методом подбора пароля⁸⁰ — это значение по умолчанию для Tails 6.0 и Qubes OS 4.1. Если вы хотите узнать больше об этом изменении, мы рекомендуем обзор Systemli⁸¹ или dys2p⁸².

Надежность пароля измеряется в «битах энтропии»⁸³. Ваши пароли/парольные фразы в идеале должны иметь энтропию около 128 бит (парольные фразы Diceware из **десяти слов** или пароль из **21 случайного символа**, включая заглавные, строчные буквы, цифры и символы) и не должны иметь менее 90 бит энтропии (парольные фразы Diceware из семи слов).



⁷⁹blog.elcomsoft.com/2020/08/breaking-luks-encryption/

⁸⁰mjb59.dreamwidth.org/66429.html

⁸¹systemli.org/en/2023/04/30/is-linux-hard-disk-encryption-hacked/

⁸²dys2p.com/en/2023-05-luks-security.html

⁸³[en.wikipedia.org/wiki/](https://en.wikipedia.org/wiki/Password_strength#Entropy_as_a_measure_of_password_strength)

[Password_strength#Entropy_as_a_measure_of_password_strength](https://en.wikipedia.org/wiki/Password_strength#Entropy_as_a_measure_of_password_strength)

- 2) Записывайте Tails на новый DVD-R/DVD+R⁵⁰ (записывайте один раз) для каждой новой версии Tails — это довольно неудобно. Не используйте DVD с маркировкой «DVD+RW» или «DVD+RAM», которые можно перезаписать.
- 3) Загрузите Tails с `toram` опцией, которая полностью загружает Tails в память. Извлеките USB-накопитель Tails в начале сеанса, прежде чем что-либо делать (будь то подключение к Интернету или подключение другого USB-накопителя), а затем используйте Tails как обычно. То, как вы используете `toram` опцию, зависит от того, загружается ли ваш USB-накопитель Tails с помощью SYSLINUX или GRUB⁵¹.
 - Для SYSLINUX, когда появится экран загрузки, нажмите Tab и введите пробел. Введите `toram` и нажмите Enter.
 - Для GRUB, когда появится экран загрузки, нажмите e и используйте стрелки клавиатуры, чтобы перейти к концу строки, которая начинается с `linux`. Строка, вероятно, перенесена и отображается в несколько строк, но это одна строка конфигурации. Введите `toram` и нажмите F10 или Ctrl+X.

Разблокировка переключателя

На USB с переключателем защиты от записи вы не сможете вносить какие-либо изменения в Tails USB, когда переключатель заблокирован. Если вы можете вносить изменения, то и вредоносное ПО может. Есть только два случая, когда переключатель должен быть разблокирован:

1. Для специального сеанса обновления.

Если вам нужно обновить Tails, вы можете сделать это в специальном сеансе с разблокированным переключателем — это необходимо, поскольку обновление должно быть записано на USB-на-

⁵⁰tails.net/install/dvd/index.ru.html

⁵¹tails.net/doc/advanced_topics/boot_options/index.ru.html

копитель Tails. После того, как вы закончите, вам следует перезапустить Tails с заблокированным переключателем.

2. Для выделенного сеанса настройки, если вы решили использовать постоянное хранилище.

Persistent Storage⁵² — это функция Tails, которая позволяет переносить данные между сеансами, которые в противном случае были бы амнезией, сохраняя данные на самом USB-накопителе Tails. Поскольку Persistent Storage требует записи на USB-накопитель Tails, его обычно непрактично использовать с переключателем защиты от записи. Альтернативой переключателю защиты от записи является использование Heads — Heads проверяет подлинность и целостность USB-накопителя Tails с помощью цифровой подписи при загрузке, и это делает запись на USB-накопитель Tails безопасной, поэтому Persistent Storage будет работать так, как и ожидалось.

Еще одна причина избегать использования функций постоянного хранения заключается в том, что многие из них хранят персональные данные на USB-накопителе Tails. Если ваш сеанс Tails скомпрометирован, данные, к которым вы получаете доступ во время этого сеанса, могут быть использованы для связывания ваших действий. Если на USB-накопителе Tails есть персональные данные, такие как почтовый ящик электронной почты, разделение сеансов Tails больше невозможно, *когда постоянное хранилище разблокировано*. Чтобы добиться разделения с разблокированным постоянным хранилищем, вам понадобится выделенный USB-накопитель Tails для каждой личности, и обновление их всех каждый месяц будет большой работой.

Однако вы можете захотеть использовать некоторые функции Persistent Storage, которые не хранят персональные данные, например, дополнительную функцию программного обеспечения.

⁵²anarsec.guide/ru/posts/tails/#neobiazatel-no-sozдание-i-nastroika-postoiannogo-khranilishcha

Вот почему важно **использовать в браузере Tor Browser настройку безопасности «Наиболее безопасный»**⁷⁷ по умолчанию, даже для «доверенных» веб-сайтов, чтобы значительно снизить риск успешной атаки вредоносного ПО на браузер Tor.

Шифрование

Пароли

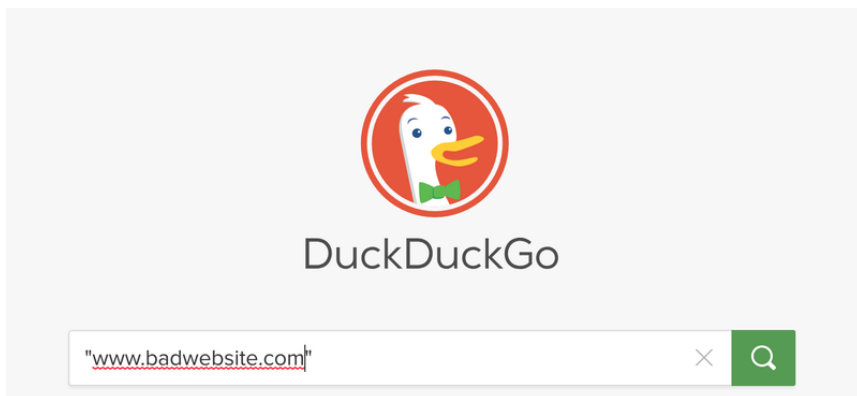
Шифрование[†] — единственное, что стоит на пути наших злоумышленников к чтению всех наших данных, если оно используется правильно. Первый шаг к обеспечению безопасности вашего шифрования — убедиться, что вы используете очень надежные пароли — большинство паролей не нужно запоминать, поскольку они хранятся в менеджере паролей KeePassXC, поэтому они могут быть абсолютно случайными. Никогда не используйте пароль повторно для нескольких целей («рециркуляция паролей») — KeePassXC упрощает хранение уникальных паролей, предназначенных для одной цели. Чтобы узнать, как использовать KeePassXC, см. Менеджер паролей⁷⁸.

В терминологии KeePassXC *пароль*[†] — это случайная последовательность символов (букв, цифр и других символов), а *парольная фраза*[†] — это случайная последовательность слов.

Шифрование LUKS[†] **эффективно только тогда, когда устройство выключено** — когда устройство включено, пароль можно извлечь из памяти. Злоумышленники могут попытаться провести атаку методом подбора пароля с использованием огромных

⁷⁷anarsec.guide/ru/posts/tails/#tor

⁷⁸anarsec.guide/ru/posts/tails/#menedzher-parolei-keepassxc



- **Не вводите никакую идентификационную информацию на веб-сайте.** Если вы переходите по ссылке из электронного письма и вас просят войти в систему, знайте, что это обычная концовка фишинговых кампаний. Вместо этого вручную перейдите на веб-сайт службы, к которой вы пытаетесь получить доступ, и войдите там. Таким образом, вы будете знать, что входите на нужный веб-сайт, поскольку вы сами ввели адрес, а не доверять ссылке в электронном письме.

Атаки на водопой

Злоумышленник также может скомпрометировать «доверенный» веб-сайт — это позволяет ему устанавливать вредоносное ПО на компьютеры любого, кто посещает веб-сайт, без необходимости заниматься фишингом. Это называется «атакой watering hole» или «компрометацией drive-by»⁷⁵, потому что она атакует многих людей одновременно. Например, ФБР взломало веб-сайт, а затем использовало эксплойт Tor Browser⁷⁶, чтобы взломать 8000 пользователей, которые его посетили.

⁷⁵attack.mitre.org/techniques/T1189/

⁷⁶[vice.com/en/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant](https://www.vice.com/en/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant)

Для этого требуется разблокировать переключатель для выделенного сеанса конфигурации Persistent Storage:

- Запустите «разблокированный» сеанс, создайте постоянное хранилище⁵³ с включенным дополнительным программным обеспечением, установите дополнительное программное обеспечение⁵⁴ и выберите «Устанавливать каждый раз» при появлении соответствующего запроса.
- Теперь, когда настройка завершена, перезапустите Tails в «заблокированном» сеансе, прежде чем фактически использовать программное обеспечение. Не устанавливайте пароль администратора, который требуется только во время первоначальной установки. В «заблокированном» сеансе ни один из файлов, с которыми вы работаете, не сохраняется на USB-накопителе Tails, поскольку он «заблокирован», но теперь дополнительное программное обеспечение настроено на установку каждый раз, когда вы вводите пароль постоянного хранилища на экране приветствия. Чтобы иметь «заблокированный» сеанс с постоянным хранилищем, переключатель USB необходимо перевести в положение «только чтение» *после* получения уведомления «Дополнительное программное обеспечение успешно установлено» (и до подключения к Интернету).

Функция постоянного хранения недоступна при использовании DVD или toram варианта загрузки.

USB-накопители с персональными данными

Где мы можем хранить персональные данные для использования между сеансами Tails, если переключатель защиты от записи не позволяет нам использовать постоянное хранилище? Мы реко-

⁵³anarsec.guide/ru/posts/tails/#neobiazatel-no-sozdanie-i-nastroika-postoiannogo-khranilishcha

⁵⁴anarsec.guide/ru/posts/tails/#ustanovka-dopolnitel-nogo-programmnogo-obespecheniia

мендуем хранить персональные данные на втором USB-накопителе LUKS. Этот USB-накопитель с «персональными данными» не должен выглядеть идентично USB-накопителю Tails, чтобы избежать путаницы. Чтобы создать этот отдельный USB-накопитель, см. [How to create an encrypted USB](#)⁵⁵. Если вы читаете это из такой страны, как Великобритания, где непредоставление паролей шифрования может привести вас в тюрьму, этот второй диск должен быть жестким диском, содержащим скрытый том Veracrypt⁵⁶ (накопители SSD и USB не подходят для скрытых томов⁵⁷).

Подход к компартиментализации, обсуждавшийся выше⁵⁸, аккуратно разделяет разные личности, используя отдельные сеансы Tails для отдельных видов деятельности — например, в сеансе Tails № 1 вы занимаетесь модерацией веб-сайта, а в сеансе Tails № 2 вы занимаетесь исследовательской деятельностью. Этот подход имеет последствия для того, как вы организуете свои USB-накопители «персональных данных». Если сохраняемые вами файлы могут использоваться для связывания ваших видов деятельности, используйте разные USB-накопители «персональных данных» для каждого вида деятельности.

⁵⁵anarsec.guide/ru/posts/tails/#kak-sozdat-zashifrovannyi-usb

⁵⁶veracrypt.fr/en/Hidden%20Volume.html

⁵⁷veracrypt.fr/en/Trim%20Operation.html

⁵⁸anarsec.guide/ru/posts/tails-best/#2-ispol-zovanie-tails-dlia-bolee-chem-odnoit-seli-odnovremenno

ми данными». Вы можете поместить ссылку на Riseup Pad, чтобы получить к ней доступ.

- **Используйте Tor Browser с настройкой Safest**⁷²! Подавляющее большинство эксплойтов против Tor Browser не будут работать с настройкой Safest.
- **Скопируйте и вставьте адрес вручную в браузер и повторно введите домен**. Например, после вставки ссылки `anarsec.guide/posts/tails` повторно введите `anarsec.guide` себя. Не переходите по гиперссылке (т. е. всегда копируйте и вставляйте), так как это может ввести вас в заблуждение относительно того, куда вы направляетесь. Повторный ввод домена защищает от «типосквоттинга» (`mailriseup.net` вместо `mail.riseup.net`), а также от «омографических атак»⁷³ (когда кириллические буквы заменяются обычными буквами).
- **Никогда не переходите по сокращенной ссылке** (например, сайт типа `bit.ly`, который берет длинные веб-адреса и делает короткие), потому что их невозможно проверить перед перенаправлением. `Unshorten.me`⁷⁴ может раскрыть сокращенные ссылки.
- **Если вы не узнаете домен, исследуйте его**. Найдите домен с доменным именем в кавычках, используя поисковую систему, сохраняющую конфиденциальность (например, `DuckDuckGo`), чтобы узнать, является ли это законным веб-сайтом. Это не надежное решение, но это хорошая мера предосторожности.

⁷²anarsec.guide/ru/posts/tails/#tor

⁷³theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers

⁷⁴unshorten.me/

Файлы

В 2017 году ФБР и Facebook совместно разработали вредоносный видеофайл, который деанонимизировал пользователя Tails⁶⁸ после того, как он открыл его, используя домашний Wi-Fi.

Для ненадежных вложений вам в идеале следует использовать Dangerzone⁶⁹ для **очистки всех отправленных вам файлов перед их открытием**. Dangerzone берет ненадежные PDF-файлы, офисные документы или изображения и превращает их в надежные PDF-файлы. Ознакомьтесь с документацией⁷⁰ по установке Dangerzone на Tails — к сожалению, в настоящее время для этого требуется использовать командную строку[†].

Если вы не используете Dangerzone, **лучше всего открывать ненадежные файлы в выделенном сеансе Tails «офлайн-режима»**⁷¹. Это предотвратит выполнение кода от установления удаленного соединения с противником, что обычно необходимо для продолжения атаки. Немедленное завершение сеанса после этого минимизирует вероятность сохранения вредоносного ПО. Однако, если вы не используете Dangerzone для очистки файлов, они останутся ненадежными.

Ссылки

При использовании ненадежных ссылок вам необходимо защитить две вещи: свою анонимность и свою информацию.

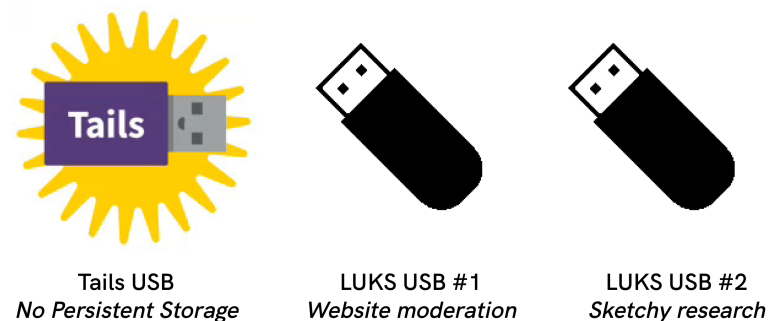
- **Лучше всего открывать ненадежные ссылки в выделенном сеансе Tails без разблокированного постоянного хранилища или подключенных USB-накопителей с «личными данными»**

⁶⁸[vice.com/en/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez](https://www.vice.com/en/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez)

⁶⁹dangerzone.rocks/

⁷⁰tails.net/doc/persistent_storage/additional_software/dangerzone/index.ru.html

⁷¹tails.net/doc/first_steps/welcome_screen/index.ru.html#index3h2



Если USB-накопитель с «личными данными» используется для сохранения очень конфиденциальных файлов (например, текста коммюнике), лучше всего перезаписать и уничтожить USB-накопитель, как только файлы вам больше не понадобятся (см. [Really delete data from a USB drive](#)⁵⁹). Это еще одна причина использовать отдельный USB-накопитель для любых файлов, которые необходимо сохранить — вы не накапливаете криминалистическую историю всех своих файлов в своем постоянном хранилище Tails, и вы можете легко уничтожить эти USB-накопители с «личными данными» по мере необходимости.

Если вы уже используете Tails и зашифрованную электронную почту, вы, возможно, знакомы с функцией постоянного хранилища Thunderbird для вашего почтового ящика и ключей PGP. Эта функция не будет работать при включенном переключателе защиты от записи. Вместо использования постоянного хранилища для электронной почты просто войдите в Thunderbird с помощью IMAP в каждом новом сеансе. Ключи PGP можно хранить на USB-накопителе «персональных данных», как и любой другой файл, и импортировать при необходимости с помощью «Диспетчера ключей OpenPGP» Thunderbird (Файл → Импортировать откры-

⁵⁹anarsec.guide/ru/posts/tails/#real-no-udalit-dannye-s-usb

тый ключ(и) из файла / Импортировать секретный ключ(и) из файла). Преимущество такого подхода в том, что если правоохранительным органам удастся обойти LUKS, они все равно не получат доступ к вашему почтовому ящику, не зная пароля вашей электронной почты.

Осведомленность о фишинге

Давайте вернемся к теме того, как злоумышленник будет проводить удаленную атаку[†], нацеленную на вас или ваш проект с целью взлома; ответ, скорее всего, «фишинг»[†]. *Фишинг* — это когда злоумышленник создает электронное письмо (или сообщение в приложении), чтобы обманом заставить вас раскрыть информацию или внедрить вредоносное ПО на ваш компьютер. *Целевой фишинг*[†] — это когда злоумышленник провел некоторую разведку и использует уже известную ему информацию о вас, чтобы адаптировать свою фишинговую атаку.

Фишинг работает только в том случае, если у злоумышленника есть способ отправить вам сообщение: вам не нужно беспокоиться об этом векторе атаки для таких действий, как отправка коммюнике или проведение исследований действий, но он актуален для проектов, ориентированных на общественность, которые имеют канал связи. Имейте в виду, что поле «от» в электронных письмах может быть подделано, чтобы обмануть вас — подпись PGP⁶⁰ смягчает это, доказывая, что электронное письмо действительно от того, от кого вы ожидаете его получить.

Вы, вероятно, слышали совет скептически относиться к переходу по ссылкам и открытию вложений — вот почему. Успех фишинга зависит от ваших действий, поэтому ваша осведомленность — лучшая защита.

⁶⁰anarsec.guide/posts/e2ee/#pgp-email

Вредоносный файл или ссылка работает, выполняя код⁶¹ на вашем компьютере. Для вредоносных файлов код выполняется при открытии файла. Для вредоносных ссылок код выполняется при посещении веб-сайта, обычно с помощью JavaScript. Цель выполнения этого кода — предоставить точку входа («начальный доступ») для заражения вашего компьютера вредоносным ПО.

Tails защищает от вредоносного ПО, деанонимизирующего вас, принудительно направляя все интернет-соединения через сеть Tor. Однако, как только противник получит «начальный доступ», он попытается продолжить свою атаку;

- чтобы сделать инфекцию стойкой,⁶²
- установить экран или кейлоггер,⁶³
- чтобы извлечь ваши данные,⁶⁴
- для достижения «повышения привилегий»⁶⁵

Повышение привилегий (т.е. переход от непривилегированного пользователя к администратору в системе) обычно необходимо для обхода Tor. Tails не имеет пароля администратора по умолчанию (его нужно установить на экране приветствия сеанса, если необходимо), чтобы затруднить «повышение привилегий».

Последний аудит Tails⁶⁶ обнаружил несколько «уязвимостей повышения привилегий» и даже уязвимость, которая выдавала IP-адрес непривилегированного пользователя. Если устойчивость к атакам вредоносного ПО является важной частью вашей модели угроз, см. [When to Use Tails vs. Qubes OS](#)⁶⁷.

⁶¹en.wikipedia.org/wiki/Arbitrary_code_execution

⁶²attack.mitre.org/tactics/TA0003/

⁶³attack.mitre.org/tactics/TA0009/

⁶⁴attack.mitre.org/tactics/TA0010/

⁶⁵en.wikipedia.org/wiki/Privilege_escalation

⁶⁶tails.net/news/audit_by_ROS/index.en.html

⁶⁷anarsec.guide/posts/qubes#when-to-use-tails-vs-qubes-os