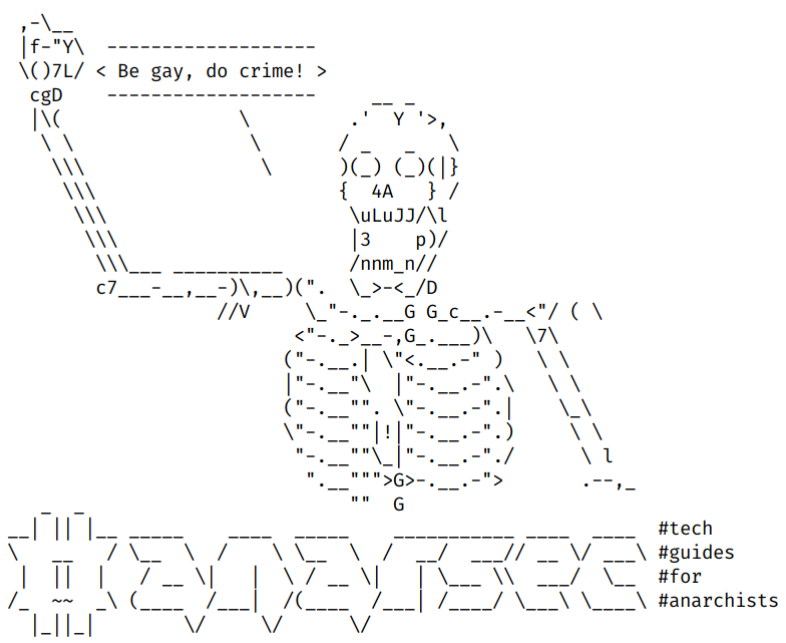
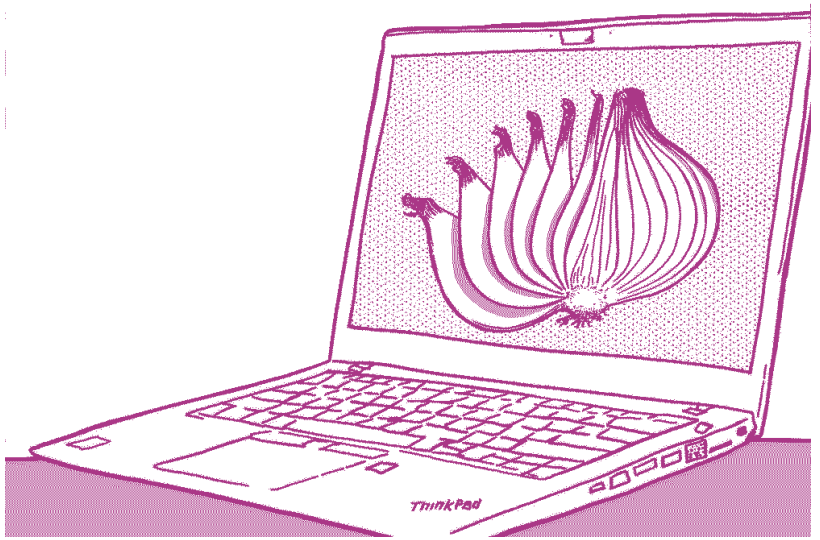
Все анархисты должны знать, как использовать Tails — в этом тексте описываются некоторые дополнительные меры предосторожности, которые вы можете предпринять, и которые имеют отношение к модели анархистской угрозы. Не все модели анархистской угрозы одинаковы, и только вы можете решить, какие меры по смягчению 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 анархистов.



Лучшие практики Tails



Серии: Защита

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.

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 твоем 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

Содержание

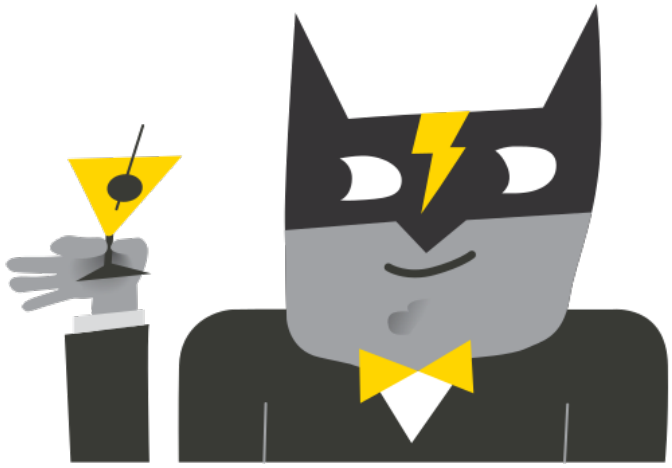
Защита вашей личности при использовании Tails 5
1. Обмен файлами с метаданными 6
2. Использование Tails для более чем одной цели одновременно 6
Ограничения сети Tor 7
1. Скрытие факта использования Tor и Tails 8
2. Защита от решительных и опытных нападающих 8
Снижение рисков при использовании ненадежных компьютеров 16
1. Установка с зараженного компьютера 16
2. Запуск Tails на компьютере с поврежденным BIOS, прошивкой 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 водопои 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 45
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 анархистов[1].

Начнем с рассмотрения трех тем, затронутых на странице предупреждений Tails[2]: защита вашей личности, ограничения сети Tor и ненадежные компьютеры.

Защита вашей личности при использовании Tails



[1] anarsec.guide/ru/posts/tails/
[2] tails.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 Files[3].

2. Использование Tails для более чем одной цели одновременно

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

- Разделение[4] 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.

[3] anarsec.guide/posts/metadata/
[4] notrace.how/threat-library/mitigations/compartmentalization.html

Tor network

Tor[178] (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 Tails[179] operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists[180] and Privacy Guides[181]. To understand the limitations of Tor, see the Whonix documentation[182].

[178] torproject.org/
[179] anarsec.guide/glossary/#tails
[180] anarsec.guide/posts/tails/#tor
[181] privacyguides.org/en/advanced/tor-overview/
[182] whonix.org/wiki/Warning

Spear phishing

Spear phishing is more sophisticated than regular phishing[170], 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 communication[171], 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 goals[172], and vulnerabilities[173], 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 attack[174]) 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 Library[175], Defend Dissent: Digital Threats to Social Movements[176] and Defending against Surveillance and Suppression[177].

[170] anarsec.guide/glossary/#phishing
[171] anarsec.guide/glossary/#asynchronous-communication
[172] anarsec.guide/glossary/#security-goal
[173] anarsec.guide/glossary/#vulnerability
[174] anarsec.guide/glossary/#ddos-attack
[175] notrace.how/threat-library/
[176] open.oregonstate.education/defenddissent/chapter/digital-threats/
[177] open.oregonstate.education/defenddissent/chapter/surveillance-and-suppression/

- Чтобы не дать злоумышленнику связать ваши действия при использовании Tails, перезапускайте Tails между различными 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 модерирования 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 ниже[5].

Ограничения сети Tor

[5] anarsec.guide/ru/posts/tails-best/#ispol-zovanie-perekliuchatelia-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

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

used for 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 attacks[163].

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 signatures[164].

To learn more, watch this video[165], or for a more detailed look, see Defend Dissent: Public-Key Cryptography[166].

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 malware[167] 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 attack[168].

For a more detailed look, see Defend Dissent: Protecting Your Devices[169].

[163] anarsec.guide/glossary/#man-in-the-middle-attack
[164] anarsec.guide/glossary/#digital-signatures
[165] youtube.com/watch?v=GSIDS_lvRv4
[166] open.oregonstate.education/defenddissent/chapter/public-key-cryptography/
[167] anarsec.guide/glossary/#malware
[168] anarsec.guide/glossary/#physical-attacks
[169] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/

Phishing

Phishing is a technique of social engineering[153]. 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 malware[154] onto a system, which can be used as a starting point for hacking. Spear phishing[155] is a more sophisticated form of phishing. For more information, see the Kicksecure documentation[156].

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 attack[157].

For more information, see Making Your Electronics Tamper-Evident[158], the Threat Library[159], the KickSecure documentation[160], and Defend Dissent: Protecting Your Devices[161].

Public-key cryptography

Public-key cryptography (or asymmetric cryptography) is the opposite of symmetric cryptography[162]. Each party has two keys (public and private). The private key must be kept secret and is

[153] anarsec.guide/glossary/#social-engineering
[154] anarsec.guide/glossary/#malware
[155] anarsec.guide/glossary/#spear-phishing
[156] kicksecure.com/wiki/Social_Engineering
[157] anarsec.guide/glossary/#remote-attacks
[158] anarsec.guide/posts/tamper
[159] notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html
[160] kicksecure.com/wiki/Protection_Against_Physical_Attacks
[161] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/
[162] anarsec.guide/glossary/#symmetric-cryptography

> сети Tor, может быть в состоянии деанонимизировать пользователей Tor. Эти атаки называются атаками *сквозной корреляции* , потому что злоумышленник должен наблюдать оба конца цепи Tor одновременно. […] Атаки сквозной корреляции изучались в исследовательских работах, но мы не знаем ни об одном фактическом использовании для деанонимизации пользователей Tor.

Нецелевые и целевые корреляционные атаки

Как описано в приведенной выше цитате, глобальный противник (то есть АНБ) может взломать Tor 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 Tor, 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 Tor».

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 наблюдения[7] и/или цифрового наблюдения[8]. Это подтип корреляционной атаки, когда предполагаемая

[7] notrace.how/threat-library/techniques/physical-surveillance/covert.html
[8] notrace.how/threat-library/techniques/targeted-digital-surveillance.html

цель уже известна, что делает атаку более легкой для достижения, поскольку это значительно сокращает объем данных для фильтрации для корреляции. Нецелевая корреляционная атака, используемая для деанонимизации пользователя Tor, является беспрецедентной в текущих доказательствах, используемых в суде, хотя «целевая» корреляционная атака использовалась в качестве подтверждающего доказательства[9] — 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 EFF[10]. 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).

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

[10] eff.org/pages/tor-and-https

people to 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 Files[149] and Defend Dissent: Metadata[150].

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 password[151], 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: Passwords[152]

[149] anarsec.guide/posts/metadata

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

[151] anarsec.guide/glossary/#password

[152] open.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 cryptography[140]. When used with email, metadata[141] (such as email addresses) remains unencrypted. It does not provide forward secrecy[142].

For more information, see this primer[143]. We don't recommend it for encrypted communications, here's why[144].

LUKS

The Linux Unified Key Setup (LUKS)[145] is a platform-independent specification for disk encryption. It is the standard used in Tails[146], Qubes OS[147], Ubuntu, etc. LUKS encryption is only effective when the device is powered off. LUKS should use Argon2id[148] 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

[140] anarsec.guide/glossary/#public-key-cryptography
[141] anarsec.guide/glossary/#metadata
[142] anarsec.guide/glossary/#forward-secrecy
[143] github.com/AnarchoTechNYC/meta/wiki/Pretty-Good-Privacy-%28PGP%29
[144] anarsec.guide/posts/e2ee/#pgp-email
[145] gitlab.com/cryptsetup/cryptsetup
[146] anarsec.guide/glossary/#tails
[147] anarsec.guide/glossary/#qubes-os
[148] anarsec.guide/posts/tails-best/#passwords

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 подозревают. 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 слежки[11] и антислежку[12] перед тем, как пойти в кофейню**, точно так же, как вы это делаете перед прямым действием.

[11] notrace.how/threat-library/mitigations/surveillance-detection.html
[12] notrace.how/threat-library/mitigations/anti-surveillance.html

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.

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 коммюнике 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 коммюнике, а затем закапывал ноутбук в лесу. Совсем недавно следователи, осуществлявшие физическое наблюдение за анархистом во Франции[14], установили скрытую камеру для контроля доступа в интернет-кафе недалеко от дома товарища и запросили записи видеонаблюдения за день, когда было отправлено коммюнике 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 конфиденциальности[15]. Если вы пишете коммюнике в офлайн-сессии Tails перед походом в общественное пространство, вам понадобится всего несколько минут, чтобы запереться в общественном туалете, чтобы отправить его.

[13] notrace.how/resources/ru/#how-submit
[14] notrace.how/resources/ru/#ivan
[15] anarsec.guide/ru/posts/tails/#ekran-konfidentsial-nosti

To learn more, watch this video[131]. 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 cryptography[134], asymmetric cryptography[135], 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-middle[137]) won't be able to decrypt those messages if the keys are compromised in the future. Modern encryption protocols such as TLS[138] 1.3 and the Signal Protocol provide FS. For more information, see Anonymous Planet[139].

[133] anarsec.guide/posts/tails-best/#appendix-gpg-explanation
[134] anarsec.guide/glossary/#symmetric-cryptography
[135] anarsec.guide/glossary/#public-key-cryptography
[136] open.oregonstate.education/defenddissent/chapter/what-is-encryption/
[137] anarsec.guide/glossary/#man-in-the-middle-attack
[138] anarsec.guide/glossary/#https
[139] anonymousplanet.org/guide.html#forward-secrecy

either a GUI (the GtkHash program) or a CLI command (`sha256sum`).

For more information, see Linux Essentials[123]. The Tech Learning Collective's «Foundations: Linux Journey» course on the command line[124] 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 network[125]. For more information, see Protecting against determined, skilled attackers[126] and Make Correlation Attacks More Difficult[127]. For research papers on the subject, see Thirteen Years of Tor Attacks[128] and the design proposal on information leaks in Tor[129].

Digital Signatures

Digital signatures are based on public-key cryptography[130]. 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.

[123] anarsec.guide/posts/linux/#the-command-line-interface
[124] techlearningcollective.com/foundations/linux-journey/the-shell
[125] anarsec.guide/glossary/#tor-network
[126] anarsec.guide/posts/tails-best/#2-protecting-against-determined-skilled-attackers
[127] anarsec.guide/posts/tails/#make-correlation-attacks-more-difficult
[128] github.com/Attacks-on-Tor/Attacks-on-Tor#correlation-attacks
[129] spec.torproject.org/proposals/344-protocol-info-leaks.html
[130] anarsec.guide/glossary/#public-key-cryptography
[131] youtube.com/watch?v=s22eJ1eVLTU&listen=false
[132] open.oregonstate.education/defenddissent/chapter/cryptographic-signing/

- Если кафе без камер видеонаблюдения встречаются редко, вы можете попробовать получить доступ к Wi-Fi кофейни снаружи, вне зоны действия камер.
- 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 данными[16]. Все USB-накопители LUKS, которые были разблокированы в сеансе Tails, теперь будут снова зашифрованы. Обратите внимание, что Tails предупреждает[17] : «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 операциях[18]. 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 BusKill[19] — однако мы рекомендуем покупать его только лично или распечатывать на 3D-принтере[20]. Это связано с тем, что любое письмо может быть перехвачено[21] и изменено, что сделает оборудование вредоносным[22].

[16] tails.net/doc/advanced_topics/cold_boot_attacks/index.ru.html
[17] tails.net/doc/first_steps/shutdown/index.ru.html
[18] dys2p.com/en/2023-05-luks-security.html#attacks
[19] buskill.in/tails/
[20] buskill.in/3d-print-2023-08/
[21] docs.buskill.in/buskill-app/en/stable/faq.html#q-what-about-interdiction
[22] ru.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 камер[23], 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 фишинга[24]) что позволяет им обойти Tor[25]. Чтобы сделать обе

[23] notrace.how/earsandeyes
[24] anarsec.guide/ru/posts/tails-best/#osvedomlennost-o-fishinge
[25] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

See When to Use Tails vs. Qubes OS[117]. 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 Anarchists[118]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[119].

Приложение: Словарь

Asynchronous Communication

Unlike synchronous communication[120], 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 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 Tails[121], you can verify the checksum[122] of a file using

[117] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[118] anarsec.guide/posts/e2ee/
[119] anarsec.guide/posts/tamper/
[120] anarsec.guide/glossary/#synchronous-communication
[121] anarsec.guide/glossary/#tails
[122] anarsec.guide/glossary/#checksums-fingerprints

like an «encrypted landline» and leave it at home when you are out of the house. See Kill the Cop in Your Pocket[109].

Your Computer

Operating system[110]: **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 network[111]. See Tails for Anarchists[112] and Tails Best Practices[113].

Operating system[114]: **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 Essentials[115]. Qubes OS can even run Windows programs such as Adobe InDesign, but much more securely than a standard Windows computer. See Qubes OS for Anarchists[116].

[109] anarsec.guide/posts/nophones/
[110] anarsec.guide/glossary#operating-system-os
[111] anarsec.guide/glossary#tor-network
[112] anarsec.guide/posts/tails/
[113] anarsec.guide/posts/tails-best/
[114] anarsec.guide/glossary#operating-system-os
[115] anarsec.guide/posts/linux
[116] anarsec.guide/posts/qubes/

эти атаки более сложными, мы рекомендуем подключаться к VPN *перед* подключением к Tor (т.е. Вы → VPN → Tor → Интернет[26]) при использовании Tails из дома, что требует запуска VPN с вашего сетевого устройства (маршрутизатора или аппаратного брандмауэра). Более подробную информацию об обосновании см. Privacy Guides[27].

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.

[26] gitlab.torproject.org/legacy/trac/-/wikis/doc/TorPlusVPN#you-vpnssh-tor
[27] privacyguides.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**:

[28] anarsec.guide/posts/qubes/

с tornet.biz[101]

Приложение: Рекомендации

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[102] for the purposes of incrimination[103] and network mapping[104]. 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 France[105]: «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].

Your Phone

Operating system[107]: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[108]. If you decide to have a phone, treat it

[101] tornet.biz/threads/luchshie-praktiki-tails.225/
[102] notrace.how/threat-library/techniques/targeted-digital-surveillance.html
[103] notrace.how/threat-library/tactics/incrimination.html
[104] notrace.how/threat-library/techniques/network-mapping.html
[105] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/
[106] notrace.how/threat-library/mitigations/digital-best-practices.html
[107] anarsec.guide/glossary#operating-system-os
[108] anarsec.guide/posts/grapheneos/

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.

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

- Согласно нашим рекомендациям (*rec*), в идеале это должна быть система Qubes OS[28], 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 Essentials[30] и см. Приложение ниже[31].
- 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-накопитель[32].

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

[29] tails.net/install/expert/index.ru.html
[30] anarsec.guide/posts/linux/
[31] anarsec.guide/ru/posts/tails-best/#prilozhenie-obiasnenie-gpg
[32] ru.wikipedia.org/wiki/BadUSB

компонентах[33] (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.

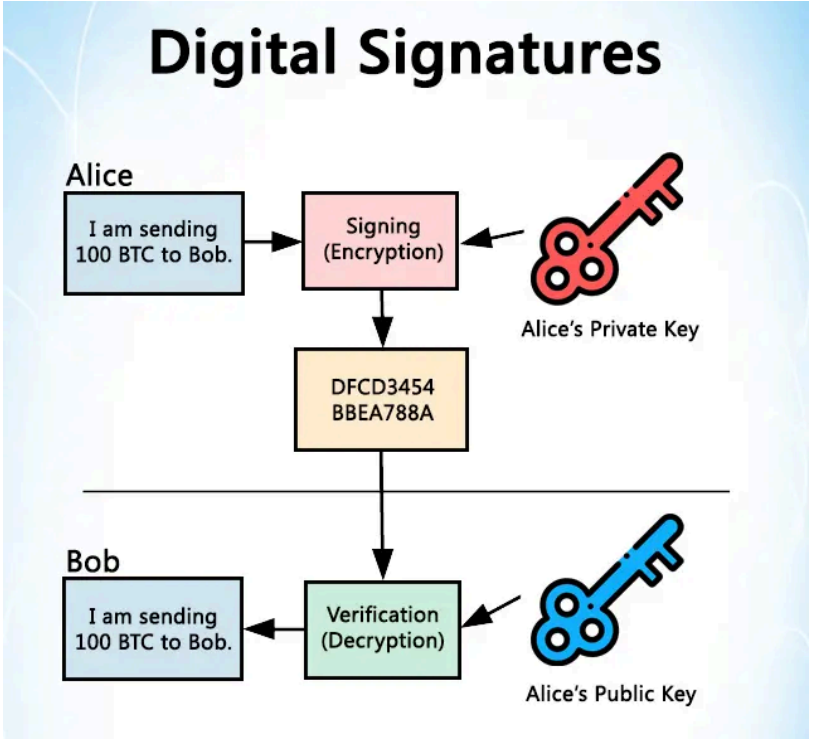
Если злоумышленник взломал аппаратное обеспечение или прошивку ноутбука, это также поставит под угрозу сеанс Tails, поскольку операционная система будет работать на вредоносной основе.

Не всем нужно применять все советы ниже. Например, если вы используете Tails только для анонимного просмотра вебстраниц 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 скомпрометирован[34]. Покупайте компьютер за наличные, чтобы его нельзя было отследить до вас, и лично,

[33] kicksecure.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 Tails[99].

Шаг: Генерация пары ключей

Tails рекомендует это руководство Riseup[100] для создания собственной пары ключей.

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

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

[100] riseup.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.

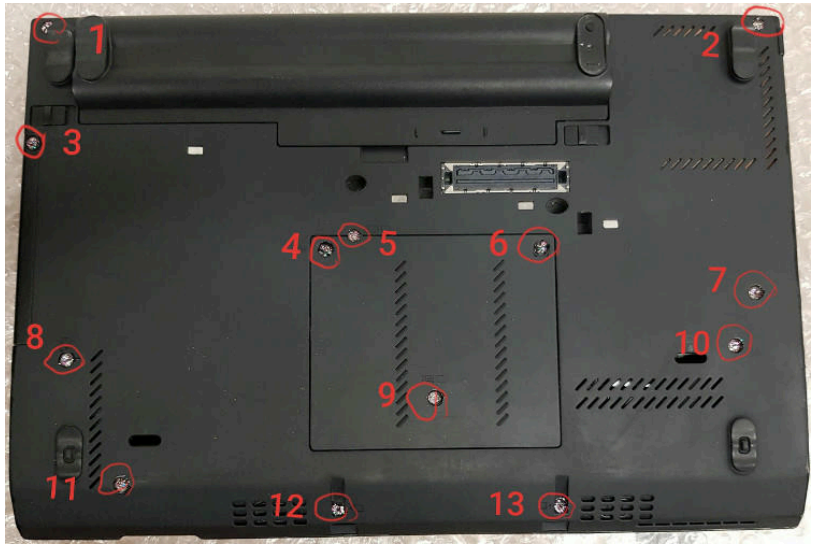
Сначала немного пояснений. PGP и GPG† — это термины, которые можно использовать взаимозаменяемо; PGP (Pretty Good Privacy) — это стандарт шифрования, а GPG (GNU Privacy Guard) — это программа, которая его реализует. PGP/GPG также используется для зашифрованной электронной переписки[97]), но мы используем 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 Computerphile[98] 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.

[97] anarsec.guide/posts/e2ee/#pgp-email
[98] youtube.com/watch?v=GSIDS_lvRv4

потому что почту 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 адаптировать винты вашего ноут-

[34] arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/
[35] anarsec.guide/posts/tamper/

бука, 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 хакерами[36]. 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 можно, по крайней мере, «отключить», наклеив

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

Для синхронных† и асинхронных† сообщений мы рекомендуем Cwtch[93], если только это не анонимный публичный проект, в этом случае мы все равно рекомендуем PGP. Для получения дополнительной информации см. Encrypted Messaging For Anarchists[94].

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 строки[95]. Если вы используете Tails, он вам вообще не понадобится, хотя для более безопасной установки[96] 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.

[93] anarsec.guide/posts/e2ee/#cwtch
[94] anarsec.guide/posts/e2ee/
[95] anarsec.guide/posts/linux/#the-command-line-interface
[96] tails.net/install/expert/index.ru.html

щью 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 недостатков[92].

[92] anarsec.guide/posts/e2ee/#pgp-email

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 Heads**[37]. Исследователи безопасности продемонстрировали атаку[38] 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 Boot[39], найденный в GrapheneOS, который устанавливает полную цепочку доверия от оборудования. Heads имеет ограниченную совместимость[40], поэтому имейте это в виду при покупке ноутбука, если вы планируете установить его — мы рекомендуем

[37] osresearch.net/
[38] youtube.com/watch?v=sNYsfUNegEA
[39] privacyguides.org/ru/os/android-overview/#_2
[40] osresearch.net/Prerequisites#supported-devices

ThinkPad X230, потому что его установка менее сложна, чем у других моделей. Процессоры этого поколения способны эффективно удалять Intel Management Engine[41] 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. документацию[42], 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 анализ[43] может выявить, как произошла компрометация, что поможет предотвратить ее повторение. Вы можете связаться со службой, например, с горячая линия по цифровой безопасности Access Now[44], хотя мы рекомендуем не отправлять им никаких персональных данных.

- **Используйте USB-накопители с защищенной прошивкой**, например Kanguru FlashTrust[45], чтобы USB-накопитель перестал работать[46], если прошивка будет скомпрометирована. Kanguru имеет розничных продавцов по всему миру[47], что позволяет вам покупать их лично, чтобы избежать риска перехвата почты.

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

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

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

[44] accessnow.org/help

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

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

[47] kanguru.com/pages/where-to-buy

ты с другой реализацией шифрования может быть полезен для особо конфиденциальных данных.

Установка SiriKali

SiriKali — это программа для зашифрованных томов, которая использует gocryptfs[88] за кулисами. Она доступна в репозитории Debian[89] и может быть легко установлена как дополнительное программное обеспечение[90]. 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 хранилище[91].

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».
  - Вам будет предложено ввести пароль. Создайте новую запись в файле KeepassXC и сгенерируйте пароль с помо-

[88] nuetzlich.net/gocryptfs/

[89] packages.debian.org/bookworm/sirikali

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

[91] anarsec.guide/ru/posts/tails-best/#razblokirovka-perekliuchatelia

пользовать 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 угроз[86] 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 отходите 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 аутентификацию[87], поэтому второй уровень защи-

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

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

- **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. Некото-

рые специальные 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 FlashTrust[48], 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 загрузкой[49].

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.

[48] kanguru.com/products/kanguru-flashtrust-secure-firmware-usb-3-0-flash-drive

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

Что такое парольная фраза Diceware? Как отмечает Privacy Guides[84], «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 игральных костей, см. Privacy Guides[85].

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

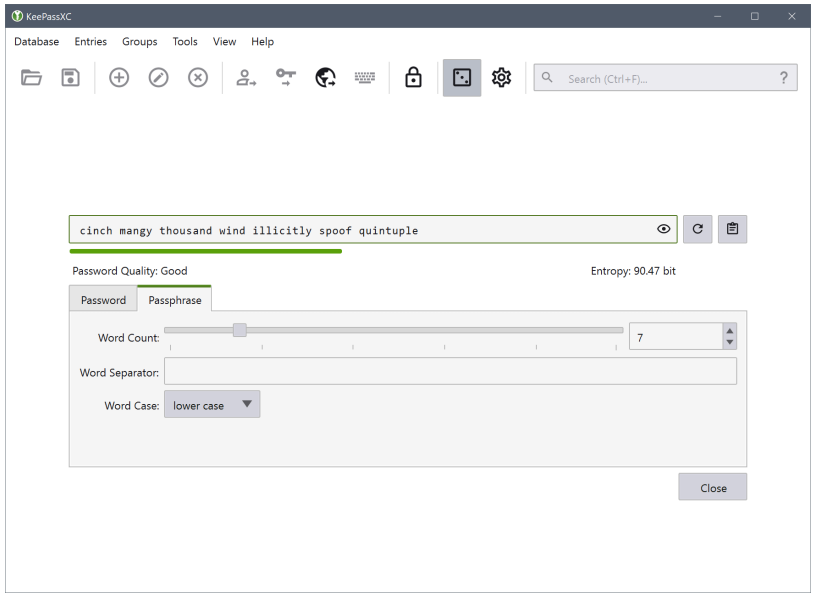
Ваши запомненные пароли Diceware могут легко забыться, если у вас есть несколько, за которыми нужно следить, особенно если вы используете какие-либо из них нечасто. Чтобы снизить риск того, что вы навсегда забудете пароль Diceware, вы можете ис-

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

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

ванием огромных объемов облачных вычислений[79]. Новая версия LUKS (LUKS2 с использованием Argon2id) менее уязвима для атак методом подбора пароля[80] — это значение по умолчанию для Tails 6.0 и Qubes OS 4.1. Если вы хотите узнать больше об этом изменении, мы рекомендуем обзор Systemli[81] или dys2p[82].

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).



[79] blog.elcomsoft.com/2020/08/breaking-luks-encryption/
[80] mjg59.dreamwidth.org/66429.html
[81] systemli.org/en/2023/04/30/is-linux-hard-disk-encryption-hacked/
[82] dys2p.com/en/2023-05-luks-security.html
[83] en.wikipedia.org/wiki/Password_strength#Entropy_as_a_measure_of_password_strength

2) Записывайте Tails на новый DVD-R/DVD+R[50] (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 GRUB[51].
   - 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

[50] tails.net/install/dvd/index.ru.html
[51] tails.net/doc/advanced_topics/boot_options/index.ru.html

USB-накопитель 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 Storage[52] — 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 дан-

[52] anarsec.guide/ru/posts/tails/#neobiazatel-no-sozdanie-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

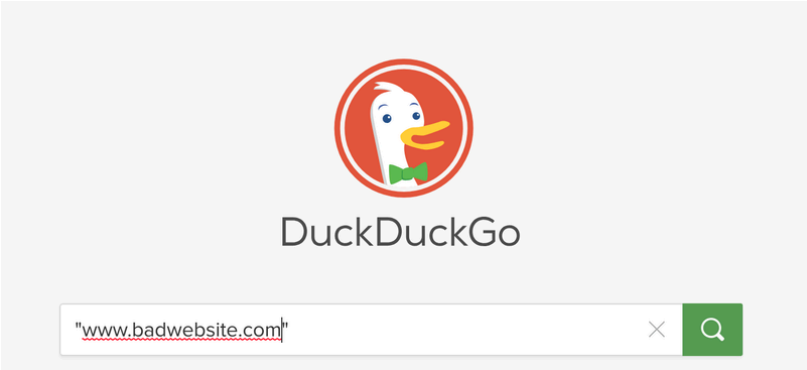
Шифрование† — единственное, что стоит на пути наших злоумышленников к чтению всех наших данных, если оно используется правильно. Первый шаг к обеспечению безопасности вашего шифрования — убедиться, что вы используете очень надежные пароли — большинство паролей не нужно запоминать, поскольку они хранятся 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 паролей[78].

> 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 использо-

[77] anarsec.guide/ru/posts/tails/#tor

[78] anarsec.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 водопои

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 Browser[76], чтобы взломать 8000 пользователей, которые его посетили.

[75] attack.mitre.org/techniques/T1189/

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

ные, например, дополнительную функцию программного обеспечения. Для этого требуется разблокировать переключатель для выделенного сеанса конфигурации Persistent Storage:

- Запустите «разблокированный» сеанс, создайте постоянное хранилище[53] с включенным дополнительным программным обеспечением, установите дополнительное программное обеспечение[54] 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

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

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

записи не позволяет нам использовать постоянное хранилище? Мы рекомендуем 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 Veracrypt[56] (накопители SSD и USB не подходят для скрытых томов[57]).

Подход к компартментализации, обсуждавшийся выше[58], 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.

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

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

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

[58] anarsec.guide/ru/posts/tails-best/#2-ispol-zovanie-tails-dlia-bolee-chem-odnoi-tseli-odnovremenno

го хранилища или подключенных USB-накопителей с «личными 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.

[72] anarsec.guide/ru/posts/tails/#tor

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

[74] unshorten.me/

Файлы

В 2017 году ФБР и Facebook совместно разработали вредоносный видеофайл , который деанонимизировал пользователя Tails[68] после того, как он открыл его, используя домашний Wi-Fi.

Для ненадежных вложений вам в идеале следует использовать Dangerzone[69] 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 документацией[70] 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 защищать две вещи: свою анонимность и свою информацию.

- **Лучше всего открывать ненадежные ссылки в выделенном сеансе Tails без разблокированного постоянно-**

[68] vice.com/en/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez

[69] dangerzone.rocks/

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

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

Tails USB
No Persistent Storage

LUKS USB #1
Website moderation

LUKS USB #2
Sketchy research

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 открытый ключ(и) из файла / Импортировать секретный ключ(и) из файла). Пре-

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

имущество 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 PGP[60] 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.

[60] anarsec.guide/posts/e2ee/#pgp-email
[61] en.wikipedia.org/wiki/Arbitrary_code_execution

Вредоносный файл или ссылка работает, выполняя код[61] 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 Tails[66] 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].

[62] attack.mitre.org/tactics/TA0003/
[63] attack.mitre.org/tactics/TA0009/
[64] attack.mitre.org/tactics/TA0010/
[65] en.wikipedia.org/wiki/Privilege_escalation
[66] tails.net/news/audit_by_ROS/index.en.html
[67] anarsec.guide/posts/qubes#when-to-use-tails-vs-qubes-os