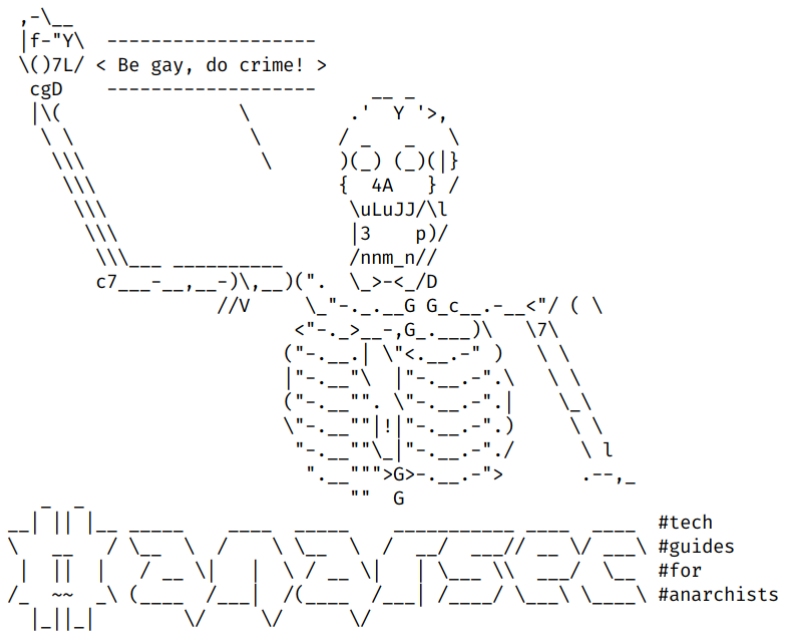
Tails — это операционная система, которая делает анонимное использование компьютера доступным для всех. Tails разработан так , чтобы не оставлять следов вашей активности на вашем компьютере, если вы явно не настроите его на сохранение определенных данных. Это достигается путем запуска с DVD или USB, независимо от установленной на компьютере операционной системы. Tails поставляется с несколькими встроенными приложениями, предварительно настроенными с учетом безопасности, и все анархисты должны знать, как использовать его для безопасного общения, исследования, редактирования и публикации конфиденциального контента.



Операционная система Tails - для анархистов

Серии: Защита

Эта версия зина была последний раз обновлена 2024-04-26. 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

documentation[129].

[129] whonix.org/wiki/Warning

Tails — это операционная система†, которая делает анонимное использование компьютера доступным для всех. Tails разработан[1] так , чтобы не оставлять следов вашей активности на вашем компьютере, если вы явно не настроите его на сохранение определенных данных. Это достигается путем запуска с DVD или USB, независимо от установленной на компьютере операционной системы. Tails поставляется с несколькими встроенными приложениями[2], предварительно настроенными с учетом безопасности, и все анархисты должны знать, как использовать его для безопасного общения, исследования, редактирования и публикации конфиденциального контента.

Документация на сайте Tails[3] превосходна и проста в использовании. В этом руководстве обобщена наиболее важная документация, а также дополнительно включены советы по настройке и использованию, относящиеся к модели угроз† анархистов. Our Лучшие практики Tails[4] article goes into more detail, but we recommend that you familiarize yourself with the basics of Tails before reading it.

TAILS: амнезическая и инкогнито живая система

Tails — это операционная система. Операционная система — это набор программ, которые управляют различными компонентами (жесткий диск, экран, процессор, память и т. д.) компьютера и позволяют ему функционировать.

Вы, вероятно, слышали о «Windows» или «macOS», двух самых распространенных операционных системах. Есть и другие операционные системы — может быть, вы слышали о

[1] tails.net/about/index.ru.html
[2] tails.net/doc/about/features/index.ru.html
[3] tails.net/doc/index.ru.html
[4] anarsec.guide/ru/posts/tails-best

Linux? Linux относится к семейству операционных систем, которое разветвляется на несколько подсемейств или различных версий Linux, одна из которых называется Debian. В подсемействе Debian мы находим Ubuntu и Tails. Tails — это дистрибутив (версия) Linux с несколькими отличительными особенностями:

- ***Живая система***
  - Tails — это так называемая живая система. В то время как другие операционные системы запускаются с жесткого диска вашего компьютера, Tails устанавливается на внешнее устройство, такое как USB (или даже SD-карта или DVD). Когда вы запускаете компьютер с подключенным устройством Tails, ваш компьютер работает с этого устройства, оставляя ваш жесткий диск нетронутым. Вы даже можете использовать Tails на компьютере без жесткого диска.
- ***Амнезия***
  - Tails разработан так, чтобы не оставлять никаких данных на компьютере, который вы используете; он ничего не записывает на жесткий диск и работает только в оперативной памяти (RAM), которая автоматически стирается после выключения. Сама система Tails live (обычно работающая на USB) также остается нетронутой. Единственный способ сохранить информацию — переместить ее на другой раздел USB перед выключением (см. ниже). Цель этого — не оставлять криминалистических следов, которые кто-то, имеющий физический доступ к вашему компьютеру или USB-накопителю Tails, мог бы позже прочитать. Такие вещи, как история поиска в Интернете, «недавно отредактированные» документы и т. д., стираются.
- ***Инкогнито***
  - Tails также является системой, которая позволяет вам оставаться инкогнито или анонимным. Она скрывает элементы, которые могут раскрыть вашу личность, местоположение и т. д. Tails использует сеть анонимности

modeling is the deliberate activity of identifying and assessing threats and vulnerabilities.

For more information, see the No Trace Project Threat Library[122], Defend Dissent: Digital Threats to Social Movements[123] and Defending against Surveillance and Suppression[124].

Tor network

Tor[125] (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[126] operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists[127] and Privacy Guides[128]. To understand the limitations of Tor, see the Whonix

[122] notrace.how/threat-library/
[123] open.oregonstate.education/defenddissent/chapter/digital-threats/
[124] open.oregonstate.education/defenddissent/chapter/surveillance-and-suppression/
[125] torproject.org/
[126] anarsec.guide/glossary/#tails
[127] anarsec.guide/posts/tails/#tor
[128] privacyguides.org/en/advanced/tor-overview/

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[115] 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[116].

For a more detailed look, see Defend Dissent: Protecting Your Devices[117].

Sandboxing

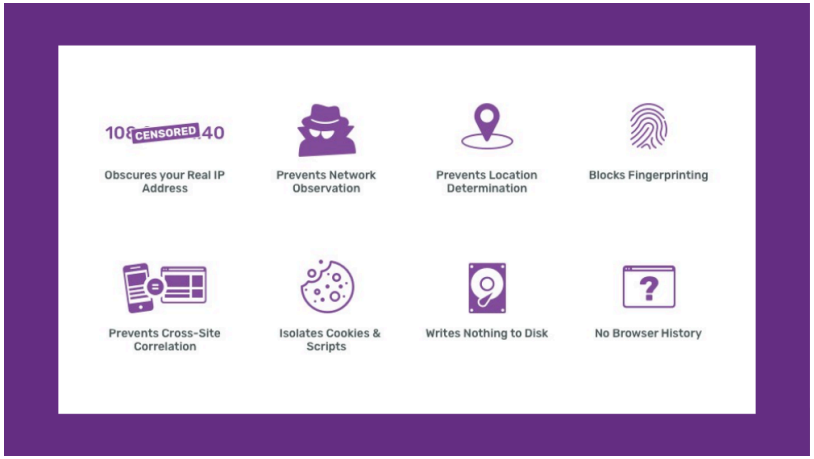
Sandboxing is the software-based isolation of applications to mitigate system failures or vulnerabilities. For example, if an attacker hacks an application that is «sandboxed», the attacker must escape the sandbox to hack the entire system. Virtualization[118] is the most powerful implementation of sandboxing.

Threat model

Threat modeling is a family of activities for improving security by identifying a set of adversaries, security goals[119], and vulnerabilities[120], 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[121]) or accidental (such as a hard drive failure). Threat

[115] anarsec.guide/glossary/#malware
[116] anarsec.guide/glossary/#physical-attacks
[117] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/
[118] anarsec.guide/glossary/#virtualization
[119] anarsec.guide/glossary/#security-goal
[120] anarsec.guide/glossary/#vulnerability
[121] anarsec.guide/glossary/#ddos-attack

Tor[†] для защиты вашей анонимности в сети, заставляя все стандартное программное обеспечение подключаться к Интернету через Tor. Если приложение пытается подключиться к Интернету напрямую, Tails автоматически заблокирует соединение. Tails также изменяет «MAC-адрес» вашего сетевого оборудования, который может использоваться для уникальной идентификации вашего ноутбука.



- ***Безопасность***
  - Tails был разработан с учетом безопасности. Минимальная, функциональная и проверенная среда уже установлена (со всем необходимым для базовой обработки текста, редактирования изображений, шифрования и т. д.).

Сегодняшняя цифровая безопасность не обязательно завтрашняя. **Защита персональных данных требует регулярных обновлений.** Цифровые инструменты ненадежны, если они никогда не обновляются, и чтобы иметь постоянную уверенность в этих инструментах, хорошо знать, что команды активно поддерживают их и что у них хорошая репутация. Важно понимать дух Tails: все разработано с учетом безопасности. Однако в программном обеспечении не существует идеального инструмента; всегда есть ограничения.

Кроме того, **способ использования Tails может создавать проблемы безопасности.**

Tails — это бесплатное программное обеспечение с открытым исходным† кодом. Любой желающий может просматривать, загружать и изменять исходный код (рецепт)… Абсолютно необходимо убедиться, что версия Tails у вас подлинная. Не пренебрегайте этапами проверки во время установки, которые подробно описаны на веб-сайте Tails.

Tails позволяет неспециалистам извлекать выгоду из цифровой безопасности и анонимности без крутой кривой обучения. Использование Tor имеет решающее значение для цифровой анонимности, и Tails помогает нам совершать как можно меньше ошибок при использовании Tor и некоторых других инструментов. Использование Tails требует совсем немного усилий, чтобы сделать повседневное цифровое поведение более безопасным, даже если иногда это кажется «неудобным». С другой стороны, «удобная» альтернатива означает повышенный риск репрессий — не только для вас, но и для тех, с кем вы общаетесь.

This tutorial is divided into several sections. The first covers the basics for getting started with Tails. The second section covers tips for using the software included in Tails, as well as what you need to know about how Tor works. The third section is about troubleshooting any problems that you might encounter with your Tails USB, so do not give up at the first problem — most of the time the solution is simple!

Концепция модели угроз

Tails — это не магия, и у нее много ограничений. Интернет и компьютеры — это враждебная территория, созданная для кражи ваших данных. Tails не защитит вас от человеческих ошибок, взлома оборудования, взлома прошивки, взлома или некоторых других типов атак. В Интернете не существует

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.

Phishing

Phishing is a technique of social engineering[106]. 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[107] onto a system, which can be used as a starting point for hacking. Spear phishing[108] is a more sophisticated form of phishing. For more information, see the Kicksecure documentation[109].

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[110].

For more information, see Making Your Electronics Tamper-Evident[111], the Threat Library[112], the KickSecure documentation[113], and Defend Dissent: Protecting Your Devices[114].

---

[106] anarsec.guide/glossary/#social-engineering
[107] anarsec.guide/glossary/#malware
[108] anarsec.guide/glossary/#spear-phishing
[109] kicksecure.com/wiki/Social_Engineering
[110] anarsec.guide/glossary/#remote-attacks
[111] anarsec.guide/posts/tamper
[112] notrace.how/threat-library/techniques/targeted-digital-surveillance/physical-access.html
[113] kicksecure.com/wiki/Protection_Against_Physical_Attacks
[114] open.oregonstate.education/defenddissent/chapter/protecting-your-devices/

LUKS

The Linux Unified Key Setup (LUKS)[100] is a platform-independent specification for disk encryption. It is the standard used in Tails[101], Qubes OS[102], Ubuntu, etc. LUKS encryption is only effective when the device is powered off. LUKS should use Argon2id[103] to make it less vulnerable to brute-force attacks.

Man-in-the-middle attack

An example of a man-in-the-middle attack is when Alice communicates with Bob over the Internet, Eve (eavesdropper) joins the conversation «in the middle» and becomes the man-in-the-middle. Eve can modify, insert, replay, or read messages at will. Protective measures include encryption (confidentiality) and checking the authenticity and integrity of all messages. However, you must also make sure that you are communicating with the expected party. You must verify that you have the real public key of the recipient. For example, this is what you do when you verify a contract's «Safety Number» in the Signal encrypted messaging app.

For a more detailed look, see Defend Dissent: The Man in the Middle[104] and the Whonix documentation[105].

Open-source

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

[100] gitlab.com/cryptsetup/cryptsetup

[101] anarsec.guide/glossary/#tails

[102] anarsec.guide/glossary/#qubes-os

[103] anarsec.guide/posts/tails-best/#passwords

[104] open.oregonstate.education/defenddissent/chapter/the-man-in-the-middle/

[105] whonix.org/wiki/Warning#Man-in-the-middle_Attacks

идеальной безопасности, поэтому так важно построить модель угроз†.

Построение модели угроз — это просто вопрос, от которого вы задаете себе определенные вопросы. От кого я защищаюсь? Каковы их возможности? Каковы были бы последствия, если бы у них был доступ к этим данным? А затем, исходя из конкретной ситуации, оцените, как вы можете защитить себя.

It makes no sense to say «this tool is secure». Security always depends on the threat model and it takes place on multiple levels (network, hardware, software, etc.). For more information on this topic, see the Threat Library[5].

I) Основы использования Tails

Предпосылки

Выберите USB/DVD:

Tails будет работать только с USB-накопителями объемом не менее 8 ГБ, DVD-дисками или SD-картами. Все данные на USB-накопителе будут полностью стерты во время установки, поэтому сохраните их в другом месте, а если вы не хотите, чтобы там остались какие-либо следы того, что там было раньше, используйте новый USB-накопитель.

В статье Лучшие практики Tails[6] рекомендуется использовать USB с переключателем защиты от записи (неизменяемый диск). При блокировке переключатель полностью предотвращает изменение содержимого USB. Это предотвращает ком-

[5] notrace.how/threat-library/

[6] anarsec.guide/ru/posts/tails-best/#ispol-zovanie-perekliuchatelia-zashchity-ot-zapisi

прометацию вашего USB-накопителя Tails скомпрометированным сеансом Tails. Переключатель защиты от записи должен быть выключен во время установки. Если у вас нет возможности получить такой USB-накопитель, вы можете запустить Tails с SD-карты, DVD-R/DVD+R или всегда загружаться с опцией `toram` (описанной в статье).

Выберите ноутбук:

Хотя Tails можно использовать на настольном компьютере, это не рекомендуется, поскольку обнаружить физическое вмешательство[7] можно только на ноутбуке. See Лучшие практики Tails[8] for more information on obtaining a laptop.

Некоторые модели ноутбуков и USB не будут работать с Tails, или некоторые функции не будут работать. Чтобы узнать, есть ли у вашей модели известные проблемы, посетите страницу известных проблем Tails[9].

Если Tails работает слишком медленно, убедитесь, что USB версии 3.0 или выше и что вы используете порт USB 3.0 на ноутбуке. Если Tails часто зависает, вы можете добавить больше оперативной памяти в компьютер. 8 ГБ должно быть достаточно.

Установка

Для установки Tails на USB-накопитель вам понадобится «источник» и USB-накопитель (8 ГБ или больше).

Для «источника» есть два решения.

[7] anarsec.guide/posts/tamper/#tamper-evident-laptop-screws

[8] anarsec.guide/ru/posts/tails-best/#snizhenie-riskov-pri-ispol-zovanii-nenadezhnykh-komp-iuterov

[9] tails.net/support/known_issues/index.ru.html

For more information, see Linux Essentials[89]. The Tech Learning Collective's «Foundations: Linux Journey» course on the command line[90] 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[91]. For more information, see Protecting against determined, skilled attackers[92] and Make Correlation Attacks More Difficult[93]. For research papers on the subject, see Thirteen Years of Tor Attacks[94] and the design proposal on information leaks in Tor[95].

HTTPS

The «S» in HTTPS stands for «secure»; which means that your Internet connection is encrypted using the Transport Layer Security (TLS)[96] protocol. This involves the website generating a certificate using public-key cryptography[97] that can be used to verify its authenticity — that you are actually connecting to the web server you intended, and that this connection is encrypted.

For more information, see our explanation[98] or Defend Dissent: Protecting Your Communications[99].

[89] anarsec.guide/posts/linux/#the-command-line-interface

[90] techlearningcollective.com/foundations/linux-journey/the-shell

[91] anarsec.guide/glossary/#tor-network

[92] anarsec.guide/posts/tails-best/#2-protecting-against-determined-skilled-attackers

[93] anarsec.guide/posts/tails/#make-correlation-attacks-more-difficult

[94] github.com/Attacks-on-Tor/Attacks-on-Tor#correlation-attacks

[95] spec.torproject.org/proposals/344-protocol-info-leaks.html

[96] youtube.com/watch?v=0TLDTodL7Lc&listen=false

[97] anarsec.guide/glossary/#public-key-cryptography

[98] anarsec.guide/posts/tails/#what-is-https

[99] open.oregonstate.education/defenddissent/chapter/protecting-your-communications/

> Essentials[82]. 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[83].

See When to Use Tails vs. Qubes OS[84]. 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[85]

Storing Electronic Devices

See Make Your Electronics Tamper-Evident[86].

Приложение: Словарь

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[87], you can verify the checksum[88] of a file using either a GUI (the GtkHash program) or a CLI command (`sha256sum`).

[82] anarsec.guide/posts/linux
[83] anarsec.guide/posts/qubes/
[84] anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
[85] anarsec.guide/posts/e2ee/
[86] anarsec.guide/posts/tamper/
[87] anarsec.guide/glossary/#tails
[88] anarsec.guide/glossary/#checksums-fingerprints

Решение 1: Установка путем загрузки (предпочтительно)

Следуйте инструкциям по установке Tails[10] важно следовать всему руководству. Злоумышленник может перехватить и изменить данные по пути к вам (это называется атакой «человек посередине»[†]), поэтому не пропускайте этапы проверки. Как обсуждалось в Лучшие практики Tails[11], метод установки GnuPG[12] предпочтительнее, поскольку он более тщательно проверяет целостность загрузки.

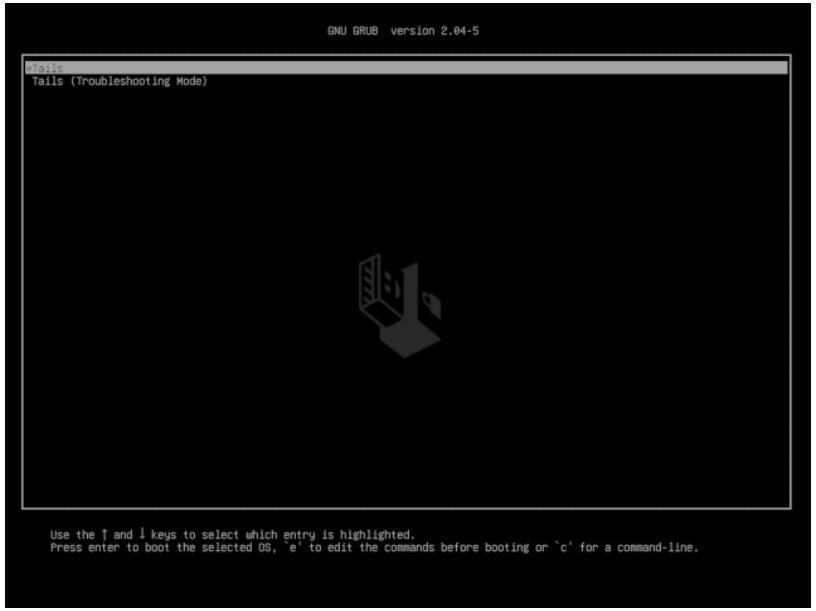
Решение 2: Установка с другого USB-накопителя Tails

Для этого необходимо знать пользователя Tails, которому вы доверяете. Очень простое программное обеспечение под названием Tails Installer позволяет вам «клонировать» существующий USB-накопитель Tails на новый за несколько минут; см. документацию по клонированию с ПК[13] или Mac[14]. Никакие данные постоянного хранилища не будут переданы. Недостатком этого метода является то, что он может распространять скомпрометированную установку.

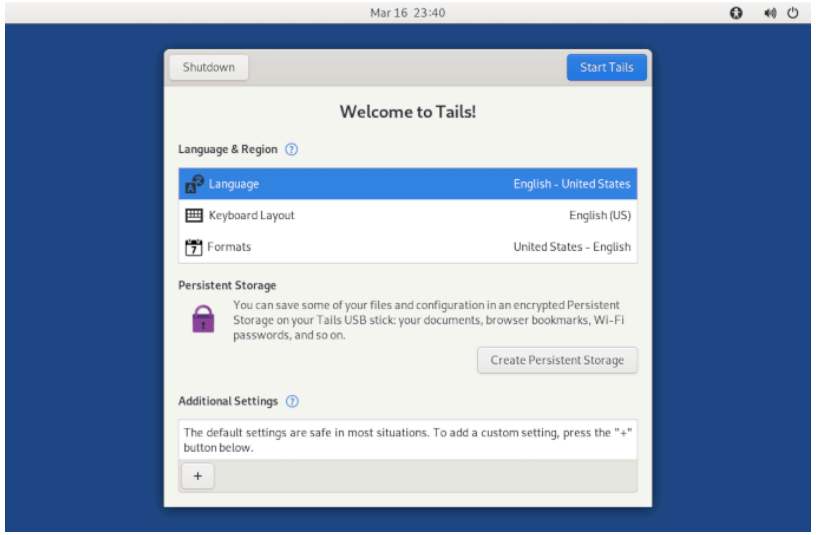
Загрузка с USB-накопителя Tails

Если у вас есть USB-накопитель Tails, следуйте инструкциям Tails по загрузке Tails на Mac или ПК[15]. USB-накопитель Tails необходимо вставить до включения ноутбука. Появится экран загрузчика, и через несколько секунд Tails автоматически запустится.

[10] tails.net/install/index.ru.html
[11] anarsec.guide/ru/posts/tails-best/#snizhenie-riskov-pri-ispol-zovanii-nenadezhnykh-komp-iuterov
[12] tails.net/install/expert/index.ru.html
[13] tails.net/install/clone/pc/index.ru.html
[14] tails.net/install/clone/mac/index.ru.html
[15] tails.net/doc/first_steps/start/index.ru.html



Примерно через 30 секунд загрузки появится экран приветствия[16].



[16] tails.net/doc/first_steps/welcome_screen/index.ru.html

Your Phone

Operating system[74]: **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists[75]. 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 Pocket[76].

Your Computer

Operating system[77]: **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[78]. See Tails for Anarchists[79] and Tails Best Practices[80].

Operating system[81]: **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

[74] anarsec.guide/glossary#operating-system-os
[75] anarsec.guide/posts/grapheneos/
[76] anarsec.guide/posts/nophones/
[77] anarsec.guide/glossary#operating-system-os
[78] anarsec.guide/glossary#tor-network
[79] anarsec.guide/posts/tails/
[80] anarsec.guide/posts/tails-best/
[81] anarsec.guide/glossary#operating-system-os

Смотрите тег Tails[64] для руководств по таким темам, как удаление идентифицирующих метаданных из файлов[65].

В статье использованы материалы TuTORiel Tails[66] *(на французском языке) и* Capulcu #1[67] *(на немецком языке).*

с tornet.biz[68]

Приложение: Рекомендации

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance[69] for the purposes of incrimination[70] and network mapping[71]. 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[72]: «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»[73].

[64] anarsec.guide/tags/tails/
[65] anarsec.guide/posts/metadata/
[66] infokiosques.net/spip.php?article1726
[67] capulcu.blackblogs.org/neue-texte/bandi/
[68] tornet.biz/threads/operacionnaja-sistema-tails-rukovodstvo.224/
[69] notrace.how/threat-library/techniques/targeted-digital-surveillance.html
[70] notrace.how/threat-library/tactics/incrimination.html
[71] notrace.how/threat-library/techniques/network-mapping.html
[72] actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/
[73] notrace.how/threat-library/mitigations/digital-best-practices.html

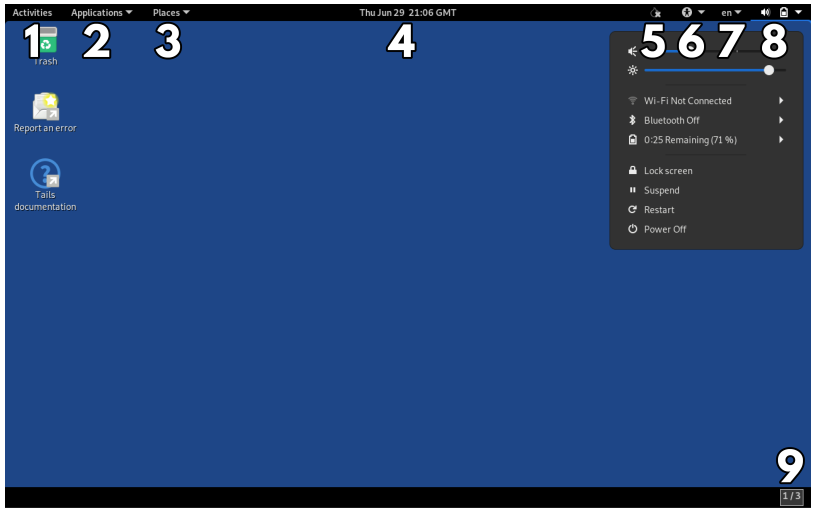
На экране приветствия выберите язык и раскладку клавиатуры в разделе **«Язык и регион»**. Для пользователей Mac есть раскладка клавиатуры для Macintosh. В разделе «Дополнительные настройки» вы найдете кнопку **+**, нажмите ее, и появятся дополнительные параметры конфигурации:

- Пароль администратора
  - Установите это, если вам нужны права администратора. Это необходимо, например, для установки дополнительного программного обеспечения, которое вы хотите использовать во время сеанса Tails. В следующем диалоговом окне вы можете ввести любой пароль (и вам нужно его запомнить!). Он будет действителен только для этого сеанса Tails. Перезапустите сеанс Tails без пароля администратора, как только вы закончите действие, для которого он требовался.
- Подмена MAC-адреса
  - Мы рекомендуем вам никогда не отключать это. По умолчанию это включено.
- Сетевое подключение
  - «Отключить все сетевые возможности» позволяет отключить все программные сетевые адаптеры при запуске. Если вы собираетесь использовать сеанс Tails в режиме «офлайн», имеет смысл сделать это до того, как Tails запустит свои сетевые возможности.
- Небезопасный браузер
  - Unsafe Browser включен по умолчанию и не использует Tor. Злоумышленник может воспользоваться уязвимостью в другом приложении в Tails, чтобы запустить невидимый Unsafe Browser и раскрыть ваш реальный IP-адрес. Это возможно, даже если вы не используете Unsafe Browser. Например, злоумышленник может воспользоваться уязвимостью в Thunderbird, отправив вам фишинговое† письмо, которое запустит невидимый Unsafe Browser, который посетит веб-сайт и раскроет ваш IP-адрес. Такая атака маловероятна, но ее может осуществить сильный злоумышленник, например правительство или

хакерская компания. По этой причине **мы рекомендуем вам отключать Unsafe Browser для каждого сеанса**. Оставляйте Unsafe Browser включенным только тогда, когда вам нужно пройти через «портал захвата» для подключения к Интернету (когда вам нужно щелкнуть поле или войти в систему для подключения к Интернету, что распространено в интернет-кафе, общественных Wi-Fi и т. д.).

Если у вас включено постоянное хранилище, в этом окне появится парольная фраза для его разблокировки. Если вы не включили постоянное хранилище, на вашем USB-накопителе Tails не будет сохранено никаких данных после этой сессии. Нажмите **Запустить Tails**. Через 15–30 секунд появится рабочий стол Tails.

Использование рабочего стола Tails



Tails — простая операционная система.

1. Меню «Действия». Позволяет просматривать обзор окон и приложений. Также позволяет искать приложения, файлы и папки. Вы также можете получить доступ к «Действи-

Я не могу установить Tails на USB

Убедитесь, что ваш USB-накопитель не имеет известных проблем[60] с Tails. Отформатируйте[61] весь USB-накопитель и повторите установку.

Приложение тормозит Tails? Экран глючит?

Попробуйте нажать клавишу Windows или клавишу Cmd для Mac, что откроет окно со всеми запущенными приложениями, из которого вы сможете выйти. Если это не сработает, вам нужно будет принудительно завершить работу, удерживая кнопку питания.

Добавить принтер

Вы переходите в **Приложения → Системные инструменты → Настройки → Устройства → Принтеры → «+» → Добавить принтер**. Некоторые модели принтеров могут не работать с Tails (или их может быть сложно настроить).

Невозможно установить новое программное обеспечение

Иногда Synaptic Package Manager отказывается устанавливать программное обеспечение. В этом случае используйте root-терминал (требующий пароль администратора): установите с помощью команды `apt update && apt install [package_name]`

Лучшие практики

Лучшие практики Tails[62] важно установить перед использованием Tails для высокочувствительных действий, таких как запрос действия[63]. Чтобы не перегружать себя, начните с изучения того, как использовать Tails в базовых целях, таких как чтение анархистских веб-сайтов или написание текстов.

[60] tails.net/support/known_issues/index.ru.html#problematic-usb-sticks
[61] anarsec.guide/ru/posts/tails/#kak-sozdat-zashifrovannyi-usb
[62] anarsec.guide/ru/posts/tails-best
[63] notrace.how/resources/ru/#how-submit

блокировать с помощью пароля. Если вы не можете получить доступ к своим данным на другом USB Tails, на котором включен Persistent Storage, ваш USB может быть неисправен.

Я не могу подключиться к публичной сети Wi-Fi со страницей аутентификации (порталом авторизации)

Если вам нужно подключиться к Wi-Fi с помощью портала захвата, вы должны включить Unsafe Browser на экране приветствия. Подключитесь к Wi-Fi, а затем откройте **Приложения → Интернет → Unsafe Browser**. Вы вводите URL-адрес сайта, который не является сомнительным (например, wikipedia.org), чтобы получить доступ к странице аутентификации. После завершения страницы портала захвата подождите, пока Tor не будет готов, а затем закройте unsafe Browser.

Что делать, если на USB-накопителе закончилось место?

Если на USB-накопителе закончилось место или вы видите меньше данных, чем на самом деле есть на USB-накопителе, установите флажок «Показывать скрытые файлы» в файловом браузере. Там вы увидите новые файлы с именем `.something`. Файл `.Trash-10xx` ххзанимает место (и если щелкнуть по нему правой кнопкой мыши и выбрать «Переместить в корзину», он будет полностью удален). Не изменяйте другие скрытые файлы.

Файл всегда открывается в режиме только для чтения или не открывается вообще?

В некоторых программах это нормально, если тот же файл уже открыт. Если это не так, используйте тот же трюк, что и в абзаце выше. Вы включаете Показывать скрытые файлы. Будет файл .lock с тем же именем, что и у файла, с которым у вас проблема. Удалите этот файл, что указывает на то, что он уже открыт в другом месте. Если проблема не в этом, вам нужно изменить права доступа файла.

ям», направив указатель мыши в верхний левый угол экрана или нажав клавишу Command/Windows (❖).

2. Меню «Приложения». Список доступных приложений (программного обеспечения), организованный по категориям.
3. Меню «Места». Ярлыки различных папок и устройств хранения, доступ к которым также можно получить через браузер «Файлы» (**Приложения → Стандартные → Файлы**).
4. Дата и время. После подключения к Интернету все системы Tails по всему миру используют одно и то же время[17].
5. Индикатор статуса Tor. Сообщает, подключены ли вы к сети Tor. Если над значком луковицы есть крестик, значит, вы не подключены. Вы можете открыть приложение Onion Circuits отсюда. Проверьте подключение Tor, посетив `check.torproject.org` Tor Browser.
6. Кнопка «Универсальный доступ». Это меню позволяет включить программное обеспечение для обеспечения доступности, такое как экранный диктор, визуальная клавиатура и большой текстовый дисплей.
7. Выбор раскладки клавиатуры. Значок, показывающий текущую раскладку клавиатуры (в примере выше `en` для английской раскладки). Щелчок по нему открывает опции для других раскладок, выбранных на экране приветствия.
8. Меню «Система». Отсюда вы можете получить доступ к громкости и яркости экрана, подключению Wi-Fi и Ethernet, состоянию батареи, а также кнопкам перезагрузки и выключения.
9. Значок «Рабочие пространства». Эта кнопка переключает между несколькими представлениями рабочего стола (называемыми «рабочими пространствами»), что может помочь уменьшить визуальный беспорядок на небольшом экране.

[17] tails.net/doc/first_steps/desktop/time/index.ru.html

Если ваш ноутбук оснащен Wi-Fi, но в системном меню нет опции Wi-Fi, см. документацию по устранению неполадок[18]. После подключения к Wi-Fi появится помощник Tor Connection, который поможет вам подключиться к сети Tor. Выберите **Connect to Tor automatically (Подключаться к Tor автоматически)**, если только вы не находитесь в стране, где нужно скрыть, что вы используете Tor (в этом случае вам нужно настроить мост[19]).

Необязательно: создание и настройка постоянного хранилища

Tails по умолчанию амнезиачен. Он забудет все, что вы сделали, как только вы закончите сеанс. Это не всегда то, что вам нужно — например, вы можете захотеть установить дополнительное программное обеспечение без необходимости переустанавливать его каждый раз при запуске. В Tails есть функция под названием Persistent Storage, которая позволяет вам сохранять данные между сеансами. Это явно менее безопасно, но необходимо для некоторых действий.

Принцип, лежащий в основе Persistent Storage, заключается в создании второй области хранения (называемой разделом) на вашем USB-накопителе Tails, которая зашифрована. Этот новый раздел позволяет вам сделать некоторые данные постоянными — то есть сохранять их между сеансами Tails. Включить Persistent Storage очень просто. Чтобы создать Persistent Storage[20], выберите **Applications → Tails → Persistent Storage**.

Появится окно с просьбой ввести парольную фразу; см. Лучшие практики Tails[21] для получения информации о надежно-

[18] tails.net/doc/anonymous_internet/no-wifi/index.ru.html
[19] tails.net/doc/anonymous_internet/tor/index.ru.html#hiding
[20] tails.net/doc/persistent_storage/create/index.ru.html
[21] anarsec.guide/ru/posts/tails-best/#paroli

видеть контент, если только они не находятся прямо перед ним.

III) Устранение неполадок

Компьютер пытается загрузить USB, но это не работает.

Проверьте сообщения об ошибках, которые вы получаете (например, если у вас старый 32-разрядный компьютер, он не будет работать с Tails). Если там написано `Error starting GDM with your graphics card`, проблема в видеокарте; проверьте документацию на предмет Известных проблем с видеокартами[56]. Вы также можете проверить список известных проблем[57] на сайте Tails для вашей модели компьютера.

Если откроется страница загрузчика Tails, попробуйте загрузиться в режиме устранения неполадок Tails.

Мой Tails USB больше не запускается! (а раньше он запускался на том же компьютере)

После обновления или по другой причине Tails больше не запускается на вашем компьютере. У вас есть три варианта:

1) Посмотрите, упоминаются ли на странице новостей Tails[58] какие-либо проблемы с обновлением.
2) Выполните ручное обновление[59], которое может потребоваться, если компьютер был выключен до завершения автоматического обновления.
3) Если первые два решения не сработали, USB слишком старый, плохого качества или сломан. Если вам нужно восстановить данные из Persistent Storage, подключите этот USB к сеансу Tails с помощью другого USB. Он будет отображаться как обычный USB, который вам нужно будет раз-

[56] tails.net/support/known_issues/graphics/index.ru.html
[57] tails.net/support/known_issues/index.ru.html
[58] tails.net/news/index.ru.html
[59] anarsec.guide/ru/posts/tails/#obnovlenie-tails-usb

торые используют Интернет[51]. Программное обеспечение, используемое в Tails, проходит аудит на безопасность, но это может быть не так для того, что вы устанавливаете. Перед установкой нового программного обеспечения лучше всего убедиться, что в Tails еще нет программного обеспечения, которое выполняет ту работу, которую вы хотите, чтобы оно выполняло. Если вы хотите, чтобы дополнительное программное обеспечение сохранялось после одного сеанса, вам нужно включить «Дополнительное программное обеспечение» в конфигурации постоянного хранилища[52].

Более подробную информацию смотрите в документации по установке дополнительного программного обеспечения[53].

Не забудьте сделать резервные копии!

USB-накопитель Tails легко потерять, а срок службы USB-накопителей намного короче, чем у жестких дисков (особенно дешевых). Если у вас есть важные данные на нем, не забывайте регулярно делать их резервные копии. Если вы используете второй USB-накопитель с шифрованием LUKS, это так же просто, как использовать файловый менеджер для копирования файлов на резервный USB-накопитель с шифрованием LUKS.

Если вы используете постоянное хранилище, ознакомьтесь с документацией по его резервному копированию[54].

Экран конфиденциальности

На экран ноутбука можно установить экран конфиденциальности[55], чтобы посторонние (или скрытые камеры) не могли

[51] tails.net/doc/persistent_storage/additional_software/index.ru.html#index5h2

[52] tails.net/doc/persistent_storage/configure/index.ru.html

[53] tails.net/doc/persistent_storage/additional_software/index.ru.html#index3h1

[54] tails.net/doc/persistent_storage/backup/index.ru.html

[55] en.wikipedia.org/wiki/Monitor_filter

сти парольной фразы. Затем вы настроите[22], что вы хотите сохранить в Persistent Storage. Persistent Storage можно включить для нескольких типов данных:

Личные документы:

- **Постоянная папка**: данные, такие как ваши личные файлы, документы или изображения, над которыми вы работаете.

Настройки системы:

- **Экран приветствия**: настройки экрана приветствия: язык, клавиатура и дополнительные настройки.
- **Принтеры**: Конфигурация принтера[23].

Сеть:

- **Сетевые подключения**: пароли для сетей Wi-Fi можно сохранить, чтобы вам не пришлось вводить их каждый раз.
- **Tor Bridge**: если включен Tor Bridge (для пользователей в странах, где Tor подвергается цензуре), будет сохранен последний использовавшийся вами Tor Bridge.

Приложения:

- **Закладки браузера Tor**: Закладки браузера Tor.
- **Биткоин-кошелек Electrum**: биткоин-кошелек и настройки.
- **Клиент электронной почты Thunderbird**: почтовый ящик Thunderbird, каналы и ключи OpenPGP.
- **GnuPG**: ключи OpenPGP, которые вы создаете или импортируете в GnuPG и Kleopatra.
- **Pidgin**: Файлы учетной записи этого приложения чата (использующего протокол XMPP).
- **SSH-клиент**: все файлы, связанные с SSH, протоколом, используемым для подключения к серверам.

Расширенные настройки:

[22] tails.net/doc/persistent_storage/configure/index.ru.html

[23] tails.net/doc/sensitive_documents/printing_and_scanning/index.ru.html

- **Дополнительное ПО**: Если эта функция включена, список дополнительного ПО по вашему выбору будет автоматически устанавливаться каждый раз при запуске Tails. Эти пакеты ПО хранятся в постоянном хранилище. Они автоматически обновляются при подключении к Интернету. Будьте осторожны с тем, что вы устанавливаете[24].
- **Dotfiles**: В Tails и Linux в целом имена файлов конфигурации часто начинаются с точки, поэтому их иногда называют «dotfiles». Их можно сохранить в постоянном хранилище. Будьте осторожны, изменяя настройки конфигурации, так как изменение значений по умолчанию может нарушить вашу анонимность.

Чтобы использовать Постоянное хранилище, вы должны разблокировать его на экране приветствия. Если вы хотите изменить парольную фразу, см. документацию[25]. Если вы когда-нибудь забудете свою парольную фразу, восстановить ее будет невозможно; вам придется удалить[26] Постоянное хранилище и начать заново.

В Лучшие практики Tails[27] мы рекомендуем не использовать Persistent Storage в большинстве случаев; большинство функций Persistent Storage не работают должным образом с USB-накопителями, имеющими переключатель защиты от записи, любые файлы, хранящиеся на USB-накопителе Tails, оставят на нем криминалистические следы, а хранение персональных данных на USB-накопителе Tails также препятствует его разделению при разблокировке Persistent Storage. Вместо этого любые файлы, которые должны быть постоянными, можно хранить на втором USB-накопителе, зашифрованном с помощью LUKS[28].

[24] tails.net/doc/persistent_storage/additional_software/index.ru.html#warning

[25] tails.net/doc/persistent_storage/passphrase/index.ru.html

[26] tails.net/doc/persistent_storage/delete/index.ru.html

[27] anarsec.guide/ru/posts/tails-best/#ispol-zovanie-perekliuchatelia-zashchity-ot-zapisi

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

По той же причине перед расшифровкой файла сначала скопируйте его в папку Tails, которая находится только в оперативной памяти (например, **Places → Documents**).

Добавление прав администратора

Tails требует пароль администратора (также называемый паролем «root») для выполнения задач системного администрирования. Например:

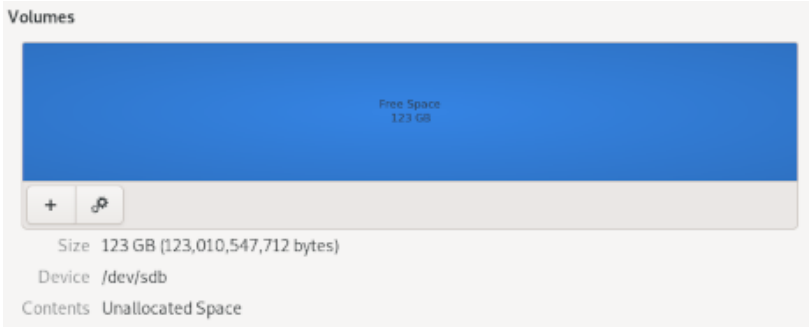
- Установка дополнительного программного обеспечения
- Доступ к внутренним жестким дискам компьютера
- Выполнение команд† в корневом терминале
- Доступ к определенным привилегиям, например, когда вы видите окно, запрашивающее аутентификацию администратора

По умолчанию пароль администратора отключен для дополнительной безопасности. Это может помешать злоумышленнику с физическим† или удаленным† доступом к вашей системе Tails получить привилегии администратора. Если вы устанавливаете пароль администратора для своего сеанса, вы создаете еще один вектор для потенциального обхода безопасности Tails.

Чтобы установить пароль администратора, необходимо выбрать пароль администратора на экране приветствия при запуске Tails. Этот пароль действителен только в течение сеанса.

Установка дополнительного программного обеспечения

Если вы устанавливаете новое программное обеспечение, вам нужно убедиться, что оно безопасно. Tails заставляет все программное обеспечение подключаться к Интернету через Tor, поэтому вам нужно будет настроить это для приложений, ко-



- Теперь вам нужно добавить зашифрованный раздел.
  - Нажмите на кнопку «+»
  - Выберите размер раздела (все свободное пространство)
  - В поле «Тип» выберите **внутренний диск, который будет использоваться только с системами Linux (Ext4)** установите **флажок «Защищенный паролем том (LUKS)»**
  - Введите надежную парольную фразу[49]

Если вы вставите зашифрованный USB-накопитель, вам будет предложено ввести парольную фразу. Перед извлечением накопителя после завершения работы с ним необходимо щелкнуть его правой кнопкой мыши в **Places → Computer** и выбрать Eject.

Шифрование файла паролем или открытым ключом

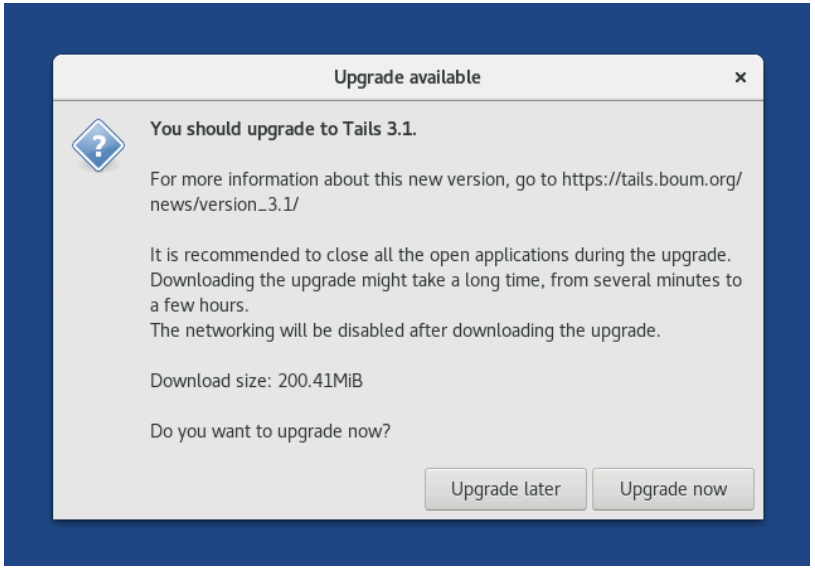
В Tails вы можете использовать приложение Kleopatra для шифрования файла[50] паролем или открытым ключом PGP. Это создаст файл .pgp. Если вы хотите зашифровать файл, сделайте это в оперативной памяти, прежде чем сохранять его на USB-накопитель LUKS. После сохранения незашифрованной версии файла на USB-накопитель USB необходимо переформатировать, чтобы удалить его.

[49] anarsec.guide/ru/posts/tails-best/#paroli
[50] tails.net/doc/encryption_and_privacy/kleopatra/index.ru.html#index1h1

Обновление Tails USB

Чтобы Tails оставался безопасным, операционная система должна постоянно развиваться, а любые уязвимости безопасности должны устраняться посредством обновлений. Важно всегда использовать последнюю версию (Tails обновляется примерно каждый месяц), поскольку в программах, используемых Tails, регулярно обнаруживаются уязвимости безопасности, что в худшем случае может привести к раскрытию вашей личности, IP-адреса и т. д. Обновление Tails исправит эти уязвимости и обычно улучшит другие функции.

Каждый раз, когда вы запускаете Tails, сразу после подключения к сети Tor, Tails Upgrader проверяет, установлена ли у вас последняя версия Tails. Существует два типа обновлений.



Автоматическое обновление

Когда автоматическое обновление[29] доступно, появится окно с информацией об обновлении, и вам нужно будет нажать

[29] tails.net/doc/upgrade/index.ru.html

«Обновить сейчас». Подождите некоторое время, пока оно не завершится, затем нажмите «Применить обновление», и ваш интернет на мгновение прервется. Подождите, пока не увидите окно «Перезапустить Tails». Если обновление не удалось (например, из-за того, что вы выключили его до его завершения), ваше постоянное хранилище не будет затронуто, но вы, возможно, не сможете перезапустить свой USB-накопитель Tails. Если вы используете USB-накопитель с переключателем защиты от записи, вам нужно будет разблокировать его для выделенного сеанса, в котором вы выполняете обновление.

Ручное обновление

Иногда окно обновления сообщит вам, что вам нужно выполнить ручное обновление. Этот тип обновления используется только для крупных обновлений (которые происходят примерно каждые два года) или если есть проблема с автоматическими обновлениями. См. документацию по ручным обновлениям[30].

II) Идем дальше: несколько советов и пояснений

Tor

Что такое Tor?

Tor†, что означает The Onion Router, — лучший способ сохранить анонимность в Интернете. Tor — это программное обеспечение с открытым исходным кодом, подключенное к публичной сети из тысяч ретрансляторов (серверов). Вместо прямого подключения к определенному месту в Интернете Tor

[30] tails.net/upgrade/tails/index.ru.html

диска требует температур выше, чем обычный огонь (например, термит), чтобы быть эффективным.

Для флэш-накопителей (USB, SSD, SD-карты и т. д.) используйте плоскогубцы, чтобы выломать плату из пластикового корпуса. Используйте высококачественный бытовой блендер, чтобы измельчить чипы памяти, включая плату, на куски, которые в идеале будут меньше двух миллиметров. Этот блендер не следует использовать для еды, поскольку его очистка не удалит токсичные следы в достаточной степени.

Как создать зашифрованный USB

Храните данные только на зашифрованных дисках. Это необходимо, если вы хотите использовать отдельный USB-накопитель LUKS вместо постоянного хранилища на USB-накопителе Tails, как рекомендовано в Лучшие практики Tails[48]. LUKS† — это стандарт шифрования Linux. Чтобы зашифровать новый USB-накопитель, перейдите в **Applications → Utilities → Disks**.

- Когда вы вставите USB, в списке должно появиться новое «устройство». Выберите его и убедитесь, что описание (бренд, название, размер) соответствует вашему устройству. Будьте осторожны, чтобы не ошибиться!
- Отформатируйте его, нажав ⚙ → **Форматировать диск**.
  - В раскрывающемся списке Стереть выберите **Перезаписать существующие данные нулями**. Обратите внимание, что этого недостаточно для удаления всех следов конфиденциальных документов, хранящихся на USB-накопителе.
  - В раскрывающемся списке «Разбиение на разделы» выберите пункт **«Совместимо со всеми системами и устройствами (MBR/DOS)»** .
  - Затем нажмите **«Форматировать»**

[48] anarsec.guide/ru/posts/tails-best/#ispol-zovanie-perekliuchatelia-zashchity-ot-zapisi

Реально удалить данные с USB

Нажатие «Удалить навсегда» или отправка файлов в «корзину» не удаляет данные… и их можно очень легко восстановить. Когда вы «удаляете» файл, вы просто сообщаете операционной системе, что вам больше не интересно содержимое этого файла. Затем она удаляет его запись в индексе существующих файлов. Затем она может повторно использовать пространство, которое занимали данные, для записи чего-то другого.

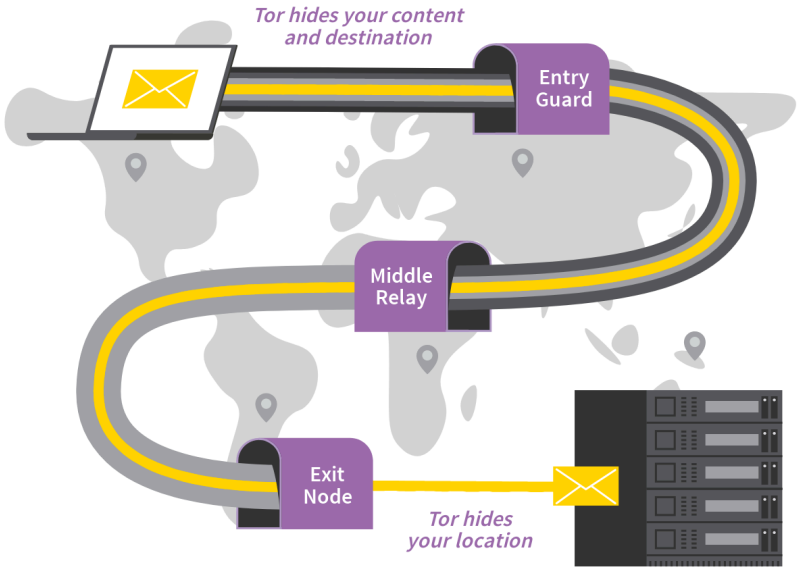
Однако могут пройти недели или годы, прежде чем это пространство будет фактически использовано для новых файлов, и в этот момент старые данные фактически исчезнут. В то же время, если вы посмотрите непосредственно на то, что записано на диск, вы можете найти содержимое файлов. Это довольно простой процесс, автоматизированный многими программами, которые позволяют вам «восстанавливать» или «восстанавливать» данные. Вы не можете на самом деле удалить данные, но вы можете перезаписать данные, что является частичным решением.

Существует два типа накопителей: магнитные (HDD) и флэш-накопители (SSD, NVMe, USB, карты памяти и т. д.). Единственный способ стереть файл на любом из них — переформатировать весь диск[47] и выбрать **«Перезаписать существующие данные нулями»**.

Однако следы ранее записанных данных все еще могут остаться. Если у вас есть конфиденциальные документы, которые вы действительно хотите стереть, лучше всего физически уничтожить USB после его переформатирования. К счастью, USB-накопители дешевы и их легко украсть. Обязательно переформатируйте диск перед его уничтожением; уничтожение диска часто является частичным решением. Данные все еще можно восстановить с фрагментов диска, а сжигание

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

делает обходной путь через три промежуточных ретранслятора. Браузер Tor использует сеть Tor, но другие приложения также могут это делать, если они правильно настроены. Все стандартные приложения, включенные в Tails, используют Tor, если им нужно подключиться к Интернету.



Интернет-трафик, включая IP-адрес конечного пункта назначения, шифруется слоями, как луковица. Каждый прыжок по трем ретрансляторам удаляет один слой шифрования. Каждый ретранслятор знает только ретранслятор до него и ретранслятор после него (выходной ретранслятор знает, что он пришел со среднего ретранслятора и что он идет на такой-то веб-сайт, но не входной ретранслятор).

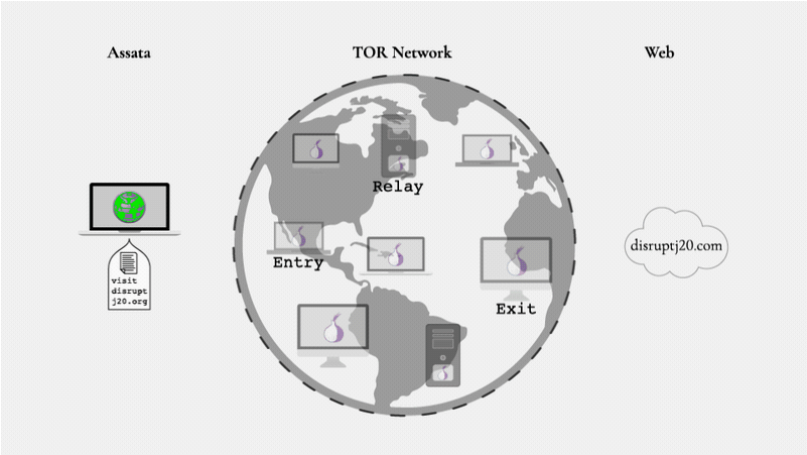


Рис. 1. See *anarsec.guide* for the animation.

Это означает, что любые посредники между вами и входным реле знают, что вы используете Tor, но они не знают, на какой сайт вы переходите. Любые посредники после выходного реле знают, что кто-то в мире переходит на этот сайт, но они не знают, кто это. Веб-сервер сайта видит, что вы заходите с IP-адреса выходного реле.

Tor имеет несколько ограничений. Например, если кто-то с техническими и юридическими средствами считает, что вы подключаетесь с определенного соединения Wi-Fi, чтобы посетить определенный сайт, он может попытаться сопоставить ваше соединение Wi-Fi с активностью на сайте («атака корреляции»). Однако, насколько нам известно, этот тип атаки сам по себе никогда не использовался для обвинения кого-либо в суде. Для конфиденциальных действий используйте интернет-соединения, которые не привязаны к вашей личности, чтобы защитить себя в случае сбоя Tor.

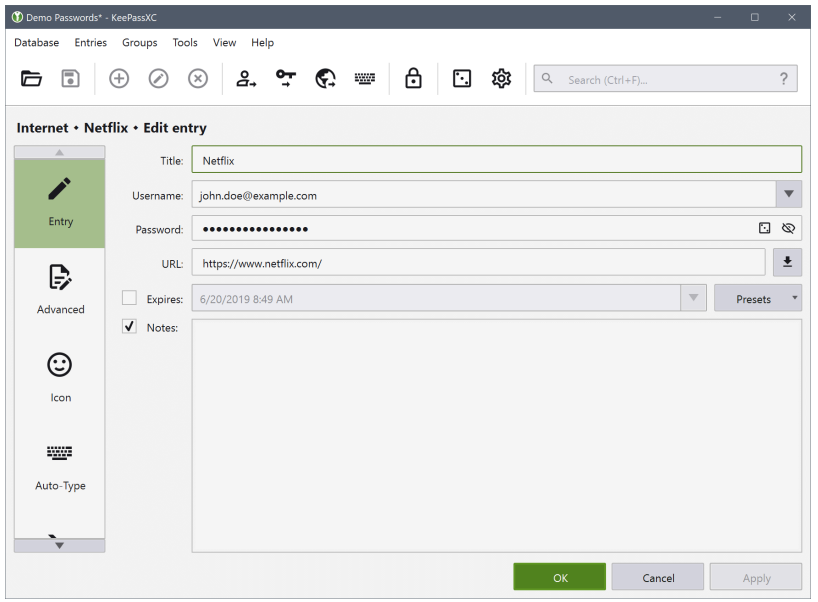
Что такое HTTPS?

Практически все веб-сайты сегодня используют HTTPS† — S означает «безопасный» (например, `https://www.anarsec.guide`). Если вы попытаетесь посетить веб-сайт без `https://`

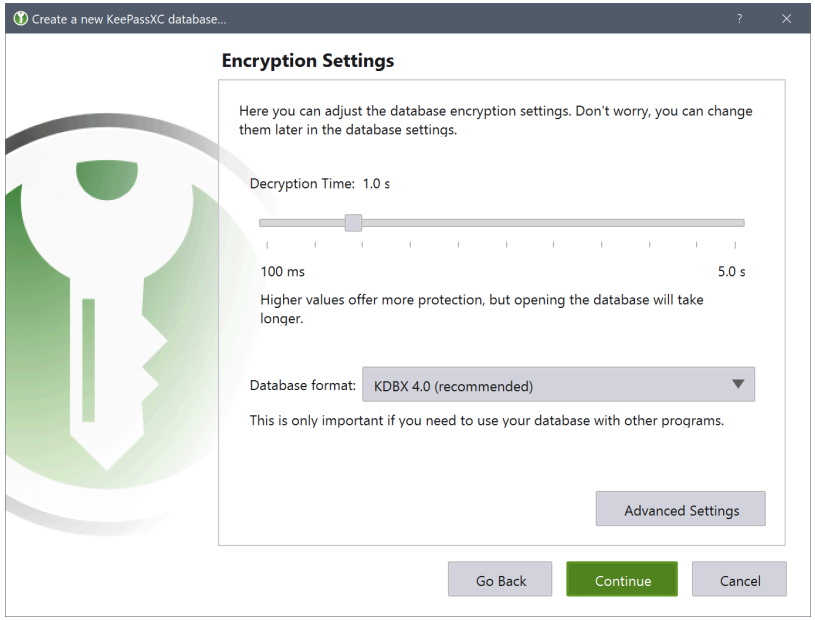
кируется. Убедитесь, что вы не забыли свою парольную фразу KeePassXC.

После создания самой базы данных вы должны увидеть пустую папку «Root». Если вы хотите организовать свои пароли в разные группы, щелкните правой кнопкой мыши эту папку и выберите «New Group...».

Теперь вы можете добавить свою первую запись. Нажмите **Записи → Новая запись** или нажмите значок «плюс». Введите название учетной записи, ваше имя пользователя для учетной записи и ваш пароль. Нажмите значок «кубик», чтобы сгенерировать случайный пароль или парольную фразу для записи.



Чтобы скопировать пароль из базы данных, выберите запись и нажмите CTRL + C. Чтобы скопировать имя пользователя, выберите запись и нажмите CTRL + B.



При создании новой базы данных KeePassXC[44] увеличьте время расшифровки в окне **настроек шифрования** со значения по умолчанию до максимального (5 секунд). Затем выберите надежную парольную[45] фразу и сохраните файл KeePassXC. Мы рекомендуем вам нажать на значок с маленьким кубиком в поле пароля, чтобы сгенерировать случайную парольную фразу из 7-10 слов.

Этот файл базы данных KeePassXC будет содержать все ваши пароли/парольные фразы и должен сохраняться между сеансами на вашем постоянном хранилище или на отдельном USB-накопителе с шифрованием LUKS, как описано в Лучшие практики Tails[46]. Как только вы закроете KeePassXC или не будете использовать его в течение нескольких минут, он забло-

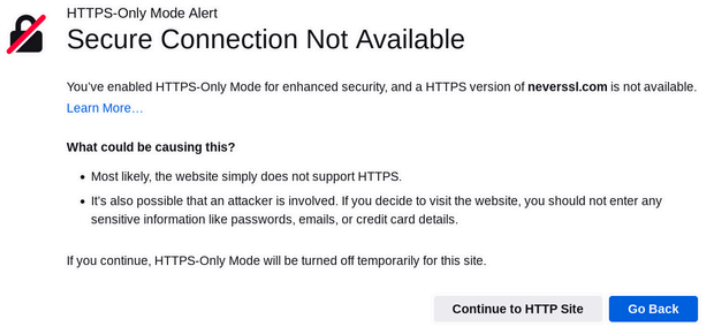
[44] tails.net/doc/encryption_and_privacy/manage_passwords/index.ru.html#index1h1

[45] anarsec.guide/ru/posts/tails-best/#paroli

[46] anarsec.guide/ru/posts/tails-best/#ispol-zovanie-perekliuchatelia-zashchity-ot-zapisi

Tor Browser, вы получите предупреждение перед продолжением. Если вы видите `http://` вместо `https://` перед адресом веб-сайта, это означает, что все посредники после выходного реле сети Tor знают, чем вы обмениваетесь с веб-сайтом (включая ваши учетные данные). HTTPS означает, что цифровая запись того, что вы делаете на посещаемом вами сайте, защищена ключом шифрования, принадлежащим сайту. Посредники после выходного реле будут знать, что вы посещаете riseup.net, например, но у них не будет доступа к вашим электронным письмам и паролям, и они не будут знать, проверяете ли вы свои электронные письма или читаете случайную страницу на сайте. Маленький замок появляется слева от адреса сайта, когда вы используете HTTPS.

Если на замке есть желтое предупреждение, это означает, что некоторые элементы на просматриваемой вами странице не зашифрованы (они используют HTTP), что может раскрыть точную страницу или позволить посредникам частично изменить страницу. По умолчанию браузер Tor использует режим HTTPS-Only, чтобы запретить пользователям посещать сайты HTTP.



HTTPS необходим как для ограничения вашего веб-отпечатка, так и для предотвращения изменения посредником данных, которыми вы обмениваетесь с веб-сайтами. Если посред-

ник не может расшифровать данные, он не может их изменить. Для обзора соединений HTTP / HTTPS с Tor и без него, а также того, какая информация видна различным третьим лицам, см. интерактивную графику EFF[31].

Короче говоря, не посещайте сайты, которые не используют HTTPS.

Onion Services: что такое .onion?

Вы когда-нибудь видели странный адрес веб-сайта с 56 случайными символами, заканчивающийся на .onion? Это называется onion-сервис, и единственный способ посетить веб-сайт, используя такой адрес, — использовать Tor Browser. «Deepweb» и «darkweb» — это термины, которые были популяризированы в СМИ для описания этих onion-сервисов.

Любой может создать сайт .onion. Но зачем им это? Ну, местоположение сервера анонимно, поэтому власти не могут узнать, где размещен сайт, чтобы закрыть его. Когда вы отправляете данные на сайт .onion, вы входите в три ретранслятора Tor этого сайта после стандартной цепи Tor. Таким образом, между нами и сайтом есть 6 ретрансляторов Tor; мы знако общие случаи использования, имеющие отношение к анархистам, но для получения дополнительной информации прочтите документацию.

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

Менеджер паролей (KeePassXC)

Когда вам нужно знать много паролей, может быть приятно иметь безопасный способ их хранения (т. е. не листок бумаги рядом с вашим компьютером). KeePassXC — это менеджер паролей, включенный в Tails (**Приложения → Избранное → KeePassXC**) который позволяет вам хранить ваши пароли в файле и защищать их одним главным паролем.

Мы рекомендуем вам разбить ваши пароли на отсеки — иметь отдельный файл KeePassXC для каждого отдельного проекта. Они могут использовать один и тот же главный пароль — смысл разбиения в том, что только пароли одного проекта разблокируются в любой момент времени. Если сеанс Tails будет скомпрометирован, злоумышленник не получит все ваши пароли одним махом, а только те, которые в данный момент разблокированы.

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

к чужому компьютеру, что мы не рекомендуем[35]. Длинный адрес .onion можно передать через другой канал (например, созданный вами Riseup Pad[36] , который легче набирать).

Усложните корреляционные атаки

Когда вы запрашиваете веб-страницу через веб-браузер, сервер сайта отправляет ее вам небольшими «пакетами», имеющими определенный размер и время (среди прочих характеристик). При использовании браузера Tor последовательность пакетов также может быть проанализирована для поиска шаблонов, которые могут быть сопоставлены с шаблонами веб-сайтов. Чтобы узнать больше, см. «1.3.3. Passive Application-Layer Traffic Patterns»[37]. Tor планирует смягчить эту проблему в будущем[38].

Чтобы затруднить эту «корреляционную атаку»†, отключите JavaScript, используя в браузере Tor настройку **«Безопаснее»**.

Кроме того, команда Tor рекомендует выполнять несколько задач одновременно[39] с помощью клиента Tor.

Включенное программное обеспечение

Tails поставляется со многими приложениями[40] по умолчанию. Документация дает обзор интернет-приложений[41], приложений для шифрования и конфиденциальности[42], а также приложений для работы с конфиденциальными документами[43]. В оставшейся части этого раздела мы рассмотрим только

[35] anarsec.guide/ru/posts/tails-best/#snizhenie-riskov-pri-ispol-zovanii-nenadezhnykh-komp-iuterov
[36] pad.riseup.net/
[37] spec.torproject.org/proposals/344-protocol-info-leaks.html
[38] gitlab.torproject.org/tpo/team/-/wikis/Sponsor-112
[39] blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations/
[40] tails.net/doc/about/features/index.ru.html
[41] tails.net/doc/anonymous_internet/index.ru.html
[42] tails.net/doc/encryption_and_privacy/index.ru.html
[43] tails.net/doc/sensitive_documents/index.ru.html

ем первые 3 ретранслятора, сайт знает последние 3, и каждый узел Tor знает только ретранслятор до и после. В отличие от обычного веб-сайта HTTPS, все это зашифровано Tor от начала до конца.

Это означает, что и клиент (ваш ноутбук), и сервер (где находится сайт) остаются анонимными, тогда как с обычным сайтом анонимным является только клиент. Помимо того, что он более анонимен для сервера, он также более анонимен для клиента: вы никогда не покидаете сеть Tor, поэтому перехватить вас после выхода из реле невозможно.

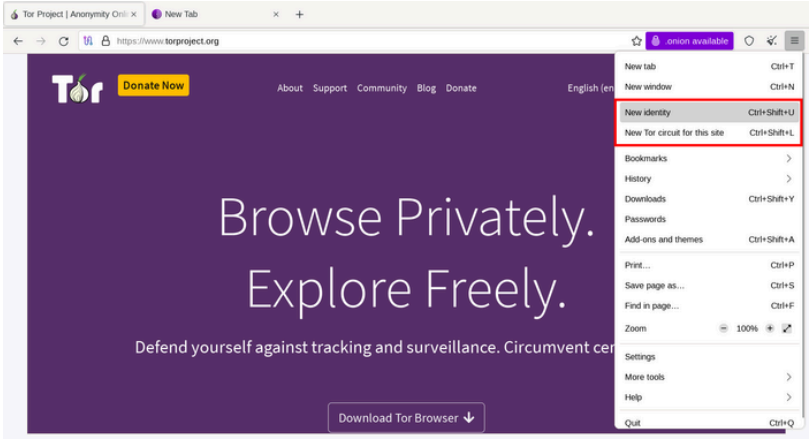
Адрес сайта .onion длинный, так как он включает сертификат сайта. HTTPS не нужен; безопасность зависит от знания адреса сайта .onion.

Некоторые сайты предлагают как классический URL, так и адрес .onion. В этом случае, если сайт был настроен на это, рядом с URL должно появиться указание «.onion available». Если нет, иногда сайт будет указывать адрес .onion где-то на своей странице. Чтобы узнать адреса сайтов, которые доступны только как .onion, вам нужно будет либо найти их по сарафанному радио, либо через веб-сайты, на которых перечислены другие сайты .onion, например, эта страница GitHub[32].

Сайты, которые блокируют Tor

Некоторые сайты блокируют пользователей, которые заходят через сеть Tor, или иным образом делают посещение сайта неудобным. Некоторые сайты могут заставить вас заполнить CAPTCHA или предоставить дополнительную личную информацию (ID, номер телефона…) перед продолжением, или они могут вообще заблокировать Tor.

[32] github.com/alecmuffett/real-world-onion-sites



Сайт может блокировать только определенные ретрансляторы Tor. В этом случае вы можете изменить узел выхода Tor, используемый для этого сайта: нажмите кнопку ⍰ → **«Новый контур Tor для этого сайта»**. Контур Tor (путь) изменится для текущей вкладки, включая другие открытые вкладки или окна с того же сайта. Вам может потребоваться сделать это несколько раз подряд, если вам не повезло и вы столкнулись с несколькими заблокированными ретрансляторами.

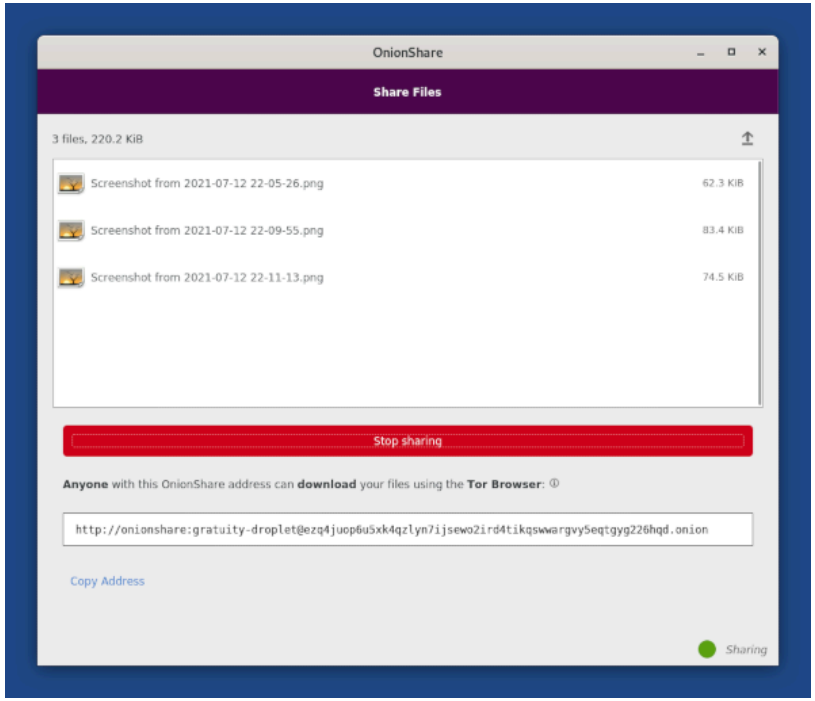
Поскольку все ретрансляторы Tor являются публичными, возможно, что сайт блокирует всю сеть Tor. В этом случае вы можете попробовать использовать прокси для доступа к сайту, например `https://hide.me/en/proxy` (но только если вам не нужно вводить личную информацию, например учетные данные для входа). Вы также можете проверить, сохранена ли страница, к которой вы хотите получить доступ, на Wayback Machine: `web.archive.org`.

Четко разделяйте анонимные личности

Не рекомендуется выполнять различные интернет-задачи, которые не должны быть связаны друг с другом во время одного сеанса Tails. Вы должны тщательно разделять различные (контекстные) личности! Например, опасно проверять

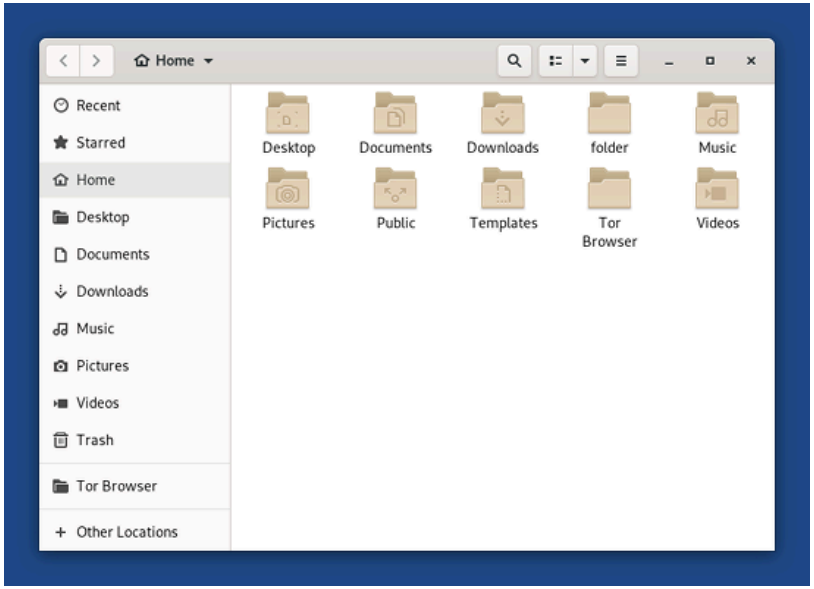
большие файлы через постоянную папку Tor Browser, которая использует USB вместо оперативной памяти.

Делитесь файлами с Onionshare



Можно отправить документ через ссылку .onion благодаря OnionShare[34] (**Приложения → Интернет → OnionShare**). По умолчанию OnionShare останавливает скрытый сервис после того, как файлы были загружены один раз. Если вы хотите предложить файлы для многократной загрузки, вам нужно перейти в настройки и снять флажок «Остановить общий доступ после первой загрузки». Как только вы закроете OnionShare, отключитесь от Интернета или выключите Tails, файлы больше не будут доступны. Это отличный способ поделиться файлами, поскольку вам не нужно подключать USB

[34] tails.net/doc/anonymous_internet/onionshare/index.ru.html



Выгрузка

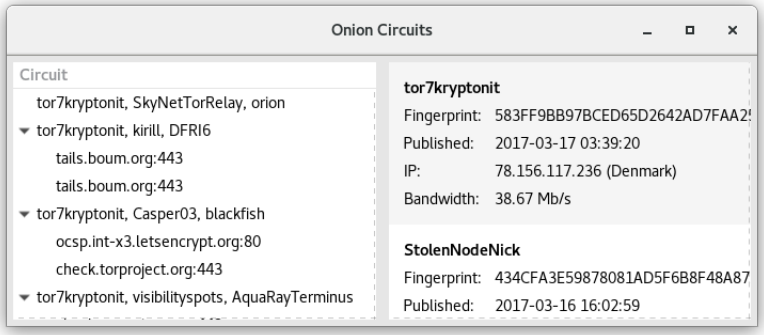
Аналогично, если вы хотите что-то загрузить с помощью Tor Browser (например, включить файл в сообщение в блоге), вам сначала нужно будет переместить или скопировать файл в папку Tor Browser. Затем он будет доступен, когда вы выберете файл для загрузки в Tor Browser.

RAM

Имейте в виду, что если вы загружаете или иным образом работаете с очень большими файлами, ваша оперативная память (RAM) может заполниться. Это происходит потому, что весь сеанс Tails выполняется в оперативной памяти (если вы не настроили постоянное хранилище, которое использует USB). Если оперативная память заполнится, Tails замедлится или выйдет из строя. Вы можете смягчить это, закрыв ненужные приложения и удалив другие загруженные вами файлы. В худшем случае вам может потребоваться временно включить постоянное хранилище, чтобы загружать или выгружать

свою личную электронную почту и публиковать анонимный текст во время одного сеанса. Другими словами, вы не должны быть идентифицируемы и анонимны в сети Tor одновременно. Вы также не должны использовать сеть Tor под псевдонимом A и псевдонимом B в одном сеансе, так как эти псевдонимы могут быть связаны через контролируемый или скомпрометированный выходной ретранслятор Tor. Выключайте и перезапускайте Tails между интернет-активностями под разными личностями!

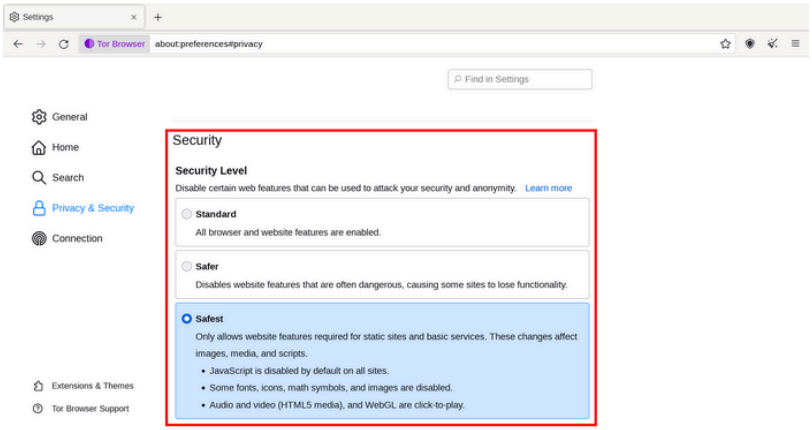
Функция «Новая идентификация» браузера Tor недостаточна для полного разделения контекстных идентификаций в Tails, поскольку она не восстанавливает соединения за пределами браузера Tor, и вы сохраняете тот же узел входа Tor. Перезапуск Tails — лучшее решение.



Приложение Onion Circuits показывает, какой канал Tor использует соединение с сервером (веб-сайтом или иным). Иногда бывает полезно убедиться, что выходной ретранслятор не находится в определенной стране, чтобы быть дальше от самого простого доступа для следственных органов. В приведенном выше примере соединение с check.torproject.org проходит через ретрансляторы tor7kryptonit, Casper03 и выходной узел blackfish. При нажатии на канал на правой панели отобразятся технические сведения о его ретрансляторах. Функция «Новый идентификатор» браузера Tor полезна для

изменения этого выходного ретранслятора без перезапуска сеанса Tails, который можно повторять до тех пор, пока у вас не будет выходного ретранслятора, который вас устроит. Мы не рекомендуем использовать «Новый идентификатор» для переключения между идентификаторами, но только если вы хотите изменить выходной узел в рамках действий одного и того же идентификатора.

Настройки безопасности браузера Tor



Как и любое программное обеспечение, Tor Browser имеет уязвимости, которые могут быть использованы — различные полицейские агентства имеют эксплойты Tor Browser для серьезных случаев. Чтобы смягчить это, важно поддерживать Tails в актуальном состоянии, и вам следует повысить параметры безопасности Tor Browser: щелкните значок щита, а затем щелкните **Настройки…**. По умолчанию он установлен на Стандартный, что обеспечивает возможности просмотра, сопоставимые с обычным браузером. **Мы настоятельно рекомендуем вам установить его на самые строгие настройки, прежде чем вы начнете просмотр: Самый безопасный**. Подавляющее большинство эксплойтов против Tor Browser не будут работать с настройкой Самый безопасный.

Макет некоторых страниц может быть изменен, а некоторые типы контента могут быть отключены (изображения SVG, видео с кликом и т. д.). Например, у anarsec.guide есть две вещи, которые будут сломаны в безопасном режиме, поскольку они полагаются на Javascript: темный режим и оглавление статьи. Некоторые сайты вообще не будут работать с этими ограничениями; если у вас есть основания доверять им, вы можете просматривать их с менее строгими настройками для каждого сайта. Помните, что настройки «Стандарт» и «Безопаснее» позволяют работать скриптам, что может нарушить вашу анонимность[33] в худшем случае.

Загрузка/выгрузка и папка Tor Browser

Tor Browser на Tails хранится в «песочнице»[†], чтобы предотвратить его от слежки за всеми вашими файлами, если вредоносный сайт скомпрометировал его. Это означает, что существуют особые соображения при загрузке или скачивании файлов с помощью Tor Browser.

Загрузка

Когда вы что-то загружаете с помощью Tor Browser, оно сохраняется в папке Tor Browser (`/home/amnesia/Tor Browser/`), которая находится внутри песочницы. Если вы хотите что-то сделать с файлом, вам следует переместить его из папки Tor Browser. Для этого `/home/amnesia/Tor Browser/` вы можете использовать файловый менеджер (**Applications → Accessories → Files**).

[33] arstechnica.com/information-technology/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/