Основные принципы

В наше смутное время использование информационных технологий может как спасти вашу жизнь, так и существенно её осложнить, особенно если вы — один из миллионов прекрасных беларусов с активной гражданской позицией, но без специализированного образования в анамнезе.

Эта статья ставит своей целью разъяснить базовые понятия информационной безопасности простым языком, чтобы помочь вам избежать типичных ошибок, которые могут быть использованы против вас бандитами в балаклавах. Изложенные здесь правила не являются ни панацеей, ни гарантией безопасности, но следование им существенно повысит ваши шансы.

Начнём, однако, не с технологий, а с нескольких базовых принципов, на которых строится любая система безопасности.

Принцип слабого звена

Прочность системы безопасности равна прочности её самого слабого звена. Поэтому нужно внимательно следить за тем, чтобы все меры вами применялись последовательно и в комплексе, не оставляя сквозных дыр в стенах из чистого вибраниума.

Принцип неуловимого Джо

Сложнее всего взломать не ту дверь, в которой самый надёжный замок, а ту, о существовании которой вы даже не подозреваете. Поэтому по возможности стоит не просто шифроваться но ещё и надёжно прятать зашифрованное.

Принцип разумной достаточности

Абсолютной защиты не существует, существует лишь защита, взломать которую стоит дороже, чем получаемая от взлома выгода. Вы должны чётко себе представлять, какой уровень безопасности достаточен именно в вашем случае, и стараться не заплывать за эти буйки слишком далеко.

"Почему же? — скажете вы, — Безопасности ведь слишком много не бывает!"

Бывает. Дело в том, что каждый новый уровень защиты делает вашу жизнь чуть менее комфортной, вызывая накопленную усталость и назойливое желание снять бронежилет хоть на минуточку. В итоге вы можете совершить ошибку, которая (принцип слабого звена) может разом скомпрометировать всю вашу защиту. Бегите медленнее — дальше добежите.

Чтобы помочь вам понять, где стоит остановиться, все изложенные ниже приёмчики кибербезопасного кунг-фу разбиты на уровни по мере увеличения ваших затрат и снижения комфорта повседневной жизни.

Нулевой уровень: личная гигиена

Тут поговорим об общих правилах информационной гигиены, которые стоит соблюдать везде и всегда — вне зависимости от степени испорченности текущей власти. То есть даже после победы.

Сразу оговорюсь: эти правила, хоть и полезны в целом, мало помогут, если вас вежливо попросят самостоятельно сдать пароли и явки, дав понять, что иначе вам проломят дубинкой голову. Но это уже другой уровень сумрака, до которого может и не дойти. Дальше, кстати, поговорим о способах выхода даже из такой ситуации. Да, они есть.

Всегда используйте HTTPS

Вот так вот сразу бабах — и технический термин, чтобы вы не расслаблялись. Без паники! Я сейчас всё объясню.

Адрес любой странички в интернете начинается с так называемого "протокола", который сообщает вашему браузеру как именно подключаться к вебсайту. Два протокола, о которых мы сегодня поговорим, это `http://` и `https://`. Казалось бы, мелочь, разница лишь в одной букве, но буква эта означает "secure" ("безопасный"), то есть для нашей с вами беседы — это самая важная буква. Проще говоря...

HTTPS — это безопасный HTTP

Чтобы стало ещё понятнее, расскажу, какую именно безопасность добавляет эта буква:

- **Полное шифрование всего, что происходит между вами и вебсайтом.** Сторонний наблюдатель может понять, на какой вебсайт вы зашли, но не узнает ни какие страницы вы посещали, ни какие данные передавали.
- **Подтверждение подлинности вебсайта.** Вы можете быть уверены, что открыв страничку `https://tut.by`, вы увидите именно её, а не совершенно посторонний вебсайт, прикидывающийся ТУТ.баем с целью украсть ваши персональные данные или чего похлеще.
- **Подтверждение подлинности контента.** Вы можете быть уверены, что на страничке `https://tut.by` вы увидите именно то, что опубликовала там редакция ТУТ.бай — ни больше, ни меньше.

Хочу! Что делать?

Как минимум следить, чтобы всегда, на какой бы вебсайт вы ни заходили, слева от его адреса в вашем браузере стоял "замочек" — таким образом все современные браузеры сообщают вам, что соединение с сайтом использует "безопасный" протокол `https://`.

Следите за тем, чтобы ссылки, по которым вы переходите, также включали в себя `https://` в начале адреса. Практически все браузеры на компьютере позволяют вам увидеть ссылку до того, как вы по ней перейдёте. В мобильных браузерах, к сожалению, ситуация похуже.

Добавляйте `https://` сами, если вводите адрес сайта вручную. Дело в том, что когда вы вводите в строку адреса "tut.by", ваш браузер автоматически добавляет пропущеный протокол. И знаете, какой именно? Правильно, "небезопасный" `http://`. К счастью, технически грамотные разработчики вебсайтов настраивают их таким образом, чтобы сразу перенаправить ваш браузер на "безопасный" `https://`, но самый первый запрос всё равно проходит по `http://`, и может оказаться тем самым слабым звеном.

Настройте автоматическую блокировку всех устройств

Все ваши девайсы (смартфоны, планшеты, компьютеры и т.д.) должны быть заблокированы паролем или пин-кодом. Не используйте разблокировку по отпечатку пальца и лицу — доступ к ним слишком просто получить, скажем так, без вашего согласия.

Разблокировка "паттерном", типичная для девайсов на Андроид, в принципе, тоже неплохой вариант, однако ваш палец зачастую оставляет хорошо видимые следы на неидеально чистом экране, поэтому пользуйтесь с осторожностью, особенно в неоднозначных ситуациях.

Также, настройте автоматическую блокировку компьютера после пяти минут простоя. Это более-менее разумный баланс между паранойей и удобством.

Включите щифрование данных на компьютере

Все современные десктопные операционные системы (Windows, MacOS, вот это вот всё) умеют шифровать данные на дисках. Это нужно для того, чтобы затруднить их извлечение с заблокированного паролем компьютера. Если шифрование не включено, данные извлекаются примерно за минуту безо всякого пароля, так что будьте бдительны, помните о принципе слабого звена. Шифование обычно включено по умолчанию, но не помешает убедиться. Инструкция для MacOS тут, инструкция для Windows тут. Если у вас Linux, то вы и так всё знаете :)

Чтобы ещё больше усложнить жизнь супостатам, можете настроить свой ноутбук на полное выключение по закрытию крышки. Да, именно не sleep, а shut down. Так что-либо вытянуть с него без пароля будет ещё сложнее, а захлопнуть крышку можно успеть почти всегда.

Кстати, о паролях.

Используйте хорошие пароли

Нигде. Никогда. Ни при каких обстоятельствах не используйте пароль или пин-код в виде вашей даты рождения. И не вашей тоже не надо. Помните, найти эти даты — дело нескольких минут.

Использовать один и тот же пароль более чем для одного сервиса — тоже чрезвычайно плохая идея. Причина банальна: узнают один — узнают все.

Ну а про записывание паролей на бумажке, наверное, даже объяснять не стоит, правда?

Однако, удивлю вас сейчас. Для нулевого уровня нашего кунг-фу, помня о принципе разумной достаточности, я бы не рекомендовал заводить для каждого сервиса пароль типа "!q5V*U*Oiy@R", так как запомнить более двух-трёх таких нереально, а про менеджеры паролей мы с вами ещё не разговаривали. В итоге вы, скорее всего, скатитесь либо к записыванию на бумажке, либо к использованию одного пароля для всего подряд.

Что же делать?

Я бы рекомендовал использовать словестные пароли — то есть сочетание трёх-четырёх совершенно случайных слов, типа "ChairTigerBoing". Такие пароли неизмеримо проще запоминать, плюс проще вводить даже если они достаточно длинные, так как наши пальцы больше привычны к набору слов, чем спец-символов, особенно на клавиатуре смартфона. Ну а стойкость к взлому у них вполне достаточна — подчеркну ещё раз — для нулевого уровня.

Настройте блокировку в Телеграме

Конечно же, куда без него. Да, есть ещё более защищённые мессенджеры (превед, Signal, поговорим о тебе позже), но в современных беларуских реалиях Телеграм — однозначный король песочницы, поэтому про него отдельной строкой на каждом уровне.

Зайдите в настройки конфиденциальности Телеграма (Privacy and Security) и включите код-пароль (Passcode Lock) — теперь Телеграм будет периодически блокироваться и вам придётся вводить пин-код для его разблокировки.

В тех же настройках конфиденциальности включите двухэтапную аутентификацю (Two-Step Verification). Это значительно затруднит недоброжелателям логин в ваш Телеграм эккаунт с другого устройства. Далее я объясню почему стандартной СМС аутентификации недостаточно.

Уровень первый: мелкие шалости

Тут поговорим о правилах, которые должен собдюдать каждый борец с несправедливостью, даже если борьба эта происходит преимущественно с дивана. Потому что иногда могут прийти и к дивану.

Да, лайкать котанов станет чутка менее удобно, но тут уж надо выбирать.

Очистите историю браузера

Полностью очистите историю браузера в телефоне и на компьютере. Начиная с этого момента для просмотра революционной прессы и прочих сомнительных мероприятий вы будете пользоваться исключительно режимом "инкогнито". Или, как его называют Edge и Firefox, "приватным" режимом.

В этом режиме браузер старается (как может) не оставлять никаких следов вашей жизнедеятельности на девайсе. Нетерпеливых прошу остыть, про VPN, Tor и Tails поговорим на следующих уровнях.

Полностью переходить на "инкогнито" не стоит. Помните, мы тут пока что не с транснациональными корпорациями боремся, а с бандой троечников-неудачников в балаклавах. Так что пользуйтесь любыми условно-безопасными сервисами в обычном режиме с сохранением всех явок и паролей. Пускай смотрят ваших котанов и считают, что кроме них вы ничего не лайкаете. Принципы неуловимого Джо и разумной достаточности в деле!

Анонимизация профиля Телеграма

Если не хотите, чтобы о вашем участии в протестных чатах стало известно кому-не-следует, позаботьтесь о том, чтобы ваш профиль в Телеграме было непросто связать с вашей реальной личностью. А именно:

- Измените фото профиля на что-нибудь абстракное. Можно в бело-красно-белых тонах.
- Измените имя на никак не связанное с настоящим. То есть если вас зовут Катя, назовитесь хоть Виссарионом, главное чтобы не "Кейти1997". Ну или будьте как Маск, назовите себя "X Æ A-12".

- Измените свой никнейм таким же образом. Потому что глупо иметь имя "X Æ A-12" и ник @vitaly.kurochkin (имя только что придумал, если ты реально есть — прости, братан).
- Зайдите в настройки приватности и настройте всё по принципу "никому ничего не показывать". Потому что друзья вас и так узнают, а с остальными общаться будете после победы.

А вот тут давайте приостановимся и добавим немного паранойи. Вся эта анонимность хороша и полезна, но вспомним принцип слабого звена. Если вы уже засветились в каком-либо публичном чате (а мы будем считать таковым любой чат, в котором есть хотя бы один человек, которого вы лично не знаете) под реальным именем и с дырявыми настройками приватности, существует риск того, что ваши данные уже записаны в пыльную тетрадку товарища майора. Если вы теперь измените своё имя и примените безопасные настройки, вы дадите владельцу тетрадки "мостик" между настоящей и анонимной личностью, так как все ваши предыдущие сообщения "переподпишутся" новым именем. Что делать? Либо рисковать, либо заводить новый, изначально безопасный и анонимный эккаунт в Телеграме — решайте исходя из степени предыдущей "засветки" и крамольности планов на будущее, пользуясь принципом разумной достаточности.

И ещё немного паранойи: удалите из адресной книги в телефоне явно устаревшие контакты. Дело в том, что Телеграм обычно доверяет вашим контактам немного больше, чем тем, кого в вашей адресной книге нет. А можете ли вы быть уверены, что номер телефона, который с 2003 года хранится у вас под именем "Семён Лакокраска" всё ещё принадлежит именно Семёну? Ну или кого вы там записали под этим именем…

Социальные сети

Анонимизировать эккаунты в социальных сетях особого смысла не имеет, так как это противоречит самой идее их существования: дать вам возможность оповестить весь мир о вашей позиции по любым вопросам и раскрыть кучу тайных подробностей вашей личной жизни впридачу.

Да, в некоторых сетях можно достаточно серьёзно "прикрутить" настройки приватности, чтобы ваши посты видели только "друзья", но тут нужно чётко понимать, что это, скорее, иллюзия безопасности, чем настоящая безопасность. Дело в том, что ваш социальный граф (список ваших "друзей", их "друзей" и т.д.), скорее всего, настолько широк, что вы не сможете поручиться за каждого лично. По статистике с 20% своих "друзей" вы не виделись более пяти лет, а с 3% вообще никогда не встречались. То есть вряд ли стоит доверять этим без сомнения замечательным людям вопросы вашей жизни и смерти.

Поэтому у вас есть три пути: - Удариться во все тяжкие и гори оно всё огнём. - Прикинуться аполитичным, то есть: постить и лайкать исключительно котанов и рецепты, на провокации не реагировать, ходить строем. Ну или просто удалить/заморозить эккаунт. - Создать новый, не связаный с вашей реальной личностью эккаунт. Ниже я расскажу, как это сделать относительно безопасно, но повторный путь к славе будет долог и тернист, так как вам придётся набирать новый соцальный граф "на голом таланте", без помощи личных связей, чтобы не раскрыться.

Идём во все тяжкие!

Ну что ж, браво! Я бы тоже так сделал, по двум причинам: во-первых, в единстве — наша сила, а во-вторых... мелкие шалости иногда помогают замаскировать шалости гораздо большего калибра, если ваш профиль по уровню экстремизма уложится в бандитский стереотип об обыкновенном "бесхребетном борцуне". Понятно, что это двойное дно имеет смысл только если под ним есть что скрывать.

Измените настройки приватности *фейсбучка* и *инсты* по принципу — друзьям всё, остальным ничего. Смените имя и фото профиля на абстрактного котана. Да, фейсбук позволяет менять настройки для всех ранее опубликованных постов. Да, вы сможете вернуть всё на место после победы. Да, всё это бесполезно.

Пользуетесь *вконтактиком* или *одноклассниками* для чего-либо небезопасного? Ну, во-первых, примите мои соболезнования. "Во-вторых", пожалуй, не будет, так как эти социальные сети находятся в зоне доступа врага, поэтому настраивать в них приватность — только углублять самообман.

КГБ читает ваши СМС

Страшно? Правильно. Система доставки СМС стара примерно как ВРИО президента и также несостоятельна в современном мире. Даже внешние (по отношению к операторам мобильной связи) хакеры могут в некоторых случаях получить к ней доступ, используя несколько известных уязвимостей, что уж тут говорить про сотрудника условного МТС, млеющего в присутствии товарища полковника то ли КГБ, то ли ФСБ, то ли обоих сразу.

Главное отличие СМС от, скажем, Телеграма состоит в том, что все ваши входящие и исходящие сообщения достаточно долгое время хранятся на серверах оператора. То есть физически, юридически и "по понятиям" в зоне влияния наших недоблестных силовых структур. Тогда как для получения доступа к сообщениям на серверах Телеграма представителям этих структур придётся договариваться лично с Дуровым, а на такое феерическое шоу я бы с удовольствием посмотрел.

Тут надо, конечно, немного тормознуть и уточнить, что чтение вашей СМС-переписки дело достаточно ресурсозатратное, поэтому если на это и идут, то лишь в особых случаях. Однако, с учётом уровня возможных негативных последствий, следует всё же принять некоторые упредительные меры. А именно:

Не пользуйтесь СМС

... для обмена любой информацией, хотя бы потенциально полезной бандитам, так как всё, что может быть использовано против вас, будет использовано против вас.

Также помните, что удаление СМС с вашего телефона, как и с телефона вашего собеседника, не удаляет его с серверов оператора связи. То есть единожны отправленное уже никак не может быть вами скрыто. Такая вот безопасность.

Помните, что "логин через СМС" может быть скомпрометирован

Этой напасти подвержены почти все мессенджеры — те же Телеграм и Сигнал, Вайбер с Ватцапом, возможно, Скайп, если вы сдуру дали ему свой номер. Не остаются в стороне социальные сети и прочие онлайн сервисы с логином или возможностью восстановления пароля по СМС (привет, Фейсбук).

Причина проста: их разработчики излишне верят в надёжность и безопасность СМС-переписки. Что, в принципе, в какой-то степени верно... в странах, где представители силовых структур не премируются за превышение служебных полномочий. На нашем же родео возможно всё, поэтому мнимая безопасность оборачивается регулярным "угоном" эккаунтов и "сливами" частных переписок.

Удостоверьтесь, что любые сервисы, содержащие чувствительную информацию, защищены чем-либо ещё. Сервис слепо верит в пуленепробиваемость СМС? Хотите большей безопасности? Читайте дальше!

Уровень второй: красная шапочка

Я выхожу. Как сделать так, чтоб меня не съели волки? А если уж съели — так чтоб хоть не насовсем.

Заведите телефон для прогулок

Ваш смартфон сегодня — не только хранилище чуть ли не всей вашей личной информации, но и удобный ключ ко всем онлайн сервисам, которыми вы регулярно пользуетесь, поэтому его попадание в руки бандитов — весьма опасное событие, чреватое не только усугублением вашей и без того незавидной ситуации ("Ах ты, ..., на Нехту подписан, ...?!") но и далеко идущими малоприятными последствиями. Вся история переписки во всех мессенджерах и имейл-эккаунтах, личные фото и видео, списки контактов из адресной книги и история звонков, сохранённые в браузере пароли от соц-сетей и других сервисов, данные банковских карточек и других платёжных систем... всё это и много чего ещё осядет в вашем деле навсегда. Крепкий пароль и шифрование из нулевого уровня помогут в случае потери или кражи телефона, но они беспомощны против ментовской дубинки, особенно если на неё надет презерватив. Поэтому, самым стойким к взлому методом является банальное неношение вашего смартфона с собой на любые околопротестные мероприятия. Купите простую звонилку с кнопками, скиньте на неё основные контакты, переставьте в неё свою симку — и идите гулять ~~наздоровье~~ с миром.

Дополнительным бонусом будет имеющаяся почти во всех таких "бабушкофонах" функция SOS-звонка. Это такая большая красная кнопка, нажатие на которую рассылает СМС-ки определённому набору контактов или начинает звонить им по кругу. Сами понимаете, в какой ситуации это может оказаться полезным. Не дай бог, но всё-таки не в шахматы тут играем.

Отслеживание положения телефона в городе

И, кстати, если вы "гуляете" с включенным телефоном (любым), у меня для вас плохие новости: ваше положение можно отследить с точностью до нескольких десятков метров. Не очень точно, но достаточно, чтобы определить, что вы именно "гуляли". Это могут сделать только операторы связи и неустановленный, но значительно более широкий, чем нам бы хотелось, круг лиц, которым операторы предоставляют доступ к своей инфраструктуре. То есть бандиты.

Работает это без вашей активной помощи. Базовые станции сотовой связи примерно догадываются, насколько далеко ваш телефон находится от каждой из них. Да, очень приблизительно, но так как в городе базовых станций полно, можно достаточно легко всё усреднить и вычислить ваши координаты более-менее точно — если очень нужно.

И да, оператор узнает, что это были именно вы, даже если из телефона достать сим-карту, так как радиомодуль в вашем телефоне имеет уникальный идентификатор, который оператор "вспомнит" как принадлежащий именно вам некоторое время назад.

Что делать? Выключать телефон или включать на нём режим полёта. В этих случаях все передающие радиомодули телефона неактивны и, соответственно, внешние слушатели о расстоянии до них ничего не знают. Да, я в курсе, что можно подсадить вам на аппарат зловредный вирус, который заставит телефон "притворяться" выключенным и продолжать палить ваши координаты, но КГБ — отнюдь не NSA, да и вы, при всём уважении, не Сноуден, так что риск пренебрежимо мал. Но если вас это беспокоит, купите телефон, из которого можно физически достать батарею (да, такие ещё есть) и доставайте её на прогулках.

Чистый Телеграм

Если вы всё же решили взять смартфон на прогулку, предварительно отпишитесь от всяких эдаких каналов и удалите секретные чаты в Телеграме. Вернётесь домой вечером — подпишитесь снова. Не вернётесь — лучи поддержки вам.

Более хардкорный вариант — удалить Телеграм с телефона напрочь и переустановить вечером.

Установите полезные приложения

Тут будет что-нибудь про Nedze и красную кнопку.

Уровень третий: шапочка из алюминиевой фольги

Тут поговорим о том, чего можно добиться с использованием бесплатных (или платных, но недорогих) сервисов, а также некоторого дополнительного оборудования. Всё упомянутое ниже по уровню сложности должно быть доступно неискушённому пользователю. Точнее, моей ментальной модели неискушённого пользователя...

VPN

Кто не слышал этого слова из трёх букв? Оно льётся на нас из каждой второй рекламы на ютубчике. Обещают полную анонимность и безопасность. Врут, естественно, но давайте разберёмся. Простите за многобукв, но уж больно важная тема.

Что такое VPN, на пальцах?

Это сервис, благодаря которому ваше устройство "выходит в интернет" не напрямую, а через какой-то неизвестный шлюз, обычно находящийся в далёкой стране победившей демократии. Ну это как если бы вы чайник включали не в свою розетку, а через удлинитель в розетку свободного от предрассудков соседа. Вот VPN и есть этот самый удлинитель, только для интернета.

Кстати, как и с удлинителем, сторонний наблюдатель не сможет понять, что именно вы через него "подключили". Примерно измерить количество проходящего тока-трафика — сможет, но понять чайник это или, скажем, тостер — нет, потому что любой VPN-канал очень неплохо зашифрован.

Чем хорош VPN?

Бонус номер один: на вас перстаёт распространяться местная цензура, так как с точки зрения интернета вы находитесь в другой стране, в которой запрещать Нашу Ніву в голову никому ещё не пришло.

Бонус номер два: можно относительно безнаказанно заниматься всякими делишками, о которых местным бандитам лучше не знать. Они будут видеть,

что с вашего устройства проложен пуленепробиваемый канал связи до VPN сервера, но что вы через этот канал там делаете они не увидят. Только имейте в виду, что если эти делишки не понравятся полиции в той стране, через которую вы вышли в эфир, вас могут прикрыть оттуда. Так что с нашим режимом боритесь неистово, но законы нормальных стран нарушать не стоит, вам потом с ними этими руками дружить.

Бонус номер три: вас немного сложнее опознать, так как ваш IP адрес (более-менее уникальный адрес устройства в интернете, по которому вас можно идентифицировать в реале) с точки зрения вебсайта или другого сервиса, которым вы пользуетесь, будет выглядеть как адрес VPN шлюза, а не ваш домашний. Ну то есть если вы зайдёте на сайт бывшего президента и случайно сломаете его, владельцы сайта могут подумать, что их сломали из какого-нибудь Амстердама, а не с Пулихова 18, квартира 37.

Почему же VPN не торт?

На самом деле проблема не в том, что VPN вреден сам по себе, а в том, что рекламная риторика зачастую наделяет его какими-то прям всеисцеляющими свойствами почище Кашпировского, что может притупить бдительность неопытного партизана, заставляя его забыть про принцип слабого звена. Конечно, пользоваться VPN можно и даже нужно, но важно помнить, что укрепляет он лишь одно звено цепи — канал связи. Ни ваши устройства, ни ваши данные он не делает неуязвимыми.

То есть пост с призывами к чему-нибудь эдакому в вашем открытом эккаунте на фейсбуке не станет невидимым для КГБ, если опубликуете вы его через VPN. Ну или если вас зовут Ник и вы звоните через VPN своему другану-шпиону Майку, чтобы обсудить какие у Лукашенко крепкие орешки, но у вас за стенкой сидит товарищ майор в тельняшке и наушниках, то всё, вы в вечерних новостях.

Ещё один нюанс, использование VPN никак не отменяет необходимости использования HTTPS. Помните, путь от вашего браузера к вебсайту долог, и через "защищённый" VPN пройдёт только первая его часть. Да, эта часть может "вывести" вас за границу, то есть из-под линии огня бандитов в балаклавах, но оставшийся маршрут может "привести" вас обратно, особенно если вашей конечной целью является беларуский сайт.

Также не стоит забывать, что если уж даже заключение договора с адвокатом у нас в государстве считается доказательством вины, то и использование VPN может рано или поздно быть интерпретировано не в вашу пользу. Они же реально на всю голову... непредсказуемые.

Tor

Раз уж мы упомянули VPN, то нельзя не рассказать про Tor. Придётся сильно упростить, да простят меня свитеробородые братья.

Tor — это большая (несколько тысяч) сеть компьютеров, разбросанных по всему миру, и специальный браузер (так и называется, Tor Browser), который умеет к этой сети подключаться. Сеть эта служит двум целям. Во-первых, в ней живёт так называемый "даркнет" — целая альтернативная вселенная полностью анонимных сайтов, созданных преимущественно для тёмных (с точки зрения различных правительств) делишек. Во-вторых, через эту сеть можно анонимно выйти в "нормальный" интернет. Анонимно, так как ваше соединение устанавливается не напрямую, а через цепочку случайных, не связанных между собой шлюзов Tor.

То есть Tor это ещё один VPN?

Нуууу, как бы не совсееееем...

Самый простой способ описать разницу таков: VPN шифрует канал, но не делает его анонимным, так как владелец VPN сервиса знает, кто вы, то есть теоретически может сдать вас властям, если вы нарушили закон с точки зрения государства, где расположен VPN-шлюз. Tor канал не шифрует, но делает его анонимным, "разрывая" цепочку связи таким образом, что ни один из её участков не видит полной картины: первый шлюз может знать, кто вы, но не знает, куда вы идёте, а последний шлюз может знать, куда вы идёте, но не знает, кто вы.

Ещё одно важное отличие: VPN сервисы, особенно платные, практически не ограничивают скорость вашего подключения, тогда как сеть Tor, работающая бесплатно и на общественных началах, может заставить вас вспомнить времена тёплых ламповых модемов. Тут я, конечно, немного утрирую, но всё-же ютубчик лучше через Tor не смотреть.

Ну и повторюсь ещё раз, потому что это действительно важно: и с VPN, и с Tor, не забывайте про HTTPS!

Хочу! Что делать?

Самый простой способ воспользоваться преимуществами сети Tor — установить себе Tor Browser. Этот браузер при запуске подключается к сети Tor, и далее вы можете либо посетить любой из сайтов даркнета (их адреса заканчиваются на `.onion`), либо зайти на любой из сайтов "обычного" интернета, пользуюясь ложным ощущением свободы.

Уровень четвёртый: маска Зорро

На этом уровне мы будем создавать себе альтернативную личность, которую, при последовательном соблюдении вами принципа слабого звена, будет очень сложно связать с вашей настоящей личностью.

Но пока что у меня закончился порох в пороховнице, так что продолжу чуть позже.