Необходимость безопасности

Арс Либрев

Предисловие

Представленная ниже работа является отрывком из пособия по вычислительной свободе.[1] Оно рассчитано на людей, которые не имеют специальных знаний в области информационной безопасности и программного обеспечения. Пособие предлагает практические инструкции по возвращению пользователем себе контроля над своими вычислениями, а также по реализации различных методов повышения безопасности. Данный отрывок включает вводную часть, где рассматриваются различные сетевые угрозы, обосновывается необходимость противостояния им и указываются принципы информационной безопасности. Пособие написано в рамках проекта LibreTrack.[2]

Сетевые угрозы

Безопасность на компьютерных устройствах

Людям редко нравится, когда на них пялятся. Обнаружив за окном своего дома любопытные взгляды или услышав, как кто-то посторонний пытается открыть входную дверь, вряд ли кто-то останется равнодушен. Тем более вряд ли кто-то спокойно отнесется к тому, чтобы этот посторонний начал ходить по его дому и рыться в его вещах. Все это воспринимается как наглость, а последнее, вовсе как преступление.

При этом огромный процент пользователей компьютерных устройств крайне пренебрежительно относится к слежке через эти устройства. Аргумент «Мне нечего скрывать» можно услышать довольно часто. При этом те, кто его произносит, не перестают, в то же время, закрывать шторы по вечерам и запирать замки на дверях. Между тем, в личной информации на их устройствах, без всяких препятствий, копается множество любопытных. В первую очередь, корпорации, внедряющие в свои программы следящий функционал для сбора информации о пользователях в коммерческих целях. Также иные злоумышленники, которые могут воспользоваться лазейками, оставленными корпорациями, — разного рода мошенники, взломщики или же крекеры, которых с подачи СМИ многие называют хакерами.

Далее, дабы показать актуальность информационной безопасности, разберу подробнее вопрос слежки программного обеспечения и сетевых угроз.

Слежка корпораций

Чтобы узнать о слежке в программном обеспечении нет необходимости проводить особый поиск в Интернете. Достаточно почитать пользовательские соглашения.

Что же мы можем в этих соглашениях обнаружить? Для начала откроем соглашение наиболее популярной операционной системы — Windows.[3] В этом заявлении, лицемерно названном «Заявлением конфиденциальности», четко сказано, что корпорация Microsoft собирает данные пользователей, полученные в процессе взаимодействия с их программами. Некоторые данные пользователь предоставляет непосредственно, в частности при регистрации, отправке запросов в Bing, загрузке документов в OneDrive и т.д.

В том же пользовательском соглашении также говориться, что корпорация может получать данные, применяя такие технологии, как файлы куки, и получая отчеты об ошибках или данные об использовании программного обеспечении, которое работает на вашем устройстве.

Собираются сведения о функциях, которые вы используете, элементах, которые вы приобретаете и веб-страницах, которые вы посещаете. Данные об операционной системе и другом ПО, установленном на вашем устройстве, в том числе электронные ключи. Кроме того, ip-адрес, идентификаторы устройств, языковые и региональные параметры. Данные о производительности, а также о проблемах, с которыми вы сталкивайтесь. Содержимое файлов, открытых при возникновении программной ошибки. Текст, данные рукописного ввода. Содержание сообщений, и сведения о взаимодействии с голосовым помощником и чат-ботами.

Интересно заметить, что в одном из разделов сказано, что могут собираться «пароли, подсказки по паролям и другие данные относящиеся к безопасности и используемые для проверки подлинности и доступа к учетным записям».

Для тех кто не осознал — ваши пароли сливаются на сервера корпорации. И не только пароли, а вся информация связанная с безопасностью ваших учетных записей, каких бы то ни было. В том числе связанная с онлайн-банкингом. Пароли от ваших банковских счетов не являются исключением для сбора. Сказано прямо «Корпорации интересны ваши платежные данные. Номер вашей банковской карты и связанный с ней защитный код». Принимая подобное соглашение (а не принимая его вы не сможете пользоваться данным программным обеспечением) вы сами отдаете всю информацию, которая касалась вашего компьютера, корпорации.

Перечислять далее, какие еще сведения собираются о вас, нет смысла. Проще было бы сказать какая информация не собирается. Вернее, сказать было бы вообще нечего, поскольку, как уже было сказано выше — вся информация, которая хоть как-то касалась устройства, на котором установлен инструмент, разработанный корпорацией, утекает этой корпорации.

Подобная ситуация характерна не только для операционных систем и иного программного обеспечения от Microsoft, но также для ПО от Apple.[4] Нечто похожее можно найти и в соглашениях иных раскрученных программ, средств для общения, таких как WhatsApp[5] и Viber[6]. Касается это и широко известных поисковых систем — Google,[7] Яндекс,[8] Yahoo,[9] Mail.ru[10] и т.д.; популярных социальных сетей — Facebook,*[11] ВКонтакте[12] и т.д. Для чего они собирают все эти сведения? Собирают они их в первую очередь в маркетинговых целях.

Как они сами заявляют, они используют их, чтобы показывать вам контекстную рекламу, т.е. рекламу тех продуктов, которые могут быть интересны именно вам. Также собранные сведения используются для улучшения своих разработок. Кроме того часто заявляется, что действия корпорации направлены на борьбу с вредоносным ПО, позволяют уведомить пользователей о наличии таких программ на их устройстве. В общем, корпорации осуществляют слежку для нашего же блага...

Представьте, что вам предлагают купить диван, к которому примонтирована стойка, на которой висит камера, направленная на этот диван. И говорят, что с помощью этой камеры производитель может следить за тем как вы «взаимодействуйте» с его диваном. Удобно ли вам на нем спать. И будет использовать полученную информацию, например, для показа вам рекламы подушек, которые сочтет для вас наиболее подходящими. Анализируя ваши кувыркания со своей второй половинкой на этом диване, он придет к выводу, например, что подкладку надо сделать более упругой, и таким образом сможет улучшить свою продукцию. А также сможет следить, не появилось ли на диване потертостей, не дерет ли его тайком ваш кот, не завелись ли в нем термиты, и в случае чего-то такого — предупредит вас и предложит варианты решения проблемы.

Удобно? Попробуйте поспорить, что не удобно. Однако, немногие из тех, кто спокойно относится к слежке корпораций и убежден в том, что она выгодна пользователям также, как и самим корпорациям, захочет приобрести себе такой диван. Как и было сказано мной в самом начале, мало кто любит, когда на него пялятся. Впрочем, раз сейчас есть те, кого не смущает подсматривание в Интернете,[13] наверняка найдутся и те, кого не смутит подсматривание за «взаимодействием» их со своей второй половинкой на мебели, выпускаемой какой-нибудь корпорацией.

В пользовательском соглашении все той же Windows также сообщается, что личные данные могут раскрываться сторонним организациям в рамках корпоративной сделки.

Microsoft увещевает о надежной сохранности ваших данных. Указывается, что эти данные хранятся на защищенных хранилищах с ограниченным доступом. А при отправке, данные защищаются с применением шифрования. Но что толку от наличия этого шифрования, если корпорация продает данные пользователей третьим лицам. Не говоря уже о том, что ей самой их информация доступна в полном объеме.

На сегодняшний день уже ни для кого не секрет, что одним из способов сбора данных являются черные ходы или бекдоры — программные лазейки, оставляемые разработчиками намеренно.[14] Оставляются такие ходы и для спецслужб, под предлогом повышения возможностей вычисления преступников.[15] Сами спецслужбы далеко не всегда ведут честную деятельность.

Такие намеренно оставленные уязвимости могут быть обнаружены и задействованы любым злоумышленником, возымевшим желание их найти и обладающим некоторыми знаниями. Или же просто купившим сведения о них на черном рынке в Интернете. Действия, которые он может совершить против вас, эксплуатируя подобные лазейки, могут быть самыми разными.

Мошенники и взломщики

Сеть наводнена мошенниками, которые пытаются заманить в свои сети пользователей, размещая баннеры на сайтах и рассылая фишинговые письма. От попадания на разводку в таких случаях могут спасти только собственные мозги. Если баннер на каком-то сайте вам обещает, что после клика на него, вы, ничего в дальнейшем не делая, станете зарабатывать тысячи долларов в день — это развод. Точно также, если вам приходит письмо в котором говориться, что чтобы получить «выигранный» миллион надо отправить тысячу рублей — это развод.

Но некоторые мошенники подходят к своему делу более обстоятельно. Они теми или иными способами узнают конкретную информацию о пользователях. И в дальнейшем пускают в ход схему развода, в которой фигурируют персональные данные людей.

Одно дело, когда вам на почту приходит письмо якобы от банка в котором к вам обращаются просто «Дорогой клиент» и говорят, что у вас есть непогашенный долг, без указания за что долг, и вам нужно, пройдя по такой-то ссылке, произвести погашение. В таком письме легко заподозрить мошенническое. Другое дело, когда в письме к вам обращаются, как и принято

у банков по Фамилии Имени Отчеству и указывают конкретные ваши счета. В таком письме уже сложнее заподозрить развод. А в абракадабре символов ссылки, по которой вам могут предлагать пройти, для авторизации и решения некоего вопроса, не каждый пользователь выявит переход на домен отличный от банковского.

Это лишь один из вариантов развода, который может быть осуществлен с использованием настоящих данных пользователей.

В сети можно найти свидетельства того, как мошенники пытаются развести людей, к примеру, на замену водосчетчиков, даже если такая замена не требуется.[16] При этом отмечается, что зачастую при обращении злоумышленники проявляют осведомленность о настоящих данных людей, — например, обращаются по настоящим ФИО.[17] А людям, заподозрившим развод остается только гадать, как они узнали его имя, адрес, телефон, лицевой счет и т.д.

Откуда мошенники берут эти данные? К ним они могут прийти разными путями. Они могут купить их у корпорации, представившись некоей компанией. Могут купить их на черном рынке в Интернете у взломщиков.

Взломщики или же крекеры (от англ. crack — взлом) — это те, кто добывают и/или изменяют данные путем взлома компьютерных систем или их элементов, аккаунтов и т.п. Обыватели обычно называют их хакерами, что некорректно. Хакер — это человек получающий удовольствие от решения интеллектуальных задач. В более узком смысле, хакер — это энтузиаст программирования, получающий наслаждение от самого процесса программирования и нахождения нестандартных решений. Конечно, взломщик может быть хакером, но это далеко не всегда так. На сегодняшний день существует большое количество готовых программных решений для взлома, и чтобы разобраться в них нет необходимости обладать специальными знаниями программирования. И точно также не каждый хакер, конечно, является взломщиком.[18]

Те, кто использует данные пользователей в корыстных целях могут и не покупать их у кого-то, а добыть самостоятельно, к примеру разработав свое ПО, которое пользователь установит у себя и оно будет сливать о нем информацию злоумышленникам. Судя по количеству разрешений, которые требуют многие приложения в магазине от Google — Play-маркете — некоторые из них могут быть сделаны именно с такими целями. Когда калькулятор требует полный доступ к Интернету и идентификаторам устройства, — это наводит на определенные мысли.[19]

И несмотря на эти мысли, пользователь все равно, скорее всего, скачает себе такое приложение, ведь разные приложения от того же Google имеют точно такой же букет разрешений. Ко всему.[20]

Точно также злоумышленники сами могут являться взломщиками. Последствия взлома ими вас могут также нести в себе все те же опасности. Они могут получить доступ к личным файлам, хранящимся на компьютере. Если у вас хранятся фотографии, на которых запечатлено ваше дорогое имущество, по этим данным преступники могут узнать, что у вас есть, что брать. А по метаданным могут выяснить, где это находится.

Метаданные — это данные о данных. К примеру, содержимое фотографии — это ее данные. А ее метаданные, это данные о самой фотографии — ее разрешение, цветопередача, а также информация о том, в какой день и в какое время она была сделана, и с помощью какого устройства, а если в устройстве есть GPS, то возможно, и где она была сделана.[21]

Таким образом, злоумышленники могут узнать куда конкретно надо прийти, чтобы вас ограбить.

Если у девушки имеются ее обнаженные фотографии, они также могут быть похищены, что и произошло с некоторыми знаменитостями.[22] Если вы не знаменитость, и вам не следует бояться ажиотажа в связи с появлением в сети ваших обнаженных фоток, то все равно они могут быть использованы для шантажа вас. К примеру, мало кому хочется, чтобы подобные фото увидели родители. Конечно, можно просто не делать таких фоток, но проблема в том, что это только один из вариантов того, как ваши личные файлы могут быть использованы против вас. Конечно, схемы по которым вам могут навредить с использованием, например, каких-то ваших повседневных фотографий, слишком изощренны, и потому вероятность того, что вы на них нарветесь исчезающе мала, чтобы ее учитывать. Чего не скажешь о сканах документов, которые могут хранится на вашем компьютере, рабочей документации, коммерческих секретах, набросках незаконченных произведений, если вы писатель, проектах чего-либо. Похищение всего вышеперечисленного злоумышленниками может нанести серьезный ущерб. Об опасности получения взломщиками паспортных данных и данных банковских счетов, думаю пояснять излишне.

Но допустим вы не храните на вашем компьютере данные документов, не ведете на нем рабочую документацию, не делайте пикантные фотографии, не пользуйтесь онлайн-банкингом. В безопасности ли вы в этом случае, если вас взломают? Нет. Если у вас нечего брать, то ваш компьютер превратят в прокси[23] и продадут доступ к нему на черном рынке в Интернете.[24] И затем, могут через ваш компьютер, к примеру, взломать сервер какой-нибудь правительственной

организации. И потом вы будете долго и нудно доказывать, что взлом осуществляли не вы.

Мошеннические схемы могут быть куда изощренней и опасности от взлома могут быть куда серьезнее, чем могут представить себе многие обыватели. Именно поэтому таким обывателям имеет смысл принимать меры по предотвращению взлома своего компьютера и утечке своих данных.

Основы компьютерной вирусологии

Вирусы — это вредоносные программы, которые могут причинять тот или иной ущерб вашему компьютеру и личным данным. Одни из них, попадая на ваш компьютер, похищают личные данные. Другие эти данные изменяют и уничтожают. Третьи пытаются получить контроль над вашим устройством. Четвертые сканируют характеристики вашего компьютера и сливают эти сведения своим разработчикам. Весьма распространены вирусы, которые шифруют все данные на компьютере или блокируют систему, пытаясь вынудить вас заплатить разработчикам вируса, чтобы получить код для разблокировки. Перечислять все вредоносные действия и их комбинации, которые могут творить те или иные вирусы, нет смысла. В конце концов, пожалуй каждый пользователь компьютерных устройств слышал о вирусах. И каждый знает, что для предотвращения их попадания на компьютер или препятствия их действиям, в случае, если такое попадание все-таки произошло, следует принимать меры.[25]

Необходимо заметить, что самой подверженной вирусам системой является наиболее распространенная — Windows. Это связано, во-первых, как раз с ее популярностью. Поскольку она наиболее распространенная, вирусы пишутся преимущественно для нее. Но есть и другая, более важная причина. Она связана с архитектурой самой системы. Windows довольно пренебрежительно относится к вопросом прав доступа. Если у вас для работы от администратора не требуется ввод пароля, ваши риски возрастают — у вируса нет дополнительного препятствия, чтобы получить доступ к системным данным.

Отдельно необходимо отметить класс вирусов, известных как полиморфные вирусы. Эти вирусы, внедряясь на ваш компьютер, сканируют его характеристики и подстраиваются под них. Таким образом, они находят наиболее эффективный способ собирать и сливать ваши данные и предоставлять контроль над вашим компьютером своим разработчикам. Они незаметны антивирусам, поскольку способны подстраиваться и под них.[26]

Касательно антивирусов.[27] То что я сейчас скажу для многих пользователей прозвучит странно, но использовать в качестве противодействия вирусам антивирусы, мера крайне сомнительная. Ведь они, как бесплатные, вроде Avast

и Camodo, так и платные, вроде Kasperskiy и Dr. Web собирают и сливают о вас сведения своим разработчикам.[28] Они точно такие же шпионы. По сути вам советуют защищаться от вирусов при помощи вирусов. Конечно, есть антивирусы, которые не занимаются шпионажем и честно выполняют свои функции, но таких немного. Забегая вперед, скажу, что в достойных операционных системах, которые не шпионят за пользователем, антивирусы не нужны, поскольку их архитектура, система прав доступа, сама прекрасно защищает их от действий вирусов.

Отдельным классом шпионящих программ являются руткиты. Они, внедряясь на компьютер, собирают и сливают информацию пользователя.[29] У систем типа Windows и антивирусов нет средств, чтобы защитится от них. Тут также нужны более серьезные меры.

Опасна ли слежка спецслужб для добропорядочного гражданина

Отвечаю сразу — да, опасна. Во-первых, если вы не профессиональный юрист, вы не можете знать насколько вы законопослушный. Люди, которые критиковали в соц. сетях РПЦ и действующую в России власть, понятия не имели, что они преступники-экстремисты, пока за ними не пришли мусора.[30] Точно также люди, покупавшие через AliExpress очки с видеокамерами и ручки с диктофонами, понятия не имели, что нарушают закон, пока их при получении товара не взяли под руки сотрудники органов.[31]

Во-вторых, к сожалению, реальность такова, что нашим доблестным стражам порядка проще выставить невинный поступок простого человека, к примеру просмотр и сохранение (даже не изготовление, а только просмотр) карикатур на некоторых представителей власти, как экстремизм, и таким образом повысить себе раскрываемость, чем связываться с настоящим террористом, который и застрелить и зарезать может.[32]

Так что не следует думать, что если вам кажется, что вы не делайте ничего противозаконного, вам не стоит бояться слежки. Как я уже сказал, если вы не профессиональный юрист, вы не можете знать, делаете ли вы что-то противозаконное или нет. К тому же, даже если вы не делаете что-то прямо противозаконное, может стражам порядка проще выставить ваши поступки как противоправные, чем париться с ловлей бандитов. Выставить как экстремизм можно любое недовольство каким-либо решением действующей власти, или структур, которым эта власть попустительствует, вроде некоторых религиозных организаций.

Несколько общих слов об опасности слежки

Человек, узнавший о ведущейся повсеместно слежке, часто задает одни и те же вопросы «Кто я такой, чтобы за мной следить? Кому я нужен? Зачем следить за простыми людьми?». Действительно, зачем следить за нами, если мы никто?

Отчасти на этот вопрос был дан ответ выше. Корпорации и компании следят, чтобы тем или иным образом монетизировать полученную информацию. К примеру, зная данные о заряде батареи в вашем смартфоне, при вызове вами такси, можно задрать цену на поездку, рассчитывая на ваш страх, что у вас вот-вот сядет устройство связи, и вы согласитесь на большую цену, чтобы быстрей добраться до пункта назначения. Зная какие товары вы просматривали в Интернете, можно предлагать вам их, аксессуары к ним и альтернативы. Зная ваши интересы, ориентируясь на ваши запросы в сети, можно предлагать вам опять же соответствующие товары, которые могут быть вам интересны, или услуги, в которых вы, возможно, нуждаетесь. Возможен даже вариант, зная ваше местоположение, предлагать вам закупиться в ближайшем магазине, или поужинать в ресторане рядом.[33]

Мошенники со взломщиками осуществляют слежку, чтобы узнать, что и как у вас можно украсть, или просто развести вас на покупку чего-либо. Или иными способами нажиться на вас — шантажом, продажей ваших данных, доступом к вашему компьютеру, подставой вас.

Правительства могут следить, для выявления и дальнейшей нейтрализации несогласных. Вместе с тем, имеющиеся у них ресурсы могут быть использованы для подстав, заметания следов их грязных дел. А также навязывания своей политики.

В связи со всем вышесказанным, вместо того чтобы разрабатывать сложные алгоритмы выявления и записи только действительно полезной информации, им проще записывать скопом все. Блогер Иван Глазков на своем youtube-канале, подвергая сомнению наличие слежки, говорит, что учитывая, как много копий Windows продается, он не думает, что за каждым купившим могут следить.[34] Иван не учитывает, что собираемую информацию записывают не люди, а роботы. По ту сторону веб-камеры вашего ноутбука не сидит никакой суровый сотрудник ФСБ, ЦРУ, АНБ или даже Microsoft. Вся информация стекается в хранилища. Она структурируется, анализируется ботами, и они уже автоматически подбирают, сообразно с ней, контекстную рекламу или проводят иные действия. Слежки в том виде, который укоренился в сознании обывателя (суровый дядька, подсматривающий через вебку) там нет. Но само хранение этой информации несет в себе потенциальную опасность.[35]

Даже оставив в стороне риски от доступа к вашей личной информации мелких злоумышленников. Вы можете совершить действие или даже просто высказать мысль, неугодную правительству. Всегда могут принять новый закон, по которому ваши действия, которые ныне вполне законные, станут незаконными. В одном из выступлений конференции TED, которое так и называлось «Зачем правительству следить за нами, если мы никто?», было замечено, что в свое время правительство Голландии решило провести перепись и узнать, сколько у них в стране представителей какой конфессии. Их намерения были вполне благими, они хотели узнать сколько у них в стране христиан, мусульман, иудеев и т.д., чтобы знать, сколько денег выделять той или иной церкви. Когда пришли нацисты, работа по выявлению евреев уже была сделана.[36]

Мы не можем знать будущего, и какую опасность может таить в себе наша сегодняшняя информация. Поэтому важно, каждому человеку, не зависимо от профессии, должности, социального статуса и личных взглядов, предотвращать утечку своей информации за пределы своих устройств, насколько это только возможно. И возможности предотвращения такой утечки гораздо больше, чем представляет себе большинство пользователей. О них данное пособие.

Принципы информационной безопасности

Вопрос свободы в мире программного обеспечения

В Интернете можно найти очень много методик по информационной безопасности. К сожалению, большинство из них предлагают лишь косметические меры. Как правило первым делом такие методики предлагают установить антивирус. О сомнительности данной меры уже было сказано выше. Что касается вполне путевых советов, например, использовать на разных ресурсах разные и сложные пароли, то при всей их корректности, они теряют смысл, если вы продолжаете работать в небезопасной среде. Таковыми являются операционные системы Windows и MacOS, которые сливают информацию, в том числе пароли, как было показано выше, разработчикам. Какая общая черта позволяет им обладать такими вредоносными функциями? Что объединяет их и другое программное обеспечение столь гнусно относящиеся к своим пользователям? Все оно является несвободным. Несвободное программное обеспечение не контролируется пользователем, оно контролирует пользователя, ограничивая его действия и/или производя действия, которые пользователь не желает (к примеру слежку). Такое программное обеспечение, в свою очередь, контролирует разработчик. Таким

образом, несвободная программа передает разработчику власть над пользователем. Несвободные программы как правило являются проприетарными (таковы Windows и MacOS) — их исходный код закрыт, и никто кроме разработчика не знает, что в действительности делает программа. Пользователь не может, ни проверить ее действительный функционал, ни помешать ей делать то, чего он не хочет. Таковыми являются не только распространенные операционные системы, но и подавляющее большинство широко известных программ — популярные Интернет-браузеры Google Chrome, Opera, Edgi, Yandex и др., программы в пакете Microsoft Office, графический редактор Photoshop и большинство из того, о чем слышал и чем пользуется обычный пользователь.

Власть, которую проприетарное ПО дает своим разработчикам над пользователями, развращает их. Они часто начинают внедрять в свои инструменты все новый и новый вредоносный функционал, собирающий все больше и больше информации о пользователе и, в свою очередь, все больше его ограничивающий и контролирующий. Один из самых вопиющих примеров DRM — цифровое управление ограничениями, позволяющее удаленно блокировать просмотр и прослушивание определенных материалов.[37]

Если мы хотим обеспечить безопасность своей информации, нам в первую очередь, необходимо избавится от шпионажа того программного обеспечения которое мы используем. Для этого необходимо уйти от проприетарного ПО и прийти к такому, которое контролируется самим пользователем, а не какой-то корпорацией. Необходимо перейти на свободное ПО.

Свободное программное обеспечение предоставляет пользователю четыре свободы

0) Свобода использовать программу, как ему угодно
1) Свобода изучать и изменять программу, как ему нужно
2) Свобода копировать и распространять копии программы
3) Свобода распространять измененные копии программы

Свобода 0 означает, что лицензия программы не может налагать ограничения на цели, с которыми может быть использована программа, и сферы, в которых она может быть применена. К примеру, лицензия музыкального плеера не может запрещать вам прослушивать с помощью него музыку какого-либо стиля (просто потому, что он не нравится разработчикам). Звучит странно, но попытки создания подобных лицензий были.[38]

Свобода 1 означает, что исходный код программы открыт для, во-первых, просмотра, и вы можете узнать, что именно и как делает программа. Во-вторых

для изменений, чтобы вы могли его исправить так, чтобы программа делала то, что вы хотите или перестала делать то, что вам не нравится. Безусловно, если вы не программист, вы не можете прямо пользоваться этой свободой. Но во-первых, велика вероятность, что найдется программист, который выявит и устранит проблему, если она есть. Сама по себе открытость уже значительно снижает возможность внедрения не заявленного или прямо вредоносного функционала. Во-вторых, вы можете нанять программиста, который модернизирует программу так, чтобы она работала как вам нужно. Данная свобода позволяет осуществлять общественный контроль над программой, производить ее независимую проверку, выявлять ошибки, уязвимости, вредоносный функционал и недочеты. В связи со всем этим, абсолютное большинство свободных программ изначально составляется без внедрения следящего или иным образом вредоносного функционала.

Свобода 2 означает, что вы можете помогать другим людям, делясь с ними копиями программы. Проприетарное ПО, как правило, асоциально. Оно разобщает пользователей, запрещая им помогать друг другу, обмениваясь копиями. Свободное ПО такого аморального запрета не накладывает. Вы можете создавать копии программы и делиться ими с другими людьми. Причем нет никаких ограничений на то, как вы можете это делать. Вы можете делиться копиями как безвозмездно, так и за плату. Можете, скачав программу бесплатно, также бесплатно ею делиться с другими. Можете, купив ее, начать предоставлять другим копии бесплатно. И точно также никто не запрещает вам, бесплатно скачав программу, давать копии, беря за них плату. В тоже время, вы можете использовать программу частным порядком — никто не требует, чтобы вы занимались распространением копий. В то время как многим людям в странах с неразвитой экономикой и беднейшим слоям в странах с развитой приходится нелегально приобретать бесплатные копии проприетарного ПО, большинство свободных программ можно приобрести бесплатно совершенно легально. Используя свободное ПО, вы не только повышайте свою безопасность, но и остаетесь морально чистым, даже если у вас нет денег, и вы вынуждены скачивать программы бесплатно. В тоже время необходимо отметить, что свободное ПО не синоним бесплатного. «Свободное» подразумевает свободу, а не халяву. Многие разработчики свободного ПО живут как раз за счет того, что продают копии своих программ, много программ создаются на гранты, ну и конечно, значительная часть свободного ПО держится на пожертвованиях.

Свобода 3 означает, что если вы каким-то образом модернизировали программу — устранили в ней ошибку, убрали из нее какой-то функционал или, наоборот, добавили новый, вы можете распространять измененные вами копии.

Эта свобода для непосредственной реализации также доступна только программистам. Однако, ее плодами могут пользоваться все без исключения пользователи.

Если все эти четыре свободы есть, пользователь контролирует программу.

Кроме того, что свободные программы этичнее и безопаснее проприетарных, они, порой, еще и надежнее. В них меньше ошибок, они более отказоустойчивы, они работают стабильнее, они менее ресурсозатратные. Причина тому та же самая — за счет наличия вышеперечисленных свобод, любой желающий может просмотреть исходный код этих программ, и в случае обнаружения ошибки или уязвимости — исправить ее. В отличие от проприетарной, над которой трудится узкая закрытая группа программистов, свободная программа доступна для улучшения широкому кругу людей.[39]

Стоит также отметить, что необходимо разделять свободное ПО и открытое. Открытое программное обеспечение имеет открытый исходный код, но при этом не предоставляет одной и более из вышеперечисленных свобод. Например, его исходный код может быть доступен для изучения, но не для изменения. Или может быть запрещен обмен измененными копиями. То есть, хотя такое ПО не является проприетарным, оно все равно несвободное. Любое свободное ПО является в тоже время и открытым, но не всегда открытое ПО является свободным. Впрочем, большинство открытых программ в тоже время и свободны.[40]

На сегодняшний день существуют свободные аналоги практически для всех повсеместно используемых проприетарных программ. Это и операционные системы и иное ПО.

Тут может возникнуть вопрос, если свободные программы настолько замечательны, почему они распространены значительно меньше проприетарных? Основная причина тому — социальная инерция. Когда система Windows впервые попала на компьютеры простых обывателей, этичные операционные системы были еще слишком неудобны для использования не специалистами. Обычный пользователь вынужден был использовать Windows, а кто-то MacOS, потому что этичные ОС не были приемлемой для него удобной альтернативой. Сейчас, когда ситуация изменилась, и свободные ОС для обычного пользователя ни чуть не сложнее, чем проприетарные, ему уже сложно отказаться от систем, к которым он так привык, и перейти на более этичные. С другим ПО ситуация аналогичная.[41] Кроме того, у проприетарного ПО мощная реклама. Крупные корпорации не жалеют средств для раскручивания своих разработок. Не жалеют они средств и для противостояния своим конкурентам в лице свободного ПО. Так, например, Microsoft специально делает форматы документов, создаваемых при помощи их программ,

закрытыми. И разработчикам свободного ПО приходится проделывать колоссальную работу для разгадки этих форматов, чтобы пользователи не отказались от использования их программ, потому что те не могут читать такие распространенные (из-за распространенности самих программ Microsoft) форматы.[42] Крупные корпорации используют и иные методы навязывания. К примеру, все та же Microsoft поставляет бесплатные копии своих операционных систем для учебных заведений. Таким образом, школьникам с самого начала навязывается пристрастие к их программам. Я полностью солидарен с мнением, что это равносильно бесплатной раздаче детям сигарет, для выработки у них привычки курить.[43] Похожую практику, судя по всему, осуществляет и Apple. До меня доходили сведения, что в некоторых школах России уроки информатики проходят на макбуках.

Свободное ПО возвращает пользователям контроль над их вычислениями. Оно безопасное и надежное. Оно способствует сотрудничеству между людьми, позволяя им помогать друг другу, обмениваясь копиями.[44] Можно найти много статей и даже книг, якобы, о том, как обеспечить свою безопасность под Windows и MacOS; о том, как настроить на, якобы, безопасную работу какой-нибудь Google Chrome или Internet Explorer. Но все это будет лишь косметика, скрывающая изъяны, но не устраняющая их. В проприетарном ПО безопасности нет, не говоря о том, что оно просто неэтично.[45]

Использование свободного ПО мера необходимая, но недостаточная. Для предотвращения взлома и Интернет-шпионажа необходимо применять и иные.

Изоляция Интернет-активности

Наиболее действенной мерой от взлома и получения доступа к вашим файлам, непомерно превышающая надежность любых антивирусов и файерволов, является изоляция вашей системы от Интернета. Я понимаю, что это и так всем очевидно, но в то же время от Интернета отказаться мало кто может. Но что если я скажу, что предлагаю не отказываться от Интернета, а использовать его без подключения к нему вашей операционной системы. Как это возможно? Поясню — без подключения основной операционной системы, на которой у вас хранятся личные файлы. Внутри этой системы нужно запустить другую операционную систему и ее подключить к Интернету. Через эту систему, развернутую внутри основной, осуществлять Интернет-серфинг. Основную операционную систему, при этом, к Интернету просто не подключать.

Существуют программные решения для запуска операционных систем внутри уже имеющихся. Такой процесс называется виртуализацией, а

операционная система, запущенная внутри основной, виртуальной машиной или виртуалкой.[46]

К сожалению, на сегодняшний день, применение виртуализации не всегда возможно. На смартфонах и планшетах даже при большом объеме оперативной памяти и мощном процессоре, к сегодняшнему дню, имеет место дефицит программных решений для реализации виртуализации. На слабом компьютере также существует проблема. Не трудно догадаться, что запуск операционной системы внутри другой, требует значительных ресурсов. Если объем оперативной памяти меньше 4 Гб, то применять виртуализацию крайне проблематично. Точно также, если процессор слабый, скажем двухъядерный Celeron или Pentium, запущенная виртуальная машина будет чудовищно тормозить, и о комфортной работе не может быть и речи. Для качественного применения виртуализации требуется не менее 4 Гб оперативной памяти, а в качестве процессора, как минимум четырехъядерный Pentium.

О том, как обеспечить безопасность на смартфоне/планшете и слабом компьютере, будет сказано в этом пособии отдельно. Когда же это возможно, следует применять виртуализацию. О том, как ее применять, также будет сказано далее.

Однако, виртуализация не защитит вас в самом Интернете. Не предотвратит прослушивание (сниффинг) вашего трафика, не помешает Интернет-ресурсам и сетевым шпионам идентифицировать вас при Интернет-прогулках, и собирать данные об этих прогулках.

Для противостояния этому нужно применять отдельные меры.

Обезличивание Интернет-трафика

Помимо опасности взлома и получения, благодаря ему, доступа к вашим файлам и контроля над вашим компьютером, которую способна устранить виртуализация, существует опасность прослушивания вашего Интернет-трафика. Можно сказать, что такой прослушкой занимается ваш провайдер, который видит на какие Интернет-ресурсы вы ходите, сколько вы на них сидите, какой объем данных при этом передается между вами и этими ресурсами, а также может увидеть сами эти данные.

Помимо провайдера прослушиванием трафика занимаются государственные системы слежения. В России это СОРМ — система оперативно-разыскных мероприятий (сейчас повсеместно внедрен СОРМ-3, который осуществляет слежку за всеми аналоговыми и цифровыми каналами связи, прослушивает телефоны и Интернет-трафик).[47] Оборудование этих систем ставится у провайдеров и в дата-центрах. Аналогичные национальные системы слежения есть и в других странах.[48]

Существуют и транснациональные системы слежения. Самая масштабная из них — Эшелон, также известная как «Пять глаз». Ее организовывают пять стран — США, Канада, Великобритания, Австралия и Новая Зеландия. Она включает в себя крупные наземные центры снимающие информацию с телекоммуникационных каналов связи, а также систему спутников.[49]

Помимо таких государственных систем прослушивания, существуют и мелкие взломщики, осуществляющие атаки, нацеленные на перехват трафика. Атака типа «Человек по середине» — это когда кто-то вклинивается между вами и сервером, к которому вы обращаетесь, и может снимать ваш трафик, узнавая, что вы делайте, какой информацией обмениваетесь с сервером, что просматриваете. А может и подменить информацию, к примеру при скачивании вами с сайта какой-то программы, подсунуть вам свою, с зашитым в нее вирусом.[50]

От прослушивания трафика, а также его подмены, спасает шифрование. Если трафик шифрован, то в случае его снятия кем-то, этот кто-то получит лишь шифрованную абракадабру, которая будет бесполезна без ключей шифрования. Также отсутствует возможность подменить трафик, поскольку не понятно, что и соответственно как подменять. Сейчас многие сайты работают как раз с применением шифрования. К сожалению, далеко не все из них шифруют полностью весь свой трафик. Не знаю как сейчас, но еще некоторое время назад Яндекс, уже давно работая по шифрующему протоколу, передавал в незашифрованном виде логины и пароли (!) в своем почтовом сервисе.[51] Кроме того, многие сайты, в тоже время, продолжают работать вовсе без применения шифрования.

Сайты, к которым вы обращаетесь, также собирают о вас информацию. Это, в первую очередь, информация о том, как вы взаимодействуйте с их сервисом. Также они стараются тем или иным образом пометить вас, чтобы в дальнейшем идентифицировать и копить на вас досье, которое может пригодится им в маркетинговых и иных целях. Способы пометить вас весьма разнообразны. В некотором роде от них защищает сама по себе виртуализация. От многих спасает грамотная настройка браузера и операционной системы. Но есть идентификаторы от которых так просто не защитишься, они связаны не с вашей системой, а с вашим соединением.

В сети основным идентификатором вас является ваш ip-адрес. Существуют статические и динамические ip-адреса. Если ip у вас статический — то он неизменный ваш идентификатор. Если динамический, то все равно он выдается вам вашим провайдером из определенного диапазона, и, зная конкретное время, в которое вы взаимодействовали с сайтом, вас в принципе можно идентифицировать.[52]

У сайтов также есть свои ip-адреса, и вашему провайдеру, следящим системам, а также взломщикам, взявшимся прослушивать ваш трафик, видно куда вы обращайтесь. Соответственно, все они также могут знать, куда в Интернете вы гуляйте, могут копить (и копят) на вас досье.

Таким образом, даже при шифровании трафика, когда защищены передаваемые данные, злоумышленникам остаются доступны метаданные. Защититься от этого можно если обращаться к целевым серверам через какой-то промежуточный узел. В этом случае, если кто-то прослушивает трафик между вами и этим узлом, он видит адрес этого узла, но не видит, к какому серверу вы за ним обращаетесь. И тут также важно, чтобы трафик между вами и промежуточным узлом был шифрован. В противном случае будет видно, куда вы за этим узлом ходите.

Когда вы обращаетесь к какому-то ресурсу через промежуточный узел, и при этом, трафик между вами и этим узлом шифруется, этот процесс можно назвать туннелированием. Создается защищенный туннель, по которому передаются данные без опасности перехвата, и не известно, куда они за этим туннелем поступают.

Следует отметить, что туннелирование не во всех случаях нужно, а в некоторых даже вредно. Например, если вы делаете заказ в Интернет-магазине, то бессмысленно маскироваться. Все равно вы или заказываете что-то к себе домой, или придете в пункт самовывоза. В любом случае, вы «спалитесь» перед этим магазином. Однако, туннелирование необходимо при большинстве Интернет-прогулок, когда вы фактически делитесь с сетью своими интересами и проблемами, а также крайне желательно при общении с близкими.

Если вы, используя только свободное ПО, из-под грамотно настроенной виртуальной машины, серфите в Интернете с применением туннелирования через, опять же, грамотно настроенный браузер, вы надежно защищены от разнообразнейших Интернет-угроз.

Критерии подбора программного обеспечения

Необходимо заострить внимание на том, как подбирать себе программное обеспечение. Уже было показано, что нужно использовать свободные программы. Однако есть некоторые нюансы. Существует очень простой принцип, следуя которому вы всегда будете иметь на своем устройстве только свободное ПО. Но об этом принципе я скажу чуть позже. Сейчас же я хотел бы рассказать о том, как искать именно свободные программы.

Все дело в том, что если вы забьете в поисковик, например, «свободные медиаплееры», вы не получите ссылок на каталоги именно свободных медиаплееров. Поисковик выдаст вам ссылки на списки медиаплееров по их

функционалу или цене — по тем характеристикам, на которые чаще всего и смотрят люди. К сожалению, выбор программы по критерию свободы не является распространенной практикой. Такая ситуация будет с любым классом программного обеспечения, которое вы возьметесь искать в сети через обычные поисковики. Есть однако известный ресурс, позволяющий искать ПО по критерию свободы — Википедия. Вы можете просто вбить в ее поисковую строку название известной вам проприетарной программы с нужным функционалом, и на ее странице внизу будет отображено, в какой категории ПО оно находится. Иногда даже сразу дается таблица, где программы распределены на свободные и проприетарные. По этим категориям легко искать нужные программы. Для того, чтобы понять подходит ли конкретная программа, смотрите лицензию. В Википедии она указана в основной информации в таблице размещенной справа. Если она свободна — присутствует в каталоге свободных лицензий, который представлен на сайте Фонда свободного программного обеспечения — то это то, что нужно.[53] Также вначале в описании программы, как правило, сразу же указывается свободная ли она.

В случае если вам требуется установить что-то специфическое, что отсутствует непосредственно в свободных операционных системах, определить насколько подходящее то или иное ПО можно похожим способом. Для начала проверьте, является ли это ПО свободным. Для этого также смотрите лицензию. Если она свободна — присутствует в каталоге свободных лицензий, который представлен на сайте Фонда свободного программного обеспечения, то можете смело ее устанавливать. Если нет, то первым делом, проверьте нет ли у нее свободных аналогов. Если их нет, то подумайте еще раз, нужно ли вам это ПО. Если нужно, то проверьте, чтобы оно было хотя бы открытым. Для этого также проверьте лицензию.[54] Если ПО открытое, то это, конечно, не лучший вариант, но все-таки приемлемый. Если же ПО не является и открытым, то опять же проверьте, нет ли у нее хотя бы открытых аналогов. Если же их нет, и ПО проприетарное, то еще раз подумайте, действительно ли оно вам нужно. Если все-таки нужно и деваться некуда, то рекомендую все же не осквернять ей свою свободную операционку, а установить ее в отдельную операционную систему. Как вариант, можно создать для нее отдельную виртуальную машину. И лучше, чтобы операционка с таким ПО не соприкасалась с сетью. С такой же осторожностью желательно отнестись к ПО, у которого лицензия вовсе отсутствует.

На самом деле, вариант описанный выше маловероятен. Как я уже писал, сейчас существуют свободные аналоги практически для всех проприетарных программ. Исключение могут составлять только специфические коммерческие программы для работы, например, со специальным промышленным или

лабораторным оборудованием. Компьютеры с таким ПО желательно держать подальше от сети.

Впрочем, есть класс программ, в котором действительно бывает сложно найти свободные аналоги. Это драйвера, программы, благодаря которым компьютер взаимодействует с теми или иными устройствами. К сожалению, на сегодняшний день, не для всех устройств есть свободные версии этих драйверов. Сетевые карты, видеокарты, МФУ, различные адаптеры, могут подкинуть вам такую подлянку. Они просто не станут взаимодействовать с компьютером со свободной операционной системой. Лучше, конечно, выкинуть либо продать такое устройство и купить себе то, для которого есть свободные драйверы. Но конечно, не всегда такой вариант приемлем. В этом случае остается установить проприетарный драйвер. Если иного варианта нет, это может считаться приемлемым. Но необходимо помнить, что несвободный компонент в системе, это изъян. И на такой шаг следует идти только в действительно крайнем случае.

Но возвращаясь к вопросу со свободным ПО, следует оговорить еще момент. Крайне желательно, чтобы ПО имело поддержку сообщества и активно разрабатывалось. Как правило, это можно проверить на официальном сайте программы. Если счет с последнего обновления пошел на годы, то такому ПО следует поискать поддерживаемые, то есть регулярно обновляемые, аналоги.

Подводя итог, повторю, информационная безопасность держится на трех китах

1) Свободное ПО
2) Виртуализация
3) Туннелирование

При этом, вируализация не всегда возможна, туннелирование не всегда целесообразно. Свободное же ПО является однозначным и необходимым условием информационной безопасности.

1 Это пособие представлено в публикации Вычислительная свобода. Практическое пособие https://mega.nz/file/S8AhkahB#LXFhqvyjbp_2JfM2pg8T1xknAE57Z1yd9YlkFvN3l9w

2 Подробности о проекте и материалах смотрите в Памятке к материалам LibreTrack https://cryptpad.fr/pad/#/2/pad/view/US9w9ly695pxvJNF4XvYMJ7Nk+-hjF21JtlRHljCEo4/

3 Заявление конфиденциальности Microsoft https://privacy.microsoft.com/ru-ru/privacystatement

4 Политика конфиденциальности Apple https://www.apple.com/ru/legal/privacy/ru/

5 Официальная информация о WhatsApp https://www.whatsapp.com/legal/?lang=ru

6 Политика конфиденциальности Viber https://www.viber.com/ru/terms/viber-privacy-policy/

7 Политика конфиденциальности Google https://policies.google.com/privacy?hl=ru

8 Политика конфиденциальности Яндекс https://yandex.ru/legal/confidential/

9 Политика конфиденциальности Yahoo https://policies.yahoo.com/ie/ru/yahoo/privacy/index.htm

10 Политика конфиденциальности Mail.Ru https://help.mail.ru/mail-help/UA

11 Политика использования данных Facebook*

12 Политика конфиденциальности ВКонтакте https://vk.com/privacy

13 С таким мнением можете ознакомиться по этой ссылке https://www.youtube.com/watch?v=QcXR4r-M-Bs

14 Подробнее о бэкдорах https://ru.wikipedia.org/wiki/%D0%91%D1%8D%D0%BA%D0%B4%D0%BE%D1%80

15 О бэкдорах, эксплуатируемых спецслужбами https://roskomsvoboda.org/34103/. Также о требованиях правительств, оставлять бэкдоры в программах можно прочитать по этой ссылке https://www.tutanota.com/ru/blog/posts/why-a-backdoor-is-a-security-risk/

16 Отзывы о мошенниках, разводящих людей на замену водосчетчиков https://zvonili.com/phone/4952597156

17 Об этом, например, говорится в этом комментарии https://zvonili.com/phone/4952597156/comment/477962

18 Подробнее о хакерах можно почитать по этой ссылке http://volgograd.lug.ru/library/hacker-howto.ru.html

19 Калькулятор в Play-маркете, требующий кучу разрешений, не связанных с его функционалом https://play.google.com/store/apps/details?id=info.woodsmall.calculator&hl=ru

20 Например популярное приложение Google Фото https://play.google.com/store/apps/details?id=com.google.android.apps.photos&hl=ru

21 Подробнее о том, что такое метаданные можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%B0%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5

22 Об этом можно прочитать по этой ссылке https://www.iguides.ru/main/other/khaker_poluchil_dostup_k_intimnym_fotografiyam_dzhennifer_lourens_i_soten_drugikh_znamenitostey/

23 О том, что такое прокси, можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%BA%D1%81%D0%B8-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80

24 О таких методах сказано здесь https://www.securitylab.ru/news/478049.php. А также здесь https://web-helps.ru/stati/troyan-dja-windows-pevrashaet-pc-v-proxy.html. И вот здесь https://xakep.ru/2017/01/26/linux-proxy-10/. Об этом же говорится здесь https://lenta.ru/articles/2018/06/28/botnets/

25 Подробнее о вирусах можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81

26 Подробнее о полиморфных вирусах можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B8%D0%BC%D0%BE%D1%80%D1%84%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81

27 Общие сведения об антивирусах можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0

28 О шпионаже антивирусов можно узнать из самих пользовательских соглашений данных программ, например из политики конфиденциальности Avast https://www.avast.ru/privacy-policy. Или Kasperskiy https://www.kaspersky.ru/web-privacy-policy

29 О руткитах подробнее можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%A0%D1%83%D1%82%D0%BA

%D0%B8%D1%82

30 Об этом можно прочитать в этой статье https://www.bbc.com/russian/news-45062731

31 Об этом можете посмотреть по этой ссылке https://www.youtube.com/watch?v=dt_lnd2D-uk

32 Об этом была передача на радио https://www.svoboda.org/a/28943937.html. Очень много ссылок по данному вопросу можно найти в этой статье http://saint-juste.narod.ru/vk.html

33 О геоконтекстной рекламе можно почитать в Википедии https://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BE%D0%BA%D0%BE%D0%BD%D1%82%D0%B5%D0%BA%D1%81%D1%82%D0%BD%D0%B0%D1%8F_%D1%80%D0%B5%D0%BA%D0%BB%D0%B0%D0%BC%D0%B0

34 Такое мнение Иван Глазков высказывает все в том же своем видео о слежке https://www.youtube.com/watch?v=QcXR4r-M-Bs

35 Много интересного по данной теме можно найти в статье по этой ссылке https://www.gnu.org/philosophy/surveillance-vs-democracy.ru.html

36 Данное видео можно посмотреть по этой ссылке https://www.youtube.com/watch?v=4tAOsN-ueR4

37 О проблеме, которую представляет DRM, можно прочитать в этой статье https://www.gnu.org/philosophy/can-you-trust.ru.html. Также об этом говориться в статье по этой ссылке https://www.gnu.org/proprietary/proprietary-drm.ru.html

38 О подобных лицензиях можете посмотреть в этом видео https://www.youtube.com/watch?v=vcEpP0JenuE

39 О надежности свободных программ https://www.gnu.org/software/reliability.ru.html

40 Подробнее данный вопрос разобран в этой статье https://www.gnu.org/philosophy/open-source-misses-the-point.ru.html

41 О социальной инерции можно почитать по этой ссылке https://www.gnu.org/philosophy/social-inertia.ru.html

42 О таком грязном противодействии свободному ПО написано в этой статье https://www.gnu.org/philosophy/microsoft.ru.html. О проблеме форматов также говорится в этой статье https://www.gnu.org/philosophy/no-word-attachments.ru.html

43 Об этом говориться в этой статье https://www.gnu.org/education/edu-schools.ru.html

44 Подробнее о свободном ПО можно почитать по этой ссылке https://www.gnu.org/philosophy/free-sw.ru.html. Также полезной будет эта

статья https://www.gnu.org/philosophy/free-software-even-more-important.ru.html

45 Сводка статей в которых раскрываются различные гнусные моменты несвободного ПО можно найти по этой ссылке https://www.gnu.org/proprietary/proprietary.ru.html

46 Подробнее о виртуализации можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F

47 Подробнее о СОРМ можно почитать в Википедии https://ru.wikipedia.org/wiki/%D0%A1%D0%9E%D0%A0%D0%9C

48 О различных национальных системах слежения можно прочитать в Википедии https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B3%D0%BE_%D1%81%D0%BB%D0%B5%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B8_%D1%80%D0%B0%D0%B4%D0%B8%D0%BE%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D1%80%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B8_%D0%BF%D0%BE_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B0%D0%BC#.D0.9D.D0.B0.D1.86.D0.B8.D0.BE.D0.BD.D0.B0.D0.BB.D1.8C.D0.BD.D1.8B.D0.B5

49 Подробнее о системе Эшелон также можно прочесть в Википедии https://ru.wikipedia.org/wiki/ECHELON

50 Подробнее об атаке «человек посередине» https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE%D1%81%D1%80%D0%B5%D0%B4%D0%BD%D0%B8%D0%BA%D0%B0

51 Это показано в одном из видео Ивана Глазкова, которое можно посмотреть по этой ссылке https://www.youtube.com/watch?v=rsO_ofHTfEA

52 Подробнее об ip-адресе https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81

53 Список свободных лицензий https://www.gnu.org/licenses/license-list.ru.html

54 Список лицензий открытого ПО можно найти по этой ссылке https://ru.qwe.wiki/wiki/Comparison_of_free_and_open-source_software_licenses

*— Запрещен на территории РФ