Security in-a-box

**Безопасность в коробке:
материалы по информационной безопасности**

Security in-a-box

Безопасность в коробке:
материалы по информационной безопасности

Сборник “Security in-a-box” разработан под руководством Tactical Technology Collective и Front Line в сотрудничестве с:

Координация, авторы текста и редакторы	Wojtek Bogusz Dmitri Vitaliev Chris Walker
Авторы фрагментов	Cormac McGuire Benji Pereira
Корректура английской версии	Caroline Kraabel Benji Pereira
Тестирование	Rosemary Warner
Дизайн	Lynne Stuart Ana Keshelashvili
Разработка плана работ	Pamela Teitelbaum Dmitri Vitaliev
Координация локализации программ	Louise Berthilson Alberto Escudero Pascual

Испанская команда

Перевод	Phol Edward Paucar Aguirre
Редактирование	Katitza Rodriguez Pereda
Веб-мастер	Angelin Venegas Ramirez
Локализация	Diego Escalante Urrelo
Корректура	Carlos Wertheman

Французская команда

Редактирование, перевод, локализация	Patrick Cadorette
Перевод и локализация	Alexandre Guedon
Корректура	Miriam Heap-Lalonde
Редактирование	Fabian Rodriguez

Российская команда

Перевод	Эмин Ахундов Алексей Бебинов Александр Лапидус
Корректура	Ксения Ширяева
Редактирование, перевод, локализация	Сергей Смирнов

Арабская команда

Редактирование, перевод, локализация	Ahmad Gharbeia
Редактирование	Manal Hassan
Перевод, локализация	Khaled Hosny
Перевод	Mahammad F Kalfat

Особые благодарности	The Citizen Lab, Robert Guerra, Internews, RiseUp, The Tor Project & VaultletSoft
Спонсор	people unlimited HIVOS

СОДЕРЖАНИЕ

Предисловие

Сегодня гражданские активисты уделяют много внимания вопросам цифровой безопасности. Тому есть причина. Компьютеры и сети позволяют работать гораздо эффективнее, чем раньше. Но возникают новые проблемы. Иногда серьезные.

Можно потерять "флешку", а вместе с ней - ценную информацию. Некоторые сайты в Интернете трудно открыть, потому что они попали в некий "черный список". Забытый пароль (ни вспомнить, ни восстановить) становится непреодолимой стеной между вами и сервером. Компьютерный вирус блокирует работу нужных программ. Не удается оформить подписку на полезные рассылки. Тут и там встречается мошенничество с электронными адресами и персональными данными. К сожалению, это не фантазии, а реальные проблемы.

В сборнике вы найдете описания таких проблем и варианты решений.

Материалы адресованы правозащитникам, но аудитория может быть гораздо шире. Ведь проблемы цифровой безопасности - не узко профильные. Всякий, кто имеет дело с компьютерами и сетями, может почерпнуть из этого сборника полезную для себя информацию.

РЕКОМЕНДАЦИИ

Сборник состоит из двух основных частей:

- буклета ("Полезные советы") и
- практического руководства ("Нужные программы").
- к руководству прилагается ряд бесплатных программ.

Буклет - это введение в тему цифровой безопасности. Забавные "живые" персонажи попадают в типичные "компьютерные" истории. Вместе с ними вы преодолеете неожиданные барьеры и получите немало полезных советов о безопасности данных и коммуникаций. Кое-где в тексте будут упоминаться конкретные программы.

Руководство заинтересует, прежде всего, прагматиков - тех, кого волнует вопрос "как сделать". Здесь описываются программы с открытым кодом для защиты информации. Шаг за шагом, начиная с установки, можно знакомиться с каждой программой и ее возможностями.

В сборник включен и раздел о "портативной безопасности". Здесь рассказано о программах, которым не нужна установка на жесткий диск компьютера. Их можно просто записать на USB-"флешку", а значит, легко

использовать на любом компьютере, где есть Windows.

Главы можно читать одну за другой или по отдельности (если вас интересует та или иная тема). Если вы не чувствуете себя достаточно уверенно в теме информационной компьютерной безопасности, советуем познакомиться с буклетом прежде, чем перейти к руководству и установке программ.

Если вы серьезно относитесь своей безопасности, не пропускайте отдельные главы лишь потому, что они кажутся вам "не очень актуальными". Обеспечение безопасности - комплексная задача. Можно хорошо защититься от вирусов, но потерять всю работу из-за сбоя в электросети. Оберегать данные на дисках от посторонних глаз - и дать самой важной информации "утечь" по открытому, незащищенному каналу электронной почты. Одно зависит от другого. Все вместе - это и есть система безопасности. Отдельные фрагменты могут быть интересны, полезны, но если вы не уделяете внимание целому, ваша защита будет состоять из "заплаток", которые легко расходятся по швам. Не допускайте этого.

О проекте security in-a-box

Этот сборник - результат совместной деятельности экспертов по безопасности, правозащитников, разработчиков программ и переводчиков из разных стран мира, которые работали под общим руководством организаций Tactical Technology Collective и Front Line. И материалы, и программы неоднократно использовались на семинарах и тренингах по компьютерной безопасности.

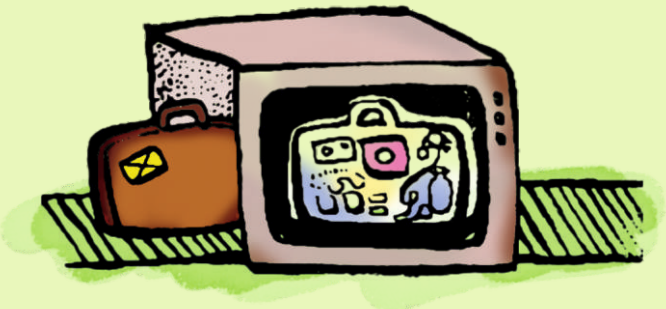
Мир компьютерных программ постоянно развивается. Появляются новые версии, инструменты, подходы. Никакое руководство не заменит толкового консультанта, который "чувствует" обстановку в вашем регионе и обладает самыми свежими знаниями в области информационной безопасности. Материалы этого сборника не следует считать истиной в последней инстанции. Это - руководство к размышлениям и действиям.

Сборник доступен на пяти языках: английском, арабском, испанском, русском и французском. Он существует как в электронном виде (на дисках и в Интернете - **www.security.ngoinabox.org**), так и в печатном. Если вам нужна печатная версия, пожалуйста, напишите нам по адресу **security@ngoinabox.org**.

Tactical Tech и Front Line надеются, что вы оцените этот сборник. Мы будем рады, если вы сможете помочь распространению материалов, переводу их на свой родной язык, использованию в тренингах и семинарах. Ваши рассказы о том, как вам пригодился этот сборник, помогут

скорректировать подготовку следующих версий и получить для них средства. Пожалуйста, присылайте комментарии, рассказы, идеи по адресу **security@ngoinabox.org**.

1 Как не допустить на компьютер вредителей



Как не допустить на компьютер вредителей

Когда что-нибудь происходит с компьютером, мы часто склонны винить в этом вирусы. Это немножко "отдает" детективом и позволяет объяснить то, что не поддается объяснению.

Василь живет и работает в Беларуси. Он работает системным администратором в университете, свое свободное время посвящает небольшой экологической организации, где тоже помогает "по компьютерной части".

Что говорит накопленный опыт Василя, когда он сталкивается с какой-то проблемой?

- Обычно вирусы ни при чем. Настоящая причина где-то еще.
- С вирусами лучше покончить заранее, чтобы искать настоящую причину.

Прежде чем придумывать сложные пароли, устанавливать на компьютер шифровальные средства, осваивать способы надежного удаления данных и делать другие шаги в области информационной безопасности, нужно убедиться, что компьютер (сеть) защищен от вредоносного кода. То есть от вирусов, программ-"шпионов", злонамеренных хакеров и прочих вредителей.

ВИРУСЫ И АНТИВИРУСЫ

Алена и Юрась - школьники. У Василя они переняли пристрастие к компьютерам, хотя до отцовского уровня им еще далеко.

- Если ты собираешь и настраиваешь новый компьютер, какую программу ты ставишь в первую очередь? - поинтересовалась однажды Алена. - Ну, после Windows, конечно.

Василь задумался.

- Наверное, антивирус.

- Откуда на новом компьютере вирусы?

- Они могут попасть из установочных комплектов программ или через Интернет. В любом случае надо быть готовым. Вот почему я устанавливаю антивирус заранее.

История вирусов полна драматизма. За одними вирусами тянется длинный шлейф разрушений. Другие потрясли мир скоростью распространения. Удивительно, что люди знают о потенциальной угрозе, но придают ей мало значения. Недолго думая, они запускают на компьютере скачанные из Интернета игрушки, без колебаний открывают почтовые вложения. Невежество? Как бы не так! Очень многие установили специальные антивирусные программы. Безграничное доверие к антивирусам заставляет пользователя забыть о том, что:

- Не все антивирусы одинаково хороши.
- Даже если у вас очень хороший антивирус, его базу данных(с информацией о вирусах) нужно регулярно обновлять.
- Создатели вирусов (логично) всегда на шаг опережают разработчиков антивирусных средств. Поэтому нельзя говорить о стопроцентной защите.

Одна из популярных, уважаемых и дружелюбных антивирусных программ - **Avast**. Единственное, что авторы просят от пользователей - раз в 14 месяцев проходить формальную регистрацию. Сам Avast, его обновления и базы данных совершенно **бесплатны**.

Смотри руководство "Avast. Уничтожаем вирусы"

- Да я все знаю про антивирусы, - похвастался Юрась, перебивая старшую сестру. - Мне папа уже про это рассказывал.

Надо установить антивирус, и он будет бороться с вирусами сам.

- Если бы все было так просто, твой папа остался бы без работы, - улыбнулся Василь. - Знаешь ли ты, к примеру, что антивирусы бывают двух главных типов: «сканеры» и «щиты»? «Сканер» запускается вручную или по составленному хозяином расписанию и осуществляет проверку компьютера (может быть, одного диска, а то и всей системы) на вирусы. «Щит» после своего запуска все время находится в памяти компьютера: это защита от вирусов в режиме реального времени. Avast объединяет и то и другое.

Несколько советов от Василя, которые могут оказаться полезными для наших читателей:

- Не запускайте на компьютере одновременно два антивируса. Эти программы часто конфликтуют между собой. Перед тем как устанавливать новый антивирус, лучше удалить прежний.
- Убедитесь, что и антивирус, и его базы данных - самых последних версий. Некоторые платные антивирусы работают и, кажется, успешно справляются со своей задачей, но их базы данных безнадежно устарели. Чтобы вернуть возможность обновлений, нужно снова платить.
- Антивирусный щит должен быть постоянно включен (обычно на системной панели, в правом нижнем углу экрана, появляется соответствующий значок). Только тогда он сможет следить за общим здоровьем компьютера и перехватывать подозрительные попытки использования системных ресурсов.
- Время от времени полезно проверять жесткий диск компьютера"на вирусы" с помощью антивирусного сканера. А если вам приносят незнакомую флешку или CD, лучше протестировать их перед использованием.
- Осторожнее с вложениями в электронных письмах. Не открывайте то, что кажется подозрительным. Ассани игнорирует даже "вроде-бы-безопасные" файлы Word, присылаемые иногда коллегами (если никаких дополнительных комментариев нет). Он слишком хорошо знает, что коллеги бывают беспечны в отношении безопасности данных.
- Существуют специальные загрузочные диски. Такой диск можно вставить в компьютер и запустить антивирусную программу, не обращаясь к жесткому диску (где, быть может, бесчинствует вирус).

- И этого достаточно, чтобы защитить компьютер от вирусов? - спросила Алена.

- Пожалуй, да. Но кроме вирусов есть и другие вредные создания. Программы-"шпионы", Интернет-"черви", наконец, злонамеренные хакеры.

- Фу, черви, - скривилась Алена. - Гадость.

- Ничего не гадость, - авторитетно вставил Юрась. - Наоборот, очень интересно. Расскажи, папа!

ПРОГРАММЫ-"ШПИОНЫ" И "ЧЕРВИ"

Программы-"шпионы" попадают в компьютер, получают нужную информацию и передают ее по сети своему владельцу. "Шпион"может записывать нажатия на клавиши клавиатуры, список посещенных веб-сайтов и др. Информация, которую вы считали конфиденциальной, оказывается в руках у того, кому она вовсе не предназначалась. "Черви" проникают в компьютер из Интернета, часто в сообщениях электронной почты в виде вложений. Беспечный пользователь щелкает по картинке, ожидая увидеть нечто совсем безобидное, а запускается вредоносный код. Он может зарегистрировать себя в Windows и выполнить какие-либоразрушительные действия. Часто "червь" находит адресную книгу и рассылает себя по всем обнаруженным адресам. Это похоже на детектив, но на самом деле случается гораздо чаще, чем можно предположить...

Антивирусной программы может оказаться недостаточно. Нужно запустить специальную программу борьбы со "шпионами", такую как Spybot. Эта программа умеет находить и удалять"шпионов". Как и антивирус, Spybot нужно периодически обновлять и регулярно запускать для проверки диска.

Смотри руководство "Spybot. Удаляем программы – "шпионы"

Некоторые советы от Василя:

- Просматривая веб-сайты в Интернете, не теряйте бдительности. Машинальный ответ "да" на предложение что-нибудь скачать и установить – и ваш компьютер под угрозой.
- Используйте дополнения к браузеру, чтобы обезопасить себя во время работы в сети. Если у вас установлен браузер Mozilla Firefox, хорошим примером может быть дополнение Noscript (подробнее см. в главе о Firefox).
- Не стоит запускать программы, скачанные из Интернета, если вы сомневаетесь в их благонадежности.

Во время работы в Интернете вам могут предложить установить (обычно на английском) "Java applets" или "ActiveX controls". Это маленькие программы, которые в ходу у веб-дизайнеров. С их помощью можно создавать насыщенные, функциональные сайты, но они также являются удобными "контейнерами" для вирусов и "шпионов". Noscript успешно блокирует то и другое.

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Межсетевой экран (его иногда еще называют «брандмауэр» или «фаервол») - это программа-сторож. Она подобна контрольной рамке в аэропорту, которая беззвучно пропускает законопослушных пассажиров, но поднимает тревогу, если злоумышленник пытается пронести на борт запрещенный предмет."Умная" рамка может быть настроена так, чтобы некоторые сотрудники аэропорта, которые по долгу службы вынуждены то и дело через нее проходить, "распознавались", и тревожный сигнал не включался.

Межсетевой экран следит за исходящим и входящим трафиком. Иными словами, экран наблюдает за всем, что приходит на ваш компьютер и отправляется с него. Если какое-то действие кажется программе подозрительным, она сообщает пользователю о проблеме, чтобы тот принял решение: "пропускать или нет". Антивирусной программы может оказаться недостаточно. Нужно запустить специальную программу борьбы со "шпионами", такую как Spybot. Эта программа умеет находить и удалять "шпионов". Как и антивирус, Spybot нужно периодически обновлять и регулярно запускать для проверки диска.

- Входящие данные - это понятно, - сказала Алена. - Это нужно для защиты компьютера. А зачем отслеживать исходящий трафик?

- Представь, что, несмотря на все твои усилия, у тебя на компьютере завелась программа-"шпион". Она пытается выйти в Интернет и передать своему хозяину какую-то информацию. Вот тут-то и пригодится межсетевой экран. Он обнаружит подозрительную попытку выйти в сеть, заблокирует ее и сообщит владельцу, то есть, тебе. Разумеется, для "нормальных" программ (например, для браузера Mozilla Firefox) нужно обеспечить "зеленую улицу". Пользователь один раз сообщает экрану, что браузер "имеет право" выходить в сеть, и с этих пор экран не станет чинить ему препятствий.

В последних версиях Windows есть встроенный межсетевой экран. По умолчанию он включен. К сожалению, это довольно ограниченная по своим возможностям программа. Поэтому если вы хотите обеспечить приличную защиту от вторжений извне, есть смысл отключить встроенный межсетевой экран Windows и установить одну из более продвинутых программ этого класса. В руководстве описана установка и использование межсетевого экрана **Comodo Personal Firewall**.

Смотри руководство "ComodoFirewall. Защищаем компьютер от вторжения"

Вот что еще советует Василь:

- Устанавливайте на компьютер только те программы, которые реально нужны. Не пользуетесь - лучше удалить.
- Если скачиваете программу из Интернета, берите ее только с сайта разработчика или из заслуживающего доверие крупного файлового архива. Не пользуйтесь частными страницами и сайтами с неясной репутацией.
- Не оставляйте компьютер без присмотра, особенно на долгое время.
- Если на вашем компьютере работает еще кто-то, кроме вас, попросите системного администратора организовать для вас раздельный вход - каждому свой. Не используйте общий пароль.
- Проверьте, на всех ли компьютерах установлены межсетевые экраны.

Только первой свежести

Компьютерные программы не идеальны. Даже приятные на глаз продукты знаменитых компаний, упакованные в глянцевые коробки с такими ценниками, которые способны вызвать инфаркту неподготовленного человека, содержат ошибки. Некоторым программам не хватает функциональности. У других интерфейс далек от совершенства. Программы постоянно дорабатываются, улучшаются, ошибки исправляются. Выходят так называемые "заплатки" ("патчи", patches), устраняющие тот или иной недостаток. Публикуются новые версии. Иметь программу со всеми последними обновлениями особенно важно, когда речь идет об информационной безопасности. Посудите сами: коммуну жен старенький антивирус, который не распознает вредителей, появившихся в последние два года? Вряд ли вы установили бы у себя на компьютере такого "сторожа".

Обновлять следует как Windows, так и прикладные программы. К счастью, многие программы сами заботятся о себе. Например, браузер Mozilla Firefox чутко следит за появлением новых версий и время от времени предлагает пользователю скачать их из Интернета. Установка обновлений тоже производится автоматически.

Будущее за бесплатными программами

Василь советует не полагаться на "пиратские" версии. Конечно, поначалу кажется заманчивым отдать всего 200 рублей за целый набор замечательного программного обеспечения. Но:

- Нет гарантий, что она будет работать "как надо".
- Скорее всего, "пиратскую" программу нельзя будет автоматически обновлять.
- Использование "пиратских" программ (на языке юристов - контрафактных) преследуется по закону. Сегодня это уже не шутка. Устанавливая "пиратскую" программу на компьютер организации, вы рискуете "подставить" не только себя, но и всю организацию.
- Наконец, **бесплатные программы** бывают просто лучше (функциональнее, удобнее), чем их платные аналоги.

Особое внимание следует обратить на программы с открытым кодом. Когда говорят "**открытый код**" это значит, что **исходные коды** программы доступны широкому кругу пользователей. Это особенно важно для программ в категории "Информационная безопасность".

- Почему? - спросила Алена.

- Коммерческие программы распространяются без исходных кодов. Это понятно: собственник не хочет, чтобы кто-то создал из его исходных кодов свою программу. Ведь она идет в продажу по очень хорошей цене. С другой стороны, можно ли дать гарантию, что платная программа, этот "черный ящик" с неизвестным содержимым, не содержит каких-нибудь критических ошибок? Можно ли поручиться, что ее создатель не встроил в эту программу по настоятельной просьбе спецслужб своей страны особую

лазейку, через которую эти люди, например, могли бы читать чужую электронную почту или проникать на компьютер из Интернета сквозь межсетевой экран?

- Пожалуй, нет.

- И я не поручусь. А программы с открытым кодом проверены сотнями придирчивых специалистов. Значит, и доверия к ним больше.

Ты говоришь о программах по безопасности, - вмешался Юрась. - Это понятно. А как насчет обычных программ? Ну, тех, которыми мы пользуемся каждый день... Windows, Word...?

- Хороший вопрос! - Василий похлопал сына по

плечу. - Я рад, что ты спросил. Очень многие люди становятся зависимыми от собственных привычек. Например, они годами пользуются Microsoft Office (чаще всего "пиратской" версией) и даже не представляют, что есть хорошая бесплатная альтернатива - **Open Office** (полностью совместим с MS Office). Некоторые программы можно с успехом заменить на бесплатные аналоги. Например: Microsoft Office – Open Office (текстовый редактор, электронные таблицы, презентации); TheBat! - **Mozilla Thunderbird** (почта); WinRAR - **7–Zip** (сжатие файлов); Nero Burning ROM - **Deep Burner Pro** (запись CD/DVD); Total Commander - **FreeCommander** (файловый менеджер).

Позвольте, уважаемый Василь, а сама Windows? И как насчет... ну, скажем, Photoshop?

- Существуют и другие операционные системы (например, **GNU/Linux**), но если люди не готовы к смене ОС, возможно, лучшим вариантом для организации будет заложить в бюджет покупку лицензионной Windows. Это не такие уж большие расходы, если сравнивать, например, со стоимостью нового компьютера. Ноутбуки - те чаще всего продаются с предустановленной ОС. А главные приложения вполне можно подобрать из ассортимента бесплатных программ, часто с открытым кодом. Что касается Adobe Photoshop, то это исключительно функциональный графический редактор, но его нельзя отнести к "программам первой необходимости". Большинство пользователей и здесь может подобрать себе бесплатную альтернативу. Те же, кто профессионально (или, скажем так, на хорошем уровне) занимается компьютерной графикой, вынуждены либо осваивать ближайший бесплатный "аналог фотошопа" - **Gimp**, либо платить за серьезный инструмент от Adobe. То же можно сказать о векторной графике, редактировании видео, верстке разных изданий и прочих специфичных программах.

ПОСЛЕСЛОВИЕ

Когда университет, где работает Василь, приобрел пару новых компьютеров, Алена и Юрась получили заманчивое предложение: самостоятельно подобрать для этих компьютеров программное обеспечение, минимальный уровень безопасности для университетских компьютеров (конечно, под руководством отца). Ребята установили все, что советовал им Василь: антивирус **Avast**, "антишпион"

Spybot, межсетевой экран **Comodo Firewall** и др.Оказалось, что даже школьники могут без особого труда справиться с этой задачей.

2 Физическая защищенность информации

Как повысить физическую защищенность информации

Специальные программы могут защитить важные файлы на компьютере. Но они не защитят от кражи, неожиданного обыска с изъятием жестких дисков или опрокинутой чашки кофе. Если мы не хотим тратить время и нервы на борьбу с последствиями "форс-мажоров", нужно не только установить умные программы, но и правильно организовать работу.

Наталья и Олег - пожилая супружеская пара. Они живут в одной из постсоветских стран. У них очень богатый опыт благотворительной работы с ВИЧ-инфицированными. Олег заинтересовался этой темой очень давно, когда его младшему брату поставили страшный диагноз. Но получить квалифицированную и быструю медицинскую помощь тогда оказалось исключительно трудно. Аспирин, бинты, йод — вот те немногие лекарства, которые использовались там, где жили тогда Олег и его семья. А ВИЧ-инфицированных в стране было много. Конечно, в крупных городах и за границей есть клиники, хорошие врачи, новые методики. Олег решил: можно и нужно изменить ситуацию, сделать медицинское обслуживание более доступным и эффективным. Он основал общественную организацию и разработал программу помощи ВИЧ-инфицированным людям.

Постепенно вокруг Олега стали собираться единомышленники. Так пятнадцать лет назад Олег познакомился с Наташей, которая пришла в организацию работать волонтером, а затем стала координатором одного из направлений работы.

Одной из главных проблем для Олега и его коллег оказалась нестабильная ситуация в регионе. Благодаря гранту благотворительного фонда Олег смог купить для своей организации четыре компьютера, но коробки с оборудованием вот уже несколько дней стоят нераспечатанными в углу. Это самая ценная помощь организации за последние годы, и Шингаи не может заставить себя рискнуть. Как подключать новенькие компьютеры к сети, если пробки "вылетают" по три-четыре раза в день? А что если компьютеры просто украдут? Может, поставить металлическую дверь?

За советом Олег и Наталья обратились к Александру, знакомому компьютерщику, который работал в министерстве труда и социальной защиты. Под началом Александра числились десятки компьютеров, и Олег благоговел перед просвещенным другом.

- Что, собственно, тебя беспокоит? - поинтересовался Александр.

Олег эмоционально обрисовал ситуацию. Компьютеры очень нужны для работы, но он, Олег, хочет защитить их от всяких угроз.

- Понятно, - сказал Александр. - В таком случае я советую вам начать с политики **информационной безопасности**.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наибольшая сохранность будет обеспечена той информации, для защиты которой используется комплексный подход. Уважающая себя организация имеет **политику информационной безопасности**.

- Можно попроще? - попросила Наталья.

Хорошо, - вежливо согласился Александр. - Если вы действительно заботитесь об информации и о компьютерах, вам нужно договориться между собой - в своей организации как вы их будете защищать. А для этого сначала нужно оценить риски. Кто вам, в принципе, может угрожать?

Олег и Наталья по очереди стали вспоминать, кто или что может вредить их работе.

- Злонамеренные хакеры и воры.
- Правительство.
- Технические проблемы (вроде сбоев в электросети).
- Собственная небрежность.

- Важно представлять источник угрозы, - продолжал Александр.

- Как видите, источники разные. Значит, и меры против них должны приниматься разные. Решетка на окне способна помешать вору. Но она не поможет, если, к примеру, кто-то из ваших сотрудников, уходя домой, забудет запереть дверь. Пойдем дальше. Какую информацию вы хотели бы защитить?

- Адресные книги.
- Почтовые сообщения.
- Документы по определенным направлениям работы (по важным делам).
- Пароли, ключи, коды доступа.
- Финансовую отчетность и прочие финансовые документы. Архив фотографий и т.д.

- Всякая защита чего-то стоит, - заметил Александр. - Денег, времени. Глупо тратить свои и без того скромные ресурсы на защиту файлов, если они не интересны никому из тех, кого мы перечислили выше. Выделите ту информацию, которая действительно нуждается в защите.

Наталье пришла в голову идея.

- Например, персональные данные ВИЧ-инфицированных. Люди доверяют нам очень личную информацию. Многие боятся, что об их состоянии станет известно, скажем, на работе или среди соседей - и тогда их жизнь превратится в кошмар. Нельзя и мысли допустить, что база данных окажется в чьих-то руках.

- Пожалуй, для нас это “объект охраны номер один”, - согласился Олег.

- Хорошо. У других общественных организаций могут быть свои особенности. Продолжим. Вы сказали, что хотите защитить компьютеры. Подумайте: может быть, есть другие носители информации, которые нуждаются в защите?

- Компьютеры в офисе.
- Компьютеры дома.
- Рабочие USB-флешки.
- Архивные CD и DVD.
- Бумажная документация (хранится в офисе).

- Итак, дело не ограничивается компьютерами. Нужно подумать и о других носителях информации, - сделал вывод Александр.

- Обратите внимание, как вы используете эту информацию и носители. Как передаете друг другу, где храните. Вспомните, какие меры обеспечения информационной безопасности принимаете сейчас. Оцените их эффективность и решите, что следует изменить. Давайте попробуем на каком-нибудь примере. Наталья, у тебя есть флешка?

- Да, и она сейчас со мной. Я всегда ношу ее в сумочке.

- А если сумочку оставляешь дома? Например, когда гуляешь с собакой?

- Обычно перекладываю флешку в карман, но... не знаю... не всегда...

- На ней хранится какая-нибудь информация, которая действительно нуждается в защите?

- База данных, о которой я говорила.

- Есть ли еще где-нибудь копии этой базы?

- Нет, я стараюсь не создавать дополнительные копии даже на рабочем компьютере.

- Имеет ли кто-нибудь еще (кроме Олега, конечно) доступ к этой флешке?

- Уверена, что нет.

- Предположим, твою флешку украли. Сможет ли вор прочитать информацию из базы данных?

- Сын моего друга посоветовал хорошую программу "Суперзащита". Мне она понравилась, я поставила ее на флешку. Теперь она под паролем.

- А теперь, - сказал Александр, - я для примера назову несколько моментов, на которые вам стоило бы обратить внимание.

- Какую реальную защиту обеспечивает программа "Суперзащита"? Что о ней говорят пользователи, профессионалы? Это действительно надежное средство, или с ней справится студент, имеющий опыт взлома компьютерных систем?
- Как согласуется хранение важных документов на флешке с практикой резервного копирования данных в организации? Если вы вообще не делаете резервные копии, может быть, следует подумать об этом?
- В нештатной ситуации (например, Наталья уедет из города) не получится ли так, что члены организации утратят доступ к важным документам на флешке?

Видя, что Олег и Наталья глубоко задумались, Александр поспешил рассеять их беспокойство.

- Вы молодцы, что решили всерьез заняться информационной безопасностью,- похвалил супругов Александр. - Многие на вашем месте просто махнули бы рукой. К сожалению, за такую беспечность однажды можно заплатить очень высокую цену. А другие установили бы несколько крутых компьютерных программ и считали бы, что могут спать спокойно. То, что мы сейчас с вами проделали (в упрощенном виде), специалисты называют «аудит информационной безопасности». Проведите его до конца, и вы сможете написать краткие, но емкие правила - политику

информационной безопасности.

- Пожалуй, мы так и сделаем, - сказал после паузы Олег. - Но, Александр, ты специалист. Может, дашь нам несколько советов п теме физической защиты данных? Что-нибудь практическое, что могли бы использовать у себя в организации.

- Почему бы нет, - согласился Александр.

ФИЗИЧЕСКАЯ ЗАЩИТА

Вот ряд советов, которые дал нашим героям Александр.

- Разузнайте побольше о соседях. Кто занимает офисные помещения справа и слева, напротив, этажами выше и ниже? Если в ваше отсутствие в офис начнет ломиться незнакомец, объясняя, что "забыл ключ", можно ли рассчитывать, что сосед снимет трубку и наберет ваш номер? Или соседу все равно? Или он сам - возможная угроза (см. список потенциальных вредителей)?
- Постарайтесь защитить двери и окна. Как минимум, поставьте приличный замок. Насколько мне известно, оконные решетки у вас есть, это хорошо. Есть смысл подумать о сигнализации или даже о видеокамере, которая следила бы за входом. У дверей здания дежурит вахтер: каковы его возможности? Способен ли он помочь вам задержать злоумышленника или сидит "для декорации"?
- Отделите приемную, куда приходят люди, от рабочих помещений. Исключите ситуацию, когда посетитель пробирается к вам мимо рабочих мест, заваленных важными документами.
- Установите, кто может брать ключи от офиса, а кто не может. Уладьте вопросы с уборщицей, если она приходит по вечерам после работы.
- Избегайте ставить оборудование вблизи проходов, где его могут случайно задеть. Компьютерные провода не должны путаться под ногами или свисать гирляндами со столов. Лучше всего убрать провод в специальный короб.
- Выясните у электрика, есть ли в розетках заземление. Если оно есть, используйте его (вилки с тремя контактами вместо двух).
- Проводка и в особенности розетки должны быть качественными. При необходимости замените их. Нет ничего более жалкого и опасного, чем вывалившаяся из стены, повисшая на проводах, искрящая розетка.
- Подключите компьютеры к электрической сети не напрямую, а через **источники бесперебойного**

питания (ИБП). Тогда броски напряжения в сети не приведут к выключению и порче компьютеров. ИБП стоят денег, но если у вас электрическая сеть такая же, как у нас в министерстве, вы быстро убедитесь, что эти затраты окупаются. Если сейчас вы никак не можете себе позволить приобрести ИБП, используйте простые и недорогие сетевые фильтры. В отличие от ИБП, они не помогут вам при вылетании пробок, но сумеют погасить высокочастотные всплески, что уже неплохо.

- Если в организации используется беспроводная связь с Интернетом, убедитесь, что для нее обеспечен соответствующий уровень защиты. Злоумышленник или просто любитель "халявы" не должен иметь возможность подключиться к вашей сети.
- Ставьте компьютер так, чтобы информация на экране не бросалась в глаза людям, проходящим мимо.
- Не забывайте про вентиляцию. В жару компьютер может перегреться. Не придвигайте корпус задней стороной в плотную к стене, не устанавливайте его под прямыми солнечными лучами или у батареи отопления.
- Если у вас есть ноутбук... (Олег: "Да, есть один!") используйте специальный замок **KensingtonLock.** Это запирающее устройство с металлическим тросиком, напоминает защиту от угона велосипедов. Ведь ноутбук относительно несложно украсть, воспользовавшись шумной, напряженной офисной обстановкой.
- Отлучаясь ненадолго, не оставляйте на экране компьютера важную информацию. Как минимум, запускайте "заставку Windows" под паролем.

  Не выпускайте из виду мобильные устройства, в частности, ноутбук и мобильные телефоны, особенно во время поездок и остановок в гостиницах. Старайтесь не демонстрировать такие устройства на публике, чтобы ненароком не привлечь внимание вора.
- Где бы вы ни были, не забывайте флешки в USB-разъемах компьютеров. Как только работа с флешкой закончена, вытащите ее из гнезда и уберите в надежное место. Проведите инвентаризацию оборудования. Если что-то пропадет, не придется спорить, было такое устройство у вас в офисе или нет. Не забудьте про технику, принадлежащую организации, которая находится "на домах" у сотрудников.
- Упорядочите процедуру создания резервных копий самых важных данных: кто, как и когда этим

занимается, где хранятся архивы CD и DVD.

- Установите пароль для доступа к компьютеру в **BIOS** (это пароль при загрузке компьютера). Это не станет преградой для изощренного вора, но помешает кому-либо "быстренько" получить доступ к содержимому диска, перезагрузив компьютер.
- Используйте **шифрование** для защиты информации не только на настольных компьютерах, но и на мобильных носителях и устройствах.

- И помните, - добавил Александр, - все технические способы защиты работают только "в связке" с административными. Мало установить на дверь надежный замок. Важно, чтобы копии ключей не валялись неизвестно где, а, например, выдавались под расписку тем, кто несет ответственность.

Олег и Наталья задали Александру еще много вопросов и ушли довольные тем, какой полезной оказалась беседа со специалистом.

ПОСЛЕСЛОВИЕ

Главной проблемой для Олега было объяснить сотрудникам своей организации, зачем нужна политик информационной безопасности. Коллеги хмуро переглядывались, вздыхали, жаловались на нехватку времени. По всему было видно, что они согласны - риск существует, но вводить какие-то меры кажется им лишней бюрократией. Положение спасла Наталья, которая с чисто женской интуицией разгадала суть проблемы. Она привела коллегам немало ярких примеров, которые заставили даже самых больших консерваторов согласиться: политика информационной безопасности не только желательна, но и необходима для такой организации, как их группа.

Олег, Наталья и еще двое сотрудников завершили начатый Александром аудит информационной безопасности. Они проанализировали все риски и обнаружили слабые места. В некоторых случаях пришлось буквально следовать советам Александра (например, переставить компьютеры в офисе подальше от батарей и окон, заменить некоторые розетки и др.) Исправляя эти ошибки, они выработали политику информационной безопасности для всех сотрудников организации. Вдобавок они придумали несколько коротких и четких планов действий в проблемных ситуациях:

- Что делать, если случилась пропажа (утечка) конфиденциальной информации?
- С кем связываться, если заискрила проводка или сломался кран в умывальнике?

- Как быть, если утром на вахте не оказалось ключа от офиса?
- Что предпринимает каждый из сотрудников, если власти нагрянули с обыском?

Политика информационной безопасности в организации Олега и Натальи доступна всем сотрудникам. Иногда (раз в год или реже) она изменяется и дополняется (смотря по ситуации). И уже приносит свои плоды. Стало меньше проблем с оборудованием, потерянных данных, конфликтов между сотрудниками. То, что раньше казалось неотвратимой бедой вроде цунами, сегодня выглядит как предсказуемая неприятность, которую легко избежать, если действовать аккуратно и с умом.

3 Создавать и хранить надежные пароли

Как создавать и хранить надежные пароли

Люди привыкли защищать важную информацию с помощью ключей. Ключ от квартиры, ключ зажигания в автомобиле, PIN-код банковской карточки, пароль к электронному почтовому ящику, и так далее. Есть ключ - есть доступ. Можно построить сложную систему запоров, задвижек, замков, сейфов, но если все это открывается единственным универсальным ключом, который висит на крючке у входной двери, грош цена такой системе безопасности.

Василь живет и работает в Беларуси. У него много обязанностей. В числе прочего он следит за локальной сетью в своей организации, а в свободное время помогает решать "компьютерные проблемы" друзьям и знакомым. Его дети- школьники, Алена и Юрась, гордятся отцом, который столько знает и умеет.

- Это, наверное, страшно сложно, - сказал однажды Юрась, заметив у отца на столе книгу об информационной безопасности.

- Не очень, - улыбнулся Василь. - Ты и сам можешь попробовать.

- Попробовать что? - удивился Юрась. - Это ты у нас специалист. А я ничего не знаю...

- Начни с простого: придумай хороший пароль, который я не смогу отгадать.

Пока юный Юрась размышляет над задачей отца, Василь делится соображениями о том, каким должен быть хороший пароль:

- Достаточно длинным. Хотя бы 8-10 символов. Иногда компьютерные программы используют целые парольные фразы.
- Неочевидным. Грубую ошибку совершает тот, кто выбирает в качестве пароля личную информацию, например, номер телефона или кличку любимой собаки. Эти данные могут быть известны другим людям, а значит, им несложно подобрать пароль. В фильме "Идеальное преступление" весь план главного героя в исполнении Майкла Дугласа развалился в один момент из-за того, что он выбрал для своего личного сейфа ужасный пароль - дату собственной свадьбы.
- Уникальным. Не используйте один и тот же пароль снова и снова. В противном случае удачный подбор - и все ваши сайты, дневники, сообщения на форумах

достанутся злоумышленнику.

- Обновляемым. Пароль - не надпись на памятнике. Меняйте его время от времени. Случается, что человек так привыкает к паролю, что не хочет с ним расставаться. Пароль не меняется месяцы, а то и годы. Чем дольше хранится пароль, тем выше вероятность, что его в конце концов узнают те, кому не следовало.
- Приватным. Некоторые наклеивают листочки с паролями на монитор. Наверное, у вас нет этой вредной привычки. Но если пароль все-таки стал известен другим людям(скомпрометирован), смените его как можно скорее. Не стоит хранить пароли в открытых текстовых файлах, документах Word, словом, в таких "контейнерах", которые с легкостью откроет и прочтет всякий.

- Ну, это понятно, - ухмыльнулся Юрась. - А есть какие-нибудь хитрости?

- Хитрости? - переспросил Василь. - Что ж, вот тебе несколько примеров.

Примеры от Василя:

- Меняйте регистр. Как вам, например, такой пароль: "сЕмнадцатьмгнОвенийвЕсны"? (Каждая первая гласная в слове дана в верхнем регистре).
- Используйте не только буквы и цифры, но и другие значки, например, точки, дефисы. Иногда можно удачно заменить букву цифрой, скажем, так: "30л0тые ябл0ки с0лнца". Здесь буквы "О" заменены нулями (а буква "З", кстати, цифрой "3").
- Попробуйте мнемонические выражения. Что такое, к примеру, "КПЧУУРЗЯСФО"? Кажется, что бессмыслица, а на самом деле - начальные буквы слов стихотворения "Ворон" Эдгара По (предлоги опущены): "Как-то в полночь в час угрюмый, утомившись от раздумий, задремал я над страницей фолианта одного".

Даже если вы забудете свои записи, такой пароль вы без большого труда сможете восстановить по памяти (если, конечно, помните первую строчку "Ворона", а если нет, кто мешает использовать строчку из вашего любимого произведения?).

"ПАРОЛЬНЫЕ" ПРОГРАММЫ

Пара-тройка сайтов, любимый форум, почтовый клиент - везде нужны пароли. Если вы активно работаете на компьютере, счет идет на десятки. Запомнить все пароли невозможно!

Некоторые записывают пароли в текстовый файл, а затем шифруют его с помощью криптографической программы. Но можно, как Василь, использовать специальную программу для создания и хранения паролей. Одна из таких программ - **KeePass** - описана в нашем руководстве. Пароли хранятся в **защищенной базе данных**. По сути дела, вам нужно запомнить единственный пароль, который дает вход в саму программу KeePass (пароль, конечно, должен быть надежным). Программа помогает создавать пароли, упорядочивать их (так, что ими становится удобно пользоваться). KeePass может работать с USB-флешки, ее удобно носить с собой.

Смотри руководство "KeePass. Храним пароли в надежном месте"

- Подожди, - Алена, которая до сих пор молчала, с интересом слушая разговор отца и брата, наконец, воспользовалась паузой. - Если я правильно поняла, эта программа позволяет хранить кучу паролей внутри себя. В одном месте. Для доступа к ней нужен еще один пароль, верно?

- Верно, - согласился Василь.

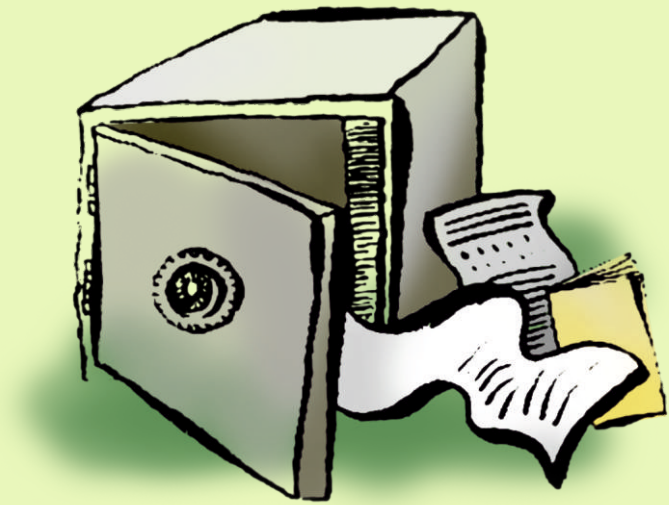
- Что если злоумышленник заполучит этот пароль, скажем, подберет или угадает? Он получит доступ ко всем остальным паролям?

- Ну, во-первых, если злоумышленник подберет пароль, что он с ним станет делать? Ему придется вдобавок украсть у тебя базу данных KeePass, а это может быть непросто. Во-вторых, я для того и рассказывал о правилах и хитростях составления хороших паролей, чтобы вы применили их для защиты (в первую очередь) этого "главного" пароля. В-третьих, его тоже можно менять.

ПОСЛЕСЛОВИЕ

Василю было приятно узнать, что его дети интересуются не только компьютерными игрушками. Но Василь не ожидал, что Юрась по информатике напишет сочинение под названием "Где живут хорошие пароли". Юрась получил за него "отлично", а поскольку его живой ум продолжал выискивать все новые знания, в своей школе Юрась вскоре прослыл знатоком компьютерных дел. Когда кто-нибудь интересовался, как ему удалось то или другое, Юрась, улыбаясь, отвечает: "Вы сами можете попробовать. Начните с самого простого: придумайте пароль, который я не смогу отгадать..."

4 Защита важных компьютерных данных



Белла и Вугар, правозащитники из одной кавказской страны, собирают информацию для доклада о нарушениях прав человека в регионе. Работа идет непросто. Обнаруживаются новые и новые факты угроз, избиений, пыток, несправедливого судебного разбирательства, волокиты и унижения человеческого достоинства. В отдаленных районах страны, где гражданские институты еще совсем не развиты, местные чиновники устанавливают собственные порядки, порой не считаясь ни с конституцией, ни с законами. Доклад Беллы и Вугара может стать первым публичным исследованием на тему прав человека, подготовленным гражданами страны, а не наблюдателями из международных организаций. Вугар использует свои многочисленные знакомства в разных городах, чтобы собрать данные "из первых рук". Он много ездит по стране, беседует с людьми, записывает, фотографирует. Белла обрабатывает информацию. Она систематизирует полученные факты, формирует из них электронную базу данных. Недопустимо, чтобы эта база попала в руки властям (да и вообще посторонним). Иначе те, кто давал сведения, окажутся под угрозой. Многие люди соглашались беседовать с Вугаром только при условии, что их имена и контакты ни в коем случае не будут раскрываться.

Белла использует все свои знания и опыт, чтобы обеспечить базе данных хорошую защиту. Вирусам и хакерам из Интернета на компьютер путь закрыт. Сделаны резервные копии. Что еще?

ЗАШИФРОВАТЬ И СПРЯТАТЬ

Попробуем выделить два основных подхода к защите информации. Данные можно **зашифровать** так, что их не сможет прочесть посторонний человек. Или их можно спрятать, чтобы злоумышленник даже не подозревал о том, что данные существуют.

Замечательная программа **Truecrypt** решает обе задачи сразу.

- Постой, постой, - возразил Вугар. - Я, как и ты, волнуюсь о сохранности базы. Но шифрование - это не слишком, а? Компьютер защищен паролем. Windows тоже требует пароль. Мне даже пришлось использовать одно и то же слово в обоих случаях, а то я постоянно путался и забывал...

- Ну и зря, - парировала Белла. - Если заботишься о безопасности всерьез, не стоит использовать один и тот же пароль на все случаи жизни. Впрочем, та защита, о которой ты говоришь, условная. Любой школьник, прочитавший книжку об устройстве компьютера или даже инструкцию к материнской плате, сумеет сбросить "пароль при включении". Нужно всего-то открыть корпус и поставить перемычку.

- Правда? - Вугар был огорчен. - А пароли для документов Word? Для архивов zip?

- Для опытного человека и это не проблема.

Подробнее о паролях мы рассказываем в главе "Как создавать и хранить надежные пароли".

Truecrypt

Зашифровать информацию - примерно то же, что и положить в хороший сейф, только надежнее. Профессионал-"медвежатник" способен взломать запоры. Сейф можно попытаться взорвать. Обладая терпением и знаниями, можно попробовать подобрать код. Компьютерные программы (многие из которых бесплатны и доступны широкому кругу людей) умеют создавать такие электронные "сейфы", на вскрытие которых даже у крупных корпораций или спецслужб с их мощными компьютерами, деньгами и специалистами уйдут не часы и даже не дни, а годы. **Truecrypt** - одна из таких программ.

Смотри руководство "TrueCrypt. Создаем "сейф" для важных данных"

Truecrypt создает на диске компьютера защищенный (зашифрованный) том. Физически это файл, который может называться как угодно (по выбору пользователя). Операционная система Windows "видит" этот файл как отдельный диск. При записи на этот "диск" данные автоматически шифруются. При чтении - расшифровываются. Все происходит "на лету", пользователь работает так, как работал бы с обычным диском.

- Никакой математики? Не нужно что-то шифровать вручную? - уточнил осторожный Вугар. Имея гуманитарное образование, он немного побаивался технических терминов. Шифрование по-прежнему казалось ему чем-то слишком трудным для простого пользователя.

- Никакой математики, — подтвердила Белла. — Просто окошко, в котором ты включаешь диск, а потом работаешь с ним, как обычно. Конечно, есть программы, которые очень сложны в использовании. Но Truecrypt не из их числа.

О том, как работать с Truecrypt, мы подробно рассказываем в нашем руководстве.

Возможно, вы имеете дело с большим количеством информации, которую нежелательно разглашать кому попало. Это могут быть данные о нарушениях прав человека, как у Вугара и Беллы, или черновики важных статей, или финансовая отчетность. Общее правило: не храните такую информацию по принципу "а пусть будет". Если без нее можно обойтись - удалите (см. главу руководства "Как надежно стереть информацию").

Как не вызвать подозрений

Бывает, однако, что сам факт использования шифрования способен вызвать нездоровый интерес злоумышленников ("если зашифровано, значит, что-то важное"). Для некоторых людей это является решающим аргументом против шифрования. Давайте не будем ничего менять, говорят они. Меньше подозрений - меньше риска.

- Эти люди ошибаются, - подумав, сказала Белла.- С одной стороны, работать с такими серьезными материалами и делать расчет только на "авось", на то, что удастся не привлечь внимание, - безответственно. В конце концов, люди доверили нам важную информацию. Случись что - пострадают, в первую очередь, они. С другой стороны, данные можно не только зашифровать, но и спрятать.

- Все, что ты говоришь, верно, - заметил Вугар. - Но ведь и нашей организации достанется. Нам скажут: "Вы шифруете информацию! Вам есть что скрывать от своей страны! Вы занимаетесь антинародной деятельностью!" Как поступить в такой ситуации? Упереться и все отрицать? Сама знаешь, это к добру не приведет.

Действительно, в некоторых странах факт использования шифрования может стать поводом для давления и репрессий в отношении гражданских активистов.

- Можно вообще отказаться от защиты важной информации. Это просто. Но в любой момент базы могут быть изъяты, пострадают люди, закроют организацию.

"Не лучший вариант", - подумал про себя Вугар.

- Можно использовать стеганографию: скрывать важную информацию в безобидных файлах, например, в картинках. Есть программы, которые умеют это делать. Но стеганография подразумевает ручную работу. Этот метод в большей степени подходит для единовременной передачи какой-то краткой информации по электронной почте.
- Можно хранить всю важную информацию не на своем компьютере, а на удаленном сервере. Идеальный вариант с точки зрения активиста, который опасается обыска и изъятия компьютерной техники. Но работа с удаленными данными требует аккуратности, четкого понимания происходящих процессов, подключения к Интернету (желательно высокоскоростного, если речь идет о больших объемах данных).
- Можно записывать самую важную информацию на флешку. Но такие устройства едва ли более надежны, чем жесткие диски. В конце концов, флешку нетрудно просто потерять.

Мысль о том, чтобы комбинировать описанные выше способы, заставила Вугара вздрогнуть. Конечно, защита информации - дело важное, но нельзя же посвящать ей все рабочее время!

- Для начала можно просто переименовать файл Truecrypt, - предложила Белла. - Например, сделать его с расширением.avi. Он будет выглядеть как видео, например, кинофильм, и не вызовет подозрений.

- Неплохо, но мало, - покачал головой осторожный Вугар. - Файл-то все равно существует. Представь, что ты устроила свой сейф в стене и закрыла его картиной. Большинство людей увидит картину. Но если к нам нагрянут следователи с обыском, они перевернут весь офис и, конечно, найдут за картиной сейф.

- Найдут, - согласилась Белла и подмигнула, - поэтому нужно убедить их, что они нашли именно то,

что искали. Хотя на самом деле вся важная информация будет храниться в другом месте.

- Тогда удастся избежать обвинений... но как? - удивился Вугар.

Что имела в виду Белла? То, что гражданский активист, обвиненный в сокрытии важной информации, может освободиться от подозрений. Truecrypt позволяет создавать "спрятанный" том внутри обычного тома. Никто, кроме вас, не знает, что"спрятанный" том вообще существует. Его невозможно увидеть и даже заподозрить. Поэтому даже если злоумышленникам в руки попадет защищенная Truecrypt информация, даже если они раздобудут пароль, они ни за что не догадаются, что внутри сейфа есть еще одно, маленькое, тайное отделение, где хранится то, что действительно важно.

ПОСЛЕСЛОВИЕ

Вскоре в офисе Вугара и Беллы начался обыск. Следственная бригада искала "экстремистские материалы". В первую очередь следователь изъял жесткие диски. Прошло несколько дней. Беллу вызвали на допрос.

Следователь: Послушайте, давайте начистоту. Мы знаем, что вы располагаете информацией о лицах, подозреваемых в экстремистской деятельности. Отпираться бессмысленно. Наши технические специалисты обнаружили на жестком диске вашего компьютера зашифрованные данные. Вот лист бумаги напишите пароль.

Белла: Уверяю вас, мы не имеем никаких экстремистских данных.

Следователь: Это уж нам судить. Давайте пароль.

Белла: Если я дам вам пароль, вы оставите в покое нашу организацию?

Следователь: Смотря какую информацию мы обнаружим. Так что вы предпочитаете: пароль или обвинение в противодействии следствию?

Белла: Ну ладно, ладно! Вот. (Пишет).

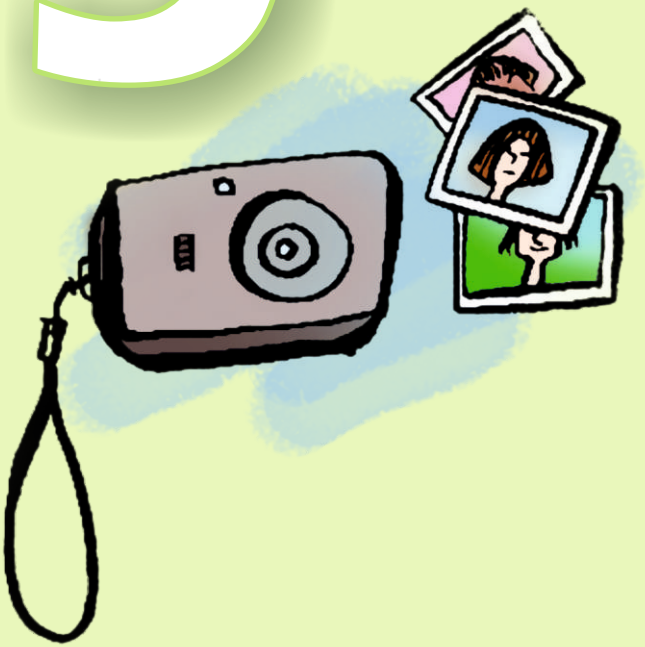
Следователь: Благоразумно с вашей стороны. Лейтенант, посмотрите, что они прячут внутри шифрованного файла, который вы обнаружили. Что там? Фотографии? Документы? Ага!

Довольный следователь уходит "с добычей". Три дня посвящены внимательному изучению содержимого шифровки. Оказывается, что фотографии принадлежат семейному фотоальбому Вугара (Вугар с женой, Вугар с

с детьми, Вугар на море, Вугар в саду и т.д.). Документы тоже не представляют большого интереса. Вся информация, которую они содержат, общеизвестна и никак не тянет на "экстремистские материалы". Ни одной фамилии, ни одного адреса!

Следователю и в голову не пришло, что списки участников мирных собраний в защиту гражданских свобод, которых он хотел упечь в тюрьму как "экстремистов", находились у него в руках. Они были спрятаны в "секретном отделении" **Truecrypt,** о котором знали только Вугар и Белла. Но как обвинишь человека в сокрытии того, что нельзя даже увидеть? А поскольку аккуратная Белла накануне сделала резервную копию этого файла (в числе прочих), работа правозащитников продолжилась без потерь.

5 Как избежать потери данных



Елена Сергеевна взглянула на часы. Она попросила племянника Колю зайти, чтобы "посмотреть компьютер". В последнее время Елене Сергеевне стало казаться, что жесткий диск стал шуметь громче обычного. Вот уже полчаса племянник исследовал его с помощью каких-то специальных программ и хмурился, глядя на экран.

- Мне главное сохранить базу данных и документы, - робко проговорила Елена Сергеевна.

- Не уверен, что получится, - буркнул племянник. - "Винчестер" старый, много плохих секторов. Но ты же делала резервные копии?

Елена Сергеевна вспомнила, как несколько месяцев назад ее бывший коллега по преподавательской деятельности рассказывал, что чуть не потерял черновик докторской диссертации "из-за компьютера". Резервных копий он не делал.

- А они действительно так часто ломаются? - спросила Елена Сергеевна.

- Жесткие диски? Как и любое другое "железо", - ответил Коля. - Но ведь дело не только в них. Данные может уничтожить компьютерный вирус. Или глючная программа. Или пожар, например. Или даже твои собственные коллеги - случайно, конечно. Ведь ты не одна работаешь на компьютере?

- Не одна, - призналась Елена Сергеевна. - Я тут только по вечерам...

- Вот-вот, - продолжал рассуждать племянник. - А ты подумала, например, что твоя правозащитная деятельность может кому-то не понравиться? Вдруг в один прекрасный день придет следователь и унесет компьютер "на экспертизу" вместе со всей твоей работой, и ты останешься у разбитого корыта? Может такое быть?

"Может", - подумала Елена Сергеевна. Она вдруг ощутила собственную беспомощность. Действительно, сломайся сейчас этот электронный ящик, и что тогда? Десятки людей, которые ждут от нее помощи, потеряют подготовленные специально для них документы. Исчезнет ценнейшая переписка. Пропадет база с огромным количеством данных, которые собирались усилиями многих людей на протяжении нескольких лет. Юридический журнал так и не получит статью, над которой она кропотливо трудилась последние три недели. Работа остановится.

- Я тебе расскажу, как обращаются с резервными копиями там, где я работаю, - предложил Коля. - Сама увидишь, это несложно.

КАКАЯ ИНФОРМАЦИЯ – САМАЯ ВАЖНАЯ?

Вот что хранится на компьютере Елены Сергеевны - самое ценное, что ни в коем случае нельзя потерять:

- база данных случаев нарушений прав человека;
- материалы по конкретным делам (ходатайства, жалобы, обращения и т.д.);
- переписка с коллегами и партнерами;
- адресная книга с контактами коллег и партнеров;
- статьи, научные работы.

А еще у Елены Сергеевны установлены и настроены разные программы, которые в случае выхода из строя жесткого диска придется восстанавливать.

У вас, конечно, получится свой список. Возможно, более длинный.

ГДЕ НАХОДИТСЯ ЭТА ИНФОРМАЦИЯ?

Елена Сергеевна попыталась провести ревизию и выяснить, где находятся ее данные. И вот что получилось:

- База данных хранится на жестком диске в папке c:\database.
- Материалы по конкретным делам Елена Сергеевна носит с собой на флешке, так как работает с ними и дома.
- Переписка с коллегами и партнерами частично сохраняется в почтовой программе MozillaThunderbird, а частично остается на сервере почтового провайдера.
- Адресная книга - где-то на компьютере (но где?).
- Статьи, научные работы и прочие важные материалы разложены в десятках разных папок в “Моих документах”. Часть их заполняет флешку.
- Много ценных контактов хранится в мобильном телефоне. (Нельзя ли скопировать их на компьютер?)

Ни для одного из этих типов данных не создавались резервные копии. По крайней мере, это не делалось регулярно.

С дистрибутивами программ все оказалось совсем плохо. Диски, коробки, руководства и драгоценные наклейки с серийными номерами обнаруживались в бумагах, в ящиках стола, на полках шкафов...

КАК ЧАСТО НУЖНО СОЗДАВАТЬ РЕЗЕРВНЫЕ КОПИИ?

Ответ на этот вопрос зависит от того, как часто изменяются сами данные. Адресная книга человека с устойчивым узким кругом контактов может пополняться новыми адресами электронной почты от силы раз в месяц. Но переписку он может вести активную, и сохранять ее понадобится часто, может быть, раз в неделю или чаще.

Если определять свою периодичность для каждого вида данных, задача может показаться весьма сложной. Но кто сказал, что все это расписание нужно держать в голове? Можно составить простой список-напоминание, указывающий дни недели, когда нужно в обязательном порядке создавать резервные копии. Если вы — руководитель организации, можете составить такие напоминания для ваших коллег и сотрудников. Пусть прикрепят на видном месте у компьютера, чтобы помнить о резервных копиях. И не забудьте указать для каждого типа данных, где создавать и хранить резервные копии.

ГДЕ СОЗДАВАТЬ И ХРАНИТЬ РЕЗЕРВНЫЕ КОПИИ?

Главное правило здесь: резервная копия должна храниться на ином носителе данных, чем оригинал. Местонахождение и условия обращения носителей должны быть такими, чтобы гибель оригинала не означала гибели резервной копии - и наоборот.

- Компакт-диск. На CD “влезает” до 700 Мб данных, в большинстве случаев этого достаточно для регулярного резервного копирования. На DVD - 4.7 Гб. Это удачный выбор, если речь идет о резервных копиях больших объемов данных, например, архивов фото или видео. Современные компьютеры обычно продаются с DVD-RW-приводами, которые позволяют записывать и CD, и DVD. Если на вашем компьютере нет такого привода, есть смысл задуматься о его приобретении. В качестве “болванок” используются более дешевые CD-R, DVR+-R с возможностью однократной записи или более дорогие CD-RW и DVR-RW - на них можно записывать, стирать, снова записывать и т.д. многократно. Понадобится также программа для записи (иногда говорят “прожига”) дисков, такая, как DeepBurner.
- USB-флешка, маленькое устройство, которое подсоединяется к порту USB компьютера (сейчас такими портами оснащены все компьютеры, в том числе ноутбуки). При подключении опознается компьютером как еще один диск, а значит, не требуется специальная программа записи данных -

файлы можно переносить на флешку в том же "Проводнике" Windows. Носитель перезаписываемый, емкость измеряется гигабайтами.

- Флеш-карточки, в основном (для восточно-европейских стран) распространенных стандартов MultimediaCard/ SecureDigital, CompactFlash, SonyMemoryStick. Хоть и не столь симпатичны с виду, как USB-флешки, карточки, однако, дешевле, и, что важно, работают не только в компьютерах (например, в цифровых камерах и КПК). Для чтения и записи на карточку требуется "кард-ридер", маленькое дешевое устройство. Специальные программы для записи не нужны.
- Съемные жесткие диски, обычные флоппи-дискеты (до сих пор используются кое-где на старых компьютерах), накопители на магнитной ленте, дискеты Zip и прочие, еще более экзотические варианты.
- Стоящий особняком способ хранения информации - запись через Интернет на удаленный сервер. Возможно, единственный реальный вариант спасения важных данных в условиях давления на организацию, репрессий в отношении активистов, обысков, изъятия компьютерной техники и т.д.

Как это автоматизировать?

Мысль о том, что ей придется регулярно вручную переписывать сотни файлов с одного диска на другой, повергла Елену Сергеевну в ужас.

- Не волнуйся, тетя, - успокоил ее Коля. - Есть программы, которые позволят тебе автоматически сохранять твои данные.

Не нужно ломать голову над тем, где расположены почтовые папки **MozillaThunderbird,** адресная книга, закладки, настройки **MozillaFirefox** и др. Небольшая удобная программа **MozBackup** быстро создаст полную или частичную (по вашему выбору) копию этой информации.

А программа **CobianBackup** позволяет не просто создавать резервные копии важных файлов, но и делать это по расписанию, переносить на удаленный сервер, сжимать и шифровать. Программа может запускаться сама, периодически, в установленное вами время, и работать в фоновом режиме, не отвлекая вас вопросами. Если вам требуется скопировать большой объем данных, программа может заняться этим, когда вы уйдете с работы, а по завершении сама выключит компьютер.

Смотри руководство "CobianBackup. Создаем резервные копии"

Маленькая программа **AllwaySync** позволит синхронизировать содержимое двух носителей (например, папки на жестком диске с оригиналом данных и папки на флешке с резервной копией данных).

План действий Елены Сергеевны

После объяснений племянника Елена Сергеевна несколько успокоилась. То, что раньше казалось ей сложной и муторной ручной процедурой, на которую вечно не хватало времени, теперь представлялось иначе.

Вместе с Колей они набросали план действий, который поможет Елене Сергеевне и ее коллегам спать спокойно, зная, что ни пожар, ни прокурор не нанесут непоправимый урон ценной информации:

- Привести в порядок файлы и папки на компьютере. Избегать ситуаций, когда файлы в рамках одной работы оказываются "в разных углах" жесткого диска.
- Не реже раза в неделю делать полное резервное копирование всех данных из уже составленного "важного списка" (автоматически).Записывать эти данные на DVD-диски.
- Хранить эти DVD-диски за пределами офиса в надежном месте.
- Часть информации сохранять на удаленном сервере в Интернете и обязательно защищать ее с помощью шифрования (конечно, тоже автоматически).
- Дистрибутивы программ, серийные номера и прочую важную информацию, доступную только в печатном виде, хранить на отдельной полке в запирающемся шкафу.
- Убедить руководство, что аккуратность и четкое следование однажды принятым правилам создания резервных копий - лучшая страховка организации на случай любых потерь информации. Пусть другие сотрудники действуют так же аккуратно, как Елена Сергеевна.

ЕСЛИ ЧТО-ТО ВСЕ-ТАКИ ПРОПАЛО

Что делать, если информация все же пропала, например, случайно стерта нерадивым коллегой?

К счастью, Windows не стирает данные буквально, а всего лишь немного меняет название файла — так, что он становится невидимым в системе. Какое-то время файл

можно сравнительно легко восстановить. Есть немало программ, которые успешно справляются с этой задачей. Стопроцентную гарантию успешного восстановления вам никто не даст. Но даже в случаях, когда данные терпят урон из-за аппаратной или программной ошибки, их бывает можно восстановить (хотя бы частично). В нашем руководстве мы рассказываем об одной из программ, которая помогает пользователям восстанавливать удаленную информацию - **UndeletePlus.**

Смотри руководство "UndeletePlus. Восстанавливаем информацию"

ПОСЛЕСЛОВИЕ

Николаю удалось "оживить" жесткий диск на компьютере своей тети. К счастью, ничего не пропало. Но разговор с племянником заставил Елену Сергеевну серьезно задуматься о "страховании" своих файлов. Она стала делать резервные копии. Поначалу это получалось у нее нерегулярно. Но с помощью Коли и собственной настойчивости Елена Сергеевна смогла наладить еженедельное автоматическое сохранение всей важной информации. Через полтора месяца юный отпрыск одного из сотрудников невесть как получил доступ к компьютеру, попытался установить модную игрушку и удалил часть рабочих файлов. Елена Сергеевна без труда восстановила их с помощью **UndeletePlus,** а что не смогла - из свежей резервной копии. Еще через два месяца в офис партнерской организации нагрянули власти. Подозревая активистов в "экстремистской деятельности", следствие изъяло все жесткие диски. На некоторых были результаты долгой и упорной коллективной работы целой коалиции НКО. Коллеги погрузились в отчаяние, но неожиданно для всех дело спасла Елена Сергеевна: у нее оказались резервные копии как базы данных, так и всей недавней переписки.

6 Как надежно стереть информацию

- Кстати, - сказал Николай, - а как ты удаляешь свои файлы? Елену Сергеевну удивил вопрос племянника. Она давно работала в правозащитной организации. Конечно, ей иногда приходилось сталкиваться с такой информацией, которая ни в коем случае не должна попасть в чужие руки. Например, вчера она работала с обращениями граждан о нарушениях прав человека в регионе. Страшно представить, какие проблемы могли бы возникнуть у этих людей, если бы их имена и адреса попали в руки местных властей. Поэтому Елена Сергеевна носила рабочий вариант базы с собой на флешке, а всякие копии старательно удаляла. Коля, компьютерщик и мастер на все руки, вызывал у Елены Сергеевны большое уважение. Наверное, он смог бы восстановить стертые данные, если бы захотел. Но как можно удалять файлы в Windows? Разве существуют другие способы?

- Нажимаю на кнопку "Del", - сдалась обескураженная Елена Сергеевна. - Файл отправляется в корзину.

- Вот-вот, - вздохнул Коля. - Всякий может его оттуда достать. А если это такая информация, которую никому нельзя разглашать?

"Читает мои мысли", - мелькнуло в голове у Елены Сергеевны.

Все правильно: если вы стерли файл в Windows, он перемещается в "Корзину". Восстановить его оттуда не представляет труда даже для начинающего пользователя (см. главу "Как избежать потери данных"). Windows не стирает файл в буквальном смысле этого слова. Операционная система только помечает файл как удаленный. Информация остается на диске, пока Windows не понадобится место, чтобы записать что-то другое. "Вторая жизнь" файла может длиться часы, дни, недели. Даже если его уже не видно в "Корзине", с помощью умных программ вроде **UndeletePlus** его можно полностью или частично восстановить. Не требуются ни специальные знания, ни дорогое оборудование.

Чтобы наверняка избавиться от ненужных копий своей базы данных, Елене Сергеевне потребуется нечто более совершенное, чем стандартная "Корзина" Windows.

Стереть без следа

Один из таких инструментов называется **Eraser.** Это небольшая программа, которая позволяет "начисто" удалять файлы с диска. Программа "дружит" с "Проводником" Windows и другими файловыми менеджерами. Достаточно щелкнуть по файлу правой кнопкой мыши и выбрать в появившемся меню пункт "Очистить".

Файл будет многократно переписан случайными данными по специальному алгоритму. После этого восстановить файл будет невозможно.

Смотри руководство "Eraser. Стираем данные начисто"

- А если я хочу удалить файл не на диске, а на флешке? - поинтересовалась Елена Сергеевна.

- Можно и на флешке.

- А несколько файлов сразу?

- Можно и несколько. Можно целую папку. Или несколько папок. Тебе не придется удалять файлы и папки вручную, по очереди. Просто выдели то, что хочешь удалить, нажми "Очистить", и Eraser выполнит всю остальную работу. Кстати, бывает очень полезно очищать неиспользуемое пространство.

- Зачем? - удивилась Елена Сергеевна. Оно ведь и так не используется, там ничего нет.

Как мы уже говорили, Windows не удаляет файлы буквально, а лишь помечает соответствующую область на диске как свободную (неиспользуемую). Очень скоро "свободное" дисковое пространство заполняется "невидимой" информацией. Не исключено, что среди этой информации есть важные данные, которые следовало бы удалить "начисто". Eraser может об этом позаботиться. Нужно время от времени запускать эту программу для очистки неиспользуемого пространства.

- Хочешь, я приведу пример? - предложил Коля. - Представь, что компания по утилизации мусора решила сэкономить. Она не стала уничтожать хлам, а попросту свалила его в яму и засыпала тонким слоем земли. Получилась ровная лужайка. Для большинства - просто лужайка. Но кто-нибудь настырный может прийти туда с лопатой и выкопать то, что люди выбросили, уничтожили (вернее, думали, что уничтожили). Windows - это компания по утилизации

и мусора. А Eraser - мусоросжигательный завод. Впрочем, в отличие от большинства реальных заводов, очень экологичный: после работы Eraser не остается никаких следов.

Вдобавок, Eraser умеет по-настоящему очищать "Корзину" Windows.

УДАЛЯЕМ НЕНУЖНЫЕ ДАННЫЕ

В "темных углах" операционной системы Windows могут скрываться данные, которые аккуратному пользователю, вероятно, хотелось бы удалить начисто. Эти файлы не были стерты самой Windows, их не всегда просто обнаружить на диске, поэтому Eraser нам здесь не помощник.

- О каких данных ты говоришь? - удивилась Елена Сергеевна, которая втайне гордилась своей аккуратностью.

Вот какие примеры привел Николай:

- Временные файлы Интернета (текст, картинки, всяческие персональные данные, список посещенных сайтов).
- Временные файлы, которые появляются из-за работы разных прикладных программ, например, рабочие копии документов.
- Разнообразные ярлыки, создаваемые Windows для удобства работы.
- Файл подкачки Windows.

- Файл под...качки? Это что-то новое для меня, - призналась Елена Сергеевна.
- Когда память компьютера переполняется (а это бывает, особенно на старых машинах, где мало памяти), Windows использует диск как память для временного хранения данных. Получается большущий файл. Его и называют файлом подкачки. Windows "подкачивает" нужную информацию из этого файла. Это могут быть фактически любые данные. Веб-страницы, текстовые документы, электронные таблицы. Даже пароли. Когда ты выключаешь компьютер, вся информация из памяти исчезает. А файл подкачки остается. Понимаешь?

"Кошмар", - подумала Елена Сергеевна.

Чтобы удалять файлы, о которых говорит Николай, разработаны специальные программы. Например, **CCleaner.** Подобно Eraser, он может быстро и надежно вычистить все эти данные, и компьютер станет меньше похож на склад старьевщика.

Смотри руководство "CCleaner. Избавляемся от мусора"

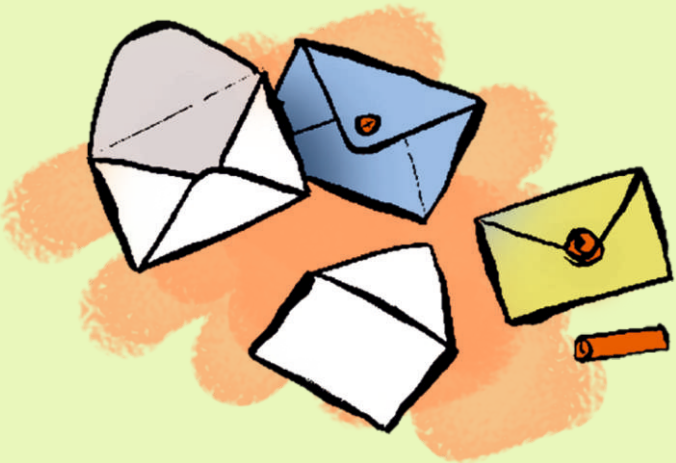
Ну а компакт-диски, на которые записаны резервные копии, "стереть начисто" не получится: эти носители позволяют лишь однократную запись. К счастью, они относительно дешевые, поэтому если возникла нужда избавиться от информации, проще уничтожить CD.

ПОСЛЕСЛОВИЕ

Обычно Елена Сергеевна во всех "компьютерных" делах составляет краткие памятки, пункт за пунктом. Но здесь все оказалось так просто, что памятка Елене Сергеевне не понадобилась. Вся работа состояла из двух пунктов, которые очень скоро вошли у нее в привычку.

- Самые важные файлы, от которых надо избавиться, не выбрасывать в "Корзину", а удалять с помощью Eraser.
- Раз в неделю запускать Eraser для очистки не используемого пространства на жестком диске, а Ccleaner - для удаления всяких временных файлов.

7 Скрыть Интернет-переписку от посторонних



Как скрыть Интернет-переписку от посторонних

Можно ли положиться на Интернет в смысле безопасности? Увы, нет. Электронное сообщение не так уж трудно перехватить, уничтожить, подделать. Многие люди это умеют. Там, где это возможно, лучше использовать защищенную связь.

Настя и Дмитрий работают в правозащитной организации в России. Дмитрий занимается мониторингом нарушений прав человека. Настя помогает ему по технической части. С ними работают и другие люди.

Добровольцы помогают Насте и Дмитрию собирать информацию в отдаленных городах и деревнях. Иногда им приходится рисковать, чтобы добыть важные данные и передать их в центральный офис. Были случаи, когда полиция прослушивала телефоны. Однажды правозащитники обнаружили "утечку" скандальных данных о подготовке мирной акции. Данные передавались по электронной почте. В тот раз властям не удалось помешать проведению акции, но Настя и Дмитрий задумались.

- Не пора ли как-то обезопасить нашу коммуникацию? - спросил Дмитрий. - Сколько можно рисковать важной информацией?!

Как бы ни передавалась информация - по электронной почте, ICQ или как-то еще -нужно, чтобы отправитель был уверен, что его сообщение дойдет в целости и сохранности и будет прочитано именно тем, кому оно в самом деле адресовано. А получатель должен быть уверен, что письмо действительно отправлено вами.

Доставить лично в руки

Мудрые люди говорят: "Не отправляйте по электронной почте то, что категорически не хотите увидеть в вечерних новостях". Это верно. Наши данные обычно "путешествуют" от сервера к серверу открыто. Злоумышленник, имея знания, опыт и должное упорство, может перехватить их.

Когда Дмитрий входит в Интернет и отправляет электронное письмо, оно стартует с почтового сервера. Этот сервер установлен на технической площадке коммуникационной компании. Письмо проходит через несколько компьютеров внутри страны, совершает прыжок через океан и через цепочку серверов оказывается, наконец, в почтовом ящике главного офиса Amnesty International в Лондоне. Если говорить обобщенно, на любом участке этого сложного пути письмо могут перехватить, прочитать, уничтожить или подделать.

- Ну что же, - рассудил Дмитрий, - давайте не будем ничего никому отправлять. Создадим почтовый ящик на каком-нибудь сервере. Пусть все наши сотрудники имеют к нему доступ. Тогда...

Увы, дорогой Дмитрий, это не решит проблему! Когда вы читаете электронное письмо, это значит, что текст был передан с сервера на ваш компьютер. Выходит, передача данных все-таки состоялась. Если правительственный агент приложил ухо к вашему каналу связи, вряд ли вы можете быть спокойны за конфиденциальность переписки.

ЗАЩИЩЕННЫЙ ПОЧТОВЫЙ ЯЩИК

- У меня уже есть почтовый ящик, - сказал Насти недоумевающий Дмитрий. - Зачем еще один?

Обычно почтовые провайдеры не предлагают никакой защиты вашей корреспонденции (кроме антиспамерских фильтров). Как и Дмитрий, мы пользуемся электронной почтой, но не знаем наверняка, сколько человек читает ее вместе с нами.

Очень многие активисты некоммерческих организаций имеют почтовые ящики на сайтах вроде yandex.ru, mail.ru и прочих бесплатных системах электронной почты. Современный почтовый сервис предлагает массу интересных возможностей. Но когда речь заходит о безопасности, популярные сервисы не могут предложить чего-либо выдающегося. Это просто почта.

Между тем, люди давно научились использовать защиту соединений с веб-сайтами. Это полезно, когда вы совершаете покупки, заказываете билеты и т.д. Способ носит название **SecureSocketsLayer (SSL)**. О том, что используется именно он, можно судить по адресной строке браузера (https вместо http). SSL обеспечивает виртуальный "тоннель" между компьютером и веб-сайтом. Этот "тоннель" защищает информацию от чужих глаз. Так можно обезопасить и веб-почту.

Американские Yahoo и Hotmail обеспечивают защиту SSL, когда вы входите в систему. Никто не может украсть ваш пароль — замечательно! Однако сами почтовые сообщения идут через обычное соединение, а значит, открыто. Gmail обеспечивает полную SSL-защиту (https://mail.google.com). Можно зарегистрировать адрес в онлайновой службе **RiseUp.** Создатели этого сервиса предлагают бесплатную почту для активистов разных стран мира, полностью защищенную SSL. RiseUp поддерживается

не коммерческой компанией, а группой энтузиастов. В нашем руководстве описано, как зарегистрироваться в RiseUp.

Смотри руководство "RiseUp. Используем безопасную веб-почту"

- Но мои друзья пишут мне на мой теперешний адрес, вздохнул Дмитрий. - Если я заведу новый, как же я буду получать от них сообщения?

- В современных почтовых системах легко установить переадресацию. Почта, которая будет приходить на твой прежний адрес, автоматически переправится на новый. Это не потребует от тебя постоянной ручной работы. Твои друзья могут писать тебе на любой адрес, их письма до тебя обязательно дойдут, - ответила Настя.

Есть бесплатная служба, которая защищает вашу электронную почту даже от почтового провайдера! Эта служба предлагает такие необычные возможности, как самоуничтожающиеся письма(удаляются сами после того, как их прочитали), безопасное хранение ваших файлов на сервере и на флешке, автоматическое шифрование всей почты и т.д. Правда, чтобы использовать все преимущества, понадобится хорошее соединение с Интернетом. Это чудо называется **VaultletSuite.** В нашем руководстве мы расскажем, как пользоваться VaultletSuite.

См. руководство "VaultletSuite. Защищаем электронную почту"

Советы Насти об электронной почте

Вдобавок ко всему сказанному Настя дала несколько советов по поводу безопасности электронной почты.

- Будьте осторожны, открывая вложенные файлы в чужих письмах. Особенно если это письма от незнакомых людей. Если на компьютере установлен и запущен достаточно свежий антивирус, он, скорее всего, пресечет всякие подозрительные действия. Но зачем экспериментировать? Например, Настя безоговорочно и быстро удаляет все приглашения "посмотреть картинку" или"распаковать архив", если адресаты вызывают сомнения. Даже файлы Word от знакомых и коллег она не принимает. Спокойнее пропустить чей-то очередной пресс-релиз, чем ликвидировать последствия вирусной атаки.

- Со своей стороны, Настя старается не отправлять по электронной почте файлы-вложения, за исключением случаев, когда без этого никак не обойтись.
- Настя настоятельно советует даже не смотреть в сторону писем с предложениями заполнить какие-либо анкеты или сообщить персональные данные. Почти всегда отправители такой почты маскируются под легальные организации, а на деле это мошенники (так называемый phishing - "фишинг"). В ту же корзину отправляются письма с известиями о баснословных выигрышах и просьбы от незнакомцев помочь "обналичить" миллионные состояния усопших африканских родственников ("нигерийские письма").
- Чтобы повысить степень своей анонимности, можно пользоваться существующими сетями вроде **TOR** (см. главу "Как сохранить анонимность и обойти цензуру").
- Создавая новый почтовый ящик, иногда имеет смысл не указывать свое настоящее имя.
- Если компьютером пользуется несколько человек, из соображений безопасности можно время от времени "очищать" временные файлы, связанные с электронной почтой (см. главу о CCleaner).
- Существует еще одна проблема, которой обычно уделяется мало внимания. Это **спам-фильтры**.

Черные списки

За последние пару месяцев Настя и Дмитрий "потеряли" несколько десятков писем. Не то чтобы конверты проваливались в щель между столом и шкафом, нет. Это были электронные письма. Приглашения на встречи, комментарии к новым законопроектам, актуальные статьи. Пропажа обнаружилась случайно. Коллега Дмитрия спросил, почему тот не участвует в дискуссии по правам детей. Ведь это одна из тем, которые, как известно, очень его интересуют. Дмитрий поделился тревогой с Настей.

- Может, за нами уже установили слежку? Нашу почту просматривают и фильтруют?

Настя потратила пару часов, чтобы выяснить причину.

- Ты заметил, Дмитрий, что все пропавшие письма относятся к двум дискуссионным группам, на которые мы с тобой были подписаны?

- И правда! Но почему "были"?

- Наш почтовый провайдер считает, что эти группы - спам.

Спам, мусорная почта. Никто не любит спам. Те, кто получает его центнерами и тоннами, ненавидят спамеров. Понятно, почему услуга электронной почты, "свободной от спама", всегда будет пользоваться популярностью. К сожалению, почтовый провайдер обычно не уточняет, как именно он борется со спамом. Иногда это незатейливый фильтр по ключевым словам, настраивать который придется вам самим. Это может быть довольно сложная система, коммерческий продукт или собственная разработка. Худший вариант - когда почтовый провайдер использует внешний **"черный список" адресов** (типа Spamhaus). В такие списки попадают не только спамеры, но и законопослушные авторы почтовых рассылок. Провайдер, который пользуется таким "черным списком", не имеет возможности им управлять. Он декларирует "эффективную защиту от спама", и все. Когда вместе со спамом клиенты перестают получать важную деловую почту, они часто об этом даже не догадываются. Именно это и произошло с Дмитрием и Настей. Рассылки, которые наши друзья привыкли читать, оказались (не по своей вине) в "черном списке" спамеров, и провайдер перестал их доставлять. Если бы коллега Дмитрия не завел разговор о круглом столе по правам детей, Дмитрий, возможно, еще несколько недель ни о чем бы не догадывался. Только удивлялся бы, почему обычно бурная дискуссия вдруг затихла.

Итак, наш почтовый провайдер может скрыто установить для нас режим цензуры входящих писем. Как от этого уберечься?

- Открывая новый ящик электронной почты, выбирайте систему, которая не использует внешние "черные списки" для фильтрации спама.
- Если у почтового провайдера есть своя собственная система фильтрации спама, уточните, сможете ли вы ее при надобности отключить для своего ящика.
- Не торопитесь объявлять новый адрес всем друзьям и коллегам. Поработайте с ним хотя бы два-три дня. Найдите в параметрах(если есть) настройки спам-фильтра и убедитесь, что можете их менять по своему усмотрению.
- Установите почтовую программу, которая имеет собственные развитые возможности фильтрации спама (например, **MozillaThunderbird**).
- Наблюдайте за периодичностью и объемом переписки. Если популярная рассылка, на которую вы были подписаны, внезапно иссякла, есть вероятность, что провайдер посчитал ее спамом.

- Но что же делать нам? - огорчился Дмитрий. - Как вернуться в рассылку?

- Самый быстрый способ, - ответила практичная Настя, открыть новый адрес в почтовой системе, которая не признает внешние "черные списки", и включить в рассылку этот адрес. А в будущем, Дмитрий, нам нужно задуматься о смене почтового провайдера. Если он, ничего нам не говоря, "чистит" нашу входящую почту от "спама", кто знает, какие еще фильтры он устанавливает, каких сюрпризов от него можно ждать?

ЕСТЬ ЛИ СЛЕЖКА?

Когда какая-нибудь программа отказывается работать или пропадают важные данные, пользователи часто винят компьютерные вирусы. Обычно причина оказывается в другом. Но и вирусы нельзя сбрасывать со счета. То же с «электронной прослушкой».

- Ты заметил, Дмитрий, что электронные письма иногда теряются, не доходят до адресата? Думаешь, их кто-то перехватывает и читает?

- Не уверен, - признался Дмитрий. - А как это выяснить?

Конечно, тот, кто организовал перехват писем, не даст Дмитрию подробный отчет. Однако Дмитрий может сам предпринять несколько умных шагов. Вот что советует в этих случаях Настя.

- Откройте новый ящик электронной почты (в другой почтовой системе), но не удаляйте прежний. Пусть останется в качестве "декорации". Пусть туда приходит почта, и недоброжелатель считает, что этот ящик — основной.
- Не рассылайте сообщения вроде "Вот мой новый адрес!" открытым текстом всем друзьям и знакомым. Сделайте так, чтобы новый адрес трудно было связать с вами (в частности, лучше не указывать свои настоящие имя и фамилию).
- Не провоцируйте фильтры, избегайте "ключевых слов" вроде "права человека", "пытки" и др.
- Используйте защищенные соединения (**SSL**) для получения и отправки почты.
- Используйте **шифрование**.

ШИФРОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

Но, возможно, вам не с руки регистрировать новый адрес электронной почты. А получить нормальную защиту хочется. **Шифрование** помогает решить проблему в корне. Можно шифровать сообщения прямо на своем компьютере, до отправки куда бы то ни было, да так, что никто посторонний не сможет их прочитать. По каким каналам и **серверам** путешествует ваше письмо, через чьи руки оно проходит - все это становится неважным. В нашем руководстве мы не станем забивать вам голову мудреными теоретическими выкладками, а предложим доступные и простые способы шифрования электронных писем.

Кстати, вы все еще пользуетесь OutlookExpress или, может быть, предпочитаете TheBat? А вот Настя давно установила на всех компьютерах своей организации **MozillaThunderbird**. Это замечательный, удобный и "умный" почтовый клиент. Еще лучше он становится, когда вместе с ним работает расширение **Enigmail.** С его помощью шифровать и расшифровывать электронную почту можно буквально на лету. В нашем руководстве рассказывается об этой связке программ.

И помните: если отправитель вложил силы в безопасность, а получатель ни о чем таком не позаботился, от защиты толку мало. Все, кто участвует в переписке, должны придерживаться общего стандарта безопасности. Например, использовать одну и ту же службу электронной почты с SSL-защитой или одну шифровальную программу. Например, GnuPG (прекрасно работает вместе с Thunderbird и Enigmail).

Смотри руководство "Thunderbird, Enigmail, GnuPG. Шифруем почту на лету"

- Подожди-ка, - задумался Дмитрий. - Если, например, я и Владимир установим у себя шифровальные программы, то как мы будем шифровать свою почту? Допустим, я зашифрую письмо. Чтобы его расшифровать, Владимиру нужно знать шифр.

-Это называется "ключ", - вставила Настя.

- Да, ключ, - продолжал свою мысль Дмитрий. - Ему нужно знать ключ. Но как я ему передам этот ключ? Владимир живет за триста километров отсюда! Если я просто пошлю ключ по электронной почте, его перехватят и будут читать всю нашу переписку, как ни в чем не бывало!

- Хороший вопрос, - улыбнулась Настя. -

Создатели шифровальных программ позаботились об этом. GnuPG использует шифрование с открытым ключом. Представь, что программа у тебя на компьютере создает не один, а два ключа, и они работают строго в паре. То, что зашифровано одним ключом, можно расшифровать только с помощью второго ключа. Первый ключ мы называем "открытым". Ты пошлешь его Владимиру по почте...

- Но...

- Послушай, ты можешь даже опубликовать этот ключ в Интернете. Всякий (в том числе Владимир) сможет взять твой открытый ключ, зашифровать им свое письмо и отправить тебе. А вот расшифровать и прочитать это письмо способен только ты. Ведь лишь у тебя есть подходящий закрытый ключ. Если тебе нужно отправить защищенное письмо Владимиру, ты шифруешь послание его открытым ключом и отправляешь по электронной почте. Пусть злоумышленник перехватит шифровку. Пусть он получит ваши открытые ключи. Без закрытых ключей он все равно ничего не сможет сделать.

"Твой старый друг Ярослав"

Однажды Дмитрий получил электронное письмо от своего давнего друга Ярослава, с которым он не виделись уже несколько месяцев. Дмитрий обрадовался старому приятелю. Ярослав писал, что находится в региональном городе. «У нас такое творится, права человека нарушаются самым страшным образом!- взволнованно писал он. - Я хочу создать здесь правозащитную группу. Но у нас мало людей. Многие просто боятся полиции. Пришли, пожалуйста, координаты тех, кто давал тебе информацию для вашего последнего отчета в Amnesty International. Мы свяжемся с ними. Твой старый знакомый Ярослав».

Осторожнее, Дмитрий! Если бы вы с Настей навели справки, то узнали бы, что Ярослав находится в тюрьме. «Письмо Ярослава» составлено правительственным агентом: он стремится получить списки «вредителей», тех, кто в его городе собирает данные о нарушениях прав человека.

Чтобы наверняка знать, кто в действительности написал вам электронное письмо, можно использовать цифровую подпись - что-то вроде хрупкой сургучной печати на королевской почте, только еще надежнее. Если с такой печатью неаккуратно обращаться - сломать, подделать, аккуратно отклеить, изменить содержимое и вернуть на место - это сразу станет заметно.

ИНТЕРНЕТ-ПЕЙДЖЕРЫ

Сегодня очень популярны программы обмена мгновенными текстовыми сообщениями. Иногда их называют “Интернет-пейджерами”. Самая популярная программа этого типа в нашей стране - ICQ. Есть довольно много программ, которые позволяют обмениваться информацией по разным протоколам, включая ICQ. В нашем руководстве описывается одна из таких программ - **Pidgin,** а также расширение OTR, которое позволяет автоматически шифровать сообщения. Чтобы общаться друг с другом в защищенном режиме по ICQ, нужно, чтобы все участники разговора установили себе эту пару программ.

Смотри руководство “Pidgin + OTR. Разговариваем без посторонних”

А знаете ли вы, что в некоторых странах общаться голосом через Интернет запрещено? Да-да. Обычно этого добиваются телефонные компании, для которых Интернет стал серьезным конкурентом. Интернет-телефония дешевле, а порой и вовсе бесплатна. В некоторых программах можно даже позвонить с компьютера на обычный телефон. В России наиболее распространен Skype. Skype шифрует голосовые сообщения “на лету” (правда, только если осуществляется связь Skype - Skype, а не Skype - обычный телефон). Настя часто пользуется Skype. Вчера, наконец, она убедила Дмитрия тоже установить эту программу.

Насколько безопасен Skype? - поинтересовался Дмитрий, который стал особенно осторожным после истории с поддельным письмом Ярослава.

Настя отправилась искать информацию, и вот что выяснилось. Вопрос “Насколько безопасен Skype?” уже не первый год занимает умы пользователей и специалистов. Известно, что Skype шифрует как текст, так и голосовую связь. Но как это происходит? Об этом создатели Skype не говорят. Это продукт с закрытым исходным кодом, поэтому нельзя быть на 100% уверенным, что Skype гарантирует безопасность коммуникаций и не содержит каких-нибудь встроенных “лазеек” для обхода защиты (надо признать, что до нынешнего дня информация о таких лазейках не поступала).

Вот характерный пример, как создатели Skype подчинились местным законам и согласились встроить в свою программу фильтр (информация с официального

сайта Skype):

Skype разрабатывается совместно с TOM Online. Существует версия Skype под названием TOM-Skype, предназначенная для использования в КНР. TOM Online предлагает пользователям свои рекомендации, как не вступить в конфликт с китайскими законами и правилами. В каждой стране, где мы работаем, мы стараемся сотрудничать с органами власти и учитывать особенности национального законодательства и традиции страны. В TOM-Skype встроен фильтр, который обрабатывает текстовые сообщения.

Фильтр содержит список слов, которые не будут отображены в чате Skype.

- Знаешь, Дмитрий, - ответила своему коллеге Настя. - Если бы я была королевой Англии и уехала бы в отпуск, то, пожалуй, не оставила бы создателям Skype свои королевские драгоценности на хранение. Но все-таки лучше использовать такое шифрование, чем просто передавать важную информацию открытым текстом.

ПОСЛЕСЛОВИЕ

Электронная почта - один из главных инструментов в работе Дмитрия. Поэтому он довольно серьезно отнесся к безопасности коммуникаций. В течение месяца при помощи Насти Дмитрий открыл новый адрес электронной почты на **RiseUp**, разобрался с "пропавшими" рассылками, установил и наладил связку **GnuPG** - **Enigmail** (почтовый клиент **Thunderbird** Дмитрий освоил давно).

Коллеги Дмитрия оказались более консервативными.

"Шифровальные ключи? - недоумевали они. - Зачем? Нам они не нужны". Но однажды активист правозащитной организации вез в столицу отпечатанные в регионе листовки для большого митинга в защиту прав и свобод. Власти изо всех сил пытались сорвать митинг. Поэтому о времени приезда курьера и о том, кто это будет, правозащитники старались не распространяться. Тем не менее, полиция задержала этого человека на вокзальной площади под предлогом установления личности. Обнаруженные листовки были изъяты: по словам начальника полиции, они могли носить экстремистский характер. Экспертиза установила, что ничего экстремистского в листовках нет. Но к этому времени митинг уже закончился. Дмитрий и Настя пришли к выводу, что полиция могла прочесть электронную переписку между правозащитниками из разных организаций, где открыто говорилось о том, когда, куда и с каким грузом прибудет

курьер. Некоторые из коллег Дмитрия согласились с ним. Теперь Настя помогает им освоить шифрование. Остальные активисты предпочли ничего не менять в своей работе. Но Дмитрий и Настя надеются, что им удастся убедить всех своих коллег использовать защищенные коммуникации, и для этого не понадобятся столь жестокие примеры.

8 Сохранить анонимность и обойти цензуру

В некоторых странах вполне официально, на государственном уровне существуют системы онлайновых фильтров. Жители этих стран лишены возможности просматривать определенные веб-сайты. Иногда блокировка происходит по названию сайта или по его адресу. А иногда фильтруются поисковые запросы со словами из "черного списка". Фильтры можно "обойти", используя специальные технологии. Это не так трудно, как может показаться.

Дорин и Марина учатся в университете в одной из восточноевропейской стран, где передовые интернет-технологии соседствуют с жесткими моральными и политическими традициями. Уже не первый месяц друзья работают над отчетом о нарушениях прав человека и пользуются, в том числе, материалами из интернета. Глядя на них, некоторые другие студенты стали активнее использовать интернет в университетской библиотеке, в интернет-кафе, на домашних компьютерах. Но странное дело: временами друзья жаловались Дорину и Марине, что не могут посмотреть тот или иной сайт. А совсем недавно Дорина вызывали в деканат, и, между прочим, не рекомендовали "чересчур увлекаться" чтением всяких "неподобающих" материалов из интернета.

В 2007 году в рамках проекта OpenNetInitiative был опубликован отчет, согласно которому в 26 странах из 40 так или иначе использовались фильтрующие технологии. Прежде всего, страдали сайты с материалами на социальные и политические темы, со статьями о межнациональных отношениях, а также те ресурсы, где рассказывалось, как обойти Интернет-цензуру. В последние годы фильтры применяются все чаще и чаще.

ИЗ ЖИЗНИ ЦЕНЗОРОВ

"Хочешь победить врага - сначала познай его привычки", - говорил Дорину его учитель восточных единоборств. Мудрый наставник дал ценный совет, который пригодился ученику и в этот раз.

Доступ к Интернету нам обеспечивает провайдер доступа. Тот, в свою очередь, зависит от "магистральных" провайдеров - компаний, обеспечивающих поток информации (Интернет-трафик) на уровне страны.

Каждый, кто входит в Интернет, имеет постоянный или временный адрес (IP-адрес). Каждый сайт тоже имеет адрес. Эти адреса нужны для нормального функционирования Интернета. К сожалению, они интересуют и спецслужбы, которые отслеживают онлайновую деятельность гражданских активистов, и цензоров, которые блокируют те или иные ресурсы.

Фильтрация - дело, в принципе, нетрудное. Бывают полезные фильтры, которые пользователи сами устанавливают на свои компьютеры (например, чтобы маленькие дети не лазили на сайты "для взрослых"). Но фильтр можно установить и на сервере Интернет-провайдера, и на магистральном канале связи. Хозяин снабжает свой фильтр "черным списком" запрещенных веб-сайтов.

- Я попробовала загрузить сайт независимого информационного портала, - делилась Марина своими наблюдениями с другими студентами, но увидела сообщение "Такой ресурс не обнаружен". Я пробовала снова и снова, на другой день, через неделю - все одно и то же. Между тем, мои друзья из-за границы рассказывали, что в то же время они спокойно входили на сайт и читали свежие материалы.

Обычно так и работает онлайновый фильтр. Иногда пользователь может получить прямое извещение, что материал заблокирован. Бывает, что человек вводит слово в поисковую систему и получает нулевой результат. "Как же так? - думает он. - Материалов на эту тему должно быть предостаточно!" Это еще один пример работы онлайнового фильтра. К счастью, фильтры такого рода дорогие, поэтому они используются сравнительно редко.

КАК ПОЛУЧИТЬ ДОСТУП К САЙТУ?

Марина не может открыть сайт независимого информационного портала, потому что адрес этого сайта попал в "черный список" и доступ к нему закрыт. Можно ли обойти запрет?

Где-то за границей, в странах с относительно свободным доступом к информации находятся компьютеры, задача которых служить посредниками между сервером и пользователем. Марина находит такой сервер (их списки постоянно обновляются и публикуются в сети) и читает все материалы, направляя запросы через него. Для фильтра такая работа выглядит совершенно невинно.

Серверы-"посредники" имеют свое название: **прокси-серверы**.

Прокси-серверы

Некоторые **прокси-серверы** - публичные. Их адреса доступны в Интернете. Воспользоваться таким сервером может каждый (если, конечно, сервер в данный момент работает). Списки публичных прокси-серверов легко найти в сети. Отдельный "вид" прокси-серверов - "анонимайзеры" (иногда их называют "веб-прокси"). Типичный "анонимайзер" - сайт с окошком, как у поисковой системы. В это окошко Марина вводит не слова для поиска, а известный ей адрес веб-сайта с материалами о пытках в полиции (тот самый, который блокируется фильтром). "Анонимайзером" пользоваться очень просто, его не нужно специально настраивать.

- А у тебя были какие-нибудь проблемы с прокси-серверами? поинтересовался Дорин, которого впечатлил рассказ Марины.

- Пересылка запросов и получение информации через любой "посреднический" сервер требует больше времени,подумав, ответила Марина.— Поэтому работа через прокси идет, как правило, медленнее. Кроме того, анонимайзеры не всегда справляются со скриптами — программами, которые выполняются на "конечном" сайте. Из-за этого некоторые сайты выглядят не совсем так, как их видят люди, обращающиеся к ним напрямую. А те, кто управляет фильтрацией, пополняют свои "черные списки" адресами прокси-серверов.

- Значит, прокси-сервером пользуются, чтобы получить доступ к какому-нибудь ресурсу, когда это действительно важно для дела?

- Да, именно так.

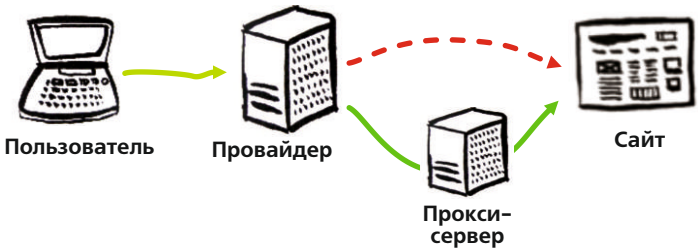
Марина рассказала еще немало интересного из того объема знаний, которые ей удалось получить из Интернета и от знакомых "компьютерщиков".

- Веб-прокси удобны для использования в Интернет-кафе, поскольку, скорее всего, изменять настройки браузера вам никто не даст (а загрузить веб-страницу - пожалуйста).
- Есть программы, которые позволяют сделать использование прокси более удобным (например, быстро переключаться между разными прокси прямо в браузере).
- Хорошо, когда прокси-сервер поддерживает защищенное соединение с пользователем (https://). Если обычный прокси позволяет вам получить доступ к заблокированному сайту, "защищенный" прокси вдобавок не дает злоумышленникам знакомиться с вашими поисковыми запросами и прочей информацией, которую вы передаете по Интернету.
- Публичные прокси нередко бывают перегружены из-за большого числа желающих ими воспользоваться.
- Вполне возможно, что злоумышленники сами откроют публичный прокси-сервер. Передача данных через такого "посредника" небезопасна. В идеале нужно использовать частный прокси, владельцу которого вы доверяете.

СПЕЦИАЛЬНЫЕ ПРОКСИ

Существуют особые прокси, которые удобно использовать для обхода Интернет-цензуры. Psiphon2 - частная анонимная система веб-прокси. Чтобы использовать **Psiphon2,** нужно иметь веб-адрес (URL) прокси-сервера и аккаунт (логин/пароль). Аккаунт можно получить по рекомендации человека, у которого уже есть аккаунт в Pshiphon2. Читатель также может использовать приглашение из печатной версии этого руководства. Подробнее см. PsiphonUser'sGuide.

SesaweHotspotShield - публичная, безопасная, бесплатная система прокси, основанная (в отличие от Psiphon2) не на веб-серверах. Чтобы пользоваться SesaweHotspotShield, нужно скачать утилиту и установить ее на компьютер. Компания-разработчик получает средства рекламодателей, поэтому при посещении сайтов, где не используется **шифрование,** пользователю придется смириться с рекламным баннером в верхней части окна браузера. Если верить разработчику, **IP-адреса** пользователей нигде не фиксируются и не накапливаются (и, тем более, не продаются).



HotspotShield использует технологию виртуальной частной сети (VirtualPrivateNetwork, VPN), поэтому весь трафик пользователя проходит через прокси, к которому этот пользователь "подключен". Это удобно, если вы используете провайдеров электронной почты или мгновенных сообщений, которые заблокированы у вас в стране. Узнать больше о HotspotShield можно, посетив веб-сайт Anchor-Free.

Your-Freedom- частная и безопасная система прокси для обхода фильтров. Так же, как и SesaweHotspotShield, она основана не на веб-серверах. Система бесплатная, но если пользователь заплатит, он получит доступ к коммерческой службе - более быстрой и с меньшими ограничениями. Чтобы использовать Your-Freedom, нужно скачать утилиту и создать аккаунт. То и другое можно сделать на веб-сайте Your-Freedom. Пользователю также придется настроить браузер, чтобы использовать эту прокси-систему. Как это сделать, можно узнать на сайте SesaweProject. **Peacefire** - большое сообщество публичных веб-прокси, которые могут быть как безопасными, так и небезопасными. Если используете прокси из системы Peacefire, нужно начинать адрес с **HTTPS**: тогда соединение между вашим компьютером и прокси-сервером будет безопасным. В большом новостном списке Peacefire регулярно появляются известия о новых прокси. Подписаться можно на веб-сайте Peacefire.

Голландец Ханс

На конференции в Египте Дорин и Марина познакомились и подружились с несколькими молодыми активистами из Европы. Один из них, голландец Ханс, работает системным администратором в правозащитной организации в Амстердаме. Узнав от Марины о проблемах с доступом к веб-сайтам, Ханс предложил свою помощь. "Давайте используем компьютер в Голландии как прокси-сервер, - сказал Ханс. - Вам не придется всякий раз искать публичный прокси, чтобы попасть на нужный сайт".

Ханс воспользовался разработкой исследовательского центра CitizensLab из канадского города Торонто, которая называется Psiphon. С помощью Psiphon всякий, у кого есть более-менее приличный доступ к Интернету и компьютер под управлением Windows, может превратить последний в прокси-сервер. Ханс так и сделал. Он заранее сообщил Марине **IP-адрес** компьютера, и они договорились о пароле для доступа к прокси. Теперь всякий раз, когда Дорин и Марина хотят зайти на "отсутствующий" (читай - заблокированный) сайт, они делают это через компьютер Ханса. А поскольку IP-адрес компьютера Ханса отсутствует в списках публичных прокси-серверов, мало шансов, что он попадет в "черный список".

ЛУКОВЫЙ МАРШРУТ

Когда Марина увлеклась темой анонимного доступа к сети и обхода всяческих фильтров, она была поражена: оказывается, в Интернете существуют целые сети взаимопомощи! Настоящие виртуальные тоннели, где информация передается от одного узла к другому. Злоумышленник уже не может отследить, кто именно читает какой сайт. Одна из наиболее известных сетей этого типа - **TOR** (http://tor.eff.org). "TOR" означает "The onionrouter", буквально - "Луковый маршрутизатор" (эмблема TOR - луковица). Программа переведена на многие языки, включая русский. У нее масса поклонников и разработчиков по всему миру. Поначалу TOR был проектом Военно-морской исследовательской лаборатории США и предназначался для оборонных и разведывательных нужд. Сейчас поддержкой проекта занимается сеть гражданских специалистов в области информационной безопасности.

Смотри руководство "Tor. Обходим цензуру"

Основа TOR - широкая сеть компьютеров, которые управляются добровольцами в самых разных уголках земного шара. Таких серверов тысячи. Они составляют друг с другом цепочки, по которым "путешествуют" запросы пользователей.

- А можно пояснить на каком-нибудь примере? - интересуется Дорин.- Представь, что ты отправляешь письмо и надписываешь на конверте адрес. Но ты не бросаешь письмо в почтовый ящик, а вкладываешь его в другой конверт. На нем ты надписываешь другой адрес, добавляешь фразу "Вскрой меня", и вкладываешь его в третий конверт. И так далее. Десять, двадцать раз. Получится этакая бандероль. Ее-то ты и относишь на почту.

- На почте возьмут мою бандероль и отправят по тому адресу, который написан на внешнем конверте. Получатель вскроет бандероль, увидит новый адрес и перешлет сообщение на него. Так будет продолжаться вплоть до самого первого, маленького конверта. И правда, похоже на "одежки" луковицы! - воскликнул Дорин.

- Верно, - улыбнулась Марина. - Только в Интернете все происходит гораздо быстрее, чем на почте. Получатель вряд ли вообще заметит, как письмо пройдет через всех "почтальонов". Ты, конечно, обратил внимание, что каждый из них "знает" только два адреса: тот, откуда к нему пришло письмо, и тот, куда его надо передать. Ни один сервер в цепочке не знает все адреса от первого до последнего. Сервер, с которого ты в конце концов запрашиваешь информацию, не знает, откуда пришел запрос. А фильтр не срабатывает, потому что не знает, что на самом деле ты получаешь информацию с сайта из "черного списка". В сети TOR сегодня около 100 тысяч пользователей. Такая популярность о чем-нибудь да говорит.

В нашем руководстве подробнее рассказывается о TOR и о том, как можно удобно настроить браузер **MozillaFirefox** для использования TOR.

ПОСЛЕСЛОВИЕ

Марина рассказала студентам о возможности использования прокси-серверов, Psiphon2 и TOR. Для большинства молодых людей ее рассказ не представлял большого интереса; они только больше зауважали Марину как "компьютерщика". Но несколько наиболее активных (а может, самых сообразительных) студентов оценили возможность читать новостные сайты, которые раньше казались им абсолютно недоступными. Понемногу ребята стали втягиваться в правозащитную работу, которой занимались Дорин и Марина.

Ханс между тем сделал доклад на конференции по информационной безопасности в Лондоне. Он рассказал о том, как установил частный прокси-сервер для Марины и еще нескольких друзей из стран, где действуют фильтры. Ханс предложил коллегам из некоммерческих организаций европейских стран последовать его примеру, и несколько НКО, в самом деле, открыли такие возможности для своих партнеров. Тем, кто заинтересовался темой прокси и обхода цензуры, Марина рекомендует несколько интересных ссылок:

- Главы “Интернет-слежка и мониторинг” и “Как обойти цензуру” из пособия Digital Security and Privacy Manual for Human Rights Defenders (англ.).
- Инструкция “Как обойти цензуру” из комплекта FLOSS Manuals (англ.).
- Список инструментов для обхода цензуры и другая полезная информация на сайте SesaweProject(рус.).
- Wiki-страница Internet Censorship Wiki (англ., нем., исп.).
- Подготовленный Citizen Lab “Справочник по обходу Интернет-цензуры” (рус.).
- Второе издание “Пособия для блоггеров” (организация “Репортеры без границ”) (рус.).
- Опубликованное Ethan Zuckerman руководство по созданию анонимных блогов с помощью Wordpress и Tor (англ.).

9 Глоссарий

Глоссарий

В нашем руководстве можно встретить некоторые понятия, которые нуждаются в пояснении. Наш словарь поможет разобраться с этим.

Avast - бесплатная антивирусная программа. Базовая система ввода/вывода (BasicInput/OutputSystem, BIOS) - программное обеспечение "нижнего уровня". С помощью BIOS реализуются многие функции управления компьютером.

Белый список - список веб-сайтов или иных ресурсов, которым пользователь разрешает совершать какие-либо действия (остальные ресурсы по умолчанию блокируются).

Бесплатное ПО - программное обеспечение, за которое не взимается плата.

Вредоносный код - общее название для разных программ, наносящих (или способных нанести) ущерб компьютеру и компьютерным данным. Сюда относятся вирусы, программы-шпионы, трояны и др.

Доменное имя - адрес сайта, например, security.ngoinabox.org. Загрузка - процедура запуска компьютера.

Защищенная база паролей - способ надежного хранения паролей на компьютере.

Источник бесперебойного питания (ИБП, UPS) - устройство на основе аккумуляторных батарей, которое позволяет компьютеру работать некоторое время в случае внезапного отключения электропитания.

Исходный код - код, написанный программистами и составляющий суть программы. Изучение исходного кода может дать специалисту представление о том, как программа работает и какой уровень безопасности обеспечивает.

Кейлоггер - программа-"шпион", которая, будучи установленной на компьютере, следит за нажатиями клавиш и пересылает собранную информацию своему "хозяину". Нередко используется для кражи паролей и других важных данных.

Межсетевой экран - программа для защиты от вторжения на компьютер извне (из Интернета).

Маршрутизатор - компьютерное устройство, которое позволяет нескольким компьютерам одновременно подключаться к Интернету.

Мнемонический способ - способ запоминания сложных паролей.

Обход - способ миновать (обмануть) Интернет-фильтры и получить доступ к нужному ресурсу.

Открытый код - исходный код программы, который публикуется автором для свободного распространения, изучения, изменения и т.д. Программы с открытым кодом проходят многочисленные независимые проверки и поэтому пользуются более высоким доверием пользователей.

Политика информационной безопасности - свод правил, которым организация следует для обеспечения безопасности компьютеров и коммуникаций, защиты от различных информационных угроз и рисков.

Провайдер доступа - компания, которая предоставляет услуги доступа к Интернету.

Прокси - служба-посредник, которой можно воспользоваться для сохранения собственной анонимности в Интернете и для доступа к ресурсам, "закрытым" цензурой. Прокси-серверы бывают бесплатные и требующие доступа (логин, пароль).

Проприетарное ПО - антипод бесплатного программного обеспечения с открытым кодом. Как правило, проприетарные программы - коммерческие, но среди них встречаются и бесплатные (со значительными ограничениями).

Сервер - компьютер, который постоянно подключен к Интернету и предоставляет какие-либо услуги, например, прием и отправку электронной почты.

Сертификат безопасности - способ для владельца веб-сайта подтвердить, что он именно тот, кем себя называет. Поддержка сертификата безопасности в действующем состоянии обеспечивается специальными службами на платной основе.

Стеганография - программный способ сокрытия важной информации в безобидном с виду "информационном контейнере", например, значимого текста - в малоинтересной фотографии.

Файл подкачки - компьютерный файл, который операционная система использует для временного хранения важных данных на жестком диске в процессе работы.

Физическая угроза - (в контексте этого руководства) любая угроза персональным данным, которая может позволить посторонним людям получить физический доступ к компьютеру. Также используется для обобщения разных угроз "физического характера": кражи, уничтожения компьютера, стихийных бедствий и др.

Хакер - (в контексте этого руководства) продвинутый пользователь или компьютерный специалист, который использует свои знания и опыт для несанкционированного удаленного доступа к компьютерной системе.

Цифровая подпись - способ подтвердить (с помощью шифрования), что электронное письмо действительно составлено отправителем.

Черный список - список заблокированных веб-сайтов или иных Интернет-ресурсов. Используется (правительством или провайдерами) для фильтрации доступа пользователей к ресурсам или блокирования услуг, предоставляемых ресурсом.

Шифрование - способ скрыть информацию от посторонних глаз. Полученное письмо может открыть только тот, кому она предназначена - тот, у кого есть соответствующий ключ или пароль.

Ccleaner - бесплатная программа, которая помогает избавляться от временных файлов, «программного мусора» и прочих ненужных данных, а также удалять следы вашей деятельности на компьютере.

ClamWin - бесплатная антивирусная программа с открытым кодом.

CobianBackup - бесплатная программа с открытым кодом для автоматизации создания резервных копий.

ComodoFirewall - бесплатная программа-файруолл (брандмауэр, межсетевой экран) для защиты от вторжения на компьютер извне (из Интернета).

Cookie - маленький файл, который Интернет-браузер сохраняет на компьютере пользователя для идентификации пользователя при посещении веб-сайта. Может содержать приватную информацию.

Enigmail - дополнение к почтовому клиенту MozillaThunderbird, которое обеспечивает использование в этом клиенте шифрования "на лету".

Eraser - программа для полного, надежного уничтожения данных (файлов, папок).

Firefox - популярный бесплатный браузер, альтернатива Microsoft InternetExplorer.

GNU/Linux - бесплатная операционная система с открытым кодом, альтернатива Microsoft Windows.

IP-адрес - уникальный идентификатор, который присваивается каждому компьютеру, подключенному к Интернету.

KeePass - бесплатная программа для организации хранения паролей на компьютере.

LiveCD - компакт-диск, который позволяет запускать на компьютере разные операционные системы без их предварительной установки на жесткий диск.

NoScript - бесплатное дополнение к браузеру MozillaFirefox, помогает защитить компьютер от вредоносного кода на неизвестных веб-страницах.

OfftheRecord (OTR) - дополнение к "онлайновому пейджеру" Pidgin, которое позволяет шифровать данные "на лету".

Peacefire - бесплатная служба, которая знакомит своих подписчиков с обновленными данными о бесплатных прокси-серверах для обхода фильтров и преодоления Интернет-цензуры.

Pidgin - бесплатная программа с открытым кодом, "онлайновый пейджер" для обмена мгновенными текстовыми сообщениям.

RiseUp - почтовая служба, которая обеспечивает лучшую защиту сообщений, чем обычная почта. RiseUp развивается благодаря команде энтузиастов.

SecureSocketsLayer (SSL) - технология, которая позволяет осуществлять безопасную передачу данных между вашим компьютером и веб-сайтами, которые вы посещаете. При подключении к веб-сайту по протоколу SSL в адресной строке браузера строчка начинается не с HTT P, а с HTT PS.

SIM-карта - маленькая карточка, которая может быть использована в мобильном телефоне. На SIM-карте могут храниться номера телефонов, сообщения SMS и другая личная информация.

Skype - бесплатная программа для обмена голосовыми и текстовыми сообщениями. Для использования голосовых возможностей Skype, помимо компьютера, необходимы динамики и микрофон.

Spybot - бесплатная программа для борьбы со "шпионами".

Thunderbird - бесплатная программа с открытым кодом, почтовый клиент. Содержит ряд полезных функций, обеспечивающих безопасность, включая шифрование с помощью Enigmail.

Tor - способ обеспечения анонимности и преодоления Интернет- цензуры.

TrueCrypt - бесплатная программа с открытым кодом, позволяет хранить данные в защищенном шифрованном "контейнере" и работать с такими данными, осуществляя шифрование/расшифровку "на лету").

UndeletePlus - бесплатная программа для восстановления случайно удаленных с компьютера данных.

VaultletSuite - система отправки/получения электронной почты, обеспечивающая надежность и шифрование коммуникаций.

Voiceover IP (VoIP) - технология, которая позволяет реализовать голосовую связь с использованием каналов передачи данных Интернета.

Your-Freedom - бесплатное средство обхода фильтров, использует технологию доступа через приватный прокси. При правильной настройке обеспечивается шифрование подключения к прокси.

УСЛОВИЯ

Программное обеспечение и документация в руководстве “Security in-a-box” (материалы по информационной безопасности) предоставляются “как есть”. Авторы руководства, оставаясь в рамках закона, не предоставляют никаких гарантий или условий, явных или косвенных, в частности, относительно использования данных материалов и программного обеспечения в каких бы то ни было целях. Ни в каком случае Front Line, Tactical Technology Collective или кто-либо из их сотрудников, представителей, авторов и редакторов не несет ответственности за прямой, косвенный, случайный, умышленный или иной ущерб (включая непредоставление товаров или услуг, потерю информации, упущенную выгоду и иные убытки в коммерческой деятельности), какими бы аргументами он ни был подтвержден и обоснован, проистекающий из использования или невозможности использования данного программного обеспечения, даже если в руководстве есть указание на вероятность такого ущерба. Ничто в данном документе не затрагивает ваши законные права.

Сборник “Security in-a-box” обновлен и переиздан при финансовой поддержке Европейского союза в 2015 году. Содержание сборника является исключительной ответственностью Белорусского дома прав человека им. Б.Звозскова и ни при каких обстоятельствах не может рассматриваться как отражающее позицию Европейского союза.

Проект реализуется Белорусским домом прав человека им. Б.Звозскова
http://humanrightshouse.org/Members/Belarus/index.html

Проект финансируется Европейским союзом
Представительство ЕС в Беларуси
http://eeas.europa.eu/delegations/belarus

‘Security in-a-box’ помогает лучше узнать риски и угрозы, которые подстерегают современного человека в сложном цифровом мире. Мы рассказываем об инструментах, с помощью которых можно решать проблемы и делать свою работу безопаснее.

Читателя ждут пошаговые инструкции, практические советы, яркие примеры.

www.tacticaltech.org
www.frontlinedefenders.org

TACTICAL
TECHNOLOGY
COLLECTIVE

Front Line
ЗАЩИТА ПРАВОЗАЩИТНИКОВ

Материалы для правозащитников

ISBN 978-609-95300-4-8

9 786099 530048