ПРИВАТНОСТЬ И БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Бабакова В.Р.,ст. гр. АА-11-19,
Волынцев А.М.,ст. гр. АА-11-19
Костикова М.В. – руководитель канд. техн. наук, доцент
ХНАДУ

На сегодняшний день трудно представить жизнь без использования сети интернет. Независимо от деятельности и потребностей, мы используем его каждый день. Будь то общение с близкими, поиск информации, чтение новостей и т. п. Но часто ли нас беспокоит наша же безопасность? Часто ли мы убеждаемся в безопасности паролей, которые используем? Часто ли задумываемся над безопасностью сервисов, которые используем? Как раз тему безопасности и хотелось бы сегодня затронуть.

Пароли

Одна из проблем паролей связана напрямую с пользователями. Они очень часто забываются. Стремясь запомнить пароли, они пытаются связать их с чем-то, что они не смогут забыть. Но зачастую такие пароли крайне легко взломать и даже угадать.

Никогда не стоит использовать персональные данные. Довольно легко угадать пароли, содержащие, например, фамилию, имя или день рождения первого ребёнка и другие подобные детали. Также не стоит прибегать к использованию реальных слов. Есть множество утилит, которые помогут подобрать пароль. С современным оборудованием, перебор всех слов из словаря не займёт много времени. Положительно повлиять на безопасность пароля может использование текста разного типа, такого как заглавные буквы, цифры и специальные символы. Однако, лучшей практикой является использование разных паролей, состоящих из случайных символов, для каждого сайта, регулярно их обновляя. Но как же их запомнить?

Каждый современный пользователь сети интернет должен использовать менеджер паролей для хранения и управления своими данными. Суть сего программного

продукта заключается в генерировании и хранении данных в зашифрованной базе данных. Однако менеджеры паролей также не могут гарантировать полную защиту, ибо многие из них хранят базы данных на сервере, следовательно, выбор сервиса должен быть тщательным и обдуманным. Несомненно, хранение базы данных локально – лучший вариант. С этой задачей с 2003 года прекрасно справляется KeePass – кроссплатформенная свободная программа для хранения паролей.

Несмотря на внушительный жизненный цикл, приложение и по сей день активно разрабатывается и усовершенствуется благодаря открытому коду. KeePass поддерживает алгоритмы Advanced Encryption Format (AES) и Twofish для шифрования своих баз данных. AES, также известный как Rijndael (произносится Рэндал) – симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США. Этот алгоритм хорошо проанализирован и сейчас широко используется. Стоит отметить, что существуют мошеннические сайты, пытающиеся торговать бесплатной программой.

Операционные системы

Windows – самая популярная операционная система, и это вполне заслуженно. Она прошла долгий путь развития и улучшения. Однако, хотя Microsoft и утверждает, что Windows 10 – лучший продукт корпорации, в некоторых вещах Linux значительно превосходит Windows.

Удобная реализация обновлений. Установка обновлений в Windows 10 может быть крайне неожиданной. Включая ПК, довольно часто можно увидеть сообщение о работе с обновлениями. Причём, на маломощном устройстве настройка может занять длительное время, тормозя выполнение важных заданий. Относительно недавно в Windows всё-таки появилась возможность отключить принудительную перезагрузку, давая пользователю возможность настроить интервал, в течение которого компьютер должен от неё воздержаться. Однако, в Home-версии Windows 10 не предусмотрена возможность откладывать обновления на более чем 12 часов. Некоторые из послед-

них обновлений на определённых устройствах могут даже препятствовать загрузке системы после их установки. В Linux проблема с продолжительными обновлениями, в течение которых пользователь не может ничего делать, отсутствует. Все патчи устанавливаются в фоновом режиме, в это же время пользователь может продолжать работу.

Перезагрузка после обновления в Linux происходит как обычно – никакого ожидания настройки обновлений. Если пользователь не желает устанавливать обновления, система не будет требовать их принудительной установки.

Простая установка приложений. Набор программ в Windows Store крайне мал. Обычно, для установки нужного ПО пользователь заходит на сайт разработчика и скачивает исполняемый файл оттуда. При его же установке есть вероятность также установить нежелательное ПО или наблюдать рекламные сообщения. Однако есть большая вероятность скачать вирус при переходе на мошеннический сайт. Во всех популярных дистрибутивах Linux имеются удобные магазины приложений, которые скачивают и устанавливают программы из сетевых источников. Плюсом источников Linux также являются автоматические обновления приложений из единого источника, вместе с патчами системы.

Высокий уровень безопасности. Хотя Microsoft проделала большую работу над повышением безопасности в Windows 10 и даже встроила собственный антивирус, Windows всё ещё остаётся уязвимой системой. Именно для неё создаётся больше всего вирусов и вредоносных программ. В Linux же практически полностью отсутствуют вирусы.

Полная конфиденциальность. Windows 10 отсылает в Microsoft сведения о том, какие приложения устанавливает пользователь, какие сайты посещает и где он находится. Конечно, эти данные обезличены. Однако, в настройках эту особенность можно отключить, но нет гарантии, что очередное обновление не вернёт опцию в её изначальное состояние. Linux лишена телеметрии. В крайнем случае, в некоторых дистрибутивах пользователю предоставлена возможность вручную

отправить разработчикам отчёт об ошибке. Впрочем, это необязательно и легко отключается.

Открытое программное обеспечение

Открытое программное обеспечение (ПО) – программное обеспечение, чей код, с разрешения правообладателя, доступен публично. Согласно подлинной лицензии с открытым исходным кодом, программное обеспечение разрабатывается совместно, и другие программисты могут просматривать, изменять или использовать код в собственных целях.

Противоположностью открытому ПО является закрытое или проприетарное ПО. Это программные продукты, написанные коммерческими компаниями. По понятным причинам эти компании не хотят, чтобы код их работы использовался и свободно распространялся вне компании, поэтому они скрывают его, используя шифрование, и любая попытка модификации или свободного использования кода без разрешения может привести к исковым заявлениям в суд или хуже.

Оба подхода к разработке ПО можно понять, но с точки зрения приватности и безопасности, закрытый код является большой проблемой. Если никто не может видеть, а, следовательно, проанализировать код программы, нет доказательств того, что программа не содержит вредоносный код. Исходя из этого, слепо верить компании, предоставляющей программное обеспечение с закрытым кодом, крайне легкомысленно.

Если код открыт, он может быть проанализирован независимыми экспертами, для проверки на уязвимости и проблемы с безопасностью. Открытое ПО не является идеальным вариантом, однако его политика – единственный вариант проверки работоспособности продукта. Даже если код не был проанализирован, сам факт того, что он доступен публично, собственно, для того чтобы быть проверенным, является индикатором доверия данному продукту. К сожалению, число специалистов, обладающих знаниями, необходимыми для проверки кода, и свободным временем, крайне мало. Из этого следует, что большинство открытых программных продуктов не подлежали тщательному анализу. Это также подкреплено фактом чрезвычайного

сложного устройства открытых программ, содержащих тысячи строк кода, и даже если код был проверен специалистами, остаётся вероятность проблем, упущенных при анализе.

Исходя из выше сказанного, открытое программное обеспечение не является идеалом, однако, единственной альтернативой является код, доступ к которому не имеет никто.

Браузеры

Использование сети интернет тесно связано с браузером. Часто на устройствах браузер является частью предустановленного программного обеспечения. Однако, стоит помнить, что браузеры часто являются целью атак, а также имеют уязвимости в коде. Пользователь, чаще всего, выбирает программный продукт, предоставляющий ему максимально комфортные условия работы, однако, далеко не всегда не всегда удобное ПО является безопасным. Из ряда свидетельств в прошлом общественности стало известно, что использование наиболее распространённых браузеров сопряжено с рисками безопасности. В первую очередь, попадают под подозрение продукты, которыми владеют крупные компании. Google, Microsoft, Apple по-видимому принимают активное участие в программе негласного сбора информации, передаваемой по сетям электросвязи (PRISM). Браузеры по своей природе очень удобный инструмент для того, чтобы собирать данные о поведении, привычках и предпочтениях пользователей, по крайней мере, в маркетинговых целях. Разумеется, чем более широко используется браузер, тем большую ценность он представляет для корпораций и правительственных организаций в качестве поставщика сведений. Но самая большая неприятность состоит в том, что мы не можем получить полное представление о том, как и для чего собранные данные могут быть использованы сейчас и в будущем, и игнорировать данный факт довольно легкомысленно.

Специалисты в области интернет безопасности (ИБ) хорошо знают, что истинная безопасность подразумевает отказ от многих зависимостей, связанных с платформами, плагинами и любыми другими избыточными элементами для получения как можно более

простого и прозрачного инструмента. Защищённым разумно считать специализированный браузер, который скорее нацелен на решение проблем конфиденциальности пользователей, предоставление им всех возможностей по управлению, исключению сбора данных, пусть даже в ущерб комфортной работе в интернете. Теперь становится понятно, что популярность браузера ни в коей мере не свидетельствует о высоком уровне его защищённости. Более того, эти два качества скорее противоречат друг другу.

Разработка браузера Tor стала своеобразным ответом на стремительное увеличение числа инцидентов безопасности при использовании интернета.

За самим браузером кроется защищённая распределённая сеть из множества прокси-серверов, создаваемая с целью обеспечения анонимности и конфиденциальности пользователя в интернете. Работа браузера основана на принципе «луковичной маршрутизации». Данные множество раз шифруются по мере передачи от сервера к серверу (три выбираемых случайным образом сервера сети Tor – те самые «луковичные слои») защищённой сети Tor, а затем передаются по виртуальному каналу. И точно так же данные расшифровываются очередным «слоем» при получении. Трафик между сетью Tor и целевым ресурсом не шифруется. Поэтому, если пользователь хочет передавать по интернету чувствительную информацию, по-прежнему нужно позаботиться о конфиденциальности за счёт использования HTTPS или иного канала сквозного шифрования, а также механизмов аутентификации. Tor Browser основан на специальной версии Mozilla Firefox с расширенным сроком поддержки (Extended Support Release (ESR)).

Повышенный по сравнению с Firefox уровень безопасности достигается за счёт следующих нововведений:

1. Применение ряда патчей для усиления конфиденциальности.
2. Изменение настроек Firefox, задаваемых по умолчанию, с акцентом на безопасность.
3. Усиление безопасности за счёт использования различных расширений для безопасного просмотра веб-сайтов: HTTPS-Everywhere, NoScript, TorButton.

4. Использование подключаемых транспортных модулей для противодействия цензуре в интернете, которая направлена на блокирование сетей Tor по IP или с помощью механизмов фильтрации потоков трафика.

По умолчанию Tor Browser не сохраняет историю посещений, а Cookies хранятся и используются только на время сеанса. Веб-сайты часто задействуют множество сторонних сервисов для сопоставления активности пользователей на различных ресурсах. Сюда можно отнести кнопки «Нравится» в социальных сетях, рекламные маяки, аналитические инструменты и т. п. Браузер Tor включает несколько дополнительных механизмов контроля за перемещениями информации, ассоциированной с пользователем. По сути, он ограничивает интерфейс взаимодействия пользователя с сервисами интернета исключительно тем веб-сайтом, что задан в адресной строке. И даже если пользователь подключается к двум разным сайтам, которые используют один и тот же сторонний сервис для слежки, браузер обеспечивает прохождение содержимого сайтов через две различные цепочки серверов. Благодаря этому инструмент слежки не будет знать, что оба подключения были установлены из браузера одного пользователя. Некоторые веб-сайты требуют вводить логин и пароль пользователя при входе. В случае с незащищённым браузером, помимо логина и пароля, зачастую раскрывается информация об IP-адресе и местоположении пользователя. С браузером Tor можно в явном виде выбирать, какая информация будет раскрыта при использовании того или иного веб-сайта. Опция «Новая личность» будет полезна, если нужно предотвратить связывание деятельности в браузере с той, что была предпринята ранее. При выборе этой опции будут закрыты все открытые вкладки и окна, очищена вся личная информация, а также будут созданы новые цепочки для всех соединений. Опция «Новая цепочка» может быть полезна, если выходной сервер не может подключиться к веб-сайту или загрузить его корректным образом. В этом случае активная вкладка или окно будут перезагружены в новой цепочке Tor. Браузер имеет элемент управления «Уровень безопасности», который позволяет повышать и снижать уровень защищённости посредством управления набором

потенциально опасных параметров. Повышение уровня может привести к тому, что некоторые страницы будут отображаться некорректно. Оценить приемлемый уровень безопасности достаточно просто, поскольку соответствующее окно настройки содержит всю необходимую информацию о возможных последствиях. Кроме того, в Tor Browser реализованы оперативные механизмы, направленные на информирование и предупреждение пользователя о потенциальных опасностях, связанных с использованием тех или иных веб-сайтов.

Однако, просмотр страниц через Tor Browser, используя, например, мобильный интернет, может быть крайне медленным. Альтернативой может послужить Mozilla Firefox.

В качестве мобильного браузера может послужить Bromite. Основан он на Chromium (open source версия Google Chrome) с блокировщиком рекламы и усиленными настройками приватности. Также предусмотрена блокировка JavaScript.

Расширения для браузера

Расширения помогают достичь наиболее комфортного использования браузера и повышая продуктивность работы. Многие расширения обещают защитить приватность пользователя, но так ли это на самом деле?

Огромное количество расширений может сильно снизить производительность браузера, а в некоторых случаях – даже мешать его корректной работе. Выбирать стоит разумно и помнить, что в данном случае количество лишь противоречит качеству. В магазине расширений Mozilla Firefox некоторые расширения были подтверждены, и их разработка наблюдается самой компанией, следовательно, на такие продукты и следует обратить внимание. Правильно подобранный набор расширений может действительно способствовать повышению защиты и приватности при просмотре веб-страниц, не влияя на работу и производительность браузера.

1. uBlock Origin. Мощный блокировщик рекламы, дающий пользователю полный контроль над процессом блокировки контента. Также стоит отметить отличную оптимизацию, приводящую к малому потреблению ресурсов.

2. NoScript. Мощный инструмент для блокировки JavaScript. Помогает заблокировать работу всех скриптов слежки и сбора аналитики. Работает крайне агрессивно, что может повлиять на работу многих сайтов, однако даёт пользователю полную свободу в выборе ресурсов, которые будут загружены.

3. Disconnect. Защищает пользователя от слежки и вредоносных программ наряду с оптимизациями проводной и беспроводной сети. Расширение блокирует внешние вредоносные Cookie и даёт полный контроль над скриптами и элементами страницы. Также Disconnect защитит пользователя от вредоносных виджетов, с помощью которых, используя украденные Cookie, можно получить доступ к персональной данным, не зная пароля.

4. HTTPS Everywhere. Является обязательным к использованию. После установки, расширение будет переключать соединение к SSL, если возможно, и находить защищённые версии страниц, использующие протокол HTTPS. Работает в автоматическом режиме и не нуждается в тонкой настройке.

Мобильные устройства

Доступ к всемирной паутине нам обеспечивают не только стационарные персональные компьютеры, но и различные мобильные устройства. В наши дни трудно представить жизнь без различных гаджетов, использующих разнообразные операционные системы, программы и приложения. Одной из самых популярных операционных систем является Android. Тут необходимо упомянуть несколько ключевых моментов влияющих на безопасность. Во-первых, Android – это открытая операционная система, что позволяет вносить изменения в её код. Во-вторых, Android принадлежит компании Google, что также накладывает некоторые отпечатки на функционале и безопасности устройства, оснащенного данной ОС.

На сегодняшний день, Android это не просто операционная система, а целая инфраструктура. Сегодня на ней работают смартфоны, планшеты, смарт часы, телевизоры и даже мультимедийные системы в автомобилях. Заметим, что компании Google, выкупившей стартап

Android, пришлось пройти долгий путь перед тем, как эту операционную систему начали повсеместно использовать.

Эта история началась в уже далеком 2003 году, когда Энди Рубин со своими товарищами решил создать операционную систему для мобильных устройств и зарегистрировал компанию Android Inc.

Однако данный проект оказался непонятым широкими массами, и не был оценён инвесторами, в связи с чем, к 2005 году Энди и его друзья потратили все свои средства и компания оказалась на грани банкротства.

По счастливой случайности, на них обратила внимания компания Google, и 17 августа 2005 года компания Android Inc. полностью вошла в состав корпорации Google.

С тех пор этот проект активно, и сегодня мы можем наблюдать уже версию Android 10.0.

Эта операционная система имеет открытый код и может использоваться сторонними компаниями для усовершенствований и адаптации к конкретным девайсам. С одной стороны это большой плюс, так как всегда можно проверить код на предмет вирусов и вредоносного софта, с другой стороны в этом кроется серьёзная опасность, ведь далеко не все компании являются честными, и очень часто используют разного рода предустановленные приложения для слежки за пользователем. В большей части случаев, эта слежка является скорее коммерческой, то есть её задача заключается в том, чтобы вычислить ваши предпочтения и вовремя показать вам «нужную» рекламу. Однако сам факт сбора информации сторонними компаниями, пусть и в сугубо коммерческих целях, является достаточно неприятным, ведь нет никаких гарантий, что ваша личная информация не попадет в руки мошенникам. Избежать этой ситуации может помочь установка неофициальной прошивки на базе Android, с возможностью отказа от различных предустановленных приложений и использованием «чистой» операционной системы. Проверенным примером такой прошивки можно считать LineageOS или же CyanogenMod.

LineageOS(CyanogenMod) – неофициальная прошивка созданная группой энтузиастов на базе операционной системы Android. Она не

содержит даже приложений от Google (Play, Services и других), они ставятся отдельно. Как правило, на CM переходят более опытные пользователи, более-менее разобравшиеся, как взаимодействовать с ОС Android.

Традиционно для неофициальных прошивок, CM предоставляет расширенный функционал и большое количество настроек, которых вы не получите в стандартных версиях Android. Это позволяет значительно повысить уровень приватности, а так же производительности смартфона, ведь очень часто случается так, что производители телефонов спустя некоторое время просто перестают выпускать обновления для своих старых моделей, и такой переход на новую, более актуальную, пусть и неофициальную прошивку позволит оживить стремительно «умирающий» экземпляр.

К сожалению, не существует идеальных вещей, и CM не исключение. У неё так же есть ряд минусов: во-первых, в связи с возросшими возможностями в плане настройки операционной системы повышается и уровень ответственности, и как следствие возникает необходимость в более высоком уровне эрудиции в данной сфере со стороны пользователя. Во- вторых, нередки проблемы со стабильностью системы, и не удивительно – группе энтузиастов трудно соперничать с крупными корпорациями.

Google Play не является единственным каталогом приложений для Android девайсов. Даже если не брать во внимание отдельные региональные платформы, используемые только в отдельно взятых государствах, можно насчитать множество популярных площадок, торгующих мобильным софтом. Однако, из-за агрессивной рекламы Google Play, который компания Google называет единственным безопасным магазином приложений, многие пользователи боятся даже подумать о том, чтобы обратиться к альтернативным площадкам. Одним из примеров действительно надежных и достойных площадок можно считать F-Droid.

F-Droid – это альтернативный каталог приложений для Android. Несмотря на свою относительную неизвестность, когда речь заходит о безопасности, равных ему

практически нет. Добиться такого уровня надёжности размещаемого ПО разработчикам F-Droid удаётся благодаря ручному анализу каждого приложения на предмет скрытых функций, трекеров и вредоносных компонентов. Убедиться в этом может любой желающий, перейдя на страницу с исходным кодом, которая дается на странице каждого приложения.

Проверку приложений производят не модераторы-энтузиасты, трудящиеся на добровольных началах, а профессиональные программисты и исследователи в области кибербезопасности. К примеру, недавно к команде F-Droid примкнули сотрудники лаборатории компьютерной безопасности Йельского университета. А уж упрекнуть их в плохой подготовке явно не удастся.

Помимо безопасности, которая для многих имеет определяющее значение, F-Droid полностью бесплатен. Все приложения распространяются на безвозмездной основе. Более того, разработчикам не позволяют встраивать инструменты проведения платежей в приложения. Поэтому единственным вариантом для пользователей поблагодарить их за труды остается пожертвование.

Оформление каталога, по сути, стандартное для большинства подобных магазинов, поэтому останавливаться на нем мы не будем. Другое дело – его функции. F-Droid позволяет выбрать для загрузки любую версию приложения, существовавшую ранее. Если последнее обновление вас чем-то не устроило, всегда можно вернуться к предыдущей версии и продолжить ее использование. Также при необходимости можно включить Tor-шифрование. В таком случае никто не сможет перехватить ваш трафик и узнать, какие именно приложения вы скачиваете. Имеется возможность скачивать ПО даже без интернета. Для этого предусмотрена функция подключения к смартфону другого пользователя F-Droid с последующей установкой P2P-соединения (рис. 1).

Однако существует два недостатка. Первый заключается в том, что тщательная проверка приводит к очень внушительному списку отсеянных приложений и как итог, к крайне узкому ассортименту.

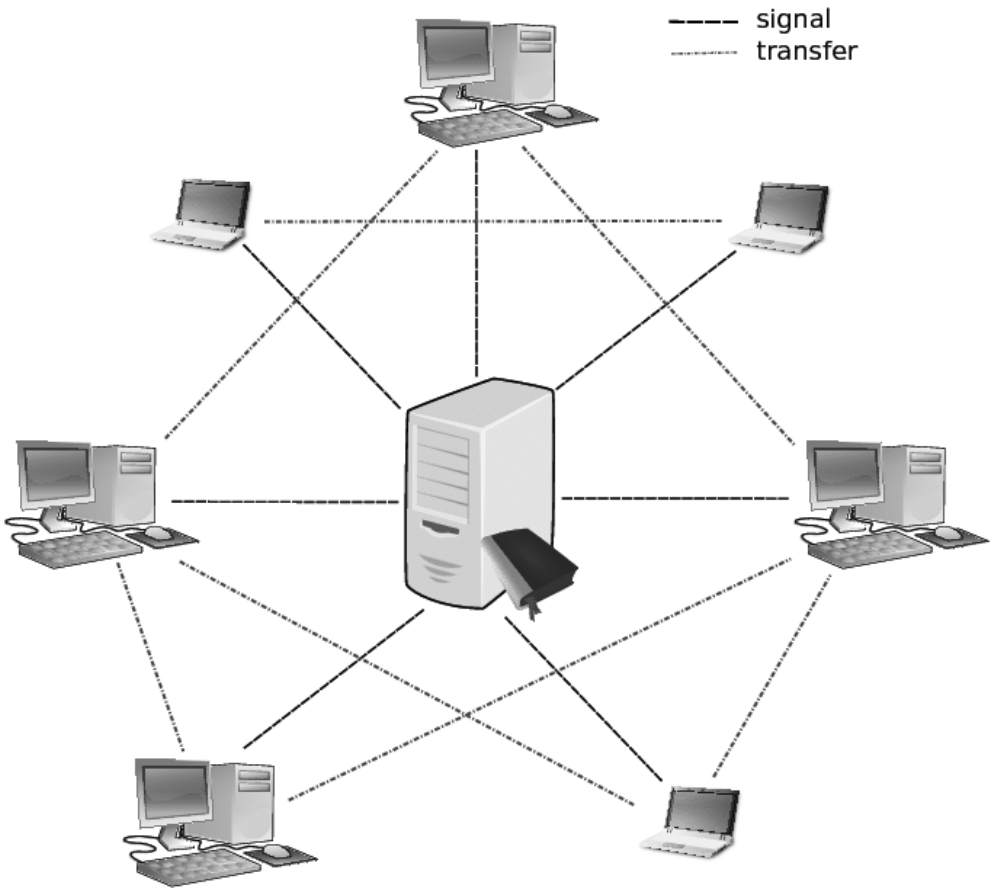

Рисунок 1 – P2P соединение

По заявлениям создателей F-Droid, на сегодняшний день на их площадке представлено всего около трёх тысяч программ и приложений. Второй же состоит в относительной бесполезности всех защитных механизмов, применённых разработчиками. Ведь, если вы пользуетесь F-Droid на постоянной основе в надежде спастись от слежки, вы встречаетесь с одной глобальной проблемой. Дело в том, что в Android и без того масса всевозможных трекеров, которые отслеживают ваши перемещения, слушают то, о чем вы говорите и отправляют эти данные в Google. Как следствие, ни о какой 100-процентной защите говорить не приходится.