Защищаем систему от вирусов

Проверка безопасности антивирусных инструментов выявила, что у самих инструментов есть очевидные слабые места. CHIP расскажет, как можно закрыть уязвимости и обезопасить себя от угроз, которое несет вредоносное ПО

Специалисты по безопасности компании Symantec регистрируют 13 миллионов новых вариантов вредоносного программного обеспечения в месяц. Антивирусные системы призваны защищать от этой опасности, но очевидно, что они сами оказываются уязвимыми и подвергаются атакам. CHIP проверил антивирусы вместе с AV-Test. Результат дает повод для тревоги: в некоторых случаях недостаточно защищены каналы передачи, в других — производители используют ненадежные библиотеки программ. Мы покажем, какие антивирусные инструменты достойны рекомендации, как работают защитные механизмы программ, и объясним, как лучше всего можно настроить эти инструменты.

Даже если вы пользуетесь хорошей антивирусной защитой, нужно дополнительно использовать и программы других производителей. Так вы сможете эффективно обезопасить не только стационарный ПК, но и мобильные устройства — и при этом не имеет значения, идет ли речь об Android или iOS.

Так защищают антивирусы

Современные антивирусные приложения не только защищают компьютеры от уже известных опасностей, но и предлагают инструменты против уязвимостей нулевого дня. Для этого они используют эвристические методы для постоянного контроля ПК. Но для того, чтобы программы могли эффективно контролировать систему, им требуются расширенные права. Доходит до того, что зачастую они могут контролировать и изменять ОС в большей степени, чем зарегистрированный пользователь. Для хакеров успешные атаки на антивирусные инструменты становятся самым простым решением, так как через эти ин-

ФОТО: santiago silver/Fotolia.com

струменты они могут сразу получить системный доступ к ПК, а также деактивировать контрольную функцию антивирусных мониторов. Производители защитных программ борются с этим тремя антихакерскими функциями.

Безопасное соединение при загрузке

Первый уровень защиты используется уже на сайте производителя. Ведь разработчики антивирусов больше не распространяют свои программы на DVD — в основном те предоставляются клиентам в виде пакета с кодом для загрузки. Преимущество в том, что у пользователя всегда будет новейшая версия. Некоторые производители распространяют программы через безопасное HTTPS-соединение. Канал передачи данных зашифровывается, манипуляции практически исключаются. Правда, есть и такие компании, которые все еще делают ставку на небезопасное HTTP-соединение. Теоретически в этом случае хакеры могут перехватить поток данных и подсунуть пользователю небезопасную, управляемую извне версию антивируса. Компания AV-Test обнаружила такой ненадежный канал загрузки у нескольких производителей (см. таблицу справа). Увидев результаты, фирмы торжественно поклялись устранить все недостатки и высказали намерение передавать данные в зашифрованном виде в самом ближайшем будущем.

Обновления только с подписью

Чтобы на ПК загружались только сертифицированные и защищенные подписями обновления для сканирования файлов, антивирусные программы используют сертификаты, хотя и не слишком последовательно (см. справа). С их помощью производитель подписывает отдельные программные пакеты. При поступлении на компьютер пользователя антивирусный инструмент проверяет аутентичность цифровой подписи и устанавливает обновления. Таким образом исключаются неправомерные апдейты. Но это выполняется при условии, что антивирусная программа отлично работает с самого начала и имеет оптимальные настройки, установленные производителем — к сожалению, очень многие приложения таким требованиям не отвечают. И вам придется действовать самостоятельно — более подробно об этом рассказывается на следующих страницах.

Защита оборудования на уровне процессора

Начиная с Windows XP SP2 операционная система Microsoft поддерживает защиту DEP (Data Execution Prevention), которая работает непосредственно в процессоре. Принцип работы относительно прост: ОС использует специальный атрибут NX-Bit (бит запрета исполнения) для определенной области памяти, где хранятся данные, имеющие критическое значение. Если какая-то программа, например, при переполнении памяти, пытается задействовать регистр процессора, DEP блокирует доступ и передает информацию об этом в операционную систему. На сегодняшний день технология является стандартом — но, несмотря на это, ее используют не все (см. справа). Сама по себе DEP не обеспечивает стопроцентную защиту. Поэтому производители используют функцию вместе с другими технологиями.

Программное обеспечение, предотвращающее переполнение памяти

Чтобы хакеры не могли угадать, где именно в памяти компьютера хранятся критически значимые данные, уже более десяти лет назад была разработана технология ASLR (Address Space Layout Randomization). При этом программы получают свои области →

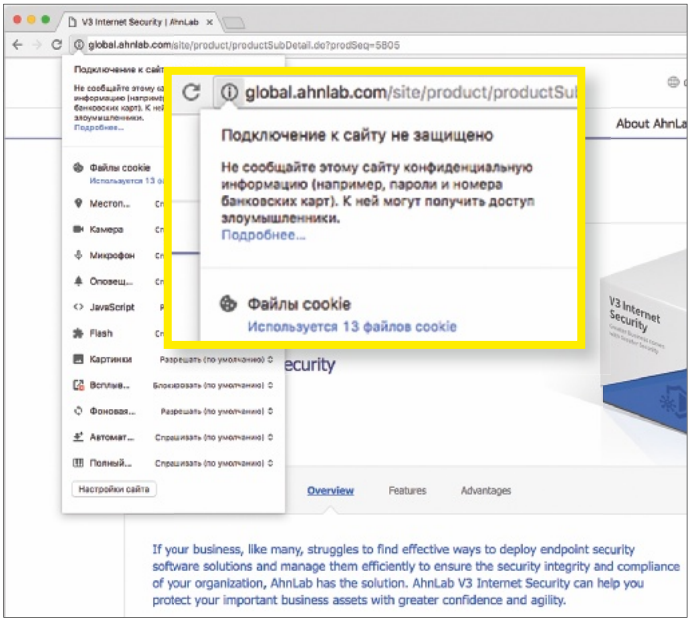
Лишь некоторые производители антивирусов защищают свои программы

Подробный анализ компании AV-Test показывает, что далеко не все производители используют сертификаты или защитные механизмы. Но по сравнению с предыдущими годами можно заметить улучшения

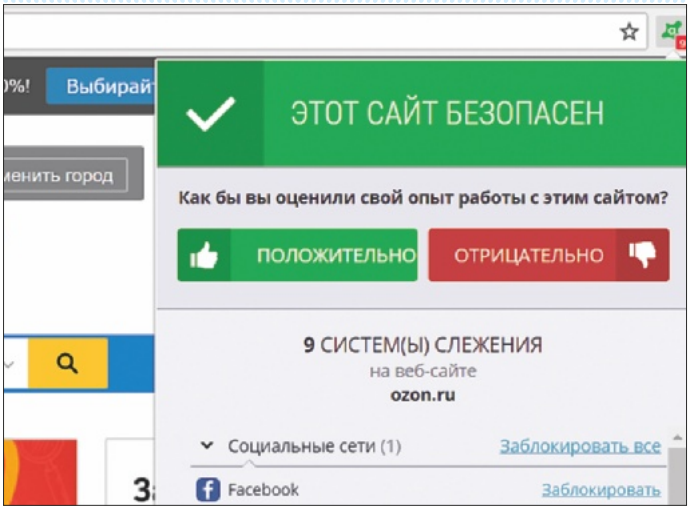
Название программы	Исполняемые программные файлы для 32-битной системы (подписанные/неподписанные/недействительный сертификат)	Исполняемые программные файлы для 64-битной системы (подписанные/неподписанные/недействительный сертификат)	Безопасная загрузка через HTTPS	Средний показатель применения защитных механизмов в процентах (ASLR и DEP)		
				2017	2015	2014
Avira Antivirus Pro 15	168/0/1	5/0/0	●	100	100	99,7
Bitdefender Internet Security 17	88/0/0	246/0/0	●	100	87,9	89,2
ESET Internet Security 10	2/0/0	81/0/0	●	100	100	100
Kaspersky Internet Security 17.0	244/0/0	14/0/0	●	100	100	96,4
G Data Internet Security 25.3	84/0/0	42/0/0	●	98,8	99,4	97,7
F-Secure SAFE 14.1	265/1/0	29/0/0	●	100	99,5	93
MicroWorld eScan IS Suite 14	139/2/0	25/0/0	○	100	91,1	17,5
Symantec Norton Security 22.8	194/0/0	20/0/0	○	100	100	99,3
Trend Micro Internet Security 11.0	32/0/0	245/6/0	○	100	76	71,8
BullGuard Internet Security 17	19/1/0	69/1/0	○	99,6	100	93,1
AVG Internet Security 17.1	157/3/0	39/1/1	○	97,2	95,9	95
Comodo Internet Security Pr. 10	11/0/0	52/0/0	○	92,2	53	56,5
Emsisoft Anti-Malware 12.1	5/0/0	28/0/0	○	92	н. д.	н. д.
avast! Free AntiVirus 17.1	132/6/0	14/1/1	○	90,1	96,9	98
McAfee Internet Security 19.0	49/0/0	324/0/0	○	88,5	100	96,7
ThreatTrack VIPRE IS Pro 2016	118/12/0	13/1/0	○	85,3	43,3	38,3
Quick Heal Total Security 15.1	33/11/0	208/29/0	○	76,4	28,9	37,3
K7 Computing Total Security 15.1	89/6/0	3/0/0	○	58,5	25,9	н. д.
AhnLab V3 Internet Security 9.0	19/2/0	90/1/0	○	36,3	34,5	24,6

По состоянию на апрель 2017 г.
ИСТОЧНИК: AV-Test

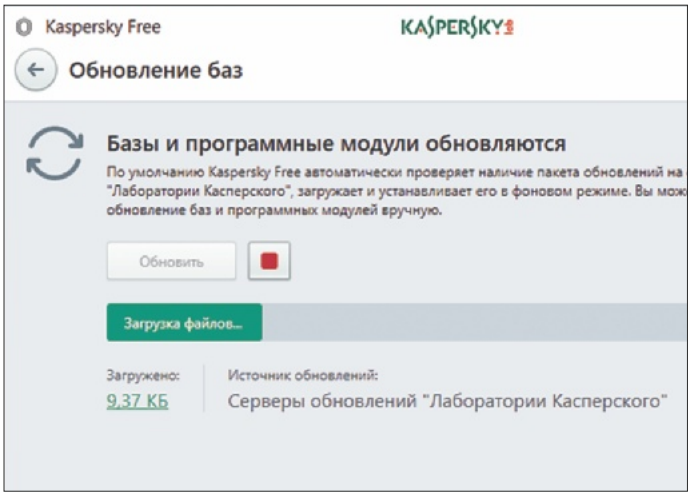
надежно потенциально ненадежно опасно
●Да ○Нет



Загрузка антивирусного ПО у некоторых производителей работает через небезопасные, доступные для манипуляций HTTP-соединения

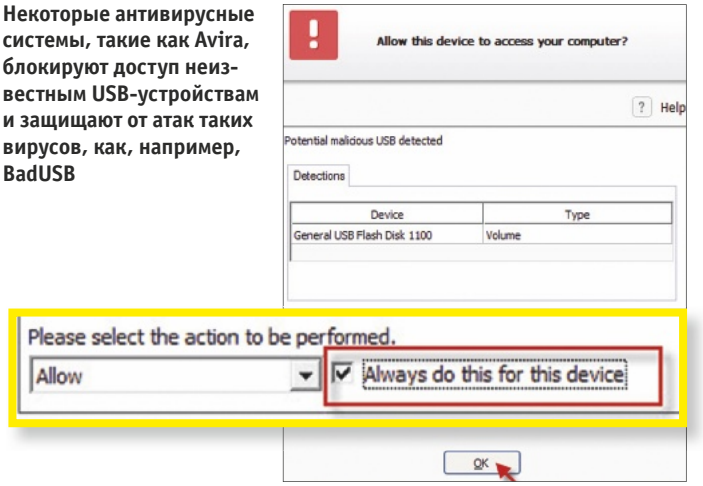


Плагины антивирусных программ для браузеров предупреждают об опасных сайтах, но в некоторых случаях сами являются ненадежными



Установленные антивирусные программы должны каждые 12 часов искать обновления программ и определений

Некоторые антивирусные системы, такие как Avira, блокируют доступ неизвестным USB-устройствам и защищают от атак таких вирусов, как, например, BadUSB



памяти по случайному принципу. Впервые ASLR была использована в Windows Vista. Среди мобильных систем первой стала iOS 4.3, потом последовала версия Android 4.0. Но и ASLR не дает стопроцентной гарантии безопасности. С помощью различных приемов хакеры обходят случайное распределение.

Например, через так называемый «спреинг» вредоносная программа распространяется по всему накопителю. Таким образом хакеры провоцируют переполнение памяти, благодаря которому они затем могут производить свои манипуляции. Чтобы это не заходило настолько далеко, производители антивирусов стараются, чтобы на компьютере допускалось использование только сертифицированного программного обеспечения.

Оптимизировать антивирусные программы

Специально для дополнений браузера и настроек обновления вам потребуются дополнительные настройки, поскольку не все функции антивирусного инструмента всегда полезны для безопасности собственной системы. Иногда даже бывает лучше полностью отключить ту или иную опцию.

Установить оптимальное время для обновления

Эффективность защиты антивирусных программ зависит от своевременного обновления. Исследователи вопросов безопасности исходят из того, что ставшие известными пробелы активно используются в течение нескольких часов. Но многие антивирусные программы запускают автоматическое обновление только раз в сутки, а то и реже. Лучше установить периодичность обновления на 12 часов. Это подходит большинству пользователей. Если вы часто заходите на неизвестные сайты или устанавливаете в системе программы, то этот интервал следует сократить до двух часов.

Панель инструментов браузера

Большинство производителей антивирусов устанавливают дополнение для браузера, которое контролирует процесс поиска и открываемые сайты. Загвоздка в том, что некоторые из дополнений веб-обозревателя сами по себе ненадежны. Специалисты по безопасности Google выяснили, что, к примеру, дополнение AVG активирует специальные JavaScript-API, которые обычно считаются небезопасными. Между тем у AVG уже есть патчи для приложения.

Помимо соображений безопасности в случае с некоторыми дополнениями для пользователей еще остро стоит вопрос надоедливой рекламы — как, к примеру, у Avast. Казалось бы, вполне благое намерение: так Avast с помощью функции SafePrice хочет показывать пользователю наиболее выгодные онлайн-цены на продукты, которые пользователь видит прямо в своем браузере. А вот что скрывается за этой заботой о пользователе: на каждом клике фирма зарабатывает деньги.

Чтобы предупредить об опасных сайтах, инструменты в фоновом режиме проверяют весь сетевой трафик браузера. Чтобы программы могли проверять на вирусы трафик зашифрованных сайтов, инструменты действуют как прокси, что похоже на атаки посредника. Правда, и здесь, в случае с SSL-прокси, специалисты по безопасности нашли слабые места. Среди них, к примеру, известный исследователь Тавис Орманди. Он считает подход производителей антивирусов фатальным, поскольку использование прокси открывает хакерам дополнительные возможности для атак. А об опасных сайтах предупреждают и сами браузеры — панели инструментов антивирусных программ никакой дополнительной защиты не несут.

Включить защиту USB

Вирусная защита, например, от Avira, помогает при атаках, исходящих от USB-устройств. Для этого инструменты блокируют доступ к внешним носителям. Вредоносные программы, такие как BadUSB, в этом случае не имеют никаких шансов. В случае с BadUSB обычные USB-флеш-накопители выполняют роль скрытой клавиатуры, с которой незаметно вводится программный код.

Такую защиту USB можно целенаправленно активировать во многих антивирусных инструментах. Если ваш антивирус не поддерживает такую функцию, в качестве альтернативы вы можете использовать MyUSBOnly (**myusbonly.com**, стоимость около $29,9/1750 рублей).

Профессиональная защита для ПК

При всем разнообразии антивирусных программ вы можете еще больше усилить защиту ваших устройств, используя для этого простые средства. Мы покажем вам, какие инструменты при этом понадобятся и какие настройки нужно будет выполнить.

Независимая проверка заражения

Если вы заходите на неизвестный сайт, о котором вы ничего не знаете, используйте онлайн-сервис **virustotal.com**. После ввода подлежащего проверке URL сервис проверяет веб-ресурс и отображает подробный отчет.

Дополнительно на портале предоставляется возможность проверки файлов. Если, например, антивирусная система предупреждает о заражении файла на вашем жестком диске, вы загружаете файл на virustotal, и там он проверяется несколькими антивирусными инструментами известных производителей. Это позволяет с достаточной достоверностью проверить ложные тревоги со стороны вашей антивирусной защиты.

Перехитрить вымогателей

От такой напасти, как трояны-шифровальщики, лучше всего помогает резервное копирование, но есть несложный прием, позволяющий перехитрить такую вредоносную программу. Новые вирусы-вымогатели шифруют не весь жесткий диск, так как антивирусные инструменты выявляют и блокируют такой доступ. Вместо этого вирусы целенаправленно ищут документы и изображения на диске и шифруют именно их. Это можно предотвратить, если хранить такие файлы в зашифрованной папке. В нее вредоносная программа забраться не сможет. Для этого вам нужно использовать инструмент VeraCrypt и создать зашифрованное хранилище для ваших документов.

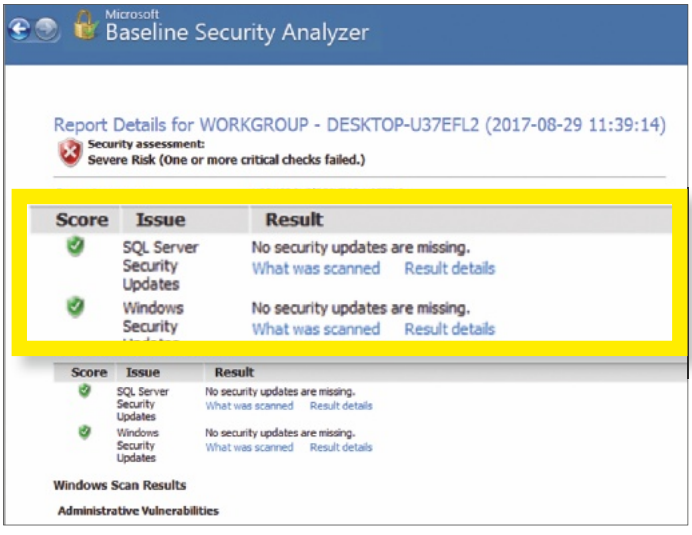
Проверка безопасности

Microsoft со своим анализатором Baseline Security Analyzer предлагает программу, которая целенаправленно ищет слабые места на ПК. Для этого данная утилита проверяет установку всех необходимых патчей и правильность конфигурации критически важных настроек в системе, например, брандмауэр и надежный пароль. Рядом с каждым предупреждением вы найдете ссылку «Действия по устранению», где будет разъяснено, как решить выявленные проблемы.

Защитить мобильные устройства

В мобильных системах также следует использовать комбинацию из антивируса и дополнительного программного обеспечения. В случае с Android это будет еще проще, так как антивирусный сканер, как и у Windows, проверяет всю систему. А вот пользователям iOS, наоборот, придется задействовать специальные инструменты.

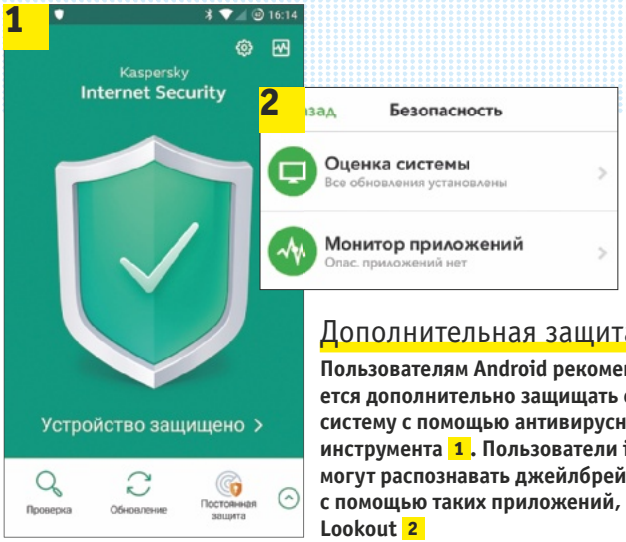
От таких хакерских атак, как вирусы-вымогатели и им подобные, некоторые файлы лучше защищать шифрованием с помощью VeraCrypt



Baseline Security Analyzer компании Microsoft проверяет важные обновления в системе и критические настройки безопасности

Установка системных обновлений

Устанавливая актуальные обновления операционной системы, вы предотвращаете большинство атак на ваш смартфон или планшет. Чтобы запустить обновления у iOS, зайдите в «Настройки | Общие | Обновление программного обеспечения». Обновление лучше всего выполнять только через эту функцию операционной системы. Если вы производите загрузку через программу зараженного компьютера, то может происходить внешнее вмешательство в файлы микропрограммного обеспечения. При обновлении внутри iOS загрузка →

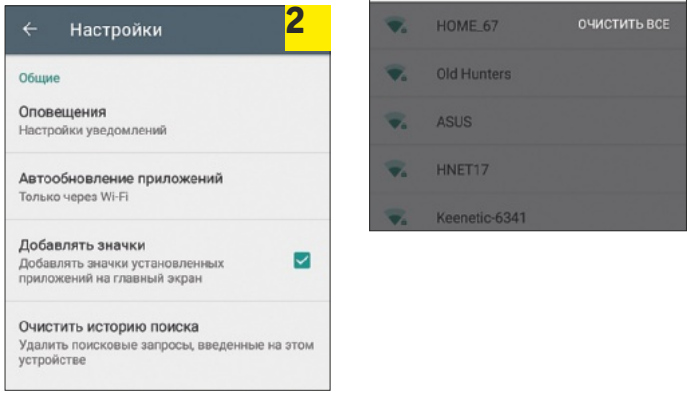


Дополнительная защита

Пользователям Android рекомендуется дополнительно защищать свою систему с помощью антивирусного инструмента 1. Пользователи iOS могут распознавать джейлбрейки с помощью таких приложений, как Lookout 2

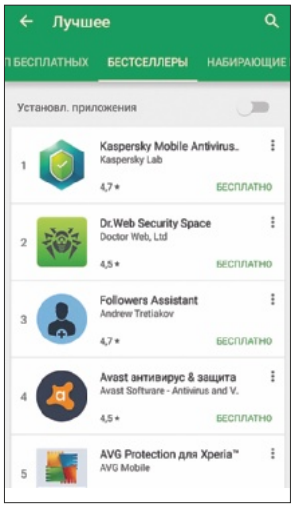
Важные обновления

В Android нужно активировать автоматические обновления 1. После этого система будет показывать необходимые патчи в собственном раскрывающемся меню 2



Вы можете использовать эти мобильные антивирусы

После тщательной проверки CHIP совместно с AV-Test рекомендует следующие антивирусы для Android



Антивирусы можно найти в Google Play Market в разделе «Инструменты | Лучшее | Бестселлеры»

осуществляется с шифрованием и с подписью. Чтобы проверить, присутствует ли в мобильной системе вредоносное ПО, используйте приложение безопасности Lookout. Оно проверяет наличие нежелательных джейлбрейков или вредоносных утилит на устройстве. Приложение можно найти в App Store.

Уровень безопасности устройств с Android несколько ниже. В частности, бюджетные модели производителей-новичков не получают обновлений микропрограммного обеспечения. Новейшая версия Android Nougat (версия 7), по данным Google, установлена на 11,5% всех устройств с Android. Почти половина работает еще с Lollipop или Kitkat — двумя уязвимыми версиями операционной системы. Чтобы проверить доступность новых версий операционной системы, откройте на своем гаджете «Настройки» и зайдите в раздел «О телефоне». Здесь выберите «Обновления ПО».

Установленные приложения также требуют поддержания в актуальном состоянии. Для этого в системе Android есть автоматический механизм, который нужно активировать в ручном режиме. Откройте приложение Play Market и нажмите на три полоски в левом верхнем углу. Затем выберите «Настройки» и в разделе «Автообновление приложений» активируйте опцию «Только через Wi-Fi». О предстоящих обновлениях система информирует в раскрывающемся меню, которое появляется, если потянуть верхний край экрана.

Установить инструменты защиты

Благодаря жесткой архитектуре iOS вам не придется использовать никаких дополнительных антивирусных программ — достаточно приложения Lookout. Программы не проверяют систему. По-иному обстоит дело у Android. Здесь вам в любом случае придется воспользоваться дополнительным ПО для обеспечения безопасности, особенно если вы используете старую версию операционной системы. Такие инструменты представлены на картинке в нижнем левом углу.

Установка антивирусной программы обеспечит хорошую защиту. От фишинговых атак вы сможете защититься с помощью дополнительной утилиты Financial Security от McAfee. Она в фоновом режиме проверяет известные приложения для банкинга и браузер на предмет правильных контрольных сумм. Таким образом почти полностью исключаются манипуляции с приложениями. Кроме этого, инструмент проверяет интернет-соединение относительно подозрительного отвода трафика. Если, к примеру, на устройстве установлена вредоносная программа, выведывающая данные, приложение McAfee это обнаружит и сразу заблокирует доступ.

Использование специального браузера

Антивирусные программы и антифишинговые приложения защищают от большинства опасностей. Но чтобы получить в руки оружие превентивного действия, вам понадобится специальная защита для пользования мобильным Интернетом. Лучше всего подойдет Cliqz Browser из Google Play Market. С одной стороны, браузер будет запрещать сбор данных посредством трекинга, а с другой — препятствовать доступу к паролям и данным учетных записей пользователя.

Если вы будете пользоваться информацией и приложениями так, как описано в этой статье, большая часть вирусов не будет представлять угрозы вашим устройствам, даже если у вашей антивирусной защиты будет пара слабых мест. Тем не менее ни в коем случае не стоит забывать о поддержании актуального состояния программ, иначе не помогут даже самые изощренные технологии.