Публикация № 091117/c/1

Безопасная работа в Интернете

Какие программы следует использовать для защиты компьютера?

При работе в Интернете пользователь и его компьютер (или иное устройство, используемое для выхода в Сеть, например мобильный телефон) подвергаются различным опасностям, связанным с загрузкой вредоносных и нежелательных программ или информации. Загрузка таких программ или информации может происходить незаметно для пользователя и без каких-либо осознанных действий с его стороны.

В настоящем обзоре классифицируются программы, предназначенные для защиты пользователя и его компьютера от различного рода вредоносных программ и нежелательной информации при работе в Интернете.

Программы для защиты компьютера при работе в Интернете

1. Межсетевой экран

Межсетевой экран (firewall) или брандмауэр предназначен для защиты компьютера от несанкционированного доступа к нему из локальной сети или Интернета. Он также позволяет подключаться к сети только тем программам, установленным на компьютере пользователя, которым это разрешено.

В первую очередь межсетевой экран помогает предотвратить попадание в компьютер вредоносных программ, заблокировать вредоносным программам, попавшим в компьютер иными путями, доступ в Интернет (для передачи похищенной информации, самообновления и т.д.) и предотвратить несанкционированный доступ к информации, находящейся в памяти компьютера.

2. Антивирус

Антивирус (antivirus) предназначен для обнаружения, предотвращения выполнения и удаления вредоносных программ (компьютерных вирусов), а также «лечения» программ и файлов пользователя, зараженных компьютерными вирусами. Некоторые антивирусы умеют также противодействовать более широкому спектру вредоносных программ, которые не относятся к компьютерным вирусам, например программам для показа рекламы, кражи персональных данных и т.п. Антивирус помогает в борьбе с компьютерными вирусами не только при работе в Интернете.

В первую очередь антивирус помогает предотвратить порчу или кражу информации, размещенной в памяти компьютера.

3. Программа для борьбы со шпионскими и рекламными программами

Программа для борьбы со шпионскими (spyware) и рекламными (adware) программами предназначена для обнаружения, предотвращения выполнения и удаления соответствующих программ, а также «лечения» программ и файлов пользователя, зараженных ими. Часто аналогичными функциями обладают и антивирусы.

В первую очередь программа для борьбы со шпионскими и рекламными программами помогает предотвратить кражу информации, размещенной в памяти компьютера, и демонстрацию пользователю нежелательной рекламы.

4. Программа для блокирования рекламы

Программа для блокирования рекламы (ad blocker) служит для удаления баннеров и иных видов рекламы с просматриваемых пользователем веб-страниц. Часто такие программы могут использоваться для удаления из просматриваемых страниц различных элементов, представляющих потенциальную угрозу для пользователей и их приватности, например счетчиков посещений веб-страниц.

В первую очередь программа для блокирования рекламы предназначена для очистки просматриваемых страниц от «информационного мусора», затрудняющего доступ к интересующей пользователя информации, угрожающего безопасности его компьютера и конфиденциальности пользователя.

5. Контентный фильтр

Контентный фильтр (content-control software, web filtering software, content filter) предназначен для ограничения доступа к размещенной в Интернете информации по различным критериям, например – содержащей ненормативную лексику или порнографические изображения.

В первую очередь контентный фильтр предназначен для предотвращения доступа детей к неподходящей для них информации.

6. Системы комплексной защиты

Системы комплексной защиты сочетают в себе сразу несколько функций вышеописанных программ, например – межсетевого экрана и антивируса. Такие системы предназначены для предотвращения сразу нескольких видов угроз, но не обязательно так же эффективны, как несколько отдельных программ, каждая из которых имеет лишь одну функцию.

Общие советы по безопасности при работе в Интернете

7. Не забывайте об обновлениях

Многие производители программ, включая операционную систему, выпускают для них обновления и исправления, предназначенные, в том числе, для повышения уровня безопасности при работе в Интернете. Обычно такие обновления можно бесплатно загрузить с веб-сайтов производителей программ. Многие программы содержат встроенные механизмы проверки наличия и установки обновлений. Регулярно проверяйте наличие обновлений и выполняйте их установку.

8. Установите для используемых программ приемлемый уровень безопасности

Некоторые программы имеют настройки по умолчанию, не обеспечивающие приемлемый уровень защиты. Таким образом производители программ «упрощают» пользователю процесс взаимодействия со своим продуктом.

Внимательно изучите настройки программ, которые имеют доступ в Интернет, и настройте их в соответствии со своими собственными предпочтениями и потребностями. Отключайте неиспользуемые функции таких программ, так как каждая из них представляет потенциальную угрозу безопасности. Большинство программ имеют справочную систему, в которой объясняется значение их настроек и функций.

9. Дорогое – не значит лучшее

Для программ, защищающих компьютер при работе в Интернете, действует то же правило, что и для любых других товаров: дорогое – не значит лучшее. Многие бесплатные и свободно распространяемые программы занимают первые места в рейтингах, составляемых профессионалами в области защиты компьютеров и информации.

10. Абсолютной защиты не бывает

Необходимо понимать, что единственная возможность гарантировать полную защиту компьютера и размещенной в его памяти информации от угроз, подстерегающих в Интернете, – вообще не подключать компьютер к сети. В противном случае, даже если вы будете принимать все мыслимые меры предосторожности, существует некоторая вероятность, что они не помогут. Особенно, если целью злоумышленников будет не любой компьютер вообще, а именно ваш компьютер и размещенная в его памяти информация.

Поэтому соблюдайте следующие организационные меры безопасности, обеспечивающие как защиту информации от кражи, так и ее «избыточность»:

- четко определите, какая часть имеющейся у вас информации ни в коем случае не должна попасть в чужие руки, а какая ни в коем случае не должна быть утеряна или повреждена;
- не храните на подключенном к сети компьютере информацию, кража которой может привести к серьезному ущербу, либо надежно шифруйте её;
- при шифровании информации не расшифровывайте её, если компьютер подключен к сети, и вы не убедились, что на нем отсутствуют вредоносные программы;
- регулярно архивируйте ценную для вас информацию на внешние носители, которые не допускают ее перезаписи (например, компакт-диски), компьютеры, не имеющие подключения к сети и т.п.;
- имейте под рукой заведомо чистые загрузочные диски, с помощью которых можно произвести поиск на компьютере вредоносных программ и переустановить безнадежно поврежденную такими программами операционную систему.