УДК 004.056

Защита WindowsTM от вирусов в сети интернет

Лосев А.А., 11-ИБ

Мы живем в век развитых информационных технологий. Сейчас уже невозможно представить свою жизнь без всезнающего интернета. И наверно каждый встречался хоть раз с такой плохой программой как «компьютерный вирус». Дело в том, что большинство (если не все) вирусов и червей просачивающихся к нам на компьютер из интернета. Но отказываться от использования интернета никто не станет, ведь он плотно связан с нашей жизнью. Значит нужно защищаться. Для защиты от нападения из вне существует множество программ и средств. Если на машине есть антивирусный сканер, он может остановить действие вредоносного кода в системе, однако далеко не всегда способен предотвратить утечку конфиденциальной информации. Чтобы избежать проникновения в ОС различных вирусов и защитить ее от хакерских атак, подобный пакет безопасности должен работать в паре с программой, обеспечивающей контроль входящего и исходящего трафика. Данную задачу весьма успешно решают межсетевые экраны, которые также называют брандмауэрами. Межсетевой экран также применим для ограничения возможностей определенных пользователей компьютера по обращению к Всемирной паутине. Например, с его помощью можно блокировать подключения интернет-пейджеров, разрешать или запрещать работу почтовых клиентов, браузеров и других программ, требующих соединения с Глобальной сетью. Все это особенно актуально для фирм и учреждений, где поддерживается строгая дисциплина, а системные администраторы бдительно следят за тем, чтобы Интернет использовался только в служебных целях.

Необходимость в защитном сетевом инструменте очевидна, и в самой операционной системе от Microsoft он появился уже давно. Данный

компонент вполне неплохо справляется со своими функциями, легко настраивается и содержит много предустановленных правил.

Чтобы перейти к подробным настройкам функций блокировки приложений, необходимо открыть «Панель управления | Все элементы Панели управления» и там выбрать и запустить «Брандмауэр Windows». Кликнуть по ссылке «Разрешить запуск программы или компонента через брандмауэр Windows». После этого на экране появится список установленных приложений, в котором флажками отмечены разрешенные. Непосредственно в этом списке можно запрещать или разрешать утилитам задействовать различные сетевые профили.

Стандартный брандмауэр Windows использует несколько профилей, в зависимости от типа установленного соединения. Обычно при обнаружении нового типа сети программа запрашивает пользователя, какой профиль следует выбрать и какие настройки для него установить. Например, тип «Общественный» нужно указывать для публичных сетей — скажем, в аэропорту или кафе, а тип «Домашний» можно выбирать для домашних или рабочих сетей.

При желании можно выполнить более тонкое конфигурирование брандмауэра Windows, но для этого необходимо переключить его в режим повышенной безопасности. Чтобы открыть нужное окно, просто нужно набрать слово «брандмауэр» в меню «Пуск». В окне с настройками режима повышенной безопасности можно описывать любые ситуации и всевозможные условия, при которых межсетевой экран будет блокировать или пропускать передаваемые данные. Это могут быть правила для отдельных приложений, портов, а также управляющие подключениями для операций Windows.

Встроенный в ОС от Microsoft брандмауэр обладает лишь базовыми функциями, и его защитных характеристик хватит лишь на безобидный серфинг в Интернете с посещением надежных сайтов. Для более высокого

уровня защиты лучше использовать сторонние приложения — например, от известных производителей антивирусного ПО.

Операционная система Windows настолько универсальна, что даже такую простую задачу, как блокировка доступа к серверу, умеет решать несколькими способами. Самый простой метод — с помощью файла hosts. Достаточно открыть его содержимое в Блокноте или другом текстовом редакторе и добавить туда строку вида «127.0.0.1 www.youtube.com». Данная команда позволит блокировать посещение популярного сервиса YouTube. Однако этот метод годится далеко не всегда, поскольку часто заранее невозможно предугадать, какой процесс будет устанавливать подключение, с каким узлом и каким образом. Кроме того, может возникнуть необходимость в избирательном ограничении доступа в зависимости от конкретного процесса.

Антивирусы можно разделить на несколько категорий по технологиям защиты:

1. Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования)
2. Продукты проактивной антивирусной защиты (продукты, применяющие только проактивные технологии антивирусной защиты)
3. Комбинированные продукты (продукты, применяющие как классические, сигнатурные методы защиты, так и проактивные)

Рассмотрим подробнее каждый пункт:

1. Обнаружение, основанное на сигнатурах — метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий:

- Удалить инфицированный файл.

- Отправить файл в «карантин» (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).
- Попытаться восстановить файл, удалив сам вирус из тела файла.

Для достижения достаточно продолжительного успеха, при использовании этого метода необходимо периодически пополнять словарь известных вирусов новыми определениями (в основном в онлайновом режиме)

2. Проактивные технологии – совокупность технологий и методов, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе.

3. Комбинированные продукты сочетают в себе первые два способа защиты, поэтому являются более предпочтительными для выбора.

Подведем итог. Некоторые пользователи порой сами открывают путь злоумышленникам, присваивая сомнительным приложениям статус доверенных программ. Инсталлируя загруженную из Сети игру или скринсейвер, нелегальное ПО и т. д., пользователь может запустить в систему «троянского коня», который откроет злоумышленнику конфиденциальные данные и предоставит возможность дистанционного управления. Нужно быть внимательным с устанавливаемыми программами, использовать антивирус и межсетевой экран.

Список литературы:

1. Антивирусная программа - Википедия [Электронный ресурс]: (с изм. и доп.) – Режим доступа: https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0; (дата обращения 26.11.2012)

2. Обнаружение, основанное на сигнатурах – Википедия [Электронный ресурс]: (с изм. и доп.) – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BD%D0%B0%D1%80%D1%83%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5,_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BD%D0%B0_%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D1%82%D1%83%D1%80%D0%B0%D1%85; (дата обращения 26.11.2012)
3. Проактивная защита – Википедия [Электронный ресурс]: (с изм. и доп.) – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B0; (дата обращения 26.11.2012)
4. Азбука сетевой безопасности – CHIP [Электронный ресурс]: (с изм. и доп.) – Режим доступа: http://www.chip.ua/stati/internet-i-seti/2012/04/azbuka-setevoi-bezopasnosti?b_start:int=0; (дата обращения 26.11.2012)