МЕТОДЫ ОБНАРУЖЕНИЯ И УДАЛЕНИЯ ВИРУСОВ. АНТИВИРУСНЫЕ ПРОГРАММЫ И КОМПЛЕКСЫ

Гончерёнок Е.Д.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

На сегодняшний день проблема обнаружениякомпьютерных вирусов достаточно актуальна. В связи с этим было создано достаточное количество методов и способов для упрощения данного поиска. Таким образом, предлагается рассмотреть некоторые из них:

1. *Сканирование.*

Сканирование является самым простым методом поиска вирусов. Он основан на последовательном просмотре памяти компьютера, загрузочных секторов и проверяемых файлов в поиске сигнатур известных вирусов. Для этого необходимо тщательно изучить принцип работы вируса и сравнить программы, заражённые данным вирусом, и незаражённые программы. Сигнатура вируса – это уникальная последовательность байтов, принадлежащая вирусу и не встречающаяся в других программах.

2. *Контроль целостности.*

Контроль целостности основан на выполнении процедуры постановки на учёт и процедуры контроля поставленного на учёт.При внедрении вируса в компьютерную систему происходят изменения в системе. Например, изменение объёма доступной оперативной памяти, изменение загрузочных секторов дисков, изменения самих файлов. Для ведения контроля достаточно запомнить характеристики, которые подвергаются изменениям в результате внедрения вируса, а после периодически сравнивать эти характеристики с действующими программами.

3. *Метод резидентного сторожа*.

Метод резидентного сторожа направлен на выявление «подозрительных» действий пользовательских программ.К таким действиям можно отнести запись на диск по абсолютному адресу, форматирование диска, изменение загрузочного сектора, изменение или переименование выполняемых программи др. При обнаружении «подозрительного» действия защитная программа присылает уведомление пользователюдля получения его согласия или отказа на выполнение такого действия.

4. *Вакцинирование программ*.

Метод вакцинирования программ заключается в дописывании к исполняемому файлу дополнительной подпрограммы, которая первой получает управление при запуске файла и выполняет проверку целостности программы.

К способам противодействия компьютерным вирусам относят профилактику заражения компьютера, восстановление поражённых объектов и антивирусные программы.

Для обнаружения и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать компьютерные вирусы. Такие программы называются*антивирусными*.Практически все антивирусные программы обеспечивают автоматическое восстановление заражённых программ и загрузочных секторов.

Различают следующие виды антивирусных программ:

1. *Программы-фаги* (*сканеры*).

Программы-фаги осуществляют поиск характерной для конкретного вируса сигнатуры путём сканирования оперативной памяти и файлов и выдают соответствующее сообщение при обнаружении. Данные антивирусы не только находят заражённые вирусами файлы, но и удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. Программы-фаги являются универсальными, однако имеют небольшую скорость поиска вирусов и относительно большие размеры антивирусных баз.Наиболееизвестныепрограммы-фаги: Aidstest, Scan, NortonAntivirus, DoctorWeb.

2. *Программы-ревизоры* (*CRC-сканеры*).

Принцип работы CRC-сканеров основан на подсчёте CRC-сумм (кодов циклического контроля) для присутствующих на диске файлов. Затем CRC-суммы сохраняются в базе данных антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменён или заражён вирусом. К числу CRC-сканеров относится широко распространённая в России программа ADinf (AdvancedDiskinfoscope) и ревизор AVP Inspector. Вместе с ADinf применяется лечащий модуль ADinfCureModule (ADinfExt).

3. *Программы-блокировщики*.

Программы-блокировщики являются резидентными программами, перехватывающиеситуации, предполагающие наличие вируса, и сообщающие об этом пользователю. Данные программы имеют способность обнаружения и остановки вируса на самой ранней стадии его размножения. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применять другие программы, например фаги.

Наиболее распространённым блокировщиком является встроенная в BIOS защита от записи в MBR винчестера.

4. *Программы-иммунизаторы*.

Программы-иммунизаторы – это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.*Иммунизаторы, сообщающие о заражении*, обычно записываются в конец файла и при запуске этого файла каждый раз проверяют его на изменение. *Иммунизаторы, блокирующие заражение каким-либо типом вируса*, защищают систему от поражения вирусом определённого типа, модифицируя программу или диск таким образом, чтобы это не отражалось на их работе, а вирус при этом воспринимает их заражёнными и поэтому не внедряется.

Существует спектр программных комплексов, предназначенных для профилактики заражения вирусом, обнаружения и уничтожения вирусов. К наиболее распространённым антивирусным программным комплексам относятся:

- антивирус Касперского (AVP) Personal;
- антивирус Dr.Web;
- антивирус SymantecAntivirus;
- антивирус McAfee;
- антивирус AntiVirPersonalEdition.

Наиболее мощными антивирусными комплексами из линеек производителей антивирусов, входящие в класс InternetSecurity, на сегодняшний день являются:

- PandaInternetSecurity 2012;
- Dr.Web 7.0 SecuritySpace;
- ComodoInternetSecurityPro 2012;
- KasperskyInternetSecurity 2012;
- EmsisoftInternetSecurity Pack;
- Eset NOD32;
- Avast 7 InternetSecurity;
- Avast 7 FreeAntivirus;
- AviraInternetSecurity 2012;
- AviraFreeAntivirus.

У каждого типа антивирусных программ есть свои достоинства и недостатки. Однако комплексное использование нескольких типов антивирусных программ может привести к желаемому результату.