Секция «Таможенное дело»

Методы обнаружения и удаления вирусов. Антивирусные программы и комплексы

Белявская М.А., Юрчук П.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

Для современных пользователей всевозможных электронных вычислительных устройств обнаружение компьютерных вирусов является очень актуальной проблемой. Поэтому существует достаточное количество методов и способов для упрощения данного поиска. Рассмотрим некоторые из них:

- Сканирование.

Сканирование является самым оптимальным и простым в использовании методом поиска вирусов, который основан на последовательном просмотре памяти компьютера, загрузочных секторов и проверяемых файлов в поиске сигнатур известных вирусов. Данный способ работает следующим образом: тщательное изучение принципа работы вируса; сравнение программы, заражённой данным вирусом, и незаражённойпрограммы. Сигнатура вируса – это последовательность байтов данных, характерных для вируса или вредоносной программы.

- Контроль целостности.

Контроль целостности – это способ, основанный на выполнении процедуры постановки на учёт и последующего контроля. При внедрении вируса в компьютерную систему происходят изменения в системе. Для ведения контроля достаточно запомнить характеристики, которые подвергаются изменениям в результате внедрения вируса, а послепериодически сравнивать эти характеристики с исходными значениями.

- Метод резидентного сторожа.

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

- Эвристический анализ.

Эвристический анализ – метод, который используется относительно недавно и предназначен для обнаружения новых неизвестных вирусов. Программы, которые реализуют этот метод, также проверяют загрузочныесекторы дисков и файлы, но в отличии от них уже пытаются обнаружить в них код, *характерный* для вирусов.

- Вакцинирование программ.

Метод вакцинирования программ состоит 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.

Также 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:

- 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, но они имеют невысокую скорость поиска вирусов и относительно большие размеры антивирусных баз. Наиболее известные программы-фаги: Aidstest, Scan, Norton Antivirus, Doctor Web.

- 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 программа ADinf и ревизор AVP Inspector. Вместе с ADinf применяется лечащий модуль ADinfCureModule (ADinfExt).

- Программы-блокировщики.

Программы-блокировщики являются резидентными программами, перехватывающие ситуации, 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.

- 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, 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 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 Symantec Antivirus; антивирус McAfee; антивирус AntiVirPersonalEdition.

Таким образом, у каждого типа антивирусных программ есть свои достоинства и недостатки. Поэтому комплексное использование нескольких типов антивирусных программ будет более надёжной защитой для компьютера.

Литература

1. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчёв, О.Г. Иванова. – Ст. Оскол: ТНТ, 2010. – 384 с.

2. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2012. – 432 с.

3. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. – М.: МГИУ, 2010. – 277 с.

4. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. – М.: Акад. Проект, 2008. – 544 с.

Электронная цифровая подпись и её применение

Галко В.А.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

В мире электронных документов подписание файла с помощью графических символов теряет смысл, так как подделать и скопировать графический символ можно бесконечное количество раз. Электронная цифровая подпись является полным электронным аналогом обычной подписи на бумаге, но реализуется не с помощью графических изображений, а с помощью математических преобразований над содержимым документа.

Электронная цифровая подпись (ЭЦП)– реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Особенности математического алгоритма создания и проверки ЭЦП гарантируют невозможность подделки такой подписи посторонними лицами, чем достигается неопровержимость авторства.

Схема электронной подписи обычно включает в себя:

– алгоритм генерации ключевых пар пользователя;
– функцию вычисления подписи;
– функцию проверки подписи.

Электронная цифровая подпись может иметь следующее назначение:

– Удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т.д.
– Защиту от изменений документа.
– Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.
– Предприятиям и коммерческим организациям сдачу финансовой отчётности в государственные учреждения в электронном виде.