**Практическая работа №6**

**Теоретические сведения**

**Антивирусные средства защиты информации**

В связи с тем, что информация является предметом собственности (государства, коллектива, отдельного лица), то неизбежно возникает проблема угрозы этой информации, заключающейся в неконтролируемом ее распространении, в хищении, несанкционированном уничтожении, искажении, передаче, копировании, блокировании доступа к информации. Следовательно, возникает проблема защиты информации от утечки и несанкционированных воздействий на информацию и ее носители, а также предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Массовое распространение вредоносного программного обеспечения, серьезность последствий его воздействия на информационные системы и сети вызвали необходимость разработки и использования специальных ***антивирусных средств*** и методов их применения.

Компьютерный вирус — вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов и даже удаление операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

Нужно отметить, что не существует антивирусных средств, гарантирующих обнаружение всех возможных программ-вирусов.

***Антивирусные средства применяются для решения следующих задач:***

* обнаружение вредоносного ПО в информационных системах;
* блокирование работы вредоносного ПО;
* устранение последствий воздействия вредоносного ПО.

**Классификация компьютерных вирусов**

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году).

Принято разделять вирусы:

* *по поражаемым объектам* (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
* *файловые вирусы* делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
* *по поражаемым операционным системам и платформам* (DOS, Windows, Unix, Linux, Android);
* *по технологиям, используемым вирусом* (полиморфные вирусы, стелс-вирусы, руткиты);
* *по языку, на котором написан вирус* (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
* *по дополнительной вредоносной функциональности* (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

**Классификация компьютерных вирусов**

По среде обитания:

*Сетевые* – распространяются по различным компьютерным сетям

*Файловые* – внедряются в исполняемые модули (COM, EXE)

*Загрузочные* – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска

*Фалово-загрузочные* – внедряются и в загрузочные сектора, и в исполняемые модули

По воздействию:

* *Неопасные* – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
* Опасные – приводят к различным нарушениям в работе компьютера
* Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

* *Паразиты* – изменяют содержимое файлов и секторов, легко обнаруживаются
* *Черви* – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
* *Стелсы* – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
* *Мутанты* – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
* *Трояны* – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

Признаки заражения:

* прекращение работы или неправильная работа ранее функционировавших программ
* медленная работа компьютера
* невозможность загрузки ОС
* исчезновение файлов и каталогов или искажение их содержимого
* изменение размеров файлов и их времени модификации
* уменьшение размера оперативной памяти
* непредусмотренные сообщения, изображения и звуковые сигналы
* частые сбои и зависания компьютера и др.

Обнаружение вредоносного ПО желательно осуществлять на стадии его внедрения в систему или, по крайней мере, до начала осуществления им деструктивных действий. При обнаружении такого программного обеспечения или его деятельности необходимо сразу же прекратить работу программы-вируса в целях минимизации ущерба от ее воздействия на систему.

Устранение последствий воздействия вирусов ведется в двух направлениях:

* удаление вирусов;
* восстановление (при необходимости) файлов, областей памяти.

**Важно!**

Процедуру удаления обнаруженного вредоносного кода из зараженной системы необходимо выполнять крайне аккуратно. Часто вирусы и троянские программы предпринимают специальные действия, чтобы скрыть факт своего присутствия в системе, или встраиваются в нее так глубоко, что задача его уничтожения становится достаточно нетривиальной.

Восстановление системы зависит от типа вируса, а также от времени его обнаружения по отношению к началу деструктивных действий. В том случае, когда программа-вирус уже запущена в системе и ее деятельность предусматривает изменение или удаление данных, восстановление информации (особенно, если она не продублирована) может быть невыполнимо. Для борьбы с вирусами используются программные и программно-аппаратные средства, которые применяются в определенной последовательности и комбинации, образуя методы защиты от вредоносного ПО.

Методы обнаружения вирусов

Известны следующие методы обнаружения вирусов, активно применяемые современными антивирусными средствами:

* сканирование;
* обнаружение изменений;
* эвристический анализ;
* использование резидентных сторожей;
* использование программно-аппаратной защиты от вирусов.

***Сканирование*** – один из самых простых методов обнаружения вирусов, осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса – ***сигнатуры***. Под сигнатурой понимается уникальная последовательность байтов, принадлежащая конкретному вирусу и не встречающаяся в других программах.

Программа фиксирует наличие уже известных вирусов, для которых сигнатура определена. Для эффективного применения антивирусных программ, использующих метод сканирования, необходимо регулярное обновление сведений о новых вирусах.

Метод ***обнаружения изменений*** базируется на использовании программ-ревизоров, которые следят за изменениями файлов и дисковых секторов на компьютере. Любой вирус каким-либо образом изменяет систему данных на диске. Например, может измениться загрузочный сектор, появиться новый исполняемый файл или измениться уже существующий, и т.п.

Как правило, антивирусные программы-ревизоры определяют и запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, характеристики всех контролируемых файлов, каталогов и номера дефектных кластеров диска. Периодически ревизор проверяет текущее состояние областей дисков и файловой системы, сравнивает с предыдущим состоянием и немедленно выдает сообщения обо всех подозрительных изменениях.

Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов.

Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными. Вирусы будут обнаружены только после размножения в системе.

***Эвристический анализ***, как и метод обнаружения изменений, позволяет определять неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе.

Эвристический анализ в антивирусных программах основан на сигнатурах и эвристическом алгоритме, призван улучшить способность программ-сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда код неизвестной программы совпадает с сигнатурой не полностью, но в подозрительной программе явно выражены более общие признаки вируса либо его поведенческая модель. При обнаружении подобных кодов, выдается сообщение о возможном заражении. После получения таких сообщений необходимо тщательно проверить предположительно зараженные файлы и загрузочные сектора всеми имеющимися антивирусными средствами.

Недостатком данного метода является большое количество ложных срабатываний антивирусных средств в тех случаях, когда в легальной программе присутствуют фрагменты кода, выполняющего действия и/или последовательности, свойственные некоторым вирусам.

Метод ***использования резидентных сторожей*** основан на применении программ, которые постоянно находятся в оперативной памяти устройства (компьютера) и отслеживают все действия, выполняемые остальными программами. В случае выполнения какой-либо программой подозрительных действий, свойственных вирусам (обращение для записи в загрузочные сектора, помещение в оперативную память резидентных модулей, попытки перехвата прерываний и т.п.), резидентный сторож выдает сообщение пользователю.

**Важно!**

Применение антивирусных программ с резидентным сторожем снижает вероятность запуска вирусов на компьютере, но следует учитывать, что постоянное использование ресурсов оперативной памяти под резидентные программы уменьшает объем памяти, доступной для других программ.

Механизмы защиты информации

Одним из условий безопасной работы в информационной системе является соблюдение пользователем ряда правил, которые проверены на практике и показали свою высокую эффективность. Их несколько:

1. Использование программных продуктов, полученных законным официальным путем. Вероятность наличия вируса в пиратской копии во много раз выше, чем в официально полученном программном обеспечении.
2. Дублирование информации. Прежде всего, необходимо сохранять дистрибутивные носители программного обеспечения. При этом запись на носители, допускающие выполнение этой операции, должна быть, по возможности, заблокирована. Следует особо позаботиться о сохранении рабочей информации. Предпочтительнее регулярно создавать копии рабочих файлов на съемных машинных носителях информации с защитой от записи. Копируется либо весь файл, либо только вносимые изменения. Последний вариант применим, например, при работе с базами данных.
3. Регулярное обновление системного ПО. Операционную систему необходимо регулярно обновлять и устанавливать все исправления безопасности от Microsoft и других производителей, чтобы устранить существующие уязвимости программного обеспечения.
4. Ограничение доступа пользователей к настройкам операционной системы и системным данным. Для обеспечения стабильной работы системы довольно часто требуется ограничивать возможности пользователей, что можно сделать либо с помощью встроенных средств Windows, либо с помощью специализированных программ, предназначенных для управления доступом к компьютеру.

В корпоративных сетях возможно применение групповых политик в сети домена Windows.

1. Для максимально эффективного использования сетевых ресурсов необходимо вводить ограничения доступа авторизованных пользователей к внутренним и внешним сетевым ресурсам и блокировать доступ неавторизованных пользователей.
2. Регулярное использование антивирусных средств. Перед началом работы целесообразно выполнять программы-сканеры и программы-ревизоры. Антивирусные базы должны регулярно обновляться. Кроме того, необходимо проводить антивирусный контроль сетевого трафика.
3. Защита от сетевых вторжений обеспечивается применением программно-аппаратных средств, в том числе: использованием межсетевых экранов, систем обнаружения/предотвращения вторжений IDS/IPS (Intrusion Detection/Prevention System), реализацией технологий VPN (Virtual Private Network).
4. Применение средств аутентификации и криптографии – использование паролей (простых/сложных/неповторяющихся) и методов шифрования. Не рекомендуется использовать один и тот же пароль на разных ресурсах и разглашать сведения о паролях. При написании пароля на сайтах следует быть особенно внимательным, чтобы не допустить ввода своего пароля на мошенническом сайте-двойнике.
5. Особую осторожность следует проявлять при использовании новых (не известных) съемных носителей информации и новых файлов. Новые съёмные носители обязательно должны быть проверены на отсутствие загрузочных и файловых вирусов, а полученные файлы – на наличие файловых вирусов. При работе в распределенных системах или в системах коллективного пользования новые сменные носители информации и вводимые в систему файлы целесообразно проверять на специально выделенных для этой цели компьютерах, не подключенных к локальной сети. Только после всесторонней антивирусной проверки дисков и файлов они могут передаваться пользователям системы.
6. При работе с полученными (например, посредством электронной почты) документами и таблицами целесообразно запретить выполнение макрокоманд средствами, встроенными в текстовые и табличные редакторы (MS Word, MS Excel), до завершения полной проверки этих файлов.
7. Если не предполагается осуществлять запись информации на внешние носители, то необходимо заблокировать выполнение этой операции, например, программно отключив USB-порты.
8. При работе с общими ресурсами в открытых сетях (например, Интернет) использовать только проверенные сетевые ресурсы, не имеющие вредоносного контента. Не следует доверять всей поступающей на компьютер информации – электронным письмам, ссылкам на Web-сайты, сообщениям на Интернет-пейджеры. Категорически не рекомендуется открывать файлы и ссылки, приходящие из неизвестного источника.

Постоянное следование приведенным рекомендациям позволяет значительно уменьшить вероятность заражения программными вирусами и защищает пользователя от безвозвратных потерь информации. Однако даже при скрупулезном выполнении всех правил профилактики возможность заражения ПК компьютерными вирусами полностью исключить нельзя, поэтому методы и средства противодействия вредоносному ПО необходимо постоянно совершенствовать и поддерживать в работоспособном состоянии.

**Практическое задание**

1. Выполненить 3 задания.

***Задание 1.*** Обновите через Интернет антивирусную программу, установленную на Вашем устройстве. Выполните полную проверку на вирусы. Дайте характеристику этой программе.

***Задание 2.*** Заполнить таблицу.

Описать 5 антивирусных программ различных разработчиков.

|  |  |  |
| --- | --- | --- |
| **Наименование антивирусной программы** | **Характеристики** | **Условия использования (платно/бесплатно)** |
| **…** | **…** | **…** |
| Kaspersky Security Cloud | * Своевременное информирование об утечках учетных данных и советы по защите * Уведомления в режиме реального времени при попытке получить доступ к вашей веб-камере или микрофону со стороны неизвестных приложений\* * Персонализированные уведомления и предупреждения прямо на ваших устройствах   \*Для Windows, Mac и Android   * Удобная облачная защита, которая не замедляет устройства * Проактивное устранение неполадок в работе жесткого диска благодаря отчетам о его состоянии * Управление хранилищем и уровнем заряда батареи с помощью специальных инструментов для устройств Android   **Системные требования**  Для всех устройств  Интернет-соединение для активации продукта, получения обновлений и доступа к некоторым функциям  Защита от слежки через веб-камеру работает только на компьютерах Windows и Mac и доступна для ряда совместимых веб-камер. Полный список совместимых устройств см. по адресу https://support.kaspersky.ru/14987 (для компьютеров Windows) или https://support.kaspersky.ru/15196 (для компьютеров Mac).  **Компьютеры и ноутбуки Windows®**  1500 Мб свободного места на жестком диске  Microsoft® Internet Explorer® 10 и выше  Microsoft .NET Framework 4 и выше  Microsoft Windows 101 Home / Pro / Enterprise2, 3  Microsoft Windows 8 & 8.1 / Pro / Enterprise2 / 8.1 с обновлением3  Microsoft Windows 7 Начальная / Домашняя базовая / Домашняя расширенная / Профессиональная / Максимальная – SP1 и выше3  Процессор 1ГГц и выше  Оперативная память (RAM): 1 Гб (32 бит) или 2 Гб (64 бит)  Планшеты Windows (на базе процессора Intel®)2  Microsoft Windows 101 Home / Pro / Enterprise3  Microsoft Windows 8 & 8.1 / Pro (64 бит3)  Минимальное разрешение экрана: 1024x768 | **платная** |
|  |  |  |
|  |  |  |
|  |  |  |

*Задание 3.*Заполнить таблицу «Сравнение антивирусных средств»

Сравнить 5 вышеописанных антивирусных программ по следующим критериям.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Критерии сравнения*** | ***Наименование антивирусного средства*** | ***Наименование антивирусного средства*** | ***Наименование антивирусного средства*** | ***Наименование антивирусного средства*** | ***Наименование антивирусного средства*** |
| ***Защита***  Блокирует вирусы, шифровальщики и другие угрозы |  |  |  |  |  |
| ***Скорость***  Обеспечивает мощную защиту без замедления системы |  |  |  |  |  |
| ***Удобство***  Легко установить, просто использовать |  |  |  |  |  |
| ***Конфиденциальность***  Блокирует шпионское ПО для отслеживания звонков, сообщений и данных о местонахождении и позволяет заблокировать, найти на карте и сбросить настройки потерянного устройства |  |  |  |  |  |
| ***Windows, Mac и мобильные устройства***  Защищает все устройства в любых комбинациях |  |  |  |  |  |
| ***Деньги*** Запускает безопасный браузер для защиты онлайн-транзакций на компьютерах Windows и Mac |  |  |  |  |  |
| ***Родительский контроль***  Блокирует нежелательный контент, обеспечивает поиск ребенка на карте и другие возможности защиты на всех устройствах |  |  |  |  |  |
| ***Диспетчер паролей***  Позволяет управлять, безопасно хранить и синхронизировать пароли на всех устройствах |  |  |  |  |  |
| ***Защита файлов***  Создает резервные копии ценных файлов, музыки и фотографий на компьютерах Windows |  |  |  |  |  |
| ***Частота обновления вирусной базы*** |  |  |  |  |  |
| ***Своевременное информирование об утечках учетных данных и советы по защите*** |  |  |  |  |  |
| ***Цена*** |  |  |  |  |  |