Лабораторная работа №8

Тема «Исследование защиты от компьютерных вирусов»

ВЫПОЛНИЛ

Олишкевич Игорь Русланович

Группа 25-ПО

Задание: изучить защиту от компьютерных вирусов; дать определение, привести классификацию.

Вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Виды антивирусов:

1. программы-детекторы, или сканеры, находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса;
2. программы-доктора, (фаги, программы-вакцины) находят зараженные файлы и "лечат" их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus;
3. программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера, затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей;
4. программы-мониторы (файерволы, брандмауэры) начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас";
5. программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа - небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.

Предотвращение попадания вирусов на компьютер. Используйте антивредоносную программу. Установите антивредоносную программу и поддерживайте ее в актуальном состоянии. Это позволит защитить ваш компьютер от вирусов и других вредоносных программ. Антивредоносные программы выполняют поиск вирусов, шпионского и другого вредоносного программного обеспечения, пытающегося проникнуть в вашу почту, операционную систему или файлы. Новые угрозы могут появляться ежедневно, поэтому необходимо регулярно проверять наличие обновлений на веб-сайте изготовителя антивредоносного приложения.

Защитник Windows — это бесплатная антивредоносная программа, входящая в состав Windows. Ее можно обновлять автоматически с помощью Центра обновления Windows. Кроме того, вы можете найти антивирусные программы, подходящие для Windows, в списке поставщиков программного обеспечения, предназначенных для защиты потребителей.

Не открывайте электронные письма, полученные от незнакомых отправителей или вложения, содержимое которых вам неизвестно. Многие вирусы передаются в виде вложений в электронные письма, и для их распространения достаточно открыть вложение. Настоятельно рекомендуем открывать только ожидаемые или известные вам вложения.

Используйте функцию блокирования всплывающих окон в браузере. Всплывающие окна — это небольшие окна в браузере, отображающиеся поверх просматриваемой вами веб-страницы. Несмотря на то, что большинство таких окон используется для рекламных целей, в них может содержаться вредоносный или небезопасный код. Блокирование всплывающих окон позволяет избавиться от некоторых или даже всех всплывающих окон. По умолчанию средство блокирования всплывающих окон в Windows Internet Explorer включено. Дополнительные сведения см. в статье [Изменение параметров безопасности и конфиденциальности для Internet Explorer](https://support.microsoft.com/ru-ru/help/17479).

Если вы используете Internet Explorer, убедитесь, что фильтр SmartScreen включен. Фильтр SmartScreen в Internet Explorer помогает защитить компьютер от фишинга и атак вредоносных программ, предупреждая вас о возможной небезопасности веб-сайта или расположения загрузки. Дополнительные сведения см. в статье [Фильтр SmartScreen: вопросы и ответы](https://support.microsoft.com/ru-ru/help/17443).

Обращайте внимание на уведомления Windows SmartScreen. С осторожностью запускайте неизвестные приложения, скачанные из Интернета. Такие приложения с большой вероятностью могут оказаться небезопасными. Когда вы загружаете и запускаете приложение из Интернета, SmartScreen использует сведения о его репутации, чтобы предупредить вас, если приложение малоизвестно и может быть вредоносным.

Регулярно обновляйте Windows. Корпорация Майкрософт регулярно выпускает особые обновления для системы безопасности, предназначенные для защиты компьютера. Обновления могут предотвратить атаки вирусов и других вредоносных программ, закрывая возможные слабые места в системе безопасности.

Сканирование. Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.

Антивирусные программы-сканеры способны найти только уже известные и изученные вирусы, для которых была определена сигнатура. Применение простых программ-сканеров не защищает Ваш компьютер от проникновения новых вирусов.

Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить сигнатуру. Поэтому простые антивирусные программы-сканеры не могут обнаружить полиморфные вирусы.

Антивирусные мониторы. Существует еще целый класс антивирусных программ, которые постоянно находятся в памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Такие программы носят название антивирусных мониторов или сторожей.

Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

Обнаружение изменений

Когда вирус заражает компьютер, он изменяет содержимое жесткого диска, например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. Таких изменений, однако, не делают «бестелесные» вирусы, обитающие не на диске, а в памяти процессов ОС.

Антивирусные программы, называемые ревизорами диска, не выполняют поиск вирусов по сигнатурам. Они запоминают предварительно характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверяют их (отсюда происходит название программы-ревизоры). Ревизор может найти изменения, сделанные известным или неизвестным вирусом.

В качестве примеров ревизоров диска можно привести программу Advanced Diskinfoscope (ADinf), разработанную в ЗАО «Диалог Наука» и ревизор AVP Inspector производства ЗАО «Лаборатория Касперского»

Вместе с ADinf применяется лечащий модуль ADinf Cure Module (ADinfExt), который использует собранную ранее информацию о файлах для восстановления их после поражения неизвестными вирусами. Ревизор AVP Inspector также имеет в своем составе лечащий модуль, способный удалять вирусы.

Защита, встроенная в BIOS компьютера

В системные платы компьютеров тоже встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение.