Антивирусные программы

Антивирусные программы Современные антивирусные программы представляют собой программные многофункциональные комплексы, в которые входят следующие модули: - программа монитор; - программа-сканер; - обновление антивирусных баз; - создание «аварийной» дискеты и др. Мониторы являются резидентными модулями, обычно они помещаются в оперативную память после загрузки операционной системы, находятся в памяти во время сеанса работы и отслеживают все действия пользователя и операции, выполняемые операционной системой, с дисками и памятью. При обнаружении подозрительного файла монитор выдает сообщение. К недостаткам можно отнести значительный объем занимаемой стандартной памяти, что может замедлять работу ПК. Сканеры запускаются в работу пользователем и позволяют выбрать область сканирования (диск, папку), и параметры сканирования. Обычно сканеры по окончании работы генерируют отчет, записываемый в текстовый файл. Все программы обнаруживают фиксированный набор известных вирусов, содержащийся в их вирусной базе (в настоящее время (2009 г.) около 1800 тыс. известных вирусов). Аппаратные средства Представляют собой интерфейсные платы, устанавливаемые в каждом отдельном ПК. Обеспечиваю защиту от вируса на аппаратном уровне, поэтому конкретный вид вируса в данном случае не важен. Недостатком является высокая стоимость и невозможность работы в компьютерных сетях. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ОБНАРУЖЕНИИ ВИРУСА 1) выключить компьютер, чтобы прекратить разрушающее действие вируса; 2) загрузить ОС с эталонной системной дискеты (защищенной от записи) или загрузочного диска; 3) просканировать компьютер на наличие вируса любой имеющейся в наличии программой. Избавиться от вирусов, если возможно; 4) если избавиться не удаётся, сделать резервную копию целых файлов и отформатировать диск. Последнее действие нежелательно; 7 ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ ПО КЛАССИФИКАЦИИ КАСПЕРСКОГО К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети. Сетевые черви К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью: • проникновения на удаленные компьютеры; • запуска своей копии на удаленном компьютере; • дальнейшего распространения на другие компьютеры в сети. Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д. Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRCсообщениях, файл в каталоге обмена P2P и т. д. Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код. Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений. Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса. Классические компьютерные вирусы К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью: • последующего запуска своего кода при каких-либо действиях пользователя; • дальнейшего внедрения в другие ресурсы компьютера. В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том 8 случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например: • при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе; • вирус скопировал себя на съёмный носитель или заразил файлы на нем; • пользователь отослал электронное письмо с зараженным вложением. Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске. Троянские программы В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях. Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети). Хакерские утилиты и прочие вредоносные программы К данной категории относятся: • утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы); • программные библиотеки, разработанные для создания вредоносного ПО; • хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов); • «злые шутки», затрудняющие работу с компьютером; • программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе; • прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.