УДК 004.4.056

АНТИВИРУСНЫЕ ПРОГРАММЫ И АНТИВИРУС KASPERSKY INTERNET SECURITY 2010

Павлов А.С.
Научный руководитель – ассистент Шапуркина Ю.С.
Сибирский федеральный университет, г. Красноярск

При работе с современным персональным компьютером пользователя (особенно начинающего) может подстерегать множество неприятностей: потеря данных, зависание системы, выход из строя отдельных частей компьютера и другие. Одной из причин этих проблем наряду с ошибками в программном обеспечении и неумелыми действиями самого оператора ПК могут быть проникшие в систему компьютерные вирусы.

Вирусы – едва ли не главные враги компьютера. Эти программы подобно биологическим вирусам размножаются, записываясь в системные области диска или приписываясь к файлам, и производят различные нежелательные действия, которые, зачастую, имеют катастрофические последствия. Еще два года назад казалось, что со владычеством вирусов покончено – со смертью DOS и DOS- совместимых программ неминуемо должны были исчезнуть и паразитирующие на них вирусы. Ведь если вирус под DOS, заражающий исполняемые файлы .com и .exe-файлы, может написать каждый, кто хоть немного разбирается в программировании, то создать полноценный вирус для Windows гораздо труднее.

Однако вирусы остались, хотя и несколько видоизменились. Сегодня самой распространенной группой вирусов стали макровирусы, заражающие не программы, а документы, созданные в Microsoft Word и Microsoft Excel.

Компьютерный вирус – это специально написанная, как правило, небольшая по размерам программа, которая может записывать свои копии в компьютерные программы, расположенные в исполнимых файлах, системных областях дисков, драйверах, документах и т.д., причем эти копии сохраняют возможность к «размножению». Процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.) называется заражением, а программа или иной объект, содержащий вирус – зараженным.

Антивирусы можно классифицировать по пяти основным группам: фильтры, детекторы, ревизоры, доктора и вакцинаторы.

Антивирусы-фильтры (сторожа) - это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях (например о попытках изменить установки CMOS). При этом выводится запрос о разрешении или запрещении данного действия.

Антивирусы-детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ.

Ревизоры - программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохранённой ранее в одном из файлов данных ревизора.

Антивирусы - вакцинаторы. Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной. Таким образом, вирус не может заразить эту программу.

В настоящее время существует множество антивирусных программ, в качестве примеров можно привести: AIDSTEST, DOCTOR WEB, ADINF. Однако мы в своей работе остановимся на рассмотрении популярной антивирусной программы 2010 года. KIS (KASPERSKY INTERNET SECURITY2010).

Kaspersky Internet Security — программа для комплексной защиты ПК от вирусов и других типов вредоносных программ, а также от хакерских атак и спама – это новое поколение решений по защите информации. Основное отличие Kaspersky Internet Security 2010 от

существующих продуктов, в том числе и от продуктов компании ЗАО "Лаборатория Касперского", – это комплексный подход к защите информации на компьютере пользователя. Программа обеспечивает не только антивирусную защиту, но и защиту от спама и сетевых атак. Также компоненты программы позволяют защищать компьютер от неизвестных угроз и интернет-мошенничества, контролировать доступ пользователей компьютера к интернету. Комплексная защита обеспечивается на всех каналах поступления и передачи информации. Гибкая настройка любого компонента позволяет максимально адаптировать Kaspersky Internet Security под нужды конкретного пользователя.

Рассмотрим детально Kaspersky Internet Security 2010.

Защита компьютера в реальном времени обеспечивается следующими компонентами защиты:

- *Файловый Антивирус;*

Файловый Антивирус контролирует файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на вашем компьютере и на всех присоединенных дисках. Каждое обращение к файлу перехватывается Kaspersky Internet Security, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если файл по каким-либо причинам невозможно вылечить, он будет удален; при этом его копия будет сохранена в резервном хранилище, или помещён на карантин.

- *Почтовый Антивирус;*

Почтовый Антивирус проверяет все входящие и исходящие почтовые сообщения вашего компьютера. Он анализирует электронные письма на присутствие вредоносных программ. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов. Кроме того, компонент анализирует почтовые сообщения на предмет фишинг-мошенничества.

- *Веб-антивирус;*

Веб-антивирус перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Строгому контролю также подвергается весь HTTP-трафик. Кроме того, компонент анализирует веб-страницы на предмет фишинг-мошенничества.

- *IM-антивирус;*

IM-антивирус обеспечивает безопасность работы с интернет-пейджерами. Компонент защищает информацию, поступающую на ваш компьютер по протоколам интернет-пейджеров. IM-антивирус обеспечивает безопасную работу со многими программами, предназначенными для быстрого обмена сообщениями.

- *Контроль программ;*

Контроль программ регистрирует действия, совершаемые программами в системе, и регулирует деятельность программ, исходя из того, к какой группе компонент относит данную программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к различным ресурсам.

- *Сетевой экран;*

Сетевой экран обеспечивает безопасность работы в локальных сетях и интернете. Компонент производит фильтрацию всей сетевой активности согласно правилам двух типов: правилам для программ и пакетным правилам.

- *Проактивная защита;*

Проактивная защита позволяет обнаружить новую вредоносную программу ещё до того, как она успеет нанести вред. Компонент основан на контроле и анализе поведения всех программ, установленных на компьютере. На основании выполняемых действий Kaspersky Internet Security принимает решение о том, является программа потенциально опасной или нет.

Таким образом, компьютер защищен не только от уже известных вирусов, но и от новых, ещё не исследованных.

- *Защита от сетевых атак;*

Защита от сетевых атак запускается при старте операционной системы и отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на компьютер, Kaspersky Internet Security блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

- *Анти-спам;*

Анти-спам встраивается в установленный на компьютере почтовый клиент и контролирует все поступающие почтовые сообщения на предмет спама. Все письма, содержащие спам, помечаются специальным заголовком. Предусмотрена также возможность настройки Анти-спама на обработку спама (автоматическое удаление, помещение в специальную папку и т. д.). Также компонент анализирует почтовые сообщения на предмет фишинг-мошенничества.

- *Мониторинг сети;*

Компонент, предназначенный для просмотра информации о сетевой активности в реальном времени.

- *Анти-фишинг;*

Компонент, встроенный в веб-антивирус, анти-спам и IM-антивирус, который позволяет проверять веб-адреса на принадлежность к спискам фишинговых и подозрительных веб-адресов.

- *Анти-баннер;*

Анти-баннер блокирует рекламную информацию, размещенную на специальных баннерах, встроенных в интерфейс различных программ, установленных на компьютере, и находящихся в интернете.

- *Безопасная среда*

Позволяет запускать приложения в безопасном для системы окружении. Это может быть использовано для запуска потенциально опасного ПО или для анонимного веб-серфинга.

- *Проверка ссылок.*

Дополнение для браузеров Internet Explorer и Mozilla Firefox, проверяющее ссылки на просматриваемой веб-странице на предмет заражения веб-страниц, на которые они ссылаются.

Системные требования: операционная система: Microsoft Windows XP; Microsoft Windows Vista; Microsoft Windows 7.

Награды: в апреле 2009 Kaspersky Internet Security 2009 получил премию «Золотой Компьютер» журнала ComputerBild. Решение стало победителем в номинации Soft и обладателем главного приза как продукт, получивший абсолютное число голосов в свою поддержку. В апреле 2009 по итогам сравнительного исследования, проведенного журналом «Мир ПК», Kaspersky Internet Security 2009 получил награду «Выбор редакции».

Одним из недостатков линейки продуктов Лаборатории Касперского является автоматический старт поиска руткитов, в ходе которого производительность компьютера достаточно резко уменьшается.

В заключение следует отметить, что в настоящее время существует множество компьютерных вирусов. И, несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых вирусов постоянно растет. Это требует от пользователей ПК знаний о природе программных вирусов, способах заражения ими и защиты от них.