

АНТИВИРУСНЫЕ ПРОГРАММЫ

Аникьева Эмилия Николаевна,

старший преподаватель

математики, физики и информационных технологий

ФГБОУ ВО Мичуринский ГАУ

г. Мичуринск, РФ

Koro_0909@mail.ru

Якунина Анастасия Николаевна,

Студентка 1 курса

Плодоовощного института

ФГБОУ ВО Мичуринский ГАУ,

г. Мичуринск, РФ.

nasty.yakunina.99@inbox.ru

Аннотация. Статья посвящена антивирусным программам в Плодоовощном институте Мичуринского ГАУ.

Ключевые слова. Признаки появления вирусов, степени воздействия, защита от вирусов.

Антивирус - программное средство, предназначенное для борьбы с вирусами.

Как следует из определения, основными задачами антивируса является:

Препятствование проникновению вирусов в компьютерную систему

Обнаружение наличия вирусов в компьютерной системе

Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы

Минимизация ущерба от действий вирусов

Компьютерные вирусы, как таковые, впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ. Одним из "пионеров" среди

компьютерных вирусов считается вирус "Brain", созданный пакистанским программистом по фамилии Алви. Только в США этот вирус поразил свыше 18 тыс. компьютеров. В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов".

Основные признаки проявления вирусов :

- Прекращение работы или неправильная работа ранее успешно функционировавших программ;
- Медленная работа компьютера;
- Невозможность загрузки операционной системы;
- Исчезновение файлов и каталогов или искажение их содержимого;
- Изменение даты и времени модификации файлов;
- Изменение размеров файлов;
- Частые зависания и сбои в работе;
- Неожиданное значительное увеличение количества файлов на диске;
- Существенное уменьшение размера свободной оперативной памяти;
- Вывод на экран непредусмотренных сообщений или изображений;
- Подача непредусмотренных звуковых сигналов.

Классификация компьютерных вирусов:

- а** - по среде обитания: сетевые, файловые, загрузочные, файлово-загрузочные;
- б** - по способу заражения: резидентные и нерезидентные;
- в**- по степени воздействия: неопасные, опасные и очень опасные;
- г** - по особенностям алгоритмов: паразитические, репликаторы, невидимки, мутанты, троянские.

Пути проникновения вирусов:

- Глобальная сеть Internet;
- Электронная почта;
- Локальная сеть;
- Компьютеры «Общего назначения»;
- Пиратское программное обеспечение;
- Ремонтные службы;
- Съёмные накопители.

По способу заражения:

Резидентные (такой вирус при инфицировании ПК оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК).

Нерезидентные (не заражают оперативную память и могут быть активными ограниченное время).

По степени воздействия:

Неопасные (как правило эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости - проигрывать заложенную в них мелодию или показывать картинку);

Опасные (эти вирусы способны создать некоторые нарушения в функционировании ПК - сбои, перезагрузки, глюки, медленная работа компьютера и т.д.);

Очень опасные (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить).

По особенностям алгоритма:

Паразитические (меняют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются);

Мутанты (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую);

Репликаторы (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их);

Троянский конь (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную (порой очень дорогую) информацию - пароли, банковские счета, электронные деньги и т.д.);

Невидимки (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.

Ремонтные службы:

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники - тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

Съемные накопители:

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.

Троянский конь - это вредоносное программное обеспечение, которое, без ведома владельца персонального компьютера может предоставить доступ к его данным или по определенному адресу выслать вашу персональную информацию. Кроме этого, вы даже себе и подумать не можете, что эта программа является "трояном", так как программы подобного рода законспирированы под нужные и безопасные приложения.

Trojan.Winlock (Винлокер) - семейство вредоносных программ блокирующих или затрудняющих работу с операционной системой, и требующих перечисление денег злоумышленникам за

восстановление работоспособности компьютера. Впервые появились в конце 2007 года. Широкое распространение вирусы-вымогатели получили зимой 2009-2010 года, по некоторым данным оказались заражены миллионы компьютеров, преимущественно среди пользователей русскоязычного Интернета. Второй всплеск активности такого вредоносного ПО пришелся на май 2010 года.

Как защититься от вирусов:

- установите на свой ПК современную антивирусную программу;
- перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом;
- после разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно);
- периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом - запускайте раз в неделю, а то и чаще);
- как можно чаще делайте резервные копии важной информации (backup);
- используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет;
- настройте браузер (программа просмотра Интернет страниц - IE, Опера и т.д.) для запрета запуска активного содержимого html-страниц.

ANTI-VIRUS PROGRAMM

Anikieva Emilia Nikolaevna,

senior lecturer

mathematics, physics and information technologies at

Michurinsk State Agrarian University

Michurinsk, Russia

Koro_0909@mail.ru

Yakunina Anastasia Nikolaevna,

1st year student

Fruit and vegetable Institute

nastya.yakunina.99@inbox.ru

Doctor of Michurinsk State Agrarian University,

Michurinsk, Russia

Annotation. The article is devoted to anti-virus programs in the fruit and Vegetable Institute of Michurinsky GAU.

Keyword. Signs of the emergence of viruses, extent impact, protection from viruses.