*Компьютерные вирусы и антивирусные программы*

*Общие сведения о вирусах*

*Компьютерный вирус –* это специальная программа, которая написана с целью наруше­ния нормальной работы компьютера незаметно для пользо­вателя путем порчи файлов и каталогов; способна самопро­извольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети. Основные источ­ники и пути проникновения вирусов: съемные магнитные и оптические диски, компьютерные сети.

Основные объекты, заражаемые вирусами: загрузочный сектор диска; файлы с расширениями EXE, СОМ, ВАТ и SYS.

Вирусы могут находиться: *в активном* состоянии, когда они загружены в оперативную память компьютера, и *в пас­сивном* состоянии, когда они просто хранятся в файлах или загрузочных записях.

Действие компьютерных вирусов может не проявляться в течение нескольких дней и даже недель. Некоторые ви­русы действуют только в определенные часы и дни. Вирус может распространяться незаметно еще до того, как начнет себя проявлять.

*Признаки* проявления вирусов:

– нарушение загрузки операционной системы;

– неправильная работа или полное прекращение работы ранее функционировавших программ;

– искажение содержимого файлов и каталогов или их исчезновение;

– изменение размеров файла, даты и времени их модификации;

– частые зависания и сбои в работе компьютера, мед­ленная работа компьютера;

– вывод на экран непредусмотренных сообщений или изо­бражений, подача непредусмотренных звуковых сигналов.

Вирусы *могут:*

– заразить программные файлы, текстовые файлы и файлы электронных таблиц или программы операционной системы и файлы документов (такие, как файлы DOT и DOC), содержащие макросы;

– заразить диски, прикрепляясь к специальным про­граммам и тех областях диска, которые называются загру­зочными записями и главными загрузочными записями;

– испортить файлы и данные.

Вирусы *не могут:*

– повредить аппаратные средства, такие как клавиату­ра и монитор. Даже если наблюдаются странные явления, например искажение экрана или «заглатывание» вводимых символов, это означает всего лишь то, что вирус поразил программу, управляющую монитором или клавиатурой;

– физически повредить диски;

– заразить диски, защищенные от записи.

*Классификация вирусов*

Основными классификаци­онными признаками вирусов являются среда обитания, способ заражения, степень воздействия, особенности ал­горитма.

По *среде обитания* различают:

– сетевые вирусы, распространяющиеся по различным компьютерным сетям;

– файловые вирусы, которые внедряются и размножа­ются главным образом в исполняемые файлы (с расшире­нием КХК и СОМ). При внедрении в другие файлы вирусы теряют способность к размножению;

– загрузочные вирусы, которые заражают загрузочный сектор диска, поражая загрузочные записи;

– файлово-загрузочные вирусы, которые внедряются в файлы и в загрузочный сектор диска;

– вирусы макросов, которые заражают файлы приложе­ний, поддерживающих использование макросов.

По *способу заражения* различают:

– резидентные вирусы, которые при включенном компьютере постоянно находятся в оперативной памяти. Они перехватывают обращения операционной системы к файлам, загрузочным секторам диска и заражают их;

– нерезидентные вирусы, которые не заражают намять компьютера и являются активными ограниченное время.

По *степени воздействия* можно выделить следующие виды вирусов:

– неопасные вирусы, которые не препятствуют нор­мальной работе компьютера, однако уменьшают объем опе­ративной памяти и памяти на дисках. Действия неопасных вирусов может проявляться в искажении графических объ­ектов или в звуковых эффектах;

– опасные вирусы, приводящие к нарушению нормаль­ной работы компьютера;

– очень опасные вирусы, которые стирают информацию в системных областях диска, уничтожают программы.

Но *особенностям алгоритмов* различают:

– паразитические вирусы, которые изменяют содержи­мое файлов и секторов дисков. Такие вирусы легко обнару­живаются и уничтожаются;

– вирусы-репликаторы (черви), которые распростра­няются по сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии;

– вирусы-невидимки (стелс-вирусы), которые перехва­тывают обращения операционной системы к пораженным файлам и секторам и переадресуют их на незараженные участки диска.

Жизненный цикл вирусов состоит из трех этапов: зара­жение, обнаружение и обезвреживание.

*Меры по защите от вирусов*

Для защиты следует:

– использовать датчик поиска вирусов для автоматиче­ской проверки компьютера на вирусы во время работы;

– использовать датчик описаний вирусов для автома­тического обновления описаний вирусов. Это даст уверен­ность в том, что компьютер будет защищен от самых новей­ших вирусов;

– приобрести и использовать хорошую программу по обнаружению и удалению вирусов;

– периодически создавать резервные копии жестких ди­сков.

*Антивирусные программы*

Программы, позволяющие обнаружить и уничтожить вирусы, называют *антивиру­сными программами.* Рассмотрим основные виды антиви­русных программ.

*Программы-детекторы.* К ним относятся такие про­граммы, которые осуществляют *поиск характерной* (для конкретного типа вирусов) *последовательности байтов в оперативной памяти* и при их обнаружении выдают со­ответствующее сообщение. Однако такие последовательно­сти могут быть известны только разработчикам вирусных программ.

*Программы доктора* (фаги, или программы-вакцины). Фаги находят не только зараженные вирусами файлы, но и удаляют из них тело программы вируса, возвращая файл в исходное, рабочее состояние. Среди фагов выделяют *поли­фаги,* предназначенные для поиска и уничтожения большого количества вирусов. К полифагам относятся следующие из­вестные программы: Aidstest, Scan, Norton Antivirus, Doctor Web и др.

*Программы-ревизоры.* Эти программы относятся к на­иболее надежным средствам защиты от вирусов. В их памя­ти хранятся незараженные вирусом программы, каталоги, системные области дисков. В процессе работы компьютера (как правило, после загрузки операционной системы) те­кущее состояние сравнивается с исходным по таким пара­метрам, как длина файла, контрольная сумма файла, дата и время модификации. Примером такой программы явля­ется программа *Adinf* фирмы «Диалог-Наука».

*Программы-фильтры, или «сторожа».* К этому виду программ относятся небольшие резидентные (постоян­но находящиеся в памяти) программы, предназначенные для обнаружения таких характерных для вирусов действий компьютера, как изменение атрибутов файлов, попытки коррекции файлов с расширение СОМ и ЕХЕ; запись в за­грузочные сектора диска, прямая запись на диск по абсо­лютному адресу; загрузка резидентной программы.

«Сторож» оповещает пользователя сообщением о по­пытке какой-либо программы произвести указанные дей­ствия с предложением их запрета или разрешения. Про­граммы-фильтры способны только обнаружить, но не уничтожают вирусы.

*Вакцины, или иммунизаторы.* Эти резидентные про­граммы предотвращают заражение файлов. Вакцина моди­фицирует программу или диск таким образом, чтобы они были работоспособны, но выглядели как зараженные. Вак­цинация возможна только от известных вирусов. В настоя­щее время их применение ограничено.

*Задание.*

*Дать ответы, оформив в текстовом редакторе Word, на контрольные вопросы.*

1. Дайте определение компьютерного вируса.
2. Перечислите основные источники и пути проникновения вирусов?
3. Перечислите основные объекты, заражаемые вирусами.
4. В каких состояниях могут находиться вирусы?
5. Перечислите признаки проявления вирусов.
6. Что вирусы могут?
7. Что вирусы не могут?
8. Перечислите основные классификационные признаки вирусов.
9. Какие вирусы различают по среде обитания?
10. Какие вирусы различают по способу заражения?
11. Какие вирусы можно выделить по степени воздействия?
12. Какие вирусы различают по особенностям алгоритмов?
13. Из каких этапов состоит жизненный цикл вирусов?
14. Перечислите меры по защите от вирусов.
15. Какие программы называют антивирусными?
16. Перечислите основные виды антивирусных программ.
17. Какие программы относят к программам-детекторам?
18. Что делают программы доктора, какие среди них выделяют и для чего они предназначены?
19. Как себя ведут программы-ревизоры?
20. Что относят к программам-фильтрам, или «сторожам», для чего они предназначены?
21. Что делают программы вакцины, или иммунизаторы?

Задания присылать в ВК в личные сообщения

<https://vk.com/id134665099>

Название файла, например: **Иванов И. ВХ-111 27.11**

Срок исполнения -03 декабря