1. **Что такое ICSA?**

Международной Ассоциации по Компьютерной Безопасности – ICSA

1. **Какие вирусы называются «дикими»?**

Вирусов, реально циркулирующих в компьютерных сетях, редко насчитывается более 300 видов (одни постепенно вымирают, вместо них появляются новые и так до бесконечности). Это, так называемые, «дикие» вирусы, которые представляют собой наиболее распространенные на данный момент вирусы, относящиеся к различным классам.

1. **Что означает термин «заражение компьютера вирусом»?**

Термин «заражение компьютера» на самом деле означает проникновение вируса на жесткий диск («винчестер»). Опасность вируса заключается в том, что он может уничтожить нужную информацию на жестком диске.

1. **Кем впервые был употреблен термин «компьютерный вирус»?**

Термин «компьютерный вирус» впервые был употреблен Фредериком Коэном в 1984 году на 7-й конференции по вопросам информационной безопасности проходившей в США.

1. **Перечислите наиболее общие черты сходства биологических и компьютерных вирусов?**

|  |  |
| --- | --- |
| Биологически вирусы | Компьютерные вирусы |
| Нападают на специальные соматические клетки | Нападают на определенный класс программ (\*.com, \*.exe и т.д.) |
| Изменяют наследственную информацию клетки | Изменяют исполняемый код зараженной программы |
| Пораженная клетка является источником новых вирусов | Зараженная программа становится источником новых вирусов |
| Инфицированная клетка не поражается одним и тем же вирусом многократно | Одна и та же программа инфицируется большинством вирусов лишь однажды |
| Пораженный организм часто в течение длительного времени не проявляет признаков заболевания | Пораженная программа в течение длительного времени может работать без ошибок |
| Вирусы могут мутировать, благодаря чему они не всегда однозначно распознаются | Вирусы могут изменять свой исполняемый код, в результате чего их невозможно однозначно идентифицировать. |

1. **Являются ли компьютерные вирусы опасными для человека?**

Нет

1. **Существует ли точное определение того, что является компьютерным вирусом?**

Компьютерный вирус – это сегмент программного кода, который может имплантировать себя в исполняемые файлы операционной системы, создавать программный код, выполняющий аналогичные функции, и внедрять его в файлы прикладных программ, системные области компьютера, вычислительные сети и т.д. Такие программы часто носят деструктивный характер, являются небольшими по размеру, и всеми возможными способами пытаются скрыть от пользователя свое присутствие в системе.

Однако, как уже было сказано выше, абсолютно точного определения компьютерного вируса не существует.

1. **Наносит ли целевая функция вируса гораздо больший ущерб, чем ущерб, наносимый размножением вируса? Ответ обосновать.**

Порой ущерб от косвенного вреда вируса является более значительным, чем от реализации его целевой функции (так было с вирусом Морриса).

1. **Насколько давно существуют идеи создания самовоспроизводящихся программ?**

Впервые идеи создания саморазмножающихся механизмов были выдвинуты еще основателем современных компьютерных систем – Джоном Фон Нейманом в 1951 году. Он разрабатывал модели автоматов, способных к самовоспроизведению и математически доказал возможность существования таких машин.

1. **Когда впервые появились программы, реализующие алгоритмы простейших вирусов?**

В 60-х и 70-х годах появились первые программы, написанные на интерпретируемом командном языке, которые обладали главной отличительной чертой всех существующих вирусов – способностью к самовоспроизведению. Эти программы даже получили свое название – Rabbit.

1. **Rabbit – это название конкретной программы или класса программ?**

Эти программы даже получили свое название – Rabbit. Поначалу такие программы возникали непреднамеренно, чаще всего в результате ошибок программистов.

1. **Когда и где впервые появился сетевой вирус?**

В начале 70-х годов, для компьютерной сети ARPAnet, была создана саморазмножающаяся программа – Creeper, которая путешествовала по сети, обнаруживая свое появление сообщением: “I’m the creeper … catch me if you can”

Однако самым широко известным вирусом, за всю историю компьютеров, пожалуй, является вирус Роберта Морриса (названный червем Морриса).

Второго ноября 1988 года студент Корнельского университета Роберт Моррис запустил на компьютере Массачусетского технологического института программу-червь, которая передавала свой код с машины на машину, используя ошибки в системе UNIX на компьютерах VAX и Sun.

Червь представлял собой программу из 4000 строк на языке Си и входном языке командного интерпретатора системы UNIX.

1. **Опишите один из первых способов борьбы с компьютерными вирусами? Применяется ли этот способ в настоящее время? Ответ обосновать.**

Для борьбы с ней была написана другая программа – Reaper, которая также распространяла себя по сети и уничтожала встретившиеся экземпляры программы Creeper. Так впервые была реализована идея вируса, распространяющегося по сети, и впервые, для борьбы с компьютерными вирусами, был реализован подход – «подобное лечится подобным». Позднее он неоднократно переоткрывался, но так и не получил широкого распространения.

1. **В каком году впервые был употреблен термин «компьютерный вирус»?**

Впервые был употреблен Фредериком Коэном в 1984 году

1. **В каких операционных системах распространялся один из наиболее известных компьютерных вирусов – вирус Морриса?**

Роберт Моррис запустил на компьютере Массачусетского технологического института программу-червь, которая передавала свой код с машины на машину, используя ошибки в системе UNIX на компьютерах VAX и Sun.

1. **Кто был создателем одного из первых полиморфных вирусов?**

Другим известным инцидентом стало создание первого полиморфного вируса. Кристофер Пайн создал вирусы Pathogen, Queeq и Smeg, из которых именно последний был наиболее опасным.

1. **Что собой представлял первый полиморфный вирус?**

Его можно было накладывать на первые два вируса и после каждого прогона программы, те меняли свою конфигурацию, поэтому было практически невозможно обнаружить все копии вируса. В результате создания и распространения этих вирусов были уничтожены файлы множества фирм, а убытки составили миллионы фунтов стерлингов.

1. **Все ли компьютерные вирусы являются оригинальными разработками?**

Среди тысяч существующих вирусов лишь несколько десятков являются действительно оригинальными разработками, использующими принципиально новые идеи. Но каждая такая идея не только выдвигает вперед вирусописателей, дает им ощутимое преимущество, но и вынуждает разработчиков антивирусных программ искать свои способы борьбы с новой заразой, приспосабливаться к измененным условиям и догонять вирусную технологию.

1. **На какие классы можно разделить вирусы по среде обитания?**

По среде обитания компьютерные вирусы можно разделить на следующие несколько классов:

* Сетевые вирусы – это вирусы, распространяющиеся по компьютерным сетям и нацеленные на сетевые операционные системы.
* Загрузочные вирусы – это вирусы, поражающие загрузочные сектора дисков.
* Файловые вирусы – это вирусы, поражающие исполняемые файлы операционных систем и файлы прикладных программ и данных.
* Комбинированные вирусы – это вирусы, сочетающие в себе свойства вышеописанных групп вирусов (например, файловых и загрузочных).

1. **Что является общим для всех классов компьютерных вирусов?**

В любом случае компьютерный вирус – это некий программный код. Поэтому сетевой вирус будет отличаться от файлового или загрузочного только местом хранения своего исполняемого кода и соответственно способом распространения, но все они могут обладать одинаковыми деструктивными возможностями или проявлять себя, на зараженном компьютере, одинаковыми спецэффектами.

1. **Какие вирусы способны выполнять свои функции до загрузки операционной системы?**

Распространение и активизация вирусов этого класса происходит в момент загрузки операционной системы, еще до того, как пользователь успел запустить какую-либо антивирусную программу. Основной их особенностью является, то, что вирус будет активизироваться при любой перезагрузке компьютера до тех пор, пока он располагается в перечисленных выше областях.

1. **Вирусы какого класса могут обходиться без использования файлов для своего размножения**

Чаще всего, сетевые вирусы проникают в оперативную память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти и процессора). Фактически их средой обитания является не столько локальный компьютер (что характерно для всех остальных типов вирусов), сколько совокупность компьютеров, образующих вычислительную сеть.

1. **Чем отличаются сетевые вирусы от загрузочных?**

Место хранения:

* Сетевые

использующие электронные сети для хранения своего кода

* Загрузочные

располагающиеся в загрузочных секторах дискет (Boot record) или в секторах, содержащих системный загрузчик жесткого диска (Master Boot Record, сокращенно MBR) или загрузчик операционной системы на логическом диске (он также называется Boot record).

Способ распространения:

* Сетевые

Чаще всего, сетевые вирусы проникают в оперативную память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.

* Загрузочные

Распространение и активизация вирусов этого класса происходит в момент загрузки операционной системы, еще до того, как пользователь успел запустить какую-либо антивирусную программу.

Кроме того, стоит упомянуть особенность сетевых вирусов: отличающиеся от всех остальных вирусов тем, что очень часто являются самостоятельными программами, т.е. они не нуждаются в других программах как «носителях» своего кода.

1. **Может ли пользователь занести на компьютер вирус, загрузившись с дискеты, не содержащей никаких файлов и не являющейся загрузочной?**

Необходимо отметить, что дискеты могут быть системными и несистемными.

Если дискета форматируется как системная, то первый сектор нулевой дорожки дискеты содержит программу начальной загрузки операционной системы (например, MS-DOS). Если же дискета форматируется как несистемная, то в первый сектор нулевой дорожки дискеты все равно записывается программа, единственным назначением которой является вывод сообщения о необходимости вставить в дисковод системную дискету (чаще всего это сообщение типа – "Non-system Disk or Disk Error").

Данное обстоятельство – присутствие загрузочной записи на несистемной дискете – играет важную роль для загрузочных вирусов, т.к. ее наличие позволяет им распространяться, несмотря на отсутствие на дискете системного загрузчика и файлов операционной системы.

1. **Какие действия следует предпринять пользователю для предотвращения попадания на его машину загрузочного вируса?**

Пользователю следует отказаться от загрузки ОС с внешних носителей(использовать только проверенные) и установить в BIOS защиту загрузочного сектора от изменений.

1. **В чем может заключаться опасность даже самого «безобидного» сетевого вируса.**

Опасность сетевых вирусов, заключается не только в их деструктивных возможностях, сложности обнаружения и удаления, но и в том, что при большой скорости распространения или ошибке в коде программы, такие вирусы, оттягивая на себя значительные сетевые ресурсы, вызывают отказы в обслуживании, тем самым, прерывая нормальное функционирование сети.

1. **Где размещается основной код загрузочного вируса?**

В загрузочных секторах дискет (Boot record) или в секторах, содержащих системный загрузчик жесткого диска (Master Boot Record, сокращенно MBR) или загрузчик операционной системы на логическом диске (он также называется Boot record).

1. **Какие действия предпринимаются загрузочным вирусом для предотвращения его обнаружения?**

Обнаружение и удаление таких вирусов затруднено из-за того, что они могут контролировать обращения операционной системы к дисковым накопителям и скрывать свое присутствие от антивирусных программ, работающих с дисками через прерывания операционной системы.

1. **Почему обнаружение загрузочного вируса может стать очень сложной задачей?**

См. вопрос 10.

1. **Все ли типы файлов заражаются компьютерными вирусами? Какие типы файлов могут инфицироваться вирусами, при каких условиях? Какие типы файлов не могут инфицироваться вирусами, при каких условиях?**

Для того чтобы файловый вирус начал функционировать после перезагрузки компьютера, инфицированная программа должна быть запущена пользователем или операционной системой на выполнение. Значит, файловые вирусы чаще всего будут располагаться в исполняемых файлах операционной системы или файлах динамических библиотек (в операционных системах MS-DOS и WINDOWS это файлы с расширениями \*.COM, \*.EXE и \*.DLL). В качестве среды их обитания могут выступать не только исполняемые файлы, но и файлы драйверов операционной системы (\*.SYS, \*.DRV, \*.BIN, \*.OVL, \*.OVY и т.д.) или файлы документов, содержащих последовательность макрокоманд (\*.DOC, \*.XLS, \*.CDR и др.), которая может быть выполнена соответствующим макроязыком.

Тексты программ и документов, информационные файлы баз данных, таблицы табличных процессоров и другие аналогичные файлы, не содержащие макрокоманд, не могут быть заражены вирусом. Они могут быть только уничтожены или изменены.

1. **Варианты размещения кода вируса при заражении исполняемых файлов?**

Вирус может размещаться в различных частях исполняемых файлов, например, в конце файла (наиболее распространенный вариант) или в середине файла (самый редкий вариант). При этом вирус может сдвигать исполняемый код программы для того, чтобы поместить свой собственный код, либо записывать свой код поверх исполняемого кода программы.

1. **Что отличает комбинированные вирусы от вирусов всех остальных классов?**

Комбинированные вирусы – это вирусы, обладающие теми особенностями, которые присущи сразу нескольким вышеперечисленным классам. Их модели поведения, особенности алгоритмов и способы распространения аналогичны тем классам, из частей которых они состоят.

1. **Являются ли комбинированные вирусы более опасными, чем сетевые? Загрузочные?**

Да, потому что они имеют большую гибкость.

1. **Всегда ли инфицированный файл представляет непосредственную опасность для пользователя?**

Нет, инфицированный файл может быть никогда не использован, соответственно вирус не получит возможность действовать.

1. **В какой момент времени нерезидентный вирус, чаще всего, выполняет свои функции?**

Нерезидентные вирусы – это вирусы, которые могут активизироваться только во время выполнения инфицированной программы и удаляют из оперативной памяти свои копии сразу же по ее завершении, а иногда и раньше. Например, после выполнения вирусом всех предусмотренных в нем функций.

1. **Чем резидентные вирусы отличаются от нерезидентных?**

Резидентные вирусы – это вирусы, которые забирают у операционной системы часть оперативной памяти компьютера и начинают перехватывать обращения к занятому участку памяти, файлам прикладных программ или системным областям диска и т.д. Таким образом, в памяти компьютера фактически запускается новый процесс, имеющий свои ресурсы, приоритет выполнения и методы взаимодействия с другими процессами, который продолжает выполняться даже после того как инфицированная программа, вызвавшая его активизацию, прекратит свою работу. Удалить из оперативной памяти такой вирус можно только в том случае, если произвести полную перезагрузку компьютера.

1. **Какие вирусы опаснее резидентные или нерезидентные?**

Файлы, пораженные нерезидентными вирусами, обычно легче поддаются обнаружению и лечению, чем файлы, содержащие резидентный вирус.

1. **На чем основан механизм действия вирусов-спутников?**

Вирусы-спутники – это вирусы, действие которых основано на особенностях работы операционных систем MS-DOS и Windows. Суть этой особенности заключается в следующем.

Если каталог содержит два исполняемых файла с одинаковыми названиями, но разными расширениями (обычно это \*.СОМ и \*.ЕХЕ) и пользователь пытается запустить файл, набрав в командной строке его название без расширения (довольно распространенное для MS-DOS явление), то выполняться будет файл с расширением \*.СОМ.

Таким образом, вирусы-«спутники» не изменяют исполняемые файлы операционной системы, а лишь создают дополнительные файлы, имеющие расширение \*.СОМ и одинаковое с \*.ЕХЕ файлом название. В результате, когда пользователь пытается запустить файл на выполнение, набрав его название в командной строке, первым запускается \*.СОМ файл, содержащий исполняемый код вируса. После выполнения всех предусмотренных действий и перед завершением работы \*.СОМ программы, вирус запускает соответствующий \*.ЕХЕ файл, необходимый пользователю. Вся эта операция происходит настолько быстро, что пользователь ничего не замечает.

1. **Возможно ли использование механизма вирусов-спутников для размножения вирусов в операционной системе Windows?**

Да. Вирусы-спутники – это вирусы, действие которых основано на особенностях работы операционных систем MS-DOS и Windows.

1. **Какие операционные системы являются наиболее удобными для распространения червей?**

Данная разновидность компьютерных вирусов, получила широкое распространение в операционных системах типа UNIX, которые наиболее часто используются для  работы в сети.

1. **Что явилось основной причиной появления стелс вирусов и вирусов призраков?**

Скорее всего распространение антивирусных программ, которые могли успешно обнаруживать и уничтожать обыкновенные вирусы.

1. **Какие механизмы используются стелс вирусами в целях выживания?**

Например, известно, что при заражении программы обычно изменяется длина файла. Когда антивирусная программа пытается определить длину файла, она передает запрос операционной системе, которая инициирует соответствующее прерывание. Вирус перехватывает это прерывание, обрабатывает его и если обнаруживает, что кто-то пытается определить размер зараженной программы, то он возвращает размер файла, который был до заражения. В результате операционная система возвращает антивирусной программе неверные данные и, соответственно, последняя не может обнаружить вирус.

Аналогичные действия производятся вирусом, когда некая программа пытается определить его наличие и место расположение в оперативной памяти компьютера.

Обнаружив запуск пользователем антивирусной программы, вирусы могут блокировать систему, выдав сообщение о системной ошибке, или, вообще, полностью удалить антивирусную программу с жесткого диска. Существуют вирусы, которые даже пытаются заразить антивирусные программы в случае начала их работы или в случае их обнаружения на жестком диске.

1. **Чем алгоритм выживания стелс вирусов отличается от соответствующего алгоритма вирусов призраков?**

Принцип действия «полиморфных» вирусов основан на том, что их исполняемый код, в каждой последующей копии вируса, непохож на предыдущий. В принципе вообще может не существовать определенной последовательности кода, по которой бы однозначно можно было бы идентифицировать данный вирус. Такой эффект достигается, встроенным в исполняемый код вируса, механизмом шифрования (так называемый механизм мутации). Этот механизм создает произвольные изменения в сигнатуре вируса, делая его последующие копии не похожими на предыдущие.

1. **К какому классу относятся вирусы, шифрующие свой код?**

К классу полиморфных вирусов.

1. **Какие еще алгоритмы (способы, методы) используемые вирусами для своего выживания вы можете предложить?**

Появились вирусы, способные выживать при настоящей “холодной” перезагрузке. Вирус перед каждым обращением к флоппи-дисководам включает в CMOS признак их наличия, а после обращения — отключает. Таким образом, большую часть времени у вас “нет” дисководов, но вы об этом не знаете — когда происходит обращение к дисководам, все внешне выглядит прилично. В момент перезагрузки системы программа начальной загрузки, не найдя дисковода A, пытается загрузиться с винчестера (таков алгоритм ее работы). Вирус получает управление, устанавливается резидентно в память и передает управление загрузочному сектору диска A.

1. **Являются ли вирусы, распространяющиеся по электронной почте – сетевыми? Ответ обоснуйте?**

Да, являются. Такие вирусы способны создавать новое письмо и внедрять в него зараженный файл-документ, отправляя по почте (Сети).

1. **Можно ли вирусы, рассылаемые по электронной почте выделить в какой-либо отдельный класс?**

Вирусы, рассылаемые по электронной почте, фактически являются червями.

1. **В каких средах распространяются макровирусы?**

Макро-вирус может изменять существующие макрокоманды и добавлять новые, внедряя свое «тело» в файл документов офисных приложений.

1. **В чем заключается основная трудность при обнаружении макровируса?**

Создание «макро»-вируса и(или) его изменение производятся значительно проще, чем в других классах вирусов, а в связи с тем, что документы распространены более широко, чем прикладные программы, то данный класс вирусов представляет собой значительную угрозу.

1. **Существуют ли способы защиты от макровирусов? Ответ обосновать?**

Для предотвращения заражения «макро»-вирусами необходимо перед просмотром или редактированием проверять новые файлы документов с помощью антивирусных программ, способных искать такие вирусы. Рекомендуется также, после установки пакета Microsoft Office, сохранять стандартный файл шаблона Normal.dot (этот файл чаще всего используется вирусами для заражения других документов) в каком-нибудь другом каталоге и в случае подозрения на «макро»-вирус заменять текущий файл шаблона его резервной копией.

1. **Можете ли вы предложить какие-либо свои методы борьбы с макровирусами?**

Не скачивать документы из непроверенных источников.

1. **Что такое антивирусная программа?**

Антивирусная программа - специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

1. **Какие типы антивирусных программ вы знаете?**

* вакцины;
* детекторы;
* ревизоры;
* сторожа;
* мониторы;
* полифаги;
* эвристические анализаторы.

1. **Что собой представляет антивирусная программа – вакцина? Каких типов они бывают?**

Вакцины – это программы, предназначенные для предотвращения заражения файлов от какого-либо одного, конкретного вируса.

1. **Почему пришлось отказаться от использования вакцин в качестве антивирусов?**

В первую очередь это связано с огромным числом компьютерных вирусов, каждый из которых имеет собственную «черную метку». Поэтому защитить таким способом все исполняемые файлы от всех известных вирусов, в принципе невозможно..

1. **Что такое детекторы?**

«Детекторы» или «сканеры» - это программы, которые осуществляют поиск характерной для конкретного вируса сигнатуры, в оперативной памяти компьютера или в файлах на жестком диске, и при обнаружении, выдают соответствующее сообщение. Недостатком этого класса антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам.

1. **Могут ли детекторы лечить зараженные программы?**

Нет, бороться с обнаруженным вирусом предстоит либо другой антивирусной программе, либо системному программисту.

1. **Чем ревизоры отличаются от других классов антивирусных программ?**

Высочайшая скорость проверки дисков (во много десятков раз превышающая скорость работы сканеров) и высокая надежность обнаружения даже неизвестных вирусов.

1. **На каком принципе основано действие большинства антивирусных программ?**

На обнаружении вирусов.

1. **Какие классы антивирусных программ могут быть использованы для обнаружения неизвестных вирусов? Результаты какого класса являются наиболее достоверными?**

Ревизоры, сторожа, эвристические анализаторы.

Ревизоры и эвристические анализаторы имеют примерно одинаковую степерь достоверности.

1. **В чем заключается основное отличие антивирусных мониторов от программ сторожей? В чем их сходство?**

И те и другие проверяют только программы/файлы, с которыми производятся манипуляции.

Главное отличие заключается в том, что мониторы используют для обнаружения вирусов базу сигнатур, а сторожи основываются на подозрительной активности.

1. **Какие классы программ объединяют в себе антивирусные программы полифаги?**

Полифаги можно разделить на две категории: универсальные и специа­лизированные сканеры. Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Также их можно разделить на резидентные мониторы, производящие сканирование «налету», и нерезидентные сканеры, обеспечивающие проверку систе­мы только по запросу. Резидентные мониторы обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска.

1. **Какие антивирусные программы являются наиболее распространенными на данный момент? Почему?**

Kaspersky AV, Dr. Web, Nod 32, Avast. Все из перечисленных антивирусных программ сочетают в себе большинство базовых типов.

1. **Что такое эвристические анализаторы? По какому принципу они работают?**

Эвристические анализаторы – программы, выполняющие под своим контролем, проверяемые программы и обнаруживающие действия, характерные для вирусов. Благодаря этому эвристические анализаторы способны находить «полиморфные» вирусы также легко, как и обычные вирусы, не использующие механизма маскировки, кроме того, они могут обнаруживать вирусы, ранее неизвестные авторам антивирусной программы.

1. **В каком случае использование эвристического анализатора является наиболее целесообразным?**

С учётом текущего разнообразия уже существующих вирусов и скорости появления новых, я не вижу ситуаций, в которых было бы не целесообразно использовать эвристический анализатор.

1. **Перечислите основные, известные вам признаки появления компьютерных вирусов?**
   * вывод на экран непредусмотренных сообщений или изображений;
   * воспроизведение различных непредусмотренных мелодий или посторонних звуков;
   * прекращение работы или неправильная работа ранее успешно функционировавших программ;
   * работа на компьютере существенно замедляется;
   * некоторые файлы данных оказываются испорченными;
   * невозможность загрузки операционной системы;
   * исчезновение файлов и каталогов или искажение их содержимого;
   * изменение даты и времени модификации файлов;
   * изменение размера файлов;
   * неожиданное значительное увеличение количества файлов на диске;
   * существенное уменьшение размера свободной оперативной памяти;
   * частые зависания и сбои в работе компьютера.
2. **Существуют ли признаки, однозначно указывающие на присутствие в системе вируса?**

Указания антивирусных программ.

1. **Всегда ли, нестандартные «действия» компьютера указывают на наличие в системе вируса?**

Следует отметить, что все вышеперечисленные признаки, необязательно вызываются присутствием в системе вируса, и могут быть следствием других причин. Например, изменением настроек операционной системы, окончанием срока работы демонстрационной версии прикладной программы, заменой некоторых файлов при установке нового пакета и т.д. Поэтому, в случае странного поведения компьютера и не нахождения инфекции антивирусом, сначала рекомендуется просмотреть настройки операционной системы и только после этого обращаться к специалистам.

1. **В чем заключается суть компьютерных мистификаций?**

К категории «компьютерных мистификаций» относятся заведомо ложные сообщения о новых, ранее неизвестных, компьютерных вирусах. В таких сообщениях пользователей «информируют» о том, что в сетях Internet появился новый вирус, распространяющийся в письмах и (или) через WWW сайты, и уничтожающий всю информацию на пораженных компьютерах.

1. **Существуют ли способы, позволяющие отличать компьютерные мистификации от настоящих вирусов?**

Если пользователь не уверен в том, что сообщение можно отнести к категории компьютерных мистификаций, он может обратиться на WWW-сервера антивирусных компаний или посетить Web-страницы, специально посвященные компьютерным мистификациям. В этих местах можно найти всю исчерпывающую информацию по возникшей проблеме.

1. **Какую опасность представляют компьютерные мистификации?**

Дезинформация неразумных пользователей с различными целями.

1. **Всегда ли безоговорочно следует доверять сообщениям антивирусных пакетов?**

Нет, порой у алгоритмов выявления подозрительной активности случаются ложно-положительные срабатывания, особенно если используется программа, встраивающаяся в другую программу или редактирующая её память.

1. **Почему антивирусы иногда могут не обнаруживать вирусы, или находить их там, где их никогда не было?**

Причин этому может быть много. Чаще всего это неудачный выбор или неправильное использование антивирусных программ, а также несвоевременное обновление баз данных антивирусных программ. Может быть и другая причина – изощренные вирусы, способные обмануть даже совершенные антивирусные программы..

1. **Можно ли устанавливать на компьютере два и более антивирусов? Ответ обосновать.**

Такой ситуации желательно избегать. Во-первых, одновременное функционирование нескольких антивирусов неизбежно приводит к конфликту из-за системных ресурсов. Каждый антивирус стремится контролировать такие операции, как установка сетевых соединений или чтение файлов, и, перехватывая нужные функции Windows, антивирусы мешают друг другу. Последствия могут быть различными: от простого замедления системы до ее полной неработоспособности или, что тоже очень плохо, неработоспособности обоих антивирусов.

Кроме того, очень часто антивирусы разных производителей детектируют те или иные файлы друг друга как вредоносные. Это не злой умысел, а следствие того, что антивирус в процессе нормальной работы выполняет много «подозрительных» (для других антивирусов) операций вроде контроля других приложений. На самом деле файлы антивируса безопасны, и все производители стараются оградить пользователя от ложных срабатываний, но иногда «белые списки» оказываются неполны.

1. **Насколько сильно регулярное обновление антивирусных баз данных влияет на безопасность работы пользователя?**

Регулярно обновлять антивирусные базы критично для безопасности компьютера, потому что в Интернете регулярно появляются десятки новых вирусов.

1. **Следует ли обращать особое внимание при выборе антивируса, на количество обнаруживаемых им вирусов?**

Нет, этот показатель является чисто коммерческой уловкой, так как основывается на всех, когда-либо существовавших вирусах, большинство из которых более не встречаются.

1. **Что вы можете рассказать про аппаратные средства антивирусной защиты?**

В 1999 году компания Calluna plc., специализирующаяся на производстве аппаратных средств безопасности для ПК, начала поставки в Россию платы “Hardwall”, предназначенной для защиты данных от вирусов. Плата “Hardwall” создает индивидуальное аппаратное заграждение для пользователя Internet, при этом область диска в которой могут производиться постоянные изменения, ограничивается до одного сектора. По заявлению разработчиков плата способна не только выявлять и обезвреживать вирусы, ограничивая повреждения, но и предупреждать пользователя о попытках взломать систему.

Так же появилась информация об аппаратно реализованных антивирусах, работающих через параллельный порт компьютера (LPT). Ожидается, что их надежность заметно превзойдет лучшие программные реализации.

1. **Можно ли решить вопрос антивирусной безопасности использованием только аппаратных средств?**

При любой аппаратной реализации, на жестком диске компьютера остаются области незащищенных данных, например системные области или программные драйвера, которые должны обеспечить работу той же самой аппаратной реализации антивирусной защиты данных. А в этом случае всегда остается шанс, что в компьютер может проникнуть вирус. Поэтому необходимо помнить, что антивирусные средства должны применяться комплексно и только такая комплексная защита с использованием надежного антивирусного ревизора, фагов, и аппаратной поддержки способна обеспечить максимальную безопасность.

1. **Как вы считаете, повышает ли уровень безопасности использование аппаратных средств антивирусной защиты?**

Да, разумеется, каждый новый слой защиты повышает общий уровень безопасности.

1. **Существует ли разница при использовании антивирусных средств различных производителей?**

Разумеется. Разные антивирусные программы используют разные наборы алгоритмов, одни потребляют больше ресурсов системы, другие – меньше.

1. **Всегда ли безоговорочно следует доверять сообщениям антивирусных пакетов?**

Никакое программное обеспечение не в силах защитить ресурсы компьютеров от всех существующих и вновь появляющихся вирусов.

1. **Насколько целесообразно разрабатывать специальную антивирусную стратегию защиты данных?**

Становится очевидным, что предотвратить – дешевле, чем лечить; при этом уровень экономически допустимых затрат на приобретение и внедрение антивирусной системы можно оценить в размере 5 - 10% от потенциальных потерь при вирусной атаке.

1. **Существуют ли ситуации, когда ликвидация последствий вирусной атаки будет проще и дешевле чем ее предотвращение?**

Скорее всего, да. Например, на домашнем компьютере, не содержащем никаких важных данных.

1. **Необходимо ли при внедрении антивирусной защиты данных использовать административные меры, или вопрос можно решить только техническими средствами?**

Следующий, не менее важный вопрос, – проблема администрирования и затраты, связанные с этим. Нетрудно подсчитать, сколько времени уходит у системных администраторов на установку и конфигурирование антивирусной защиты на каждом компьютере сети, а впоследствии – на обновление баз данных вирусных сигнатур. Ясно, что только сетевая антивирусная система, имеющая нормальные средства централизованной инсталляции, конфигурирования и обновления может снять все эти неоправданные затраты. Теперь уже имеет смысл говорить о разработке стратегии антивирусной безопасности. Прежде всего, определим цель стратегии антивирусной безопасности. Это – эффективное предотвращение заражения вирусами информационной системы организации. Другими словами, не максимально быстрое обнаружение и удаление появляющихся вирусов, а создание условий, при которых уже само появление вируса на пользовательской машине или, еще хуже, на сервере будет рассматриваться как ЧП.

В основе всей стратегии антивирусной безопасности организации должны лежать следующие разделы: политика антивирусной безопасности, план работ по обеспечению антивирусной безопасности, порядок действий в критических ситуациях.

1. **Насколько сильно отличается стратегия защиты информации для персонального компьютера и локальной сети?**

Порядок действий в критических ситуациях, т.е. в тех случаях, когда вирусная инфекция в силу каких-либо причин все же попала в систему, разрабатывается после завершения создания и внедрения предыдущих этапов. Такая ситуация может никогда и не возникнуть, но сам факт создания документа вселит в персонал уверенность, что даже в самых сложных случаях вопросы будут решаться оперативно и продуманно.

Прежде всего, в специальном корпоративном документе должна быть отражена классификация чрезвычайных ситуаций. Вряд ли стоит относить к чрезвычайным ситуациям самые простые случаи - обнаружение антивирусной системой инфекции на рабочей станции с моментальным отключением ее от сети (естественно, когда антивирусная система это предусматривает). Однако обнаружение вируса или вирусоподобных признаков на сервере (например, изменение контрольных сумм сразу нескольких файлов) или в архиве - это уже ЧП. В классификации надо отразить и степень поражения системы: насколько глубоко инфекция успела проникнуть в систему.

В зависимости от класса ситуации предусматривается тот или иной порядок работы:

* немедленное предотвращение распространения инфекции;
* документирование (фиксация) состояния системы, которое будет в дальнейшем использовано для анализа ситуации и поиска причин происшедшего;
* определение степени поражения системы. Это выполняется только самыми квалифицированными специалистами;
* уничтожение вирусной инфекции;
* восстановление работоспособности системы или ее части.

Это, что касается крупных компаний, имеющих большие вычислительные системы, естественно, что для обычного пользователя домашнего персонального компьютера, не включенного в локальную сеть, появление вируса хотя и неприятно, но не грозит потерей десятков тысяч долларов. Поэтому рекомендации, по выбору и настройке антивирусных программ, для такого пользователя будут выглядеть несколько иначе.

* оснастить компьютер современными антивирусными пакетами, такими как Antiviral Toolkit Pro, Doctor Web или какими-либо другими;
* проверить все жесткие диски компьютера полифагом, имеющимся в антивирусном пакете;
* вылечить или удалить с компьютера все обнаруженные, зараженные файлы;
* в случае изменения системных областей диска (главной загрузочной записи и загрузочной записи) использовать ревизоры, которые позволяют восстановить их, даже в том случае если не известно, какой именно вирус там находится;
* настроить антивирусный монитор на автоматический запуск при загрузке компьютера;
* для обеспечения большей безопасности использование полифагов необходимо сочетать с повседневным использованием ревизоров диска и антивирусных мониторов;
* постоянно обновлять базы данных антивирусных программ сигнатурами новых вирусов;
* при переносе на свой компьютер файлов в архивированном виде проверять их сразу же после разархивирования антивирусной программой;
* периодически (раз в месяц) проверять на наличие вирусов, жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков;
* перед считыванием с дискет информации, записанной на других компьютерах, проверять их на наличие вирусов антивирусными программами своего компьютера;
* использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;
* обязательно делать архивные копии ценной информации;

1. **Насколько давно существует уголовная ответственность за преступления в сфере информационных технологий?**

Тем не менее, относительно недавно (1996), в уголовном кодексе Российской Федерации появилась целая глава, посвященная преступлениям в сфере информационных технологий (глава 27 уголовного кодекса). Помимо нескольких других статей там содержится и статья, касающаяся вирусов. Она называется – «Создание, использование и распространение вредоносных программ для ЭВМ».

1. **Какой раздел уголовного кодекса посвящен преступлениям в сфере информационных технологий?**

N 63-ФЗ (Глава 28)

1. **За какие преступления в сфере информационных технологий предусмотрена ответственность в уголовном кодексе Российской Федерации?**

* создание вредоносной программы для ЭВМ;
* внесение вредоносных изменений в существующие программы;
* использование вредоносной программы для ЭВМ;
* распространение вредоносной программы для ЭВМ.

1. **Существуют ли причины препятствующие соблюдению закона в данной области? Являются ли эти причины объективными?**

Примером может быть, потеря важной финансовой информации в результате сбоя бухгалтерской программы. И здесь уже сложно говорить об умышленных или неумышленных действиях оператора, работавшего с базой данных, или программиста, который не мог учесть всех условий работы программы, в том числе и в новых операционных системах.

1. **Насколько реальным является соблюдение закона в сфере информационных технологий в нынешних условиях?**

Нереальным. Пиратство – наше все.

1. **Что необходимо предпринять чтобы соблюдение закона стало реальным?**

З\П от 100 000р.