Министерство образования Республики Беларусь

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ  
«ГРОДНЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМЕНИ ЯНКИ КУПАЛЫ»

Кафедра лазерной физики и спектроскопии

**РЕФЕРАТ**по курсу «Методика преподавания информатики» на тему:

«Вредоносное программное обеспечение и защита информации»

Гродно 2010

# Оглавление

[Оглавление 2](#_Toc280304089)

[1. .Краткие сведения о вирусах и антивирусах 3](#_Toc280304090)

[1. 1 Исторические данные о первых вируса, антивирусах и вирусных эпидемиях 3](#_Toc280304091)

[1. 2.Вирусы. Антивирусы. И их классификация 10](#_Toc280304092)

[2. Методические разработки 18](#_Toc280304093)

[Глоссарий 27](#_Toc280304094)

[Литература 30](#_Toc280304095)

# .Краткие сведения о вирусах и антивирусах

## 1 Исторические данные о первых вируса, антивирусах и вирусных эпидемиях

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Давайте рассмотрим с чего это начиналось.

**1945 год.** Рождениетермина. Вице-адмирал ВМФ США Грейс Мюррей Хоппер, руководившая информационным отделом военно-морского штаба, столкнулась с тем, что электронно-счетные машины (прототипы современных компьютеров) начали давать сбои. Причиной стал мотылек, залетевший внутрь одного из реле. Адмирал назвала эту проблему "жуком" , используя термин, применявшийся физиками США и Великобритании с конца XIX века (он обозначал любого рода неполадку в электрических устройствах). Адмирал также впервые использовала термин "избавление от жука" , который ныне применяется для описания действий, ставящих своей целью устранение неполадок в компьютере.

**1949 год.** Ученый Джон фон Науманн разработал математическую теорию создания самовоспроизводящихся программ. Это была первая теория создания компьютерных вирусов, вызвавшая весьма ограниченный интерес у научного сообщества.

**Примерно 1950 год.** Математики, работающие в исследовательском подразделении корпорации Bell, придумали игру: они создают программы, отбирающие друг у друга компьютерное пространство. Это были предтечи вирусов.

**1963 год.** Руководитель компьютерной лаборатории Агентства Передовых Исследовательских Проектов Джон Ликлидер предложил первую детально разработанную концепцию компьютерной сети.

**1969 год.** ARPA создало компьютерную сеть ARPANET. К ней подключаются компьютеры ведущих, в том числе и невоенных, лабораторий и исследовательских центров США.

**Конец 1960-х годов.** Появление первых вирусов. В ряде случаев это были ошибки в программах, приводившие к тому, что программы копировали сами себя, засоряя жесткие диски компьютеров, что снижало их производительность, однако считается, что в большинстве случаев вирусы сознательно создавались для разрушения. Вероятно, первой жертвой настоящего вируса, написанного программистом для развлечения, стал компьютер Univax 1108. Вирус назывался Pervading Animal и заразил только один компьютер, на котором и был создан.

**1974 год.** Создана сеть Telenet — коммерческая версия ARPANET.

**1975 год.** Через Telenet распространяется сетевой вирус "The Creeper". Для противодействия ему написана антивирусная программа "The Reeper".

**1979 год.** Инженеры из исследовательского центра компании Xerox создали компьютерный "червь" (worm).

**1981 год.** Ричард Скрента написал один из первых загрузочных вирусов для ПЭВМ Apple II— ELK CLONER. Другие вирусы для Apple II были созданы студентом Техасского университета A&M Джо Деллинджером в 1981 году. Они были рассчитаны на операционную систему MS-DOS3. Вторая версия этого вируса «ускользнула» от автора и начала распространяться по университету. Ошибка в вирусе вызывала подавление графики популярной игры под названием CONGO, и в течение нескольких недель все («пиратские») копии этой игры перестали работать. Для исправления ситуации автор запустил новый, исправленный вирус, предназначенный для «замещения» предыдущей версии.

**983 год.** Ученый Фред Кохен из Университета Северной Каролины вводит термин "компьютерный вирус".

**1984 год.** Писатель Уильям Гибсон вводит понятие "киберпространство"

**1985 год.**Том Нефф. начал распространять по различным BBS список «Грязная дюжина— список опасных загружаемых программ» , в котором были перечислены известные на тот момент программы-вандалы. В дальнейшем этот список, включающий большинство выявленных троянских программ и «взломанные» или переименованные копии коммерческого программного обеспечения для MS-DOS, стал широко известен под кратким названием «грязная дюжина» .

**1986 год.** Создан вирус для IBM PC — "The Brain". Два брата-программиста из Пакистана написали программу, которая должна была "наказать" местных "пиратов", ворующих ПО у их фирмы. В программе значились имена, адрес и телефоны братьев. Однако неожиданно для всех "The Brain" вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Успех вируса был обеспечен тем, что компьютерное сообщество было абсолютно не готово к подобному развитию событий.

**1987 год.** Программист Ральф Бергер написал книгу об искусстве создания вирусов и борьбы с ними — "Компьютерные вирусы. Болезнь высоких технологий".

**1988 год.** 23-летний американский программист создал "червя", поразившего 6000 компьютеров ARPANET. И впервые суд приговорил автора вируса к $10 тыс. штрафа и 3 годам испытательного срока.

**1989 год.** ARPANET официально переименован в Интернет. Создано антивирусное ПО для IBM PC. В том же году появился "троянский конь" AIDS. Вирус делал недоступной всю информацию на жестком диске и высвечивал на экране лишь одну надпись: "Пришлите чек на $189 на такой-то адрес". Автор программы был арестован в момент обналичивания денег и осужден за вымогательство. Создан вирус для противодействия антивирусному ПО ("Темный Мститель"). Он заражал новые файлы, пока антивирусная программа проверяла жесткий диск компьютера.

Клифф Столл , сотрудник Lawrence Berkeley National Laboratory опубликовал книгу "Кукушкины яйца" (в которой предостерегал, что всемирная компьютерная сеть может служить не только целям добра, но и активно использоваться военными, преступниками и хулиганами. Столл рекомендовал заблаговременно принять меры для недопущения подобного развития событий.

**1990 год глобализация проблемы вирусов**.Компьютерный журнал PC Today разослал подписчикам инфицированную дискету. В начале года выходит первый полиморфный вирус— Chameleon. Данная технология была быстро взята на вооружение и в сочетании со стелс-технологии и бронированием позволила новым вирусам успешно противостоять существующим антивирусным пакетам. Во второй половине 1990 года появились два стелс-вируса— Frodo и Whale. Оба вируса использовали крайне сложные стелс-алгоритмы, а 9-килобайтный Whale к тому же применял несколько уровней шифровки и антиотладочных приёмов.

В Болгарии открывается первая в мире специализированная BBS, с которой каждый желающий может скачать свежий вирус. Начинают открываться конференции Usenet по вопросам написания вирусов. В этом же году выходит «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига. На проблему противостояния вирусам были вынуждены обратить внимание крупные компании — выходит Symantec Norton Antivirus.

**1991 год.** Написана программа, предназначенная исключительно для создания вирусов — VCS vl.O. Начало 1991 года отмечено массовой эпидемией полиморфного загрузочного вируса Tequila. Летом 1991 появился первый link-вирус, который сразу же вызвал эпидемию.

**1992 год**. Известен как год появления первых конструкторов вирусов для PC— VCL (для Amiga конструкторы существовали и ранее), а также готовых полиморфных модулей и модулей шифрования. Начиная с этого момента, каждый программист мог легко добавить функции шифрования к своему вирусу. Кроме того, в конце 1992 появился первый вирус для Windows 3.1— WinVer.

**1993 год.** Вирус "SatanBug" поражает сотни компьютеров в столице США, Вашингтоне. Страдают даже компьютеры Белого дома. ФБР арестовало автора, — им оказался 12-летний подросток.

Зафиксировано появление "бомб замедленного действия" — вирусов, которые проникают в компьютеры и активизируются по достижении определенной даты. Это мог быть день рождения Мао Цзе Дуна, Новый год и так далее. Первой от подобного вируса пострадала газета "The New York Times".

**1994 год.** В Великобритании, США, Норвегии арестованы несколько авторе в вирусов. Они отделываются штрафами.

**1995 год.** Корпорация Microsoft выпустила бета-версию ОС Windows 95 на дискетах, зараженных вирусом. Появление макровирусов, рассчитанных на поражение программной платформы определенной программы. Макровирус Concept поразил программу MS Word.

**1998 год.** Два калифорнийских подростка создали вирус, который поразил более 500 компьютеров Пентагона. После этого инцидента в Министерстве обороны США пришли к выводу, что атаки в киберпространстве не менее опасны, чем традиционные виды ведения боевых действий, и создали термин "гонка компьютерных вооружений".

**1999 год.** Вирус "Melissa" вызвал эпидемию мирового масштаба, поразил десятки тысяч компьютеров и нанес ущерб в $80 млн. После этого инцидента в мире начался обвальный спрос на антивирусные программы. В 2002 году автор вируса "Melissa" — 33-летний программист Дэвид Смит (David L. Smith) приговорен к 20 месяцам тюремного заключения.

**2000 год, май.** Рекорд вируса "Melissa" побил вирус "I Love You!", поразивший миллионы компьютеров в течение нескольких часов. Расследование показало, что вирус создал филиппинский студент, который не был осужден из-за отсутствия соответствующих законов в законодательстве Филиппин. В том же году подписано первое международное соглашение о противодействии компьютерным вирусам. Несколько десятков популярных сайтов (в том числе "Yahoo!", "eBay", "Amazon") на некоторое время были выведены из работы в результате DOS-атаки (настолько большая перегрузка Интернет-сервера запросами на обслуживание, что тот вынужден отказывать нормальным пользователям). Вирусом были заражены десятки тысяч компьютеров, которые и "выбили" пострадавшие сайты из Сети. Атаку организовали с компьютеров учебного центра Калифорнийского университета, однако злоумышленники остались необнаруженными.

**2001 год.** 20-летний голландец Ян Де Вит был приговорен к 150 часам исправительных работ за создание вируса "Anna Kournikova". Суд пришел к выводу, что он не может точно определить размер ущерба, который нанесла "Anna Kournikova" экономике Нидерландов. У Де Вита также была конфискована коллекция из 7,5тыс. вирусов. Де Вит заявил суду, что не имел представления, что написанная им программа окажется вирусом и нанесет кому-либо ущерб.

**2002 год.** Вирус поразил 13 узловых Интернет-серверов, обеспечивающих функционирование Всемирной Сети. Аналитики предупреждают, что хорошо подготовленная и проведенная компьютерная атака может на недели уничтожить Интернет.

**2003 год.** Рекорды быстроты распространения побил червь "Slammer", заразивший 75 тыс. компьютеров за 10 минут. Вирус поразил компьютеры Госдепартамента США, где повредил базу данных. Консульства США по всему миру вынуждены были на 9 часов прервать процесс выдачи виз. 22-летний Саймон Вэллор приговорен британским судом к двум годам тюремного заключения за создание вирусов "Gokar", "Redesi" и "Admirer", которые инфицировали 27 тыс. компьютеров в 42странах мира.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

# 2.Вирусы. Антивирусы. И их классификация

**Вредоносной программой** называется любое программное обеспечение, предназначенное для получения несанкционированного доступа к информации, хранимой на компьютере, с целью причинения вреда владельцу информации, хранимой на компьютере, с целью причинения вреда владельцу информации или владельцу компьютера.

**Компьютерный вирус** - программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере. Или ***компьютерный вирус –*** это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их.

* **Признаки заражения:**
* 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;
* Неожиданное значительное увеличение количества файлов на диске;
* Существенное уменьшение размера свободной оперативной памяти;
* Вывод на экран непредусмотренных звуковых сигналов;
* Частые зависания и сбои в работе компьютера.
* **Схема работы компьютерных вирусов:**
* ***Заражение.***

Происходит при запуске инфицированной программы или при обращении к носителю, имеющему вредоносный код в системной области; обычно код вируса сначала поступает в оперативную память работающего компьютера, откуда он копируется на запоминающие устройства.

* ***Размножение.***

Вирусный код может воспроизводить себя в теле других программ. Происходит как серия последовательных заражений; в первую очередь поражаются файлы самой операционной системы, чем чаще срабатывает механизм, тем больше файлов поражается.

* ***Атака.***

Последняя фаза развития вируса; во время атаки вирус производит более или менее разрушительные действия. После создания достаточного числа копий программный вирус начинает осуществлять разрушение: нарушение работы программ и ОС, удаление информации на жестком диске, самые разрушительные вирусы вызывают форматирование жесткого диска. Некоторые вирусы могут уничтожать данные, в этом случае требуется замена микросхемы (хотя считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение ПК).

* **Классификация компьютерных вирусов:**
* по среде обитания;
* по способу заражения;
* по воздействию;
* по особенностям алгоритма.

***По среде обитании:***

* *файловые вирусы.*

Внедряются в файлы, имеющие расширение COM и EXE. Внедряются в программу и активизируются при их запуске. После запуска заражённой программы вирусы находятся в оперативной памяти компьютера и могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.

* *загрузочные вирусы.*

Располагаются в служебных секторах носителей данных и поступают в оперативную память только при загрузке компьютера с этого носителя. Внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска.

* *файлово-загрузочные вирусы.*

Заражают файлы и загрузочные сектора дисков.

* *сетевые вирусы.*

Обитают только в оперативной памяти компьютеров и не копируют себя на носители данных. Распространяются по различным компьютерным сетям. Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключенных к этой сети. Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.

* *Макровирусы.*

Заражают файлы документов, например, текстовых документов. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового документа.

***По способу заражения*** *:*

* ***Резидентные****.*

При заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения

* ***Нерезидентные*** *.*

Не заражают оперативную память и активны ограниченное время.

***По воздействию*** *.*

* ***Неопасные****.*

Не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках. Занимаются только размножением.

* ***Опасные*** *.*

Приводят к различным нарушениям в работе компьютера. Беспокоят неожиданными сообщениями, экранными и звуковыми эффектами.

* ***Очень опасные****.*

Могут приводить к потере программ, данных, стиранию информации в системных областях дисков.

***По особенностям алгоритма*** *.*

* ***Паразиты****.*

Не изменяют содержимое файлов и секторов, легко обнаруживаются.

* ***Черви*** *.*

Вычисляют адреса сетевых компьютеров и отправляют по ним свои копии.

* ***Стелсы****.*

Перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области.

* ***Мутанты****.*

Содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую.

* ***Трояны****.*

Не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему.

* **Правила защиты от компьютерных вирусов**:
* Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ
* Перед считыванием информации с дискет проверяйте их на наличие вирусов
* Всегда защищайте свои дискеты от записи при работе на других компьютерах
* Делайте архивные копии ценной для вас информации
* Не оставляйте дискету в дисководе
* Не используйте программы, поведение которых непонятно
* **Методы борьбы с компьютерными вирусами:**

1. Резервное копирование всех программ, файлов и системных областей дисков на дискеты, чтобы можно было восстановить данные в случае вирусной атаки. Создание системной и аварийной дискеты.
2. Ограничение доступа к машине путем введения пароля, администратора, закрытых дисков.
3. Использование только лицензионного программного обеспечения, а не пиратских копий, в которых могут находиться вирусы.
4. Проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети.
5. Применение антивирусных программ и обновление их версий.
6. Периодическая проверка компьютера на наличие вирусов при помощи антивирусных программ.

**Антивирусные программы** – это программы для обеспечения комплексной защиты данных на компьютере от вредоносных программ и способов их проникновения на компьютер. К наиболее популярным антивирусным программам относятся: Avast, NOD32, Антивирус Касперского, Dr. Web, Norton Antivirus, Вирус Блокада.

* **Классификация антивирусного программного обеспечения**
* Сканеры (детекторы)
* Мониторы
* Ревизоры

***Сканеры***

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.

**Примеры программ-сканеров**

* ***Aidstest Дмитрия Лозинского*** умеет обнаруживать около 2000 вирусов
* ***Сканер антивирусного пакета Евгения Касперского AntiviralToolkitPro*** распознает по сигнатурам более 10.000 вирусов
* ***База сигнатур антивирусного сканера NortonAntiVirus*** распознает более 8.000 вирусов

***Мониторы***

Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии.

**Примеры программ-мониторов**

* Вместе с антивирусным пакетом ***AntiviralToolkidPro (AVP),*** созданным фирмой Е. Касперского поставляется резидентрый монитор ***Antiviral*** ***Monitor***. Он позволяет обнаружить и сообщить обо всех проявлениях, которые могут быть вызваны компьютерными вирусами.
* В комплект ***McAfee*** ***Virus*** ***Scan*** входит резидентный монитор, позволяющий постоянно контролировать работу компьютера.
* В состав комплекта ***Norton*** ***Antivirus*** входит приложение ***Norton*** ***AntiVirus*** ***Auto***-***Protect***. Кроме проверки запускаемых файлов ***Norton*** ***AntiVirus*** ***Auto***-***Protect*** выполняет все функции обычного резидентного монитора, позволяя при этом пользователям сделать установки случаев, в которых необходимо сообщать о подозрительном действии.
* В комплекте антивируса ***DrWeb*** входит монитор ***SpIDer*** ***Guard***, который перехватывает обращения к файлам и системным областям дисков, осуществляя проверку на наличие в них компьютерных вирусов «на лету».

***Ревизоры***

Программы—ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.

**Примеры программ-ревизоров**

* Простейшая программа-ревизор ***MicrosoftAnti-Virus*** входит в состав операционной системы MS-DOS.
* Более известна программа-ревизор ***Adinf***, созданная Дмитрием Юрьевичем Мостовым.

# Методические разработки

**1.Тест. «Вирусы и антивирусные программы»**

1. Что такое компьютерный вирус?

1. Прикладная программа
2. Системная программа
3. Программа, выполняющая на компьютере несанкционированные действия
4. База данных.

2. Компьютерным вирусом является

1. Программа проверки и лечения дисков
2. Любая программа, созданная на языках низкого уровня
3. Программа, скопированная с плохо отформатированной дискеты
4. Специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью " размножаться "

3. Заражение компьютерными вирусами может произойти в процессе ...

1. Работы с файлами
2. Форматирования дискеты
3. Выключения компьютера
4. Печати на принтере

4. Основные типы компьютерных вирусов:

1. Аппаратные, программные, загрузочные
2. Программные, загрузочные, макровирусы
3. Файловые, программные, макровирусы

5. Что называется вирусной атакой?

1. Неоднократное копирование кода вируса в код программы
2. Отключение компьютера в результате попадания вируса
3. Нарушение работы программы, уничтожение данных, форматирование жесткого диска

6. Какие существуют методы реализации антивирусной защиты?

1. Аппаратные и программные
2. Программные, аппаратные и организационные
3. Только программные

7. Какие существуют основные средства защиты?

1. Резервное копирование наиболее ценных данных
2. Аппаратные средства
3. Программные средства

8. Какие существуют вспомогательные средства защиты?

1. Аппаратные средства
2. Программные средства
3. Аппаратные средства и антивирусные программы

9. На чем основано действие антивирусной программы?

1. На ожидании начала вирусной атаки
2. На сравнении программных кодов с известными вирусами
3. На удалении зараженных файлов

10. Какие программы относятся к антивирусным

1. AVP, DrWeb, Norton AntiVirus
2. MS-DOS, MS Word, AVP
3. MS Word, MS Excel, Norton Commander

**Ключ**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Ответ | 3 | 4 | 1 | 2 | 3 | 2 | 3 | 3 | 2 | 1 |

**2.Практическое задание. «Проверка объектов на наличие вирусов»**

***Цель работы:*** формирование практических навыков при работе с антивирусной программой Антивирус Касперского.

* Запустите антивирусную программу Антивирус Касперского:
* откройте Главное меню, нажав на кнопку Пуск
* выберите пункт Программы
* в пункте Программы выберите пункт Антивирус Касперского 5.0 для Windows
* в раскрывшемся подменю выберите пункт Антивирус Касперского
* Протестируйте 2 дискеты и проанализируйте результат:
* вставьте дискету 1 в дисковод
* на вкладке Защита выберите команду Проверить съемные диски
* после чего будет открыто окно, где произведется проверка диска
* в окне Проверка на странице Статистика можно видеть результат тестирования
* нажмите кнопку Закрыть
* аналогичным образом проверьте дискету 2
* Протестируйте дискету следующим образом:
* откройте Мой компьютер
* вызовите контекстное меню Диска 3,5
* выберите команду Проверить на вирусы
* Протестируйте папку **Мои документы**:
* на вкладке Защита выберите команду Проверить объекты
* после чего будет открыто окно Выбор объектов для проверки
* в списке объектов выберите папку Мой компьютер
* нажмите кнопку Проверить
* в окне Проверка на странице Статистика можно видеть результат тестирования

нажмите кнопку Закрыть

* Закройте антивирусную программу.

**3.«Компьютерные вирусы и антивирусные программы».**

*Разгадайте кроссворд и запишите ключевое слово, находящееся в вертикальной строке кроссворда:*

По горизонтали:

1. Часть ПК, где происходит обработка информации.
2. Русское название распространенного сетевого вируса
3. Наиболее частый "переносчик" инфекции в ПК.
4. Программа - .... "Doctor Web".
5. Фамилия создателя "Doctor Web".
6. Взломщик защищенной информации.
7. Вредоносная программа.
8. "Невидимка" на ПК.

По вертикали:

1. Общее название программ, защищающих ПК от " непрошенных гостей".

***Таблица 1***

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | 99 |  |  |  |  |
|  |  |  |  | 11 |  | ; |  |  |  |  |
|  | 22 |  |  |  |  |  |  |  |  |  |
| 33 |  |  |  |  |  |  |  |  |  |  |
| 4 |  | 44 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | 55 |  |  |  |  |  |  |  |  |
|  | 66 |  |  |  |  |  |  |  |  |  |
|  |  | 77 |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 88 |  |  |  |  |  |

Ответы на кроссворд

***Таблица 2***

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | 99 |  |  |  |  |
|  |  |  |  | 1 | П | А | М | Я | т | Ь |
|  | 22 | тТ | рР | оО | яЯ | нН |  |  |  |  |
| 33 | дД | иИ | сС | кК | еЕ | тТ | аА |  |  |  |
|  |  | 44 | пП | оО | лЛ | иИ | аФ | гА | гГ |  |
|  |  |  |  |  |  | вВ |  |  |  |  |
|  |  | 55 | дД | аА | нН | иИ | лЛ | оО | вВ |  |
|  | 66 | хХ | аА | кК | еЕ | рР |  |  |  |  |
|  |  | 77 | вВ | И и | рР | уУ | сС |  |  |  |
|  |  |  |  |  | 88 | С с | тТ | еЕ | лл | С |

**4. Выполнение теста по теме: "Компьютерные вирусы. Антивирусные программы"**

1. Выберите правильный ответ из предложенных вариантов. Что такое компьютерный вирус?

1. Прикладная программа.
2. Системная программа.
3. Программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.
4. База данных.

4. Выберите правильный ответ из предложенных вариантов. Какие существуют вспомогательные средства защиты?

1. Аппаратные средства.
2. Программные средства.
3. Аппаратные средства и антивирусные программы.

5. Выберите правильный ответ из предложенных вариантов. На чем основано действие антивирусной программы?

1. На ожидании начала вирусной атаки.
2. На сравнение программных кодов с известными вирусами.
3. На удалении зараженных файлов.

6. Выберите правильный ответ из предложенных вариантов. Какие программы относятся к антивирусным?

1. AVP, DrWeb, Norton AntiVirus.
2. MS-DOS, MS Word, AVP.
3. MS Word, MS Excel, Norton Commander.

7. Вставь пропущенное слово, определив тип антивирусной программы:

Антивирусные программы: - это программы, перехватывающие "вирусоопасные" ситуации и сообщающие об этом пользователю.

8. По предложенному описанию определите тип вируса.

Заражают файлы документов Word и Excel. Являются фактически макрокомандами, которые встраиваются в документ.Макровирусы

9. Компьютерным вирусом называется:

1. средства для сжатия дисков и работы сними
2. программный код, способный выполнить на компьютере несанкционированные действия
3. совершенные программы, которые нельзя увидеть средствами операционной системы

10. Какова схема работы компьютерных вирусов?

1. заражение - размножение - атака
2. размножение - заражение - атака
3. атака - размножение - заражение
4. размножение - заражение

11. Заражение происходит при:

1. загрузке операционной системы
2. включении питания
3. запуске инфицированной программы или при обращении к носителю, имеющему вредоносный код в системной области
4. загрузке непроверенного носителя информации

12. Вирусы, обитающие только в оперативной памяти компьютеров и не копирующие себя на носители данных, называется:

1. сетевыми
2. макро вирусами
3. файловыми
4. загрузочными

13. Вирусы, способные обитать в файлах документов:

1. сетевыми
2. макровирусами
3. файловыми
4. загрузочными

14. Вирусы, располагающиеся в служебных секторах носителей данных и поступающие в оперативную память только при загрузке компьютера:

1. сетевыми
2. макро вирусами
3. файловыми
4. загрузочными

15. Независимые компоненты для Windows и Dos, предназначенные для антивирусной проверки дисков компьютера:

1. AVP Инспектор
2. AVP Монитор
3. AVP сканер
4. AVP Центр Управления

16. Оболочка, предназначенная для организации установки и обновления компонентов пакета, для автоматического запуска задач по расписанию и контроля результатов

1. AVP Инспектор
2. AVP Монитор
3. AVP сканер
4. AVP Центр Управления

17. Удаление вируса называется

1. атакой
2. лечением
3. обеззараживанием
4. макрокомандой

18. Большинство антивирусных программ выявляют вирусы по

1. алгоритмам маскировки
2. образцам их программного кода
3. среде обитания
4. разрушающему воздействию

19. Вирусы, предназначенные не для разрушения, а для фиксирования нажатия клавиш в момент ввода парольных или регистрационных данных и записывать их в невидимый файл

1. сетевые вирусы
2. макро вирусы
3. "троянские кони"
4. вирусы "невидимки"

**5. Выполнение задания по теме: "Компьютерные вирусы. Антивирусные программы"**

Запустите на вашем ПК антивирусную программу. (Какая у Вас установлена программа и как ее запустить, спросите у преподавателя).

Перенесите в тетрадь таблицу и заполните ее.

|  |  |
| --- | --- |
| Название антивирусной программы |  |
| Проверяемый логический или физический диск (диски) |  |
| Всего проверено файлов |  |
| Число зараженных файлов |  |
| Число подозрительных файлов |  |
| Число потенциально опасных, но разрешенных к использованию файлов |  |

## Глоссарий

**Антивирусные программы** – это программы для обеспечения комплексной защиты данных на компьютере от вредоносных программ и способов их проникновения на компьютер. К наиболее популярным антивирусным программам относятся: Avast, NOD32, Антивирус Касперского, Dr. Web, Norton Antivirus, Вирус Блокада.

**Вредоносная программа –** этолюбое программное обеспечение, предназначенное для получения несанкционированного доступа к информации, хранимой на компьютере, с целью причинения вреда владельцу информации, хранимой на компьютере, с целью причинения вреда владельцу информации или владельцу компьютера.

**Загрузочные вирусы -** это вирусы, которыерасполагаются в служебных секторах носителей данных и поступают в оперативную память только при загрузке компьютера с этого носителя. Внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска.

**Компьютерный вирус** - программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере.

**Макровирусы -** это вирусы, которыезаражают файлы документов, например, текстовых документов. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового документа.

**Мониторы** -антивирусное программное обеспечение, которое постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии.

**Мутанты** - это вирусы, которыесодержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую.

**Неопасные вирусы** *-* это вирусы, которыене мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках. Занимаются только размножением.

**Нерезидентные вирусы -**это вирусы, которыене заражают оперативную память и активны ограниченное время.

**Опасные вирусы -** это вирусы, которыеприводят к различным нарушениям в работе компьютера. Беспокоят неожиданными сообщениями, экранными и звуковыми эффектами.

**Очень опасные** - это вирусы, которыемогут приводить к потере программ, данных, стиранию информации в системных областях дисков.

**Паразиты** *-* это вирусы, которыене изменяют содержимое файлов и секторов, легко обнаруживаются.

**Ревизоры -** антивирусное программное обеспечение, первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.

**Резидентные вирусы -** это вирусы, которыепри заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения

**Сетевые вирусы -** это вирусы, которыеобитают только в оперативной памяти компьютеров и не копируют себя на носители данных. Распространяются по различным компьютерным сетям. Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключенных к этой сети. Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.

**Сканеры** - антивирусное программное обеспечение, принцип работы которых основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.

**Стелы** *-* это вирусы, которыеперехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области.

**Трояны** - это вирусы, которыене способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему.

**Файлово-загрузочные вирусы** *-* это вирусы, которыезаражают файлы и загрузочные сектора дисков.

**Файловый компьютерный вирус –** это вирусы, которыевнедряются в файлы, имеющие расширение COM и EXE. Внедряются в программу и активизируются при их запуске. После запуска заражённой программы вирусы находятся в оперативной памяти компьютера и могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.

**Черви** *-* это вирусы, которыевычисляют адреса сетевых компьютеров и отправляют по ним свои копии.

## Литература

* 1. Информатика 8 класс // Минск « Народная асвета» 2010 г.
  2. Информация, разработки уроков на сайте festival@1september.ru
  3. Патрушина С.М. Информатика.: Учеб. пособие, издание второе. – М.: изд. центр “Март”, 2004.
  4. Информатика. Компьютерные вирусы.: под ред. Островского С.П., №32 август, 2001.
  5. Информатика и информационные технологии. Учебник для 10-11 классов / Н.Д. Угринович. – 3-е изд. – М.: БИНОМ. Лаборатория знаний, 2006. – 511 с.
  6. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации – М.: Академия, 2006
  7. Лесничная И.Г., Миссинг И.В., Романова Ю.Д., Шестаков В.И. Информатика и информационные технологии. – М.: Эксмо, 2006
  8. Хореев П.Б. Методы и средства защиты информации в компьютерных системах – М.: Академия, 2005
  9. Чирилло Д. Защита от хакеров – СПб.: Питер, 2002
  10. Информатика: базовый курс. Под. ред. Симоновича С.В. – СПб.: Питер, 2001.
  11. Эндри Ротбом «ПК для «чайников»». 4-е издание М. 2000.
  12. О.А. Соколова «Поурочные разработки по информатике» – Москва «ВАКО» 2007.
  13. Информатика и информационные технологии (Угринович Н. Д.)