**Тема лекции: "Компьютерные вирусы и антивирусные программы"**

**Цель:**  
*дидактическая:*сформировать понятие компьютерного вируса; ознакомить обучающихся с историей возникновения, видами и типами вирусов, путями заражения ПК вирусами и основными методиками борьбы с вирусами;

*развивающая:* развивать логическое мышление, внимание, память;

*воспитательная:* воспитывать современного человека, который владеет информационной компетентностью и цифровой грамотностью.

**Ход лекции:**

1. Организационный момент (5 мин)
2. Информационная минутка (5 мин).
3. Изучение новой темы (70 мин)
4. Подведение итогов (10 мин)
5. **Что такое компьютерный вирус**
6. Краткая история.
7. **Какой вред наносят вирусы**.
8. **Что указывает на вирусное заражение**.
9. **Какие бывают вирусы**.
10. **Что такое антивирусная программа**
11. **Как защитить компьютер от вирусов**

**1. Организационный момент**

Проверка явки, заполнение классного журнала

**2. Информационная минутка**

•          Сегодня мы с вами проведем необычную информационную минутку. Мы ,6удем  
говорить о болезнях. Скажите, ребята, а как распространяются болезни?  
Ответы детей необходимо прокомментировать: через грязные руки (поэтому руки надо чаще мыть!) или по воздуху (помещение тоже необходимо проветривать!). Так вот, чаще всего разносчиками болезней являются микробы или вирусы.

1. Вот и наш компьютер может заболеть. Вы, наверное, много уже слышали о компьютерных вирусах. Поделитесь, пожалуйста, своим опытом и знаниями.
2. Так что же представляет собой компьютерный вирус?

Основной вывод, который должен сделать учитель после ответов детей: компьютерный вирус — это программа. И распространяются, как правило, вирусы через программы на дискетах. После запуска зараженной программы мы вирус может поразить и "здоровые" программы.

1. Вирусы, как и все другие программы, создаются людьми, причем очень грамотными специалистами. И это тот случай, когда знания одних людей обращаются во вред другим людям. (Можно попросить высказаться детей о том, как они относятся к людям, которые создают программы-вирусы.)
2. Чтобы излечиться от какой-либо болезни, вы принимаете лекарства. Как же пролечить компьютер от вирусов? Есть много разных программ, которые следят за "здоровьем" наших компьютеров. Некоторые из них так и называются — программы-"доктора". И все знают людей, которые создают такие программы: Дмитрий Лозинский, Игорь Данилов и др. И все, кто работает с компьютерами, очень часто им говорят "спасибо": знают они очень много, и их знания служат людям, приносят пользу. А как вы относитесь к таким специалистам? (Выслушать мнение детей.)
3. **Изучение новой темы**

**1. Что такое компьютерный вирус**

|  |
| --- |
| ***Компьютерный вирус* это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.** |

Программа, внутри которой находится вирус, называется **зараженной (инфицированной)**. Когда инфицированная программа начинает работу, то сначала управление получает вирус. Вирус заражает другие программы, а также выполняет запланированные деструктивные действия. Для маскировки вирус активизируется не всегда, а лишь при выполнении определенных условий (время, действие). После того, как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится.

Подобно настоящим вирусам, компьютерные вирусы прячутся, размножаются и ищут возможность перейти на другие ЭВМ.

**2. Краткая история**

**Теория самовоспроизводящихся автоматов**

Что такое компьютерный вирус? Идея компьютерных вирусов впервые обсуждалась в серии лекций математика Джона фон Неймана в конце 1940-х годов; в 1966 году вышла его монография [«Теория самовоспроизводящихся автоматов»](http://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf) – по сути, это мысленный эксперимент, рассматривающий возможность существования «механического» организма – например, компьютерного кода – который бы повреждал машины, создавал собственные копии и заражал новые машины аналогично тому, как это делает биологический вирус.

## Программа Creeper

Как отмечается на сайте Discovery, программа Creeper, о которой часто говорят как о первом вирусе, была создана в 1971 году сотрудником компании BBN Бобом Томасом. По факту, Creeper был создан как тестовая программа, чтобы проверить, возможна ли в принципе самовоспроизводящаяся программа. Оказалось, что в некотором смысле возможна. Заразив новый жесткий диск, Creeper пытался удалить себя с предыдущего компьютера. Creeper не совершал никаких вредоносных действий – он только выводил простое сообщение: "I'M THE CREEPER. CATCH ME IF YOU CAN!" (Я CREEPER. ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ!)

## Вирус Rabbit

Согласно сайту [InfoCarnivore](http://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/" \t "_blank), вирус Rabbit (также известный как Wabbit) был создан в 1974 г. с вредоносной целью и мог самовоспроизводиться. Попав на компьютер, он делал большое количество копий себя, значительно ухудшал работоспособность системы и в итоге приводил к отказу компьютера. Имя («Кролик») было дано вирусу из-за того, что он очень быстро самовоспроизводился.

## Первый троянец

Согласно сайту [Fourmilab](http://www.fourmilab.ch/documents/univac/animal.html" \t "_blank), первый троянец по названием ANIMAL (хотя есть [споры](https://securelist.com/threats/1970s/) относительно того, были ли это действительно троянец или просто вирус) был разработан компьютерным программистом Джоном Уолкером в 1975 г. В то время были очень популярны компьютерные игры, в которых пользователь загадывал какое-нибудь животное, а программа должна была его угадать за 20 вопросов. Уолкер написал одну из таких игр, и она стала популярной. Чтобы поделиться ее со своими друзьями, Уолкер записывал и передавал ее на магнитной ленте. Чтобы упростить эту процедуру, Уолкер создал программу PERVADE, которая устанавливалась на компьютер вместе с игрой ANIMAL. Пока пользователь играл в игру, PREVADE проверял все доступные пользователю директории на компьютере, а затем копировал ANIMAL во все директории, где этой программы не было. Вредоносной цели здесь не было, но ANIMAL и PREVADE подпадают под определение троянца: по сути, внутри программы ANIMAL была запрятана другая программа, которая выполняла действия без согласия пользователя.

## Вирус загрузочного сектора Brain

Brain, первый вирус для IBM-совместимых компьютеров, появился в 1986 году – он заражал пятидюймовые дискеты. Как сообщает Securelist, вирус был написан двумя братьями – Баситом и Амджадом Фаруком Алви, которые держали компьютерный магазин в Пакистане. Братьям надоело, что покупатели нелегально копировали купленное у них ПО, и они создали этот вирус, которые заражал загрузочные сектора дискет. Brain заодно оказался и первым вирусом-невидимкой: при обнаружении попытки чтения зараженного сектора диска вирус незаметно подставлял его незараженный оригинал. Также он записывал на дискету фразу «(c) Brain», но при этом не портил никаких данных.

## Вирус ILoveYou

Одна из самых серьезных эпидемий новой эры была вызвана червем ILoveYou, который появился 4 мая 2000 г. Как указывает [Securelist](https://securelist.ru/threats/2001/" \t "_blank), ILoveYou следовал модели ранее существовавших вирусов, распространявшихся по почте. При этом, в отличие от макровирусов, широко распространенных с 1995 года, ILoveYou распространялся не в виде зараженного документа Word, а в виде VBS-файла (такое расширение имеют скрипты, написанные в Visual Basic). Метод оказался простым и действенным – пользователи еще не привыкли остерегаться незапрошенных электронных писем. В качестве темы письма была строчка «I Love You», а в приложении к каждому письму был файл «LOVE-LETTER-FOR-YOU-TXT.vbs». По задумке создателя Онеля де Гузмана, червь стирал существующие файлы и поверх них записывал собственные копии, благодаря которым червь рассылался по всем адресам из списка контактов пользователя. Поскольку письма, как правило, приходили со знакомых адресов, получатели обычно открывали их – и заражали червем свой компьютер. Таким образом, ILoveYou на практике подтвердил эффективность методов социальной инженерии.

## Червь Code

Червь Code Red был так называемым бестелесным червем – он существовал только в памяти и не предпринимал попыток заразить файлы в системе. Используя брешь в системе безопасности Microsoft Internet Information Server, червь всего за несколько часов распространился по всему миру и вызвал хаос, внедряясь в протоколы обмена информацией между компьютерами.

Как пишет сайт [Scientific American](http://www.scientificamerican.com/article/code-red-worm-assault-on/), зараженные компьютеры в итоге были использованы для проведения DDoS-атаки на веб-сайт Белого дома – Whitehouse.gov.

## Heartbleed

Угроза Heartbleed появилась в 2014 г. и сразу поставила под угрозу множество интернет-серверов. В отличие от вирусов и червей, Heartbleed – это уязвимость в OpenSSL – криптографической библиотеке универсального применения, широко использующейся по всему миру. OpenSSL периодически рассылает соединенным устройствам специальные сигналы, подтверждающие актуальность соединения. Пользователи могут отослать некоторый объем данных и в ответ запросить такое же количество данных – например, отослать один байт и получить в ответ тоже один байт. Максимальное количество данных, отправляемых за один раз – 64 килобайта. Как объясняет специалист по безопасности [Брюс Шнайер](https://www.schneier.com/blog/archives/2014/04/heartbleed.html), пользователь может объявить, что отсылает 64 килобайта, а по факту отправить только один байт – в этом случае сервер в ответ пришлет 64 килобайта данных, хранящихся в его оперативной памяти, в которых может оказаться все что угодно – от имен пользователей до паролей и криптостойких ключей.

## Будущее компьютерных вирусов

На протяжении уже более 60 лет компьютерные вирусы находятся в сфере коллективного человеческого сознания. То, что однажды было лишь кибер-вандализмом, быстро превратилось в киберпреступление. Быстро развиваются черви, троянцы и вирусы. Хакеры мотивированы и умны, они всегда стремятся тестировать на прочность системы и код, расширять границы доступных им методов и изобретать новые способы заражения. В будущем киберпреступники, вероятно, будут чаще взламывать PoS-терминалы – в качестве хорошего примера можно привести недавний троянец удаленного доступа [Moker](https://threatpost.com/new-moker-rat-bypasses-detection/114948/). Этот новый троянец сложно обнаружить, тяжело удалить – он обходит все известные механизмы защиты. Ничего не известно наверняка; постоянные перемены – в самой природе постоянной борьбы между киберпреступниками и системами защиты.

**3 Какой вред наносят вирусы**

Различные вирусы выполняют **различные деструктивные действия**:

* выводят на экран мешающие текстовые сообщения;
* создают звуковые эффекты;
* создают видео эффекты;
* замедляют работу ЭВМ, постепенно уменьшают объем оперативной памяти;
* увеличивают износ оборудования;
* вызывают отказ отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;
* имитируют повторяющиеся ошибки работы операционной системы;
* уничтожают FAT-таблицу, форматируют жесткий диск, стирают BIOS, стирают или изменяют установки в CMOS, стирают секторы на диске, уничтожают или искажают данные, стирают антивирусные программы;
* осуществляют научный, технический, промышленный и финансовый шпионаж;
* выводят из строя системы защиты информации, дают злоумышленникам тайный доступ к вычислительной машине;
* делают незаконные отчисления с каждой финансовой операции и т.д.;

Главная опасность самовоспроизводящихся кодов заключается в том, что программы-вирусы начинают жить собственной жизнью, практически не зависящей от разработчика программы. Так же, как в цепной реакции в ядерном реакторе, запущенный процесс трудно остановить.

**4. Что указывает на вирусное заражение**

Основные **симптомы вирусного заражения** ЭВМ следующие:

* замедление работы некоторых программ;
* увеличение размеров файлов;
* появление не существовавших ранее файлов;
* уменьшение объема доступной оперативной памяти;
* появление сбоев в работе операционной системы;
* запись информации на диски в моменты, когда этого не должно происходить.

**5. Какие бывают вирусы**

Рассмотрим **основные виды вирусов**. Существует большое число различных классификаций вирусов:

* по среде обитания:
  + **сетевые** вирусы, распространяемые различными компьютерными сетями;
  + **файловые** - инфицируют исполняемые файлы, имеющие расширение exe и com. К этому же классу относятся и **макровирусы**, написанные с помощью макрокоманд. Они заражают неисполняемые файлы (в Word, Excel);
  + **загрузочные** - внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска. Некоторые вирусы записываются в свободные секторы диска, помечая их в FAT-таблице как плохие;
  + **загрузочно-файловые** - интегрируют черты последних двух групп;
* по способу заражения (активизации):
  + **резидентный** вирус логически можно разделить на две части - **инсталятор** и **резидентный модуль**. При запуске инфицированной программы управление получает инсталятор, который выпоняет следующие действия:
    1. размещает резидентный модуль вируса в ОЗУ и выполняет операции, необходимые для того, чтобы последний хранился в ней постоянно;
    2. подменяет некоторые обработчики прерываний, чтобы резидентный модуль мог получать управление при возникновении определенных событий.
  + **нерезидентный** вирусы не заражают оперативную память и проявляют свою активность лишь однократно при запуске инфицированной программы;
* по степени опасности:
  + **не опасные** - звуковые и видеоэффекты;
  + **опасные** - уничтожают часть файлов на диске;
  + **очень опасные** - самостоятельно форматируют жесткий диск;
* по особенностям алгоритма:
  + **компаньон-вирусы** не изменяют файлы. Алгоритм их работы состоит в том, что они создают для exe-файлов новые файлы-спутники (дубликаты), имеющие то же имя, но с расширением com. (com-файл обнаруживается первым, а затем вирус запускает exe-файл);
  + **паразитические** - при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов (все вирусы кроме компаньонов и червей);
  + **черви (репликаторы)** - аналогично компаньонам не изменяют файлы и секторы диска. Они проникают в компьютер по сети, вычисляют сетевые адреса других компьютеров и рассылают по этих адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов;
  + **невидимки (стелс)** - используют набор средств для маскировки своего присутствия в ЭВМ. Их трудно обнаружить, т.к. они перехватывают обращения ОС к пораженным файлам или секторам и подставляют незараженные участки файлов;
  + **полиморфики (призраки, мутанты)** - шифруют собственное тело различными способами. Их трудно обнаружить, т.к. их копии практически не содержат полностью совпадающих участков кода;
  + **троянская программа** - маскируется под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу или собирает на компьютере информацию, не подлежащую разглашению. В отличие от вирусов, троянские программы не обладают свойством самовоспроизводства.
* по целостности:
  + **монолитные** - программа представляет единый блок;
  + **распределенные** - программа разделена на части. Эти части содержат инструкции, которые указывают как собрать их воедино, чтобы воссоздать вирус.

**6. Что такое антивирусная программа**

Для борьбы с вирусами разрабатываются **антивирусные программы**.

|  |
| --- |
| ***Антивирусное средство* это программный продукт или устройство, выполняющее одну, либо несколько из следующих функций: 1) защиту данных от разрушения; 2) обнаружение вирусов; 3) нейтрализацию вирусов.** |

Различают следующие виды:

* **программы-детекторы** рассчитаны на обнаружение конкретных, заранее известных программе вирусов и основаны на сравнении характерной последовательности байтов (сигнатур), содержащихся в теле вируса, с байтами проверяемых программ. Программы-детекторы снабжаются блоками эвристического анализа. В этом режиме делается попытка обнаружить новые или неизвестные вирусы по характерным для всех вирусов кодовым последовательностям.
* **программы-дезинфекторы** (фаги) не только находят зараженные файлы, но и лечат их, удаляя из файла тело программы-вируса. В России получили широкое распространение детекторы, одновременно выполняющие функции дезинфекторов: AVP, Aidstest, DoctorWeb.
* **программы-ревизоры** анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние загрузочного сектора, FAT-таблицы, а также длина файлов, их время создания, атрибуты, контрольные суммы. (ADinf)
* **программы-фильтры** (мониторы) оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия. Фильтры контролируют обновление программных файлов и системной области диска, форматирование диска, резидентное размещение программ в ОЗУ.

**7. Как защитить компьютер от вирусов**

Рассмотрим основные **меры по защите** ЭВМ от заражения вирусами:

* Необходимо оснастить ЭВМ современными антивирусными программами и постоянно обновлять их версии.
* При работе в сети обязательно должна быть установлена программа-фильтр.
* Перед считыванием с дискет информации, записанной на других ЭВМ, следует всегда проверять эти дискеты на наличие вирусов.
* При переносе файлов в архивированном виде необходимо их проверять сразу же после разархивации.
* При работе на других компьютерах необходимо защищать свои дискеты от записи.
* Делать архивные копии ценной информации на других носителях.
* Не оставлять дискету в дисководе при включении или перезагрузке ЭВМ, это может привести к заражению загрузочными вирусами.
* Получив электронное письмо, к которому приложен исполняемый файл, не следует запускать этот файл без предварительной проверки.
* Необходимо иметь аварийную загрузочную дискету, с которой можно будет загрузиться, если система откажется сделать это обычным образом

**4 . Подведение итогов**

1. Что такое компьютерный вирус и троянская программа?
2. Укажите пути проникновения компьютерного вируса в компьютер.
3. Какие типы компьютерных вирусов Вам известны?
4. Укажите основные признаки заражения компьютера.
5. Какие существуют методы борьбы с компьютерными вирусами?
6. Какие основные антивирусные программы Вы знаете?
7. Как защитить компьютер от вирусов?