ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КИМРСКИЙ КОЛЛЕДЖ»

# МЕТОДИЧЕСКАЯ РАЗРАБОТКА УЧЕБНОГО ЗАНЯТИЯ ПО ДИСЦИПЛИНЕ ИНФОРМАТИКА

## ЗАЩИТА ИНФОРМАЦИИ
## ТЕМА УРОКА:
## «КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ»

**Разработал преподаватель:**
**Преподаватель ГБП ОУ «Кимрский колледж»**
**Соловьева Татьяна Алексеевна**

**Г. КИМРЫ**
**2021**

Урок проводится по дисциплине Информатика в группе I курса по профессиям: Мастер по ремонту и обслуживанию автомобилей, Сварщик (ручной и частично механизированной сварки (наплавки)).

**Тип учебного занятия** – объяснение нового материала, и совершенствование умений и навыков.

**Цели урока:**

Обучающая: **научить применять ранее полученные знания по защите информации от вирусов.**

Воспитательная: **воспитание рациональной организации труда, интереса к выбранной профессии, формирование самостоятельности.**

Развивающая: **развитие логического мышления, памяти**

Студент должен знать: **виды вирусов и способы защиты от них, назначение антивирусных программ и их виды, действия пользователя при наличии признаков заражения компьютера.**

Студент должен уметь: **использовать антивирусные программы для устранения вирусов, меры по профилактике заражения компьютера.**

Формируемые компетенции:

**ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.**

**ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности**

Материально-техническое обеспечение урока**:**

- **Компьютер;**
- **Жидкокристаллическая панель Samsung;**
- **Презентация по теме: Компьютерные вирусы.**

**Методы обучения**: наглядный, частично-поисковый, репродуктивный, метод проектов, информационно-развивающий, фронтальный опрос.

**Формы организации познавательной деятельности**: групповая, индивидуальная.

**ТЕХНОЛОГИЧЕСКАЯ КАРТА УРОКА**

**Предмет** Информатика

**Тема** Антивирусные средства зашиты

**Тип урока** урок открытия нового знания

**Прогнозируемы результаты**

Личностные

**Учить проверять себя;**

**Учить давать оценку своим действиям;**

**Учить работать в группе, чувствовать свой вклад в общую работу.**

Метапредметные

**Учить анализировать и выделять общее;**

**Учить находить наиболее оптимальный алгоритм решения.**

Предметные

**Дать определение понятиям компьютерный вирус, червь, вирус, троянские программы, на какие типы вредоносных программ делятся вирусы, пути распространения вирусов. Для чего предназначены антивирусные программы, классификация антивирусных программ**

Дидактические средств: **учебник, презентация.**

Оборудование:

- **Компьютер;**
- **Жидкокристаллическая панель Samsung;**
- **Презентация по теме: Компьютерные вирусы.**

**Тема урока:** «Компьютерные вирусы и антивирусные программы»

**Цели урока:** изучение основных понятий темы урока.

**Задачи урока:**

**- обучающие:**

- изучить понятие «компьютерный вирус» и «антивирусная программа»;
- изучить способы защиты информации.

**- развивающие:**

- развить навыки распознавания заражения компьютера.

**- воспитательные:**

- воспитать информационную культуру;
- сформировать представление о способах заражения компьютерными вирусами.

**Тип урока:** урок изучения и закрепления новых знаний; интерактивный урок.

**Оборудование:** мультимедийное оборудование для презентаций, интерактивная доска, приложение – Microsoft PowerPoint.

**Ход урока**

**1. Организационный момент**

Приветствие, проверка присутствующих.

**2. Сообщение темы и цели урока**

**(Слайд 1)**. Объявление темы урока.

Сегодня мы узнаем, что такое компьютерные вирусы и как с ними бороться. Наверняка, каждый, у кого есть компьютер, встречался с проблемой вирусов. А кто может сказать:

- что такое компьютерный вирус?
- каким образом они попадают в машину?
- зачем придумали их?
- как с ними бороться?

Сегодня мы подробно разберем все эти вопросы.

**3. Изучение нового материала**

**(Слайд 2).** Итак. Откуда же взялись современные компьютерные вирусы? А началось всё с американца венгерского происхождения Джона фон Неймана, который в 1951 году основал теорию самовоспроизводящихся механизмов и предложил методы их создания. После чего, в 1961 году, уже были известны рабочее применение таких программ.

Первыми известными собственно вирусами стали «Virus 1,2,3» и «Elk Cloner», работающими только на ПК Apple II (1981 г.).

Первыми средствами борьбы с вирусами стали утилиты – «CHK4BOMB» и «BOMBSQAD» (Энди Хопкинс, 1984 г.).

Первое массовое распространение компьютерного вируса выпало на 1986 год. Вирус с именем – «Brain» (*англ.* «мозг») заражал дискеты персональных компьютеров.

На сегодняшний день известны десятки тысяч компьютерных вирусов, распространяющихся через Интернет по всему миру.

**(Слайд 3). Компьютерные вирусы** – это компьютерные программы, способные «размножаться» (самокопироваться) и незаметно для пользователя внедрять свой программный код в файлы, документы, Web-страницы и сообщения электронной почты.

**Виды вирусов:**

**Черви** – это класс вредоносных программ, использующих для распространения сетевые ресурсы. Название этого класса было давно исходя из способности «червей» переползать с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Обладают высокой скоростью распространения.

**Вирусы** – это программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске заряженных файлов. Скорость заражения вирусов ниже, чем у «червей».

**Троянские программы** – программы, которые выполняют на поражаемых компьютерах несанкционированное пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к зависанию, воруют конфиденциальную информацию. Троянские программы не способны самостоятельно проникать на компьютеры и распространяться злоумышленниками под видом полезного программного обеспечения.

Как только вирус заразил компьютер, он начинает вредоносные действия – уничтожение программ и данных. Запуск вируса может произойти после определенных событий: наступление определенной даты, запуск приложения и т.д.

По способу существования компьютерные вирусы можно разделить на резидентные и нерезидентные. **Резидентный вирус**, единожды запущенный, остаются работающим в оперативной памяти. При этом такие вирусы могут создавать дополнительные процессы, тем самым, перегружая оперативную память. **Нерезидентный вирус** является частью зараженного приложения и может функционировать только во время его запуска.

**(Слайд 4).** По среде обитания вирусы различают:

- **файловые** – наиболее распространенный тип вирусов. Внедряются в приложения и активизируются при их запуске.
- **загрузочные** – прописываются в загрузочных секторах диска (boot-сектор).
- **макровирусы** – заражают файлы документов, обычно текстовые документы.
- **сетевые** – передают свой программный код по компьютерным сетям. Заражение происходит через электронную почту или Интернет.

**(Слайд 5).** Наибольшую опасность создают почтовые сетевые вирусы. Опасность заключается в их массовости. Например, даже если в адресных книгах пользователей имеется только два адреса, то через три рассылки вирусом будет заражено уже восемь компьютеров.

Всемирная эпидемия заражения почтовым вирусом началась 5 мая 2000 года, когда десятки миллионов компьютеров, получили почтовое сообщение с привлекательным названием «ILOVEYOU». Сообщение содержало вложенный вирус. После прочтения этого письма вирус начинал разрушать файловую систему.

**(Слайд 6).** Признаки заражения компьютера вирусами.

- Увеличение размера файлов
- Замедление работы программ и операционной системы в целом
- Уменьшение объема оперативной памяти
- Появление неизвестных файлов
- Некорректная работа приложений

**(Слайд 7).** Антивирусная программа – специальная программа для обнаружения вирусов, а также нежелательных программ и восстановления зараженных файлов.

Антивирусные программы, на сегодняшний день, одно из самых эффективных средств в борьбе с вирусами. Антивирусные программы используют постоянно обновляемые списки известных вирусов. Если антивирусная программа обнаружит код вируса в каком-либо файле, той файл считается зараженным вирусом и подлежит лечению.

Антивирусные программы предназначены для антивирусной защиты персонального компьютера и выполняют следующие функции:

- Защита от вирусов и вредоносных программ – обнаружение и уничтожение вредоносных программ, проникающих через съемные и постоянные файловые носители, электронную почту и протоколы Интернета;
- Постоянная защита компьютера – проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов;
- Проверка компьютера по требованию – проверка и «лечение» как всего компьютера в целом, так и отдельных дисков, файлов или каталогов (пользователь может запускать проверку самостоятельно или настроить ее регулярный автоматический запуск);
- Восстановление работоспособности после вирусной атаки, когда полная проверка и «лечение» позволяют удалить все вирусы поразившие данные при атаке;
- Проверка и «лечение» входящей –исходящей почты – анализ на присутствие вирусов и лечение входящей почты до ее получения в почтовый ящик и исходящей почты в режиме реального времени;
- Обновление антивирусных баз и программных модулей – пополнение антивирусных баз информацией о новых вирусах и способах «лечения» зараженных ими объектов, а также обновление собственных модулей программы;
- Рекомендации по настройке программы и работе с ней – советы от экспертов, создателей антивирусной программы, и рекомендуемые настройки, соответствующие оптимальной антивирусной защите;
- Формирование отчета – фиксирование всех результатов работы антивируса в отчете. Подробный отчет о результатах проверки включает в себя общую статистику по проверенным объектам, хранит настройки, с которыми была выполнена та или иная задача, а также последовательность проверки.

**(Слайд 8).** Профилактика защиты от вирусов:

- Не работать под привилегированными учётными записями без крайней необходимости.
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасный функционал системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

**(Слад 9)** Контрольные вопросы.

- К каким последствиям может привести заражение компьютера компьютерным вирусом?
- Какие типы компьютерных вирусов вы знаете, чем они отличаются друг от друга, и какова должна быть профилактика заражения?
- Каким способом антивирусные программы обнаруживают компьютерные вирусы и обеспечивают их нейтрализацию?