**21.10.2021 Учебная группа 1СТМ, 4-я пара**

**Преподаватель Иванова Наталия Викторовна**

дисциплина ЕН.02 ИНФОРМАТИКА

**Тема:** Защита информации от несанкционированного доступа. Антивирусная защита

**Цель занятия:**

*Образовательная:*познакомить с основными возможностями антивирусных программ;

*развивающая*: формирование и развитие познавательных способностей, развитие навыков самостоятельного мышления.

*воспитательная:* воспитание таких базовых качеств личности, как коммуникативность, самостоятельность, толерантность, ответственность за собственный выбор и результаты своей деятельности

**Задачи занятия:** познакомить с основными способами защиты информации от несанкционированного доступа; рассмотреть основные возможности защиты информации с помощью антивирусных программ.

**Мотивация:** Добрый день, уважаемый слушатель! В этом модуле вы познакомитесь с программно-техническими мерами защиты информации. Мы подробно рассмотрим сервисы безопасности, познакомимся и разберем различные виды антивирусной защиты, выберем антивирусное средство, подходящее для конкретных целей и познакомимся с такими понятиями как протоколирование и аудит. Желаю успехов в изучении!

**Задание студентам:**

1. Посмотреть видеоурок по темам:
   1. «Антивирусная защита» <https://ru.coursera.org/lecture/metody-i-sredstva-zashity-informacii/antivirusnaia-zashchita-YeUmN>
   2. «Типы вредоносных программ»

<https://ru.coursera.org/lecture/metody-i-sredstva-zashity-informacii/tipy-vriedonosnykh-proghramm-drKzb>

* 1. «Принципы обнаружения вредоносных программ»

<https://ru.coursera.org/lecture/metody-i-sredstva-zashity-informacii/printsipy-obnaruzhieniia-vriedonosnykh-proghramm-gbU3R>

* 1. «Выбор антивирусных средств»

<https://ru.coursera.org/lecture/metody-i-sredstva-zashity-informacii/vybor-antivirusnykh-sriedstv-ZnASZ>

1. Пройти тестовое задание <https://onlinetestpad.com/ru/test/19363-szhatie-informacii-programmy-arkhivatory>
2. Познакомиться с материалом по видеоуроку <https://yandex.ua/video/preview/11002821802903987494>
3. Сделать конспект лекции. Ответить на вопросы

Фотографию с выполненным заданием прислать на электронный адрес **atata17@yandex.ru** в срок **до 08.00 21.10.2021** **г.**

**План:**

1. Понятие компьютерного вируса. Классификация компьютерных вирусов.
2. Антивирусные программы.
3. **Вопросы и задания.**

**Литература:**

*Литература основная*: Семакин И.Г., Хеннер Е.К., Шейна Т.Ю. Информатика, учеб, 10 кл. базовый уровень/ И.Г. Семакин, Е.К. Хеннер, Т.Ю. Шейна изд.-М.: Бином. Лаборатория знаний, 2015.-264 с.

*Литература дополнительная*: Дыбкова Л.М. «Информатика и компьютерная техника» - М.: Издательство А.С.К., 2003 -512с.: ил.

Информатика. 10 класс. Углубленный уровень. В 2 ч. Поляков К.Ю., Еремин Е.А., М.: 2013 — Ч.1 - 344с., Ч.2 - 304с.

Интернет технологии в экономике знаний: Учебник под ред. Абдиксева Н.М. : - М.: ИД. "Форум" : ИНФРА - М. 2012-448с. 2. Симонович С.В. Информатика базовый курс: Учебник для вузов. 3-е изд. Стандарт 3-го поколения.- Спб.: Питер, 2012-640с. 3. Компьютерные сети. Принципы, технологии, протоколы / В.Г.Олифер, Н.А.Олифер. – СПб.: Питер, 2010.

**Лекция№7**

**1. Понятие компьютерного вируса. Классификация компьютерных вирусов.**

Одна из главных потерь информации на компьютере в наше время возникает вследствие деятельности компьютерных вирусов. Ежегодный ущерб от компьютерных вирусов составляет сотни миллиардов долларов, и еще примерно столько же приходится на косвенные убытки, связанные с разработкой программного обеспечения и проведения профилактических мероприятий по защите от вирусов.

Кроме полезных программ, которые помогают пользователю обрабатывать данные, существуют и вредоносные программы.

По уровню опасности действий вредоносные программы делят на:

*безопасные* – проявляются видео и звуковыми эффектами, не изменяют файловую систему, не повреждают файлы и не выполняют шпионские действия;

*опасные* ‒ приводят к перебоям в работе компьютерной системы: уменьшают размер доступной оперативной памяти, перезагружают компьютер и т.п.;

*очень опасные* – уничтожают данные с постоянной и внешней памяти, выполняют шпионские действия и т.п.

По принципам распространения и функционирования вредоносные программы делят на:

*компьютерные вирусы* ‒ программы, способные саморазмножаться и выполнять несанкционированные деструктивные действия на пораженном компьютере. Среди них выделяют:

*дисковые (загрузочные) вирусы* – размножаются копированием себя в служебные участки дисков и других съемных носителей, которое происходит при попытке пользователя считать данные с пораженного носителя;

*файловые вирусы* ‒ размещают свои копии в составе файлов различного типа. Как правило, это файлы готовых к выполнению программ с расширением имени ехе или соm. Однако существуют так называемые макро вирусы, поражающие, например, файлы текстовых документов, электронных таблиц, баз данных и т.д.;

*черви компьютерных сетей* – пересылают свои копии компьютерными сетями с целью проникновения на удаленные компьютеры. Большинство червей распространяются, прикрепившись к файлам электронной почты, электронных документов и т.п. С пораженного компьютера черви пытаются проникнуть на другие компьютеры, используя список электоронных почтовых адресов или другими способами. Кроме размножения, черви могут выполнять деструктивные действия, которые характерны для вредоносных программ;

*троянские программы* ‒ программы, которые проникают на компьютеры пользователей вместе с другими программами, которые пользователь «получает» компьютерными сетями. Вредоносные программы он получает «в подарок», так как в свое время защитники Трои получили в подарок от греков деревянного коня, внутри которого размещались греческие воины. Отсюда и название этого вида вредоносных программ. Как и другие вредоносные программы, троянские программы могут выполнять указанные выше деструктивные действия, но в основном их используют для выполнения шпионских действий.

Значительная часть вредоносных программ в начальные периоды заражения не выполняет деструктивных действий, а лишь размножается. Это так называемая пассивная фаза их существования. Через некоторое время, в определенный день или по команде с компьютера в сети вредоносные программы начинают выполнять деструктивные действия – переходят в активную фазу своего существования.

Среди вирусов выделяют те, которые используют специальные способы скрытия своих действий и нахождения в операционной системе компьютера:

*полиморфные (мутанты*) ‒ вирусы, которые при копировании изменяют свое содержимое так, что каждая копия имеет разный размер; их труднее определить, используя поиск по известной длине кода вируса.

*стелс* – (англ. ‒ хитрость, уловка, вирус – невидимка) ‒ вирусы, пытающиеся различными средствами скрыть факт своего существования в операционной системе. Например, вместо действительного объекта, пораженного вирусом, антивирусной программе предоставляется для проверки его непораженная копия.

**2. Антивирусные программы.**

Для защиты данных и устройств компьютера от вредоносных программ используется специальное программное обеспечение – **антивирусные программы**.

**Различают следующие антивирусные программы:**

*детекторы (сканеры)* ‒ программы, способные проводить проверку компьютера на наличие вредоносных программ и уведомлять пользователя об их наличии. В ходе проверки программы используют данные из так называемых антивирусных баз – совокупности данных об известных на данный момент времени вредоносные программы и способы борьбы с ними;

*доктора* - программы, осуществляющие «лечение» компьютеров от обнаруженных вредоносных программ, то есть обезвреживают их, а при невозможности обезвреживания могут удалять зараженные объекты или располагать их в специальных папках. Как и детекторы, доктора используют антивирусные базы для обновления данных о способах борьбы с вредоносными программами;

*мониторы* ‒ программы, которые постоянно (резидентно) находятся в оперативной памяти компьютера с момента загрузки операционной системы и проверяют все файлы и диски, к которым идет обращение, блокируют действия, которые могут идентифицироваться как действия вредоносной программы;

*ревизоры* – программы, которые анализируют состояние системных файлов и папок и сравнивают их с состоянием, которое было в начале работы антивирусной программы. При определенных изменениях, характерных для деятельности вредоносных программ, программа-ревизор выводит сообщение о возможности поражения вредоносной программой;

*блокировщики* ‒ программы, которые анализируют обмен данными компьютера пользователя с другими компьютерами в сети. Программа блокирует соединение с определенным компьютером в сети, если фиксирует действия, характерные для вредоносных компьютерных программ, и выводит сообщение о попытке их проникновения на компьютер пользователя.

*охранники* – автоматически проверяют на наличие вирусов файлы, которые запускаются, и дискеты, которые вставляются в дисководы. При обнаружении вируса программа-охранник может выдавать предупредительное сообщение.

*антивирусные комплексы* ‒ это комплексы, совмещающие функции детектора, ревизора и охранника. К таким комплексам относятся Norton Antivirus, а также Antiviral Toolkit Pro (сокращенно AVP).

***В состав AVP пакета входят следующие компоненты:***

1) проверка электронной почты в процессе принятия ее;

2) постоянная проверка системы;

3) создание дисков аварийного восстановления;

4) проверка системы по запросу пользователя;

5) обновление пакета AVP;

6) проверка дисков на наличие измененных папок и файлов;

7) защита от макровирусов в документах Ms Office.

**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

**Вопросы для самоконтроля:**

1. Что тако компьютерный вирус?
2. На какие типы разделяются компьютерные вирусы в зависимости от среды обитания?
3. Что собой представляют файловые вирусы, загрузочные вирусы?
4. Чем отличаются макровирусы от файловых вирусов?
5. Что такое резидентные и нерезидентные компьютерные вирусы?
6. Какие типы антивирусных программ ввам известны?
7. Перечислите профилактические меры для борьбы с заражением вирусами?
8. В каком файле находится информация о зараженных и выличенных файлах?