**Тема урока: Защита от вредоносных программ.
Классификация вирусов.**

***Изучить предложенный материал.***

Чтобы бороться с врагом надо знать его в лицо. Поскольку разнообразие компьютерных вирусов слишком велико, то они, как и их биологические прообразы, нуждаются в классификации. Классифицировать вирусы можно по следующим признакам:

|  |  |
| --- | --- |
| • | по среде обитания; |
| • | по способу заражения среды обитания; |
| • | по деструктивным возможностям; |
| • | по особенностям алгоритма вируса.**Классификация вирусов по среде обитания**    По среде обитания вирусы можно разделить на: * **Файловые вирусы**, которые внедряются в выполняемые файлы (\*.СОМ, \*.ЕХЕ, \*.SYS, \*.BAT, \*.DLL).
* **Загрузочные вирусы**, которые внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot Record).
* **Макро-вирусы**, которые внедряются в системы, использующие при работе так называемые макросы (например, Word, Excel).

    Существуют и сочетания - например, *файлово-загрузочные* вирусы, заражающие как файлы, так и загрузочные сектора. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему и их труднее обнаружить.**Классификация вирусов по способам заражения**По способам заражения вирусы бывают **резидентные и нерезидентные**.    *Резидентный вирус* при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. *Нерезидентные вирусы* не заражают память компьютера и являются активными лишь ограниченное время.**Классификация вирусов по деструктивным возможностям**По деструктивным возможностям вирусы можно разделить на: * **безвредные**, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
* **неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
* **опасные** - вирусы, которые могут привести к серьезным сбоям в работе;
* **очень опасные**, приводят к потере программ, уничтожают данные, стирают необходимую для работы компьютера информацию, записанную в системных областях памяти и т.д.

**Классификация вирусов по особенностям алгоритма**Здесь можно выделить следующие основные группы вирусов: * **компаньон-вирусы** (companion) - Алгоритм работы этих вирусов состоит в том, что они создают для ЕХЕ-файлов файлы-спутники, имеющие то же самое имя, но с расширением СОМ. При запуске такого файла DOS первым обнаружит и выполнит СОМ-файл, т.е. вирус, который затем запустит и ЕХЕ-файл;
* **вирусы-«черви»** (worm) - вариант компаньон-вирусов. «Черви» не связывают свои копии с какими-то файлами. Они создают свои копии на дисках и в подкаталогах дисков, никаким образом не изменяя других файлов и не используя СОМ-ЕХЕ прием, описанный выше;
* **«паразитические»** - все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются «червями» или «компаньон-вирусами»;
* **«студенческие»** - крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок;
* **«стелс»-вирусы** (вирусы-невидимки, stealth), представляют собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и «подставляют» вместо себя незараженные участки информации. Кроме того, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы;
* **«полиморфик»-вирусы** (самошифрующиеся или вирусы-призраки, polymorphic) - достаточно труднообнаруживаемые вирусы, не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика;
* **макро-вирусы** - вирусы этого семейства используют возможности макроязыков (таких как Word Basic), встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время широко распространены макро-вирусы, заражающие документы текстового редактора Microsoft Word и электронные таблицы Microsoft Excel;
* **сетевые вирусы (сетевые черви)** - вирусы, которые распространяются в компьютерной сети и, так же, как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в 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). Сетевых вирусов известно всего несколько штук. Например, XMasTree, Вирус Морриса (Internet Worm).
 |

**Защита от компьютерных вирусов**

Ваш компьютер работает медленно? Может быть, он ведет себя странно?

Как и большинство пользователей компьютеров, вы можете прийти к выводу, что он заразился вирусом. Однако это может быть какое-то вредоносное ПО.

Вредоносное ПО - это любое программное обеспечение, специально созданное для нанесения ущерба ПК, клиенту, серверу или компьютерной сети. Некоторые опасны, а другие просто раздражают. В худшем случае они могут отключить вашу сеть и получить доступ к личной информации или повредить устройство.

Почти 30% компьютеров в домохозяйствах стран имеют некоторые виды вредоносных программ. И многие люди потеряли деньги или стали жертвами учетных записей, скомпрометированных из-за вредоносного ПО.

Зачем ждать таких неприятных и травмирующих результатов?

**Вот несколько советов о том, как защитить компьютер от вредоносных программ.**

**Установите антивирус**

Это похоже на легкую задачу. Однако не все пользователи знают о том, как защитить компьютер от вредоносных программ, и не все из них имеют антивирус на своем компьютере.

Антивирусное программное обеспечение является первой линией защиты от угроз. Оно также предупреждает вас о потенциальных угрозах в системе, так как постоянно появляются новые вредоносные программы.

Вы можете выбрать одну из бесплатных антивирусных программ, таких как Panda, Bitdefender и Avira. Однако, если вы ищете продвинутый уровень защиты, вы можете выбрать платное антивирусное программное обеспечение, такое как Norton, Comodo, Avast и Kaspersky.

**Сканируйте компьютер регулярно**

Запланируйте программное обеспечение, чтобы регулярно сканировать ваше устройство. Хотя раз в неделю это хорошо, вам не нужно ждать так долго, чтобы выполнить сканирование.

Запустите сканирование, когда вы не используете свой компьютер, например, ночью. Вы можете запустить антивирусную программу в определенное время. Убедитесь, что компьютер не переключается в режим гибернации и не отключается автоматически во время сканирования.

**Обновите антивирусное программное обеспечение**

Установки антивирусного программного обеспечения не достаточно. Вам нужно обновить его, чтобы он мог предотвращать запуск новых вирусов и вредоносных программ каждый день. Запомнить, когда нужно обновлять антивирус, довольно сложно.

Поэтому включите функцию автоматического обновления вашего антивируса, чтобы обновления могли происходить самостоятельно. Также обновите другие программы, установленные на вашем компьютере.

**Берегите внешние устройства**

Флэш-накопители USB и внешние устройства стали обычным явлением для передачи данных с одного компьютера на другой. И в равной степени верно, что они могут передавать вирусы вместе с данными.

Многие вирусные программы автоматически активируются, когда USB-карта вставляется в порт ПК. Есть смысл иметь антивирусную программу, которая автоматически сканирует внешние устройства.

**Держите вашу сеть в безопасности**

Наши ПК подключены к принтерам, устройствам и Интернету через Wi-Fi. Попадание в незащищенную сеть является хакером. Убедитесь, что ваш Wi-Fi и другие сети защищены надежным паролем.

Избегайте трансляции открытого соединения Wi-Fi и всегда используйте шифрование WPA или WPA2. WEP устарел, поскольку он недостаточно силен. Если у вас есть пользователи, которые пользуются вашим Интернетом, обязательно предоставьте гостевой SSID, который использует другой пароль, на тот случай, если ваши друзья играют во «вредоносные игры».

**Всегда обновляйте ОС**

У всех поставщиков программного обеспечения есть свои ОС, и у каждого есть уникальная антивирусная защита. Тем не менее, они должны обновляться для борьбы с новыми угрозами. Эти обновления минимизируют вашу подверженность потенциальным эксплойтам.

Группы безопасности операционных систем выпускают новые исправления угрозы и уязвимости. Если вы продолжаете использовать более старую ОС - игнорируете постоянный запрос на обновление вашей ОС до более новой версии, то ваш компьютер рано или поздно может оказаться вредоносным ПО.

**Загружайте программное обеспечение из надежных источников**

Будьте осторожны при загрузке, установке программ или инструментов на ваш компьютер, особенно из бесплатных и неизвестных источников. Не загружайте программное обеспечение по нежелательным ссылкам, которые вы получаете по электронной почте или сообщению. Избегайте загрузки программ, если вы сомневаетесь в его достоверности.

Некоторые программы просят вас загрузить их другие функции или инструмент во время установки. Однако избегайте их, поскольку они могут быть шпионскими программами. Предпочитайте скачивание из надежных источников, таких как Microsoft, Apple и Adobe.

**Это некоторые шаги, чтобы защитить ваш компьютер от вредоносных программ. Они не только повысят безопасность вашего ПК, но и его производительность.**

Задание

**Ответить письменно на вопросы**

1. Что называется компьютерным вирусом?
2. Какой из файлов принято называть зараженным?
3. Перечислите этапы, которые проходит компьютерный вирус в своем развитии.
4. В чем отличие файлового вируса от загрузочного вируса?
5. Какой из видов компьютерных вирусов принято называть макровирусом?
6. В чем отличие программы типа "Троянский конь" от вируса-червя?
7. Какие виды антивирусных программ вам известны?
8. Как классифицируются вирусы по среде обитания?
9. Какие типы компьютерных вирусов выделяются по способу воздействия?
10. Что могут заразить вирусы?
11. Как маскируются "невидимые" вирусы?

Присылать задания в группу **в контакте** в сообщения сообщества:

<https://vk.com/club200304731>

Название файла, пример: **17.11.20. Патокина Анастасия, ОЖЭС-111**

**Срок исполнения задания: 20.11.2020.**

**Литература:**

**[1] *О.П. Новожилов Информатика: учебник для СПО/ О.П. Новожилов.-3-е изд. перераб. и доп.-М.: Издательство Юрайт,2019.-620с.-Серия: Профессиональное образование. - Режим доступа.-*** [***https://urait.ru/book/informatika-v-2-ch-chast-2-448996***](https://urait.ru/book/informatika-v-2-ch-chast-2-448996)

***Глава 12, тема: 12.1-12.6***