Компьютерные угрозы безопасности и основы антивирусной защиты

Выполнил: Цирулик И.А

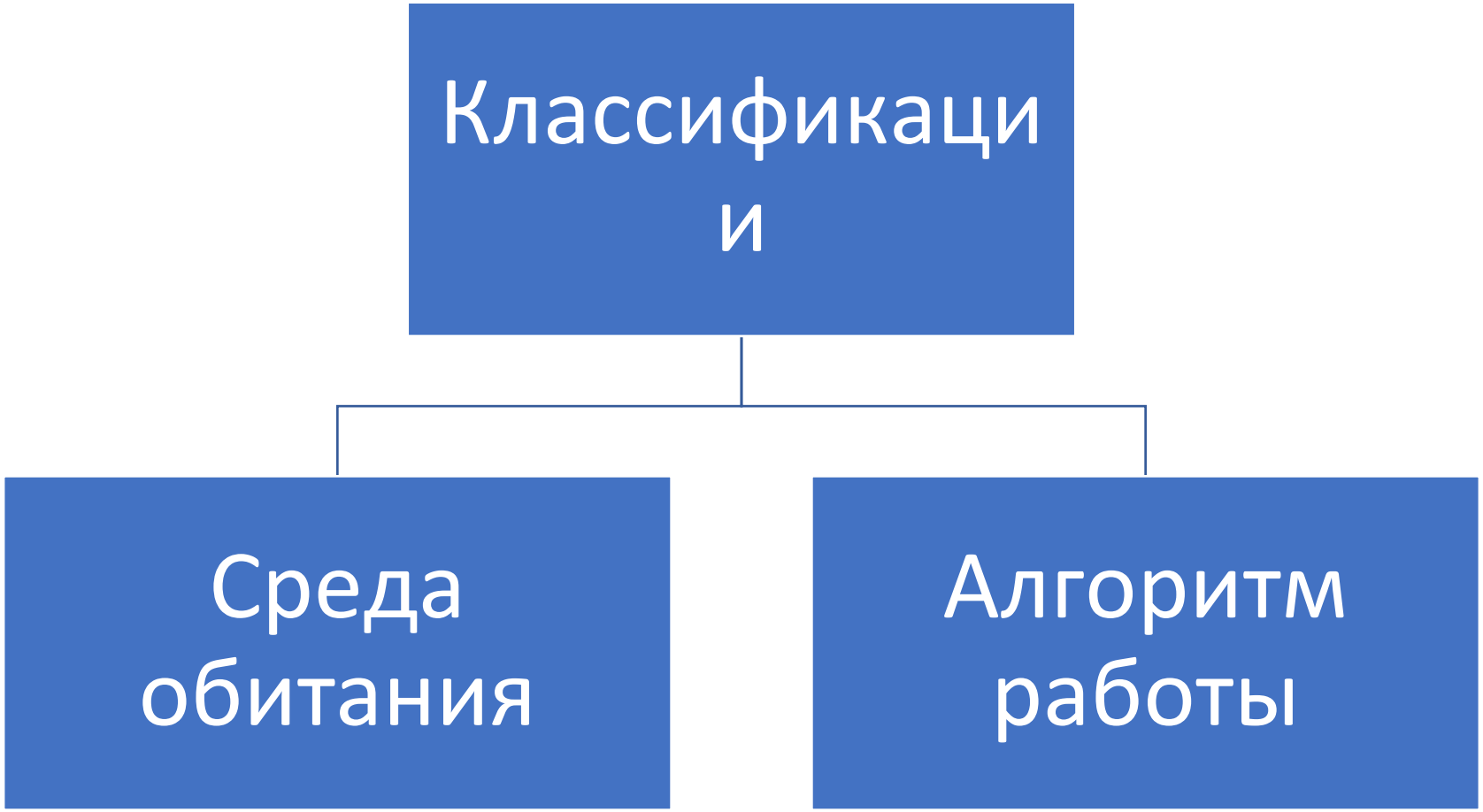
Актуальность:

- В современном мире информация является самой главной ценностью, и именно поэтому необходимо знать виды угроз, которые могут разрушить и повредить её

Цели

- Рассмотреть возможные виды компьютерных угроз
- Классифицировать угрозы по нескольким признакам
- Проанализировать полученные данные
- Сделать вывод

Классификации:



Возможная среда обитания:

- ***Файловые вирусы*** - заражают исполняемые файлы и активизируются при каждом запуске инфицированного объекта.
- ***Вирусы загрузочного сектора*** - такие вирусы активируются в момент загрузки операционной системы
- ***Макровирусы*** - файлы-документы, к которым относятся как текстовые документы, так и электронные таблицы, разработанные на макроязыках.
- ***Сетевые (скриптовые) вирусы*** - используют протоколы компьютерных сетей и команды скриптовых языков.

Алгоритмы работы:

- ***Вирусы-спутники*** (вирусы-компаньоны) не изменяют исполняемые файлы, а создают их копии с тем же самым названием, но другим, более приоритетным расширением.
- ***Вирусы-черви*** самостоятельно распространяются в каталогах жестких дисков и компьютерных сетях, путем создания там собственных копий.
- ***Вирусы-призраки*** (полиморфные или самошифрующиеся вирусы) имеют зашифрованное тело, благодаря чему две копии одного вируса не имеют одинаковых частей кода.
- ***Руткиты*** позволяют злоумышленникам скрывать следы своей деятельности во взломанной операционной системе. Такого рода программы занимаются сокрытием вредоносных файлов и процессов, а так же собственного присутствия в системе.

Меры защиты:

- В вашей операционной системе должна быть установлена регулярно обновляющаяся хорошая антивирусная программа.
- Наиболее ценные данные должны быть подвержены резервному копированию.
- Разбивайте жесткий диск на несколько разделов. Это позволит изолировать важную информацию и не держать ее на системном разделе, куда была установлена ваша ОС. Ведь именно он является основной мишенью злоумышленников.
- Не посещайте веб-сайты сомнительного содержания и особенно те, которые занимаются незаконным распространением контента, ключей и генераторов ключей к платным программам. Как правило, там, помимо бесплатной «халявы», находится огромное количество вредоносных программ всех разновидностей.
- При использовании электронной почты не открывайте и не запускайте почтовые вложения из писем от незнакомых адресатов.
- Всем любителям общения с помощью интернет-пейджеров (QIP, ICQ) так же следует остерегаться скачивания файлов и переходов по ссылкам, присланными незнакомыми контактами.

Вывод:

- После прочтения данного материала, вы теперь понимаете, насколько важно со всей серьезностью отнестись к вопросу безопасности и защищенности вашего компьютера от вторжений злоумышленников, и воздействий на него вредоносными программами.
  На данный момент существует огромное количество компаний, которые занимаются разработкой антивирусного ПО и как вы понимаете, запутаться с его выбором не составит труда. А ведь это очень ответственный момент, так как именно антивирус является стеной, ограждающей вашу систему от потока заразы, льющейся из сети. И если у этой стены будет много брешей, то и толку-то в ней ноль.

Спасибо за внимание!