«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ**

**Используя параграф 1.10 электронного пособия «Компьютерные вирусы и антивирусные программы», выполните задания.**

**Задание 1.** Вставьте пропущенные слова в определении компьютерного вируса

*Компьютерный вирус* – это \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, которая способна самостоятельно \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в другие программы и системные области дисковой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ компьютера либо распространяться по \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Задание 2.** Заполните схему «Признаки классификации вирусов»

|  |
| --- |
| **Признаки классификации вирусов** |
|  |  |  |  |  |

**Задание 3.** Запишите виды вирусов по различным классификациям.

|  |
| --- |
| **КЛАССИФИКАЦИЯ ВИРУСОВ** |
| **По среде обитания** | **По разрушительным возможностям** | **По особенностям построения** | **По способу заражения** | **По целостности** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Задание 4.** Какие еще вредоносные программы (кроме вирусов) существуют?

|  |  |  |
| --- | --- | --- |
| Название |  |  |
| Особенности заражения компьютера |  |  |

**Задание 5.** Запишите определение понятия «антивирус».

*Антивирусная программа (антивирус) -* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Задание 6.** Какие существуют пять основных типов антивирусных средств защиты? В чем их особенности?

|  |  |
| --- | --- |
| **Тип антивируса** | **Особенность** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Задание 7.** Перечислите методы защиты компьютера от вирусов

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Задание 8.** Выполните интерактивное задание в пособии.

**ДОМАШНЕЕ ЗАДАНИЕ.**

**Заполните таблицу «Сравнительная характеристика антивирусных программ», используя различные источники информации (в том числе сеть Интернет)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Параметр сравнения** | **Антивирус Касперского** | [**Dr. Web**](file:///C%3A%5CProgram%20Files%5C%D0%9E%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D1%8B%5C%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%2C%2010%20%D0%BA%D0%BB%5CE4HOME_INFORM_10%5Cdata%5Cres%5CDL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442%5C%5BINF10_01_10_2%5D.html) | [**Антивирус Avast!**](file:///C%3A%5CProgram%20Files%5C%D0%9E%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D1%8B%5C%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%2C%2010%20%D0%BA%D0%BB%5CE4HOME_INFORM_10%5Cdata%5Cres%5CDL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442%5C%5BINF10_01_10_5%5D.html) | [**Eset NOD32**](file:///C%3A%5CProgram%20Files%5C%D0%9E%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D1%8B%5C%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%2C%2010%20%D0%BA%D0%BB%5CE4HOME_INFORM_10%5Cdata%5Cres%5CDL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442%5C%5BINF10_01_10_3%5D.html) |
| Логотип | **C:\Program Files\Образовательные комплексы\Информатика, 10 кл\E4HOME_INFORM_10\data\res\DL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442\Images\scene6_1.png** | **C:\Program Files\Образовательные комплексы\Информатика, 10 кл\E4HOME_INFORM_10\data\res\DL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442\Images\scene6_2.png** | C:\Program Files\Образовательные комплексы\Информатика, 10 кл\E4HOME_INFORM_10\data\res\DL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442\Images\scene6_5.png | C:\Program Files\Образовательные комплексы\Информатика, 10 кл\E4HOME_INFORM_10\data\res\DL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442\Images\scene6_3.png |
| Производитель |  |  |  |  |
| Число сигнатур |  |  |  |  |
| Отличительные положительные черты |  |  |  |  |
| Возможность обновления антивирусных баз |  |  |  |  |
| Электронный адрес техподдержки |  |  |  |  |
| Стоимость клиентской версии (для домашнего использования) |  |  |  |  |

**Классификация по среде обитания**:
• *сетевые* – вирусы, которые распространяются по различным компьютерным сетям (локальным, беспроводным или через Интернет);
• *файловые* – вирусы, заражающие исполнительные файлы и загружающиеся после запуска зараженных программ, в которых они находятся;
• *загрузочные* – вирусы, которые внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки ОС с системного диска;
• *файлово-загрузочные* – файлово-загрузочные – вирусы, которые способны заражать и файлы, и загрузочные секторы.

**Классификация по разрушительным возможностям:**
• *безвредные* – вирусы, которые только лишь уменьшают объем памяти на диске в результате своего распространения и несколько замедляют работу компьютера;
• *неопасные* – вирусы, которые уменьшают объем памяти, замедляют работу компьютера, а также мешают работе пользователя, порождая графические, звуковые и другие эффекты, но не наносят существенного вреда;
• *опасные* – вирусы, которые могут привести к различным нарушениям в работе компьютера (например к зависанию операционной системы или неправильной печати документа);
• *очень опасные* – вирусы, действие которых может привести к потере программ и данных, стиранию информации в системных областях памяти и т.д.

**Классификация по особенностям построения**:
• *паразитические* – вирусы, которые изменяют содержимое файлов или дисковых секторов, записывая в них свои копии;
• *невидимки* (*стелс-вирусы*) – вирусы, которые трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам или секторам дисков и подставляют вместо себя незараженные участки информации;
• *мутанты* (*призраки, полиморфные вирусы, полиморфики*) – вирусы, которые сложно обнаружить, так как копии одного и того же вируса практически не имеют ни одной повторяющейся цепочки байт;
• *макровирусы* – вирусы, которые используют возможности макроязыков, встроенных в системы обработки данных;

**По способу заражения:**
• *резидентные* – вирусы, оставляющие в оперативной памяти свою резидентную (постоянную) часть, которая потом перехватывает обращения к заражаемым программам и внедряется в них;
• *нерезидентные* – вирусы, которые не заражают оперативную память и проявляются лишь при запуске инфицированной программы.

**По целостности**:
• *монолитные* – вирусы, программы которых представляют собой единый блок;
• *распределенные* – вирусы, программы которых разделены на части, содержащие инструкцию по воссозданию вируса(например, одна какая-то часть заражает компьютер, а затем загружает из Интернета остальные части, выполняющие вредоносное действие).

**Другие вредоносные программы**
Кроме рассмотренных выше компьютерных вирусов, существуют и другие виды вредоносных программ. Среди них, например, можно назвать:
• *cетевые черви* – вредоносные программы, которые распространяются по компьютерным сетям, вычисляя адреса сетевых компьютеров и рассылая по этим адресам свои копии;
• *троянские программы* («*троянские кони*», *квазивирусы*) – вредоносные программы, которые не способны к самораспространению, а маскируются под какую-то полезную или интересную программу, разрушают загрузочный сектор и файловую систему или собирают и пересылают своему создателю информацию, не подлежащую разглашению (например, ваши личные пароли);

**Определение.** *Антивирусная программа* (*антивирус*) – это программа для обнаружения компьютерных вирусов и других вредоносных программ, лечения и восстановления инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

Антивирусные программы

настоящее время не существует единой классификации антивирусных средств защиты компьютеров, однако их можно разделить на пять основных типов.

|  |
| --- |
| **Определение.** *Программы-детекторы* (*сканеры*) обеспечивают поиск и обнаружение конкретных вирусов. Основаны на сравнении специфической последовательности байтов (сигнатур, или масок вирусов), содержащихся в теле вируса, с байтами проверяемых файлов. Их недостатком является то, что они могут находить только вирусы, уже известные разработчикам таких программ.  |

*Универсальные детекторы* проверяют неизменность файлов путем подсчета и сравнения их [**контрольной суммы**](file:///C%3A%5CProgram%20Files%5C%D0%9E%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D1%8B%5C%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0%2C%2010%20%D0%BA%D0%BB%5CE4HOME_INFORM_10%5Cdata%5Cres%5CDL_RES_DD4CF99F-A669-4974-B9FE-ECFF6CF3B442%5C%5BINF10_01_10_6%5D.html) с эталоном. Эталонная контрольная сумма указывается в документации на программный продукт или подсчитывается в самом начале эксплуатации с помощью специального модуля программы. Недостаток таких детекторов связан с невозможностью определения причин искажения файлов.

*Специализированные детекторы* ввыполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Их недостаток состоит в том, что они способны обнаруживать только часть известных вирусов (для которых в их вирусной базе есть сигнатуры) и не могут обнаруживать новые вирусы, еще не занесенные в их вирусную базу.

Детектор, позволяющий обнаруживать несколько различных видов вирусов, называют *полидетектором*.

|  |
| --- |
| **Определение.** *Программы-докторы* (*фаги*, *дезинфекторы*) не только находят файлы, зараженные вирусом, но и лечат их, удаляя из файлов тело вируса и возвращая файлы в исходное состояние. Полифаги – программы-докторы, предназначенные для поиска и уничтожения большого количества разных видов вирусов.  |

|  |
| --- |
| **Определение.** *Программы-ревизоры* анализируют текущее состояние файлов и системных областей дисков и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние Boot-сектора, FAT, а также длина файлов, код циклического контроля (контрольная сумма файла), дата и время модификации, атрибуты и другие параметры файлов.  |

|  |
| --- |
| **Определение.** *Программы-фильтры* – резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия, а пользователь сам принимает решение о разрешении или запрещении выполнения этих действий. Фильтры контролируют обновление программных файлов и системной области дисков, форматирование диска, загрузку программ в ОЗУ. Однако они не способны обезвредить вирус, для этого нужно применять фаги.  |

|  |
| --- |
| **Определение.** *Программы-иммунизаторы* (*вакцины*) –  резидентные программы, предотвращающие заражение файлов. Принцип их работы состоит в том, что в программу записываются признаки конкретного вируса, так что подобный вирус считает ее «уже зараженной» и не производит повторное инфицирование. Эти программы наименее эффективны и морально устарели. |