**Практическая работа №18**

**Тема:** Решение задач по обеспечению защиты ОС.

**Цель**: Ознакомление и приобретение практических навыков работы с программными антивирусными средствами.

**Задание(я):**

1. Ознакомиться с теоретическими сведениями.

2. Установить антивирусную программу.

3. Выполнить самостоятельное задание.

4. Оформить отчёт согласно требованиям.

*Вывод.*

**Методические указания к выполнению:**

Выполнение задания 1

Вредительские программы и, прежде всего, [вирусы](https://pandia.ru/text/category/virus/) представляют очень серьезную опасность для информации в КС. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. Вредит использованию всех возможностей КС и чрезмерное преувеличение опасности вирусов. Знание механизмов действия вирусов, методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и потерь от их воздействия.

**«Компьютерные вирусы»** это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения (репликации) в компьютерной системе. Вирусы могут выполнять изменение или уничтожение [программного обеспечения](https://pandia.ru/text/category/programmnoe_obespechenie/) или данных, хранящихся в КС. В процессе распространения вирусы могут себя модифицировать.

**Классификация компьютерных вирусов**

Все компьютерные вирусы могут быть классифицированы по следующим признакам:

• по среде обитания;

• по способу заражения;

• по степени опасности [деструктивных](https://pandia.ru/text/category/destruktciya/) (вредительских)воздействий;

• по алгоритму функционирования.

**По среде обитания** компьютерные вирусы делятся на:

• сетевые;

• файловые;

• загрузочные;

• комбинированные.

Средой обитания сетевых вирусов являются элементы компьютерных сетей. Файловые вирусы размещаются в исполняемых файлах. Загрузочные вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (bootсекторах). Иногда загрузочные вирусы называют бутовыми. Комбинированные вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат загрузочно-файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов.

**По способу заражения среды обитания** компьютерные вирусы делятся на:

• резидентные;

• [нерезидентные](https://pandia.ru/text/category/nerezidenti/).

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя, как правило, привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. В отличие от резидентных нерезидентные вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания. Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

Арсенал [деструктивных](https://pandia.ru/text/category/destruktciya/) или вредительских возможностей компьютерных [вирусов](https://pandia.ru/text/category/virus/) весьма обширен. Деструктивные возможности вирусов зависят от целей и квалификации их создателя, а также от особенностей компьютерных систем.

**По степени опасности** для информационных ресурсов пользователя компьютерные вирусы можно разделить на:

• безвредные вирусы;

• опасные вирусы;

• очень опасные вирусы.

Безвредные компьютерные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам КС. Деструктивное воздействие таких вирусов сводится к выводу на экран монитора невинных текстов и картинок, исполнению музыкальных фрагментов и т. п. Однако эти вирусы наносят определенный ущерб КС. Во-первых, такие вирусы расходуют ресурсы КС, в той или иной мере снижая ее эффективность функционирования. Во-вторых, компьютерные вирусы могут содержать ошибки, вызывающие опасные последствия для информационных ресурсов КС. Кроме того, при модернизации операционной системы или аппаратных средств КС вирусы, созданные ранее, могут приводить к нарушениям штатного алгоритма работы системы. К опасным относятся вирусы, которые вызывают существенное снижение эффективности КС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. Последствия таких вирусов могут быть ликвидированы без особых затрат материальных и временных ресурсов. Примерами таких вирусов являются вирусы, занимающие память ЭВМ и каналы связи, но не блокирующие работу сети; вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы или повторной передачи данных по каналам связи и т. п.

Очень опасными следует считать вирусы, вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию (в том числе и шифрование) информации, а также вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств и наносящие ущерб здоровью пользователям. Такие вирусы стирают отдельные файлы, системные области памяти, форматируют диски, получают несанкционированный доступ к информации, шифруют данные и т. п. Известны публикации, в которых упоминаются вирусы, вызывающие неисправности аппаратных средств. Предполагается, что на резонансной частоте движущиеся части электромеханических устройств, например в системе позиционирования накопителя на магнитных дисках, могут быть разрушены. Именно такой режим и может быть создан с помощью программы-вируса.

Использование в современных ПЭВМ постоянной памяти с возможностью перезаписи привело к появлению вирусов, изменяющих программы BIOS, что приводит к необходимости замены постоянных запоминающих устройств. Возможны также воздействия на психику человека оператора ЭВМ с помощью подбора видеоизображения, выдаваемого на экран монитора с определенной частотой (каждый двадцать пятый кадр). Встроенные кадры этой видеоинформации воспринимаются человеком на подсознательном уровне. В результате такого воздействия возможно нанесение серьезного ущерба психике человека.

В соответствии **с особенностями алгоритма функционирования** вирусы можно разделить на два класса:

• вирусы, не изменяющие среду обитания (файлы и секторы) при распространении;

• вирусы, изменяющие среду обитания при распространении.

В свою очередь, вирусы, не изменяющие среду обитания, могут быть разделены на две группы:

• вирусы «спутники» (companion);

• вирусы «черви» (worm).

Вирусы «спутники» не изменяют файлы. Механизм их действия состоит в создании копий исполняемых файлов. Например, в MS DOS такие вирусы создают копии для файлов, имеющих расширение. ЕХЕ. Копии присваивается то же имя, что и исполняемому файлу, но расширение изменяется на. СОМ. При запуске файла с общим именем операционная система первым загружает на выполнение файл с расширением. СОМ, который является программой-вирусом. Файл-вирус запускает затем и файл с расширением. ЕХЕ.

Вирусы-«черви» попадают в рабочую станцию из сети, вычисляют адреса рассылки вируса по другим абонентам сети и осуществляют передачу вируса. Вирус не изменяет файлов и не записывается в загрузочные секторы дисков. Некоторые вирусы-«черви» создают рабочие копии вируса на диске, другие размещаются только в оперативной памяти ЭВМ.

По сложности, степени совершенства и **особенностям маскировки алгоритмов** вирусы, изменяющие среду обитания, делятся на:

• студенческие;

• «стелс» вирусы (вирусы-невидимки);

• полиморфные.

К студенческим относят вирусы, создатели которых имеют низкую квалификацию. Такие вирусы, как правило, являются [нерезидентными](https://pandia.ru/text/category/nerezidenti/), часто содержат ошибки, довольно просто обнаруживаются и удаляются.

«Стелс» - вирусы и полиморфные вирусы создаются квалифицированными специалистами, хорошо знающими принцип работы аппаратных средств и операционной системы, а также владеющими навыками работы с машинно-ориентированными системами программирования. «Стелс» - вирусы маскируют свое присутствие в среде обитания путем перехвата обращений операционной системы к пораженным файлам, секторам и переадресуют ОС к незараженным участкам информации. Вирус является резидентным, маскируется под программы ОС, может перемещаться в памяти. Такие вирусы активизируются при возникновении прерываний, выполняют определенные действия, в том числе и по маскировке, и только затем управление передается на программы ОС, обрабатывающие эти прерывания. «Стелс» вирусы обладают способностью противодействовать резидентным антивирусным средствам.

Полиморфные вирусы не имеют постоянных опознавательных групп сигнатур. Обычные вирусы для распознавания факта заражения среды обитания размещают в зараженном объекте специальную опознавательную двоичную последовательность или последовательность символов (сигнатуру), которая однозначно идентифицирует зараженность файла или сектора. Сигнатуры используются на этапе распространения вирусов для того, чтобы избежать многократного заражения одних и тех же объектов, так как при многократном заражении объекта значительно возрастает вероятность обнаружения вируса. Для устранения демаскирующих признаков полиморфные вирусы используют шифрование тела вируса и модификацию программы шифрования. За счет такого преобразования полиморфные вирусы не имеют совпадений кодов.

**Файловые вирусы** могут внедряться только в исполняемые файлы: командные файлы (файлы, состоящие из команд операционной системы), саморазархивирующиеся файлы, пользовательские и системные программы в машинных кодах, а также в документы (таблицы), имеющие макрокоманды. Макрокоманды или макросы представляют собой исполняемые программы для автоматизации работы с документами (таблицами). Поэтому такие документы (таблицы) можно рассматривать как исполняемый файл.

Для IBM совместимых ПЭВМ вирус может внедряться в файлы следующих типов: командные файлы (ВАТ), загружаемые драйверы (SYS), программы в машинных (двоичных) кодах (ЕХЕ, СОМ), документы Word (DOC) с версии 6.0 и выше, таблицы165EXCEL (XLS). Макровирусы могут внедрятся и в другие файлы, содержащие макрокоманды. Файловые вирусы могут размещаться в начале, середине и конце заражаемого файла. Независимо от места расположения вируса в теле зараженного файла после передачи управления файлу первыми выполняются команды вируса.

В начало файла вирус внедряется одним из трех способов. Первый из них заключается в переписывании начала файла в его конец, а на освободившееся место записывается вирус. Второй способ предполагает считывание вируса и зараженного файла в оперативную память, объединение их в один файл и запись его наместо файла. При третьем способе заражения вирус записывается в начало файла без сохранения содержимого. В этом случае зараженный файл становится неработоспособным.

В середину файла вирус может быть записан также различными способами. Файл может «раздвигаться», а в освободившееся место может быть записан вирус. Вирус может внедряться в середину файла без сохранения участка файла, на место которого помещается вирус.

Чаще всего вирус внедряется в конец файла. При этом, как и в случае с внедрением вируса в середину файла, первые команды файла заменяются командами перехода на тело вируса.

**Алгоритм работы файлового вируса.** Несмотря на многообразие файловых вирусов, можно выделить действия и порядок их выполнения, которые присутствуют при реализации большинства вирусов этого класса. Такой обобщенный алгоритм может быть представлен в виде следующей последовательности шагов:

1. Резидентный вирус проверяет, заражена ли оперативная память, и при необходимости заражает ее. Нерезидентный вирус ищет незараженные файлы и заражает их.

2. Выполняются действия по сохранению работоспособности программы, в файл которой внедряется вирус (восстановление первых байт программы, настройка адресов программ и т. д.)

3. Осуществляется деструктивная функция вируса, если выполняются соответствующие условия.

4. Передается управление программе, в файле которой находится вирус.

**Особенности макровирусов**.

Особое место среди файловых вирусов занимают макровирусы. Макровирусы представляют собой вредительские программы, написанные на макроязыках, встроенных в текстовые редакторы, электронные таблицы и др.

Для существования вирусов в конкретной системе (редакторе) необходимо, чтобы встроенный в нее макроязык, имел следующие возможности:

• привязку программы на макроязыке к конкретному файлу;

• копирование макропрограмм из одного файла в другой;

• получение управления макропрограммой без вмешательства пользователя.

Таким условиям отвечают редакторы MS Word, MS Office, Ami Pro, табличный процессор MS Excel. В этих системах используются макроязыки Word Basic и Visual Basic. При выполнении определенных действий над файлами, содержащими макропрограммы (открытие, сохранение, закрытие и т. д.), автоматически выполняются макропрограммы файлов. При этом управление получают макровирусы, которые сохраняют активность до тех пор, пока активен соответствующий редактор (процессор). Поэтому при работе с другим файлом в «зараженном редакторе (процессоре)», он также заражается. Здесь прослеживается аналогия с резидентными вирусами по механизму заражения.

Для получения управления макровирусы, заражающие файлы MSOffice, как правило, используют один из приемов:

1) в [вирусе](https://pandia.ru/text/category/virus/) имеется автомакрос (выполняется автоматически, при открытии документа, таблицы);

2) в вирусе переопределен один из стандартных макросов, который выполняется при выборе определенного пункта меню;

3) макрос вируса автоматически вызывается на выполнение при нажатии определенной клавиши или комбинаций клавиш.

**Загрузочные вирусы.**

Загрузочные вирусы заражают загрузочные (Boot) сектора гибких дисков и Boot-сектора или Master Boot Record (MBR) жестких дисков. Загрузочные вирусы являются резидентными. Заражение происходит при загрузке операционной системы с дисков. После включения ЭВМ осуществляется контроль ее работоспособности с помощью программы, записанной в постоянном запоминающем устройстве. Если проверка завершилась успешно, то осуществляется считывание первого сектора с гибкого или жесткого диска. Порядок использования дисководов для загрузки задается пользователем при помощи программы Setup. Если диск, с которого производится загрузка ОС заражен загрузочным вирусом, то обычно выполняются следующие шаги:

1. Считанный из 1го сектора диска загрузочный вирус (часть вируса) получает управление, уменьшает объем свободной памяти ОП и считывает с диска тело вируса.

2. Вирус переписывает сам себя в другую область, чаще всего в старшие адреса памяти.

3. Устанавливаются необходимые вектора прерываний (вирус резидентный).

4. При выполнении определенных условий производятся [деструктивные](https://pandia.ru/text/category/destruktciya/) действия.

5. Копируется Boot-сектор в ОП и передается ему управление.

Если вирус был активизирован с гибкого диска, то он записывается в загрузочный сектор жесткого диска. Активный вирус, постоянно находясь в ОП, заражает загрузочные сектора всех гибких дисков, а не только системные диски. Заражение рабочих гибких дисков загрузочными вирусами выполняется в расчете на ошибочные действия пользователя ЭВМ в момент загрузки ОС. Если установлен порядок загрузки ОС сначала с гибкого диска, а затем с жесткого, то при наличии гибкого диска в накопители будет считан 1-й сектор с гибкого диска. Если диск был заражен, то этого достаточно для заражения ЭВМ. Такая ситуация наиболее часто имеет место при перезагрузке ОС после «зависаний» или отказов ЭВМ.

Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации, образуя методы борьбы с вирусами.

Можно выделить **методы обнаружения вирусов** и методы удаления вирусов:

• сканирование;

• обнаружение изменений;

• эвристический анализ;

• использование резидентных сторожей;

• [вакцинирование](https://pandia.ru/text/category/vaktcina/) программ;

• аппаратно-программная защита от вирусов.

**Сканирование** один из самых простых методов обнаружения вирусов. Сканирование осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса сигнатуры. Программа фиксирует наличие уже известных вирусов, за исключением полиморфных вирусов, которые применяют шифрование тела вируса, изменяя при этом каждый раз и сигнатуру. Программы-сканеры могут хранить не сигнатуры известных вирусов, а их [контрольные суммы](https://pandia.ru/text/category/kontrolmznaya_summa/). Программы-сканеры часто могут удалять обнаруженные вирусы. Такие программы называются полифагами. Метод сканирования применим для обнаружения вирусов, сигнатуры которых уже выделены и являются постоянными. Для эффективного использования метода необходимо регулярное обновление сведений о новых вирусах.

**Метод обнаружения изменений** базируется на использовании программ-ревизоров. Эти программы определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы. При периодическом выполнении программ-ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков. По результатам ревизии программа выдает сведения о предположительном наличии вирусов. Обычно программы-ревизоры запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, характеристики всех контролируемых файлов, каталогов и номера дефектных кластеров. Могут контролироваться также объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры. Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов. Совершенные программы-ревизоры обнаруживают даже «стелс» - вирусы. Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными. Вирусы будут обнаружены только после размножения в системе. Программы-ревизоры непригодны для обнаружения заражения макровирусами, так как документы и таблицы очень часто изменяются.

**Эвристический анализ** сравнительно недавно начал использоваться для обнаружения вирусов. Как и метод обнаружения изменений, данный метод позволяет определять неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе. Сущность эвристического анализа заключается в проверке возможных сред обитания вирусов и выявление в них команд (групп команд), характерных для вирусов. Такими командами могут быть команды создания резидентных модулей в оперативной памяти, команды прямого обращения к дискам, минуя ОС. Эвристические анализаторы при обнаружении «подозрительных» команд в файлах или загрузочных секторах выдают сообщение о возможном заражении. После получения таких сообщений необходимо тщательно проверить предположительно зараженные файлы и загрузочные сектора всеми имеющимися антивирусными средствами.

**Метод использования резидентных сторожей** основан на применении программ, которые постоянно находятся в ОП ЭВМ и отслеживают все действия остальных программ. В случае выполнения какой-либо программой подозрительных действий (обращение для записи в загрузочные сектора, помещение в ОП резидентных модулей, попытки перехвата прерываний ит. п.) резидентный сторож выдает сообщение пользователю. Программа-сторож может загружать на выполнение другие антивирусные программы для проверки «подозрительных» программ, а также для контроля всех поступающих извне файлов (со сменных дисков, по сети).Существенным недостатком данного метода является значительный процент ложных тревог, что мешает работе пользователя, вызывает раздражение и желание отказаться от использования резидентных сторожей.

**Под вакцинацией программ** понимается создание специального модуля для контроля ее целостности. В качестве характеристики целостности файла обычно используется контрольная сумма. При заражении вакцинированного файла, модуль контроля обнаруживает изменение контрольной суммы и сообщает об этом пользователю. Метод позволяет обнаруживать все вирусы, в том числе и незнакомые, за исключением «стелс» - вирусов.

Самым надежным методом защиты от вирусов является **использование аппаратно-программных антивирусных средств**. В настоящее время для защиты ПЭВМ используются специальные контроллеры и их [программное обеспечение](https://pandia.ru/text/category/programmnoe_obespechenie/). Контроллер устанавливается в разъем расширения и имеет доступ к общей шине. Это позволяет ему контролировать все обращения к дисковой системе. В программном обеспечении контроллера запоминаются области на дисках, изменение которых в обычных режимах работы не допускается. Таким образом, можно установить защиту на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др. При выполнении запретных действий любой программой контроллер выдает соответствующее сообщение пользователю и блокирует работу ПЭВМ. Аппаратно-программные антивирусные средства обладают рядом достоинств перед программными:

• работают постоянно;

• обнаруживают все вирусы, независимо от механизма их действия;

• блокируют неразрешенные действия, являющиеся результатом работы вируса или неквалифицированного пользователя.

Недостаток у этих средств один зависимость от аппаратных средств ПЭВМ. Изменение последних ведет к необходимости замены контроллера.

В настоящее время существует огромное количество антивирусных программ от различных разработчиков, многие из которых имеют мировую известность, другие появились на рынке антивирусных средств защиты компьютеров недавно, но, несмотря на это, быстро прогрессируют, составляя ощутимую конкуренцию наиболее популярным производителям антивирусов.

Сегодня известно довольно много компаний, профессионально тестирующих и составляющих рейтинги антивирусов. Несмотря на их [авторитет](https://pandia.ru/text/category/avtoritet/) и профессионализм, результаты этих рейтингов не одинаковы. Это объясняется тем, что они применяют различные методики тестирования антивирусов, а также не одинаковые критерии оценки качества антивирусных пакетов.

К наиболее известным программным антивирусным средствам относятся компании:

- GriSoft (AVG);

- Avira;

- Dr. Web;

- Антивирус Касперского;

- Panda Software;

- McAfee;

- Eset NOD32 и др.

**Kaspersky Internet Security** - программа для комплексной защиты ПК от вирусов и других типов вредоносных программ, а также от хакерских атак и спама.

Выполняет защиту компьютера от вирусов, сетевых атак, червей, предотвращает дальнейшие несанкционированные действия вредоносных программ после их обнаружения, проверяет файлы и программы по мере их задействования (просмотр списка файлов в папке, открытие документа или программы и т. п.).

К основным функциям относятся:

*Базовая защита*

* Комплексная защита от всех видов вредоносных программ.
* Проверка файлов, почтовых сообщений и интернет-трафика.
* Защита интернет-пейджеров (ICQ, MSN).
* Автоматическое обновление баз.

*Расширенная защита*

* Персональный сетевой экран.
* Безопасная работа в сетях Wi-Fi и VPN.
* Защита от сетевых атак.

*Предотвращение угроз*

* Инновационная система установки правил и контроля работы приложений.
* Проактивная защита от новых и неизвестных угроз.
* Поиск уязвимостей в ОС и установленном ПО.
* Блокирование ссылок на зараженные сайты.

*Защита конфиденциальных данных*

* Блокирование ссылок на фишинговые сайты.
* Виртуальная клавиатура для безопасного ввода логинов и паролей.
* Предотвращение кражи данных, передаваемых через SSL-соединение (по HTTPS-протоколу).
* Блокирование несанкционированных телефонных звонков.

*Защита от нежелательного контента*

* Родительский контроль.
* Защита от спама.

Выполнение задания 2

Данное задание мы будем выполнять скачав бесплатную антивирусную программу, например Avast:

1. В поиске вводим скачать антивирусную программу Avast.

2. В открывшемся окне нажимаем кнопку скачать.

3. Сохраняем файл на Рабочий стол и выполняем алгоритм действий которые указаны в Установщике.

4. Антивирус установлен.

Просмотрите видео по установке антивирусной программы Avast. Ссылка дана в списке литературы.

Выполнение задания 3

Самостоятельно выполните следующие задания:

Составьте рекомендации по защите компьютеров от [вирусов](https://pandia.ru/text/category/virus/):

1)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перечислите наиболее известные антивирусные программы:

1)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Перечислите организационные мероприятия по защите ценной информации:

1)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Сопоставьте названия программ и изображений:**

1) 2) 3) 

4)  5) 6) 

* \_\_ Avira
* \_\_ DrWeb
* \_\_ Nod 32
* \_\_ Antivirus Kaspersky
* \_\_ Avast
* \_\_ Antivirus Panda

**На этом практическое занятие завершено, ответьте на вопросы для самоконтроля, а также оформите отчёт согласно требованиям.**

**Вопросы для самоконтроля:**

1. Назовите признаки классификации компьютерных [вирусов](https://pandia.ru/text/category/virus/).

2. Поясните принцип действия «стелс»-вирусов и полиморфных вирусов.

3. Приведите структуру файлового вируса и поясните алгоритм его работы.

4. В чем заключаются особенности алгоритмов функционирования макровирусов и загрузочных вирусов?

5. Дайте характеристику методов обнаружения вирусов.

6. Опишите интерфейс программы антивирус Касперского

7. Что такое файл трассировки и как его создать

8. Опишите алгоритм работы компонента Антивирусная защита файловой системы

9 . Что такое Контроль доступа. Как изменить параметры работы Контроля доступа

10. Опишите этапы проверки компьютера на вирусы

11. Опишите этапы обновления программы Антивирус

12. Дайте понятие «черный список адресов» и «белый список адресов»

13. Дайте определение понятию маска файла и маска подсети

14. Что такое спам?

**15. Просмотрите видео (ссылка на видео дана в списке литературы)**.

**Список литературы и ссылки на Интернет-ресурсы, содержащие информацию по теме:**

1. <https://studopedia.ru/11_130623_bezopasnost-operatsionnih-sistem-sredstva-zashchiti-informatsii-v-seti.html>, Защита ОС (справочные материалы).

2. <https://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html> Компьютерные вирусы (статьи).

3. <https://yadi.sk/i/uAONH0yolydcJw> Установка антивирусной программы Avast (видео).