**02.11.2021 МДК0301**

**03.11.2021 МДК0301**

**Лабораторная работа №3 -4 часа**

# Средства защиты компьютера от вирусов. Работа с антивирусными пакетами.

**Цель работы:** ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы. Получить навыки работы с антивирусным пакетом **Антивирус Касперского**.

# Теоретические сведения

**Компьютерный вирус** - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

## Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

* общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
* профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
* специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

* копирование информации - создание копий файлов и системных областей дисков;
* разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей. Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

**Основными путями проникновения вирусов в компьютер**являются **съёмные диски**(гибкие и лазерные), а также **компьютерные сети**. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А: и перезагрузили компьютер, при этом дискета может быть и не системной. Заражение дискеты происходит, даже если её просто вставили в дисковод зараженного компьютера или, например, прочитали её оглавление.

**Признаки заражения**

* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* неожиданное открытие и закрытие лотка CD-ROM-устройства;
* произвольный, без вашего участия, запуск на компьютере каких-либо программ;

Есть также **косвенные признаки заражения** вашего **компьютера**:

* частые зависания и сбои в работе компьютера;
* прекращение работы или неправильная работа ранее успешно работавших программ;
* медленная работа компьютера при запуске программ;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* изменение размеров файлов;
* неожиданное значительное увеличение количества файлов на диске;
* существенное уменьшение размеров свободной оперативной памяти;
* частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
* Microsoft Internet Explorer "зависает" или ведет себя неожиданным образом.

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуем вам провести **полную проверку вашего компьютера**.

**Антивирусные программы.**

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные антивирусные программы. Различают следующие **виды антивирусных программ**:

* **Программы-детекторы**осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатки: могут находить только те вирусы, которые известны разработчикам этой программы, поэтому быстро устаревают и требуют регулярного обновления.
* **Программы-доктора**или**фаги** не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файл в исходное состояние. **Полифаги** – программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Недостатки те же, что и у программ-детекторов.
* **Программы-ревизоры**относятся к самым надежным средствам защиты. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора.
* **Программы-фильтры**или**«сторожа»**представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов (попытки коррекции файлов с расширением EXE или COM, изменение атрибутов файла, запись в загрузочные сектора и т.п.). При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Эти программы способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не лечат файла и диски. Для уничтожения вируса требуется применить другие программы.
* **Вакцины**или **иммунизаторы** это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, лечащие этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. Имеют ограниченное применение.

**Назначение и основные функции Антивируса Касперского Personal**

Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционной системы Windows.

Антивирус Касперского Personal выполняет следующие **функции**:

* **Защита от вирусов и вредоносных программ** - обнаружение и уничтожение вредоносных программ, проникающих через съемные и постоянные файловые носители, электронную почту и протоколы интернета. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):
	+ **Постоянная защита компьютера** - проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
	+ **Проверка компьютера** **по требованию** - проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.
* **Восстановление работоспособности после вирусной атаки**. Полная проверка и лечение позволяет вам удалить все вирусы, поразившие ваши данные при вирусной атаке.
* **Проверка и лечение входящей/исходящей почты** - анализ на присутствие вирусов и лечение входящей почты до ее поступления в почтовый ящик и исходящей почты в режиме реального времени. Кроме того, программа позволяет проверять и лечить почтовые базы различных почтовых клиентов по требованию.
* **Обновление антивирусных баз и программных модулей** - пополнение антивирусных баз информацией о новых вирусах и способах лечения зараженных ими объектов, а также обновление собственных модулей программы. Обновление выполняется с серверов обновлений Лаборатории Касперского или из локального каталога.
* **Рекомендации по настройке программы и работе с ней**- советы от экспертов Лаборатории Касперского, сопровождающие вас в процессе работы с Антивирусом Касперского Personal, и рекомендуемые настройки, соответствующие оптимальной антивирусной защите.
* **Карантин** - помещение объектов, возможно зараженных вирусами или их модификациями, в специальное безопасное хранилище, где вы можете их лечить, удалять, восстанавливать в исходный каталог, а также отправлять экспертам Лаборатории Касперского на исследование. Файлы на карантине хранятся в специальном формате и не представляют опасности.
* **Формирование отчета**- фиксирование всех результатов работы Антивируса Касперского Personal в отчете. Подробный отчет о результатах проверки включает общую статистику по проверенным объектам, хранит настройки, с которыми была выполнена та или иная задача, а также последовательность проверки и обработки каждого объекта в отдельности.

**Как проверить CD-диск или дискету.**

Через дискеты, CD и другие съемные диски легко заразить компьютер вирусом. Если дискета (или загрузочный CD-диск) заражена загрузочным вирусом, и вы оставили ее в дисководе и перезагрузились, результаты могут быть самые печальные.

**Рекомендуем вам проверять все съемные диски перед их использованием**.

Вы можете запустить проверку сменных дисков из главного окна Антивируса Касперского Personal, а также из контекстного меню Windows.

**Для проверки сменных дисков из контекстного меню Windows**

1. Выберите диски (вы можете выбрать сразу и CD-диск и дискету).
2. Установите курсор мыши на имени выбранного объекта.
3. Щелчком по правой кнопке мыши откройте контекстное меню Windows и выберите пункт **Проверить на вирусы**.



Чтобы проверить **CD-диск или дискету на присутствие вирусов из главного окна Антивируса Касперского Personal**

1. Вставьте CD-диск в CD-ROM-устройство или дискету в дисковод. Обратите внимание, программа сможет проверить и CD-диск и дискету за один прием.
2. Воспользуйтесь гиперссылкой Проверить съемные диски, расположенной в левой части закладки **Защита**.



**или**

По гиперссылке Проверить объекты перейдите в окно **Выбор объектов для проверки**, выберите съемные диски и нажмите на кнопку **Проверить**.



Сразу после запуска проверки на экране откроется окно **Проверка**, где будет отображаться процесс выполнения действия над выбранными объектами списка.



Если для проверки вы выбрали только один съемный диск (устройство), по окончании проверки Антивирус Касперского Personal предложит вставить следующий диск (устройство).

**Обратите внимание на некоторые особенности работы программы:**

* Если вы забыли вставить диск или дискету перед запуском проверки, либо съемный накопитель, дисковод или CD-ROM, отключен, проверка проводиться не будет, и программа не выдаст никакого дополнительного сообщения по этому поводу.
* Если вы вставили дискету в дисковод уже после запуска проверки, она не будет проверена. То же относится к CD-диску и другим съемным дискам.
* Если вы вынули дискету из дисковода или отключили съемный диск во время его проверки, программа занесет в отчет сообщение об ошибке, но не выдаст на экран никакого дополнительного сообщения. Программа перейдет к проверке следующего съемного диска, если таковой есть.

В момент монтирования съемного диска в систему (когда диск определяется операционной системой как новое устройство) Антивирус выполнит проверку такого диска и на присутствие **boot-вируса.**

Во время выполнения проверки компьютера, выбранных объектов, обновления антивирусных баз, а также постоянной защиты формируется отчет о проверенных объектах и результатах их обработки, а также общая статистика. Полный список всех выполняемых задач ведется Антивирусом Касперского в окне **Отчеты**, открыть который можно по гиперссылке Просмотреть отчеты в левой части закладки **Защита**. Здесь фиксируется статус каждой задачи, а также дата и время ее окончания.

## Полный список выполняемых задач Антивирусом Касперского в окне Отчеты

Информация по обработке объекта может быть следующих видов:

 или   Информационное сообщение (например: задача запущена, задача завершена, задача выполняется, задача приостановлена).

 Внимание (например: Внимание! Остались необработанные объекты).

** Примечание (например: задача прервана).

Выделив любой отчет и нажав на кнопку Подробнее можно просмотреть информацию о ходе проверки:



а на вкладке Отчет информацию о зараженных и вылеченных объектах:



**Профилактика заражения компьютера вирусами.**

Никакие самые надежные и разумные меры не смогут обеспечить стопроцентную защиту от компьютерных вирусов и троянских программ, но, выработав для себя ряд правил, вы существенно снизите вероятность вирусной атаки и степень возможного ущерба.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика состоит из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.

Ниже перечислены основные правила безопасности, выполнение которых позволит вам избегать вирусных атак.

**Правило № 1**: защитите ваш компьютер с помощью антивирусных программ и программ безопасной работы в интернете. Для этого:

* Безотлагательно установите антивирусную программу.
* Ежедневно обновляйте антивирусные базы. Обновление можно проводить несколько раз в день при возникновениях вирусных эпидемий
* Задайте рекомендуемые настройки для постоянной защиты. Постоянная защита вступает в силу сразу после включения компьютера и затрудняет вирусам проникновение на компьютер.
* Задайте рекомендуемые настройки для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю.

**Правило № 2**: будьте осторожны при записи новых данных на компьютер:

* Проверяйте на присутствие вирусов все съемные диски (дискеты, CD-диски, флэш-карты и пр.) перед их использованием.
* Осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми. В особенности не доверяйте письмам якобы от антивирусных производителей.
* Внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности.
* Если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его антивирусной программой.
* Внимательно относитесь к выбору посещаемых вами интернет-сайтов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернет-червями.

**Правило № 3**: внимательно относитесь к информации об эпидемиях компьютерных вирусов..

В большинстве случаев о начале новой эпидемии сообщается задолго до того, как она достигнет своего пика. Вероятность заражения в этом случае еще невелика, и, скачав обновленные антивирусные базы, вы сможете защитить себя от нового вируса заблаговременно.

**Правило № 4**: с недоверием относитесь к вирусным мистификациям - "страшилкам", письмам об угрозах заражения.

**Правило № 5**: пользуйтесь сервисом Windows Update и регулярно устанавливайте обновления операционной системы Windows.

**Правило №6**: покупайте дистрибутивные копии программного обеспечения у официальных продавцов.

**Правило № 7**: ограничьте круг людей, допущенных к работе на вашем компьютере.

**Правило № 8**: уменьшите риск неприятных последствий возможного заражения:

* Своевременно делайте резервное копирование данных. В случае потери данных система достаточно быстро может быть восстановлена при наличии резервных копий. Дистрибутивные диски, дискеты, флэш-карты и другие носители с программным обеспечением и ценной информацией должны храниться в надежном месте.
* Обязательно создайте системную аварийную дискету, с которой при необходимости можно будет загрузиться, используя "чистую" операционную систему.

# Задание 1.

Подготовить доклад(презентацию) на тему: «Общие сведения и особенности работы антивирусной программы [***Название антивирусной программы***]» (**Название антивирусной программы выбрать согласно своему варианту из *Вариантов заданий к работе***).

# Задание 2.

Изучить антивирусный пакет ***Антивирус Касперского***. Подготовить отчет по лабораторной работе.

# Порядок выполнения

## Скачать и установить Антивирус Касперского

## <https://drive.google.com/file/d/1Epr99wjgglsznxrYLTlLdK6CygERY8eO/view?usp=sharing>

## Сканирование папок на наличие вирусов:

* + Двойным щелчком на значке антивируса на панели индикации открыть главное окно программы;
	+ Изучить содержимое окна: обратить внимание на дату последнего обновления антивирусной базы и дату последней полной проверки компьютера;
	+ В своей личной папке создать папку **Подозрительные файлы** и создать там 2 файла: ***Текстовый файл*** и ***Документ Microsoft Word***. Имена файлов ввести согласно своему варианту по **Вариантам задания к работе**;
	+ Выбрав пункт в главном окне программы пункт **Управление задачами – Выборочная проверка** и добавить в окно область проверки папку **Подозрительные файлы**.
	+ Выполнить проверку папки. По завершению сканирования, используя кнопку

«**Отчеты**» - **«Сохранить отчет…»**, сохранить отчет с результатами проверки в папке **Подозрительные файлы**. Имя файла-отчета – **Scan\_Log**.

## Обновление антивирусной базы:

* + Нажмите на пункт **Обновление** и, используя кнопку **Обновить**, осуществите обновление базы известных вирусов.
	+ По завершению обновления, используя кнопку «**Отчеты**» - **«Сохранить отчет…»**,, сохранить отчет об обновлении в папке **Подозрительные файлы**. Имя файла- отчета – **Upd\_Log.**
	+ Закройте окно **Антивируса Касперского**.

# Содержание отчета:

1). Название и цель лабораторной работы; 2). Доклад на выбранную по варианту тему;

1. Содержимое файла **Scan\_Log.txt** по пункту 1 **Порядка выполнения работы**

Содержание файла **Upd\_Log.txt** по П.2 **Порядка выполнения работы.**

1. Выводы.

# Контрольные вопросы

1). Что называется компьютерным вирусом?

 2). Какая программа называется "зараженной"?

3). Что происходит, когда зараженная программа начинает работу?

4). Как может маскироваться вирус?

1. Каковы признаки заражения вирусом?
2. Каковы последствия заражения компьютерным вирусом?
3. По каким признакам классифицируются компьютерные вирусы?
4. Как классифицируются вирусы по среде обитания?

9). Какие типы компьютерных вирусов выделяются по способу воздействия?

10). Что могут заразить вирусы?

1. Как маскируются "невидимые" вирусы?
2. Каковы особенности самомодифицирующихся вирусов?
3. Какие методы защиты от компьютерных вирусов можно использовать? 14). В каких случаях применяют специализированные программы защиты от

компьютерных вирусов?

15). На какие виды можно подразделить программы защиты от компьютерных вирусов?.

* 1. Каков принцип действия программ-ревизоров, программ-фильтров, программ- вакцин?
1. Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?
2. Перечислите меры защиты информации от компьютерных вирусов. 22). Каковы современные технологии антивирусной защиты?
3. Каковы возможности антивируса Касперского для защиты файловых серверов? почтовых серверов?
4. Какие модули входят в состав антивируса Касперского для защиты файловых систем?
5. Каково назначение этих модулей антивируса Касперского для защиты файловых систем?

# Варианты заданий к работе

|  |  |  |
| --- | --- | --- |
| **Вариант** | **Название антивирусной программы** | **Название файла** |
| 1 | Антивирус Касперского | Test\_01\_01.txt Test\_02\_01.doc |
| 2 | McAfee VirusScan | Test\_01\_02.txtTest\_02\_02.doc |
| 3 | Dr.Web | Test\_01\_03.txtTest\_02\_03.doc |
| 4 | Panda Anti-Virus | Test\_01\_04.txt Test\_02\_04.doc |
| 5 | Avast! | Test\_01\_05.txt Test\_02\_05.doc |
| 6 | AVS | Test\_01\_06.txtTest\_02\_06.doc |
| 7 | AVG | Test\_01\_07.txt Test\_02\_07.doc |
| 8 | Avira | Test\_01\_08.txt Test\_02\_08.doc |
| 9 | Clam AntiVirus | Test\_01\_09.txt Test\_02\_09.doc |
| 10 | ClamWin | Test\_01\_10.txtTest\_02\_10.doc |
| 11 | NOD32 | Test\_01\_11.txt Test\_02\_11.doc |
| 12 | Trojan Hunter | Test\_01\_12.txtTest\_02\_12.doc |
| 13 | VirusBuster | Test\_01\_13.txtTest\_02\_13.doc |
| 14 | Norton AntiVirus | Test\_01\_14.txt Test\_02\_14.doc |
| 15 | Windows Live OneCare | Test\_01\_15.txt Test\_02\_15.doc |
| 16 | PC-cillin | Test\_01\_16.txt Test\_02\_16.doc |
| 17 | F-Prot | Test\_01\_17.txtTest\_02\_17.doc |
| 18 | F-Secure Anti-Virus | Test\_01\_18.txt Test\_02\_18.doc |
| 19 | Comodo AntiVirus | Test\_01\_19.txtTest\_02\_19.doc |
| 20 | Bitdefender | Test\_01\_20.txt Test\_02\_20.doc |
| 21 | Windows Defender Offline | Test\_01\_21.txtTest\_02\_21.doc |
| 22 | VBA32 | Test\_01\_22.txt Test\_02\_22.doc |
| 23 | Zillya!  | Test\_01\_23.txtTest\_02\_23.doc |
| 24 | Sophos | Test\_01\_24.txtTest\_02\_24.doc |

Присылать Отчеты **kuzn117@yandex.ru Срок 05.11.2021**