**Тема 3-4 Современные компьютерные угрозы и методы борьбы с ними**

**Цель:** Изучить существующие компьютерные угрозы и основные методы противодействия угрозам

**Вопросы практического занятия:**

*Компьютерные вирусы. Классификация компьютерных вирусов. Методы построения и внедрения шпионов. Профилактика и лечение информационных инфекций. Программы обнаружения и защиты от вирусов и вредоносные программные средства. Устройство, принципы внедрения и действий компьютерных вирусов и вредоносных программных средств.*

**Задания практического занятия:**

1 Подготовьте конспект по вопросам практического занятия

2 Ответьте на контрольные вопросы. Обоснуйте свои ответы.

3 Дискуссия на темы(устный доклад):

5.1 Типы шпионов. Отличие от «классических» вирусов.

5.2 Жизненный цикл шпиона.

5.3 Методы построения и внедрения шпионов.

5.4 Обзор некоторых представителей шпионского ПО.

5.5 Методы борьбы со шпионами. Пример anti spyware.

**Контрольные вопросы:**

**Контрольные вопросы:**

1. Что могут заразить вирусы?

[Дискеты](http://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D0%B5%D1%82%D0%B0" \o "Дискета). Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

[Флеш-накопители](http://ru.wikipedia.org/wiki/%D0%A4%D0%BB%D0%B5%D1%88-%D0%BF%D0%B0%D0%BC%D1%8F%D1%82%D1%8C" \o "Флеш-память) (флешки). В настоящее время [USB-флешки](http://ru.wikipedia.org/wiki/USB_flash_drive" \o "USB flash drive) заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая [цифровые фотоаппараты](http://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%84%D0%BE%D1%82%D0%BE%D0%B0%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82" \o "Цифровой фотоаппарат), цифровые видеокамеры, [портативные цифровые плееры](http://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D0%B8%D0%B3%D1%80%D1%8B%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C" \o "Цифровой проигрыватель), а с 2000-х годов всё большую роль играют [мобильные телефоны](http://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D1%82%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD" \o "Сотовый телефон), особенно[смартфоны](http://ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82%D1%84%D0%BE%D0%BD" \o "Смартфон) (появились [мобильные вирусы](http://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81" \o "Мобильный вирус)). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла[autorun.inf](http://ru.wikipedia.org/wiki/Autorun.inf" \o "Autorun.inf), в котором можно указать программу, запускаемую [Проводником Windows](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%B8%D0%BA_Windows" \o "Проводник Windows) при открытии такого накопителя. В [Windows 7](http://ru.wikipedia.org/wiki/Windows_7" \o "Windows 7) возможность автозапуска файлов с переносных носителей была отключена.

[Электронная почта](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0" \o "Электронная почта). Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный [веб-сайт](http://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B0%D0%B9%D1%82" \o "Веб-сайт), содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа [Outlook](http://ru.wikipedia.org/wiki/Outlook" \o "Outlook) для рассылки самого себя дальше.

[Системы обмена мгновенными сообщениями](http://ru.wikipedia.org/wiki/Instant_messaging" \o "Instant messaging). Здесь также распространена рассылка [ссылок](http://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BF%D0%B5%D1%80%D1%81%D1%81%D1%8B%D0%BB%D0%BA%D0%B0" \o "Гиперссылка) на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по[ICQ](http://ru.wikipedia.org/wiki/ICQ_(%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82)" \o "ICQ (клиент)) и через другие [программы мгновенного обмена сообщениями](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D0%BC%D0%B3%D0%BD%D0%BE%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%BE%D0%B1%D0%BC%D0%B5%D0%BD%D0%B0_%D1%81%D0%BE%D0%BE%D0%B1%D1%89%D0%B5%D0%BD%D0%B8%D1%8F%D0%BC%D0%B8" \o "Программа мгновенного обмена сообщениями).

[Веб-страницы](http://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D1%8B" \o "Веб-страницы). Возможно также заражение через страницы [Интернета](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82" \o "Интернет) ввиду наличия на страницах всемирной паутины различного «активного» содержимого: [скриптов](http://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82" \o "Скрипт), [ActiveX](http://ru.wikipedia.org/wiki/ActiveX" \o "ActiveX)-компонент. В этом случае используются уязвимости [программного обеспечения](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5" \o "Программное обеспечение), установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

[Интернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82" \o "Интернет) и [локальные сети](http://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C" \o "Локальная сеть) ([черви](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%87%D0%B5%D1%80%D0%B2%D0%B8" \o "Сетевые черви)). Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» ([уязвимости](http://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)" \o "Уязвимость (компьютерная безопасность))) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки [спама](http://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC" \o "Спам) или для [DDoS-атак](http://ru.wikipedia.org/wiki/DDoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0" \o "DDoS-атака).

2. Как маскируются «невидимые» вирусы?

Многие резидентные вирусы (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Такие вирусы называются невидимыми, или stealth (стелс) вирусами. Разумеется, эффект "невидимости" наблюдается толькона зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.  
*Замечания.* 1. Некоторые антивирусные программы могут обнаруживать "невидимые" вирусы даже на зараженном компьютере. Для этого они выполняют чтение диска, не пользуясь услугами DOS. Такими программами являются, в частности, ADinf фирмы "Диалог-Наука", Norton AntiVirus и др.  
2. Некоторые антивирусные программы используют для борьбы с вирусами свойство "невидимых" файловых вирусов "вылечивать" зараженные файлы. Они считывают (при работающем вирусе) информацию из зараженных файлов и записывают ее в файл или файлы. Затем, уже после загрузки с "чистой" дискеты, исполнимые файлы восстанавливаются в исходном виде.

3. Каковы особенности самомодифицирующихся вирусов?

Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с

помощью дизассемблеров нельзя было разобраться в механизме их работы.

Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры

этой кодировки, а кроме того, изменяют и свою стартовую часть, которая

служит для раскодировки остальных команд вируса. Таким образом, в теле

подобного вируса не имеется ни одной постоянной цепочки байтов, по которой

можно было бы идентифицировать вирус. Это, естественно, затрудняет

нахождение таких вирусов программами-детекторами.

4. Какие методы защиты от компьютерных вирусов можно использовать?

Для защиты от вирусов можно использовать:

* Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
* профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

специализированные программы для защиты от вирусов.

5. В каких случаях применяют специализированные программы защиты от компьютерных вирусов?

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

Антивирусы можно подразделить на две категории: программы, которые непрерывно сканируют потоки данных, например, интернет-трафика, принудительно запускаемые программы с целью сканирования определенных, указанных объектов. Во-вторых, антивирусные программы различаются по виду (способу) защиты от вирусов. Тут можно выделить следующие: Программы-детекторы, или сканеры, находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса. Программы-доктора, (фаги, программы-вакцины) находят зараженные файлы и "лечат" их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus. Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера, затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей. Программы-мониторы (файерволы, брандмауэры) начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас". Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа - небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.  
7. Как действуют программы-детекторы?

**Программы-детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

8. Что называется сигнатурой?

Сигнатура (лат. "signature" – "указывать") — в сфере безопасности компьютерных систем обозначает фрагмент кода или функцию, характерные для определенного типа вирусов. Соответственно, метод обнаружения вредоносного ПО при помощи проверки сигнатур называется "сигнатурным методом". © https://www.bestfree.ru/glossary/rus-s/signatura.php

9. Всегда ли детектор распознает зараженную программу?

Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции ОС, а они перехватываются вирусом, который говорит, что все хорошо. Правда, Aidstest и другие детекторы пытаются выявить вирус путем просмотра оперативной памяти, но против некоторых "хитрых" вирусов это не помогает. Большинство программ-детекторов имеют функцию "доктора", т.е. они пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.  
Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов. К таким программам относится AVSP фирмы "Диалог-МГУ".

10. Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?

**Ревизоры.** Принцип работы ревизоров (например, ADinf) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и т. д.

    При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.

    Недостаток ревизоров состоит в том, что они не могут обнаружить вирус в новых файлах (на дискетах, при распаковке файлов из архива, в электронной почте), поскольку в их базах данных отсутствует информация об этих файлах.

Антивирусы-фильтры - это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия.

Фильтры контролируют следующие операции:

* обновление программных файлов и системной области диска;
* форматирование диска;
* резидентное размещение программ в ОЗУ.

Обнаружив попытку выполнения таких действий, программа сообщает об этом пользователю, который принимает окончательное решение по выполнению данной операции.

**Программы-вакцины (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. Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

11.Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?

12. Перечислите меры защиты информации от компьютерных вирусов.

Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

* оснастите свой компьютер современными антивирусными программами, например Aidstest,DoctorWeb, и постоянно возобновляйте их версии
* перед считыванием с дискет информации, записанной на других компьютерах, всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера
* при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами
* периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты
* всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации
* обязательно делайте архивные копии на дискетах ценной для вас информации
* не оставляйте в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами
* используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей

для обеспечения большей безопасности применения AidstestиDoctorWebнеобходимо сочетать с повседневным использованием ревизора дискаAdinf

13. Каковы современные технологии антивирусной защиты?

Современный рынок программного обеспечения для защиты от различных видов внешних угроз представлен 4-мя основными направлениями:

* антивирусные программы, работающие как по сигнатурному принципу (выявление вредоносного кода), так и на основе эвристического анализатора (анализ кода по нескольким заданным показателям и заключение об опасности/безвредности приложения)
* корпоративные межсетевые экраны (firewall), которые часто используются совместно с network intrusion detection, контролирующей потоки информации в компьютерной сети
* персональные файрволы, анализирующие трафик на конкретном ПК

и, наконец, передовые программы класса Host Intrusion Prevention, основанные на системе проактивной защиты ПК от любых видов угроз, базирующейся на анализе поведения компонентов информационной системы