Министерство образования Республики Беларусь
Частное учреждение образования
«Гродненский колледж бизнеса и права»

Лабораторная работа № 8

по дисциплине
«Защита компьютерной информации»

Тема: Защита от компьютерных вирусов

для учащихся 3 курса специальности
2-40 01 01 «Программное обеспечение информационных технологий»

Тема: Защита от компьютерных вирусов
Цели:
*Образовательная***:**
- сформировать навыки диагностики заражения компьютерным вирусом и работы с антивирусным ПО;

Развивающие:
- научить анализировать, выделять главное, сравнивать, строить аналогии, обобщать и систематизировать;
- создать условия для развития способности четко формулировать свои мысли.

Воспитательные:
- создать условия для воспитания в обучающихся средствами урока уверенности в своих силах;
- создать условия для воспитания сознательного и серьёзного отношения обучающихся к учебной дисциплине.

Тип занятия: лабораторная работа
Время выполнения: 2 часа
Оборудование и методическое обеспечение: IBM PC, карточки с заданием.
План проведения лабораторной работы:

1. **Организационный этап занятия**
2. **Проверка домашнего задания**
3. **Теоретические сведения**
4. **Исполнительский этап занятий**
5. **Постановка домашнего задания**
6. **Оценочно-рефлексивный этап занятия**

Ход занятия

1 Организационный этап занятия

Проверка готовности учащихся к занятию, отметка отсутствующих, объявление темы и цели занятия.

2 Проверка домашнего задания

Устный опрос:
1. Что такое компьютерный вирус?
2. Каким образом могут проявляться действия вирусов?
3. Как можно классифицировать компьютерные вирусы?
4. Назовите меры защиты от компьютерных вирусов.
5. Назовите главные направления профилактики заражения вирусами.

3 Теоретические сведения

Компью́терный ви́рус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. Они приводят к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Бывает, форматируют весь жесткий диск на компьютере. Кроме того, вирусы обычно занимают некоторое место на накопителях информации и отбирают некоторые другие ресурсы системы(портят файлы или таблицу размещения файлов (FAT) на диске, "засоряют" оперативную память). Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру.

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273).

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.Первыми известными собственно вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и

BOMBSQAD авторства Анди Хопкинса (англ. Andy Hopkins). В начале 1985 года Ги Вонг (англ. Gee Wong) написал программу DPROTECT — первый резидентный антивирус.
Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения.
Обычным вирусом могут быть заражены следующие виды файлов:
Исполняемые файлы, т.е. файлы с расширениями имен .com и .exe, а также оверлейные файлы, загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются файловыми. Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые после своего запуска остаются в памяти резидентно — они могут заражать файлы и вредить до следующей перезагрузки компьютера. А если они заразят любую программу, запускаемую из файла AUTOEXEC.BAT или CONFIG.SYS, то и при перезагрузке с жесткого диска вирус снова начнет свою работу.
Загрузчик операционной системы и главная загрузочная запись жесткого диска. Вирусы, поражающие эти области, называются загрузочными или BOOT-вирусами. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения — заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска. например в конце корневого каталога диска или в кластере в области данных диска (обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных на диск).
Драйверы устройств, т.е. файлы, указываемые в предложении DEVICE файла CONFIG.SYS. Вирус, находящийся в них начинает свою работу при каждом обращении к соответствующему устройству. Вирусы, заражающие драйверы устройств, очень мало распространены, поскольку драйверы редко переписывают с одного компьютера на другой. То же относится и к системным файлам DOS (MSDOS.SYS и IO.SYS) — их заражение также теоретически возможно, но для распространения вируса малоэффективно.
Как правило, каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполняемые файлы. На втором месте по распространенности загрузочные вирусы. Некоторые вирусы заражают и файлы и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполняемые файлы.

Классификация

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Изначально вирусы распространялись на дискетах и других носителях, а сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.
Принято разделять вирусы:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, макровирусы, вирусы, поражающие исходный код);
- по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, скриптовый язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

По признаку вероломности:

- вирусы, моментально поражающие компьютер, форматируют жесткий диск, портят таблицу размещения файлов, портят загрузочные сектора, стирают так называемое Flash-ПЗУ (где находится BIOS) компьютера (вирус "Чернобыль"), другими словами, как можно быстрее наносят непоправимый урон компьютеру. Сюда же можно отнести и результаты обид программистов, пишущих вирусы, на антивирусные программы. Имеются в виду так называемые аллергии на определенные антивирусные программы. Эти вирусы достаточно

вероломны. Вот например, аллергия на Dr.Weber при вызове этой программы, не долго думая блокирует антивирус, портит все, что находится в директории с антивирусом и C:\WINDOWS. В результате приходится переустанавливать операционную систему и затем бороться с вирусом другими средствами.

- вирусы, рассчитанные на продолжительную жизнь в компьютере. Они постепенно и осторожно заражают программу за программой, не афишируя, свое присутствие и производят подмену стартовых областей программ на ссылки к месту где расположено тело вируса. Кроме этого они производят незаметное для пользователя изменение структуры диска, что даст о себе знать только когда некоторые данные уже будут безнадежно утеряны (вирус "OneHalf-3544","Yankey-2C").

Признаки заражения

Существует ряд признаков, которые могут сопутствовать заражению вирусом: появление на экране непредусмотренных сообщений и запросов, изображений и звуковых сигналов; самопроизвольный запуск программ без участия пользователя; попытки неизвестных программ подключиться к Интернету без ведома пользователя и т. п. О поражении вирусом через почту может свидетельствовать то, что друзья и знакомые пользователя говорят о сообщениях от него, которые он не отправлял; наличие в почтовом ящике большого количества сообщений без обратного адреса и заголовков.

Среди косвенных признаков можно назвать частые зависания и сбои в работе компьютера, замедленная (по сравнению с изначальным поведением) работа компьютера при запуске программ, невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого, частое обращение к жёсткому диску (часто мигает лампочка на системном блоке), браузер Internet Explorer «зависает» или ведёт себя неожиданным образом (например, окно программы невозможно закрыть). Но основной причиной для подобных симптомов являются всё же не вирусы, а сбои в аппаратном обеспечении, конфликты между программами и баги («жучки», дефекты) в них.

Механизм распространения

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.).

Каналы

Дискеты.

Флеш-накопители (флешки). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. В Windows 7 возможность автозапуска файлов с переносных носителей была отключена.

Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ.

Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта.

Интернет и локальные сети (черви). Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют уязвимости (ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный

код) в программном обеспечении операционных систем..

Способы маскировок и защит, применяемых вирусами

Вероломность — вирус моментально производит непоправимые действия/

Регенеративные вирусы делят свое тело на несколько частей и сохраняют их в разных местах жесткого диска. Соответственно эти части способны самостоятельно находить друг друга и собираться для регенерации тела вируса.

Есть вирусы, которые прячутся и от антивирусных программ. Эти "хамелеоны" изменяют сами себя с помощью самых хитрых и запутанных операций, применяя и текущие данные (время создания файла), и используя команды процессора.

"Невидимые" вирусы применяют так называемый метод, заключающийся в том, что вирус, находящийся в памяти резидентно, перехватывает обращения DOS (и тем самым прикладных программ) к зараженным файлам и областям диска и выдает их в исходном (незараженном) виде.

Также получили распространение вирусы, изменяющую файловую систему на диске. Эти вирусы обычно называются DIR. Такие вирусы прячут свое тело в некоторый участок диска (обычно в последний кластер диска) и помечают его в таблице размещения файлов (FAT) как конец файла. Для всех .com- и .exe- файлов, содержащихся в соответствующих элементах каталога, указатели на первый участок файла заменяются ссылкой на участок диска, содержащий вирус, а правильный указатель в закодированном виде прячется в неиспользуемой части элемента каталога.

Профилактика и лечение

В настоящий момент существует множество антивирусных программ, но нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учётными записями без крайней необходимости.
2. Не запускать незнакомые программы из сомнительных источников.
3. Стараться блокировать возможность несанкционированного изменения системных файлов.
4. Отключать потенциально опасный функционал системы (например autorun носителей в MS Windows, сокрытие файлов, их расширений и пр.).
5. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
6. Пользоваться только доверенными дистрибутивами.
7. Постоянно делать резервные копии важных данных и иметь образ системы со всеми настройками для быстрого развёртывания.
8. Выполнять регулярные обновления часто используемых программ, особенно, обеспечивающих безопасность системы.

Для защиты от вирусов можно использовать:

1) Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
2) профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
3) специализированные программы для защиты от вирусов.

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

a. копирование информации — создание копий файлов и системных областей дисков;
b. разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Специализированные программы для защиты от вирусов:

- Программы - детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
- Программы - доктора, или фаги, "лечат" зараженные программы или диски, восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
- Программы - ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении

несоответствий, об этом сообщается пользователю.

- Доктора - ревизоры — это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
- Программы - фильтры располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
- Программы - вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными.

Стратегия защиты от вирусов

Наилучшей стратегией защиты от вирусов является многоуровневая, "эшелонная" оборона.

Средствам разведки в "обороне" от вирусов соответствуют программы - детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов. Они смотрят, 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 режим лечения или уничтожения зараженных файлов. Программа - детектор может обнаруживать только те вирусы, которые ей известны (т.е. занесены в антивирусную базу данных этой программы), некоторые могут с помощью эвристического анализа находить модифицированные вирусы.

На переднем крае обороны находятся программы-фильтры (резидентные программы для защиты от вируса). Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Ревизоры обнаруживают нападение даже тогда, когда вирус сумел "просочиться" через передний край обороны. Программы-доктора применяются для восстановления зараженных программ, если ее копий нет в архиве. Но они не всегда лечат правильно. Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

Самый глубокий эшелон обороны — это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

И наконец, в "стратегическом резерве" находятся архивные копии информации и "эталонные" дискеты с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

Действия при заражении вирусом

Все действия по обнаружению вида заражения и лечению компьютера следует выполнять только после перезагрузки компьютера с защищенной от записи "эталонной" дискеты с операционной системой. При этом следует пользоваться исполняемыми файлами находящимися только на защищенных от записи "эталонных" дискетах. Несоблюдение этого правила может привести к очень тяжелым последствиям, поскольку при загрузке ОС или запуске программы с зараженного диска в компьютере может быть активирован вирус, а при работающем вирусе лечение компьютера будет бессмысленным, так как оно будет сопровождаться дальнейшим заражением дисков и программ.

Если вирус уже успел заразить или испортить какие-то файлы на дисках компьютера:

1. Перезагрузить ОС с заранее подготовленной эталонной дискеты. Эта дискета должна быть защищена от записи. Перезагрузку нельзя выполнять , используя комбинацию клавиш <Ctrl><Alt><Del>, так как некоторые вирусы способны анализировать это прерывание клавиатуры и продолжать работать. Они могут сымитировать перезагрузку компьютера, а могут ответить жестоким образом. Для перезагрузки нужно использовать кнопку "RESET" на системном блоке или вообще перезапустить питание.
2. Проверить правильность конфигурации компьютера при начальной загрузке компьютера.
3. Запустить программу - детектор для определения типа вируса и зараженных файлов.
4. Поочередно обезвредить все диски, которые могли подвергнуться заражению. Если жесткий диск разделен на несколько логических дисков, то при перезагрузке с дискеты будет виден

только логический диск, с которого стартует ОС. Необходимо прежде всего очистить от заражения его, а затем, перегрузившись с жесткого диска, заняться его остальными разделами.
5. Когда известно, что вирусов типа DIR на диске нет или они успешно вылечены можно проверить целостность файловой системы и поверхности диска программой NDD или ChkDsk. Если повреждения FAT (файловой системы) значительные, то целесообразно попробовать сделать копии необходимой информации, после чего отформатировать диск. При незначительных повреждениях можно попробовать восстановить диск, также применяя программу DiskEdit из комплекса Norton Utilities.
6. Если до заражения использовалась программа - ревизор, можно запустить ее для диагностики изменений в файлах. Можно проверить архивные копии на наличие вируса.
7. Удалить с диска все файлы, которые были изменены и имеют копии на других дисках. Нельзя оставлять на диске .exe и .com файлы, которые были изменены. Оставлять их можно только в исключительных случаях.
8. Если обрабатываемый диск системный, то его систему стоит обновить с "эталонной" дискеты командой SYS.
9. Файлы, которые доктор не смог восстановить, уничтожить.
10. С помощью архивных копий восстановить файлы, размещавшиеся на диске.
Если имеется хорошая программа - фильтр, целесообразно некоторое время поработать с ней.

<u>Профилактика против заражения вирусом</u>

- Обновлять архивные и эталонные копии используемых пакетов программ и данных. Перед архивацией данных целесообразно проверить их на наличие вируса.
- Скопировать на дискеты служебную информацию диска (FAT, загрузочные сектора) и CMOS (энергонезависимая память компьютера).
- Установить защиту от записи на архивных дискетах.
- Не заниматься нелицензионным и нелегальным копированием программного обеспечения с других компьютеров.
- Все данные, поступающие извне, проверять на вирусы, особенно файлы, "скачанные" из Интернета.
- Подготовить восстанавливающий пакет на дискетах с защитой от записи.
- На время обычной работы, не связанной с восстановлением компьютера, отключить загрузку с дискеты. Это предотвратит заражение загрузочным вирусом.
- Использовать программы - фильтры для раннего обнаружения вирусов.
- Проверять диск программами - детекторами или докторами - детекторами или ревизорами для обнаружения возможных провалов в обороне.
- Обновлять базу антивирусных программ.
- Не допускать к компьютеру сомнительных пользователей (разграничение доступа).

4 Исполнительский этап занятий

Задание к работе: Изучить предлагаемый теоретический материал. Исследовать методы защиты от компьютерных вирусов. Провести анализ современных антивирусных программ. Оформить отчет.

Содержание отчета

1. ФИО, № группы.
2. Тема лабораторной работы.
3. Задание.
4. Описание результатов исследования методов защиты от компьютерных вирусов и проведенного анализа современных антивирусных программ.
5. Выбрать любую антивирусную программу и продемонстрировать её работу (прикрепить скриншоты). Обязательно должно быть “обнаружение вируса”.

Учащийся получает отметку «зачтено», если выполнены все задания лабораторной работы, оформлен отчет, в соответствии с требованиями и защищен в устной форме по предложенному теоретическому материалу.

5 Постановка домашнего задания: в соответствии с КТП

Литература:

№№ п/п	Название	Авторы	Издание, год
1.	Методы и средства защиты компьютерной информации	А.А.Безбогов	Тамбов, 2006
		А.В.Яковлев,	
		В.Н.Шамкин	
2.	Информационная безопасность: учеб. пособие	С.И.Макаренко	Ставрополь, 2009
3.	Основы криптографии: учеб. пособие	А.П.Алферов и др.	Москва, 2002

6 Оценочно-рефлексивный этап занятия

Выставление отметок учащимся.

Учащимся необходимо ответить на поставленные вопросы:

1. Что нового Вы узнали на занятии?
2. Вы вызвало затруднение при выполнении задания?
3. Было ли вам интересно на занятии?