**Лабораторная работа № 7. Защита от компьютерных вирусов**

**Цель занятия:** закрепить сведения о классификации компьютерных вирусов, способах их распространения, способах борьбы с ними; закрепить сведения о классификации и назначении антивирусных программ.

**Порядок выполнения работы:**

1. Ответить на контрольные вопросы
2. Запишите результаты выполнения пункта 7.
3. Запишите информацию из пункта 8 выполнения работы.
4. Запишите информацию из пункта 10 выполнения задания: о чём может предупреждать программа пользователя.
5. Запишите информацию из пункта 11 выполнения задания.

Отчет переименовать следующим образом: **ЗКИ\_ЛР8\_Фамилия\_№группы** и сдать на проверку преподавателю

**Теоретическая часть**

Наиболее защищенный компьютер — это тот компьютер, который отключен от сети и заперт в сейф.

***Понятие вируса.***

Официальное появление *первого компьютерного вируса* датируется 1981 годом, задолго до выхода первой версии Microsoft Windows. Этот вирус, замаскированный под компьютерную игру, атаковал наиболее популярный компьютер того времени — Apple II. Распростра­нялся он с черепашьей скоростью (с помощью дискет).

Согласно подсчетам экспертов, объем *malware* (общепринятое название всех видов вредоносных программ) возрастает более чем на 15 % в год. Согласно данным компании Sophos, разработчика антивирусных программ, каждый день появляются примерно 30 новых вирусов, а перечень активных вирусов пополняется 10 тыс. новых наименований в год.

*Вирус* — это часть программного кода, которая тиражируется путем добавле­ния в другой объект, обычно незаметно и без разрешения пользователя.

Встреча компьютера с вирусом влечет несколько последствий.

• Появление необычных системных сообщений.

• Исчезновение файлов или увеличение их размеров.

• Замедление работы системы.

• Внезапный недостаток дискового пространства.

• Диск становится недоступным.

***Классификация вирусов.***

Вирусы могут быть безвредными, малоопасными и разрушительными.

Вирусы могут заражать программные файлы, документы (так называе­мые *макровирусы*) или файловые и дисковые структуры низкого уровня, такие как загрузочный сектор или таблица размещения файлов *(Boot – вирусы)*. *Файловые вирусы* заражают исполнимые файлы, имплантируя в них опасный код. Вирусы могут акти­визироваться при запуске инфицированной программы; также они могут по­стоянно находиться в памяти и заражать открываемые пользователем файлы или создавать свои собственные. Когда вирус проникает в компьютер, на кото­ром установлена система Windows, он может изменять значения в системном реестре, замещать собой системные файлы и внедряться в почтовую программу с целью дальнейшего размножения (черви). *Сетевые вирусы* обитают в оперативной памяти компьютеров и не копируют себя на носители данных. Они обитают в сети, когда хотя бы один компьютер включен, поэтому не опасны для индивидуального пользователя. Вирус не обязательно представля­ет собой отдельную программу и не всегда является деструктивным по своей сути, все зависит от его конкретной разновидности. Хотя основную угрозу для пользователей представляют именно компьютерные вирусы, существует несколь­ко видов вредоносных программ:

*Троянский конь* представляет собой компьютерную программу, которая маскируется или скрывается в части программы. Некоторые формы троянских коней могут быть запро­граммированы на саморазрушение и не оставляют никаких следов, кроме причинен­ных ими разрушений. Некоторые хакеры используют троянских коней для получения паролей и отсылки их обратно хакеру. Кроме того, они могут использоваться для банковских мошенничеств, когда небольшие суммы денег снимаются с законных счетов и передаются на секретный счет.

*Черви* представляют собой программы, которые разрушают компьютерную систему. Они могут проникать в программы обработки данных и подменять или разрушать данные. Как вирусы, они могут причинять большие разрушения, ес­ли их не обнаружить вовремя. Намного проще ликвидировать червя или троянского коня, если существует только единственная копия программы-разрушителя.

*Логические бомбы* подобны программам, используемым для троянских коней. Однако логические бомбы имеют таймер, который взрывает их в заданную дату и время. На­пример, вирус Michelangelo имеет триггер, установленный на день рождения знамени­того художника Микеланджело – б марта. Логические бомбы часто используются не­довольными служащими, которые могут установить их на активацию после того, как они оставят компанию. Например, логическая бомба может «взорваться», когда имя этого служащего исключается из платежной ведомости. Благодаря встроенному меха­низму задержки, логические бомбы активно используются для шантажа. Например, шантажист может послать сообщение, говорящее, что если ему будет выплачена опре­деленная сумма денег, он предоставит инструкцию для отключения логической бомбы.

*Смешанные коды* представляют собой новый класс изощренных вредоносных программ, которые сочетают в себе характеристики вирусов, червей и оеия, что позволяет злоумышленнику осуществить особо эффективную атаку. В от­личие от большинства доморощенных вирусов, которые распространяются бла­годаря взлому адресных книг на компьютерах под управлением Windows, це­лью таких программ являются web-серверы и сети, что значительно повышает их опасность.

***Пути проникновения вирусов в компьютер.***

Вирусы попадают в вашу компьютерную систему из множества разнообразных *источников* – исполняемых программ, программ и файлов, передаваемых вам, или программного обеспечения, приобретаемого в архивированной форме.

*Гибкие диски и компакт-диски* могут хранить файлы данных, программ и программное обеспечение oneрационных систем. Гибкий диск состоит из загрузочного сектора и данных. При необходимости, в загрузочном секторе может храниться информация, нужная для загрузки компьютера. Кроме того, здесь же хранится информация о разделах, информация по управлению загрузкой и информация о размещении файлов. Данные представляют собой всю ту содержательную информацию, которая храниться на гибком диске. Очень легко распространяются вирусы с флеш-карт.

Излюбленным местом обитания вирусов являются загрузочные сектора и исполняемые файлы, хранимые на гибком диске. Помещенные в загрузочном секторе, вирусы могут запускаться при загрузке системы с дискеты. Вирусы, помещенные в исполняемые файлы, запускаются вместе с зараженной программой, после чего начинают свою деятельность.

Если в *локальной сети* заражён хотя бы один компьютер, то вирус моментально распространится и на все остальные компьютеры.

*Интернет* предоставил пользователям новые возможности, которые увеличивают потенциальную опасность прорех в системе защиты от вирусов.

***Места обитания вирусов.***

Место обитания вируса связано с его функционированием самым непосредственным образом (как и у настоящих живых вирусов). Вирусные атаки можно даже классифицировать по месту их расположения в компьютере. Типы вирусныхатак: *атака загрузочного сектора; инфицирование файла; атака с использованием макросов.*

Вирусы загрузочного сектора инфицируют загрузочный сектор или главную загрузочную запись компьютерной системы. Когда компьютер загружается, вирусная программа активируется. Вирусы загрузочного сектора прежде всего перемещают в другое место записывают исходный загрузочный код и замещают его инфицированным загрузочным кодом. Информация исходного загрузочного сектора переносится на другой сектор диска, который помечается как дефектная область диска и далее не используется.

Поскольку загрузочный сектор – первый элемент, загружаемый при запуске компьютера, обнаружение вирусов загрузочного сектора может оказаться нелегкой задачей. Вирусы загрузочного сектора – один из самых популярных типов вирусов. Они могут распространяться путем использования инфицированных гибких дисков при загрузке компьютера. Это может легко произойти, если при перезагрузке компьютера гибкий диск вставлен в дисковод.

Вирусы, инфицирующие файлы, поражают *исполняемые файлы*. Они могут активироваться только при исполнении файла. Чаще прочих поражаются файлы типов СОМ, ЕХЕ, DLL, BIN, SYS и VXD. Вирусы, инфицирующие файлы, могут становиться резидентными и присоединяться к другим исполняемым программам. Вирусы, инфицирующие файлы, обычно заменяют инструкции загрузки программы исполняемого файла собственными инструкциями. Затем они переносят исходную инструкцию загрузки программы в другой раздел файла. Этот процесс увеличивает размер файла, что может помочь обнаружению вируса.

Вирусы в основе которых лежат макросы (*макровирусы),* исполняют непредусмотренные действия путем использования макроязыка приложения для своего распространения документы. Они могут, например, инфицировать файлы .DOT и .DOC приложения Microsoft Word, а также файлы Microsoft Excel. Эти вирусы относятся к межплатформенным вирусам и могут инфицировать как системы Macintosh, так и PC.

Прочие вирусы могут иметь черты одного или нескольких описанных выше типов.

*Вирусы-невидимки* (жаргонное название – «стелс-вирусы») при работе пытаются вся как от операционной системы, так и антивирусных программ. Чтобы перехватить все попытки использования операционной системы, вирус должен находиться в памяти. Вирусы невидимки могут скрывать все изменения, которые они вносят в размеры файлов, структуру каталогов или иные разделы операционной системы. Это значительно затрудняет их обнаружение. Чтобы блокировать вирусы-невидимки,их следует обнаружить, когда они находятся в памяти.

*Зашифрованные вирусы* во время работы шифруют свой вирусный код, что позволяет им предотвратить обнаружение и распознание вируса.

*Полиморфные вирусы* могут изменять свой внешний вид при каждом инфицировании. Для изменения внешнего вида и затруднения обнаружения они используют механизмы мутаций. Полиморфные вирусы способны принимать более двух миллиар­дов различных форм, поскольку при каждом инфицировании изменяют алгоритм шифрование.

*Многокомпонентные вирусы* инфицируют как загрузочные секторы, так и исполняе­мые файлы. Это один из самых сложных для обнаружения вирусов, поскольку мно­гокомпонентные вирусы могут сочетать некоторые или все методы скрытия своей деятельности, присущие вирусам-невидимкам и полиморфным вирусам.

*Самообновляющиеся вирусы,* которые появились в самое последнее время, способные скрытно обновляться через Интернет во время сеансов связи.

***Проблемы.***

*Новые вирусы.* Сигнатуры новых вирусов появляются постоянно. Когда разра­батывается новый вирус, разработчики антивирусных программ должны «ра­зобрать» его на составные части, проанализировать поведение, добавить его сиг­натуру в базу данных антивируса и опубликовать данное обновление. Даже если ваша антивирусная программа настроена на регулярное обновление, какой-то короткий период времени вы не защищены от новейших вирусов. Эта проблема может показаться не столь серьезной в момент начала распространения вируса.

Поскольку новые вирусы появляются непрерывно, никогда не стоит рассчиты­вать только на антивирусную программу. Для создания нескольких уровней защиты необходимо блокировать исполняемые почтовые вложения и устано­вить все необходимые обновления безопасности.

*Ложные тревоги.* Иногда антивирусный сканер может принять обычный файл за инфицированный, если база данных антивируса содержит некорректное опи­сание вирусной программы или если алгоритм эвристического анализатора ска­нера содержит ошибки.

***Действия антивирусных программ.***

Антиви­русная программа должна выполнять *три основные задачи*: обнаружение вируса, удаление вируса, превентивная защита.

Чтобы предотвратить вирусную атаку, антивирусная программа реализует *множество различных методов* обнаружения. Различные антивирусные программы используют не­которые или все методы из следующей группы.

*Сканирование цифровой сигнатуры* используется для идентификации уникального цифрового кода вируса. Цифровая сигнатура представляет собой предварительно установленный шестнадцатеричный код, наличие которого в файле свидетельствует о его заражении вирусом. Сканирование цифровой сигнатуры представляет собой в выс­шей степени успешный метод идентификации вирусов. Он, однако, всецело зависит от поддержки базы данных с цифровыми сигнатурами вирусов и тонкостей механизма сканирования. Возможно ложное обнаружение вируса в неповрежденном файле.

*Эвристический анализ* (или сканирование по заданным правилам) выполняется быст­рее, чем сканирование большинством традиционных методов. Этот метод использует набор правил для эффективного анализа файлов и быстро обнаруживает подозри­тельный вирусный код. Как отмечено в [9], все эвристические методы в той или иной форме выполняют эмулирование исполнения кода вируса. Поэтому, при наличии не­которого опыта, разработчик вируса может защитить свое «изделие» от обнаружения эвристическим анализом. Эвристический анализ склонен к ложным тревогам, и, к сожалению, зависит от корректности набора правил выявления вируса, которые все время изменяются.

*Исследование памяти —* еще один метод, обычно успешно применяемый для обнару­оеия вирусов. Он зависит от распознания местоположения известных вирусов и их кодов, когда они находятся в памяти. И хотя исследование памяти обычно приводит к успеху, использование такого метода может потребовать значительных ресурсов компьютера. Кроме того, он может вмешиваться в нормальный ход выполнения опе­раций компьютера.

*Мониторинг прерываний* работает путем локализации и предотвращения вирусных атак, использующих вызовы прерываний. Вызовы прерываний представляют собой запросы различных функций через системные прерывания. Мониторинг прерываний, подобно исследованию памяти, также может отвлечь значительные системные ресур­сы. Он может стать причиной проблем при легальных системных вызовах и замед­лить работу системы. Из-за большого числа вирусов и легальных системных вызовов, мониторинг прерываний может испытывать трудности в локализации вирусов.

*Контроль целостности* (известный также как *вычисление контрольных сумм)* про­сматривает характеристики файлов программ и определяет, были ли они модифици­рованы вирусным кодом. Этот метод не нуждается в обновлении программного обеспечения, поскольку не зависит от цифровых подписей вирусов. Однако он требу­ет от вас поддержания базы данных контрольных сумм файлов, свободных от виру­сов. Контроль целостности не способен обнаруживать пассивные и активные вирусы-невидимки. Кроме того, он не может идентифицировать обнаруженные вирусыпоименам или типам.

Непрерывной контроль может быть неподходя­щим средством для домашнего использования, поскольку может привести к обработке слиш­ком большого объема информации, а это замедляет работу компьютера. На клиентской машине предпочтительнее конфигурировать антивирусную программу на запуск в определенное время. Например, она может запускаться при загрузке компьюте­о или считывании нового файла с гибкого диска. В некоторых пакетах (например, Norton AntiVirus и MacAfee VimsScan) используют метод, известный как сканирование по расписанию, для выполнения поиска вирусов на жестком диске в заданные периоды времени. Еще один метод заключается в использовании антивирусной программы в период простоя компьютера. Например, его можно использовать как часть программы экранной заставки.

Основные принципы компьютерной безопасности.

1. Обучите всех, кто пользуется вашим компьютером или сетью, основным прин­ципам обеспечения компьютерной безопасности.
2. Установите антивирусную программу на компьютер. Установите на компьютер персональный брандмауэр.
3. Настройте почтовый клиент таким образом, чтобы он блокировал или поме­щал в отдельный каталог все потенциально опасные вложения.
4. Не пользуйтесь дисками, дискетами, флеш-картами, которыми Вы пользовались в заражённых ПК, не проверив их на наличие вирусов и не вылечив их.
5. Не поддавайтесь на сомнительные предложения в Интернете: просмотр интересного фильма или установка бесплатной программы и т.п.
6. Настройте свое антивирусное ПО таким образом, чтобы выполнялось регуляр­ное обновление, как минимум раз в неделю.
7. Используйте авторитетные источники информации о компьютерных вирусах и «ложных тревогах».
8. Пользуйтесь программами для резервного копирования данных. Разработайте план восстановления системы на случай вирусной атаки.

***ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ***

1. Посмотрите, какие антивирусные программы установлены на Вашем ПК*.*
2. Откройте программу ESET NOD32 Antivirus и изучите окно программы (Рис.6).
3. Почитайте информацию на вкладках: Состояние защиты, Обновление, Настройка, Служебные программы, Справка и поддержка.
4. Посмотрите на вкладке Настройка, все ли опции включены: Защита в режиме реального времени, Защита электронной почты, Защита доступа в Интернет.
5. Включите вкладку Сканирование ПК. Выберите выборочное сканирование. Просканируйте диск локальный D.
6. Пока идёт сканирование, изучите содержимое вкладки Сервис. Какие файлы были помещены на карантин?

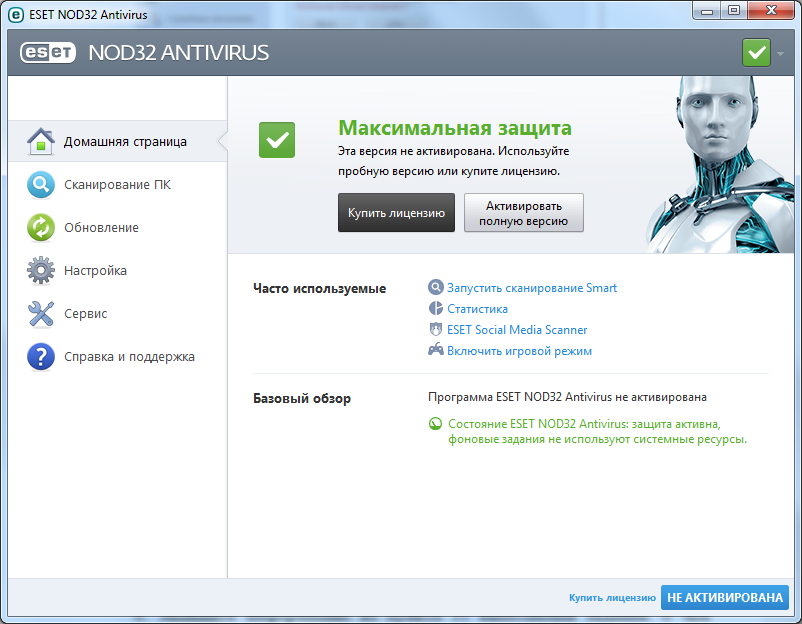


Рис.6

1. Результаты сканирования диска и дискеты запишите в отчёт.
2. В разделе Справочной системы программы найдите информацию о том, какие три уровня очистки поддерживает программа и запишите эту информацию в отчёт.
3. Изучите раздел справки Работа с ESET NOT32 Antivirus.
4. Изучите раздел справки Предупреждения и уведомления.
5. В служебных программах в Планировщике почитайте, какие задачи запланированы на ближайшее время и запишите эту информацию в отчёт.

Контрольные вопросы.

1. Что такое вирус?
2. Какие разновидности вирусов Вы знаете?
3. Как вирусы классифицируются по среде обитания?
4. Как вирусы классифицируются по степени вредного воздействия?
5. Какие виды вредоносных программ Вы знаете?
6. Как вирусы маскируются?
7. Когда обнаружили первый вирус?
8. Как Вы думаете, зачем изобретают вирусы?
9. Какие действия могут выполнять антивирусные программы?
10. Какие три задачи должна выполнять антивирусная программа?
11. Как обеспечить безопасность своей информации?