АПОО

«Техникум экономики и предпринимательства»

Информационные технологии в профессиональной деятельности

Модуль 4

г.Тамбов

Учебное пособие рекомендовано в качестве основного учебного материала студентам, получающим среднее специальное образование в заочной форме посредством ДОТ.

Информационные технологии в профессиональной деятельности. — Тамбов: типография ТЭП. — 24 с.
Идентификатор публикации: тер-e-it_v_рd-mod4-2013-01

Подготовлено научно—редакционным коллективом техникума экономики и предпринимательства:

Руководитель проекта	Никольская Н.Н.
Выпускающий редактор	Колмаков А.В.
Составитель учебного материала	Удалова Т.В.
Верстка	Колмаков А.В.

Вы можете оставить свои замечания по данному курсу на сайте http://elearning.ttep.su/feedback , или сообщить нашему ответственному сотруднику в г.Тамбове по тел. +7(4752)48-20-32

Модуль 4. Основы информационной и компьютерной безопасности.

УЭ 1. Информационная безопасность.

Здравствуйте, уважаемые студенты! Сегодня Вы продолжаете изучать дисциплину «Информационные технологии в профессиональной деятельности».

Целью изучения дисциплины является усвоение студентами теоретических знаний и приобретение умений использовать современные инновационные технологии в профессиональной деятельности.

В процессе изучения данного модуля рассмотрим следующие вопросы:

- Информационная безопасность;
- Защита от компьютерных вирусов;
- Организация безопасной работы с компьютерной техникой.

Если говорить о проблемах компьютерной безопасности, то просматриваются несколько аспектов, а именно: информационная безопасность, безопасность самого компьютера и организация безопасной работы человека с компьютерной техникой.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Важно уметь не только работать на компьютере, но и защитить ваши документы от чужих глаз.

Абсолютной защиты быть не может. Бытует такое мнение: установил защиту и можно ни о чем не беспокоиться. Полностью защищенный компьютер — это тот, который стоит под замком в бронированной комнате в сейфе, не подключен ни к какой сети (даже электрической) и выключен. Такой компьютер имеет абсолютную защиту, однако использовать его нельзя.

Первой угрозой безопасности информации можно считать некомпетентность пользователей. Если мы говорим об информации, хранящейся в компьютере на рабочем месте, то также серьезную угрозу представляют сотрудники, которые чем-либо не довольны, например зарплатой.

Одна из проблем подобного рода — это так называемые слабые пароли. Пользователи для лучшего запоминания выбирают легко угадываемые пароли. Причем проконтролировать сложность пароля невозможно. Другая проблема — пренебрежение требованиями безопасности. Например, опасно использовать непроверенное или пиратски изготовленное программное обеспечение. Обычно пользователь сам «приглашает» в систему вирусы и «троянских коней».

Чем шире развивается Интернет, тем больше возможностей для нарушения безопасности наших компьютеров, даже если мы и не храним в них сведения, содержащие государственную или коммерческую тайну. Нам угрожают хулиганствующие хакеры, рассылающие вирусы, чтобы просто позабавиться; бесконечные любители пожить за чужой счет; нам угрожают наша беспечность (ну что стоит раз в день запустить антивирус!) и беспринципность (как же отказаться от дешевого пиратского ПО, возможно, зараженного вирусами?).

За последнее время в Интернете резко увеличилось число вирусных, а также «шпионских» программ типа «троянского коня» и просто краж паролей нечистоплотными пользователями.

Безопасность в информационной среде

Любая технология на каком-то этапе своего развития приходит к тому, что соблюдение норм безопасности становится одним из важнейших требований. И лучшая защита от нападения — не допускать нападения. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

С точки зрения компьютерной безопасности каждое предприятие обладает своим собственным корпоративным богатством — информационным. Его нельзя спрятать, оно должно активно работать. Средства информационной безопасности должны обеспечивать содержание информации в состоянии, которое описывается тремя категориями требований: доступность, целостность и конфиденциальность. Основные составляющие информационной безопасности сформулированы в Европейских критериях, принятых ведущими странами Европы:

- доступность информации — обеспечение готовности системы к обслуживанию поступающих к ней запросов;
- целостность информации — обеспечение существования информации в неискаженном виде;
- конфиденциальность информации — обеспечение доступа к информации только авторизованному кругу субъектов.

Классификация средств защиты

Классификацию мер защиты можно представить в виде трех уровней.

Законодательный уровень. В Уголовном кодексе

РФ имеется глава 28. Преступления в сфере компьютерной информации. Она содержит три следующих статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Административный и процедурный уровни. На административном и процедурном уровнях формируются политика безопасности и комплекс процедур, определяющих действия персонала в штатных и критических ситуациях. Этот уровень зафиксирован в руководящих документах, выпущенных Гостехкомиссией РФ и ФАПСИ.

Программно- технический уровень. К этому уровню относятся программные и аппаратные средства, которые составляют технику информационной безопасности. К ним относятся и идентификация пользователей, и управление доступом, и криптография, и экранирование, и многое другое.

И если законодательный и административный уровни защиты не зависят от конкретного пользователя компьютерной техники, то программно-технический уровень защиты информации каждый пользователь может и должен организовать на своем компьютере.

Программно-технический уровень защиты

Не будем рассматривать существующие сложные программно-аппаратные криптографические комплексы, ограничивающие доступ к информации за счет шифров, а также программы тайнописи, которые могут «растворять» конфиденциальные материалы в объемных графических и звуковых файлах. Использование таких программ может быть оправдано лишь в исключительных случаях.

Обычный пользователь, такой как мы с вами, как правило, не является профессиональным шифровальщиком или программистом, поэтому нас интересуют «подручные» средства защиты информации. Рассмотрим средства защиты информации и попробуем оценить их надежность. Ведь знание слабых мест защиты может уберечь нас от многих неприятностей.

Первое, что обычно делает пользователь персонального компьютера — ставит два пароля: один пароль в настройках BIOS и другой — на заставку экрана. Защита на уровне BIOS будет требовать ввод пароля при загрузке компьютера, а зашита на заставке экрана перекроет доступ к информации при прошествии определенного, вами заданного, времени бездействия компьютера.

Установка пароля на уровне BIOS — достаточно тонкий процесс, требующий определенных навыков работы с настройками компьютера, поэтому желательно его устанавливать с коллегой, имеющим достаточный опыт такой деятельности. Пароль на заставку экрана поставить не так сложно, и его может поставить сам пользователь.

Для задания пароля на заставку необходимо выполнить следующие действия: нажмите кнопку *Пуск*, выберите команды *Настройка и Панель управления*, дважды щелкните по значку *Экран* и в открывшемся окне *Свойства экрана* выберите вкладку *Заставка*. Задайте вид заставки, установите временной интервал (предположим, 1 мин), установите флажок *Пароль* и нажмите на кнопку *Изменить*.

В открывшемся окне *Изменение пароля* введите пароль на заставку экрана, затем повторно его наберите для подтверждения и нажмите на кнопку *ОК*.

Если вы решили сами снять пароль на заставку, то проделайте все вышеизложенные процедуры, только в окне *Изменение пароля* не следует ничего набирать, а просто нажмите на кнопку *ОК*. Пароль будет снят.

После установки паролей можно считать, что первый уровень защиты вы сделали, и информационная защита обеспечена. Однако не обольщайтесь: существует как минимум три способа разрушить эту защиту.

Первый способ — воспользоваться одной из лазеек, часто предусмотренных производителями системной платы, так называемым «универсальным паролем для забывчивых людей». Обычный пользователь, каковыми мы и являемся, как правило, его не знает.

Можно использовать *второй способ* взлома секретности: снимите кожух компьютера, выньте примерно на 20...30 мин литиевую батарейку на системной плате, после чего вставьте ее обратно. После этой операции BIOS на 99 % забудет все пароли и пользовательские настройки. Кстати, если вы сами забыли пароль, что достаточно часто случается на практике, то можно воспользоваться именно этим способом.

Третий способ узнать постороннему лицу нашу защищенную информацию — вынуть из компьютера жесткий диск и подключить его к другому компьютеру в качестве второго устройства. А дальше без проблем можно читать и копировать чужие секреты. При определенном навыке эта процедура занимает 15...20 мин. Так что постарайтесь при вашем длительном отсутствии просто не допускать посторонних лиц в помещение, где находится компьютер.

Защита жесткого диска (винчестера)

Любую часть компьютерной системы можно заменить на новую, но утратив данные, записанные на жестком диске, вы будете вынуждены воссоздать их заново. На это могут уйти месяцы, а то и годы. Гораздо проще заранее организовать защиту содержимого жесткого диска.

Начинать следует с создания аварийной загрузочной дискеты. Она очень пригодится, если по какой-то причине не удастся загрузить операционную систему с жесткого диска. Владельцам Windows-систем придется создать дискету аварийной загрузки самостоятельно.

Создание аварийного загрузочного диска

Приготовив чистую дискету, выполните в среде Windows следующие действия:

- в меню *Пуск* выберите *Настройка/Панель управления;*
- выберите позицию *Установка и удаление программ;*
- щелкните по закладке *Системный диск* в Windows-95 или *Загрузочный диск* в Windows-98;
- щелкните на кнопке *Создать диск;*
- по требованию вставьте дискету в дисковод и щелкните по кнопке *О К;*
- по завершении процедуры выньте дискету из дисковода, наклейте на нее этикетку с маркировкой «Аварийная загрузочная дискета» и положите в безопасное место.

Резервное копирование данных

Другой враг нашей информации — сбои самого компьютера. Даже при самом строгом соблюдении мер профилактики нельзя быть абсолютно застрахованным от потери данных, хранящихся на жестком диске. Рано или поздно что-нибудь случается, и восстановить все в прежнем виде можно будет только в том случае, если у вас имеется копия содержимого жесткого диска.

Логика здесь очень простая: если одни и те же данные хранятся в двух разных местах, вероятность лишиться их значительно уменьшается. Поэтому всегда следует хранить данные в двух экземплярах: один на жестком диске, другой на сменных носителях, используемых для резервного копирования. Чтобы определиться со стратегией создания резервных копий, необходимо решить, каким носителем вы будете пользоваться и какие данные нужно продублировать. Информацию можно хранить на различных съемных носителях: дискетах, zip-дисках и дисках CD-ROM.

Чаще всего для хранения резервных копий используют дискеты, однако дискета — ненадежный носитель. К тому же, на одну дискету можно записать не очень много информации, но они дешевы и общедоступны. Вероятно поэтому — это самый распространенный на сегодняшний день носитель для резервного копирования. Устройства со сменным диском, например zip, более универсальны, поскольку их можно использовать как для резервного копирования, так и в качестве обычных накопителей. Они просты и удобны в использовании, однако из-за высокой цены они мало применяются.

Следует не забывать, что наша конфиденциальная информация интересна не только взломщику, но и нам самим, и потерять ее не хочется. В этом смысле самый надежный способ хранения — диски CD-ROM, поскольку дискеты и zip-диски имеют склонность выходить из строя в самый неподходящий момент.

Однако для записи информации на CD-диск в компьютере должно быть установлено специальное аппаратное и программное обеспечение — записывающий CD-ROM и программы типа DirectCD или InCD. Да и диск должен быть специального перезаписывающего типа — CD-RW. Записывающие CD-ROM сегодня стоят значительно дороже, чем обычные, но наблюдается тенденция к снижению цены.

При резервировании информации на записывающем CD-диске можно говорить о сравнительно надежном и одновременно безопасном хранении важной информации.

Коварство мусорной корзины

При удалении информации она не исчезает бесследно, а попадает сначала в *Корзину*, если только документ не находился на дискете. Это ежедневно спасает многих небрежных пользователей, случайно

удаливших документ неосторожным нажатием клавиши [Delete], поскольку документы из *Корзины* можно восстанавливать.

Для полного удаления информации из *Корзины*, т.е. ее очистки, сделайте щелчок правой кнопкой мыши по значку *Корзины* на рабочем столе и в открывшемся контекстном меню выберите команду *Очистить корзину* или выберите в окне *Корзина* команду очистки корзины.

Считается, что после принудительной очистки *Корзины* документы теряются безвозвратно, но это не совсем так. Физические данные с жесткого диска никуда не исчезают и могут быть легко восстановлены специальными программами вплоть до того момента, пока на то же место винчестера не будет записана другая информация. А ведь это может произойти через неделю или месяц. Чтобы быть точно уверенным, что ваши данные уничтожены навсегда, систематически проводите дефрагментацию жесткого диска. Программа дефрагментации Defrag входит в состав служебных программ *(Пуск/Программы/Стандартные/Служебные)* и перемещает данные на диске таким образом, чтобы файлы и свободное пространство размещались оптимально.

Эта процедура может занять от нескольких минут до получаса и более в зависимости от степени фрагментации диска. Желательно проводить дефрагментацию не реже одного раза в месяц, а при большом количестве операций по удалению файлов — еженедельно.

Установка паролей на документ

Известно, что любое приложение MS Office позволяет закрыть любой документ паролем, и многие успешно пользуются этим проверенным средством. Для установки пароля на текстовый документ необходимо его открыть, далее в меню *Сервис* выберите команду *Параметры*. В открывшемся окне на вкладке *Сохранение* наберите пароль для открытия файла вашего документа, сделайте подтверждение его повторным набором и нажмите на кнопку *ОК*.

В документации к MS Office ничего не говорится о криптостойкости используемых схем парольной защиты, есть только фраза: «Внимание! Забытый пароль восстановить невозможно». В версии MS Office-2000 на открытие файлов MS Word предусмотрена сравнительно надежная защита. Защита электронных таблиц MS Excel и пользовательской информации MS Outlook более слабая, чем у текстовых документов.

Обычному пользователю, не имеющему конкретной цели узнать вашу информацию, вскрыть пароль практически невозможно. Однако и специалисту-взломщику при использовании современного компьютера на взлом пароля методом прямого перебора вариантов понадобится примерно один месяц.

Парольная защита, входящая в комплект многих архиваторов, вполне может уберечь документ от посторонних глаз. В сети Интернет можно найти ряд специальных программ «шифрования» отдельных документов и целых разделов винчестера, однако стопроцентной гарантии от взлома паролей они не дают. Осложнить процесс взлома защиты вы можете, используя достаточно длинные и сложные пароли, исключающие ваше имя, фамилию и телефон. Лучше всего в качестве пароля выбирать фразу, в которой отсутствует осмысленная информация об авторе пароля. Скажем, фразу типа «Остались от козлика ножки да рожки» можно считать почти идеальным паролем — достаточно длинным и бессмысленным относительно автора.

Напоследок дадим несколько коротких практических советов по защите и резервному копированию ваших данных.

Полезные советы. Как защитить данные?

- Установите пароли на BIOS и на экранную заставку.
- Исключите доступ посторонних лиц к вашему компьютеру,
- Создайте аварийную загрузочную дискету.
- Систематически делайте резервное копирование данных.
- Регулярно очищайте *Корзину* с удаленными файлами.
- Устанавливайте пароли на файлы с важной информацией.
- При установке пароля не используйте ваше имя, фамилию, телефон.
- Проводите архивацию файлов.
- После удаления большого количества файлов, но не реже одного раза в месяц, производите дефрагментацию жесткого диска.

Говоря о безопасности информации, мы сознательно глубоко не затрагивали проблему компьютерных вирусов, и могло сложиться мнение, что такая проблема не актуальна. Ничего подобного! Борьба с

вирусами — это несомненно часть информационной безопасности, просто мимоходом говорить о такой важной проблеме неправильно. Борьба с вирусами — это тема отдельного разговора.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ:

1. Какие действия относятся к области информационных преступлений?
2. Зачем нужны законодательные акты в информационной сфере?
3. Какие действия уголовный кодекс классифицирует как преступления в компьютерной информационной среде?
4. Назовите меры защиты компьютерной информации.
5. Какие средства программно-аппаратного уровня защиты вы знаете?
6. Как устанавливать пароли на BIOS и экранную заставку?

Тест 1 (для самопроверки) :

1. Какой уровень безопасности документа Microsoft Office запрещает запускать макросы?
   1. средний
   2. низкий
2. Какой уровень безопасности документа Microsoft Office позволяет запускать модули VBA?
   1. средний
   2. низкий
   3. высокий
3. Какой способ защиты документов от компьютерных вирусов используется в пакете Microsoft office?
   1. парольный доступ для открытия документов с правом записи
   2. парольный доступ для открытия документов с правом чтения
   3. установка высокого уровня безопасности документа
4. Назовите уровни классификации мер защиты
   1. Законодательный уровень
   2. Административный и процедурный уровни.
   3. Программно- технический уровень
5. Какие виды ограничения доступа реализованы в Word?
   1. свободный доступ
   2. защита отдельных абзацев документа
   3. защита отдельных разделов документа
   4. парольный доступ для открытия документа с правом записи
   5. парольный доступ для открытия документа с правом чтения
6. Какие виды ограничения доступа реализованы в Excel?
   1. парольный доступ для открытия рабочей книги с правом записи
   2. парольный доступ для открытия листов рабочей книги с правом чтения
   3. парольный доступ для открытия листов рабочей книги документа с правом записи
   4. парольный доступ для открытия рабочей книги с правом чтения
   5. защита отдельных ячеек листов рабочей книги
   6. защита отдельных листов рабочей книги

УЭ 2. ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Вы глубоко ошибаетесь, если считаете, что лично вам вторжение вирусов не грозит. Компьютеры, установленные у вас на работе и дома, да и сама сеть Интернет являются настоящим рассадником потенциально опасных компьютерных инфекций.

Компьютерные вирусы — это программы, творящие на компьютере всевозможные безобразия, начиная с выдачи раздражающих экранных сообщений и кончая устройством полного хаоса на жестком диске.

Как правило, компьютер послушен своему хозяину, но если вы заметили какие-либо странности в его поведении, следует прежде всего проверить программное обеспечение на наличие вируса.

Некоторые компьютерные вирусы совершенно безвредны, однако многие из них способны нанести серьезный ущерб вашей информации.

История возникновения компьютерных вирусов

Возникновение компьютерных вирусов связано с идеей создания самовоспроизводящихся программ и уходит корнями в пятидесятые годы. В 1951 г. Дж. Нейман предложил метод создания самовоспроизводящихся механизмов. Затем идея вирусоподобных программ неоднократно возрождалась. И после опубликования в 1959 г. в одном из американских журналов материалов на эту тему, Ф. Шталь запрограммировал биокибернетическую модель существ, питающихся словами, размножающихся и пожирающих себе подобных.

Весной 1977 г. появился первый персональный компьютер фирмы Apple (Macintosh), а уже к середине 1983 г. общее количество проданных персональных компьютеров превысило 3 млн штук.

Тогда уже появились первые банки свободно распространяемых программ и данных — BBS, куда любой программист мог переслать свою программу, а любой пользователь сети мог ее взять и запустить на своем компьютере. Именно в тот момент возникли реальные возможности создания и быстрого распространения компьютерных вирусов. Тогда и получил развитие новый вид хулиганства — компьютерный, когда некая программа-вандал после выполнения какого-то условия или через некоторое время уничтожала данные на компьютере пользователя.

Мир помнит несколько случаев массового заражения компьютеров. Так, в 1987 г. было целых три таких эпидемии. Так называемый Пакистанский вирус только в США заразил более 18 тыс. компьютеров; Лехайский вирус в течение нескольких дней уничтожил содержимое нескольких сотен личных дискет и дискет библиотеки вычислительного центра одноименного университета США, заразив около 4 тыс. ПК, а в конце того же года в Иерусалимском университете был обнаружен вирус, который за короткое время распространился по всему цивилизованному миру, заразив только в США порядка 3 тыс. ПК. Крупный всплеск вирусной эпидемии был зарегистрирован в 1999 г. Вирус «Чернобыль», созданный тайваньским офицером, 26 апреля 1999 г., в годовщину чернобыльской аварии, вывел из строя огромное число компьютеров по всему миру.

Очередной пик вирусной атаки пришелся на 1 августа 2001 г., когда активизировался новый сетевой вирус-«червь» Code Red Worm. Атаке подверглись операционные системы Windows-2000, -NT. Только 19 июля 2001 г. этот вирус вывел из строя 230 тыс. серверов.

В настоящее время насчитывается уже порядка 20 тыс. различных вирусов и ежемесячно на волю вырываются до трехсот новых экземпляров. В России издана уникальная вирусная энциклопедия, содержащая описание 26 тыс. компьютерных вирусов и даже демонстрацию эффектов, производимых ими.

Что такое компьютерный вирус?

Точного научно-технического определения этого явления до сих пор не существует. Можно сказать, что компьютерный вирус — это программа, нарушающая нормальную работу других программ и компьютерной техники. Она обладает способностью самовоспроизведения, распространения, внедрения в другие программы.

Действия вируса зависят от фантазии, квалификации и нравственных принципов его создателя.

Характеры вирусов в какой-то мере отражают сущность их творцов — иногда это простые, шутливые и безобидные программы, но встречаются и чрезвычайно коварные, агрессивные и разрушительные экземпляры. Их названия говорят сами за себя: «Марихуана», «Террорист», «Киллер», «Захватчик».

Что же реально может вирус? Существует мнение, что человек может заразиться от техники компьютерными вирусами. Путаница происходит от использования одного и того же термина — вирус. Подчеркнем, что компьютерный вирус — это условное наименование специфических компьютерных программ, которые по своему механизму действия схожи с биологическими вирусами.

Компьютерные вирусы могут заразить только себе подобных, т.е. программы, поэтому программы надо защищать. Действие большинства вирусов не ограничивается только размножением или безобидными шутками. Вирусы могут разрушать изображение на экране, выводить на экран неприличные надписи, замедлять работу компьютера, исполнять различные мелодии, без разрешения удалять файлы и каталоги, уничтожая информацию. Как инфекция передается от человека к человеку, так и компьютерные вирусы переходят от одного компьютера к другому, изменяя имеющиеся файлы и дописывая в них свой код. При запуске зараженной программы или при открытии поврежденного файла данных вирус загружается в системную память компьютера, откуда пытается поразить другие программы и файлы.

Виды компьютерных вирусов

Чтобы успешно бороться с вирусами, надо их знать. Рассмотрим наиболее распространенные типы вирусов, с которыми вы в любой момент можете столкнуться.

Макровирусы. Эти вирусы распространяются зараженными файлами данных и учиняют разгром, используя механизм макросов программы-хозяина. Они распространяются значительно быстрее любых других компьютерных вирусов, так как поражаемые

ими файлы данных используются наиболее часто. Хакеры используют языки программирования таких популярных программ, как Word и Excel, чтобы искажать написание слов, изменять содержание документов и даже удалять файлы с жестких дисков.

Вирусы, поражающие загрузочный сектор и главную загрузочную запись. В качестве примера можно назвать вирусы «Микеланджело», «Килрой», «Джек-Потрошитель». Они передаются с компьютера на компьютер через зараженные дискеты. При обращении к дисководу, в который установлена такая дискета, операционная система считывает и выполняет вирусный код. Пожалуй, самый знаменитый вирус «Микеланджело», заставивший трепетать весь компьютерный мир, заслуживает того, чтобы ему было уделено некоторое внимание. Ежегодно 6 марта, в день рождения Микеланджело, вирус производил свою главную атаку, заменяя содержимое секторов жестких дисков случайными данными. Эффект ужасающий: восстановить информацию уже нельзя.

Файловые вирусы. Они внедряются в исполняемые файлы и делают свое черное дело, когда вы запускаете зараженную программу.

«Бомбы замедленного действия» и «троянские кони». Это особые разновидности вирусов, поражающих загрузочные секторы и файлы. До наступления определенной даты или определенного события они «дремлют» в компьютере, а затем активизируются и наносят удар.

Однако четкого разделения между ними не существует, и все они могут использовать комбинацию вариантов взаимодействия — своеобразный вирусный «коктейль».

Троянские программы действуют подобно «троянскому коню» из греческой мифологии. Они искусно маскируются под личиной какой-либо полезной программы, но стоит заинтересованному пользователю установить и запустить подобную программу на своем компьютере, как она незаметно начинает выполнять свою скрытую вражью функцию.

После того как «троянец» выполнит свою задачу, программа может самоуничтожаться, тем самым затрудняя обнаружение истинных причин «пожара» на вашем компьютере. Троянские программы часто используются для первоначального распространения вирусов.

Логической бомбой называют программу (или ее отдельные модули), которая при выполнении условий, определенных ее создателем, осуществляет несанкционированные действия, например при наступлении обусловленной даты или, скажем, появлении или исчезновении какой-либо записи в базе данных происходит разрушение программ или БД.

Известен случай, когда программист, разрабатывавший систему автоматизации бухгалтерского учета, заложил в нее логическую бомбу, и, когда из ведомости на получение зарплаты исчезла его фамилия, специальная программа-бомба уничтожила всю систему.

Полиморфные вирусы. Как подсказывает само название, каждый раз, когда такой вирус заражает систему, он меняет обличье, дабы избежать выявления антивирусными программами. Новые изощренные полиморфные вирусы значительно труднее обнаружить и куда сложнее нейтрализовать, поскольку при заражении каждого нового файла они изменяют свои характеристики.

Вирусы многостороннего действия. Хитроумные гибриды, одновременно с файлами поражающие загрузочные секторы или главную загрузочную запись.

Организация защиты от компьютерных вирусов

Компьютерные вирусы представляют реальную угрозу безопасности вашего компьютера, и, как водится, лучший способ лечения — это профилактика заболевания.

И если уж ваш компьютер подхватил вирус, вам не удастся с ним справиться без специальных средств — антивирусных программ.

Что должна делать антивирусная программа?

- Проверять системные области на загрузочном диске при включении компьютера.
- Проверять файлы на установленных в дисковод сменных носителях.
- Предоставлять возможность выбора графика периодичности проверки жесткого диска.
- Автоматически проверять загружаемые файлы.
- Проверять исполняемые файлы перед их запуском.
- Обеспечивать возможность обновления версии через Интернет.

В России антивирусными проблемами уже много лет профессионально занимаются в основном две серьезные фирмы: «Диалог Наука» (рис. 15.7) (программы Aidstest, Doctor WEB, ADinf, комплекс

Sheriff) и «Лаборатория Касперского» (Kami, программы серии AVP). Все новые вирусы в первую очередь попадают к ним.

Эти фирмы имеют большой авторитет и на международной арене. Продукция компании «Диалог Наука» хорошо знакома большому числу владельцев компьютеров. Первая версия антивирусной программы Doctor WEB с графическим интерфейсом появилась в апреле 1998 г., после чего пакет постоянно развивался и дополнялся. Сегодняшняя версия программы Doctor WEB имеет удобный, интуитивно понятный и наглядный графический интерфейс. Что касается возможностей по поиску вирусов, то их высокая оценка подтверждается победами в тестах авторитетного международного журнала «Virus Bulletin». Так, этот антивирусный пакет оказался единственным в мире, способным обнаруживать в памяти компьютера и обезвреживать вирус-невидимку нового поколения, прославившийся под именем Code Red Worm в августе 2001 г.

«Лаборатория Касперского» является крупнейшим российским разработчиком антивирусных систем безопасности: в 1999 г. 50% российских пользователей выбрали качество и надежность антивирусных программ этой фирмы. Разработка основного продукта «Лаборатории Касперского» — антивирусного комплекса «Антивирус Касперского» серии AVP (рис. 15.9) — началась в 1989 г.

«Лаборатория Касперского» — признанный лидер в антивирусных технологиях. Многие функциональные особенности практически всех современных антивирусов были впервые разработаны именно в этой компании. Исключительные надежность и качество антивирусных программ подтверждаются многочисленными наградами и сертификатами российских и зарубежных компьютерных изданий, независимых тестовых лабораторий.

Учитывая многообразие путей распространения вирусов, не стоит рассчитывать на то, что вы сможете обойтись без специальной антивирусной программы. Как правило, такую программу можно использовать периодически или запускать в фоновом режиме, чтобы отлавливать вирусы непосредственно при загрузке файлов или копировании со сменного носителя. Проверка в фоновом режиме — более надежный способ защиты (контроль ведется постоянно), требующий, однако, увеличенного объема памяти и повышенной производительности системы.

Можно установить на компьютере антивирусный монитор (сторож) — резидентную антивирусную программу, которая постоянно находится в оперативной памяти и контролирует операции обращения к файлам и секторам. Прежде чем разрешить доступ к объекту (программе, файлу), сторож проверяет его на наличие вируса. Таким образом, он позволяет обнаружить вирус до момента реального заражения системы.

Примерами таких программ являются McAfee VirusShield (антивирусный комплект McAfee VirusScan) и AVP Monitor (комплект AntiViral Toolkit Pro Касперского). Необходимо учитывать, что далеко не все программы-мониторы снабжены «лечащим» блоком, поэтому, чтобы обезвредить вирус, придется либо удалять зараженный файл, либо установить соответствующий «лечащий» блок (антивирусную программу).

Популярные антивирусные программы позволяют выбрать режим защиты от вирусов. Кроме того, фирмы-разработчики таких программ постоянно обновляют используемую для обнаружения вирусов базу данных и, как правило, размещают ее на Web-узле в открытом доступе для зарегистрированных пользователей. Если вы принадлежите к числу таковых, ежемесячно заглядывайте на узел, чтобы сделать свежую «прививку».

Проблемы вирусных атак волнуют и разработчиков программ приложений. Большое внимание при разработке новой версии Office-2000 было уделено безопасности работы с документами. Так, например, для предотвращения заражения документов вирусами для Office-2000 разработан новый программный интерфейс Microsoft Office Antivirus API, предоставляющий возможность антивирусным программам независимых разработчиков проверять документы Office непосредственно перед их загрузкой в приложение. Кроме того, в Office-2000 улучшена встроенная система защиты от макровирусов, имеющая теперь несколько уровней безопасности.

Советы по организации антивирусной защиты. Ниже приведенные советы помогут вам избежать неприятностей, связанных с вирусным заражением компьютера.

1. Если хотите избежать больших затрат и потерь, сразу предусмотрите приобретение и установку комплексной антивирусной программно-аппаратной защиты для вашей компьютерной системы.

Если таковая пока не установлена, не забывайте регулярно проверять свой компьютер свежими версиями антивирусных программ и установите программу-ревизор диска (например, ADinf), которая будет отслеживать все изменения, происходящие на вашем компьютере, и вовремя сигнализировать о вирусной опасности.

2. Не разрешайте посторонним работать на вашем компьютере, по крайней мере, без вашего разрешения.

3. Возьмите за строгое правило обязательно проверять все дискеты, которые вы используете на своем компьютере, несмотря на все уверения их владельца, последними версиями антивирусных программ (Doctor WEB, AVP и др.).

4. Если вы не собираетесь ничего записывать на дискеты в 3,5 дюйма, особенно при их использовании на «чужом» компьютере, непременно защитите их от записи, поставив защелку защиты от записи вниз (на себя) так, чтобы полностью открыть оконце. Этим вы закроете доступ на них вирусам с чужого компьютера. Все дистрибутивы программного обеспечения, записанные на дискетах, следует также защитить от записи.

5. Настоятельно советуем проверять на наличие вирусов все CD-ROM, в том числе и фирменные, но особенно купленные с рук или взятые со стороны.

6. Соблюдайте осторожность, обмениваясь файлами с другими пользователями. Этот совет особенно актуален, когда дело касается файлов, загружаемых вами из сети Интернет или приложенных к электронным посланиям. Поэтому лучше сразу проверять все входящие файлы (документы, программы) на наличие вируса, что неплохо умеют делать антивирусные мониторы, например AVP Monitor.

7. Делайте резервные копии своих данных. Это поможет восстановить информацию в случае воздействия вируса, сбоя в системе или выхода из строя жесткого диска.

8. Проверяйте на наличие вирусов старые файлы и диски. Обычные вирусы, равно как и макровирусы, пробуждаются только в тот момент, когда вы открываете или загружаете инфицированный файл. Таким образом, вирусы могут долгое время незаметно храниться на жестком диске в зараженных программах и файлах данных, приложениях к непрочитанным электронным письмам и сжатых файлах.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ:

1. Как защититься от вирусной атаки?
2. Перечислите известные вам антивирусные программы.
3. Что должна делать антивирусная программа?
4. Дайте определение компьютерному вирусу.
5. Какие типы вирусов вы знаете?

Тест 2 (для самопроверки):

1)Антивирусные программы типа «детектор» способны:

1. могут обнаруживать и "лечить" зараженные файлы, удаляя из файла тело вируса;
2. небольшие резидентные (постоянно находящиеся в оперативной памяти) программы, подающие сигнал тревоги, но лечить неспособны;
3. запоминают исходное состояние системных областей диска, каталогов и файлов и сразу после загрузки операционной системы производят сравнение;
4. производят поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса), поэтому могут находить только известные им вирусы.

2)Что такое компьютерный вирус?

1. Прикладная программа
2. Системная программа
3. Программа, выполняющая на компьютере несанкционированные действия
4. База данных.

3) Компьютерным вирусом является

1. Программа проверки и лечения дисков
2. Любая программа, созданная на языках низкого уровня
3. Программа, скопированная с плохо отформатированной дискеты
4. Специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью " размножаться "

4) Заражение компьютерными вирусами может произойти в процессе ...

1. Работы с файлами
2. Форматирования дискеты
3. Выключения компьютера
4. Печати на принтере

5)Самым опасным по отношению к файловой и операционной системе является следующий тип вируса:

1. Червь
2. Макровирус
3. троян

6) Что называется вирусной атакой?

1. Неоднократное копирование кода вируса в код программы
2. Отключение компьютера в результате попадания вируса
3. Нарушение работы программы, уничтожение данных, форматирование жесткого диска

7)На чем основано действие антивирусной программы?

1. На ожидании начала вирусной атаки
2. На сравнении программных кодов с известными вирусами
3. На удалении зараженных файлов

8)Какие программы относятся к антивирусным:

1. AVP, DrWeb, Norton AntiVirus
2. MS-DOS, MS Word, AVP
3. MS Word, MS Excel, Norton Commander

9)Антивирусные программы типа «сторож» способны:

1. могут обнаруживать и "лечить" зараженные файлы, удаляя из файла тело вируса;
2. небольшие резидентные (постоянно находящиеся в оперативной памяти) программы, подающие сигнал тревоги, но лечить неспособны;
3. запоминают исходное состояние системных областей диска, каталогов и файлов и сразу после загрузки операционной системы производят сравнение;
4. производят поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса), поэтому могут находить только известные им вирусы.

10)Антивирусные программы типа «доктор» способны:

1. могут обнаруживать и "лечить" зараженные файлы, удаляя из файла тело вируса
2. небольшие резидентные (постоянно находящиеся в оперативной памяти) программы, подающие сигнал тревоги, но лечить неспособны;
3. запоминают исходное состояние системных областей диска, каталогов и файлов и сразу после загрузки операционной системы производят сравнение;

11) Антивирусные программы типа «ревизор» способны:

1. могут обнаруживать и "лечить" зараженные файлы, удаляя из файла тело вируса;
2. небольшие резидентные (постоянно находящиеся в оперативной памяти) программы, подающие сигнал тревоги, но лечить неспособны;
3. запоминают исходное состояние системных областей диска, каталогов и файлов и сразу после загрузки операционной системы производят сравнение;
4. производят поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса), поэтому могут находить только известные им вирусы.

12) Антивирусные программы типа «детектор» способны:

1. могут обнаруживать и "лечить" зараженные файлы, удаляя из файла тело вируса;
2. небольшие резидентные (постоянно находящиеся в оперативной памяти) программы, подающие сигнал тревоги, но лечить неспособны;
3. запоминают исходное состояние системных областей диска, каталогов и файлов и сразу после загрузки операционной системы производят сравнение;
4. производят поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса), поэтому могут находить только известные им вирусы.

Практическая работа № 4.

Тема: Основы информационной и компьютерной безопасности.

Цель: защита от вирусов: обнаружение и лечение; овладеть практическими навыками выбора политики защиты и установки защиты.

Для выполнения практической работы необходимо:

1. Изучить теоретические вопросы модуля

Задания для выполнения практической работы

Задание 1. Установить с помощью программы BIOS Setup защиту загрузочного сектора системного диска от вирусов.

1. Включить компьютер. Наблюдать процесс тестирования компьютера. Для входа в BIOS Setup в процессе тестирования нажать клавишу Delete.
2. Установите курсор на пункте меню BIOS FEATURES SETUP, и нажать клавишу Enter.
3. На появившейся панели установить курсор на элемент конфигурационных данных Anti-Virus Protection и установить значение Enable.
4. Для предохранения данных от несанкционированного доступа можно с помощью BIOS Setup установить пароль для входа в систему. Обязательно хорошо запомните пароль, т.к. в случае его утери вход в систему становится невозможным (сброс пароля возможен только аппаратно, путем отключения микросхемы от источника питания).

- Открыть панель SUPERVISOR PASSWORD
- На появившейся панели Enter Password ввести пароль и нажать клавишу Enter. Повторно ввести пароль для подтверждения его правильности.

Задание 2. Обнаружение и лечение.

1. Запустить полиграф-сканер Kaspersky Anti-Virus Scanner. В появившемся окне активизировать значок **Объекты.** В левой панели выбрать диски и папки для проверки. В правой панели выбрать тип действия в случае обнаружения вируса и тип проверяемых объектов.
2. Щелчком по кнопке **Пуск** начать проверку. После окончания проверки щелкнуть по значку **Статистика.** В окне приложения появится информация о количестве проверенных секторов, папок и файлов, об обнаруженных вирусах и вылеченных файлах.

Задание 3. Защита сетевого приложения

А. Для разработанного фрагмента базы данных установите пароль, зашифруйте базу данных. Сделайте необходимые распечатки, демонстрирующие эффективность примененных способов защиты базы данных. Сформулируйте выводы относительности возможности использования этих способов при эксплуатации БД в архивах.

Чтобы выполнить операцию шифрования или дешифрования:

1. Запустите *Access*, не открывая базу данных.
2. Выберите команду **Сервис, Защита, Шифровать/дешифровать** (*Tools*, *Security*, *Encrypt/Decrypt Database*).
3. Появится диалоговое окно **База данных для шифрования или дешифрования** (*Encrypt/Decrypt Database*) (рисунок 1). Укажите имя базы данных, которую требуется зашифровать или дешифровать, и нажмите кнопку *OK*.
4. Если выбранная на предыдущем шаге база данных не является зашифрованной, появится диалоговое окно **Шифрование базы данных под именем** (*Encrypt Database As*), в другом случае появится диалоговое окно **Дешифрование базы данных под именем** (*Decrypt Database As*). Укажите имя, диск и папку для конечной базы данных и нажмите кнопку *OK*.

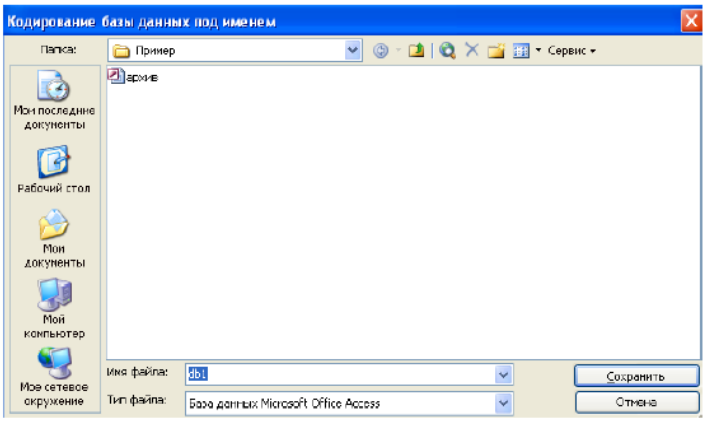

Рисунок 1

Чтобы установить пароль для защиты базы данных:

1. Закройте базу данных. Если база данных совместно используется в сети, убедитесь, что остальные пользователи ее закрыли.
2. Сделайте резервную копию базы данных и сохраните ее в надежном месте.
3. В меню Access выберите команду **Файл, Открыть**.
4. Выделите файл базы данных.
5. Щелкните по стрелке, расположенной справа от кнопки **Открыть**. В раскрывающемся списке режимов открытия базы данных выделите элемент **Монопольно**. База данных откроется в режиме монопольного доступа.
6. Выберите команду **Сервис, Защита, Задать пароль базы данных**. Появится диалоговое окно **Задание пароля базы данных.**
7. В поле **Пароль** введите пароль для защиты базы данных с учетом регистра символов.
8. Введите пароль еще раз в поле **Подтверждение**.
9. Нажмите кнопку ***ОК***.

Теперь база данных защищена паролем и всякий раз, когда пользователь будет открывать базу данных, будет отображаться диалоговое окно с требованием ввести пароль. Запомните или сохраните пароль в надежном месте. Если пароль будет забыт, невозможно будет открыть базу данных.

Б. Удалите пароль базы данных. Подтвердите соответствующей распечаткой проделанные действия.

Чтобы удалить пароль защиты базы данных:

1. Откройте базу данных в режиме монопольного доступа.
2. В диалоговое окно **Необходимо ввести пароль** введите пароль.
3. Выберите команду **Сервис, Защита, Удалить пароль базы данных**. Появится диалоговое окно **Удаление пароля базы данных**.
4. Введите текущий пароль базы данных.
5. Нажмите кнопку ***ОК***.

С. Установить защиту БД на уровне пользователей с помощью **Мастера защиты**. Для этого необходимо произвести следующие действия:

- выбрать команду **Сервис, Защита, Мастер;**
- на вопрос: «Создать файл рабочей группы или изменить текущий файл?» выбрать вариант «Создать файл рабочей группы»;
- в следующем окне **Мастера защиты** выбрать пункт «***Создать ярлык для защищенной базы данных***». В противном случае создаваемый файл рабочей группы будет использован по умолчанию для всех пользователей ***MS Access***;
- далее следует указать, что должны быть защищены ***все объекты*** базы данных. Этот вариант действий установлен по умолчанию. В случае снятия какого-либо флажка доступ к соответствующему объекту БД может получить любой пользователь системы;
- в следующем окне **Мастера защиты** необходимо указать сформированные ранее рабочие группы пользователей;
- запретить какие-либо разрешения для группы ***Users***. Все пользователи входят в эту группу, поэтому установка каких-либо разрешений приведет к наличию этих разрешений для всех категорий пользователей;
- далее следует добавить созданные ранее *функциональные* группы пользователей и назначить для них пароли;

• после этого необходимо указать, в какие рабочие группы входят *функциональные* группы пользователей;

• принять заданное по умолчанию имя резервной копии незащищенной БД;

• осуществить публикацию сформированного отчета **Мастера защиты** в *MS Word*.

Д. Распечатайте отчет о защите БД. Закройте БД и *Access*.

Е. Добавьте учетную запись нового пользователя. Включите его в одну из имеющихся групп пользователей. Задайте для него пароль. Подтвердите соответствующими распечатками проделанные действия.

Чтобы добавить учетную запись пользователя:

1. На вкладке **Пользователи** нажмите кнопку **Создать**.
2. Появится диалоговое окно **Новый пользователь или группа** (рисунок 2).
3. В поле **Имя** введите имя пользователя, а в поле **Код** - идентификатор пользователя. Нажмите кнопку *OK*.

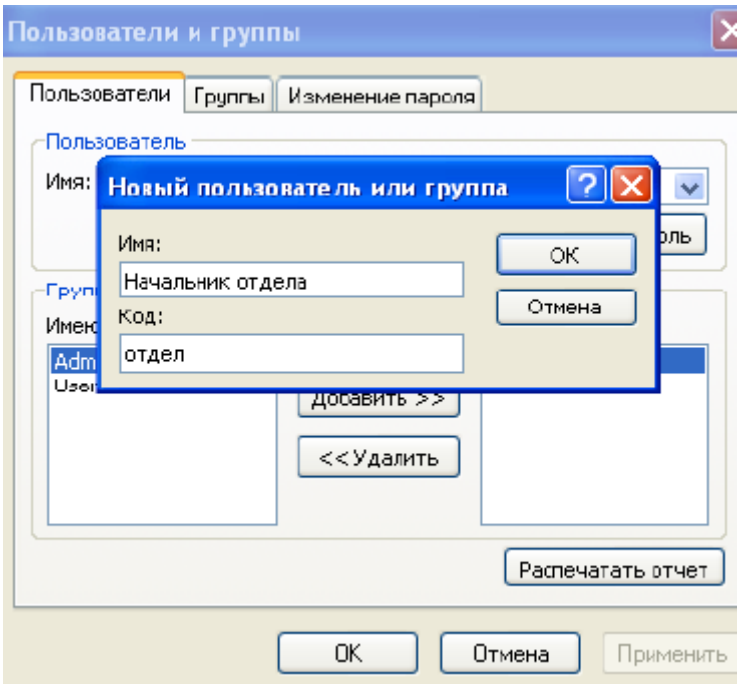

Рисунок 2

Чтобы добавить пользователя в группу:

1. На вкладке **Пользователи** в раскрывающемся списке **Имя** выберите имя пользователя, которого нужно добавить в некоторую группу. В списке **Участие в группе** отобразится список групп, в которые включена учетная запись пользователя.
2. В списке **Имеющиеся группы** отображаются все группы, имеющиеся в файле рабочей группы. Выделите в этом списке группу, в которую нужно добавить пользователя.
3. Нажмите кнопку **Добавить** (эта кнопка отмечена стрелками вправо). Выделенное имя группы появится в списке **Участие в группе**.

Чтобы задать или изменить пароль пользователя:

1. Откройте базу данных и зарегистрируйтесь с именем пользователя, пароль которого нужно изменить.
2. Выберите команду **Сервис, Защита, Пользователи и группы**. Появится диалоговое окно **Пользователи и группы**.
3. Раскройте вкладку **Изменение пароля**.
4. В поле **Пользователь** отображается имя пользователя, которое было использовано при регистрации. В поле **Текущий пароль** введите текущий пароль пользователя. Если пароль пользователя не был задан, оставьте это поле пустым.
5. В поля **Новый пароль** и **Подтверждение** введите новый пароль пользователя. Нажмите кнопку *OK*.

Чтобы получить отчет со списком пользователей и групп рабочей группы:

1. Откройте диалоговое окно **Пользователи и группы**.
2. На вкладке **Пользователи** нажмите кнопку **Распечатать отчет**.

И. Разграничьте права доступа нового пользователя и ранее созданного пользователя таким образом, чтобы ранее созданный пользователь, например, имел разрешение на чтение первых трех таблиц БД и запрет на чтение последующих таблиц, а новому пользователю, наоборот, запретить чтение первых трех таблиц БД и разрешить чтение последующих таблиц. Подтвердите соответствующими распечатками проделанные действия. Приведите пример практической ситуации, в которой могли бы потребоваться действия, рассмотренные в п.п.Е,И.

Чтобы открыть диалоговое окно для назначения прав доступа к объектам базы данных:

1. Откройте защищённую базу данных, подключив необходимый файл рабочей группы.
2. Зарегистрируйтесь с именем пользователя, обладающего административными правами.
3. Выберите команду **Сервис, Защита, Разрешения**. Появится диалоговое окно **Разрешения**.

Чтобы назначить права доступа к объектам базы данных конкретной группе:

1. На вкладке **Разрешения** выберите переключатель **Группы.**
2. В списке **Пользователи и группы** отобразится список всех групп в рабочей группе. Выделите в этом списке группу, права доступа которой нужно изменить.
3. Измените права доступа к объектам базы данных и нажмите **ОК**.

Чтобы назначить права доступа к объекту базы данных конкретному пользователю:

1. На вкладке **Разрешения** выберите переключатель **Пользователи**.
2. В списке **Пользователи и группы** отобразится список всех пользователей в рабочей группе. Выделите в этом списке пользователя, права доступа которого нужно изменить.
3. Измените права доступа к объектам базы данных и нажмите кнопку **ОК**.

Чтобы назначить выбранному пользователю или группе права доступа к объекту базы данных:

1. На вкладке **Разрешения** в раскрывающемся списке **Тип объекта** выберите тип объекта (**Таблица**, **Запрос**, **Форма**, **Отчет** или **Макрос**).
2. В списке **Имя объекта** выделите имя объекта, права доступа к которому нужно изменить.
3. Чтобы предоставить определенный вид доступа, установите соответствующий флажок в группе **Разрешения**. Чтобы запретить определенный вид доступа, сбросьте соответствующий флажок в этой группе.
4. Нажмите кнопку **Применить**, иначе при выборе другого пользователя или группы появится диалоговое окно, требующее подтверждения сделанных изменений. Чтобы подтвердить изменения, нажмите кнопку **Да**.

Чтобы назначить пользователю или группе права доступа к базе данных:

1. На вкладке **Разрешения** в раскрывающемся списке **Тип объекта** выберите элемент **База данных**.
2. В списке **Имя объекта** отобразится элемент **<Текущая база данных>** .
3. Установите необходимые разрешения и нажмите кнопку **Применить**.

Чтобы назначить права доступа к создаваемым объектам базы данных, предоставляемые пользователю или группе:

1. На вкладке **Разрешения** в раскрывающемся списке **Тип объекта** выберите тип объекта (например, **Форма**).
2. В списке **Имя объекта** выделите элемент, обозначающий новые объекты заданного типа, права доступа к которым требуется изменить (например, <**Новые формы**>).
3. Установите необходимые разрешения и нажмите кнопку **Применить**.

УЭ 3. ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ РАБОТЫ С КОМПЬЮТЕРНОЙ ТЕХНИКОЙ

Компьютерная техника является источником излучений и электромагнитных полей, а также местом накопления статического электричества, потенциально опасных для человека. Однако не следует забывать, что эти явления присутствуют и в быту, и в природе, а не только присущи исключительно компьютеру. А статическое электричество накапливает даже обычная расческа. И пока эти излучения и поля не превосходят установленный медициной предельно допустимый уровень (ПДУ), они не наносят ощутимого урона здоровью человека.

Из всех устройств, связанных с компьютером, для здоровья наибольшую потенциальную опасность представляет монитор.

Именно он сочетает относительно высокий уровень излучения и достаточно малое расстояние до человека.

Строго говоря, клавиатура, находящаяся в непосредственном контакте с пальцами

пользователя, тоже является источником излучения, но оно практически неотличимо от естественного фона и не идет ни в какое сравнение с излучением монитора.

Компьютер столь же безопасен, как и любой другой бытовой прибор. Но, как и в случае с другими бытовыми приборами, существуют потенциальные угрозы для здоровья, связанные с его применением.

Рассматривая влияние компьютеров на здоровье, отметим несколько факторов риска. Сюда относятся:

- проблемы, связанные с электромагнитным излучением;
- проблемы зрения;
- проблемы, связанные с мышцами и суставами.

В каждом из этих случаев степень риска прямо пропорциональна времени, проводимому за компьютером и вблизи него.

Начнем с наиболее спорного момента, связанного с вредным влиянием электромагнитного поля, создаваемого монитором компьютера.

Защита от электромагнитного излучения

Каждое устройство, которое производит или потребляет электроэнергию, создает электромагнитное излучение. Это излучение концентрируется вокруг устройства в виде электромагнитного поля.

Одни из них, такие как электрический чайник, создают вокруг себя небольшой уровень излучения. Другие устройства: высоковольтные линии, микроволновые печи, телевизоры, мониторы компьютеров — создают гораздо более высокие уровни излучения.

Электромагнитное излучение нельзя увидеть, услышать, понюхать, попробовать на вкус или потрогать, но, тем не менее, оно присутствует повсюду. Хотя вредное влияние обычных уровней электромагнитного излучения на здоровье никем пока не доказано, но многих эта проблема волнует.

Каждый, кто знаком с принципом действия монитора компьютера, называемого также видеотерминалом или дисплеем, согласится с тем, что нет смысла говорить о рентгеновском излучении, поскольку незначительное количество ионизирующего излучения, создаваемого катодно-лучевой трубкой внутри монитора, эффективно гасится стеклом трубки.

Что касается влияния на человеческий организм электромагнитного излучения более низких частот — излучения очень низкой частоты и сверхнизкой частоты, создаваемого компьютерами и другими бытовыми электроприборами, то здесь ученые и защитники прав потребителей пока не пришли к единому мнению.

Излучение монитора на базе электронно-лучевой трубки непосредственно в сторону пользователя резко падает пропорционально удаленности от экрана, а вот электромагнитное поле распространяется во все стороны. Причем непосредственно перед экраном оно несколько ослаблено теневой маской и арматурой кинескопа, а от боковых и задних стенок монитора оно распространяется беспрепятственно.

В настоящее время в России действуют согласованные с международными нормативами законодательные акты, гарантирующие потребителю соответствие прошедших сертификацию мониторов общепринятым нормам безопасности. Такими законодательными актами являются ГОСТ Р 50948—96 «Дисплеи. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности» и СанПиН 2.2.2.542—96 «Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы».

Принятые на сегодня санитарные нормы устанавливают минимальное расстояние от экрана до пользователя 50...70 см (примерно длина вытянутой руки), в то время как это расстояние от боковой и задней стенки до рабочих мест должно быть не менее 1,5 метров.

Для каждого оснащенного компьютером рабочего места определена минимальная площадь — не менее 6 м2. Клавиатура и руки пользователя должны находиться в максимально возможном удалении от компьютера.

У плоскопанельного жидкокристаллического монитора полно стью отсутствуют вредные излучения. Использование жидкокристаллических мониторов, практически не имеющих вредных излучений, в портативных компьютерах-ноутбуках создало распространенное мнение об их безвредности по сравнению со стационарными компьютерами.

Однако не следует забывать, что переменные электромагнитные поля, создаваемые импульсными преобразователями системы питания, у некоторых типов ноутбуков ничуть не меньше полей устаревших типов мониторов с ЭЛТ. Кроме того, вследствие размещения клавиатуры в едином блоке с процессором портативный компьютер находится

намного ближе к пользователю, чем стационарный, а уровень электромагнитного поля, как мы уже говорили, усиливается по мере приближения к компьютеру.

Полезные советы. Приведем несколько советов, содержащих сведения о том, как обезопасить себя, когда приходится иметь дело с компьютерами или электромагнитными полями.

1. Поскольку электромагнитное излучение исходит от всех частей монитора (многие измерения показали, что уровень излучения по бокам и сзади монитора выше, чем спереди), то наиболее безопасно установить компьютер в углу комнаты или в таком месте, где те, кто на нем не работают, не оказывались бы сбоку или
сзади от монитора.
2. Не оставляйте компьютер или монитор надолго включенными. Если компьютер не используется, выключите его. Это, может быть, не очень удобно (и может даже оказать некоторое влияние на срок службы компьютера), но все же это не слишком большая плата за защиту от потенциальной опасности электромагнитного поля.
3. Старайтесь сидеть по возможности дальше от экрана компьютера, но не в ущерб удобству. Согласно испытаниям, проведенным различными исследователями, пользователи, сидевшие по крайней мере в 70 см от экрана, получают минимальную дозу электромагнитного излучения. Рекомендуется при работе за компьютером помещать монитор на расстояние вытянутой руки (руки взрослого с вытянутыми пальцами).
4. Дети и беременные женщины должны проводить за компьютером не больше нескольких часов в день.

Компьютер и зрение

Природой наши глаза были предназначены для охоты и собирательства, т.е. для фокусировки на дальних расстояниях, а не для рассматривания близких предметов. Компьютер оказывает определенное отрицательное влияние на зрение человека. Мышцы, которые управляют глазами и фокусируют их на определенном предмете, просто устают от чрезмерной нагрузки.

Глазные мышцы расслаблены, когда мы смотрим вдаль. Рассматривая что-то вблизи, мы напрягаем глазные мышцы, поэтому после нескольких часов работы за монитором глаза устают.

Потенциальная усталость глаз существует при любой работе, в которой участвует зрение, но наиболее велика она, когда нужно рассматривать объект на близком расстоянии.

Проблема еще более возрастает, если такая деятельность связана с использованием устройств высокой яркости, например монитора компьютера. Наиболее часто утомляемость приводит к тому, что люди становятся вялыми и раздражительными.

Компьютерный зрительный синдром. Напряжение, которое испытывают глаза при работе за компьютером, зачастую приводит к развитию состояния, получившего название *компьютерного зрительного синдрома (КЗС)*. Оно характеризуется покраснением век, болью в глазах, глаза начинают слезиться или, наоборот, в них появляется ощущение сухости, рези, жжения. Эти ощущения повышают утомляемость. Появление КЗС связано не только со световым излучением, ведь глаза человека, смотрящего на монитор, выполняют не совсем привычную работу: они воспринимают изображение, принципиально отличающееся от природного. Прежде всего, монитор светится, в отличие, например, от книжной страницы, но, кроме того, он мерцает, четкость и цвета объекта на экране отличаются от естественных, а само изображение состоит из точек.

Чрезмерное увлечение работой за компьютером может также усугубить уже имеющиеся проблемы со зрением. Хотя еще и не доказано, что компьютеры действительно могут вызвать ухудшения зрения, некоторые офтальмологи высказывают опасения, что чрезмерное увлечение ими может оказать негативное влияние на мышцы, управляющие глазами, в результате чего потом будет очень трудно концентрировать зрение на определенном предмете, особенно в таких занятиях, как чтение. Если это произойдет, проблему коррекции зрения придется решать с помощью очков.

Полезные советы. К счастью, большинство этих проблем удается достаточно легко избежать. Вот некоторые способы.

1. Самое очевидное решение — это ограничить количество времени, проводимого за компьютером без перерыва. Рекомендуется делать короткий перерыв через каждые 15...30 мин занятий, или через каждый час работы. Идеальной «разрядкой» между компьютерными занятиями может быть физическая активность, не требующая напряжения зрения — прогулка, игра в мяч на воздухе или даже поход в магазин.

2. Некоторые специалисты предлагают упражнения для глаз, помогающие избежать ненужных проблем, связанных с использованием компьютера. Это могут быть такие простые упражнения, как, например, слежение за объектами, движущимися в поле зрения, или концентрация зрения на удаленных предметах. Чередование работы за компьютером с другими видами деятельности полезно еще и тем, что последние часто включают в себя зрительные движения, являющиеся хорошими упражнениями для глаз.

При первых признаках усталости сделайте одно или несколько простых упражнений на расслабление из приведенных ниже.

Упражнение 1. Плотно закройте глаза руками так, чтобы через них не проходил свет. Следите при этом за тем, чтобы посадка была удобной. Особое внимание — на спину и шею, они должны быть прямыми и расслабленными.

Закройте глаза и попытайтесь увидеть перед глазами абсолютно черный цвет. Удастся это не сразу, скорее всего постоянно будут возникать цветные полоски, ромбики и кляксы. Тут можно пойти на различные ухищрения, представляя себе, например, увеличивающуюся букву «О» с черной, как смоль, типографской краской. Чем чернее будет цвет, тем лучше вы расслабили глаза. Многие люди со слабой близорукостью могут добиться полного восстановления зрения сразу после выполнения этого упражнения.

Упражнение 2. Закройте глаза и сквозь веки посмотрите на солнце или яркую лампу. Поворачивайте глаза вправо-влево, делайте круговые движения. После окончания упражнения крепко сожмите веки на несколько секунд. Упражнение носит скорее не расслабляющий, а возбуждающий характер, поэтому рекомендуем
после него сделать упражнение 1.

Есть другой вариант этого упражнения. Отличается только тем, что при его выполнении необходимо быстро-быстро моргать глазами, а не закрывать их. При этом в поворотах вправо-влево могут участвовать не только глаза, но и голова.

3. Неплохо также разнообразить характер занятий за компьютером. Например, работу с текстовым процессором можно чередовать с игрой, в которой присутствуют движущиеся объекты. Такое чередование будет требовать от глаз совершенно разного поведения и воспрепятствует их утомляемости, вызванной длительной концентрацией зрения на одной и той же цели.

4. Есть еще один способ уменьшить риск перенапряжения глаз, он состоит в выборе хорошего монитора. Мониторы с высоким разрешением всегда удобнее для глаз, чем мониторы с низким разрешением. Если вы собираетесь сидеть у компьютера долго, то вам необходимо иметь дисплей с высокой четкостью.

5. Наконец, важно принять меры по уменьшению отражений от монитора. Яркое и неровное освещение в комнате может вызвать неприятные отражения на экране. Если вам доставляют беспокойство отражения от монитора или его собственная яркость, то перед ним можно установить специальный антибликовый экран.

Проблемы, связанные с мышцами и суставами

У людей, проводящих много времени за компьютером, наибольшее число жалоб на здоровье связано с заболеваниями мышц и суставов. Чаще всего это просто онемение шеи, боль в плечах и пояснице или покалывание в ногах. Но бывают более серьезные заболевания. Наиболее распространен кистевой туннельный синдром (capral tunnel syndrome), при котором нервы руки повреждаются вследствие частой и длительной работы на компьютере.

Имеет смысл последить за положением своего тела, если вы чересчур засиделись за компьютером. Обязательно проследите, чтобы стул, на котором вы сидите, не был слишком высоким или слишком низким. Заставляйте себя во время работы за компьютером не горбиться. Если вы выработаете привычку сидеть ровно и смотреть прямо на компьютер, то вероятнее всего вам удастся в будущем избежать проблем с мышцами и суставами.

Активные физические упражнения, гимнастика или просто движение являются профилактикой для суставов и мышц, поэтому старайтесь не реже одного раза в час встать из-за компьютера и сделать несколько физических упражнений или хотя бы просто пройтись по комнате.

Рациональная организация рабочего места

С понятием эргономики мы связываем рациональную организацию рабочего места. При «правильной» работе возрастет не только скорость, но и качество работы.

Чтобы работа была комфортной и эффективной, необходимо позаботиться о внешних условиях.

Основное — это освещение. Оно должно быть достаточно ярким (300...500 лк), но рассеянным. Стол надо располагать боком к окну, окно должно иметь жалюзи или плотные шторы (в случае попадания прямого солнечного света).

Если дома вы работаете по ночам, включайте верхний свет, соотношение яркостей экрана и окружающих предметов не должно быть больше 10: 1. Монитор располагайте так, чтобы исключить появление бликов от искусственного или естественного освещения.

Много говорят о необходимости поддержания невысокой температуры на рабочем месте. В настоящее время исследователи считают, что оптимальной является температура 22...24°С зимой и 23... 25 °С летом. Гораздо реже вспоминают о другом условии: разница температур на уровне пола и головы сидящего оператора не должна превышать трех градусов.

Ну, и наконец, влажность воздуха в помещении должна лежать в пределах 40...60 %. Остерегайтесь сквозняков. Их на рабочем месте не должно быть, как и разного рода вентиляторов. Кстати, сквозняком российские стандарты считают перемещение воздуха со скоростью более 0,1 м/сек.

Рабочий стол. Основной параметр, влияющий на удобство работы — высота стола. Наука говорит о том, что оптимальное значение этой цифры 72,5 см. Но лучше, конечно, покупать стол с регулируемой высотой. Тогда вы сможете более точно установить удобную для вас высоту. Но это еще не все. Под столом должно быть достаточно места для ног. Выбирая стол, обратите внимание, что под ним должны помещаться как вытянутые ноги (глубина не менее 65 см), так и закинутые одна на другую (высота пространства под столом не менее 60 см).

Стол должен иметь такие размеры, чтобы на нем можно было разместить монитор, клавиатуру и документы.

Кресло (стул). Казалось бы, требования к нему сформулировать предельно просто — оно должно быть удобным. Но это не все. Кресло должно позволять телу принимать физиологически рациональную рабочую позу, при которой не нарушается циркуляция крови и не происходит других вредных воздействий.

Физиологи нарисовали портрет «идеального» кресла, обеспечивающего комфортную продолжительную и безопасную работу.

Итак, кресло обязательно должно быть с подлокотниками и иметь возможность поворота, изменения высоты и угла наклона сиденья и спинки. Желательно иметь возможность регулировки высоты и расстояния между подлокотниками, расстояния от спинки до переднего края сиденья. Важно, чтобы все регулировки были независимыми, легко осуществимыми и имели надежную фиксацию.

Размер сиденья должен быть не менее 40 х 40 см. Угол его наклона варьируется от 15° вперед до 5° назад. Оптимальная высота сиденья от 40 до 55 см. Особые требования к спинке кресла: высота опорной поверхности 30±2 см, ширина не менее 38 см, радиус кривизны в горизонтальной плоскости 40 см, угол наклона от 0 до 30°, расстояние до переднего края сиденья от 26 до 40 см.

Подлокотники должны быть не менее 25 см в длину, 5...7 см в ширину, находиться над сиденьем на высоте 25 ±3 см и на расстоянии от 35 до 50 см друг от друга.

Клавиатура. Требования к эргономичности клавиатуры заключаются исключительно в том, что располагаться она должна на расстоянии 10...30 см от края стола или на специальной регулируемой по высоте подставке. В любом случае, если вы набираете много текстов, то стоит позаботиться о том, чтобы запястья не висели в воздухе.

Монитор. Требования к качеству монитора мы рассмотрим ниже, а сейчас поговорим о том, как его располагать на рабочем столе. Он должен стоять так, чтобы изображение было четко видно без необходимости поднимать или опускать голову. Монитор обязательно должен быть расположен ниже уровня глаз. При взгляде вверх быстро устает шея. Подставка монитора должна быть как можно ниже. Угол наблюдения должен составлять 0...600. Расстояние до монитора не менее 40 см.

Советы по организации безопасной работы с компьютерной техникой

Элементарный здравый смысл подсказывает: если есть реальная или потенциальная опасность, связанная с влиянием каких-либо факторов, необходимо постараться свести их к минимуму.

В нашем случае надо сделать так, чтобы компьютерное излучение и электромагнитные поля были максимально приближены к природным фоновым значениям.

Решение трех проблем поможет достижению этой цели.

1. Приобретение монитора с параметрами, максимально приближенными к естественному фону. «Классические» мониторы на базе электронно-лучевых трубок, безусловно, испускают электромагнитное излучение, что очевидно уже из названия этих приборов. Множество существующих стандартов безопасности часто ставят покупателя в тупик: ISO 9241, многочисленные варианты TCO и MPR — что все это может значить и чему доверять? Если говорить в общих чертах, то эти стандарты определяют максимально допустимые значения электромагнитных полей, создаваемых монитором при работе. В каждой экономически развитой стране действуют и собственные стандарты, но особую популярность завоевали те, что были разработаны в Швеции. Они известны под наименованиями TCO и MPR 2.

Рекомендации TCO касаются не только пределов различных излучений, но минимально приемлемых значений ряда параметров мониторов, например поддерживаемых разрешений, интенсивности свечения люминофора, запаса яркости, энергопотребления и т.п. MPR 2 определяет максимально допустимые величины излучения электромагнитных полей и методы их измерения.

Самым жестким и соответственно самым благоприятным для пользователя является стандарт TCO 99, спецификации которого включают в себя требования, взятые из стандартов TCO 95, ISO, 1EC и EN, а также из Шведского национального стандарта MPR 1990:8 (MPR 2). Впрочем, все современные модели мониторов, как правило, соответствуют и самым современным стандартам.

Для того чтобы свести к минимуму риск возникновения компьютерного зрительного синдрома, желательно работать на компьютере, удовлетворяющем следующим требованиям:

- количество цветов на цветном экране не менее 256;
- разрешение 800x600 точек при отсутствии мерцания;
- размер зерна не менее 0,28 мм, а лучше еще меньше;
- размер экрана как минимум 15 дюймов по диагонали;
- частота регенерации не менее 85 Гц (оптимальной считается установка максимально возможной частоты при отсутствии мерцания).

А если вы только собираетесь приобретать монитор, то проследите, чтобы на корпусе стоял значок одной из версий шведского стандарта.

На практике намного важнее, оказывается, правильно настроить купленный монитор и выставить на нем параметры, обеспечивающие наиболее комфортные для работы и безопасные для зрения условия. Что касается разных типов защитных экранов, то отметим следующее: дешевые «поделки» за 8...20 долл. разве что успокоят вам нервную систему и снимут электростатический заряд с монитора.

В некоторых случаях они могут быть даже вредны, внося оптическое искажение (блики) в воспринимаемую вами «картинку».

Качественные фильтры, реально защищающие пользователя от различных излучений монитора устаревшего типа, стоят порядка 80... 150 долл. (в зависимости от размеров экрана), так что намного целесообразнее использовать эти деньги для приобретения нового монитора, которому защитный экран не понадобится.

2. Правильная организация рабочего места. Мало приобрести компьютерную технику с хорошими показателями безопасности — ее нужно еще грамотно установить. Превышающие допустимый уровень излучения электромагнитные поля могут возникать даже у качественной сертифицированной техники, если она неправильно установлена. Поэтому при установке компьютерной техники необходимо следующее.

• Проследить за правильной расстановкой компьютеров в помещении, ведь наличие большого количества мониторов в ограниченном пространстве может привести к превышению допустимого уровня магнитных полей.

• Предохранять компьютер от попадания на него прямых солнечных лучей. Рабочее кресло должно находиться на безопасном расстоянии, да и от боковой и задней стенок монитора лучше держаться подальше.

• Обязательно применять сетевой фильтр, а если позволяют финансы — источник бесперебойного питания. Обеспечить надежное заземление компьютерной техники и источников питания.

• Правильно сориентировать монитор относительно источников света — лучше всего сидеть спиной к окну. Минимизировать блики на экране от расположенных рядом с монитором источников света, светлого оборудования, ярких поверхностей, не зашторенных окон.

• При использовании ноутбуков желательно подключать к ним обыкновенную клавиатуру и мышь для максимального удаления рук от процессорного блока.

• Поддерживать невысокий уровень запыленности помещения. При наличии кондиционера не забудьте его включать.

3. Обеспечение оптимального режима работы с компьютером.

Прежде всего необходимо обеспечить общие гигиенические нормы режима работы: ограничение времени работы на компьютере, необходимые перерывы, периодическая смена видов деятельности, зарядка для глаз и разминка для восстановления кровообращения.

Снимать утомление глаз необходимо даже во время работы: в течение нескольких секунд повращайте ими по часовой стрелке и обратно, чередуя это с легкими гимнастическими упражнениями для всего тела (например, подниманием и опусканием рук). После каждого часа работы делайте 5... 10-минутные паузы. При этом можно подойти к окну и на расстоянии 30 ...50 см от стекла проделать упражнения для тренировки аккомодации глаз: посмотреть в течение нескольких секунд на метку на стекле, а после перевести взгляд на дальний объект за окном. Затем упражнение следует повторить.

Не следует сидеть за монитором вообще без света, особенно по вечерам. Позаботьтесь, чтобы яркость освещения помещения несильно отличалась от яркости экрана.

Приобретите удобное для спины и ног рабочее кресло. Следите за тем, чтобы посадка была удобной. Особое внимание — на спину и шею, они должны быть прямыми и расслабленными.

Одежда, способствующая накоплению статики, — враг компьютера и источник болезненных ощущений человека.

Старайтесь долгое время не стоять рядом с задней частью работающего монитора. И не забывайте выключать монитор, когда он не нужен.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ:

1. Как предостеречь пользователя от влияния электромагнитного излучения?
2. Как уберечься от компьютерного зрительного синдрома?
3. Перечислите меры эргономической организации рабочего компьютерного места.
4. Назовите критерии оптимального режима работы с компьютером.

КОНЕЦ ЧЕТВЕРТОГО МОДУЛЯ

КЛЮЧИ К ТЕСТАМ

Модуль 4. Основы информационной и компьютерной безопасности.

Тест 1.

1	2	3	4	5	6
1	2	3	1, 2, 3	1, 4, 5	2

Тест 2.

1	2	3	4	5	6	7	8	9	10	11	12
4	3	4	1	3	1	2	1	2	1	3	4