

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ
УНИВЕРСИТЕТ»**

**Методические рекомендации для
самостоятельной работы обучающихся по дисциплине**

Б1.Б.07 Информатика

Направление подготовки 35.03.07 Технология производства и переработки
сельскохозяйственной продукции

Профиль подготовки Хранение и переработка сельскохозяйственной
продукции

Форма обучения очная

СОДЕРЖАНИЕ

1. Организация самостоятельной работы	3
2. Методические рекомендации по самостоятельному изучению вопросов	4

1. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1.1. Организационно-методические данные дисциплины

№ п.п.	Наименование темы	Общий объем часов по видам самостоятельной работы				
		подготовка курсового проекта (работы)	подготовка реферата/эссе	индивидуальные домашние задания (ИДЗ)	самостоятельное изучение вопросов (СИВ)	подготовка к занятиям (ПкЗ)
1	2	3	4	5	6	7
1	Текстовые редакторы и процессоры	-	-	-	4	-
2	Электронные таблицы	-	-	-	6	-
3	Системы управления базами данных (СУБД)	-	-	-	6	-
4	Программы создания презентаций	-	-	-	4	-
5	Информационная безопасность и её составляющие	-	-	-	4	-
6	Угрозы безопасности информации и их классификация. Организационные меры, инженерно-технические и иные методы защиты информации	-	-	-	4	-
7	Антивирусная защита	-	-	-	4	-

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1. Текстовые редакторы и процессоры.

Вопросы:

1. Современные текстовые процессоры.
2. Основные объекты текстового редактора и их свойства.
3. Операции над объектами текстового редактора.

При изучении вопроса необходимо обратить внимание на следующие особенности

Современные программы предусматривают множество функций, позволяющих готовить текстовую часть документа на типографическом уровне. Кроме того, современные программы позволяют включать в текст графические объекты: рисунки, диаграммы, фотографии. Благодаря этим возможностям файл, представляющий собой текстовый документ, может содержать, помимо алфавитно-цифровых символов, обширную двоичную информацию о форматировании текста, а также графические объекты.

При выборе текстового редактора для работы нужно учитывать многие факторы: и сложность документов, и масштаб (объемы) текстов, и требования к качеству документа на бумаге, и характер материалов (например, простая «беллетристика» или таблицы, формулы, уравнения и т.п.).

«Наиболее известные редакторы текстов можно условно разделить «по специализации» на три группы:

- процессоры общего назначения («Лексикон», Microsoft Word, и др.);
- редакторы научных документов (ChiWriter и др.);
- редакторы исходных текстов программ (Multi-Edit и встроенные редакторы систем программирования BASIC, Pascal и т.д.)»[

5.2 Электронные таблицы.

Вопросы: 1. Технология работы с электронными таблицами.

2.Адресация ячейки.

3. Построение диаграмм и графиков.

При изучении вопроса необходимо обратить внимание на следующие особенности

При изучении электронных таблиц целесообразно опираться на уже приобретенные учащимися знаниями по правилам записи числовых выражений (здесь следует обратить внимание на работу с функциями). Уместно так же использовать сформированное ранее понятие величины: клетки таблицы интерпретировать как простые переменные величины, рассматривая шифр клетки как имя величины, содержимое - как ее значение, а по значению определяя тип содержимого клетки.Электронные таблицы удобны в таких случаях:

- многократное выполнение однотипных вычислений;
- использование табличных данных;

- создание графиков (электронные таблицы – удобный способ представления данных в виде графика);
- анализ зависимости от параметра;
- представление результатов в читабельном виде.

5.3.Системы управления базами данных (СУБД)

Вопросы:

- 1.Классификация СУБД
- 2.Создание запросов
- 3.Создание форм и отчётов

При изучении вопроса необходимо обратить внимание на следующие особенности.

СУБД предполагает работу пользователя с базой данных в разных режимах: режим "ассистента" с использованием разветвленного меню - наиболее простой способ работы, не требующий специальной подготовки пользователя, кроме общих представлений о работе с базами данных; командный режим, предполагающий диалог пользователя и системы на языке команд СУБД, требует от пользователя знания этого языка; программный режим, использующий язык СУБД и позволяющий создать пользовательские программы различной степени сложности, удобно оформленные, выполняющие все функции, необходимые для решения задачи. Выбор СУБД определяется многими факторами, но главный из них - возможность работы с построенной моделью данных. Поэтому одной из важнейших характеристик является тип модели, который поддерживается СУБД. Имеются системы для работы с иерархическими и сетевыми моделями, однако большинство СУБД для персональных ЭВМ работают с реляционной моделью. Таковы системы dBase, FoxPro, Clipper, Paradox, R:base. Реляционные СУБД для персональных ЭВМ различаются набором реляционных операций, которые СУБД может выполнять. Перечисленные СУБД эффективны для создания небольших изолированных систем с несложной структурой данных, с небольшими объемами данных (10-40 Мбайт) и несложными запросами. За пределами такого рода ограничений эффективность использования указанных СУБД существенно снижается.

5.4 Программы создания презентаций.

Вопросы:

1. История компьютерных презентаций
2. Программы для презентаций от Microsoft.
3. Наложение на слайды переходов и создание анимации

При изучении вопроса необходимо обратить внимание на следующие особенности

Презентация (от английского слова – представление) – это набор цветных картинок-слайдов на определенную тему, который хранится в файле

специального формата с расширением РР. Термин «презентация» (иногда говорят «слайд-фильм») связывают, прежде всего, с информационными и рекламными функциями картинок, которые рассчитаны на определенную категорию зрителей (пользователей).

Мультимедийная компьютерная презентация – это:

- динамический синтез текста, изображения, звука;
- яркие и доходчивые образы;
- самые современные программные технологии интерфейса;
- интерактивный контакт докладчика с демонстрационным материалом;
- мобильность и компактность информационных носителей и оборудования;
- способность к обновлению, дополнению и адаптации информации;
- невысокая стоимость.

С точки зрения организации презентации можно разделить на три класса:

- интерактивные презентации;
- презентации со сценарием;
- непрерывно выполняющиеся презентации.

Интерактивная презентация - диалог между пользователем и компьютером. В этом случае презентацией управляет пользователь, т. е. он сам осуществляет поиск информации, определяет время ее восприятия, а также объем необходимого материала. В таком режиме работает ученик с обучающей программой, реализованной в форме мультимедийной презентации. При индивидуальной работе мультимедийный проектор не требуется.

Все интерактивные презентации имеют общее свойство: они управляются событиями. Это означает, что когда происходит некоторое событие (нажатие кнопки мыши или позиционирование указателя мыши на экранном объекте), в ответ выполняется соответствующее действие. Например, после щелчка мышью на фотографии картины начинается звуковой рассказ об истории ее создания.

Презентация со сценарием - показ слайдов под управлением ведущего (докладчика). Такие презентации могут содержать "плывущие" по экрану титры, анимированный текст, диаграммы, графики и другие иллюстрации. При этом, автор должен понимать, что объекты, особенно меняющие положение, должны быть обоснованы целью презентации. Сами по себе это объекты отвлекают внимание и могут мешать воспринимать информацию. Порядок смены слайдов, а также время демонстрации каждого слайда определяет докладчик. Он же произносит текст, комментирующий видеоряд презентации.

В непрерывно выполняющихся презентациях не предусмотрен диалог с пользователем и нет ведущего. Такие самовыполняющиеся презентации обычно демонстрируют на различных выставках.

Общие требования:

1. На слайдах должны быть только тезисы, ключевые фразы и графическая информация (рисунки, графики и т.п.) – они сопровождают подробное изложение мыслей докладчика, но не наоборот;
2. Количество слайдов должно быть не более 20;
3. При докладе рассчитывайте, что на один слайд должно уходить в среднем 1,5 минуты;
4. Не стоит заполнять слайд большим количеством информации. Наиболее важную информацию желательно помещать в центр слайда;
5. По желанию можно раздать слушателям бумажные копии презентации.

5.5 Информационная безопасность и её составляющие.

Вопросы:

1. Основные составляющие информационной безопасности
2. Основные определения и критерии классификации угроз

При изучении вопроса необходимо обратить внимание на следующие особенности.

Информационная безопасность направлена на обеспечение доступности, целостности конфиденциальности информационных ресурсов.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Наконец, конфиденциальность – это защита от несанкционированного доступа к информации.

Информационная безопасность — это состояние защищённости информационной среды, а защита информации представляет собой деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

В процессе эксплуатации информационных систем возникают ситуации, в результате которых информация, содержащаяся и обрабатываемая в ИС, может быть частично или полностью разрушена или потеряна. Это относится и к отдельным персональным компьютерам.

Под разрушением информационного массива понимают переход информационного массива в такое состояние, в котором в результате потери всей или части содержащейся в нем информации становится невозможным его дальнейшее использование.

Разрушение информации в информационной системе может быть вызвано различными факторами, которые по результату воздействия можно разделить на факторы, вызывающие полное или частичное разрушение физического носителя информации и факторы, вызывающие полное или частичное разрушение информационных массивов, но не воздействующие на физический носитель.

Среди факторов первой группы можно отметить следующие:

- несовершенство производства носителей информации, приводящее к появлению дефектов в виде повреждения магнитного слоя жестких дисков и дискет;

- естественный износ накопителей;
- ошибки обслуживающего персонала;
- неисправности дисководов и др.

К факторам второй группы относятся:

- ошибки в программах;
- аппаратные сбои при функционировании ЭВМ;
- ошибки операторов или пользователей ЭВМ;
- несанкционированный доступ к информации;
- разрушающее воздействие вирусов.

5.6 Угрозы безопасности информации и их классификация. Организационные меры, инженерно-технические и иные методы защиты информации

Вопросы:

1. Методы защиты информации
2. Понятие информационной безопасности
3. Важность и сложность проблемы информационной безопасности

При изучении вопроса необходимо обратить внимание на следующие особенности.

В ряде случаев стоимость обрабатываемой информации значительно превосходит стоимость оборудования, входящего в состав автоматизированной системы. В таких ситуациях ставится задача сохранения информации даже в условиях производственных катастроф и стихийных бедствий.

Для того чтобы сформулировать задачи защиты информации от злоумышленников, необходимо представить себе их цели и возможности по достижению этих целей.

Обычно различают следующие цели нарушителя:

- незаконное завладение конфиденциальной информацией;
- модификация информации;
- уничтожение информации;
- нарушение функционирования АС;
- незаконное копирование программ (и другой ценной информации);

- отказ от информации

Под конфиденциальной информацией понимается информация, доступ к которой ограничен в соответствии с законодательством. Факт попадания такой информации злоумышленнику называют утечкой информации и говорят о защите информации от утечки. Утечка информации может быть разной по последствиям. Так, например, утечка информации, связанная с хищением носителя или даже компьютера в целом, очень быстро обнаруживается. В то же время негласная для законного владельца утечка информации наносит больший вред.

Модификация информации всегда подразумевается неявной для законного владельца информации. Модификация информации может проявляться по-разному. Например, в финансовом документе она может заключаться в "исправлении" номера счета, куда надо переслать деньги, или размера суммы, подлежащей перечислению по указанному адресу. В сетях с коммутацией пакетов модификация может заключаться в изъятии из канала связи части сообщения, изменение порядка следования частей сообщения. Наконец,

возможен повтор или посылка фальсифицированного сообщения, например, с указанием банку перечислить деньги.

Уничтожение информации может привести к краху вычислительной системы, если не были приняты профилактические меры по резервному копированию информации, и к временному выходу системы из строя при наличии резервных копий.

Под нарушением функционирования автоматизированной системы подразумевают (в отличие от уничтожения информации) скрытные действия, мешающие нормально функционировать системе. Такие действия могут осуществляться захватом ресурсов, запуска на решение посторонних задач или повышением приоритетности задач, не требующих срочного решения. К указанным вмешательствам в работу наиболее чувствительны информационные системы, работающие в режиме реального времени или в режиме оперативного принятия решений.

Говоря о незаконном копировании программ, имеют в виду копирование не конфиденциальной информации, а информации, распространяемой на коммерческой или другой договорной основе. Незаконное копирование программ и другой ценной информации рассматривается как нарушение авторских прав разработчиков программного продукта и баз данных.

Отказ от информации характерен для следующих ситуаций взаимодействия двух удаленных абонентов в телекоммуникационной сети. Если абонент А посылает абоненту В сообщение, а позднее отказывается от факта отправки такого сообщения, то говорят об отказе от факта передачи сообщения. Если абонент В получив сообщение от абонента А, позднее отказывается от факта получения сообщения, то говорят об отказе от факта получения сообщения. Первый случай реален, например, если посланное сообщение содержало некоторые обязательства отправителя по отношению к

получателю, а второе – если полученное сообщение содержало некоторые поручения для получателя. Отказ от информации делает практически невозможным взаимодействие удаленных абонентов с использованием прогрессивных компьютерных и сетевых технологий.

5.7 Антивирусная защита

Вопросы

1. Виды антивирусных программ.
2. Организация антивирусной защиты

При изучении вопроса необходимо обратить внимание на следующие особенности.

В зависимости от проявления и дальнейшего поведения вирусы условно можно разделить на следующие группы: «черви», троянские кони, программы группы риска, непосредственно вирусы.

Вирусы классифицируются по следующим основным признакам:

1. среда обитания
2. способ заражения
3. степень воздействия
4. особенности алгоритма работы.

По среде обитания вирусы можно разделить на:

1. файловые
2. загрузочные
3. файлово-загрузочные
4. сетевые
5. макро-вирусы.

По способу заражения вирусы делятся на:

1. резидентные
2. нерезидентные .

По степени воздействия вирусы можно разделить на следующие виды:

1. неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках. Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;

2. опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

3. очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают

обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программами. Наиболее традиционным методом поиска вирусов является сканирование.

Признаками появления вируса являются:

- замедление работы компьютера;
- невозможные загрузки информационной системы;
- частые зависания и сбои в работе компьютера;
- увеличение количества файлов на диске и их размеров;
- изменение даты и времени создания файлов;
- периодическое появление на экране монитора неуместных сообщений и т.п.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.