



**ЧОУ ВПО «ИНСТИТУТ ЭКОНОМИКИ, УПРАВЛЕНИЯ И
ПРАВА (г. КАЗАНЬ)»**

Факультет менеджмента и инженерного бизнеса

«УТВЕРЖДАЮ»

Председатель приемной комиссии

Тимирязева А.В. Тимирязова

«15» *сентября* 2014 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ
для поступающих на базе профессионального образования
по направлению подготовки бакалавриата
10.03.01 «Информационная безопасность»

Форма обучения

Очная, заочная

Казань – 2014 г.

СОДЕРЖАНИЕ

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

II. СОДЕРЖАНИЕ ПРОГРАММЫ

II. ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ
ИСПЫТАНИЮ

III. КРИТЕРИИ ОЦЕНКИ СДАЧИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

IV. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ ДЛЯ
ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая программа предназначена для подготовки к вступительному испытанию для поступающих на направление подготовки 10.03.01 Информационная безопасность. Программа включает пояснительную записку, содержание программы вступительного экзамена, вопросы для подготовки к вступительному испытанию, перечень рекомендуемых нормативно-правовых актов и специальной литературы для подготовки к вступительному экзамену.

Программа сформирована на основе федерального государственного образовательного стандарта среднего общего образования, федерального государственного образовательного стандарта основного общего образования и соответствующих федеральных государственных образовательных стандартов среднего профессионального и (или) высшего образования.

1. Цель и задачи вступительного испытания

Целью вступительного испытания является определение у поступающих знаний в области информатизации, умения анализировать информационные системы и закономерности защиты информации в условиях распространения компьютерных систем.

Задачами вступительного испытания являются:

- проверка у абитуриента уровня знаний защиты информации;
- проверка у абитуриента наличия навыков профессиональной деятельности;
- определение склонности абитуриента к научно-исследовательской деятельности;
- определение сферы научных интересов абитуриента.

2. Порядок проведения и оценка вступительного экзамена

Вступительные испытания проводятся в форме собеседования. Вступительные испытания оцениваются в 100-бальной системы оценки.

Вступительное испытание считается сданным на оценку «неудовлетворительно», если абитуриент получил суммарно за ответы на все вопросы менее 40 баллов.

В ходе вступительного экзамена абитуриент должен показать, что он:

- знает основные понятия, категории и законы экономики, общие и специфические закономерности возникновения, функционирования и развития рыночной экономики;
- умеет анализировать и оценивать экономические явления и процессы;
- умеет корректно и убедительно отстаивать свою позицию;
- владеет специальной экономической терминологией;
- владеет навыками самостоятельной работы и активной познавательной деятельности.

II. СОДЕРЖАНИЕ ПРОГРАММЫ

1. Понятие ЭВМ. Классификация ЭВМ по различным признакам.

Классификация ЭВМ по быстродействию: суперЭВМ, большие ЭВМ, средние (малые) ЭВМ, персональные ЭВМ, встраиваемые микропроцессоры. Классификация ЭВМ по месту и роли в компьютерной сети: кластерные структуры (многомашинные вычислительные системы), серверы, рабочие станции, сетевые компьютеры.

Электронная вычислительная машина – это комплекс технических и программных средств, предназначенный для автоматизации подготовки и решения задач пользователей.

Классификация средств вычислительной техники, в основу которой положено их разделение по быстродействию:

1. СуперЭВМ для решения крупномасштабных вычислительных задач, для обслуживания крупнейших информационных банков данных.

2. Большие ЭВМ (mainframe) для комплектования ведомственных, территориальных и региональных вычислительных центров. Представляют собой многопользовательские машины с центральной обработкой, с большими возможностями для работы с базами данных, с различными формами удаленного доступа.

3. Средние ЭВМ широкого назначения для управления сложными технологическими производственными процессами.

4. Персональные и профессиональные ЭВМ, позволяющие удовлетворять индивидуальные потребности пользователей.

5. Встраиваемые микропроцессоры, осуществляющие автоматизацию управления отдельными устройствами и механизмами.

С развитием сетевых технологий все больше начинает использоваться другой классификационный признак, отражающий место и роль ЭВМ в сети:

1. Мощные машины и вычислительные системы для управления гигантскими сетевыми хранилищами информации. Предназначаются для обслуживания крупных сетевых банков данных и банков знаний.

2. Кластерные структуры - многомашинные распределенные вычислительные системы, объединяющие несколько серверов.

3. Серверы - вычислительные машины и системы, управляющие определенным видом ресурсов сети.

4. Рабочие станции: ориентированны на работу профессиональных пользователей с сетевыми ресурсами.

5. Сетевые компьютеры - упрощенные персональные компьютеры, вплоть до карманных ПК. Их основным назначением является обеспечение доступа к сетевым информационным ресурсам.

2. Общие принципы построения современных ЭВМ. Классическая структура ЭВМ Дж. фон Неймана.

Основным принципом построения всех современных ЭВМ является программное управление. В основе его лежит представление алгоритма решения любой задачи в виде программы вычислений.

Алгоритм - конечный набор предписаний, определяющий решение задачи посредством конечного количества операций. **Программа** (для ЭВМ) - упорядоченная последовательность команд, подлежащая обработке. Принцип программного управления может быть осуществлен различными способами. Стандартом для построения практически всех ЭВМ стал способ, описанный Дж. фон Нейманом в 1945 г. при построении еще первых образцов ЭВМ.

Сущность фон-неймановской концепции вычислительной машины можно свести к четырем принципам: (1) двоичного кодирования; (2) программного управления; (3) • однородности памяти; (4) адресуемости памяти.

Согласно **принципу двоичного кодирования**, вся информация, как данные, так и команды, кодируются двоичными цифрами 0 и 1. Каждый тип информации представляется в двоичном виде и имеет свой формат.

Согласно **принципу программного управления**, все вычисления, предусмотренные алгоритмом решения задачи, должны быть представлены в виде программы, состоящей из последовательности управляющих слов - команд. Каждая команда предписывает некоторую операцию из набора операций, реализуемых вычислительной машиной.

Согласно **принципу однородности памяти**, команды и данные хранятся в одной и той же памяти и внешне в памяти неразличимы. Распознать их можно только по способу использования. Это позволяет производить над командами те же операции, что и над числами.

Согласно **принципу адресуемости памяти**, структурно основная память состоит из пронумерованных ячеек, причем процессору в произвольный момент доступна любая ячейка. Двоичные команд и данных разделяются на единицы информации, называемые словами, и хранятся в ячейках памяти, а для доступа к ним используются номера соответствующих ячеек — адреса.

Типичная фон-неймановская ЭВМ содержит следующие основные устройства, с помощью которых должны быть реализованы вышеперечисленные принципы: память, устройство управления, арифметико-логическое устройство и устройства ввода/вывода.

3. Функциональная и структурная организация современных ЭВМ. Центральные и периферийные устройства. Состав и характеристика центральных устройств: процессор, основная память, системная магистраль. Состав и

характеристика периферийных устройств: внешние запоминающие устройства, устройства ввода-вывода.

Структурная схема персонального компьютера с минимальным составом внешних устройств включает:

1. **Микропроцессор (МП)** — центральное устройство ПК, предназначенное для управления работой всех блоков машины и для выполнения арифметических и логических операций над информацией.

В состав микропроцессора входят: (1) устройство управления (УУ), (2) арифметико-логическое устройство, (3) микропроцессорная память, (4) интерфейсная система, (5) генератор тактовых импульсов.

2. **Системная шина** — основная интерфейсная система компьютера, обеспечивающая сопряжение и связь всех его устройств между собой. Системная шина включает в себя: кодовую шину данных, кодовую шину адреса, кодовую шину инструкций, шину питания.

Все блоки (их порты ввода-вывода), через соответствующие унифицированные разъемы подключаются к шине единообразно: непосредственно или через контроллеры (адаптеры). Управление системной шиной осуществляется микропроцессором либо непосредственно, либо, что чаще, через дополнительную микросхему контроллера шины, формирующую основные сигналы управления.

3. **Основная память (ОП)** предназначена для хранения и оперативного обмена информацией с прочими блоками машины. ОП содержит два вида запоминающих устройств: постоянное запоминающее устройство (ПЗУ) и оперативное запоминающее устройство (ОЗУ).

4. **Внешняя память** относится к внешним устройствам ПК и используется для долговременного хранения любой информации, которая может когда-либо потребоваться для решения задач.

5. **Источник питания** — блок, содержащий системы автономного и сетевого энергопитания ПК.

6. **Таймер** — внутримашинные электронные часы реального времени.

7. **Внешние устройства.**

К внешним устройствам относятся:

- внешние запоминающие устройства (ВЗУ) или внешняя память ПК;
- диалоговые средства пользователя (видеомонитор, устройства речевого ввода-вывода, средства мультимедиа);
- устройства ввода информации (клавиатура, графические планшеты, устройства целеуказания, сканеры, сенсорные экраны);
- устройства вывода информации (принтеры, графопостроители);
- средства связи и телекоммуникаций (сетевые интерфейсные платы, модемы).

4. Вычислительные сети. Классификация вычислительных сетей по различным признакам: по принципу территориальной рассредоточенности, по способу управления, по принципу передачи информации, по топологии.

Телекоммуникационная вычислительная сеть (ТВС) - это сеть обмена и распределенной обработки информации, образуемая множеством взаимосвязанных абонентских систем (АС) и средствами связи; средства передачи и обработки информации ориентированы в ней на коллективное использование общесетевых ресурсов - аппаратных, информационных, программных.

По степени территориальной рассредоточенности элементов сети (абонентских систем, узлов связи) различают:

- локальные (ЛВС, LAN — Local Area Network);
- региональные (РВС, MAN — Metropolitan Area Network);
- глобальные (ГВС, WAN—Wide Area Network).

В **локальной сети** абоненты находятся на небольшом (до 10-15 км) расстоянии друг от друга. К ЛВС относятся сети отдельных предприятий, фирм, банков, офисов, корпораций и т. д. **РВС** связывают абонентов города, района, области. Обычно расстояния между абонентами РВС составляют десятки-сотни километров. **Глобальные сети** соединяют абонентов, удаленных друг от друга на значительное расстояние, часто расположенных в различных странах или на разных континентах.

По способу управления ТВС делятся на сети с централизованным (в сети имеется один или несколько управляющих органов), децентрализованным (каждая АС имеет средства для управления сетью) и смешанным управлением, в которых в определенном сочетании реализованы принципы централизованного и децентрализованного управления.

По организации передачи информации сети делятся на сети с селекцией информации и маршрутизацией информации. В сетях с селекцией информации, строящихся на основе моноканала, взаимодействие АС производится выбором адресованных им блоков данных: всем АС сети доступны все передаваемые в сети кадры, но копию кадра снимают только АС, которым они предназначены. В сетях с маршрутизацией информации для передачи кадров от отправителя к получателю может использоваться несколько маршрутов.

По типу организации передачи данных сети с маршрутизацией информации делятся на сети с коммутацией каналов и коммутацией пакетов.

По топологии, т.е. конфигурации элементов в ТВС, сети делятся на два класса: широковещательные и последовательные. Широковещательные конфигурации и значительная часть последовательных конфигураций (кольцо, звезда с интеллектуальным центром, иерархическая) характерны для ЛВС. Для глобальных и региональных сетей наиболее распространенной является произвольная (ячеистая топология).

5. Техническое, информационное и программное обеспечение сетей. Рабочая станция, сервер, хост-компьютер. Концентраторы. Коммутаторы. Маршрутизаторы. Сетевые карты.

Техническое (аппаратное) обеспечение составляют:

- компьютеры (хост-компьютеры, сетевые компьютеры, рабочие станции, серверы), размещенные в узлах сети;
- аппаратура и каналы передачи данных, с сопутствующими им периферийными устройствами;
- интерфейсные платы и устройства (сетевые платы, модемы);
- маршрутизаторы и коммутационные устройства.

Рабочая станция — подключенный к сети компьютер, через который пользователь получает доступ к ее ресурсам.

Сервер (server) — это выделенный для обработки запросов от всех рабочих станций сети многопользовательский компьютер, предоставляющий этим станциям доступ к общим системным ресурсам (вычислительным мощностям, базам данных, библиотекам программ, принтерам, факсам и т. д.) и распределяющий эти ресурсы.

Компьютеры, имеющие непосредственный доступ в глобальную сеть, часто называют **хост-компьютерами**.

Узлы коммутации вычислительных сетей содержат устройства коммутации (**коммутаторы**). Если они выполняют коммутацию на основе иерархических сетевых адресов, их называют **маршрутизаторами**.

Концентраторы также используются для коммутации каналов в компьютерных сетях. Основные функции концентратора заключаются в повторении сигналов (повторитель) и концентрировании в себе (концентратор) как в центральном устройстве функций объединения компьютеров в единую сеть.

Модем (МОдулятор-ДЕМодулятор) — устройство прямого и обратного преобразования сигналов к виду, принятому для использования в определенном канале связи.

Вместо модема в локальных сетях можно использовать **сетевые адаптеры** (сетевые карты), выполненные в виде плат расширения, устанавливаемых в разъем материнской платы.

Информационное обеспечение сети представляет собой единый информационный фонд, ориентированный на решаемые в сети задачи и содержащий массивы данных общего применения, доступные для всех пользователей сети, и массивы индивидуального пользования, предназначенные для отдельных абонентов.

Программное обеспечение вычислительных сетей выполняет координацию работы основных звеньев и элементов сети; организует коллективный доступ ко всем ресурсам сети, динамическое распределение и перераспределение ресурсов с целью повышения эффективности обработки информации; выполняет техническое обслуживание и контроль работоспособности сетевых устройств.

6. Понятие операционной системы, функциональные компоненты операционных систем: управление процессами, управление памятью, управление файлами, управление внешними устройствами, защита данных и администрирование, интерфейс прикладного программирования, пользовательский интерфейс.

Операционная система (ОС) - это набор программ, контролирующих работу прикладных программ и системных приложений и исполняющих роль интерфейса между пользователями, прикладными и системными, приложениями и аппаратным обеспечением компьютера.

Функции ОС группируются в соответствии с типами локальных ресурсов, которыми управляет ОС. Наиболее важными подсистемами управления ресурсами являются подсистемы управления процессами, памятью, файлами и внешними устройствами, а подсистемами, общими для всех ресурсов, являются подсистемы пользовательского интерфейса, защиты данных и администрирования.

Для каждой выполняемой программы ОС организует один или более процессов. Каждый такой процесс представляется в ОС информационной структурой, содержащей данные о потребностях процесса в ресурсах, а также о фактически выделенных ему ресурсах. В современных мультипрограммных ОС может существовать одновременно несколько процессов. Поскольку процессы могут одновременно претендовать на одни и те же ресурсы, **подсистема управления процессами** планирует очередность выполнения процессов, обеспечивает их необходимыми ресурсами, осуществляет взаимодействие и синхронизацию процессов.

Подсистема управления памятью производит распределение физической памяти между всеми существующими в системе процессами, загрузку и удаление программных кодов и данных процессов в отведенные им области памяти, настройку адресно-зависимых частей кодов процесса на физические адреса выделенной области, а также защиту областей памяти каждого процесса.

Функции управления файлами сосредоточены в файловой системе ОС. Файловая система преобразует символьные имена файлов, с которыми работает пользователь или программист, в физические адреса данных на дисках, организует совместный доступ к файлам, защищает их от несанкционированного доступа.

Функции управления внешними устройствами возлагаются на подсистему управления внешними устройствами (подсистему ввода-вывода).

Безопасность данных вычислительной системы обеспечивается средствами отказоустойчивости ОС, направленными на защиту от сбоев и отказов аппаратуры и ошибок программного обеспечения, а также средствами защиты от несанкционированного доступа.

Возможности операционной системы доступны программисту в виде набора функций, который называется интерфейсом прикладного программирования

(Application Programming Interface, API). Приложения обращаются к функциям API с помощью системных вызовов.

Современные ОС поддерживают развитые функции **пользовательского интерфейса** для интерактивной работы за терминалами двух типов: алфавитно-цифровыми и графическими.

7. Определение алгоритма. Основные свойства алгоритма. Схемы представления алгоритма.

Алгоритм – описание последовательности действий (план), строгое исполнение которых приводит к решению поставленной задачи за конечное число шагов.

Основные свойства алгоритма:

- **Массовость**, т.е. алгоритм может быть пригоден для решения всех задач данного класса.
- **Результативность**, т.е. алгоритм должен приводить к получению результата за конечное число шагов.
- **Определенность**, т.е. описание алгоритма должно быть точным и понятным для получения однозначного результата при заданных исходных данных.
- **Дискретность**, т.е. описываемый алгоритмом процесс и сам алгоритм могут быть разбиты на отдельные элементарные этапы, возможность выполнения которых на компьютере у пользователя не вызывает сомнений.

На основании этих свойств иногда дается определение алгоритма, например: «Алгоритм – это последовательность математических, логических или вместе взятых операций, отличающихся детерминированностью, массовостью, направленностью и приводящая к решению всех задач данного класса за конечное число шагов».

Алгоритм должен быть формализован по некоторым правилам посредством конкретных изобразительных средств. К ним относятся следующие способы записи алгоритмов:

- **Словесный**. Представляет собой описание последовательных этапов обработки данных в произвольном изложении на естественном языке.
- **Графический**. Алгоритм изображается в виде последовательности связанных между собой функциональных блоков, каждый из которых соответствует выполнению одного или нескольких действий.
- **Псевдокоды**. Полуформализованные описания алгоритмов на условном алгоритмическом языке, включающие в себя как элементы языка программирования, так и фразы естественного языка, общепринятые математические обозначения и др.
- **Программная**. Алгоритм записывается в виде текста на языках программирования).

Наибольшее распространение благодаря своей наглядности получил графический (блок-схемный) способ записи алгоритмов.

Блок-схемой называется графическое изображение логической структуры алгоритма, в котором каждый этап процесса обработки информации представляется в виде геометрических символов (блоков), имеющих определенную конфигурацию в зависимости от характера выполняемых операций. Перечень символов, их наименование, отображаемые ими функции, форма и размеры определяются ГОСТами.

8. Принципы структурной алгоритмизации. Базовый набор структур. Линейная структура. Структура ветвления. Циклическая структура.

Значительный вклад в теорию программирования внес сотрудник фирмы «Барроуз» голландский ученый Э. Дейкстра. По его мнению, использование трех типов управляющих структур – простой последовательности, альтернативы (ветвления) и повторения (цикла) – позволило бы программистам обходиться **без оператора безусловного перехода** и тем самым добиться простоты написания и модификации программы. Сегодня структурное программирование является распространенной технологией программирования, наряду с объектно-ориентированным программированием.

Структурное программирование основывается на двух принципах:

- Последовательная детализация алгоритма «сверху вниз».
- Ограниченность базового набора структур для построения алгоритма любого уровня сложности.

В теории программирования доказано, что программу для решения задачи любой сложности можно составить из трех основных структур: последовательную, ветвления и цикла. Эти три структуры называют базовыми конструкциями структурного программирования:

1. Последовательная структура. Наиболее простая в реализации структура. Операторы (простые или составные) в ней выполняются последовательно один за другим.

2. Структура ветвления. В этой структуре выполняются те операторы (простые или составные), которые отвечают определенным условиям.

3. Циклическая структура. Циклом называется многократно повторяемый участок вычислений. Вычислительный процесс, содержащий один или несколько циклов, называется циклическим. По количеству выполнения циклы делятся на циклы с определенным (заранее заданным) числом повторений и циклы с неопределенным числом повторений. Количество повторений последних зависит от соблюдения некоторого условия, задающего необходимость выполнения цикла. При этом условие может проверяться в начале цикла — тогда речь идет о цикле с предусловием, или в конце — тогда это цикл с постусловием.

9. Понятие информационных систем (ИС). Особенности подходов к классификации информационных систем: по типу хранимых данных, по степени автоматизации, по характеру использования информации, по сфере применения.

Информационная система - это совокупность взаимосвязанных элементов, представляющих собой информационные, кадровые и материальные ресурсы, процессы, которые обеспечивают сбор, обработку, преобразование, хранение и передачу информации в организации.

В зависимости от объема решаемых задач, используемых технических средств, организации функционирования, информационные системы делятся на ряд групп (классов).

По типу хранимых данных ИС делятся на фактографические и документальные. Фактографические системы предназначены для хранения и обработки структурированных данных в виде чисел и текстов. В документальных системах информация представлена в виде документов, состоящих из наименований, описаний, рефератов и текстов.

Основываясь на **степени автоматизации информационных процессов** в системе управления фирмой, информационные системы делятся на ручные, автоматические и автоматизированные. Ручные ИС характеризуются отсутствием современных технических средств переработки информации и выполнением всех операций человеком. В автоматических ИС все операции по переработке информации выполняются без участия человека. Автоматизированные ИС предполагают участие в процессе обработки информации и человека, и технических средств, причем главная роль в выполнении рутинных операций обработки данных отводится компьютеру.

В зависимости от **характера обработки** данных ИС делятся на информационно-поисковые и информационно-решающие. Информационно-поисковые системы производят ввод, систематизацию, хранение, выдачу информации по запросу пользователя без сложных преобразований данных. Информационно-решающие системы осуществляют, кроме того, операции переработки информации по определенному алгоритму.

В зависимости от **сферы применения** различают следующие классы ИС: ИС организационного управления (предназначены для автоматизации функций управленческого персонала как промышленных предприятий, так и непромышленных объектов); ИС управления технологическими процессами (служат для автоматизации функций производственного персонала по контролю и управлению производственными операциями); ИС автоматизированного проектирования (САПР; предназначены для автоматизации функций инженеров-проектировщиков, конструкторов, архитекторов, дизайнеров при создании новой техники или технологии); интегрированные (корпоративные) ИС (используются для

автоматизации всех функций фирмы и охватывают весь цикл работ от планирования деятельности до сбыта продукции).

10. Состав и структура информационных систем.

Информационная система является элементом большой системы и обеспечивает задачи управления информационными ресурсами, поэтому для эффективной работы всей системы большое значение имеет ее структура и состав.

Все информационные системы (ИС) включают один и тот же набор компонентов:

- функциональные компоненты;
- компоненты систем обработки данных;
- организационные компоненты.

Функциональные компоненты – это задачи предметной области, методы и алгоритмы их решения. Задача включает набор исходных данных в виде атрибутов, отношения, показателей, базы данных.

Компоненты системы обработки данных – это совокупность систем, обеспечивающих функционирование всех структур ИС.

Организационные компоненты – состав и структура организаций, обеспечивающих эффективное функционирование экономического объекта.

Общую **структуру информационной системы** можно представить как совокупность обеспечивающих подсистем, среди которых обычно выделяют:

1. Информационное обеспечение — совокупность единой системы классификации и кодирования информации, унифицированных систем документации, схем информационных потоков, циркулирующих в организации, а также методология построения баз данных. Назначение подсистемы информационного обеспечения состоит в своевременном формировании и выдаче достоверной информации для принятия управленческих решений.

2. Техническое обеспечение — комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы.

3. Математическое и программное обеспечение — совокупность математических методов, моделей, алгоритмов и программ для реализации целей и задач информационной системы, а также нормального функционирования комплекса технических средств.

4. Организационное обеспечение — совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации информационной системы.

5. Правовое обеспечение — совокупность правовых норм, определяющих создание, юридический статус и функционирование информационных систем,

регламентирующих порядок получения, преобразования и использования информации.

11. Жизненный цикл информационных систем. Модели жизненного цикла ИС: каскадная, поэтапная, спиральная.

Жизненный цикл ИС можно представить как ряд событий, происходящих с системой в процессе ее создания и использования.

Можно выделить следующие фазы развития информационной системы:

- **Формирование концепции.** Главным содержанием работ на этой фазе является определение проекта, разработка его концепции.

- **Разработка технического задания.** Главным содержанием этой фазы является разработка технического предложения и переговоры с заказчиком о заключении контракта.

- **Проектирование.** На этой фазе определяются подсистемы, их взаимосвязи, выбираются наиболее эффективные способы выполнения проекта и использования ресурсов.

- **Изготовление.** На этой фазе производится координация и оперативный контроль работ по проекту, осуществляется изготовление подсистем, их объединение и тестирование.

- **Ввод системы в эксплуатацию.** На этой фазе проводятся испытания, опытная эксплуатация системы в реальных условиях, ведутся переговоры о результатах выполнения проекта и о возможных новых контрактах.

Модель жизненного цикла отражает различные состояния системы, начиная с момента возникновения необходимости в данной ИС и заканчивая моментом ее полного выхода из употребления. **Модель жизненного цикла** - структура, содержащая процессы, действия и задачи, которые осуществляются в ходе разработки, функционирования и сопровождения программного продукта в течение всей жизни системы, от определения требований до завершения ее использования.

В настоящее время известны и используются следующие модели жизненного цикла:

1. **Каскадная модель** предусматривает последовательное выполнение всех этапов проекта в строго фиксированном порядке. Переход на следующий этап означает полное завершение работ на предыдущем этапе.

2. **Поэтапная модель** с промежуточным контролем. Разработка ИС ведется итерациями с циклами обратной связи между этапами. Межэтапные корректировки позволяют учитывать реально существующее взаимовлияние результатов разработки на различных этапах; время жизни каждого из этапов растягивается на весь период разработки.

3. **Спиральная модель.** На каждом витке спирали выполняется создание очередной версии продукта, уточняются требования проекта, определяется его

качество и планируются работы следующего витка. Особое внимание уделяется начальным этапам разработки - анализу и проектированию, где реализуемость тех или иных технических решений проверяется и обосновывается посредством создания прототипов (макетирования).

12. Определение информационных технологий (ИТ). Эволюция ИТ. Составляющие информационных технологий.

Информационная технология – это совокупность средств и методов переработки информационного ресурса с целью получения новой информации (информационного продукта) на базе аппаратного и программного обеспечения.

Эволюционное развитие можно представить в пять этапов:

1-й этап (до второй половины XIX в.) – «ручная» информационная технология, инструментарий которой составляли: перо, чернильница, книга. Коммуникации осуществлялись ручным способом путем передачи через почту писем, пакетов, депеш. Основная цель технологии – представление информации в нужной форме.

2-й этап (с конца XIX в.) – «механическая» технология, инструментарий которой составляли: пишущая машинка, телефон, диктофон, оснащенная более совершенными средствами доставки почта. Основная цель технологии – представление информации в нужной форме более удобными средствами.

3-й этап (40 – 60-е гг. XX в.) – «электрическая» технология, инструментарий которой составляли: большие ЭВМ и соответствующее программное обеспечение, электрические пишущие машинки, ксероксы, портативные диктофоны. Изменяется цель технологии, акцент начинает перемещаться с формы представления информации на формирование ее содержания.

4-й этап (с начала 70-х гг.) – «электронная» технология, основным инструментарием которой становятся большие ЭВМ и создаваемые на их базе автоматизированные системы управления (АСУ) и информационно-поисковые системы (ИПС), оснащенные широким спектром базовых и специализированных программных комплексов.

5-й этап (с середины 80-х гг.) – «компьютерная» («новая») технология, основным инструментарием которой является персональный компьютер с широким спектром стандартных программных продуктов разного назначения. На этом этапе происходит процесс персонализации АСУ, который проявляется в создании систем поддержки принятия решений определенными специалистами.

Информационная технология базируется и зависит от технического, программного, информационного, методического и организационного обеспечения.

Техническое обеспечение - это персональный компьютер, оргтехника, линии связи, оборудование сетей.

Программное обеспечение, находящееся в прямой зависимости от технического и информационного обеспечения, реализует функции накопления, обработки, анализа, хранения данных.

Информационное обеспечение - совокупность данных, представленных в определенной форме для компьютерной обработки.

Организационное и методическое обеспечение представляют собой комплекс мероприятий, направленных на функционирование компьютера и программного обеспечения для получения искомого результата.

13. Классификация информационных технологий. Особенности ИТ, различаемых по способу реализации в ИС, по степени охвата ИТ задач управления, по классам реализуемых технологических операций, по типу пользовательского интерфейса, по вариантам использования сети ЭВМ, по обслуживаемой предметной области.

ИТ в настоящее время можно классифицировать по ряду признаков.

По **способу реализации** ИТ в информационных системах выделяют традиционные и новые информационные технологии. Традиционные ИТ прежде всего существовали в условиях централизованной обработки данных, новые информационные технологии связаны с информационным обеспечением процесса управления в режиме реального времени.

По **степени охвата** ИТ задач управления выделяют электронную обработку данных, когда с использованием ЭВМ без пересмотра методологии и организации процессов управления ведется обработка данных с решением отдельных экономических задач, и автоматизацию управленческой деятельности.

По **классам реализуемых технологических операций** ИТ рассматриваются в программном аспекте и включают: текстовую обработку; электронные таблицы; автоматизированные банки данных; обработку графической и звуковой информации; мультимедийные и другие системы.

По **типу пользовательского интерфейса** ИТ рассматриваются с точки зрения возможностей доступа пользователя к информационным и вычислительным ресурсам. Пакетная ИТ исключает возможность пользователя влиять на обработку информации, пока она производится в автоматическом режиме. Диалоговая ИТ предоставляет пользователю неограниченную возможность взаимодействовать с хранящимися в системе информационными ресурсами в реальном масштабе времени.

Интерфейс **сетевой АИТ** предоставляет пользователю средства доступа к территориально распределенным информационным и вычислительным ресурсам благодаря развитым средствам связи.

В настоящее время наблюдается тенденция к объединению (интеграции) различных типов ИТ в единый компьютерно-технологический комплекс. Он

поддерживает единый способ представления данных и взаимодействия пользователей с компонентами системы, обеспечивает информационные и вычислительные потребности специалистов в их профессиональной работе.

Повышение требований к оперативности информационного обмена и управления привело к созданию не только локальных, но и многоуровневых и распределенных систем организационного управления объектами (банковские, налоговые, снабженческие, статистические и др. службы). Эту проблему в новых информационных технологиях решают распределенные системы обработки данных с использованием каналов связи для обмена информацией между базами данных различных уровней.

14. Этапы проектирования баз данных. Инфологическое моделирование. Даталогическое моделирование. Физическое проектирование баз данных.

База данных (БД) - именованная совокупность данных, отражающая состояние объектов и их отношений в рассматриваемой предметной области. Другие определения:

Этапы проектирования БД:

Этап 1 – включает в себя изучение, анализ и описание информационных процессов предметной области, выявление информационных потребностей пользователей и формулирование требований к содержанию БД и обработке данных.

Этап 2 – построение инфологической модели предметной области.

Этап 3 предполагает построение вариантов логической структуризации БД (Даталогическая модель), их анализ и выбор согласно критериям качества (НЕизбыточность, НЕпротиворечивость, Независимость проектируемой БД).

Этап 4 - выполняется построение вариантов физической структуры, их анализ выбор согласно требованиям к основным эксплуатационным характеристикам БД (время, память, уровень защиты данных). На этапе физического проектирования решаются вопросы, связанные с производительностью системы, определяются структуры хранения данных и методы доступа.

Модель данных – совокупность структур данных и операций по их обработке.

Создание **инфологической модели** является естественным продолжением исследований предметной области, но в отличие от него является представлением БД с точки зрения проектировщика (разработчика). Инфологическую модель можно представить в виде словесного описания, однако наиболее наглядным является использование специальных графических нотаций, разработанных для проведения подобного рода моделирования.

Даталогическая модель БД - модель логического уровня, представляющая собой отображение логических связей между элементами данных, независимо от их содержания и среды хранения. Основной задачей даталогического моделирования

является описание свойств понятий предметной области, их взаимосвязь и ограничения, накладываемые на данные. Даталогическая модель является начальным прототипом создаваемой базы данных.

Физическое проектирование БД – доводка логического проекта с учетом особенностей выбранной системы управления базами данных (СУБД) и требований к эксплуатационным характеристикам БД. Эта доводка включает в себя установку явных связей между таблицами, определение индексов таблиц, определение запоминающих устройств, методов доступа, способов защиты и данных.

15. Основные понятия реляционной модели данных и их определения: отношение, тип данных, домен, атрибут, кортеж, первичный ключ.

Реляционная модель основана на математическом понятии отношения, физическим представлением которого является таблица.

В любой реляционной СУБД предполагается, что пользователь воспринимает базу данных как набор таблиц.

Атрибут - именованный столбец отношения.

Домен - набор допустимых значений одного или нескольких атрибутов.

Кортеж - строка отношения. Кортежи могут располагаться в любом порядке, при этом отношение будет оставаться тем же самым, а значит, и иметь тот же смысл.

Первичным ключом (ключевым атрибутом) называется атрибут отношения, однозначно идентифицирующий каждый из его кортежей. Ключ может быть **составным (сложным)**, то есть состоять из нескольких атрибутов.

Каждое отношение обязательно имеет комбинацию атрибутов, которая может служить ключом. Ее существование гарантируется тем, что отношение — это множество, которое не содержит одинаковых элементов — кортежей. То есть в отношении нет повторяющихся кортежей, а это значит, что по крайней мере вся совокупность атрибутов обладает свойством однозначной идентификации кортежей отношения.

Возможны случаи, когда отношение имеет несколько комбинаций атрибутов, каждая из которых однозначно определяет все кортежи отношения. Все эти комбинации атрибутов являются **возможными ключами** отношения. Любой из возможных ключей может быть выбран как первичный.

Ключи обычно используют для достижения следующих целей:

- исключения дублирования значений в ключевых атрибутах (остальные атрибуты в расчет не принимаются);
- упорядочения кортежей. Возможно упорядочение по возрастанию или убыванию значений всех ключевых атрибутов, а также смешанное упорядочение (по одним — возрастание, а по другим — убывание);
- ускорения работы к кортежами отношения;

- организации связывания таблиц.

Внешний ключ - единственный или группа атрибутов, которые могут служить в качестве первичного ключа для других таблиц. Внешний ключ в одной таблице (дочерней) является ссылкой на первичный ключ другой таблицы (родительской). С помощью внешних ключей устанавливаются связи между отношениями.

16. Понятие информационной безопасности (ИБ). Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.

Под **информационной безопасностью** понимают состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации).

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Самая распространенная модель информационной безопасности базируется на обеспечении трех свойств информации: конфиденциальность, целостность и доступность.

Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем. Если доступ к информации получает неуполномоченное лицо, происходит утрата конфиденциальности.

Для некоторых типов информации конфиденциальность является одним из наиболее важных атрибутов (например, данные стратегических исследований, медицинские и страховые записи, спецификации новых изделий и т. п.). В определенных случаях важно сохранить конфиденциальность сведений о конкретных лицах (например, сведения о клиентах банка, о кредиторах, налоговые данные; сведения медицинских учреждений о состоянии здоровья пациентов и т. д.).

Целостность информации определяется ее способностью сохраняться в неискаженном виде. Неправомочные, и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к потере целостности. Целостность особенно важна для данных, связанных с функционированием объектов критических инфраструктур (например, управления воздушным движением, энергоснабжения и т. д.), финансовых данных.

Доступность информации определяется способностью системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Уничтожение или блокирование

информации (в результате ошибки или преднамеренного действия) приводит к потере доступности.

Доступность — важный атрибут для функционирования информационных систем, ориентированных на обслуживание клиентов (системы продажи железнодорожных билетов, распространения обновлений программного обеспечения).

Кроме перечисленных трех свойств дополнительно выделяют еще два свойства, важных для информационной безопасности: аутентичность и апеллируемость.

Аутентичность — возможность достоверно установить автора сообщения.

Апеллируемость — возможность доказать, что автором является именно данный человек и никто другой.

17. Угрозы информационной безопасности. Классификация угроз информационной безопасности.

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Соответственно угрозой информационной безопасности называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или компоненты ИС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Атака — попытка реализации угрозы.

Нарушение — реализация угрозы.

Определение, анализ и классификация возможных угроз безопасности ИС является одним из важнейших аспектов проблемы обеспечения ее безопасности. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты.

Классификацию угроз ИБ можно выполнить по нескольким критериям:

1. **По аспекту ИБ:** угрозы конфиденциальности, угрозы целостности, угрозы доступности. Дополнительно можно выделить угрозы аутентичности и апеллируемости.

2. **По компонентам ИС, на которые нацелена угроза:** данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура).

3. **По расположению источника угроз:** внутри или вне рассматриваемой ИС.

4. **По природе возникновения:** естественные (объективные) и искусственные (субъективные). Естественные угрозы — это угрозы, вызванные воздействиями на ИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека. Искусственные угрозы — угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно

выделить непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании ИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п., и преднамеренные (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты.

18. Вредоносное программное обеспечение. Классификация вирусов. Троянские кони.

Компьютерным вирусом называется программа, способная к саморазмножению. Это означает, что программа, будучи запущенной, способна создавать свои копии (возможно, модифицированные) и распространять их некоторым образом с компьютера на компьютер.

Вирус, как программа, состоит из двух частей: механизм размножения и начинка. Механизм размножения определяет способ, которым копии вируса создаются, распространяются и запускаются. Начинка представляет собой дополнительное поведение вируса (помимо размножения) на зараженном компьютере.

Начинка некоторых вирусов является вполне безобидной (например, вывод сообщения на экране), а некоторых — весьма опасной: уничтожение данных, похищение информации. В любом случае вирус оказывает негативное воздействие, расходуя ресурсы процессора, оперативную память и дисковое пространство. По этой причине вирусы называют вредоносными программами.

Вредоносной программой называют любую программу, которая устанавливает себя на компьютер без ведома его владельца и осуществляет нежелательные для него функции.

Общепринятая классификация вирусов — по механизму их размножения. Выделяются файловые вирусы, макровирусы, загрузочные вирусы и сетевые черви:

- **Файловые вирусы** внедряются в исполняемые файлы на компьютере (заражают их), дописывая самих себя в начало, в середину или в конец файла. Таким образом, при запуске пользователем зараженного файла автоматически будут выполнены и команды вируса (поиск незараженных файлов, их заражение, а также начинка).

Макровирусы не отличаются по механизму размножения от файловых вирусов; их особенность в том, что заражают они не исполняемые файлы, а файлы некоторых популярных форматов документов (в частности, .doc и .xls). Макровирусы оказались опасны тем, что пользователи привыкли к мысли о том, что зараженной может быть только программа и не опасались получить вирус вместе с документом. Макровирус представляет собой программу на макроязыке, внедренную в документ соответствующего формата и запускающуюся автоматически обычно при открытии документа.

- Вирусы, распространяющие свои копии по локальной сети или через Интернет называются **сетевыми червями**. Большинство сетевых червей являются резидентными (автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти). Вирусы, распространяющиеся через Интернет, являются наиболее популярными и представляют наибольшую угрозу.

- **Загрузочные вирусы** заражают носители данных. Изначально заражению подвергались дискеты и жесткие диски. Загрузочный вирус прописывает себя в первый (нулевой) сектор раздела, где обычно находится программа-загрузчик. Сама эта программа перемещается в другое место, а при загрузке с зараженного носителя сначала запускается вирус. Вирус предпринимает меры к тому, чтобы закрепиться в оперативной памяти и получить контроль над системой, после чего позволяет загружаться стандартному загрузчику.

Троянским конем называется вредоносная программа, которая не имеет (в отличие от вирусов) способности к саморазмножению, а вместо этого маскируется под программу, выполняющую полезные функции. Таким образом, распространение троянских коней часто происходит посредством самих пользователей, которые скачивают их из Интернета или друг у друга, не догадываясь о последствиях.

Особая опасность в том, что пользователи принимают их за легальные программы. Поэтому запуская троянского коня пользователь может вручную дать ей все необходимые права, открыть доступ в Интернет и к системным ресурсам. Одна из распространенных начинок троянских коней — бэкдор — программа, позволяющая злоумышленнику получать удаленный доступ к системе (а в некоторых случаях полностью ее контролировать).

19. Меры противодействия угрозам безопасности: законодательные, административные, процедурные и программно-технические.

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: законодательные (правовые), административные (организационные), процедурные и программно-технические.

К **законодательным мерам защиты** относятся действующие в стране нормативно-правовые акты, регламентирующие правила обращения с информацией,

закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Важное значение имеют стандарты в области защиты информации (в первую очередь, международные). Среди этих стандартов выделяются «Оранжевая книга», рекомендации X.800 и «Общие критерии оценки безопасности информационных технологий» (Common Criteria for IT Security Evaluation).

«Оранжевая книга» — крупнейший базовый стандарт. В ней даются важнейшие понятия, определяются основные сервисы безопасности и предлагается метод классификации информационных систем по требованиям безопасности.

Рекомендации X.800 в основном посвящены вопросам защиты сетевых конфигураций. Они предлагают развитый набор сервисов и механизмов безопасности.

Осенью 2006 года в России был принят национальный стандарт ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология — Практические правила управления информационной безопасностью», соответствующий международному стандарту ИСО 17799. Стандарт представляет собой перечень мер, необходимых для обеспечения информационной безопасности организации, включая действия по созданию и внедрению системы управления информационной безопасности.

Административные меры защиты — меры организационного характера, регламентирующие процессы функционирования ИС, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

1. Подбор и подготовку персонала системы.
2. Организацию охраны и пропускного режима.
3. Организацию учета, хранения, использования и уничтожения документов и носителей с информацией.
4. Распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.д.).

Меры процедурного уровня — отдельные мероприятия, выполняемые на протяжении всего жизненного цикла ИС. Они ориентированы на людей (а не на технические средства) и подразделяются на:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Программно-технические меры защиты основаны на использовании специальных аппаратных средств и программного обеспечения, входящих в состав ИС и выполняющих функции защиты: шифрование, аутентификацию,

разграничение доступа к ресурсам, регистрацию событий, поиск и удаление вирусов и т.д.

20. Основные принципы построения систем защиты информационных систем: простота механизма защиты, системность, комплексность, непрерывность, разумная достаточность, гибкость, открытость алгоритмов и механизмов защиты.

К основным принципам построения систем защиты информационных систем относят:

1. **Простота механизма защиты.** Используемые средства защиты не должны требовать от пользователей специальных знаний или значительных дополнительных трудозатрат. Они должны быть интуитивно понятны и просты в использовании,

2. **Системность.** При разработке системы защиты и вводе ее в эксплуатацию необходим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для обеспечения безопасности. В частности, должны быть учтены все слабые места ИС, возможные цели и характер атак, возможность появления принципиально новых угроз безопасности.

3. **Комплексность.** Предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Целесообразно строить эшелонированную систему защиты, обеспечивающую комплексную безопасность на разных уровнях (внешний уровень — физические средства, организационные и правовые меры; уровень ОС; прикладной уровень).

4. **Непрерывность.** Мероприятия по обеспечению информационной безопасности ИС должны осуществляться на протяжении всего ее жизненного цикла — начиная с этапов анализа и проектирования и заканчивая выводом системы из эксплуатации. При этом наилучший результат достигается, когда разработка системы защиты идет параллельно с разработкой самой защищаемой ИС. Не допускается также никаких перерывов в работе средств защиты.

5. **Разумная достаточность.** Один из основополагающих принципов информационной безопасности гласит: абсолютно надежная защита невозможна. Любой самый сложный механизм защиты может быть преодолен злоумышленником при затрате соответствующих средств и времени. Система защиты считается достаточно надежной, если средства, которые необходимо затратить злоумышленнику на ее преодоление значительно превышают выгоду, которую он получит в случае успеха. Иногда используется обратный принцип: расходы на систему защиты (включая потребляемые ей системные ресурсы и неудобства, возникающие в связи с ее использованием) не должны превышать стоимость защищаемой информации.

6. **Гибкость.** Система защиты должна иметь возможность адаптироваться к меняющимся внешним условиям и требованиям.

7. **Открытость алгоритмов и механизмов защиты.** Система должна обеспечивать надежную защиту в предположении, что противнику известны все детали ее реализации. Или иными словами, защита не должна обеспечиваться за счет секретности структуры и алгоритмов системы защиты ИС.

II. ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

1. Понятие ЭВМ. Классификация ЭВМ по различным признакам. Классификация ЭВМ по быстродействию: суперЭВМ, большие ЭВМ, средние (малые) ЭВМ, персональные ЭВМ, встраиваемые микропроцессоры. Классификация ЭВМ по месту и роли в компьютерной сети: кластерные структуры (многомашинные вычислительные системы), серверы, рабочие станции, сетевые компьютеры.

2. Общие принципы построения современных ЭВМ. Классическая структура ЭВМ Дж. фон Неймана.

3. Функциональная и структурная организация современных ЭВМ. Центральные и периферийные устройства. Состав и характеристика центральных устройств: процессор, основная память, системная магистраль. Состав и характеристика периферийных устройств: внешние запоминающие устройства, устройства ввода-вывода.

4. Вычислительные сети. Классификация вычислительных сетей по различным признакам: по принципу территориальной рассредоточенности, по способу управления, по принципу передачи информации, по топологии.

5. Техническое, информационное и программное обеспечение сетей. Рабочая станция, сервер, хост-компьютер. Концентраторы. Коммутаторы. Маршрутизаторы. Сетевые карты.

6. Понятие операционной системы, функциональные компоненты операционных систем: управление процессами, управление памятью, управление файлами, управление внешними устройствами, защита данных и администрирование, интерфейс прикладного программирования, пользовательский интерфейс.

7. Определение алгоритма. Основные свойства алгоритма. Схемы представления алгоритма.

8. Принципы структурной алгоритмизации. Базовый набор структур. Линейная структура. Структура ветвления. Циклическая структура.

9. Понятие информационных систем (ИС). Особенности подходов к классификации информационных систем: по степени автоматизации, по назначению, по характеру использования информации, по признаку

структурированности задач, по степени централизации обработки информации, по уровню управления.

10. Состав и структура информационных систем.

11. Жизненный цикл информационных систем.

12. Определение информационных технологий (ИТ). Эволюция ИТ. Составляющие информационных технологий.

13. Классификация информационных технологий. Особенности ИТ, различаемых по способу реализации в ИС, по степени охвата ИТ задач управления, по классам реализуемых технологических операций, по типу пользовательского интерфейса, по вариантам использования сети ЭВМ, по обслуживаемой предметной области.

14. Этапы проектирования баз данных. Информатическое моделирование. Даталогическое моделирование. Физическое проектирование баз данных.

15. Основные понятия реляционной модели данных и их определения: тип данных, домен, атрибут, кортеж, отношение, первичный ключ.

16. Понятие информационной безопасности (ИБ). Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность.

17. Угрозы информационной безопасности. Классификация угроз информационной безопасности.

18. Вредоносное программное обеспечение. Классификация вирусов. Троянские кони.

19. Меры противодействия угрозам безопасности: законодательные, административные, процедурные и программно-технические.

20. Основные принципы построения систем защиты информационных систем: простота механизма защиты, системность, комплексность, непрерывность, разумная достаточность, гибкость, открытость алгоритмов и механизмов защиты.

III. КРИТЕРИИ ОЦЕНКИ СДАЧИ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

При оценке ответов абитуриентов в процессе вступительного испытания учитываются:

- уверенные знания, умения и навыки, включенные в соответствующие вопросы;

- способность устанавливать причинно- следственные связи в изложении материала, делать выводы;

- умение применять теоретические знания для анализа конкретных экономических ситуаций и решения прикладных проблем современной экономики;

- общий (культурный) и специальный (профессиональный) язык ответа;

- знание ситуации и умение применить правильный научный и методический подход и инструментарий для решения управленческих задач;

- умение выделять приоритетные направления в менеджменте организаций.

Оценка производится по 100 бальной шкале.

Оценка от 0 до 40 баллов выставляется при неполном соответствии уровня знаний абитуриента программе среднего (полного) образования. Он не усвоил ряд положений программного материала, вследствие чего допустил при ответе грубые ошибки. На дополнительные вопросы он также не ответил.

Оценка от 41 до 80 баллов выставляется при соответствии в целом уровня знаний абитуриента программе среднего (полного) образования. Однако при ответе допустил ошибки, на дополнительные вопросы ответил не точно.

Оценка от 81 до 100 баллов выставляется при полном соответствии уровня знаний абитуриента программе среднего (полного) образования. При ответе продемонстрированы глубокие знания. Однако на дополнительные вопросы ответы даны не исчерпывающие и не уверенные.

100 баллов выставляются при безупречном ответе абитуриента на основной и дополнительные вопросы.

III. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

1. Городов, О. А. Информационное право: учебник / О. А. Городов. - М.: Проспект, 2011.
2. Рассолов, И. М. Информационное право [Электронный ресурс]: учебник / И. М. Рассолов. - М. : Юрайт, 2011.
3. Ярочкин В.И. Информационная безопасность. Учебное пособие для студентов непрофильных вузов. – М.: Междунар. отношения, 2010 г. – 400 с.
4. Абрамян М. Э. Практикум по информатике. Работа с текстовыми документами, электронными таблицами и базами данных в системе Microsoft Office. –М.: Дашков и Ко, 2011
5. Аляев Ю.А., Гладков В.П., Козлов О.А. Практикум по алгоритмизации и программированию на языке Паскаль: Учеб. пособие. –М.: Финансы и статистика, 2010
6. Культин Н. Turbo Pascal в задачах и примерах. –СПб.: Питер, 2011
7. Молодцов В.А. Информатика. Тесты, задания, лучшие методики. –М.: Феникс, 2010
8. Вовк Е.Т. Информатика: пособие для подготовки к ЕГЭ. Кудиц-пресс, 2012