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

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.1.24 Безопасность систем баз данных

Направление подготовки (специальность) **10.05.03 Информационная безопасность автоматизированных систем**

Профиль образовательной программы **Информационная безопасность автоматизированных систем критически важных объектов**

Форма обучения: **очная**

СОДЕРЖАНИЕ

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция №1-6 (12 часов).

Тема: «Основы информационной безопасности автоматизированных систем. Характеристика автоматизированных систем и информационных процессов.**»**

1.1.1 Вопросы лекции:

1. Понятие базы данных

2. Назначение и основные компоненты системы баз данных

1.1.2 Краткое содержание вопросов:

1.

Банк данных (БнД) – это система специально организованных данных, программных, языковых, организационных и технических средств, предназначенных для централизованного накопления и коллективного многоцелевого использования данных.

Под базой данных (БД) обычно понимается именованная совокупность данных, отображающая состояние объектов и их отношений в рассматриваемой предметной области. Характерной чертой баз данных является постоянство: данные постоянно накапливаются и используются; состав и структура данных, необходимых для решения тех или иных прикладных задач, обычно постоянны и стабильны во времени; отдельные или даже все элементы данных могут меняться – но это и есть проявление постоянства – постоянная актуальность.

Услугами БнД пользуется обычно большое число пользователей. Поэтому в БнД предусматривается специальное средство приведения всех запросов к единой терминологии — словарь данных. Кроме того, используются специальные методы эквивалентных грамматических преобразований запросов для построения оптимальных процедур их обработки, специальные методы доступа к одним и тем же данным различных пользователей при совпадении во времени поступивших запросов — механизм транзакций.

2.

Многоаспектное использование данных (принцип однократного ввода данных для разных пользователей и приложений)

Комплексная оптимизация. (Например, выбор структуры хранения данных, которая обеспечивает наилучшее обслуживание в целом). В максимальной степени удовлетворяются противоречивые требования.

Обеспечение возможности стандартизации (упрощение обмена данных, контроля и восстановления данных).

Обеспечение возможности санкционированного доступа к данным. Интеграция данных приводит к тому, что данные, используемые различными пользователями, могут пересекаться различным образом. Следовательно, важно наличие в этих условиях механизма защиты данных от несанкционированного доступа к ним.

БнД через СУБД обеспечивает независимость прикладных программ от данных, чтобы не выполнять трудоемких ручных операций по внесению соответствующих изменений в прикладные программы.

Рассматривая данные как один из ресурсов АС (автоматизированных систем), можно сказать, что БнД централизованно управляет этим ресурсом в интересах всей системы. Наличие централизованного управления данными — главная отличительная черта БнД.

БнД — информационная система, реализующая централизованное управление данных в интересах всех пользователей АС. (Средство интеграции данных).

БнД — может рассматриваться в узком и широком смысле этого понятия. В узком БнД=БД + СУБД. В широком БнД =АС (автоматизированная система).

БнД в узком смысле включает в состав две основные компоненты: БД СУБД — для реализации централизованного управления данными, хранимыми в базе, доступа к ним, поддержание их в состоянии, соответствующем состоянию ПО.

В широком смысле БнД — это АСУправляет БнД администратор банка данных (АБД).Словарь данных (СД) представляет собой специальную систему в составе БнД, предназначенную для хранения единообразной информации обо всех ресурсах данных конкретного банка. В словаре содержатся сведения об объектах, их свойствах и отношениях для данной ПО, сведения о данных, хранимых в базе об их возможных значениях и форматах представления, об источниках их возникновении. Основной функцией АБД является обеспечение структур данных и взаимосвязь между ними, эффективных для обслуживания именно всего коллектива пользователей. Это функция администрирования БД. БнД отличаются тем, что их внедрение и последующая эксплуатация занимает довольно продолжительное время. Поэтому функции АБД являются долгосрочными и направлены на координацию всех этапов проектирования, реализации и ведения БД. На стадии проектирования АБД выступает основным идеологом, руководит всеми работами по разработке или приобретению ПО, обучение обслуживающего персонала и т.п. На стадии эксплуатации отвечает за нормальную эксплуатацию и функционирование БнД, управляет режимом работы, отвечает за

сохранность данных.Функции АБД: решать вопросы организации данных об объектах ПО и установлении связей между этими данными с целью объединения информации о различных объектах; согласовывать представления пользователей; координировать все действия по проектированию, реализации и ведению БД; учитывать текущие и перспективные требования пользователей; следить, чтобы БД удовлетворял актуальным информационным потребностям; вопросы расширения БД в связи с изменением границ ПО; защита данных от некомпетентного использования, от сбоев ТС, определения степени секретности части информации и разграничения доступа к ним; ведение СД, контроль избыточности и противоречивости, достоверность; методы хранения данных, пути доступа к ним, связей между данными, определение форматов данных, определять степень влияния изменений в данные на всю БД; координация вопросов технического обеспечения системы; координация работы системных программистов, разрабатывающих дополнительные ПО для улучшения эксплуатационных характеристик системы; координация работы прикладных программистов, разрабатывающих новые прикладные программы в рамках состава ПО системы . Структура БнД: информационная база – данные, отражающие состояние определенной предметной области и используемые информационной системой. Состоит из двух компонент: 1) коллекции записей собственно данных; 2) описания этих данных – метаданных. Данные могут использоваться (т. е. представляться) по-разному. С одной стороны, разные прикладные задачи требуют разных наборов данных, в совокупности обеспечивающих функциональную полноту информации, а с другой – они должны быть различны для различных категорий субъектов (разработчиков или пользователей). Назначение – представление данных на трех уровнях. В литературе по БД упоминается три уровня представления данных: концептуальный - пользователь, разработчик ИС, внешний (логический) – прикладной программист, внутренний (физической) — СУБД; лингвистические средства обеспечивают интерфейс пользователей разных категорий с банком данных и базируются на языковых средствах СУБД. Включают в себя ЯОД, описание, модель данных и их отношения и ЯМД – средства запросов к БД и поддержания БД;программные средства осуществляют обработку данных и управление этой обработкой в вычислительной среде, а также взаимодействие с операционной системой и прикладными программами. Компоненты: ядро (обеспечивает управление данными во внешней и оперативной памяти, а также протоколирование изменений), процессор языка баз данных (обработка – трансляция или компиляция – и оптимизация запросов на выборку и изменение данных), подсистема (библиотека) поддержки программных вызовов (обслуживает прикладные программы управления данными, взаимодействующие с СУБД через средства пользовательского

интерфейса), сервисные программы (системные и внешние утилиты) (обеспечивают настройку СУБД, восстановление после сбоев и ряд дополнительных возможностей обслуживания);

• технические средства служат для обеспечения эффективной и бесперебойной работы баз данных. Должны быть отказоустойчивыми, иметь надежные устройства ввода-вывода и объемные быстродействующие накопители;

• организационно-административные подсистемы и нормативно-методическое обеспечение – не являются технической компонентой системы, однако трудно рассчитывать на устойчивое и долговременное функционирование банка данных, если будут отсутствовать необходимые методические и инструктивные материалы, регламентирующие работу пользователей, различных по своему статусу и уровню полноценности.

1. 2 Лекция №7-12 (12 часов).

Тема: «Угрозы безопасности автоматизированных систем**»**

1.2.1 Вопросы лекции:

1. Назначение СУБД
2. Структура систем управления базами данных.

1.2.2 Краткое содержание вопросов:

1.

Первые БД берут свое начало с 50-х годов XX века. Это были файловые системы, в которых применялись универсальные программные средства, такие как Фортран, Алгол, Кобол и др. В 60-х годах появились первые системы управления базами данных **(СУБД) - это совокупность программ, предназначенных для построения и обслуживания БД**. Для примера можно назвать такие СУБД, как IMS, которая поддерживала иерархическую модель данных, а позже dBASE, FoxPro, Delphi, Informix, Oracle, MS Access, MySQL, SyBase и др. - реляционного типа. СУБД развиваются в направлении взятие на себя все большего количества функций, но только общих, которые касаются всех или большинства работ. Они не могут учитывать специфику конкретных потребностей, поэтому выглядят стандартными. Таким образом, программное обеспечение БД можно условно поделить на стандартное, которое поставляется вместе с СУБД и прикладное, изготовленное программистами во время построения и ведения БД с помощью специальных программных средств, которые имеет СУБД. Кроме уже вышеперечисленных видов работ по обработке данных,

прикладные программы обеспечивают выдачу отчетов, в том числе в графическом виде, предоставляют пользователю БД выгодный интерфейс, например, формы, в которых может содержаться не только информация, но и средства управления данными и программами, такие как кнопки, списки и т.п., следят за состоянием данных, например, автоматически выдают своевременное предупреждение о наличии горячих курортных путевок, об истечения срока хранения товаров, обеспечивают связь с сетью Internet и многое другое.В рамках этого пособия ознакомимся с двумя СУБД, которые будут использованы для демонстрации примеров работ в БД, а именно: MS Access (версия MS Access 2003) и Oracle (версия Oracle 8i). Первая характерна выгодным местоположением и легкодоступностью, потому что это дополнение к Windows. Она сравнительно проста в пользовании, поэтому выгодна на первых этапах изучения организации БД. Вторая принадлежит к числу наиболее мощных современных СУБД, она обеспечивает знакомство с практически всеми тонкостями, касающихся построения и администрирования БД.**Модель "сущность-связь" (ER-модель)** (англ. Entity-relationship model или entity-relationship diagram) - модель данных, позволяющая описывать концептуальные схемы с помощью обобщенных конструкций блоков. ER-модель - это метамодель данных, то есть средство описания моделей даных.

2.

Сама по себе база данных является хранилищем данных. Для того, чтобы извлечь нужную информацию из базы данных или внести новые сведения необходимо специальное программное обеспечение, которое называется Системой Управления Базами Данных (СУБД).

СУБД представляет собой программу, которая позволяет создать новую базу данных, открыть существующую, просмотреть записи, выбрать необходимую информацию по условию, удалить запись и т. д. Управление производится с помощью меню или специальных команд в командном окне. С помощью специальных средств, предоставляемых СУБД, можно создать свою программу, которая будет автоматически осуществлять определенные операции с конкретной базой данных.

Все СУБД хранят базу данных в файлах своего формата. Чтобы это подчеркнуть, используются специальные расширения файла. Поэтому, база данных, созданная с помощью одной СУБД, может не работать с другой. Далее в таблице приведены расширения файлов, созданных различными СУБД.

Программа Microsoft Access – одна из наиболее распространенных в нашей стране систем управления базами данных (файл базы данных имеет расширение .mdb).

В нашей стране также распространены системы управления базами данных: Visual FoxPro, Clipper, Paradox, Oracle, Microsoft SQL Server. Эти системы имеют англоязычный интерфейс, и одно из основных преимуществ Microsoft Access – это интерфейс с пользователем на русском языке.

Введем основные определения объектов базы данных:

Таблицы– информация в базе данных хранится в виде таблиц (таблица – это совокупность данных, упорядоченных по строкам и столбцам);

Запросы– при помощи запросов можно выбирать нужные данные из таблиц (например, у Вас в таблице хранятся сведения по клиентам за все время работы Вашей фирмы, а Вы хотите отобрать новых клиентов за последние два месяца, то можно на основе таблицы клиенты построить нужный запрос);

Формы– позволяют отображать данные, содержащиеся в таблицах или запросах в удобном для восприятия виде;

Отчеты– предназначены для распечатки данных, содержащихся в таблицах и запросах в красиво оформленном виде;

Макросы и модули– программы на языке Visual Basic for Application позволяющие автоматизировать повторяющиеся операции.

Элементы управления– это объекты, предназначенные для отображения или управления данными в формах или отчетах (например элемент «поле» в форме или отчете может отображать строку из таблицы, кнопка «Новая запись» добавляет новую строку в таблицу). Некоторые элементы управления предназначены для оформления – это различные линии и надписи.

1. 3 Лекция №13-17 (10 часов).

Тема: «Основы принципы защиты информационных процессов в автоматизированных системах**»**

1.3.1 Вопросы лекции:

1. Модели данных

1.3.2 Краткое содержание вопросов:

1. Набор принципов, определяющих организацию логической структуры хранения данных в базе, получил название модели данных.Модели баз данных определяются тремя компонентами:

— допустимой организацией данных;

— ограничениями целостности;

— множеством допустимых операций

В теории систем управления базами данных выделяют модели трех основных типов: иерархическую, сетевую и реляционную.Терминологической основой для иерархической и сетевой моделей являются понятия: атрибут, агрегат и запись. Под атрибутом (элементом данных) понимается наименьшая поименованная структурная единица данных. Поименованное множество атрибутов может образовывать агрегат данных. В некоторых случаях отдельно взятый агрегат может состоять из множества экземпляров однотипных данных, или, как еще говорят, являться множественным элементом. Наконец, записью называют составной агрегат, который не входит в состав других агрегатов.

1. Иерархическая модель данных.

В иерархической модели все записи, агрегаты и атрибуты базы данных образуют иерархически организованный набор, то есть такую структуру, в которой все элементы связаны отношениями подчиненности, и при этом любой элемент может подчиняться только одному какому-нибудь другому элементу. Такую форму зависимости удобно изображать с помощью древовидного графа (схемы, состоящей из точек и стрелок, которая связна и не имеет циклов).Типичным представителем семейства баз данных, основанных на иерархической модели, является Information Management System (IMS) фирмы IBM, первая версия которой появилась в 1968 г.Концепция сетевой модели данных связана с именем Ч. Бахмана. К основным понятиям иерархической структуры относятся уровень, элемент или узел и связь. Узел - это совокупность атрибутов, описывающих некоторый объект. На схеме иерархического дерева узлы представляются вершинами графа. Каждый узел на более низком уровне связан только с одним узлом, находящимся на более высоком уровне. Иерархическое дерево имеет только одну вершину (корень дерева), не подчиненную никакой другой вершине и находящуюся на самом верхнем (первом) уровне. Зависимые (подчиненные) узлы находятся на втором, третьем и так далее уровнях. Количество деревьев в базе данных определяется числом корневых записей.К каждой записи базы данных существует только один (иерархический) путь от корневой записи.В иерархической модели данных автоматически поддерживается целостность ссылок между предками и потомками. Основное правило: никакой потомок не может существовать без своего родителя.2. Сетевая модель данных.Сетевой подход к организации данных является расширением иерархическогоСетевая БД состоит из набора записей и набора связей между этими записями, точнее, из набора экземпляров записей

заданных типов (из допустимого набора типов) и набора экземпляров из заданного набора типов связи. Примером системы управления данными с сетевой организацией является Integrated Database Management System (IDMS) компании Cullinet Software Inc.,

разработанная в середине 70-х годов. Она предназначена для использования на "больших" вычислительных машинах. Архитектура системы основана на предложениях Data Base Task Group (DBTG), Conference on Data Systems Languages (CODASYL), организации, ответственной за определение стандартов языка программирования Кобол.

3. Реляционная модель данных.Концепции реляционной модели впервые были сформулированы в работах американского ученого Э. Ф. Кодда. Для формального определения реляционной модели используется фундаментальное понятие отношения. Собственно говоря, термин "реляционная" происходит от английского relation - отношение. Отношения представлены в виде таблиц, строки которых соответствуют кортежам или записям а столбцы - атрибутам отношений, доменам, полям. Поле, каждое значение которого однозначно определяет соответствующую запись, называется простым ключом. Если записи однозначно определяются значениями нескольких полей, то такая таблица базы данных имеет составной ключ. Чтобы связать две реляционные таблицы, необходимо ключ первой таблицы ввести в состав ключа второй таблицы или ввести в структуру первой таблицы внешний ключ - ключ второй таблицы. Если заданы произвольные конечные множества D1, D2 ,…, Dn, то декартовым произведением этих множеств D1 ? D2 ? … ? Dn называют множество всевозможные наборов вида (d1, d2 ..., dn), где d1 D1, d2 D2,..., dn Dn. Отношением R определенным на множествах D1, D2 ,…, Dn,, называется подмножество декартова произведения Dl x D2x ... x Dn. При этом множества D1 ? D2 ? … ? Dn называются доменами отношения, а элементы декартова произведения - кортежами отношения. Число я определяет степень отношения, а количество кортежей - его мощность. Наряду с понятиями домена и кортежа при работе с реляционными таблицами используются альтернативные им понятия поля и записи. В реляционной базе данных каждая таблица должна иметь первичный ключ (ключевой элемент) - поле или комбинацию полей, которые единственным образом идентифицируют каждую строку в таблице. Важным преимуществом реляционной модели является то, что в ее рамках действия над данными могут быть сведены к операциям реляционной алгебры, которые выполняются над отношениями. Это такие операции, как объединение, пересечение, вычитание, декартово произведение, выборка, проекция, соединение, деление. В реляционной модели данных фиксируются два базовых требования целостности, которые должны поддерживаться в любой реляционной СУБД. Первое требование называется требованием целостности сущностей, которое состоит в том, что любой кортеж любого отношения должен быть отличим от любого другого кортежа этого отношения, то есть любое отношение должно содержать первичный ключ. Второе требование называется требованием целостности по ссылкам и состоит в том, что для

каждого значения внешнего ключа в отношении, на которое ведет ссылка, должен найтись кортеж с таким же значением первичного ключа, либо значение внешнего ключа должно быть неопределенным. Важнейшей проблемой, решаемой при проектировании баз данных, является создание такой их структуры, которая бы обеспечивала минимальное дублирование информации и упрощала Процедуры обработки и обновления данных.

Коддом был предложен некоторый набор формальных требований универсального характера к организации данных, которые позволяют эффективно решать перечисленные задачи. Эти требования к состоянию таблиц данных получили название нормальных форм. Первоначально были сформулированы три нормальные формы. В дальнейшем появилась нормальная форма Бойса-Кодда и нормальные формы более высоких порядков. Однако они не получили широкого распространения на практике.Говорят, что отношение находится во второй нормальной форме, если оно удовлетворяет требованиям первой нормальной формы и каждый не ключевой атрибут функционально полно зависит от ключа (однозначно определяется им).Говорят, что отношение находится в третьей нормальной форме, если оно удовлетворяет требованиям второй нормальной формы и при этом любой не ключевой атрибут зависит от ключа нетранзитивно. Заметим, что транзитивной называется такая зависимость, при которой какой-либо не ключевой атрибут зависит от другого не ключевого атрибута, а тот, в свою очередь, уже зависит от ключа. Принципиальным моментом является то, что для приведения таблиц к состоянию, удовлетворяющему требованиям нормальных форм, или, как еще говорят, для нормализации данных над ними, должны быть осуществлены перечисленные выше операции реляционной алгебры. Основным достоинством реляционной модели является ее простота.

1. 4 Лекция №18-20 (6 часов).

Тема: «Организация и средства защиты информационных процессов в автоматизированных системах**»**

1.4.1 Вопросы лекции:

1. Общая характеристика, информационные технологии и автоматизированные системы

2. Примеры информационных технологий, государственные стандарты на разработку и создание автоматизированных систем

1.4.2 Краткое содержание вопросов:

1. **Информационный ресурс** - это особый вид ресурса, основанного на идеях и

знаниях, накопленных в результате научно-технической деятельности людей и представленный в форме, пригодной для сбора, реализации и воспроизведения.

Информационный ресурс имеет ряд характерных особенностей частности, в отличие от других (материальных) ресурсов, он практически неисчерпаем. С развитием общества и ростом объема используемых знаний этот ресурс не уменьшается, а наоборот, растет. Применение нового информационного ресурса вместо устаревшего потенциально может привести к действиям радикального характера, многократно повысить продуктивность труда, улучшить использование других ресурсов.

Как и любым ресурсом, информационными ресурсами можно управлять. На уровне организации можно и нужно изучать информационные потребности, планировать и управлять информационными ресурсами.

Управление информационными ресурсами означает:

- оценки информационных потребностей на каждом уровне и в пределах каждой функции управления;

- изучения документооборота организации, его рационализацию, стандартизацию типов и форм документов, типизацию информации и данных;

- решения проблемы несовместимости типов данных;

- создание системы управления данными и т.д.

С понятием «информационный ресурс» тесно связано понятие «информационная технология» (технология обработки информации).

Информационная технология - процесс, использующий совокупность методов и средств реализации операций сбора, регистрации, передачи, накопления и обработки информации на базе программно-аппаратного обеспечения для решения управленческих задач экономического объекта.

Информационная технология- это системно-организованная последовательность операций, выполняемых над информацией с использованием средств и методов автоматизации. Операциями являются элементарные действия над информацией.

Процедура передачи информации включает кроме самой передачи операции ввода данных в систему, в сеть, преобразования из цифровой формы в аналоговую и наоборот, операции вывода сообщений, контроль ввода и вывода, защиту данных.

Процедуры обработки информации являются главными в информационных технологиях. Остальные процедуры носят вспомогательный характер.

Цель информационной технологии - производство информации для её анализа человеком и принятия на основе этого анализа решение на выполнение какого-либо действия.

Практическое приложение методов и средств обработки данных может быть различным, поэтому целесообразно выделить глобальную, базовую и конкретную информационные технологии.

Глобальная информационная технология включает модели методы и средства, формализующие и позволяющие использовать информационные ресурсы общества.

Базовая информационная технология предназначена для определенной области применения (производство, научные исследования, обучение и т.д.).

Конкретные информационные технологии реализуют обработку данных при решении функциональных задач пользователей (например, задачи учета, планирования, анализа).

Как и все технологии, информационные технологии находятся в постоянном развитии и совершенствовании. Этому способствуют появление новых технических средств, разработка новых концепции, методов организации данных, их передачи, хранения и обработки и т.д. Существует несколько точек зрения на развитие информационных технологий с использованием компьютеров, которые определяются различными признаками деления. Отсюда можно выделить несколько этапов в развитии информационных технологий:

По признаку - вид задач и процессов обработки информации - выделяются два этапа:

1-й этап (60 - 70-е гг.) - обработка данных в вычислительных центрах в режиме коллективного пользования. Основным направлением развития информационной технологии являлась автоматизация операционных рутинных действий человека.

2-й этап (с 80-х гг.) - создание информационных технологий, направленных на решение стратегических задач.

По признаку - проблемы, стоящие на пути информатизации общества выделяются четыре этапа:

1-й этап (до конца 60-х гг.) характеризуется проблемой обработки больших объемов данных в условиях ограниченных возможностей аппаратных средств.

2-й этап (до конца 70-х гг.) связывается с распространением ЭВМ серии IBM/360. Проблема этого этапа - отставание программного обеспечения от уровня развития аппаратных средств.

3-й этап (с начала 80-х гг.) - компьютер становится инструментом непрофессионального пользователя, а информационные системы - средством поддержки принятия его решений. Проблемы - максимальное удовлетворение потребностей пользователя и создание соответствующего интерфейса работы в компьютерной среде.

4-й этап (с начала 90-х гг.) создание современной технологии межорганизационных связей и информационных систем. Проблемы того этапа весьма многочисленны. Наиболее существенными из них являются: выработка соглашений и установление стандартов, протоколов компьютерной связи; организация доступа к стратегической информации; организация защиты и безопасности информации.

2. Содержание документов является общим для всех видов АС и, при необходимости, может дополняться разработчиком документов в зависимости от особенностей создаваемой АС. Допускается включать в документы дополнительные разделы и сведения, объединять и исключать разделы. Содержание каждого документа определяет разработчик в зависимости от объекта проектирования (система, подсистема и т.д.). Ниже приводится краткий обзор документов.

1. *Пояснительные записки* к эскизному, техническому проектам содержат следующие разделы: общие положения; описание процесса деятельности; основные технические решения; мероприятия по подготовке объекта автоматизации к вводу системы в действие.

В разделе "Общие положения" приводят:

• наименование проектируемой АС и наименования документов, их номера и даты утверждения, на основании которых ведут проектирование АС;

• перечень организаций, участвующих в разработке системы, сроки выполнения стадий;

• цели, назначение и области использования АС;

• подтверждение соответствия проектных решений действующим нормам и правилам техники безопасности, пожаро- и взрывобезопасности и т.п.;

• сведения об использованных при проектировании нормативно-технических документах;

• сведения о НИР, передовом опыте, изобретениях, использованных при разработке проекта;

• очередность создания системы и объем каждой очереди.

Раздел "Описание процесса деятельности" включает пункты, которые:

• отражают состав процедур с учетом обеспечения взаимосвязи и совместимости процессов автоматизированной и неавтоматизированной деятельности;

• формируют требования к организации работ в условиях функционирования АС.

В разделе "Основные технические решения" приводят:

• решения по структуре системы, подсистем, средствам и способам связи для информационного обмена между компонентами системы, подсистем;

• решения по взаимосвязям АС со смежными системами, обеспечению ее совместимости;

• решения по режимам функционирования, диагностированию работы системы;

• решения по численности, квалификации и функциям персонала АС, режимам его работы, порядку взаимодействия;

• сведения об обеспечении заданных в техническом задании (ТЗ) потребительских характеристик системы (подсистем), определяющих ее качество;

• состав функций, комплексов задач, реализуемых системой (подсистемой);

• решения по комплексу технических средств, его размещению на объекте;

• решения по составу информации, объему, способам ее организации, видам машинных носителей, входным и выходным документам и сообщениям, последовательности обработки информации и другим компонентам;

• решения по составу программных средств, языкам деятельности, алгоритмам процедур и операций и методам их реализации.

В разделе "Мероприятия по подготовке объекта автоматизации к вводу системы в действие" приводят:

• мероприятия по приведению информации к виду, пригодному для обработки на ЭВМ;

• мероприятия по обучению и проверке квалификации персонала;

• мероприятия по созданию необходимых подразделений и рабочих мест;

• мероприятия по изменению объекта автоматизации;

• другие мероприятия, исходящие из специфических особенностей создаваемых АС.

2. *Схема функциональной структуры*содержит:

• элементы функциональной структуры АС (подсистемы АС), автоматизированные функции и/или задачи (комплексы задач); совокупности действий (операций), выполняемых при реализации автоматизированных функций только техническими средствами (автоматически) или только человеком;

• информационные связи между элементами и с внешней средой с кратким указанием содержания сообщений и/или сигналов;

• детализированные схемы частей функциональной структуры (при необходимости).

3. *Описание автоматизируемых функций*содержит разделы: исходные данные; цели АС и автоматизированные функции; характеристика функциональной структуры; типовые решения (при наличии).

В разделе "Исходные данные" приводят:

• перечень исходных материалов и документов, использованных при разработке функциональной части проекта АС;

• особенности объекта управления, влияющие на проектные решения по автоматизированным функциям;

• данные о системах управления, взаимосвязанных с разрабатываемой АС, и сведения об информации, которой она должна обмениваться с абонентами и другими системами;

• описание информационной модели объекта вместе с его системой управления.

В разделе "Цели АС и автоматизированные функции" приводят описание автоматизированных функций, направленных на достижение установленных целей.

Раздел "Характеристика функциональной структуры" содержит:

• перечень подсистем АС с указанием функций и/или задач, реализуемых в каждой подсистеме;

• описание процесса выполнения функций (при необходимости);

• необходимые пояснения к разделению автоматизированных функций на действия (операции), выполняемые техническими средствами и человеком;

• требования к временному регламенту и характеристикам процесса реализации автоматизированных функций (точности, надежности и т.п.) и решения задач.

В разделе "Типовые решения" приводят перечень типовых решений с указанием функций, задач, комплексов задач, для выполнения которых они применены.

4. *Описание постановки задачи*(комплекса задач) содержит разделы: характеристики комплекса задач; выходная информация; входная информация.

В разделе "Характеристики комплекса задач" приводят:

• назначение комплекса задач;

• перечень объектов (технологических объектов управления, подразделений предприятия и т. п.), при управлении которыми решают комплекс задач;

• периодичность и продолжительность решения;

• условия, при которых прекращается решение комплекса задач автоматизированным способом (при необходимости);

• связи данного комплекса задач с другими комплексами (задачами) АС;

• должности лиц и/или наименования подразделений, определяющих условия и временные характеристики конкретного решения задачи (если они не определены общим алгоритмом функционирования системы);

• распределение действий между персоналом и техническими средствами при различных ситуациях решения комплекса задач.

Раздел "Выходная информация" содержит:

• перечень и описание выходных сообщений;

• перечень и описание имеющих самостоятельное смысловое значение структурных единиц информации выходных сообщений (показателей, реквизитов и их совокупностей, сигналов управления) или ссылку на документы, содержащие эти данные.

В описании по каждому выходному сообщению следует указывать:

• идентификатор;

• форму представления сообщения (документ, видеокадр, сигнал управления) и требования к ней;

• периодичность выдачи;

• сроки выдачи и допустимое время задержки решения;

• получателей и назначение выходной информации.

В описании по каждой структурной единице информации следует указывать:

• наименование;

• идентификатор выходного сообщения, содержащего структурную единицу информации;

• требования к точности и надежности вычисления (при необходимости).

Раздел "Входная информация" должен содержать:

• перечень и описание входных сообщений (идентификатор, форму представления, сроки и частоту поступления);

• перечень и описание структурных единиц информации входных сообщений или ссылку на документы, содержащие эти данные.

В описании по каждой структурной единице информации входных сообщений следует указывать:

• наименование;

• требуемую точность ее числового значения (при необходимости);

• источник информации (документ, видеокадр, устройство, кодограмма, информационная база на машинных носителях и т. д.);

• идентификатор источника информации.

5. *Общее описание системы*содержит разделы: назначение системы: описание системы; описание взаимосвязей АС с другими системами; описание подсистем (при необходимости).

В разделе "Назначение системы" указывают:

• вид деятельности, для автоматизации которой предназначена система;

1. 5 Лекция №21-22 (4 часа).

Тема: «Обеспечение доступности, целостности и конфиденциальности в автоматизированных системах и базах данных**»**

1.5.1 Вопросы лекции:

1. Различные нотации ER-моделей.

2. Метод IDEF1.X.

1.5.2 Краткое содержание вопросов:

1.

Сущность (Entity) — множество экземпляров реальных или абстрактных объектов (людей, событий, состояний, идей, предметов и др.), обладающих общими атрибутами или характеристиками. Любой объект системы может быть представлен только одной сущностью, которая должна быть уникально идентифицирована. При этом имя сущности должно отражать тип или класс объекта, а не его конкретный экземпляр (например, АЭРОПОРТ, а не ВНУКОВО).

Каждая сущность должна обладать уникальным идентификатором. Каждый экземпляр сущности должен однозначно идентифицироваться и отличаться от всех других экземпляров данного типа сущности. Каждая сущность должна обладать некоторыми свойствами:

- иметь уникальное имя; к одному и тому же имени должна всегда применяться одна и та же интерпретация; одна и та же интерпретация не может применяться к различным именам, если только они не являются псевдонимами;
- иметь один или несколько атрибутов, которые либо принадлежат сущности, либо наследуются через связь;
- иметь один или несколько атрибутов, которые однозначно идентифицируют каждый экземпляр сущности.

Каждая сущность может обладать любым количеством связей с другими сущностями модели.

Связь (Relationship) — поименованная ассоциация между двумя сущностями, значимая для рассматриваемой предметной области. Связь — это ассоциация между сущностями, при которой каждый экземпляр одной сущности ассоциирован с произвольным (в том числе нулевым) количеством экземпляров второй сущности, и наоборот.

Атрибут (Attribute) — любая характеристика сущности, значимая для рассматриваемой предметной области и предназначенная для квалификации, идентификации, классификации, количественной характеристики или выражения состояния сущности. Атрибут представляет тип характеристик или свойств, ассоциированных с множеством реальных или абстрактных объектов (людей, мест, событий, состояний, идей, предметов и т.д.). Экземпляр атрибута — это определенная характеристика отдельного элемента множества. Экземпляр атрибута определяется типом характеристики и ее значением, называемым значением атрибута. На диаграмме "сущность-связь" атрибуты ассоциируются с конкретными сущностями. Таким образом, экземпляр сущности должен обладать единственным определенным значением для ассоциированного атрибута.

2.

Наиболее распространенными методами для построения ERD-диаграмм являются метод Баркера и метод IDEFI.

Метод Баркера основан на нотации, предложенной автором, и используется в case-средстве Oracle Designer.

Метод IDEFI основан на подходе Чена и позволяет построить модель данных, эквивалентную реляционной модели в третьей нормальной форме. На основе совершенствования метода IDEFI создана его новая версия — метод IDEFIX, разработанный с учетом таких требований, как простота для изучения и возможность автоматизации. IDEFIX-диаграммы используются в ряде распространенных CASE-средств (в частности, ERwin, Design/IDEF).

В методе IDEFIX сущность является независимой от идентификаторов или просто независимой, если каждый экземпляр сущности может быть однозначно идентифицирован без определения его отношений с другими сущностями. Сущность называется зависимой от идентификаторов или просто зависимой, если однозначная идентификация экземпляра сущности зависит от его отношения к другой сущности (рис. 10.1, 10.2).

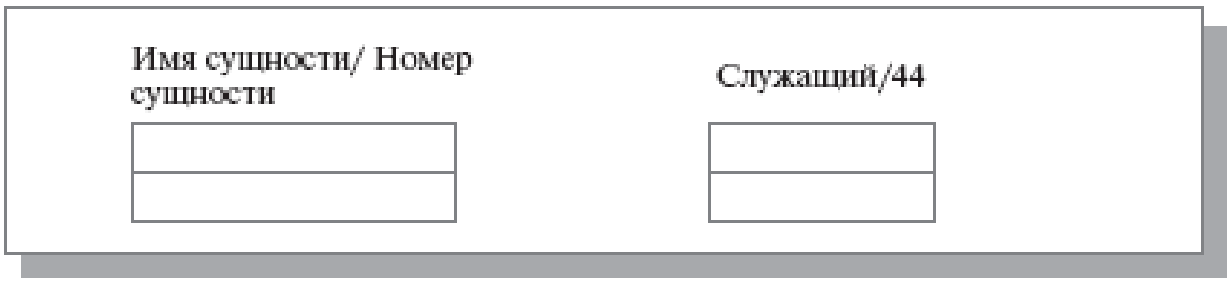


Рис. 10.1. Независимые от идентификации сущности

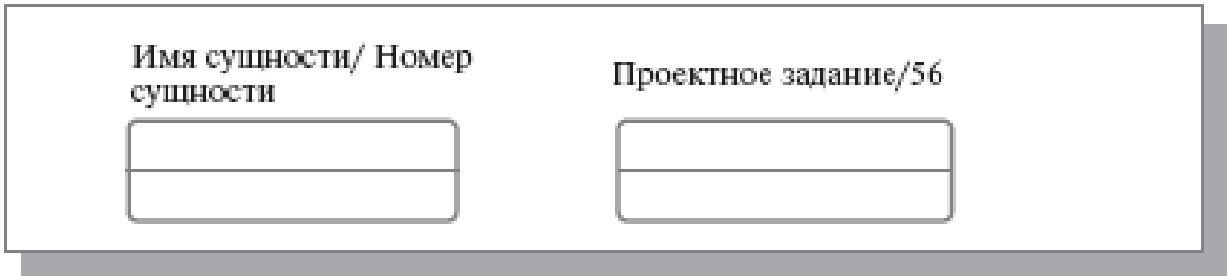


Рис. 10.2. Зависимые от идентификации сущности

Каждой сущности присваиваются уникальные имя и номер, разделяемые косой чертой "/" и помещаемые над блоком.

Связь может дополнительно определяться с помощью указания степени или мощности (количества экземпляров сущности-потомка, которое может порождать каждый экземпляр сущности-родителя). В IDEFIX могут быть выражены следующие мощности связей:

- каждый экземпляр сущности-родителя может иметь ноль, один или более одного связанного с ним экземпляра сущности-потомка;
- каждый экземпляр сущности-родителя должен иметь не менее одного связанного с ним экземпляра сущности-потомка;
- каждый экземпляр сущности-родителя должен иметь не более одного связанного с ним экземпляра сущности-потомка;
- каждый экземпляр сущности-родителя связан с некоторым фиксированным числом экземпляров сущности-потомка.

Если экземпляр сущности-потомка однозначно определяется своей связью с сущностью-родителем, то связь называется идентифицирующей, в противном случае — неидентифицирующей.

Связь изображается линией, проводимой между сущностью-родителем и сущностью-потомком, с точкой на конце линии у сущности-потомка (рис. 10.3). Мощность связей может принимать следующие значения: N — ноль, один или более, Z —

ноль или один, P — один или более. По умолчанию мощность связей принимается равной N.

Рис. 10.3. Графическое изображение мощности связи

Идентифицирующая связь между сущностью-родителем и сущностью-потомком изображается сплошной линией. Сущность-потомок в идентифицирующей связи является зависимой от идентификатора сущностью. Сущность-родитель в идентифицирующей связи может быть как независимой, так и зависимой от идентификатора сущностью (это определяется ее связями с другими сущностями).

Пунктирная линия изображает неидентифицирующую связь (рис. 10.4). Сущность-потомок в неидентифицирующей связи будет не зависимой от идентификатора, если она не является также сущностью-потомком в какой-либо идентифицирующей связи.

Атрибуты изображаются в виде списка имен внутри блока сущности. Атрибуты, определяющие первичный ключ, размещаются наверху списка и отделяются от других атрибутов горизонтальной чертой (рис. 10.4).

Сущности могут иметь также внешние ключи (Foreign Key), которые могут использоваться в качестве части или целого первичного ключа или неключевого атрибута. Для обозначения внешнего ключа внутрь блока сущности помещают имена атрибутов, после которых следуют буквы FK в скобках (рис. 10.4).

Рис. 10.4. Неидентифицирующая связь

1. 6 Лекция №23-24 (4 часа).

Тема: «Защита информации базы данных средствами СУБД**»**

1.6.1 Вопросы лекции:

1. Основные определения и понятия безопасности информационных систем и баз данных.

2. Основные определения и понятия безопасности информационных систем и баз данных.

1.6.2 Краткое содержание вопросов:

1. **О**сновной формой организации информационных массивов в ИС являются базы данных. Базу данных можно определить как совокупность взаимосвязанных хранящихся вместе данных при наличии такой минимальной избыточности, которая допускает их использование оптимальным образом для одного или нескольких приложений. В отличие от файловой системы организации и использования информации , БД существует независимо от конкретной программы и предназначена для совместного использования многими пользователями. Такая централизация и независимость данных в технологии БД потребовали создания соответствующих СУБД - сложных комплексов программ, которые обеспечивают выполнение операций корректного размещения данных, надежного их хранения, поиска, модификации и удаления.

Основные требования по безопасности данных, предъявляемые к БД и СУБД, во многом совпадают с требованиями, предъявляемыми к безопасности данных в компьютерных системах – контроль доступа, криптозащита, проверка целостности, протоколирование и т.д.

Под управлением целостностью в БД понимается защита данных в БД от неверных (в отличие от несанкционированных) изменений и разрушений . Поддержание целостности БД состоит в том, чтобы обеспечить в каждый момент времени корректность (правильность) как самих значений всех элементов данных, так и взаимосвязей между элементами данных в БД . С поддержанием целостности связаны следующие основные требования.

1.Обеспечение достоверности. В каждый элемент данных информация заносится точно в соответствии с описанием этого элемента .Должны быть предусмотрены механизмы обеспечения устойчивости элементов данных и их логических взаимосвязей к ошибкам или неквалифицированным действиям пользователей.

2.Управление параллелизмом. Нарушение целостности БД может возникнуть при

одновременном выполнении операций над данными, каждая из которых в отдельности не нарушает целостности БД . Поэтому должны быть предусмотрены механизмы управления данными, обеспечивающие поддержание целостности БД при одновременном выполнении нескольких операций.

3.Восстановление. Хранимые в БД данные должны быть устойчивы по отношению к неблагоприятным физическим воздействиям (аппаратные ошибки, сбои питания и т .п .) и ошибкам в программном обеспечении . Поэтому должны быть предусмотрены механизмы восстановления за предельно короткое время того состояния БД, которое было перед появлением неисправности.**В**опросы управления доступом и поддержания целостности БД тесно соприкасаются между собой, и во многих случаях для их решения используются одни и те же механизмы. Различие между этими аспектами обеспечения безопасности данных в БД состоит в том, что управление доступом связано с предотвращением преднамеренного разрушения БД, а управление целостностью - с предотвращением непреднамеренного внесения ошибки.

2.

В системе SQL-сервер организована двухуровневая настройка ограничения доступа к данным. На первом уровне в системе необходимо создать так называемую учетную запись пользователя, что позволяет ему подключиться к самому серверу. С другой стороны, на втором уровне для каждой базы данных SQL-сервера на основании учетной записи необходимо создать запись пользователя. Иначе говоря, с помощью учетных записей пользователей осуществляется подключение к SQL-серверу, после чего определяются уровни доступа этого пользователя для каждой базы данных в отдельности. Настройка доступа уже зарегистрированного (с созданной учетной записью) пользователя к объектам базы данных называется настройкой записи пользователя.

При этом в системе SQL-сервер существуют дополнительные объекты - роли, которые определяют уровень доступа к объектам SQL-сервера. В данном случае роли также подразделяются на роли (Server Roles), назначаемые для учетных записей пользователя сервера, и роли, используемые для ограничения доступа к объектам базы данных (Roles), т.е. роли для записей пользователей базы данных. Например, к серверной роли относится security-admin, назначение которой разрешает пользователю добавлять и изменять учетные записи других пользователей. С другой стороны, назначение роли db_backupoperator разрешает пользователю осуществлять процедуру резервного копирования базы данных, в которой ему определена эта рать. В этом случае роль securityadmin относится к группе серверных ролей, а db_backupoperator - к группе ролей

базы данных.

1. 7 Лекция №25-26 (4 часа)

Тема: «Стандарты по защите баз данных**»**

1.7.1 Вопросы лекции:

1. Проектирование модели.
2. Создание базы данных

1.7.2 Краткое содержание вопросов:

1.

Концептуальное (инфологическое) проектирование — построение семантической модели предметной области, то есть информационной модели наиболее высокого уровня абстракции. Такая модель создаётся без ориентации на какую-либо конкретную СУБД и модель данных. Термины «семантическая модель», «концептуальная модель» и «инфологическая модель» являются синонимами. Кроме того, в этом контексте равноправно могут использоваться слова «модель базы данных» и «модель предметной области» (например, «концептуальная модель базы данных» и «концептуальная модель предметной области»), поскольку такая модель является как образом реальности, так и образом проектируемой базы данных для этой реальности.

Конкретный вид и содержание концептуальной модели базы данных определяется выбранным для этого формальным аппаратом. Обычно используются графические нотации, подобные ER-диаграммам.

Чаще всего концептуальная модель базы данных включает в себя:

- описание информационных объектов или понятий предметной области и связей между ними.
- описание ограничений целостности, т.е. требований к допустимым значениям данных и к связям между ними.

Логическое (даталогическое) проектирование — создание схемы базы данных на основе конкретной модели данных, например, реляционной модели данных. Для реляционной модели данных даталогическая модель — набор схем отношений, обычно с указанием первичных ключей, а также «связей» между отношениями, представляющих собой внешние ключи.

Преобразование концептуальной модели в логическую модель, как правило, осуществляется по формальным правилам. Этот этап может быть в значительной степени автоматизирован.

На этапе логического проектирования учитывается специфика конкретной модели данных, но может не учитываться специфика конкретной СУБД.

Физическое проектирование — создание схемы базы данных для конкретной СУБД. Специфика конкретной СУБД может включать в себя ограничения на именование объектов базы данных, ограничения на поддерживаемые типы данных и т.п. Кроме того, специфика конкретной СУБД при физическом проектировании включает выбор решений, связанных с физической средой хранения данных (выбор методов управления дисковой памятью, разделение БД по файлам и устройствам, методов доступа к данным), создание индексов и т.д.

2.

Создание новой базы данных с помощью Конструктора

После запуска Access в режиме «создания Новой база данных» в предложенном диалоговом окне задать имя для файла БД. После этого на экране появляется окно базы данных (рисунок 6.2), из которого можно получить доступ ко всем ее объектам: таблицам, запросам, отчетам, формам, макросам, модулям.

Для создания новой таблицы нужно перейти на вкладку Таблица и нажать кнопку Создать. В следующем окне следует выбрать способ создания таблицы - Конструктор.

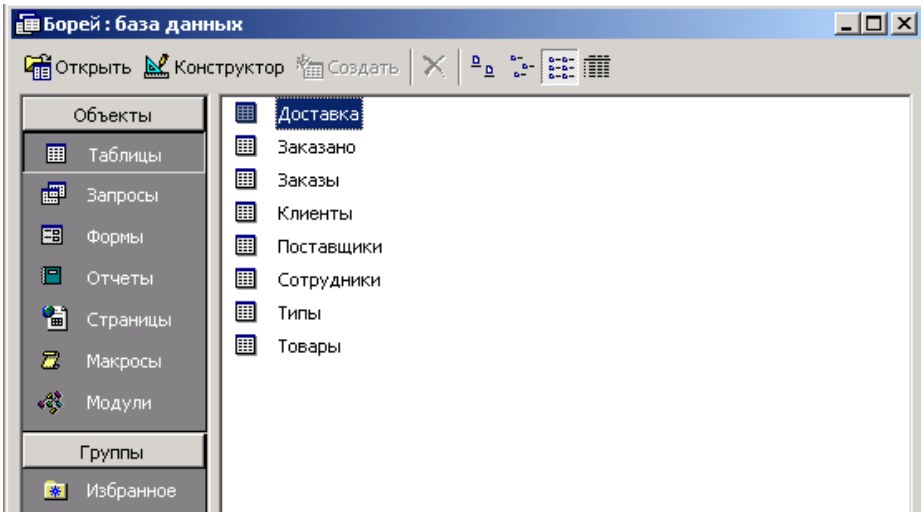


Рисунок 6.2 - Окно базы данных (фрагмент)

После этого Access выводит окно Конструктора таблицы (рисунок 6.3), в котором задаются имена, типы и свойства полей для создаваемой таблицы.

Каждая строка в столбце Тип данных является полем со списком, элементами которого являются типы данных Access. Тип поля определяется характером вводимых в него данных.

Среди типов данных Access есть специальный тип - Счетчик. В поле этого типа Access автоматически нумерует строки таблицы в возрастающей последовательности. Редактировать значения такого поля нельзя.

Каждое поле обладает индивидуальными свойствами, по которым можно установить, как должны сохраняться, отображаться и обрабатываться данные. Набор свойств поля зависит от выбранного типа данных. Для определения свойств поля используется бланк Свойства поля в нижней части окна конструктора таблиц.

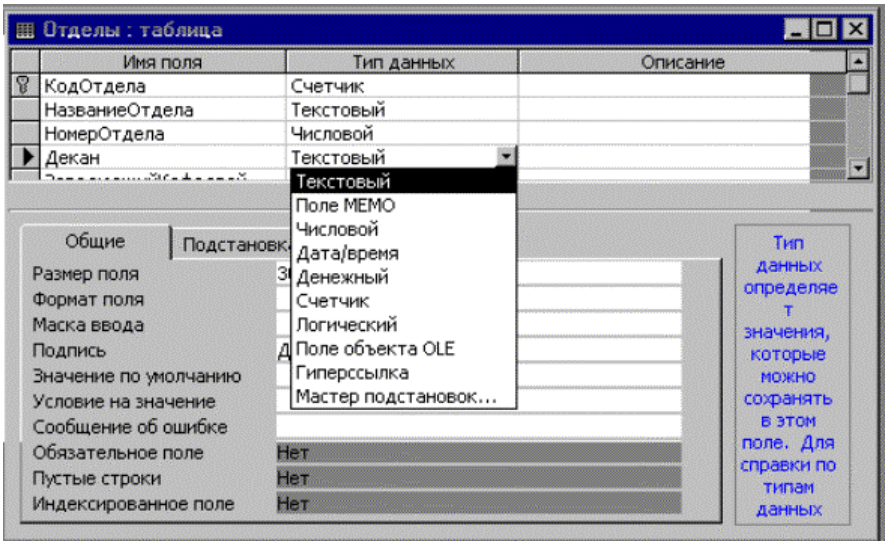


Рисунок 6.3 - Окно Конструктора таблицы

Размер поля - определяется только для текстовых и Memo-полей. Размер поля указывает максимальное количество символов в данном поле. По умолчанию длина текстового поля составляет 50 символов.

Формат поля – определяется для полей числового, денежного типа, полей типа Счетчик и Дата\Время. Выбирается один из форматов представления данных.

Число десятичных знаков - определяет количество разрядов в дробной части числа.

Маска ввода - определяет шаблон для ввода данных. Например, можно установить разделители при вводе телефонного номера.

Подпись поля - содержит надпись, которая может быть выведена рядом с полем в форме или отчете (данная надпись может и не совпадать с именем поля, а также может содержать поясняющие сведения).

Значение по умолчанию - содержит значение, устанавливаемое по умолчанию в данном поле таблицы. Например, если в поле Город ввести значение по умолчанию - Уфа, то при вводе записей о проживающих в Уфе это поле можно пропускать, а соответствующее значение (Уфа) будет введено автоматически. Это облегчает ввод

значений, повторяющихся чаще других.

Условие на значение - определяет множество значений, которые пользователь может вводить в это поле при заполнении таблицы. Это свойство позволяет избежать ввода недопустимых в данном поле значений. Например, если стипендия студента не может превышать 250 рублей, то для этого поля можно задать условие на значение: <=250.

Сообщение об ошибке - определяет сообщение, которое появляется на экране в случае ввода недопустимого значения.

Обязательное поле - установка, указывающая на то, что данное поле требует обязательного заполнения для каждой записи. Например, поле Домашний телефон может быть пустым для некоторых записей (значение Нет в данном свойстве), а поле Фамилия не может быть пустым ни для одной записи (значение Да).

Пустые строки - установка, которая определяет, допускается ли ввод в данное поле пустых строк (“ “).

Индексированное поле - определяет простые индексы для ускорения поиска записей.

Для сохранения структуры таблицы нужно ввести команду Файл\Сохранить и в окне Сохранение ввести имя таблицы.

Кроме вышеперечисленных типов данных в списке есть элемент Мастер подстановок, который позволяет представить значения полей в виде простого или комбинированного списка. Дополнительные свойства такого поля представлены на вкладке Подстановка окна конструктора таблиц.

2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

2.1 Лабораторная работа №1-3 (6 часов).

Тема: «Основы информационной безопасности автоматизированных систем. Характеристика автоматизированных систем и информационных процессов**»**

2.1.1 Цель работы: Познакомится с различными видами защиты информации в пэвм.

2.1.2 Задание для работы:

1. Виды информации в ПЭВМ.
2. Методы защиты информации в ПЭВМ.

2.1.3 Перечень приборов, материалов, используемых в лабораторной работе:

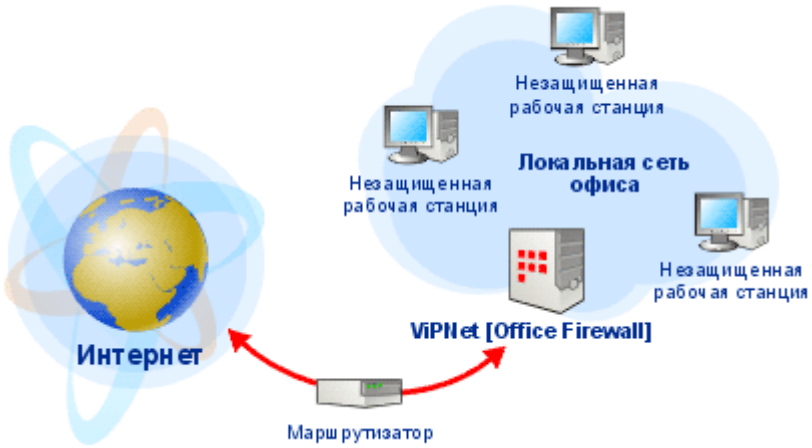
1.Персональный компьютер с установленным специальным ПО.
2. Мультимедийное оборудование

2.1.4 Описание (ход) работы:

1. Теоретические сведения.

Межсетевые экраны (firewall) - это средство, которое разграничивает доступ между

двумя сетями (или, в частном случае, узлами) с различными требованиями по обеспечению безопасности. В самом распространенном случае межсетевой экран устанавливается между корпоративной сетью и Internet.



Межсетевой экран, защищающий сразу множество (не менее двух) узлов, призван решить две задачи, каждая из которых по-своему важна и в зависимости от организации, использующей межсетевой экран, имеет более высокий приоритет по сравнению с другой:

- Ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающие получить доступ к серверам баз данных, защищаемых межсетевым экраном.
- Разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требуемым для выполнения служебных обязанностей.

2. Подготовка к работе.

4.1. Изучить теоретические сведения (п. 2).
4.2. Включить ПК, открыть файл с документацией *VIPNET OFFICE FIREWALL*

3. Программа работы.

5.1. Изучить назначение, основные возможности, систему окон и меню ПО *VIPNET OFFICE FIREWALL*
5.2. Изучить главы 8 – 11 документации

4.Контрольные вопросы

6.1. Что представляет собой внешний интерфейс?
6.2. Что представляет собой внутренний интерфейс?
6.3. Что представляют собой режимы безопасности интерфейса?
6.4. Что такое антиспуфинг?
6.5. В чем заключаются функции режима «Бумеранг»?
6.6. В чем заключаются правила фильтрации IP-трафика?
6.7. Чем отличаются между собой режимы жесткого и мягкого бумеранга?
6.8. Чем отличаются между собой режимы «1» и «5» безопасности интерфейса?
6.9. Какова структура сетевого фильтра?
6.10. В чем заключаются достоинства системы обнаружения атак?
6.11. Для чего нужна трансляция сетевых адресов (NAT)?
6.12. В чем заключаются следующие виды атак: атака Land, атака Jolt2, атака Smurf?

2.2 Лабораторная работа №4-6 (6 часов).

Тема: «Угрозы безопасности автоматизированных систем**»**

2.2.1 Цель работы: Познакомится с различными видами мероприятий по защите информации.

2.2.2 Задание для работы:

1. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания
2. Защита программ и данных от несанкционированного копирования

2.2.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.2.4 Описание (ход) работы:

1. Теоретические сведения.

Благодаря своей открытой архитектуре сеть Internet стала одним из самых удобных средств коммуникации. Вместе с тем открытость Internet породила множество проблем, связанных с безопасностью. Здесь как нельзя лучше подходит изречение: «Каждый — за себя, только Бог — за всех». Любой имеющий выход в Internet компьютер должен рассматриваться как потенциальный объект для атаки. Проблема особенно остро стоит в случае организаций, поскольку им необходимо контролировать работу в Internet большого количества компьютеров и сетевых устройств.

Безопасность при подключении к Internet обеспечивается с помощью следующих специализированных средств:

межсетевых экранов;

сетевых сканеров, призванных находить изъяны и потенциально опасные участки внутри сетей;

снифферов, или анализаторов протоколов, позволяющих отслеживать входящий и исходящий трафики;

средств протоколирования событий в сетях;

средств построения виртуальных частных сетей и организации закрытых каналов обмена данными.

Важное место в списке средств обеспечения безопасного подключения к Internet занимают межсетевые экраны (часто называемые брандмауэрами, или, по-английски, firewall). Согласно «Руководящему документу. Межсетевые экраны» Гостехкомиссии при Президенте РФ «межсетевым экраном называется локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т. е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе». К сожалению, такое определение имеет чересчур общий характер и подразумевает слишком расширенное толкование.

В обиходе межсетевыми экранами (МЭ) называют средства защиты, устанавливаемые между общедоступной (такой, как Internet) и внутренней сетью. Межсетевой экран выполняет двойную функцию. Во-первых, он призван ограничить доступ во внутреннюю сеть со стороны общедоступной сети за счет применения фильтров и средств аутентификации, чтобы злоумышленники не могли получить несанкционированный доступ к информации или нарушить нормальную работу сетевой инфраструктуры. Во-вторых, МЭ служит для контроля и регулирования доступа пользователей внутренней сети к ресурсам общедоступной сети, когда те представляют угрозу безопасности или отвлекают сотрудников от работы (порнографические, игровые, спортивные серверы).

Сейчас, правда, сетевые экраны устанавливают и внутри корпоративных сетей, в

целях ограничения доступа пользователей к особо важным ресурсам сети, например к серверам, содержащим финансовую информацию или сведения, относящиеся к коммерческой тайне. Существуют также персональные межсетевые экраны, призванные регулировать доступ к отдельным компьютерам и устанавливаемые на эти компьютеры.

Межсетевые экраны по понятным причинам используются для сетей TCP/IP и классифицируются в соответствии с уровнем эталонной модели взаимодействия открытых систем (сетевой моделью) OSI. Однако такая классификация, в силу ряда обстоятельств носит достаточно условный характер. Во-первых, сетевая модель сетей TCP/IP предусматривает только 5 уровней (физический, интерфейсный, сетевой, транспортный и прикладной), в то время как модель OSI — 7 уровней (физический, канальный, сетевой, транспортный, сеансовый, презентационный и прикладной). Поэтому установить однозначное соответствие между этими моделями далеко не всегда возможно. Во-вторых, большинство выпускаемых межсетевых экранов обеспечивают работу сразу на нескольких уровнях иерархии OSI. В-третьих, некоторые экраны функционируют в режиме, который трудно соотнести с каким-то строго определенным уровнем иерархии.

Тем не менее поддерживаемый уровень сетевой модели OSI является основной характеристикой при классификации межсетевых экранов. Различают следующие типы межсетевых экранов:

- управляемые коммутаторы (канальный уровень);
- сетевые фильтры (сетевой уровень);
- шлюзы сеансового уровня (circuit-level proxy);
- посредники прикладного уровня;
- инспекторы состояния (stateful inspection), представляющие собой межсетевые экраны сеансового уровня с расширенными возможностями.

Существует также понятие «межсетевой экран экспертного уровня». Такие МЭ обычно базируются на посредниках прикладного уровня или инспекторах состояния, но обязательно комплектуются шлюзами сеансового уровня и сетевыми фильтрами. К МЭ экспертного класса относятся почти все имеющиеся на рынке коммерческие брандмауэры.

Межсетевые экраны могут опираться на один из двух взаимоисключающих принципов обработки поступающих пакетов данных. Первый принцип гласит: «Что явно не запрещено, то разрешено». Т. е. если МЭ получил пакет, не подпадающий не под одно из принятых ограничений или не идентифицированный правилами обработки, то он передается далее. Противоположный принцип — «Что явно не разрешено, то запрещено» — гарантирует гораздо большую защищенность, но оборачивается дополнительной нагрузкой на администратора. В этом случае внутренняя сеть изначально полностью недоступна, и администратор вручную устанавливает разрешенные при обмене данными с общедоступной сетью сетевые адреса, протоколы, службы и операции.

Правила обработки информации во многих межсетевых экранах экспертного класса могут иметь многоуровневую иерархическую структуру. Например, они могут позволять задать такую схему: «Все компьютеры локальной сети недоступны извне, за исключением доступа к серверу A по протоколу ftp и к серверу B по протоколу telnet, однако при этом запрещен доступ к серверу A с операцией PUT сервиса ftp».

Межсетевые экраны могут выполнять над поступающими пакетами данных одну из двух операций: пропустить пакет далее (allow) или отбросить пакет (deny). Некоторые МЭ имеют еще одну операцию — reject, при которой пакет отбрасывается, но отправителю сообщается по протоколу ICMP о недоступности сервиса на компьютере-получателе информации. В противовес этому при операции deny отправитель не информируется о недоступности сервиса, что является более безопасным.

2. Подготовка к работе.

4.1. Изучить теоретические сведения (п. 2).

4.2. Включить ПК, открыть файл с документацией *VIPNET PERSONAL FIREWALL*

3. Программа работы.

5.1. Изучить назначение, основные режимы использования, систему окон и меню ПО *VIPNET PERSONAL FIREWALL*

5.2. Изучить главы 8 – 11 документации

4. Контрольные вопросы

6.1. Чем отличаются между собой МЭ *VIPNET OFFICE FIREWALL* и МЭ *VIPNET PERSONAL FIREWALL*?

6.2. Чем отличаются между собой режимы «3» и «4» безопасности интерфейса?

6.3. Какова структура настроек фильтра МЭ *VIPNET PERSONAL FIREWALL*?

6.4. В чем заключаются функции системы обнаружения атак?

6.5. В чем заключаются следующие виды *событий* системы обнаружения вторжений: IP-опции нулевой длины, ICMP-запрос маски подсети, фрагментация ICMP-заголовка?

2.3 Лабораторная работа №7-8 (4 часа).

Тема: «Основы информационной безопасности автоматизированных систем. Характеристика автоматизированных систем и информационных процессов**»**

2.3.1 Цель работы: Познакомится с различными современными системами защиты пэвм от несанкционированного доступа к информации.

2.3.2 Задание для работы:

1. Системы защиты ПЭВМ.
2. Несанкционированный доступ к информации.

2.3.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.3.4 Описание (ход) работы:

1. Теоретические сведения.

Системы построения VPN

Из пункта А в пункт Б необходимо передать информацию таким образом, чтобы к ней никто не смог получить доступ. Вполне реальная и часто возникающая на практике ситуация, особенно в последнее время. В качестве пунктов А и Б могут выступать отдельные узлы или целые сегменты сетей. В случае с передачей информации между сетями в качестве защитной меры может выступать выделенный канал связи, принадлежащей компании, информация которой требует защиты. Однако поддержание таких каналов связи - это очень дорогое удовольствие. Проще, если информация будет передаваться по обычным каналам связи (например, через Internet), но каким-либо способом будет отделена или скрыта от трафика других компаний, циркулирующего в Internet. Но не стоит думать, что задача конфиденциальной передачи информации возникает в глобальных сетях. Такая потребность может возникнуть и в локальных сетях, в которых требуется отделать один тип трафика, от другого (например, трафик платежной системы от трафика информационно-аналитической системы). Итак, как сделать так, чтобы информация могла передаваться по тем же проводам, что и обычная информация, но при этом была недоступна для других? Помочь в этом может технология виртуальных частных сетей (virtual private network, VPN).

Классификация

Можно выделить два основных способа реализации VPN:

- Разделение трафика в канале передачи;

- Шифрование трафика в канале передачи.

Разделение трафика в канале передачи.

Первая технология достаточно недавно получила широкое распространение. Она может применяться как в глобальных, так и в локальных сетях. Причем второй случай распространен чаще - это всем известная технология виртуальных локальных сетей (VLAN), используемая для структуризации современных локальных сетей, построенных на базе коммутаторов. Однако помимо структуризации VLAN могут применяться и для отделения одного типа трафика от другого. Т.к. VLAN реализуются на канальном уровне, то их область применения не выходит за рамки локальной сети, но и тут они неплохо справляются со своими задачами. В частности, независимо от адреса канального уровня (уникального, группового или широковещательного) смешение данных из разных VLAN невозможно. В то же время внутри одной VLAN кадры передаются как обычно, только на тот порт, на который указывает адрес назначения кадра.

Узлы, входящие в VLAN могут группироваться на основе различных признаков:

- Группировка по портам. Классический и самый простой способ формирования VLAN, согласно которому каждому порту коммутатора соответствует номер VLAN.

- Группировка по MAC-адресам. Принадлежность к VLAN определяется по MAC-адресам сетевых пакетов.

- Группировка по номерам подсетей сетевого уровня. В данном случае VLAN является аналогом обычной подсетью, которая известна по протоколам IP или IPX.

- Группировка по меткам. Самый эффективный и надежный способ группирования узлов в VLAN, согласно которому номер виртуальной сети добавляется к кадру, передаваемому между коммутаторами.

Существуют и другие способы формирования VLAN, но все они менее распространены, чем вышеназванные. Технология VLAN реализована сейчас в большинстве коммутаторов ведущих сетевых производителей.

В глобальных сетях распространение получил аналог VLAN - технология MPLS (MultiProtocol Label Switching), которая также использует метки для разделения трафика и образования виртуальных каналов в IP-, ATM- и других сетях. Однако у технологии MPLS

есть один недостаток (с точки зрения безопасности) - он может применяться только для связи "сеть - сеть" и не применим для соединения с отдельными узлами. Есть и второй недостаток - данные разных пользователей хоть и не смешиваются, но все-таки к ним можно получить данные, прослушивая сетевой трафик. Кроме того, провайдер, предлагающий услуги MPLS будет иметь доступ ко всей передаваемой информации. Однако данные технологии все же имеют право на существование, т.к. обеспечивают некоторый уровень защищенности информации и достаточно дешевы. Основным поставщиком MPLS является компания Cisco Systems.

Шифрование трафика в канале передачи

Большую известность получила технология шифрования трафика, которая скрывает от глаз содержание данных, передаваемых по открытым сетям. Именно эта технология применяется многими разработчиками средств сетевой безопасности.

Варианты построения

Можно выделить четыре основных варианта построения сети VPN, которые используются во всем мире. Данная классификация предлагается компанией Check Point Software Technologies, которая не без основания считается законодателем моды в области VPN.

1. Вариант «Intranet VPN», который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики.

2. Вариант "Remote Access VPN", который позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямиком со своего собственного компьютера, на котором и устанавливается программное обеспечение, реализующее функции VPN.

Компонент VPN для удаленного пользователя может быть выполнен как в программном, так и в программно-аппаратном виде. В первом случае программное обеспечение может быть как встроенным в операционную систему (например, в Windows 2000), так и разработанным специально. Во втором случае для реализации VPN используются небольшие устройства класса SOHO (Small Office\Home Office), которые не требуют серьезной настройки и могут быть использованы даже неквалифицированным персоналом. Такие устройства получают сейчас широкое распространение за рубежом.

3. Вариант «Client/Server VPN», который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, описанную выше. Но вместо разделения трафика, используется его шифрование.

4. Последний вариант «Extranet VPN» предназначен для тех сетей, к которым подключаются так называемые пользователи "со стороны" (партнеры, заказчики, клиенты и т.д.), уровень доверия к которым намного ниже, чем к своим сотрудникам. Хотя по статистике чаще всего именно сотрудники являются причиной компьютерных преступлений и злоупотреблений.

Варианты реализации

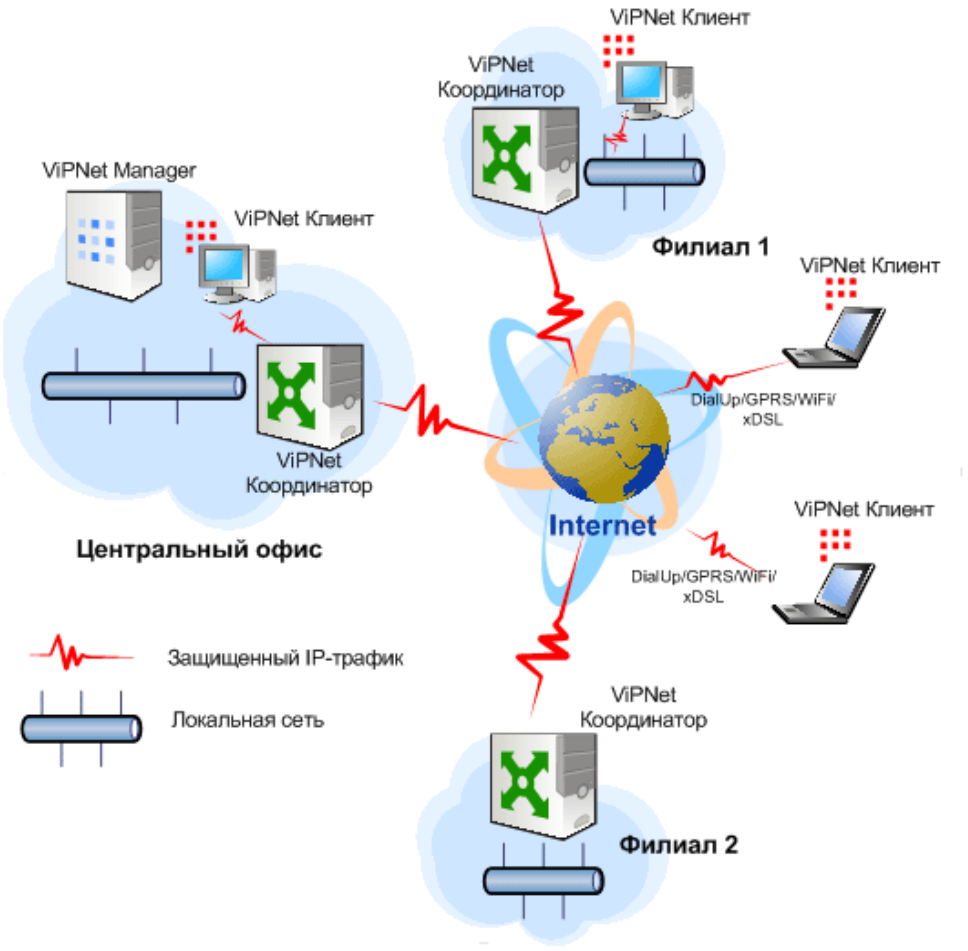
Средства построения VPN могут быть реализованы по-разному:

- В виде специализированного программно-аппаратного обеспечения, предназначенного именно для решения задач VPN. Основное преимущество таких устройств - их высокая производительность и, более высокая по сравнению с другими решениями, защищенность. Такие устройства могут применяться в тех случаях, когда необходимо обеспечить защищенный доступ большого числа абонентов. Недостаток таких решений состоит в том,

что управляются они отдельно от других решений по безопасности, что усложняет задачу администрирования инфраструктуры безопасности, особенно при условии нехватки сотрудников отдела защиты информации. На первое место эта проблема выходит при построении крупной и территориально-распределенной сети, насчитывающей десятки устройств построения VPN. И это не считая такого же числа межсетевых экранов, систем обнаружения атак и т.д. Примером такого решения является Cisco 1720 или Cisco 3000

- В виде программного решения, устанавливаемого на обычный компьютер, функционирующий, как правило, под управлением операционной системы Unix. Российские разработчики «полюбили» ОС FreeBSD. Именно на ее изученной «вдоль и поперек» базе построены отечественные решения «Континент-К» и «Шип». Для ускорения обработки трафика могут быть использованы специальные аппаратные ускорители, заменяющие функции программного шифрования. Также в виде программного решения реализуется абонентские пункты, предназначенные для подключения к защищаемой сети удаленных и мобильных пользователей.

- Интегрированные решения, в которых функции построения VPN реализуются наряду с функцией фильтрации сетевого трафика, обеспечения качества обслуживания или распределения полосы пропускания. Основное



Типовая схема защищенной сети на базе решения ViPNet OFFICE

преимущество такого решения - централизованное управление всеми компонентами с единой консоли. Второе преимущество - более низкая стоимость в расчете на каждый компонент по сравнению с ситуацией, когда такие компоненты приобретаются отдельно. Пожалуй, самым известным примером такого интегрированного решения является VPN-1 от компании Check Point Software, включающий в себя помимо VPN-модуля, модуль, реализующий функции межсетевого экрана, модуль, отвечающий за балансировку

нагрузки, распределение полосы пропускания и т.д. Кроме того, это решение имеет сертификат Гостехкомиссии России.

2. Подготовка к работе.

4.1. Изучить теоретические сведения (п. 2).

4.2. Включить ПК, открыть файл с документацией *VIPNET OFFICE*

3. Программа работы.

5.1. Изучить общие положения гл. 1 документации ПО *VIPNET OFFICE*

5.2. Изучить главу 6 документации.

4. Контрольные вопросы

6.1. Для каких целей используется программное обеспечение *VIPNET OFFICE?*

6.2. Каковы функции ViPNet Manager?

6.3. Каковы функции ViPNet Координатор?

6.4. Каковы функции ViPNet Клиент?

6.5. Какие сервисные функции предоставляет пакет ViPNet OFFICE?

2.4 Лабораторная работа №9-11 (6 часов).

Тема: «Организация и средства защиты информационных процессов в автоматизированных системах**»**

2.4.1 Цель работы: Познакомится с различными методы, затрудняющими считывание скопированной информации

2.4.2 Задание для работы:

1. Считывание информации.
2. Методы считывания информации.

2.4.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.4.4 Описание (ход) работы:

1. Теоретические сведения.

Угроза несанкционированного доступа к информационным ресурсам КС представляется достаточно опасной с точки зрения возможных последствий. Для несанкционированного доступа злоумышленник обычно использует:

- знания о КС и умения работать с ней;
- сведения о системе защиты информации;
- сбои или отказы технических и программных средств;
- ошибки в работе обслуживающего персонала и пользователей.

Часто реализация угрозы НСД не требует постоянного участия в этом процессе злоумышленника, а осуществляется с помощью разработанных им программных средств, которые вводятся в КС в виде соответствующих закладок.

Для защиты информации от НСД создается система разграничения доступа (СРД), контролирующая любые запросы к информационным ресурсам КС со стороны пользователей (или их программ) по установленным для них правилам и видам доступа.

В системе разграничения доступа по отношению к любому субъекту доступа (пользователю, программе, техническому средству) должны быть предусмотрены следующие основные этапы доступа в КС:

- идентификация субъектов и объектов доступа;
- установление подлинности (аутентификация);
-определение полномочий для последующего контроля и разграничения доступа к

компьютерным ресурсам.

2. Подготовка к работе.

4.1. Изучить теоретические сведения (п. 2).

4.2. Включить ПК, открыть файл с документацией **ViPNet DISCguise**

3. Программа работы.

5.1. Изучить общие положения гл. 1 документации ПО **ViPNet DISCguise**

5.2. Изучить главу 4 - 6 документации.

4. Контрольные вопросы

6.1. Для каких целей используется программное обеспечение *ViPNet DISCguise?*

6.2. В чем отличие между ключами recov.pub и recov.sec?

6.3. В чем заключается особенность хранения ключа recov.sec?

6.4. Какие алгоритмы шифрования поддерживаются пакетом *ViPNet DISCguise*?

2.5 Лабораторная работа №12-13 (4 часа).

Тема: «Обеспечение доступности, целостности и конфиденциальности в автоматизированных системах и базах данных»

2.5.1 Цель работы: Познакомится с различными методами, препятствующими использование скопированной информации

2.5.2 Задание для работы:

1. Копирование информации
2. Системы защиты от копирования

2.5.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.
2. Мультимедийное оборудование

2.5.4 Описание (ход) работы:

1. Теоретические сведения.

Как показывает практика, несанкционированный доступ (НСД) представляет одну из наиболее серьезных угроз для злоумышленного завладения защищаемой информацией в современных АСОД. Как ни покажется странным, но для ПЭВМ опасность данной угрозы по сравнению с большими ЭВМ повышается, чему способствуют следующие объективно существующие обстоятельства:

1) подавляющая часть ПЭВМ располагается непосредственно в рабочих комнатах специалистов, что создаст благоприятные условия для доступа к ним посторонних лиц;

2) многие ПЭВМ служат коллективным средством обработки информации, что обезличивает ответственность, в том числе и за защиту информации;

3) современные ПЭВМ оснащены несъемными накопителями на ЖМД очень большой емкости, причем информация на них сохраняется даже в обесточенном состоянии;

4) накопители па ГМД производятся в таком массовом количестве, что уже используются для распространения информации так же, как и бумажные носи гели;

5) первоначально ПЭВМ создавались именно как персональное средство автоматизации обработки информации, а потому и по оснащались специально средствами защиты от НСД.

Основные механизмы защиты ПЭВМ от НСД могут быть представлены следующим перечнем:
1) физическая защита ПЭВМ и носителей информации;
2) опознавание (аутентификация) пользователей и используемых компонентов обработки информации;
3) разграничение доступа к элементам защищаемой информации;
4) криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных);
5) криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки;
6) регистрация всех обращений к защищаемой информации.
Ниже излагаются общее содержание и способы использования перечисленных механизмов.

2. Подготовка к работе.

4.1. Изучить теоретические сведения (п. 2).
4.2. Включить ПК, открыть файл с документацией ViPNet SafeDisk

3. Программа работы.

5.1. Изучить общие положения гл. 1 документации ПО ViPNet SafeDisk
5.2. Изучить главу 4 - 14 документации.

4. Контрольные вопросы

6.1. Для каких целей используется программное обеспечение ViPNet SafeDisk?
6.2. В чем заключаются принципы защиты информации ПО ViPNet SafeDisk?
6.3. С какими видами электронных ключей поддерживает работу программное обеспечение ViPNet SafeDisk?
6.4. Какова особенность использования ПО ViPNet SafeDisk в режимах «опасность» и «большая опасность»?
6.5. Какова особенность использования ПО ViPNet SafeDisk в режиме работы под контролем злоумышленников?

2.6 Лабораторная работа №14-15 (4 часа).
Тема: «Защита информации базы данных средствами СУБД**»**

2.6.1 Цель работы: Познакомится с основными функциями средств защиты от копирования.

2.6.2 Задание для работы:

1. Защита от копирования
2. Функции средств защиты

2.6.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.
2. Мультимедийное оборудование

2.6.4 Описание (ход) работы:

1. Теоретические сведения.

Наиболее часто применяемыми методами идентификации и аутентификации пользователей являются методы, основанные на использовании паролей. В простейшем случае пароль представляет собой некоторую последовательность символов, сохраняемую в секрете и предъявляемую при обращении к компьютерной системе. Для ввода пароля, как правило, используется штатная клавиатура КС. В процессе ввода пароль не должен

отображаться на экране монитора. Чтобы пользователь мог ориентироваться в количестве введенных символов, на экран выдаются специальные символы (например звездочки).

Пароль должен запоминаться субъектом доступа. Запись пароля значительно повышает вероятность его компрометации (нарушения конфиденциальности). Легко запоминаемый пароль должен быть в то же время сложным для отгадывания. Не рекомендуется использовать для этой цели имена, фамилии, даты рождения и т.п.

Желательным является наличие в пароле парадоксального сочетания букв, слов, полученного, например, путем набора русских букв пароля на латинском регистре. Другими словами, чем не тривиальнее пароль, тем сложнее он становится для отгадывания. Однако такой пароль труднее запомнить и его приходится записывать на бумаге.

Для того чтобы воспрепятствовать использованию злоумышленником похищенного пароля, в его тексте должны быть мысленно предусмотрены не записываемые на бумаге пробелы или другие символы в начале, внутри, а также в конце основных символов пароля. В этом случае незаконно полученный лист бумаги с основными символами пароля не будет достаточным условием раскрытия пароля в целом.

Вероятность подбора пароля уменьшается также при увеличении его длины и времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля.

Ожидаемое время раскрытия пароля TP можно вычислить по следующей приближенной формуле:

$TP = (A \cdot S \cdot t) / 2$,

где $t = E / R$ – время, необходимое на попытку введения пароля;

R – скорость передачи символов пароля (симв. / мин);

E – число символов в сообщении, передаваемом в систему при попытке получить к ней доступ (включая пароль и служебные символы);

S – длина пароля;

A – число символов в алфавите, из которых составляется пароль (например 26 символов латинского алфавита).

В приведенной формуле учитывается, что злоумышленник имеет возможность непрерывно осуществлять подбор пароля. Например, если A = 26, t = 2c и S = 6 символов, то ожидаемое время раскрытия TP пароля приблизительно равно одному году. Если в данном примере после каждой неудачной попытки ввода пароля предусмотреть временную задержку в 10 с, то ожидаемое время раскрытия пароля увеличится в 5 раз.

Следует также отметить, что на безопасное время раскрытия пароля оказывает существенное влияние длина пароля S (в степенной зависимости). Так, если для трехсимвольного пароля, выбранного из 26-символьного алфавита, время TP составит 3 месяца, то для четырехсимвольного – 65 лет.

2. Подготовка к работе.

4.1. Изучить теоретические сведения (п. 2).

4.2. Включить ПК, открыть файл с документацией ***ViPNet Генератор паролей***

3. Программа работы.

5.1. Изучить общие положения гл. 1 документации ПО ***ViPNet Генератор паролей***

5.2. Изучить главу 4 - 6 документации.

4. Контрольные вопросы

6.1. Для каких целей используется программное обеспечение ViPNet Генератор паролей?

6.2. Приведите пример создания пароля программой ViPNet Генератор паролей на основе какой нибудь фразы.

6.3. Для чего используется вкладка «электронная рулетка»?
6.4. Каковы минимальные требования к ПК для установки на нем программного обеспечения ViPNet Генератор паролей?

2.7 Лабораторная работа №16-17 (4 часа).

Тема: «Стандарты по защите баз данных**»**

2.7.1 Цель работы: Познакомится с различными видами хранения ключей.

2.7.2 Задание для работы:

1. Разновидность хранения ключей
2. Безопасность хранения ключей

2.7.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.
2. Мультимедийное оборудование

2.7.4 Описание (ход) работы:

1. Теоретические сведения.

Сущность разграничения доступа к элементам защищаемой информации заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий, и исключить возможности превышения своих полномочий. В этих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, к программам обработки информации, к полям (областям ЗУ) и к массивам (базам) данных. Само разграничение может осуществляться несколькими способами, а именно:

- 1) по уровням (кольцам) секретности;
- 2) по специальным спискам;
- 3) по так называемым матрицам полномочий;
- 4) по специальным мандатам.

Разграничение доступа по уровням (кольцам) секретности заключается в том, что защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве (каждой базе) содержались данные одного уровня секретности (например, только с грифом "конфиденциально" , или только "секретно", или только "совершенно секретно", иди каким-либо другим). Каждому зарегистрированному пользователю предоставляется вполне определенный уровень допуска (например, "секретно", "совершенно секретно" и т.п.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня и массивам (базам) низших уровней, и запрещается доступ к массивам (базам) более высоких уровней.

Разграничение доступа по специальным спискам заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

Разграничение доступа по матрицам полномочий предполагает формирование двумерной матрицы, по строкам которой содержатся идентификаторы зарегистрированных пользователей, а по столбцам - идентификаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя относительно соответствующего элемента. Например, при размерах элементов матрицы в два бита их содержание может быть следующим: 00 - доступ запрещен, 01 - разрешено только чтение, 10 - разрешена только запись, 11 - разрешены и чтение и запись.

Разграничение доступа по мандатам есть способ разового разрешения на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уникальная метка, после чего доступ к этому

элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владелец элемента.

2. Подготовка к работе.

4.1. Изучить теоретические сведения (п. 2).
4.2. Включить ПК, открыть файл с документацией **DeviceLock.**

3. Программа работы.

5.1. Изучить общие положения гл. 1 документации ПО **DeviceLock.**
5.2. Изучить главу 2 документации.
5.3. Просмотреть видеокурс (кликнуть на **devlock.exe**)
5.4. Просмотреть видеокурс (кликнуть на **portslock.exe**)
5.5. Просмотреть видеокурс (кликнуть на **rtm.exe**)

4. Контрольные вопросы

6.1. Для каких целей используется программное обеспечение **DeviceLock**?
6.2. Каковы функциональные особенности (решаемые задачи) ПО **DeviceLock?**
6.3. Что представляет собой *белый список* USB устройств?
6.4. Какие типы протоколирования аудита поддерживаются программой **DeviceLock**?
6.5. В чем отличие *dlservice.exe* от *dlmanager.exe*?

3. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие №1-6 (12 часов).

Тема: «Основы информационной безопасности автоматизированных систем. Характеристика автоматизированных систем и информационных процессов**»**

3.1.1 Задание для работы:

1. Классификация по значимости
2. Классификация критически важных объектов по видам угроз
3. Классификация критически важных объектов по уровням угроз

3.1.2 Краткое описание проводимого занятия:

1. Классификация по значимости

В основе перечня КВО -перечни, категории или списки важных государственных объектов, особо важных объектов и др., которые подлежат охране и обороне от угроз террористического и военного характера и утверждены либо указами Президента Российской Федерации, либо постановлениями Правительства Российской Федерации. К ним по предложениям федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации или полномочных представителей Президента Российской Федерации в федеральных округах могут быть добавлены перечни объектов, которые не вошли в выше указанные.

Применив к данным перечням, категориям или спискам объектов систему соответствующих критериев вышеуказанные органы исполнительной власти должны дать предложения в проект перечня **критически важных для национальной безопасности объектов инфраструктуры Российской Федерации.**

Объекты федерального уровня:
объекты, в которых размещены аппараты высших органов государственной власти и управления;
объекты, которые могут использоваться террористами или террористическими организациями в целях нарушения государственной безопасности, дестабилизации государственного строя, либо оказания воздействия на принятие решений высшими органами государственной власти для побуждения их к совершению действия в интересах террористов;
объекты, уничтожение или прекращение действия которых, представляет угрозу для национальной (информационной, экономической, военной, внешнеполитической, экологической) безопасности Российской Федерации

2. Классификация критически важных объектов по видам угроз

• **ядерно - опасные** (атомные электростанции, предприятия ядерно--оружейного комплекса);
• **радиационно - опасные** (спецкомбинаты «Радон», места хранения жидких радиоактивных отходов, отработанного ядерного топлива и др.);
• **химически - опасные** (предприятия нефтехимического, металлургического, машиностроительного, радио- и электротехнического и оборонного производства, пищевой промышленности);
• **биологически-опасные** (крупные предприятия по производству, переработке и хранению сельхозпродукции, фармацевтические комплексы и др.);
• **техногенно - опасные** (крупные железнодорожные узлы, морские порты, аэропорты в крупных городах, метрополитены, мосты и тоннели длиной более 500 м, крупные гидротехнические сооружения промышленного и водохозяйственного назначения, объекты топливо — энергетического комплекса, тепловые электростанции и магистральные линии электропередач);
• **пожаро - взрывоопасные** (магистральные газо-, нефте- и продуктопроводы, газокомпрессорные и нефтеперекачивающие станции, а также хранилища сжиженных газов и нефти, крупные предприятия по производству и переработке жидкофазных или твердых взрывоопасных материалов);
• **объекты государственного управления, финансово-кредитной, информационной и телекоммуникационной инфраструктуры -** предприятия и учреждения финансовой системы страны, стационарные и мобильные пункты управления, узлы телефонной, телевизионной, радио-связи и оповещения, архивы, концертные залы, объекты для проведения массовых мероприятий и др.

3. Классификация критически важных объектов по уровням угроз

1 класс — критически важные объекты, аварии на которых или прекращение функционирования которых могут являться источниками возникновения федеральных и/или трансграничных чрезвычайных ситуаций;

2 класс — критически важные объекты, аварии на которых или прекращение функционирования которых могут являться источниками возникновения региональных чрезвычайных ситуаций

3.2.3 Результаты и выводы:

Объекты, которые могут использоваться террористами или террористическими организациями в целях нарушения государственной безопасности, дестабилизации государственного строя, либо оказания воздействия на принятие решений высшими органами государственной власти для побуждения их к совершению действия в интересах террористов;
объекты, уничтожение или прекращение действия которых, представляет угрозу для национальной (информационной, экономической, военной, внешнеполитической, экологической) безопасности Российской Федерации

3.2 Практическое занятие №7-11 (10 часов).

Тема: «Угрозы безопасности автоматизированных систем**»**

3.2.1 Задание для работы:

1. Организация физической защиты критически важных объектов
2. Организация информационной защиты критически важных объектов

3.2.2 Краткое описание проводимого занятия:

1. Организация физической защиты критически важных объектов

В зависимости от категории объекта, наличия на объекте вооруженной охраны, ее возможностей, особенностей объекта и его критических элементов, принятых угроз и моделей нарушителя, принятых на объекте мер по обеспечению технологической и других видов безопасности цель системы физической защиты достигается выполнением следующих задач:

- предупреждением террористических актов в отношении критических элементов объекта;
- своевременным обнаружением несанкционированных действий;
- оперативным реагированием на несанкционированные действия сил охраны по сигналам тревоги, задержкой (замедлением) продвижения нарушителя;
- предотвращением террористических актов путем нейтрализации нарушителей вне зоны совершения террористических актов или путем блокирования критического элемента (до начала террористического акта);
- предотвращение террористического акта путем нейтрализации нарушителей в процессе совершения террористического акта до того, как будут достигнуты недопустимые для объекта последствия.

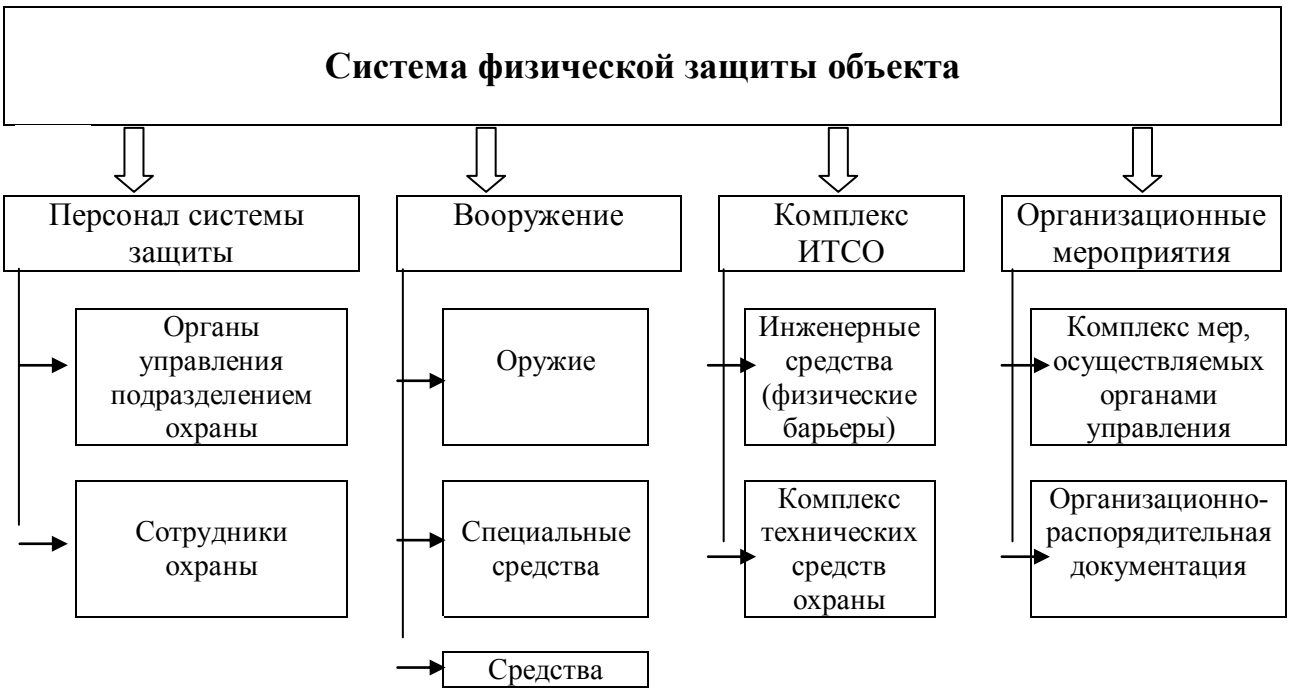
Существующая система физической защиты и охраны должна обеспечивать следующие варианты предотвращения террористических актов:

– для объектов 1 класса опасности – до начала проведения ТА;
– для объектов 2 и 3 класса опасности – до или вовремя проведения ТА;
– для объектов 4 класса опасности – во время проведения ТА;
– для объектов 5 класса опасности – реагирование.

Категория объекта. Мероприятия	1 класс	2, 3 класс	4, 5 класс
Организация охраны объекта в соответствии с требованиями для действующего на объекте вида охраны	+	+	+
Физическая защита критических элементов	+	+	+
Наличие на объекте структурного подразделения по физической защите и/или охране	+	+	+/-
Обеспечение пропускного режима	+	+	+/-
Обеспечение внутриобъектового режима	+	+	+
Выделение на объекте охраняемых зон	+	+	+/-
Выделение на объекте зон ограниченного доступа	+	+	+
Создание в СФЗ пункта (пунктов) управления	+	+	+/-
Организация взаимодействия персонала СФЗ с персоналом объекта	+	+	+/-
Организация взаимодействия с органами МВД России	+	+	+
Организация взаимодействия с органами ФСБ России	+	+/-	+/-
Организация контроля за соблюдением требований по физической защите и охране	+	+	+
Организация контроля за техническим состоянием ИТСО и работоспособностью ТСФЗ	+	+	+
Организация профессиональной подготовки персонала	+	+	+

Приведенные в таблицах знаки «+» и «-» означают соответственно обязательность или необязательность выполнения указанных мероприятий на объектах данной категории. Знак «+/-» означает, что решение по данному мероприятию принимается на конкретном объекте на основе результатов анализа его уязвимости и оценки эффективности СФЗ.

Систему физической защиты (охрану) объекта можно представить в виде функционально завершенных компонентов, позволяющих оптимальным образом задавать требования к ним в разрабатываемых нормативных документах.



связи

Под охраной объекта подразумевается комплекс мер, направленных на своевременное выявление угроз и предотвращение нападения на охраняемые объекты, совершения террористического акта, других противоправных посягательств в т.ч. экстремистского характера, а также возникновения чрезвычайных ситуаций.

Достаточность системы физической защиты объекта определяется по отношению к каждому критическому элементу, находящемуся на территории объекта и выявленному в процессе анализа уязвимости объекта, а также по отношению к другим элементам объекта. Защищенность объекта в целом определяется защищенностью его критических элементов, а также других элементов объекта, определяющих его важность (режимность, категорию по гражданской обороне и т.д.).

2. Организация информационной защиты критически важных объектов

Инженерно-техническая укрепленность объекта - это совокупность мероприятий, направленных на усиление конструктивных элементов зданий, помещений и охраняемых территорий, обеспечивающих необходимое противодействие несанкционированному проникновению (случайному проходу) в охраняемую зону, взлому и другим преступным посягательствам.

Основой обеспечения надежной защиты объекта от угроз террористического характера и иных посягательств экстремистского характера является их надлежащая инженерно-техническая укрепленность в сочетании с оборудованием данного объекта системами охранной и тревожной сигнализации.

В целесообразных случаях для усиления защиты объекта и оперативного реагирования применяются системы контроля и управления доступом, охранного телевидения и оповещения.

В обоснованных случаях, по согласованию с территориальным подразделением вневедомственной охраны, допускается для защиты отдельных конструктивных элементов объекта и уязвимых мест использовать только системы контроля и управления доступом или охранного телевидения, при наличии в них устройств, выполняющих аналогичные функции систем охранной и тревожной сигнализации.

Особенности оборудования объектов водоснабжения

Склады хлора и аммиака должны иметь сплошное глухое ограждение высотой не менее двух метров, с глухими, плотно закрывающимися воротами.

Согласно требованиям строительных норм и правил водопроводные сооружения должны иметь по периметру глухое ограждение высотой 2,5 м.

Открытые емкостные сооружения сетей водоснабжения и канализации, если их стены возвышаются над отметкой пола, площадки или планировки менее чем на 0,75 м, должны иметь по внешнему периметру дополнительное ограждение, при этом общая высота до верха ограждения должна быть не менее 0,75 м. Для стен, ширина верхней части которых более 0,3 м, допускается возвышение над полом, площадкой или планировкой не менее 0,6 м без ограждения. Отметка пола или планировки должна быть ниже верха стен открытых емкостных сооружений не менее чем на 0,15 м.

Подземные емкостные сооружения, имеющие обвалование грунтом высотой менее 0,5 м над спланированной поверхностью территории, должны иметь ограждения от возможного заезда транспорта или механизмов.

Все опасные места на территории и в помещениях сооружений водоснабжения и канализации должны быть надежно укрыты, закрыты или ограждены.

3.1.3 Результаты и выводы:

Организация и проведение противопожарных мероприятий, включая оснащение объекта системой пожарной сигнализации, осуществляется в соответствии с действующими нормативными документами Государственной противопожарной службы МЧС России. Пожарная сигнализация при наличии технической возможности подключается на отдельные номера пультов централизованного наблюдения.

3.3 Практическое занятие №11-16 (10 часов).

Тема: «Основы и принципы защиты информационныхтпроцессов в автоматизированных системах»

3.3.1 Задание для работы:

1. Общие требования к идентификации критически важных объектов на региональном уровне
2. Требования к регистрации объектов
3. Требования к формированию сведений и ведению перечня

3.3.2 Краткое описание проводимого занятия:

1. Общие требования к идентификации критически важных объектов на региональном уровне

1. Идентификация КВО для их регистрации в Перечне проводится с целью выявления КВО и эксплуатируемых организаций.

2. Идентификацию КВО проводит организация, эксплуатирующая эти объекты. При идентификации КВО осуществляются выявление и отнесение объекта к категории КВО, определение его наименования, признаков отнесения к КВО и типа КВО.

3. В эксплуатирующей организации должен быть издан приказ (распоряжение), определяющий сроки проведения идентификации; сроки и порядок представления в регистрирующий орган сведений, необходимых для регистрации объектов в Перечне, внесения изменений в Перечень; лицо (лица), ответственное за проведение идентификации и представление сведений. В дополнение к представляемым документам, содержащим необходимые сведения, организация должна представлять в регистрирующий орган их электронные копии на магнитном носителе.

4. В результате идентификации определяются количественные и качественные характеристики КВО и иные, характеризующие его сведения. На основании сведений, характеризующих КВО, организация заполняет карту учета объекта в Перечне (далее – карта учета) по форме, приведенной в приложении № 1. Порядок оформления карты учета приведен в приложении № 2.

5. В процессе идентификации выявляются все КВО, признаки опасности и тип каждого КВО, эксплуатируемого организацией, с учетом требований законодательных и иных нормативных правовых актов и на основе анализа состава предприятия (имущественного комплекса), проектной документации, технологических регламентов и

других документов, связанных с эксплуатацией объектов.

6. При идентификации КВО в качестве объединяющего признака используются производственная площадка (земельный участок) или производственное здание в границах генплана предприятия.

Критически важным объектом считается не отдельный механизм, оборудование или технологическая площадка, а объект целиком.

В качестве КВО следует выделять предприятие, расположенное на одной производственной площадке.

7. Если на предприятии эксплуатируется несколько объектов, и лишь один из них обладает признаками КВО, то следует рассматривать в качестве КВО лишь этот объект, а не предприятие в целом.

Наименования объектов устанавливаются по результатам их идентификации в соответствии с Перечнем типовых видов КВО.

8. Правильность проведения идентификации КВО контролирует регистрирующий орган.

2. Требования к регистрации объектов

1. Все объекты, имеющие признаки отнесения их к КВО, подлежат обязательной регистрации.

При регистрации объектов в Перечне производится занесение в базу данных Перечня сведений о действующих объектах, присвоение им регистрационных номеров в Перечне и выдача свидетельства о регистрации этих объектов эксплуатирующим их организациям.

При перерегистрации объектов в Перечне производится регистрация всех объектов, эксплуатируемых организацией по истечении пяти лет со дня регистрации ее первого объекта или предшествующей перерегистрации, занесение в базу данных Перечня сведений о действующих объектах и выдача свидетельства о регистрации этих объектов с указанием нового срока перерегистрации.

Организация, которая вновь ввела в эксплуатацию объект, имеющий признаки КВО, представляет в регистрирующий орган сведения, необходимые для регистрации этого объекта в Перечне, в срок не позднее 30 дней с даты начала его эксплуатации. Регистрирующий орган перерегистрирует КВО, эксплуатируемые организацией, через 5 лет после регистрации или предыдущей перерегистрации объектов этой организации. Дата перерегистрации исчисляется с даты регистрации первого КВО эксплуатирующей организации.

Арендуемые КВО регистрируются или перерегистрируются как объекты, эксплуатируемые организацией-арендатором, которая представляет в регистрирующий орган сведения, необходимые для регистрации или перерегистрации объектов в Перечне. Организация, сдавшая в аренду зарегистрированный КВО, представляет в регистрирующий орган копию договора аренды и заявление об исключении из Перечня эксплуатировавшегося ею объекта. По окончании срока аренды арендатор представляет в регистрирующий орган копию договора аренды и заявление об исключении эксплуатировавшегося им объекта из Перечня.

2. Для регистрации или перерегистрации объектов в Перечне эксплуатирующая организация направляет в регистрирующий орган заявление по форме, приведенной в

приложении № 3, с приобщением к нему:

а) карт учета объектов (в двух экземплярах на каждый объект);

б) сведений, характеризующих каждый КВО;

в) ранее выданного свидетельства о регистрации (при перерегистрации);

г) дополнительных сведений о КВО и эксплуатирующей их организации в составе и объеме, установленных соответствующим федеральным органом исполнительной власти в пределах его компетенции (по требованию регистрирующего органа).

3. Регистрирующий орган в срок до 45 дней со дня приема заявления:

а) проверяет полноту пакета представленных документов, правильность их заполнения и правильность применения критериев идентификации при их составлении;

б) при соответствии представленных документов настоящему Положению, вносит сведения об объекте и эксплуатирующей организации в базу данных Перечня, присваивает каждому КВО регистрационный номер в Перечне в соответствии с приложением № 4;

в) вносит сведения о регистрации и регистрационные номера объектов в их карты учета, которые заверяет печатью;

г) оформляет свидетельство о регистрации объектов в Перечне по форме, приведенной в приложении № 5; заверяет его печатью; вносит запись о выдаче свидетельства в компьютерную базу данных выданных свидетельств (в базе данных указываются дата записи, номер и дата свидетельства, эксплуатирующая организация, количество объектов, дата перерегистрации, номер и дата свидетельства, взамен которого выдано настоящее свидетельство, сведения о лице, которому выдано свидетельство);

д) выдает свидетельство о регистрации КВО и по одному экземпляру каждой карты учета представителю эксплуатирующей организации, уполномоченному на их получение, второй экземпляр использует в контрольной работе и работе по формированию соответствующей базы данных Перечня;

е) при перерегистрации отправляет документы, представленные при регистрации (предыдущей перерегистрации), на уничтожение в установленном порядке;

ж) при несоответствии представленных документов настоящему Положению, возвращает их (с указанием причин возвращения) эксплуатирующей организации, которая переоформляет их в течение 30 дней;

з) при отказе в регистрации объекта, как не обладающего признаками КВО, документы не переоформляются.

4. Организация обеспечивает хранение свидетельства о регистрации в комплекте с картой (картами) учета в качестве документов, подтверждающих регистрацию эксплуатируемых объектов в Перечне и предъявляет указанный комплект документов по требованию должностных лиц регистрирующего органа.

5. Для внесения в Перечень изменений в связи с изменениями сведений, содержащихся в свидетельстве о регистрации или в картах учета, организация направляет в регистрирующий орган заявление по форме, приведенной в приложении № 3, с приобщением к нему:

а) вновь оформленных или измененных карт учета объектов, в двух экземплярах;

б) сведений, характеризующих и подтверждающих изменения;

в) ранее выданного свидетельства о регистрации;

г) дополнительных сведений о КВО и эксплуатирующей их организации в составе и объеме, установленных соответствующим федеральным органом исполнительной власти в пределах его компетенции (по требованию регистрирующего органа).

6. Регистрирующий орган в срок до 30 дней со дня приема заявления:

а) проверяет полноту пакета представленных документов, правильность их

заполнения и правильность применения критериев идентификации при их составлении;

б) при соответствии представленных документов настоящему Положению присваивает каждому вновь регистрируемому объекту регистрационный номер в Перечне;

в) вносит сведения о регистрации и регистрационные номера объектов в их карты учета и заверяет их печатью;

г) при внесении в карты учета изменений, затрагивающих содержание свидетельства о регистрации, оформляет новое свидетельство о регистрации; заверяет его печатью; вносит запись о выдаче свидетельства в компьютерную базу данных выданных свидетельств; выдает свидетельство о регистрации и по одному экземпляру каждой вновь оформленной или измененной карты учета представителю эксплуатирующей организации, уполномоченному на их получение; второй экземпляр использует в контрольной работе и работе по формированию соответствующей базы данных Перечня;

д) при внесении в карты учета изменений, не затрагивающих содержания свидетельства о регистрации, направляет организации по одному экземпляру каждой измененной карты учета, вторые экземпляры использует в контрольной работе и работе по формированию соответствующей базы данных Перечня;

е) отправляет ранее представленные документы, не содержащие сведений об изменениях, на уничтожение в установленном порядке;

ж) при несоответствии представленных документов настоящему Положению возвращает их эксплуатирующей организации, которая переоформляет их в течение 30 дней со дня возврата документов (в случае отказа в регистрации объекта, как объекта, не обладающего признаками КВО, документы не переоформляются).

При внесении изменений регистрационные номера и даты регистрации зарегистрированных ранее объектов не изменяются, регистрационные номера новым объектам присваиваются в соответствии с приложением № 4.

7. Для внесения в Перечень сведений об исключении объекта вследствие ликвидации, вывода из эксплуатации (списания с баланса), сдачи в аренду, консервации (не менее года) объекта, смены эксплуатирующей организации или изменения объекта, в связи с которым у объекта не стало признаков отнесения к КВО, организация направляет в регистрирующий орган письмо по форме, приведенной в приложении № 3, с приобщением к нему:

а) копии документа, подтверждающего ликвидацию или вывод из эксплуатации (списание с баланса) объекта (в случае его ликвидации, вывода из эксплуатации);

б) карты учета исключаемого из Перечня объекта;

в) свидетельства о регистрации, подтверждающего, что этот объект включен в Перечень;

г) копии договора аренды (в случае сдачи объекта в аренду).

При исключении объекта из Перечня вследствие изменений объекта, в связи с которыми у объекта не стало признаков принадлежности к КВО, в письме организации должны быть указаны эти изменения.

При проведении эксплуатирующей организацией мероприятий по консервации ранее зарегистрированного объекта на срок не менее одного года основанием для исключения этого объекта из Перечня на время консервации являются подписанные руководителем организации заявление и документы, подтверждающие осуществление указанных мероприятий.

8. Регистрирующий орган в срок до 20 дней:

а) проверяет полноту пакета представленных документов и правильность их заполнения;

б) вносит в Перечень сведения об исключении объекта из Перечня КВО;

в) в случае, если в Перечне зарегистрированы другие, кроме исключенного, КВО,

эксплуатируемые организацией, оформляет новое свидетельство о регистрации объектов в Перечне; вносит запись о его выдаче в компьютерную базу данных выданных свидетельств; выдает свидетельство о регистрации представителю эксплуатирующей организации, уполномоченному на его получение;

г) сдает копию документа, подтверждающего ликвидацию или вывод из эксплуатации (списание с баланса) объекта, выданное ранее свидетельство о регистрации и соответствующую карту учета в архив, где они хранятся до следующей перерегистрации объектов, эксплуатируемых этой организацией, или, при отсутствии таких объектов, в течение 5 лет, а затем передаются на уничтожение в установленном порядке.

9. Если у зарегистрированного в Перечне объекта отсутствует или неизвестна эксплуатирующая организация, либо от эксплуатации ранее эксплуатировавшая его организация отказалась, и при условии, что этот объект может быть признан в соответствии с гражданским законодательством Российской Федерации бесхозяйной недвижимой вещью, регистрирующий орган может обратиться в орган местного самоуправления, на территории которого находится объект, с предложением о признания указанного объекта бесхозяйной вещью с последующим принятием его на учет органом, осуществляющим государственную регистрацию права на недвижимое имущество.

Вышеуказанный объект может быть исключен из Перечня до признания его бесхозяйной вещью в случае, если у него не стало признаков отнесения к КВО на основании акта комиссии, созданной регистрирующим органом, подтверждающего отсутствие у объекта ранее выявленных признаков отнесения к КВО.

10. В случае утраты свидетельства о регистрации эксплуатирующей организации на основании ее заявления по форме, приведенной в приложении № 3, выдается дубликат свидетельства о регистрации с надписью «Дубликат» в правом верхнем углу.

…….

3. Требования к формированию сведений и ведению перечня критически важных объектов на региональном уровне

1. При ведении Перечня производится накопление в базе данных Перечня сведений о действующих объектах, внесение в банк данных необходимых изменений, анализ и хранение систематизированной информации о зарегистрированных объектах и об организациях, эксплуатирующих эти объекты.

При внесении изменений в Перечень производится внесение (изменение) в базу данных Перечня в соответствии с изменившимися сведениями об объекте или эксплуатирующей его организации.

При исключении объекта из Перечня производится занесение в базу данных Перечня сведений об исключении объекта из Перечня вследствие ликвидации, вывода из эксплуатации (списания с баланса) объекта, передачи его в аренду, консервации на срок не менее одного года или изменения объекта, в связи с которым у объекта не стало признаков отнесения к КВО.

2. Занесение сведений о зарегистрированном объекте (объектах) или внесение изменений в базу данных производится регистрирующим органом до выдачи свидетельства о регистрации и возврата карт учета.

3.3.3 Результаты и выводы:

Предоставление информации заинтересованным федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской

Федерации, органам местного самоуправления производится на основании их заявлений путем выдачи выписок из Перечня критически важных объектов на региональном уровне. Заявление должно содержать мотивированное обоснование указанными органами власти соответствия запрашиваемой информации объему, необходимому для выполнения ими своих полномочий.

3.4 Практическое занятие №17-21 (10 часов).

Тема: «Организация и средства защиты информационных процессов в автоматизированных системах**»**

3.4.1 Задание для работы:

1. Разработка плана повышения защищенности критически важного объекта

3.4.2 Краткое описание проводимого занятия:

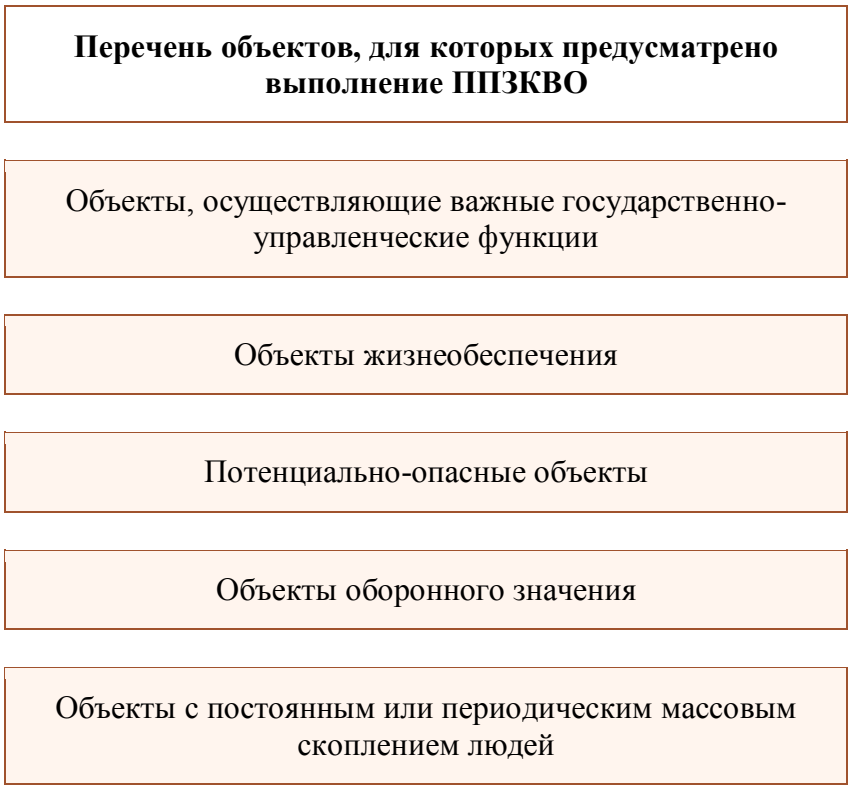
1. *Разработка плана повышения защищенности критически важного объекта*

План повышения защищенности критически важного объекта (ППЗКВО)

Выполнение ППЗКВО предусматривается согласно требованиям [5; 6; 7].

ППЗКВО разрабатывается для объектов, включенных в перечень КВО (критически важных объектов).

Перечень объектов, для которых предусматривается выполнение ППЗКВО, приведен на блок-схеме 1.



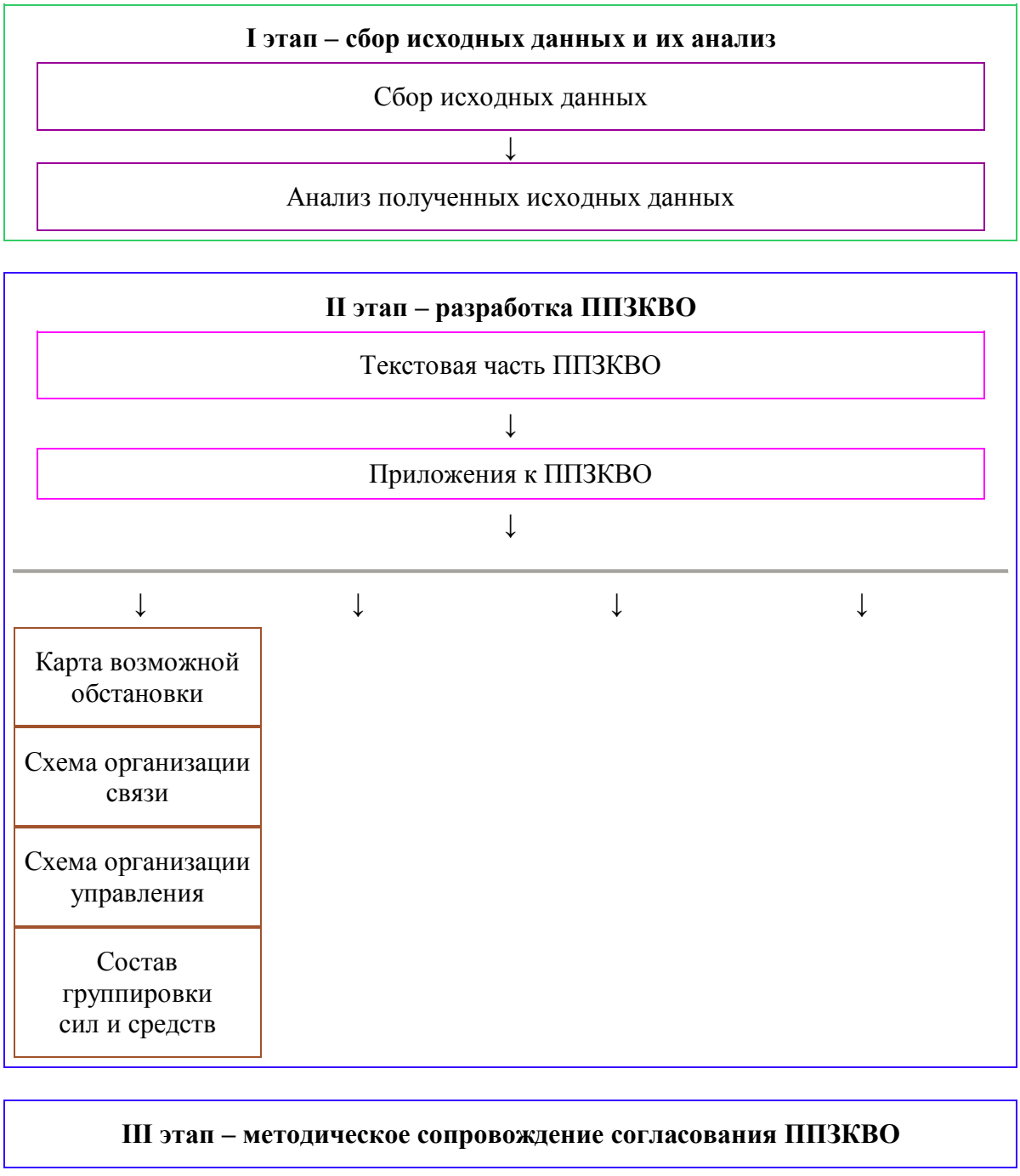
Объекты истории и культуры

Блок-схема 1

Выполнение ППЗКВО

Выполнение ППЗКВО делится на три этапа:
I этап – сбор исходных данных и их анализ;
II этап – разработка ППЗКВО;
III этап – методическое сопровождение согласования ППЗКВО в органах управления МЧС России, МВД России и ФСБ России по субъекту Российской Федерации.

Этапы выполнения ППЗКВО представлены в виде блок-схемы 2.



Блок-схема 2

При **выполнении ППЗКВО** учитываются общие характеристики КВО, последствия при возникновении и угрозах ЧС (чрезвычайных ситуаций) и ТА(террористических актов), мероприятия по повышению уровня защищенности КВО.

Состав ППЗКВО и требования к запрашиваемым для его выполнения исходным данным определен рекомендациями [7] и включает в себя текстовую часть и приложения.

Текстовая часть включает в себя общую характеристику КВО, оценку защищенности и мероприятия по повышению уровня защищенности КВО, списки должностных лиц и перечень организаций, ответственных за мероприятия по повышению защищенности КВО, а также организацию взаимодействия, управления и контроля при выполнении мероприятий по повышению защищенности КВО.

ППЗКВО включает 4 приложения, в том числе: карту (план, схему) возможной обстановки; схему организации связи; схему организации управления; состав группировки сил и средств для ликвидации ЧС на КВО.

3.4.3 Результаты и выводы:

Нормативные документы

1. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму».
2. Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».
3. Указ Президента Российской Федерации от 15.02.2006 № 116 «О мерах по противодействию терроризму».
4. Указ Президента Российской Федерации от 13.09.2004 № 1167 «О неотложных мерах по повышению эффективности борьбы с терроризмом».
5. Распоряжение Правительства Российской Федерации от 23.03.2006 № 411-рс «Об утверждении перечня критически важных объектов Российской Федерации».
6. Решение совместного заседания Совета Безопасности Российской Федерации и президиума Государственного совета Российской Федерации «О мерах по обеспечению защищенности критически важных для национальной безопасности объектов инфраструктуры и населения страны от угроз техногенного,

природного характера и террористических проявлений» (протокол от 13.11.2003 № 4).

7. Методические рекомендации по разработке Планов повышения защищенности критически важных объектов, территорий субъектов Российской Федерации и муниципальных образований», утвержденные заместителем министра МЧС России А. П. Чуприян 28.12.2011 № 2-4-60-21-14.

3.5 Практическое занятие №22-26 (10 часов).

Тема: «Обеспечение доступности, целостности и конфиденциальности в автоматизированных системах и базах данных**»**

3.5.1 Задание для работы:

1. Матричный подход
2. Полномочный подход

3.5.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **прогнозирование успеваемости по ИИС на основе данных по социальному статусу их родителей** и провести СК-анализ семантической информационной модели

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **прогнозирование направления деятельности фирмы на основе данных о расположении и внешнем виде ее офиса** и провести СК-анализ семантической информационной модели

3.5.3 Результаты и выводы:

В ходе блока практических работ, студент изучает систему разграничения доступа к информации в кс. Благодаря этому, обучающийся узнает структуру разграничения доступа к информации в кс.

3.6 Практическое занятие №27-31 (10 часов).

Тема: «Защита информации базы данных средствами СУБД**»**

3.6.1 Задание для работы:

1. Идентификация и аутентификация субъекта доступа
2. Проверка прав доступа субъекта к объекту

3.6.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **выбор автомобиля для приобретения по его признакам** (обучающую выборку взять на автомобильном рынке) и провести СК-анализ семантической информационной модели

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **выбор вариантов приобретения жилья по его признакам** и

провести СК-анализ семантической информационной модели

3.6.3 Результаты и выводы:

В ходе блока практических работ, студент изучает методы разграничения доступа. Благодаря этому, обучающийся лучше узнает методы разграничения доступа.

3.7 Практическое занятие №32-35 (8 часов).

Тема: «Стандарты по защите баз данных**»**

3.7.1 Задание для работы:

1. Процесс эксплуатации КСЗИ
2. Эксплуатация системы разграничения доступа

3.7.2 Краткое описание проводимого занятия:

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **идентификацию трехмерных тел (шар, куб, тетраэдр, конус, цилиндр, пирамида, призма и других) по их проекциям** и провести СК-анализ семантической информационной модели

Описать этапы разработки приложения в системе "Эйдос", обеспечивающее **оценку важности различных видов городского транспорта и различных маршрутов в разрезе по остановкам** и провести СК-анализ семантической информационной модели

3.7.3 Результаты и выводы:

В ходе блока практических работ, студент изучает организацию доступа к ресурсам кс. Благодаря этому, обучающийся лучше узнает организацию ресурсов кс.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ПРОВЕДЕНИЮ СЕМИНАРСКИХ ЗАНЯТИЙ

Не предусмотрено учебным планом