7 Практические задания

7.1 Практическая работа № 1. Характеристика объекта защиты

Цель. Анализ структуры, деятельности и защищаемых ресурсов объекта. Категорирование объекта защиты.

Задачи.

1 Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта.

2 Определение содержания и местонахождения защищаемых ресурсов на объекте.

3 Построение плана объекта. Определение защищаемых зон на плане.

4 Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты.

5 Построение структурной модели защищаемой информации.

6 Определение категории защищаемого объекта.

Задание 1. Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта.

Структура подразделений объекта может быть представлена в виде схемы или таблицы. Под организационной структурой предприятия понимаются состав, соподчиненность, взаимодействие и распределение работ по подразделениям и органам управления, между которыми устанавливаются определенные отношения по поводу реализации властных полномочий, потоков команд и информации. Организационная структура объекта построена по линейно-функциональному признаку.

В качестве примера рассмотрим объект информатизации больница. Руководителем является главный врач. В подчинении у главного врача находятся заместитель по медицинской части, заместитель по экономическим

вопросам, главный бухгалтер, начальник отдела кадров, заместитель главного врача архиватор и информационно вычислительный центр и служба охраны, включающая в себя руководителя охраны помещений, руководителя пожарной охраны и штат охранников. Главный врач контролирует работу управлений, которым подчинены различные отделы. Каждый отдел подчиняется начальнику отдела. Организационная структура объекта показана на рисунке 7.1.

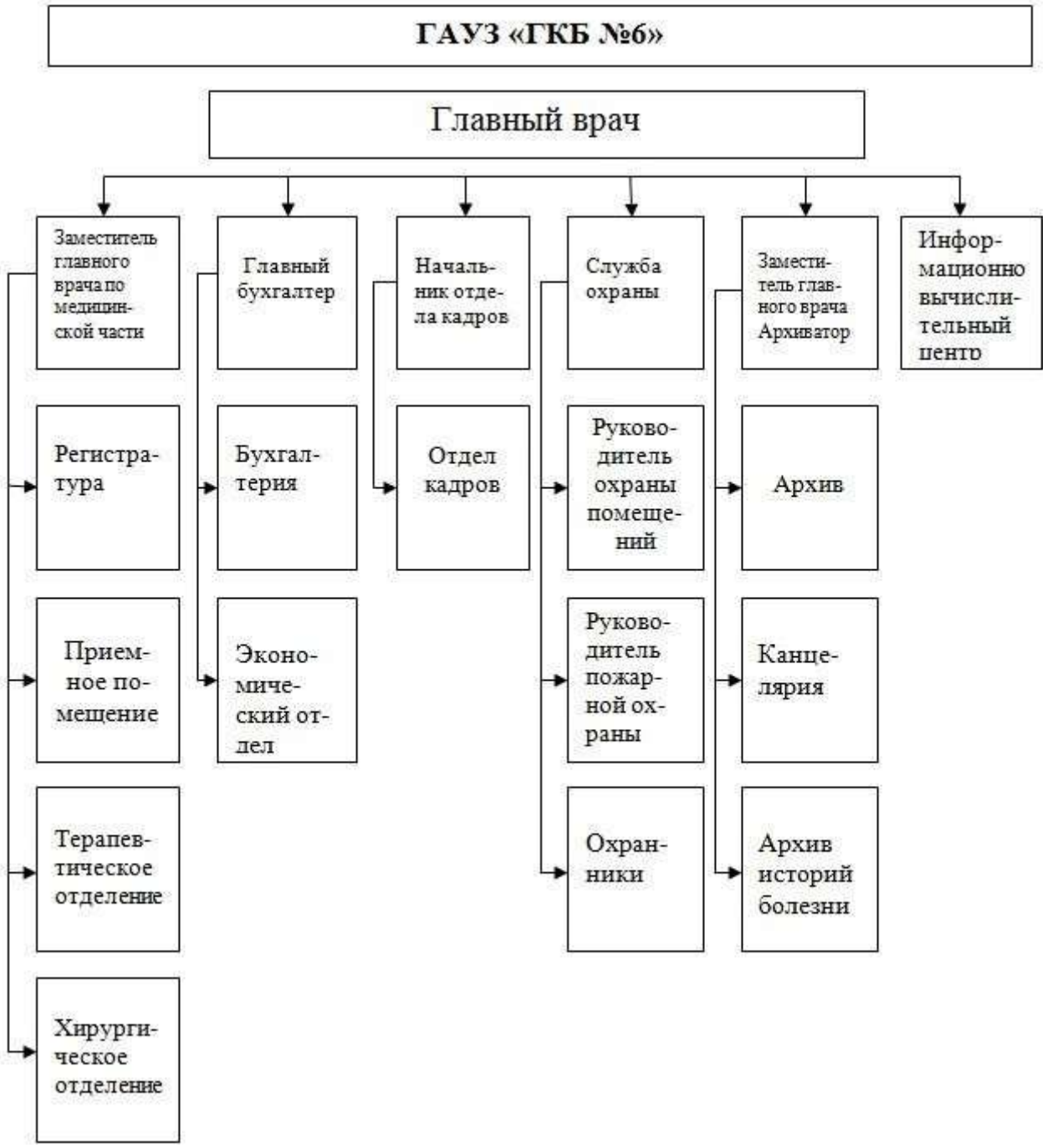

Рисунок 7.1 - Пример организационной структуры объекта

Далее необходимо перечислить решаемые задачи и направления деятельности, осуществляемой на объекте. Привести описание ведущихся на объекте работ, дать характеристику операций, выполняемых на объекте и условий их выполнения. Сформулировать назначение объекта.

Определение функционально-отраслевой принадлежности объекта. По назначению все объекты информатизации делятся на:

- производственные;
- строительные;
- транспортные;
- топливно-энергетического комплекса;
- оборонно-промышленного комплекса;
- социального назначения;
- культурного назначения.

Определить к какому типу относится заданный объект. Определить виды и масштабы возможного ущерба в результате нарушения безопасности. Определить категорию заданного объекта по уровню важности в соответствии с ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации».

Задание 2. Определение содержания и местонахождения защищаемых ресурсов на объекте. Пример приведен в таблице 7.1.

Таблица 7.1 - Основные объекты защиты ГАУЗ «ГКБ № 6»

Объект защиты	Место расположения
Персонал, пациенты	Основное здание больницы и прилегающая к ней территория
Здания, сооружения	Территория предприятия
Конфиденциальная информация	Регистратура, кабинеты больницы
Носители конфиденциальной информации: документы, содержащие ПДн, служебную и коммерческую информацию	Основное здание больницы (кабинеты 5,6,3)
Оборудование и медтехника	кабинеты 3,4
Средства вычислительной техники	Кабинеты 3,4,5,6
Финансовые ценности	Кабинет руководителя (кабинет 2)
Фармацевтические препараты	Аптека больницы

Задание 4. Построение плана объекта. Определение защищаемых зон на плане. Построить план объекта, с помощью принятых стандартом условных обозначений показать все объекты защиты. Определить категории защищаемых зон. Определить структуру контролируемых зон. Пример плана объекта показан на рисунке 7.2.

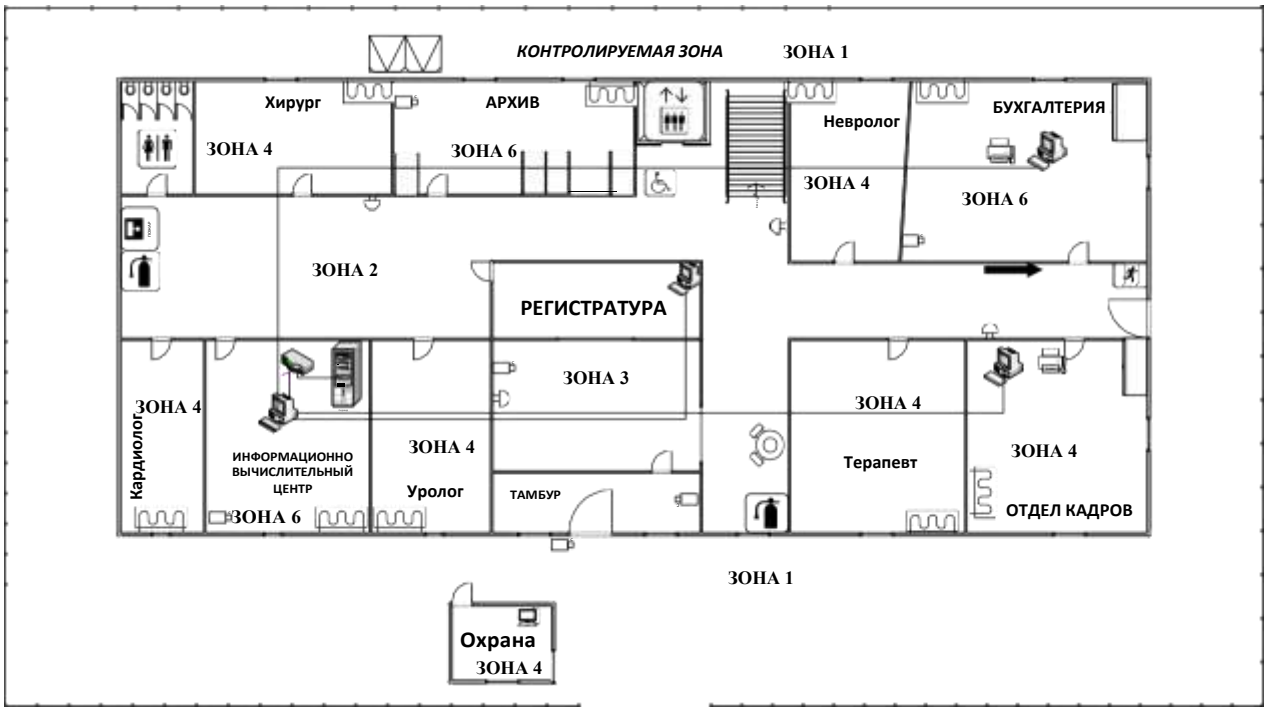

Рисунок 7.2 – Пример плана объекта защиты

На данном объекте показаны несколько зон системы безопасности, которые имеют структуру вложенных зон. В целях физической защиты объектов на базе построения зоны безопасности предприятия имеется система доступа и управления, которая также позволяет минимизировать возможность возникновения угроз. Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к различным составляющим объекта путем разделения его пространства на контролируемые зоны.

Определить категории контролируемых зон, заполнить таблицу 7.2 по данным исследуемого объекта защиты.

Таблица 7.2 – Описание контролируемых зон объекта по уровню доступа

Кате го-рия	Наименова ние зоны	Функциональ ное назначение зоны объекта	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны
I	Свободная	Заполнить по данному объекту	Свободный	Свободный	Есть
II	Наблюдаем ая	Заполнить	Свободный	Свободный	Есть
III	Регистраци онная	Заполнить	Свободный	Свободный с регистрацией по удосто-верениям личности	Есть
IV	Режимная	Заполнить	По служебн. удостоверения м или идентификаци онным картам	По разовым пропускам	Усилен-ная охрана
V	Усиленной защиты	Заполнить	По спецдоку-ментам	По спецпро-пускам	Усилен-ная охрана
VI	Высшей защиты	Заполнить	По спецдоку-ментам	По спецпро-пускам	Усилен-ная охрана

Задание 4. Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты. Проанализировать характеристики технической укрепленности объекта защиты, заполнить таблицу 7.3.

Таблица 7.3 – Характеристики технической укрепленности объекта защиты

Наименование параметра	Данные
1	2
Площадь, кв.м	
Высота потолка, м	
Толщина стен: наружных, внутренних, м	
Окна: количество, размер	

Продолжение таблицы 7.3

1	2
Двери: размер проема, тип замков	
Описание смежных помещений: сверху, сбоку слева, сбоку справа, снизу	
Система электропитания (освещение): тип светильников и их количество	
Система заземления	
Системы сигнализации	
Система вентиляции (тип)	
Наличие экранов на батареях	
Телефонные линии: городская сеть, тип розеток	

Построение пространственной модели объекта защиты. Провести анализ месторасположения объекта (в какой части города расположен объект), какие объекты находятся в ближайшем окружении. Составить пространственную модель объекта по примеру таблицы 7.4.

Таблица 7.4 - Пространственная модель контролируемых зон

Пространственная характеристика помещения	Функциональная, конструктивная и техническая характеристика помещения		
Этаж	2	Площадь, м^2	56
Количество окон, тип сигнализации, наличие штор на окнах	3 окна, жалюзи на окнах, плотные шторы, датчики разбития стекла «Breakglass 2000», F2, Y2, M1:2	Куда выходят окна	Проспект Сталинграда
Двери, кол-во, одинарные, двойные	4 двери звукоизолирующие тяжелые	Куда выходят двери	Коридор, каб. №3, каб. №2, каб. №1
Соседние помещения, название, толщина стен	1.С западной стороны находится Помещение №3, отштукатуренная с двух сторон стена (толщина - 1,5 кирпича). 2. С восточной стороны расположен коридор.		

Задание 5. Построение структурной модели конфиденциальной информации. Для создания полной модели объекта защиты необходимо проанализировать защищаемую информацию и провести её структурирование.

Основные виды источников и носителей защищаемой информации. С точки зрения защиты информации ее источниками являются субъекты и объекты, от которых информация может поступить к несанкционированному получателю (злоумышленнику). Очевидно, что ценность этой информации определяется информированностью источника. Основными источниками информации являются следующие:

- люди;
- документы;
- продукция;
- измерительные датчики;
- интеллектуальные средства обработки информации;
- черновики и отходы производства;
- материалы и технологическое оборудование.

Основные объекты защищаемой информации можно объединить в следующие группы:

- собственники, владельцы и пользователи;
- носители и технические средства передачи и обработки информации;
- системы информатизации связи и управления, военная техника;
- объекты органов управления, военные и промышленные объекты.

В целях обеспечения безопасности, прежде всего, необходимо обеспечить защиту прав собственников и пользователей информацией в сфере информационных процессов и информации, а так же определить их обязанности и ответственность за нарушение режима защиты информационных ресурсов.

В группе носителей и технических средств передачи и обработки информации защите подлежат следующие объекты:

– носители информации в виде информационных физических полей, химических сред, сигналов, документов на различных основах;

– средства вычислительной техники;

– средства связи;

– средства преобразования речевой информации;

– средства визуального отображения;

– средства размножения документов;

– вспомогательные технические средства, расположенные в помещении, где информация обрабатывается;

– помещения, выделенные для проведения мероприятий.

В интересах ЗИ о вооружении и военной технике защите подлежат:

– характеристики и параметры конкретных образцов вооружений и военной техники на всех этапах их жизненного цикла;

– научно-исследовательские, опытно-конструкторские и экспертные работы военно-прикладной направленности.

Для объектов органов управления, военных промышленных объектов защите подлежит следующая информация:

– о местоположении объекта;

– о предназначении, структуре объекта и режимах его функционирования;

– информация, циркулирующая в технических средствах, используемых на объекте;

– информация о разрабатываемых и эксплуатационных образцах вооружения, военной техники и технологии;

– информация о научно-исследовательских и опытно-конструкторских работах.

Структурирование производится путем классификации защищаемой информации в соответствии с функциями, задачами и дальнейшей привязкой элементов информации к их носителям.

Провести классификацию и структурирование информации в соответствии с функциями, задачами и структурой организации, в результате чего защищаемая информация должна быть представлена в виде отдельных элементов информации. Пример структурной модели приведен на рисунке 2.1.

Для структурирования информации в качестве исходных данных используется перечень сведений составляющих государственную, ведомственную, коммерческую, врачебную тайну, а также перечень источников информации в организации. Структурирование информации производится путем классификации информации в соответствии с функциями, задачами и структурой организации с привязкой элементов информации к ее источникам.

Схема классификации разрабатывается в виде графа-структуры, причем нулевой (верхний) уровень иерархической структуры соответствует понятию «защищаемая информация». Нижний уровень соответствует элементам информации одного источника из перечня источников информации.

Результаты структурирования оформляются в виде таблиц. Структурная модель объекта защиты – вербальная модель, таблица со столбцами:

– наименование элемента информации,
– категория информации,
– наименование источников информации,
– местонахождение источников информации.

Моделирование объекта защиты включает в себя:

– определение источников защищаемой информации,
– описание пространственного расположения основных мест размещения источников защищаемой информации,
– выявление путей распространения носителей защищаемой информации за пределы контролируемых зон,
– описание объекта защиты с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

Моделирование состоит в анализе на основе рассмотренных пространственных моделей того, какие могут быть пути распространения информации за пределы контролируемой зоны, и в определении уровней полей и сигналов на границах контролируемых зон. Уровни полей и сигналов рассчитываются с учетом уменьшения мощности на выходе источников сигнала (в дБ) на суммарную величины их ослабления в среде распространения. В результате моделирования объекта защиты оценивается состояние безопасности информации и определяются слабые места существующей системы защиты.

Результаты моделирования показаны на примере таблицы 7.5.

Таблица 7.5 - Структурная модель защищаемой информации

Наименование элемента информации	Категория информации	Источник информации	Вид носителя информации	Место нахождения информации
Структура предприятия	Служебная тайна	Документация	Бумажные и электронные носители	Шкаф с документами, каб. 1,3,5. ПЭВМ в каб. 1,2.3
Личные данные сотрудников	Персональные данные	Личные карточки сотрудников, трудовые книжки, трудовые договоры	Бумажные и электронные носители	Шкаф с документами, каб. 1,3,5, ПЭВМ в каб. 1,2.3
Финансовые документы	Коммерческая тайна	Ведомости, приходно-расходные ордеры, счет-фактуры	Бумажные и электронные носители	Сейф с документами, каб., ПЭВМ каб.3
Приказы по организации	Служебная тайна	Документация	Бумажные и электронные носители	Шкаф , каб. 1,3,5. ПЭВМ в каб. 1,2.3

Задание 6. Определение категории защищаемого объекта. В результате выполнения задач были определены функционально-отраслевая принадлежность исследуемого объекта, виды и масштабы возможного ущерба в результате нарушения безопасности, категория важности защищаемой информации на объекте.

Кроме названных характеристик необходимо определить пожаро- и взрывоопасность данного объекта, что осуществляется в соответствии с Федеральным законом № 117-ФЗ от 10 июля 2012 г. «Технический регламент о требованиях пожарной безопасности».

Результаты решения поставленной задачи занести в таблицу 7.6.

Таблица 7.6 – Категорирование исследуемого объекта защиты

Информативный признак категории	Категория исследуемого объекта
По функционально-отраслевой принадлежности	Заполнить в соответствии с данными объекта защиты
По виду возможного ущерба	Заполнить в соответствии с данными объекта защиты
По масштабу возможного ущерба	Заполнить в соответствии с данными объекта защиты
По важности объекта	Заполнить в соответствии с данными объекта защиты
По категория информации	Заполнить в соответствии с данными объекта защиты
По пожаро- и взрывоопасности	Заполнить в соответствии с данными объекта защиты
По численности персонала свыше 500 человек	Заполнить в соответствии с данными объекта защиты
По материальным активам свыше 500 МРОТ	Заполнить в соответствии с данными объекта защиты

Варианты объектов физической защиты

В таблице 7.7 представлены варианты объектов информатизации, для которых необходимо провести анализ защищаемой информации, угроз, разработать модель системы физической защиты в соответствии с заданиями практических работ.

Таблица 7.7 - Варианты объектов защиты

№ варианта	Объект информатизации
1	Здание администрации завода железобетонных изделий
2	Здание торгового центра
3	Здание поликлиники
4	Корпус университета
5	Здание научно-производственного объединения
6	Здание фармацевтической фирмы
7	Здание районного отдела полиции
8	Здание банка
9	Здание патентного бюро
10	Здание редакции научного издания
11	Здание научно-исследовательского института
12	Здание склада текстильной продукции
13	Здание рекламного агентства
14	Здание производственных цехов бурового оборудования
15	Здание птицефабрики
16	Здание республиканской библиотеки
17	Здание музея изобразительных искусств
18	Здание школы
19	Здание больницы
20	Здание районного суда

Контрольные вопросы

1 Дать определение системы физической защиты объекта информатизации. Пояснить цель и основные задачи физической защиты объектов информатизации.

2 Назвать и дать характеристику структуры и состава системы физической защиты объекта.

3 Назвать и охарактеризовать инженерно-технические средства защиты объектов информатизации.

4 Назовите основные организационные мероприятия физической защиты.

5 Назвать и дать определение принципов физической защиты.

6 В чем заключается принцип многозональности, назвать и пояснить виды контролируемых зон по структурной организации.

7 Назвать и дать характеристику всех возможных категорий контролируемых зон по условиям доступа.

8 В чем заключается принципы многорубежности, непрерывности, адаптируемости системы физической защиты?

9 Назвать и дать характеристику методов физической защиты объектов информатизации.

10 Назвать и пояснить этапы анализа объекта физической защиты.

11 По каким признакам проводится категорирование исследуемого объекта защиты. дать характеристику категорий по функционально-отраслевой принадлежности, по виду и масштабу ущерба.

12 Каким образом проводится категорирование объектов защиты по важности и по секретности информации? Назвать руководящие документы.

13 Назвать и дать характеристику категории защищаемых объектов по пожаро- и взрывоопасности.

14 Что представляет собой структурная модель защищаемой информации?