

22 кафедра

Обеспечение безопасности информации в автоматизированных системах

**«Разработка проекта состава и
содержание программно-
аппаратных мер по обеспечению
безопасности информации на объекте
информатизации»**

Подготовил: курсант Глодян Дмитрий Владимирович

ГЛАВНАЯ ЦЕЛЬ КУРСОВОЙ РАБОТЫ: НАУЧИТЬ ОБУЧАЮЩИХСЯ

самостоятельно применять полученные знания для решения конкретных практических задач

привить навыки самостоятельного проектирования, производства расчетов, проведения научных исследований

обосновывать принимаемые решения

развитие навыков работы со специальной литературой

ИСХОДНЫЕ ДАнные

Уровень конфиденциальности информации	
общедоступная информация	+
сведения составляющие служебную тайну	+
секретные сведения	+
совершенно секретные сведения	+

Звено управления - общевойсковое соединение

Тип объекта информатизации: распределенные ВС, состоящие из ЛВС

Условия расположения объекта информатизации: все ЭВМ и каналы связи расположились в одной контрольной зоне (КЗ).

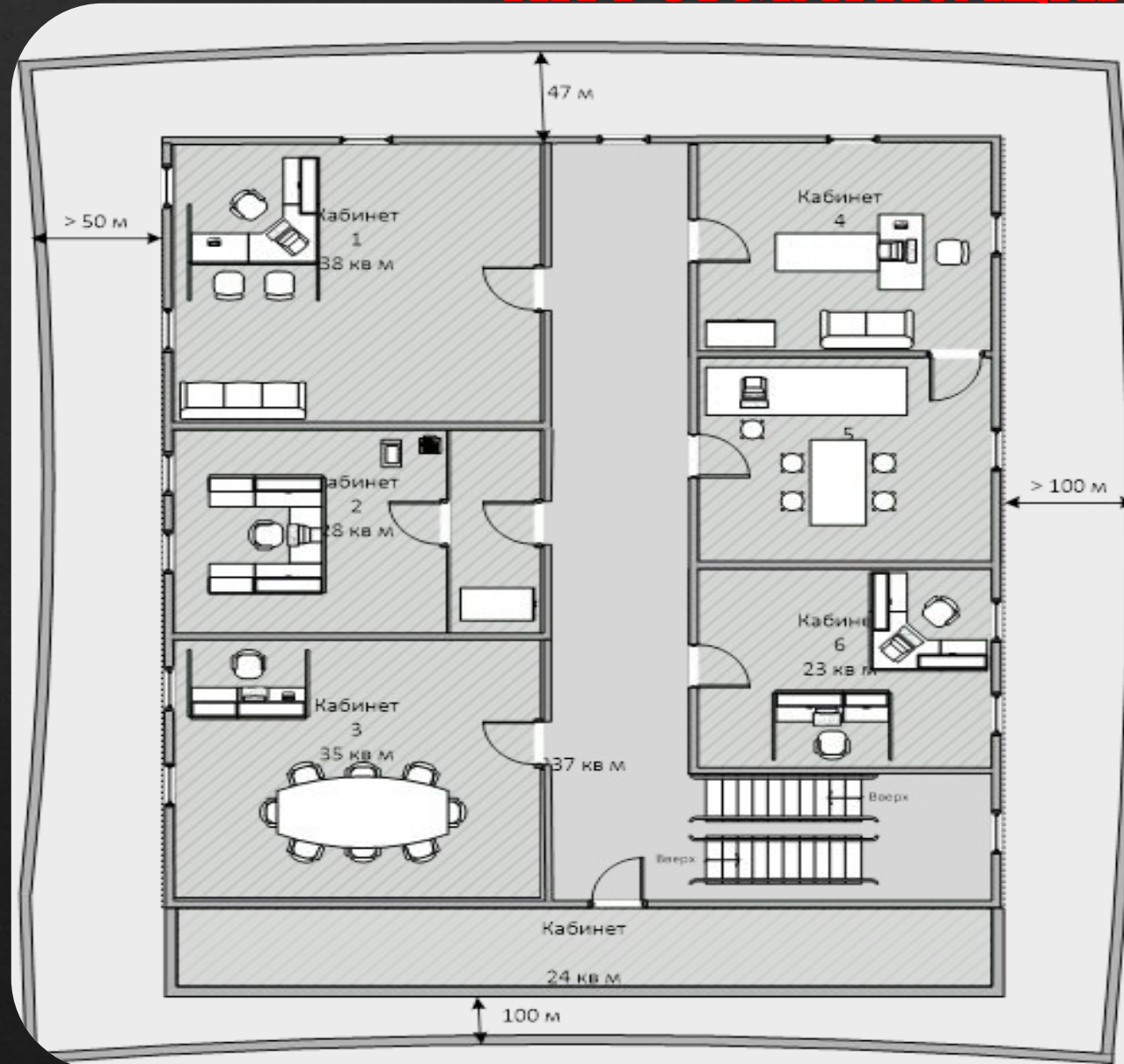
Распределение полномочий пользователей: пользователи имеют разные уровни допуска.

Состав информационной базы: пользователи ограничены в допуске к различным разделам информационной базы.

Построение системы защиты информации от НСД: с применением специальных программных средств защиты от НСД.

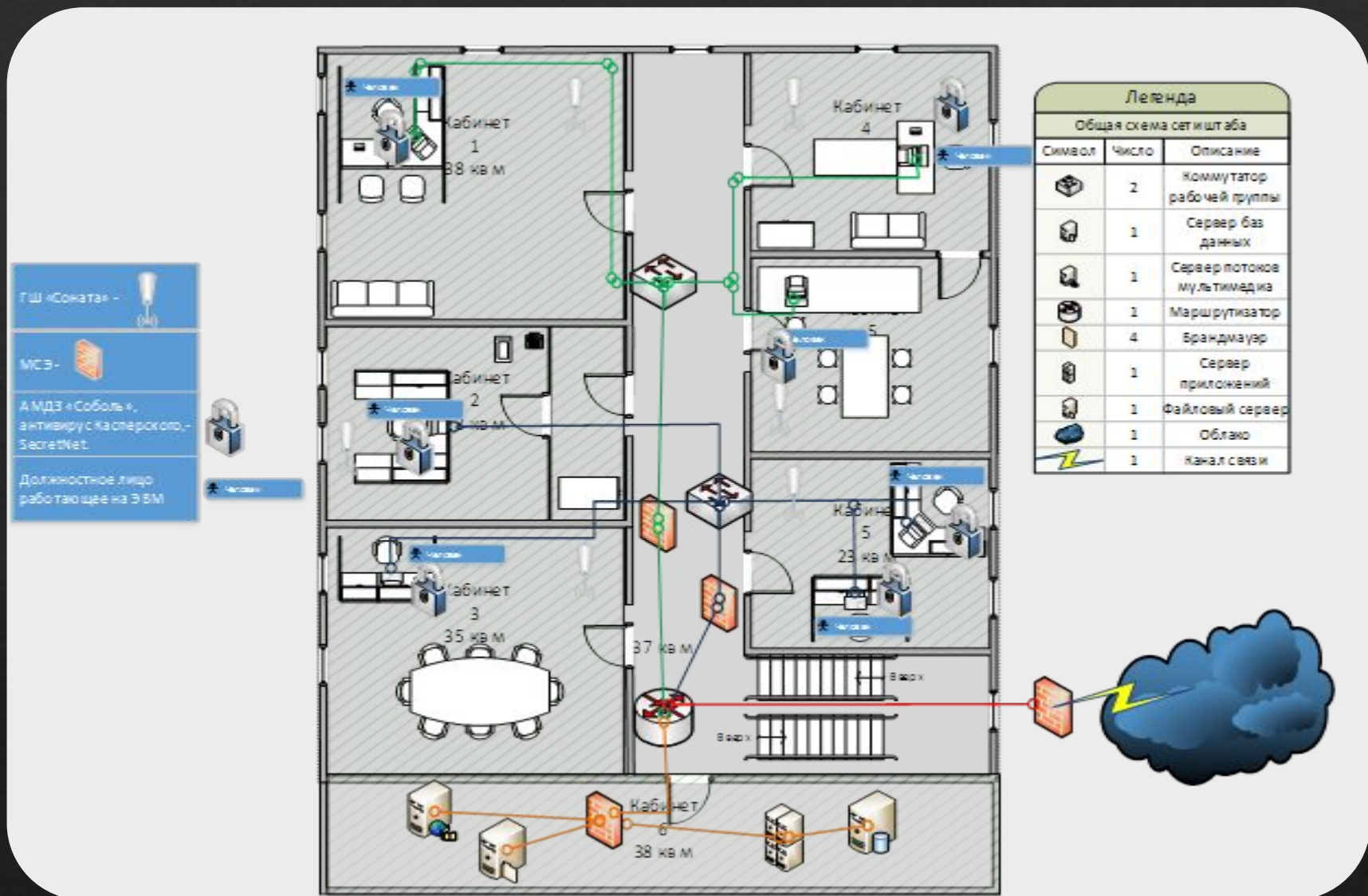
Разработать структуру ресурсов (каталогов) для заданного количества пользователей ОИ: количество начальников отделов – 1, количество заместителей начальника отдела – 3, количество специалистов в отделах - 3

СТРУКТУРНАЯ СХЕМА ОБЪЕКТА ИНФОРМАТИЗАЦИИ



Названия кабинетов
1. Кабинет НШ
2. Кабинет начальника СЗГТ
3. Кабинет начальника отдела кадров
4. Кабинет начальника оперативного отделения
5. Кабинет офицеров ОБИ
6. Серверная

СТРУКТУРНАЯ СХЕМА ПОДСИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ



ОБОСНОВАНИЕ ПРОЕКТНЫХ РЕШЕНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Лучшим подходом к интеграции средств защиты информации для разнородной информационной системы является выбор средств защиты на основе однотипных сетевых технологий. Это позволит организовать информационный обмен между элементами комплексной системы защиты и построить основу для создания централизованной системы управления защитой информации.

Для построения ОИ, обрабатывающих информацию ограниченного доступа, должны выбираться только сертифицированные СВТ и криптографические средства защиты информации.

Спасибо за внимание!