Перечень используемых определений и сокращений в настоящем документе приведён в таблице №1.

Таблица №1Перечень определений проекта третьей практической работы

Сокращение	Расшифровка
VLAN	Виртуальная сеть (RFC 802.1q)
АС	Автоматизированная система
РС	Рабочая станция (PC- personal computer)
СОД	Система обработки данных
БД	База данных
ВТСС	Вспомогательные технические средства и системы
ИС	Информационная система
АСПД	Автоматизированная система персональных данных
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
МЭ	Межсетевой экран
НМД	Нормативно-методический документ
ОС	Операционная система
ОТСС	Основные технические средства и системы
ПД	Персональные данные
ПО	Программное обеспечение
РД	Руководящий документ
РП	Технорабочий (рабочий) проект
САЗ	Система анализа защищенности
СВТ	Средство вычислительной техники
СЗИ	Система защиты информации
СЗПД	Система защиты персональных данных
ТЗ	Техническое задание
ТП	Технический проект
ФСБ	Федеральная Служба Безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

В данном проекте приняты следующие определения :

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин

Автоматизированная система (АС) -
система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Безопасность информации - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней),целостность и доступность информации при ее обработке техническими средствами.

Комплексная система защиты информации (КСЗИ) – это совокупность сил, средств, методов и мероприятий, используемых во взаимодействии и дополнении друг друга и предназначенных для обеспечения на регулярной основе и на заданном уровне защиты информации на этом объекте.

Дисциплина: проектирование систем распределенной и параллельной обработки данных

Тема: ПРОЕКТНОЕ РЕШЕНИЕ

на разработку

архитектуры системы распределенной и параллельной безопасной обработки информации малого предприятия

Время выполнения: 8 часов

Цель работы: составление архитектуры информационной системы малого предприятия с архитектурой системы защиты информации при размещении в помещении

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Этапы создания системы защиты информации (СЗИ) в ИС распределенной и параллельной обработки информации малого предприятия

1 этап. Оценка объекта информатизации.

1.1 Обследование объекта информатизации.
На данном этапе определяются:
- состав и структурная схема защищаемого объекта;
- виды и характеристики каналов связи;
- возможности утечки информации на объекте информационной деятельности Заказчика по техническим каналам;
- особенности компонентов вычислительной системы СОД и их взаимное влияние друг на друга.

Осуществляются:

- обследование и анализ объекта информационной деятельности;
- модернизация средств вычислительной техники и средств защиты, по результатам анализа;
- проверка средств вычислительной техники, находящихся на объекте информационной деятельности Заказчика и выдача предписания на эксплуатацию;
- исследование на объекте информационной деятельности Заказчика эффективности комплекса технической защиты информации, носителями которой являются электромагнитные поля и электрические сигналы;

Итог: Разрабатывается модель угроз, которая является основополагающим документом для выполнения работ по технической защите информации и предписание на эксплуатацию электронно-вычислительной техники СОД.

* Для формирования модели угроз СОД Заказчик должен предоставить Исполнителю следующий набор документов и выполнить следующие работы:

–План-схему помещения, схему занимаемых сотрудниками рабочих мест (список пользователей СОД), схему расположения рабочих мест с указанием оборудовании, структуру управления предприятием, обоснование необходимости защиты информации СОД, перечень сведений конфиденциального характера, подлежащих защите в СОД;

–Письмо о наличии иностранных представительств, дипломатических посольств и т.п. в 200-метровой зоне относительно объекта информационной деятельности;

–Инженерно-строительную и/или проектную документацию (систем электропитания ** , заземления ** , телефонизации, охранной и пожарной сигнализации, вентиляции ** , компьютерных сетей);

** Исполнитель работ согласовывает дополнительно по каждой из подсистем для СОД.

2 этап. Проектирование системы защиты информации

2.1 Разработка технического задания по созданию СЗИ.
2.2 Разработка проектной документации
2.3 Моделирование элементов защиты СОД.
2.4 Разработка эксплутационной документации СОД.

Итог: ***Техническое задание*** согласовывается с предприятием Заказчиком. Согласно утвержденного Заказчиком технического задания производится построение комплексной системы защиты информации.

3 этап. Развертывание и тестирование

3.1 Построение элементов защиты, тестирование, разработка документов по технической защите информации (ТЗИ).

3.2 Разработка программы и методики внутренних испытаний, оформление протокола испытаний СЗИ СОД.

4 этап. Опытная эксплуатация.

5 этап. Обучение.

6 этап. Сопровождение.

Общая продолжительность всех вышеприведенных работ по созданию системы защиты информации СОД - не более 6 месяцев.

Стоимость проекта по разработке СЗИ отображается в Приложении 1.

1 этап. Предпроектная стадия.

Предпроектное обследование объекта информатизации.

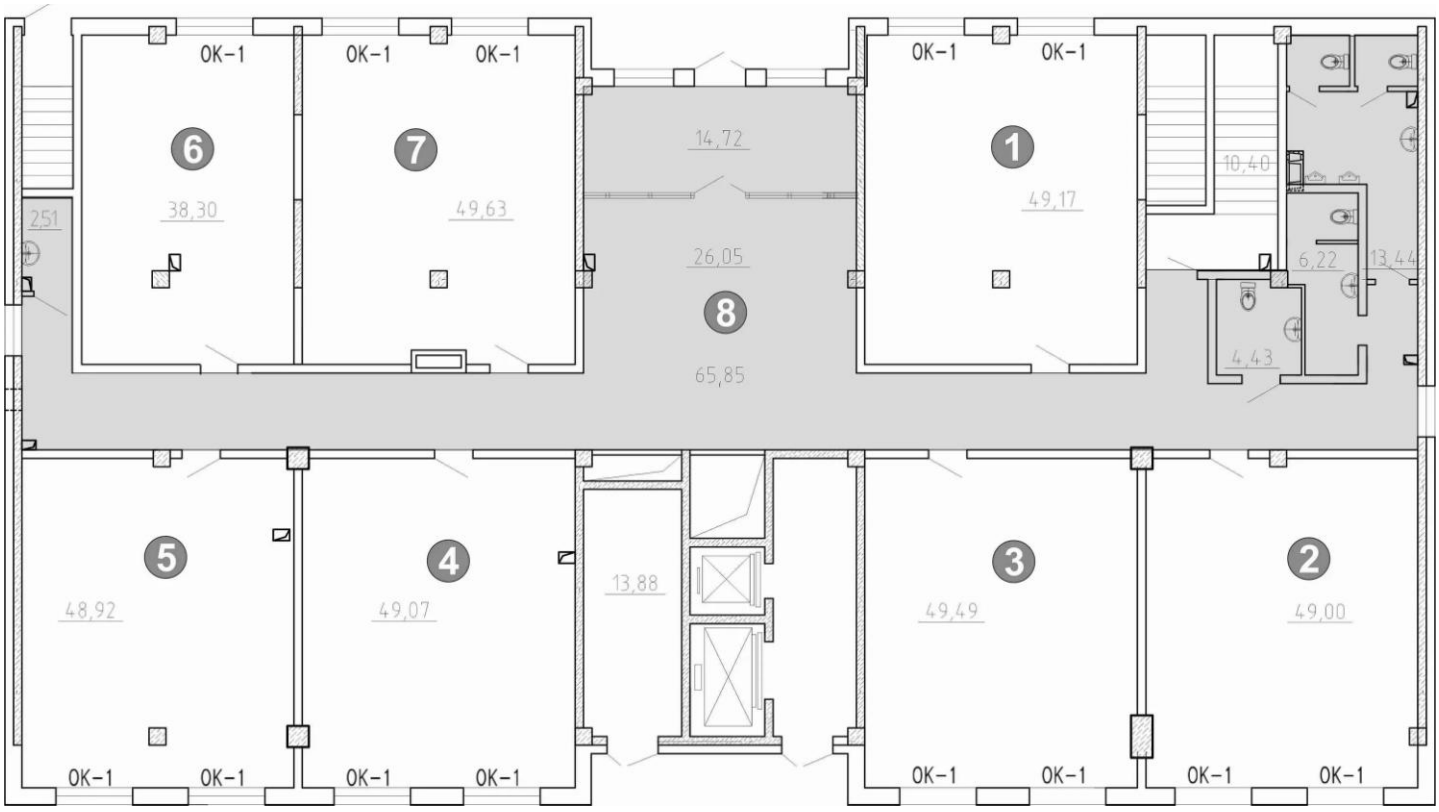
Объектом информатизации выступают данные обрабатываемые в ИС распределенной и параллельной обработки информации малого предприятия (СОД)

Задание 1 : Проведение описание помещения, в котором размещена / или будет размещена ИС (СОД)

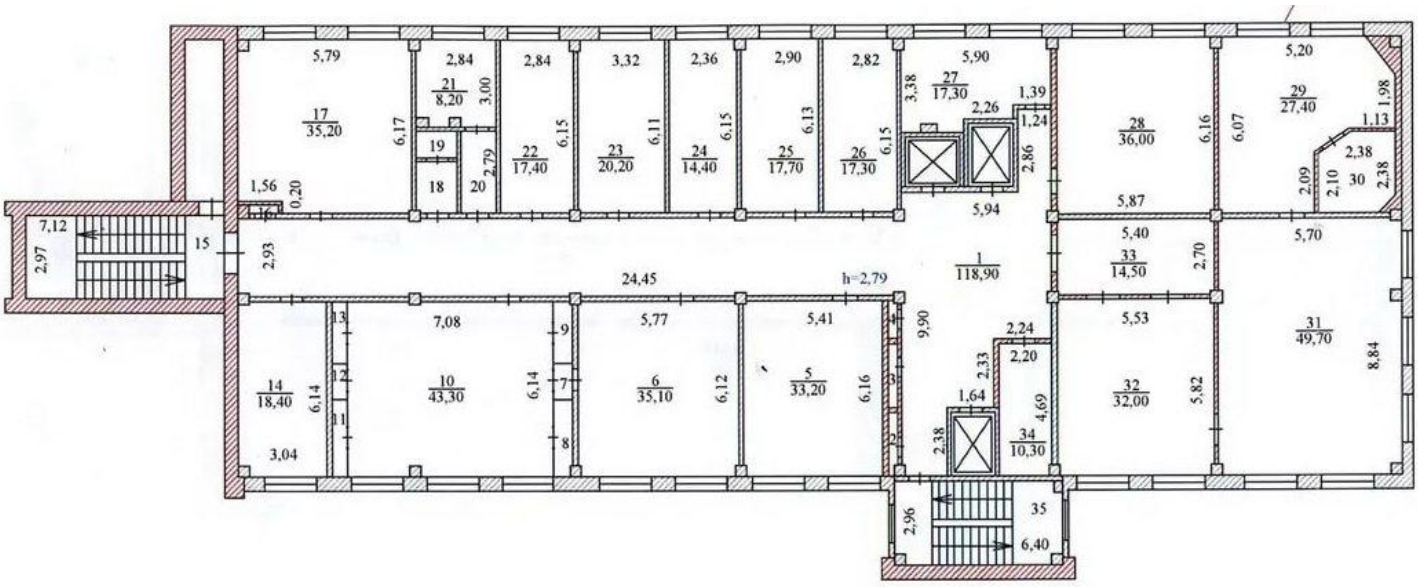
Занимаемое помещение малого предприятия состоит из _____ комнат:
Например:

1- переговорная
2- комната администратора сети и безопасности и бухгалтера;
3- серверная;
4- приемная секретаря;
5- кабинет генерального директора предприятия;
6- инженерный отдел;
7- отдел по внедрению проектов;
8- коридор;
9- лестница на этаж
10- смежное помещение (с/у);

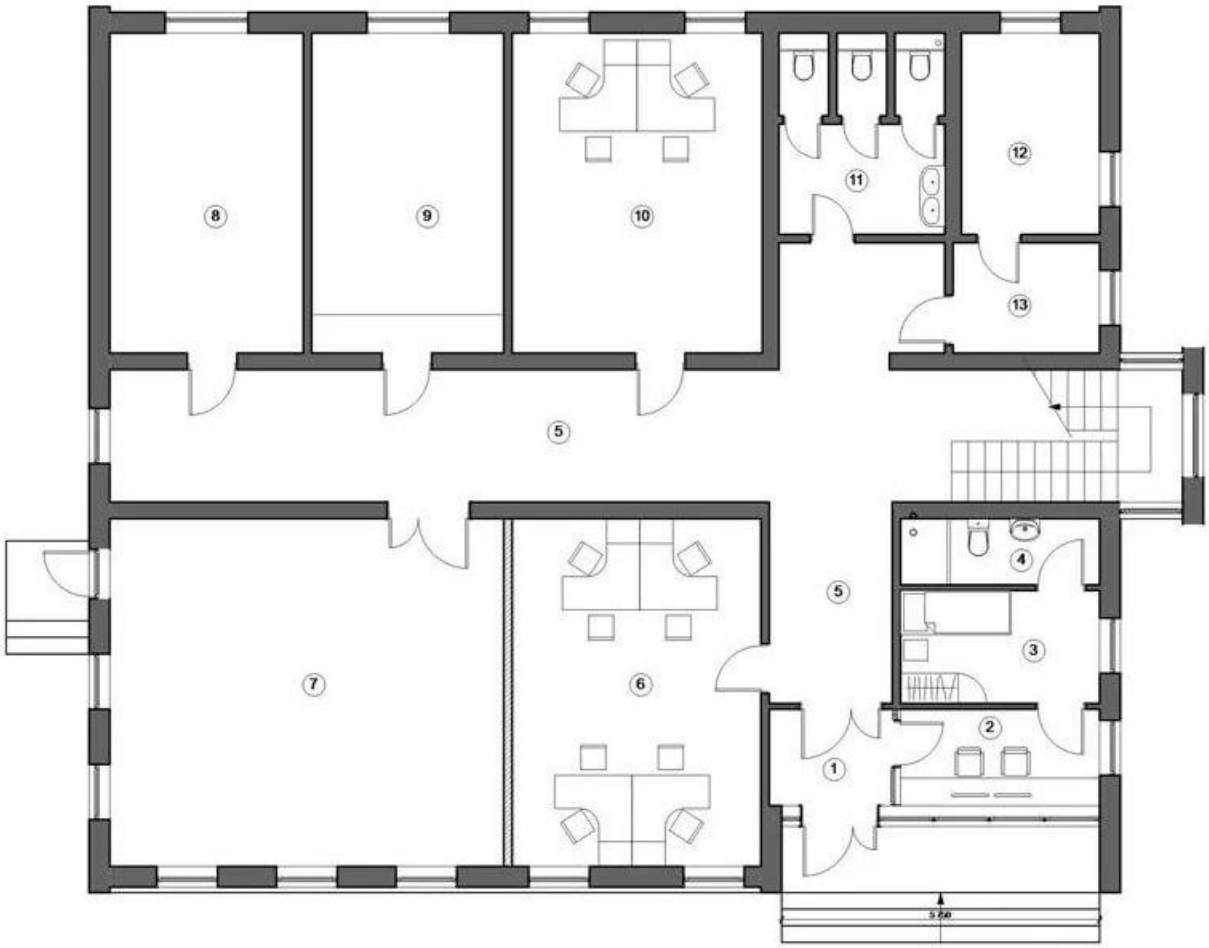
Номер в журнале группы = номер варианта задания (а значит и плана помещения)



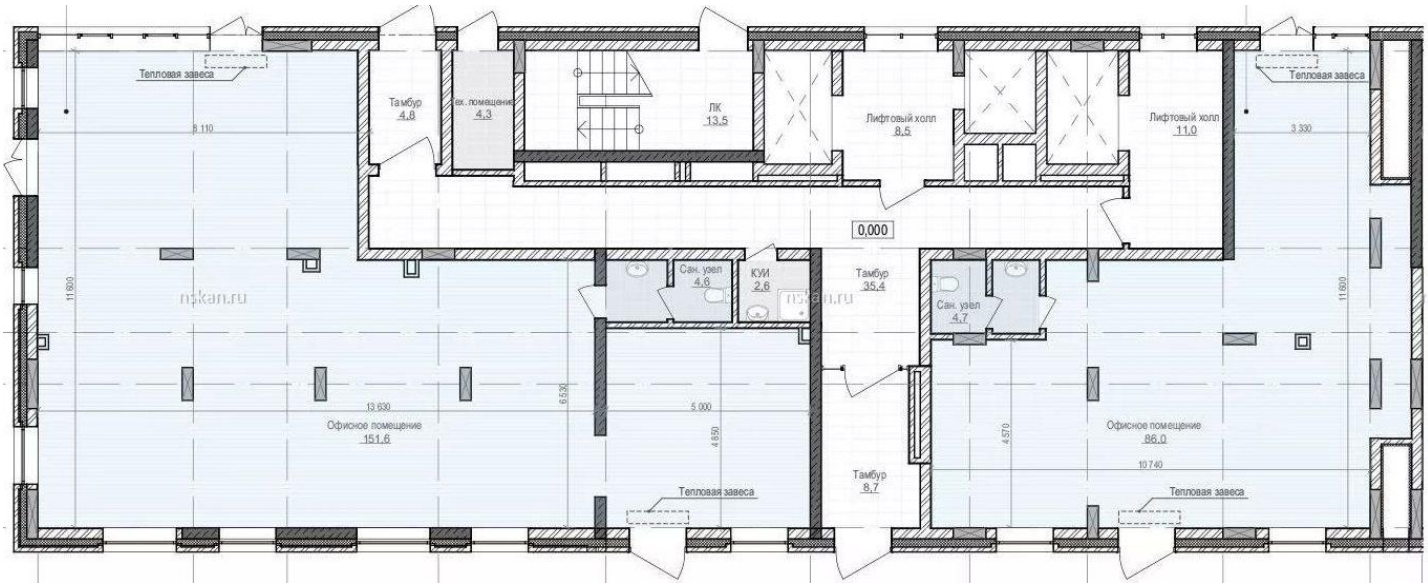
План 1 (вариант 1), верхний этаж



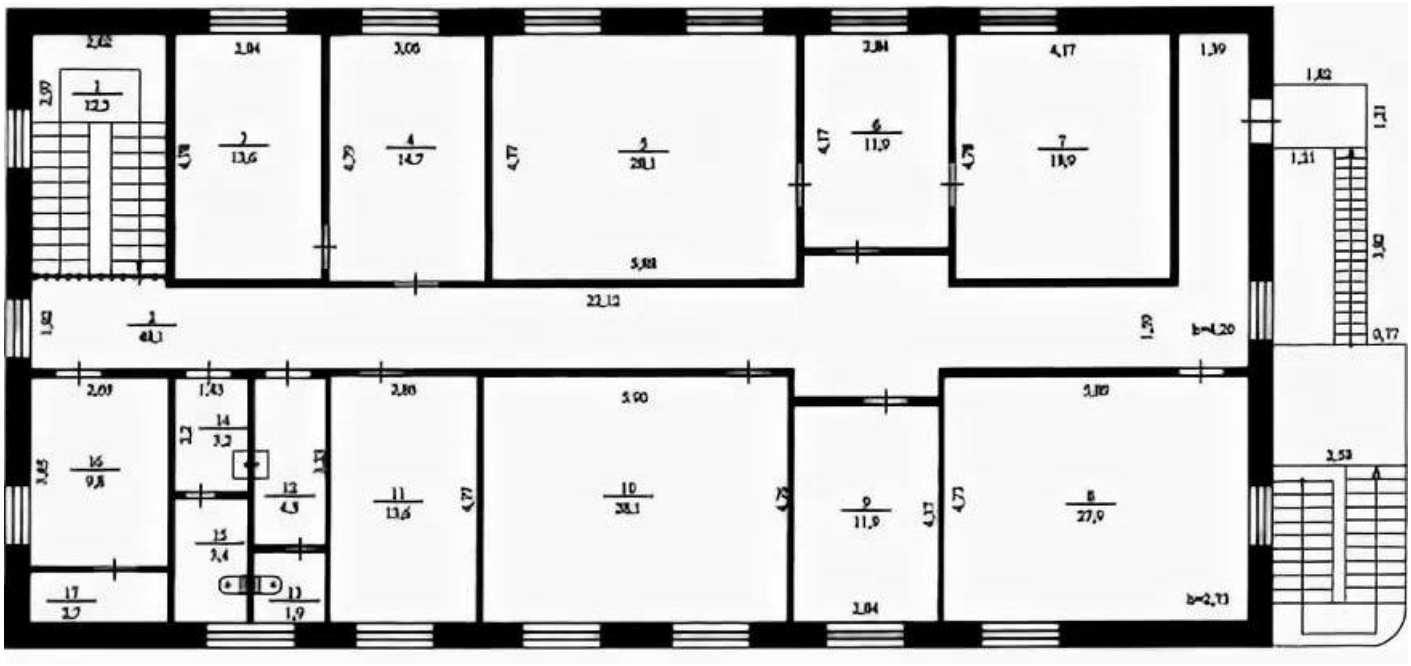
План 2 (вариант 2), нижний этаж



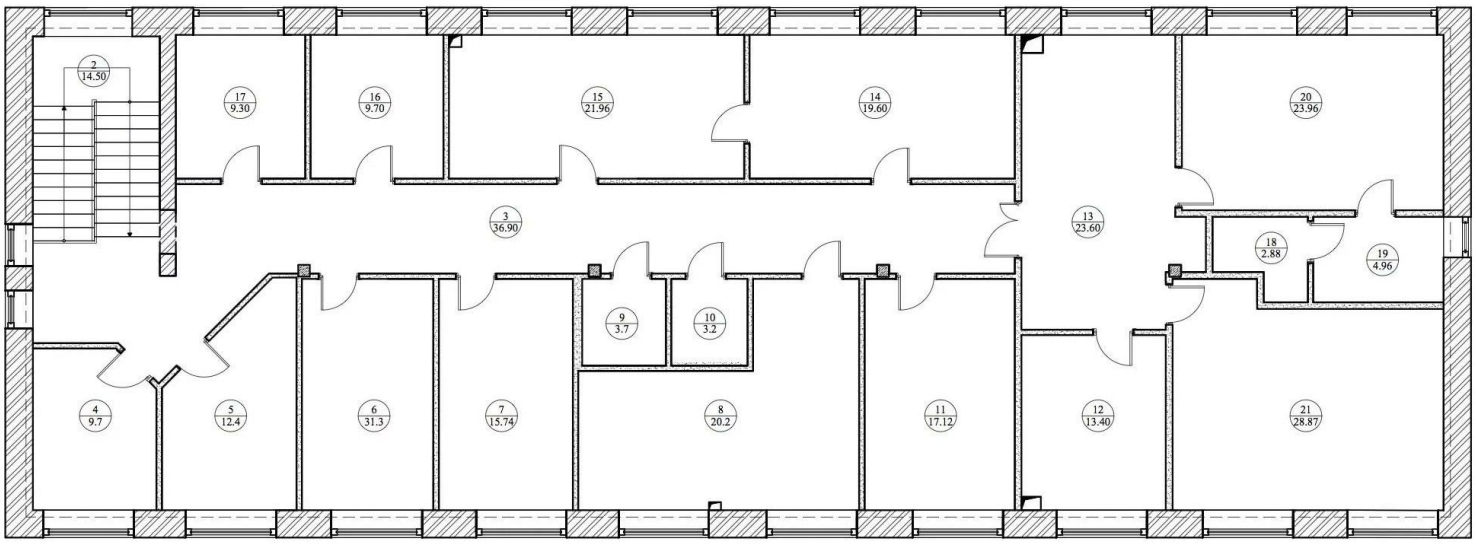
План3 (вариант 3), нижний этаж



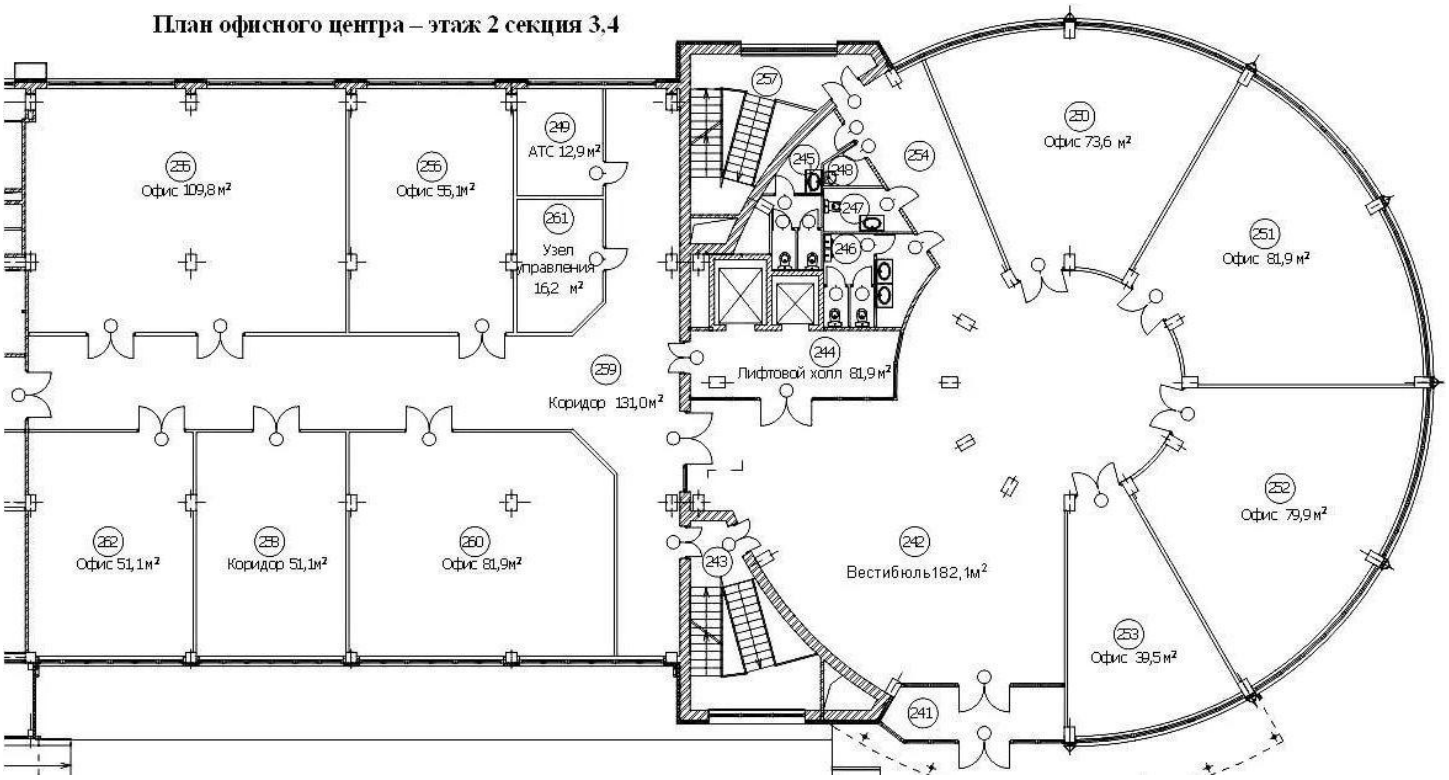
План 4 (вариант 4), в центре строения, входные двери трех сторон плана.



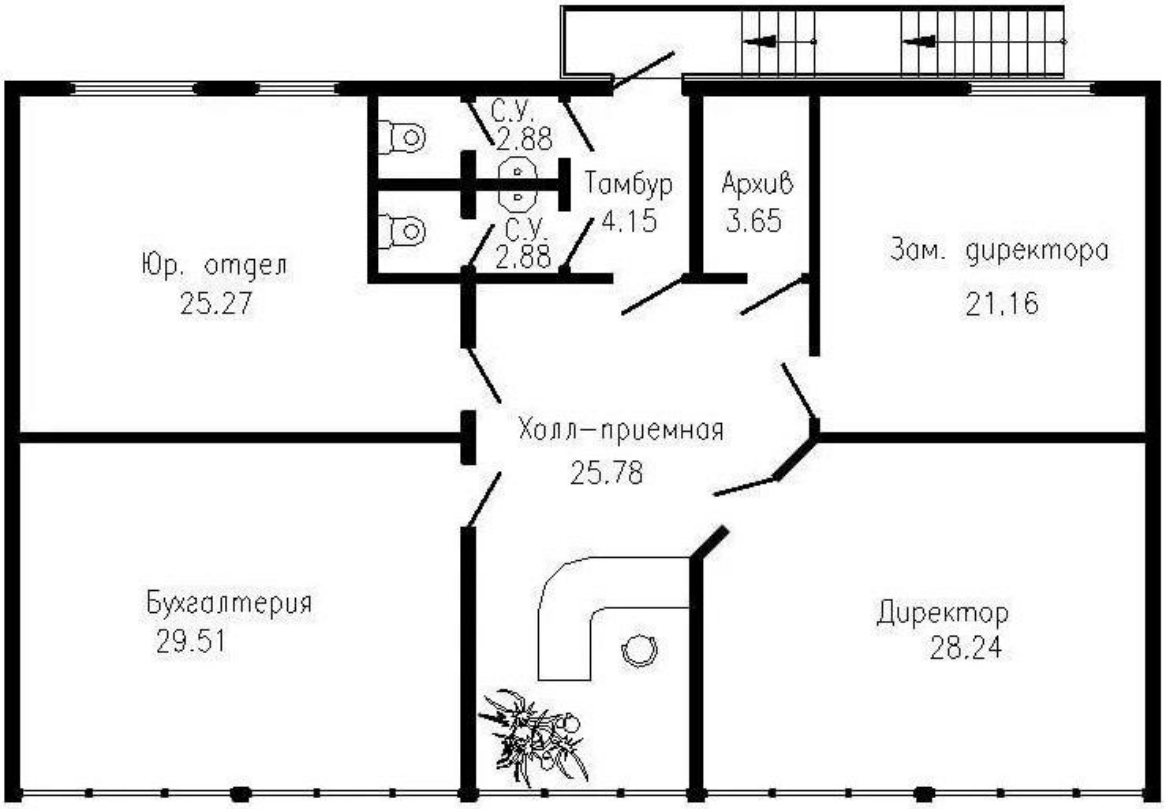
План 5 (вариант 5), на среднем этаже здания



План 6 (вариант 6), нижний первый этаж



План 7 (вариант 7), на среднем этаже офисного здания



План 8 (вариант 8), подвальное помещение

Задание 2 : Проведение описание иерархии сотрудников (пользователей) ИС (СОД) малого предприятия (по примеру)

Персонал состоит из постоянного и переменного состава:

Задание 3: Составление Рис. ___ Схема расположения рабочих мест с указанием оборудования СОД (на основе плана №___)

Указание «Условных обозначений» на рис____ (подробные обозначения, согласно таблице 1 настоящего задания.)

РАСПОЛОЖИТЕ РАБОЧИЕ МЕСТА СОД ОПТИМАЛЬНО В ПОМЕЩЕНИИ , ОСОБОЕ ВНИМАНИЕ УДЕЛЯЯ СЕРВЕРАМ

Задание 4: Определение перечня сведений конфиденциального характера СОД, подлежащих защите

Согласно данным задания (по вариантам) из Таблицы 2 описать специфику работы предприятия и особенности , обеспечения безопасности информации в ИС (СОД).

Пример:

Перечень сведений конфиденциального характера, подлежащих защите.

- Персональные данные заказчиков, полученные при выезде и осмотре объекта на котором предстоит построить СЗИ (адрес, телефон, план дома или предприятия, сведения, полученные при анкетировании, на предприятии заказчика).

Для обработки защищаемой информации используется _____ компьютера

- инженеров (комната 6) - 4
- специалистов по внедрению проектов (комната 7) – 2.
- зам. генерального директора (комната 7) - 1.

Специфика работы предприятия определяет ……..

Таблица 2 Распределение заданий по вариантам СОД

Номер плана помещения	**Категория информации, обрабатываемой в СОД**	**Работающая ОС (клиент и ОС серверная)**	**Политика ИБ**
1	Коммерческая тайна, ПДн	Linux	мандатная – ролевая
2	Коммерческая тайна, ПДн	Windows	дискреционная- ролевая
3	Коммерческая тайна, ПДн	Linux	мандатная – ролевая
4	Коммерческая тайна, ПДн	Windows	дискреционная– ролевая
5	Коммерческая тайна, ПДн	Linux	дискреционная– ролевая
6	Коммерческая тайна, ПДн	Windows	ролевая
7	Коммерческая тайна, ПДн	Windows	ролевая
8	Коммерческая тайна, ПДн	Linux	ролевая

ПДн– персональные данные.

Задание 5: Согласно варианту и заданию в таблице 2

Заполнить таблицу 3 для каждого критического элемента СОД при ролевой политике безопасности

Таблица 3. Матрица разграничения привилегий пользователей БД СОД

USER_NAME	SELECT	DELETE	INSERT	UPDATE	EXECUTE	With grand option	Password
должность	Y			Y	Y		******(1) **** (2) ******(3) ********(4)
должность	Y	Y	Y	Y	Y		***** (1) *****(2)
должность	Y	Y	Y	Y	Y	Y	*********
	Y			Y	Y		*******
должность	Y						*****

Запросы:
SELECT – извлечение записей.
DELETE - удаление записи
INSERT - добавление записи
UPDATE - редактирование записи
EXECUTE - выполнение
With grand option – с правами наследования
Password - пароль для входа в БД , у каждого свой ,на месяц, выдается (SYSDBA).

Задание 6: определение основных объектов защиты СОД малого предприятия

Объекты ЗИ (объекты информатизации) :

O_1–
O_2–
O_3–
O_4–
…
O_X–

Пример:

Основными объектами защиты на предприятии «Амулет» являются:
данные обрабатываемые в СОД предприятия, отнесенные в соответствии с действующим законодательством к персональной тайне, (в дальнейшем - защищаемой информации);

Объекты ЗИ:

Согласно ГОСТ Р 50922-96 «Защита информации: Основные термины и определения» дает следующее определение объекта защиты:

Объект защиты – информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Согласно этому определению, к объектам защиты должны относиться:
1. лица, допущенные к работе с охраняемой законом информацией либо имеющие доступ в помещения, где эта информация обрабатывается;
2. объекты информатизации – средства и системы информатизации, технические средства приема, передачи и обработки информации, помещения, в которых они установлены, а также помещения, предназначенные для проведения служебных совещаний, заседаний и переговоров;

Объекты ЗИ:
О1 - компьютеры, на которых обрабатывается, хранится и передается выделенная информация;
О2 – отчуждаемые носители информации (выдаваемые специалистам по внедрению проектов и для их работы с заказчиками, выезд на объект)
О3 – устройства принтер-сканер – копир
О4 – серверная
О5 - система безопасности, система доступа
Следует также учесть
О6- бумажная документация с важной информацией, анкеты (содержащие ответы Заказчика о структуре предприятия, сети, организации предприятия, адрес, сведения о распорядке дня заказчика, состава семьи и т.д)
В связи с гарантией Заказчика, что бумажная документация с важной информацией после внесения в ИС предприятия уничтожается (с помощью шредера) – данный объект рассматриваться не будет.

Задание 7: составление архитектуры СОД малого предприятия (на основе данных таблицы 1, теоретического опыта лекционных занятий по дисциплине «Проектирование систем распределенной и параллельной обработки данных»)

Задание 8: определение перечня угроз на объекты защиты СОД (ИС) малого предприятия

(ЧЕМ БОЛЬШЕЕ ЧИСЛО УГРОЗ БУДЕТ ОПРЕДЕЛЕНО, ТЕМ ЛУЧШЕ)

>= 15

Задание 9: Составление модели угроз объектов информатизации СОД (ИС)

Порядок составление модели угроз будет рассмотрен на лекции

Объекты информатизации СОД	угрозы объектов информатизации
>= 6	>= 15

Задание 10: из Таблицы 4 путем удаления лишних элементов – оставить в каждом из обязательных 23 программных продуктов по одному наименованию ПП (или обосновать почему нужно несколько)

Таблица 4 перечень программных продуктов, которые будут закупаться Заказчиком для СОД по Вашей рекомендации

Название программного продукта для СЗИ СОД малого предприятия
1. Межсетевые экраны
Juniper
Checkpoint
Cisco ASA, FWSM
Microsoft ForeFront (бывшая ISA)
Z-2
Атликс
2. Системы обнаружения вторжений
Juniper IDP
Checkpoint IPS
Cisco IPS
3. Защита каналов связи (ГОСТ)
S-Terra
VipNet CUSTOM

ТРОПА
Заслон, Сито
Атликс VPN
Checkpoint + Crypto PRO Checkpoint Crypto PRO
4. Контроль сетевых подключений
Cisco NAC
RADIUS
Juniper
Cisco ACS
4. Антивирусное ПО
Symantec
Kaspersky
Dr Web
5. СЗИ НСД
Dallas Lock
Блок-хост сеть
Аккорд/NT 2000
Соболь/SecretNet SecretNet TouchMemory Card
Страж
6. Хостовые IDS
Cisco Securty Agent
Symantec Critical System Protection /SEP
Checkpoint HIDS
7. Сканеры безопасности
XSpider
MaxPatrol
App Detective
8. Контроль подключения внешних устройств СОД
Z-Lock
Lumension Device Control
Device Lock
9. Шифрование носителей информации
Aladdin SecretDisk
zServer
10. PKI (Удостоверяющие центры)
КриптоПро УЦ
MS CA
Keon (Certificate Manager)
11. HSM
Атликс HSM
nCipher
12. Tokens
RSA SecureID
eToken/NG/Java +TMS
eToken OTP
13. Контроль целостности
Tripwire Enterprise

14. Защита СУБД СОД
IBM Guardium
Imperva
15. Анализ уязвимостей и compliance
MaxPatrol
Lumencion
Qualys
Symantec Control Compliance Suite
16. Сбор и анализ корреляции событий
ArcSight ESM и Express
Symantec SIM
RSA enVision
Cisco MARS
netForensics SIM One
17. DLP
Дозор
Symantec DLP
RSA, Codegreen
18. Контроль доступа в Интернет
Дозор
Blue Coat
IronPort серии S
Optenet
eSafe
19. Электронная почта СОД
Microsoft Exchange
Communigate Pro
IronPort серии C
ProofPoint
20. Identity Management
Oracle Identity Manager
IBM Tivoli Identity Manager
SAP Netweaver Identity Manager
Sun Identity Manager
Microsoft Forefront Identity Manager
21. Access Management
Oracle AM
IBM Tivoli AM
Oracle eSSO
Rainbow/ActiveIdentity eSSO
IBM eSSO
22. Rights Management
Oracle IRM
Microsoft RMS
23. GRC

SAP GRC
Oracle GRC

11. Hardware security module (HSM) — аппаратное вычислительное устройство, предназначенное для безопасного осуществления криптографических операций. HSM содержит специальный криптопроцессор, предназначенный для высокоскоросного выполнения криптографических процедур. Крупнейшие производители HSM на мировом рынке: Thales, SafeNet, Utimaco.

20. Управление учётными данными (англ. Identity management, сокр. IdM, иногда IDM) — комплекс подходов, практик, технологий и специальных программных средств для управления учётными данными пользователей, системами контроля и управления доступом (СКУД), с целью повышения безопасности и производительности информационных систем при одновременном снижении затрат, оптимизации времени простоя и сокращения количества повторяющихся задач.

23. GRC – обеспечение постоянной взаимосвязи трех основных компонентов, по которым можно разложить деятельность практически любой компании: корпоративное управление (governance), управление рисками (risk) и соблюдение требований (compliance).

В качестве основных называются стандарты по управлению ИТ и организации ИБ, такие как COBIT, ISO 17799:2005 (BS 7799), ISO 27001:2005.

Из технологических стандартов, как считают эксперты, создатели СОД прежде всего должны придерживаться следующих:

- ✓ общие стандарты по информационной безопасности - XKMS, PKI, XML-SIG, XML-ENC, SSL/TLS, PKCS, S/MIME, LDAP, Kerberos, X.509 и др.;
- ✓ стандарты по обмену идентификационными данными пользователей - SAML, WS-Fed, XACML, SPML и др.;
- ✓ стандарты интеграции - WSDL, WSRP, JSR-115, JCP, SOAP и др.;
- ✓ стандарты Web-сервисов - WS-Security, WS-Fed, WS-Policy, WS-Trust и др.;
- ✓ стандарты служб каталогов - X.500, DSML, LDAP, JDBC и др.

Задание 11: Составление итоговой архитектуры СОД малого предприятия с архитектурой системы защиты информации при размещении в помещении

архитектуры СОД (итог задания 7) и архитектуры ПП Таблицы 4 вместе

Задание 12 : составление отчета по требования оформления , предъявляемым к отчетам по дисциплине ПСРиПОД.

РЕКОМЕНДУЕМЫЕ ИСТОЧНИКИ

1. Руководящий документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», https://fstec.ru/component/attachments/download/289 (дата обращения 29.04.2019г).

2. Статья «Система идентификации и управления доступом Identity and Access Management (IdM, IAM)», http://www.tadviser.ru/index.php/Статья:Identity_and_Access_Management_-_определения (дата обращения 29.04.2019г).