Презентация по курсовой работе на тему:

“Разработка комплексной системы защиты информации предприятия ОПК «Спецсвязьремонт»”

Выполнил :
Студент 5 курса группы 100502-ЗИСа-о18
Педан А.О.

ВВЕДЕНИЕ

- В современном мире для хранения, обработки и передачи различного рода информации широко используются информационные технологии. В связи с этим значительно возросло число информационных атак, приводящих к значительным финансовым и материальным потерям во всех направлениях деятельности человека, в том числе в результате утечек конфиденциальной информации.
- Создание комплексной системы защиты информации отражает системный подход к обеспечению информационной безопасности компании, предотвращению хищений и утечек информации ограниченного доступа, а также оптимизирует работу ИТ-системы предприятия, снижает капитальные и операционные затраты компании.

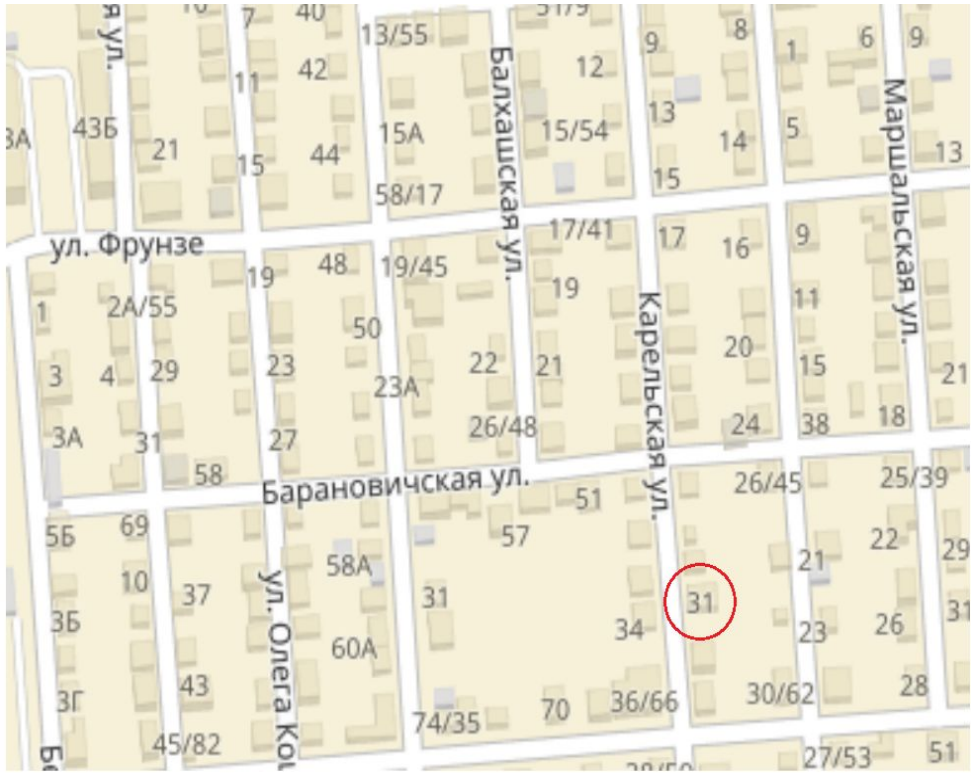
Цель работы

- Создание комплексной системы защиты информации на ОПК «Спецсвязьремонт».

Исходные данные по объекту:

Наименование организации: ОПК «Спецсвязьремонт»

Расположение объекта: Объект расположен по адресу г. Барнаул ул. Карельская 31



План-схема объекта ОПК «Спецсвязьремонт»

Защищаемые активы

Виды активов:

- Коммерческая тайна:
  - договоры;
  - технологии;
- Служебная тайна:
  - системы зашиты;
  - режимные мероприятия;
- Персональные данные:
  - специальные;
  - биометрические;
  - общедоступные;
  - иные.

Классификация объекта

Категории субъектов персональных данных	Обрабатываются персональные данные;
Категории обрабатываемых персональных данных	В ГИС «ОПК «Спецсвязьремонт»» обрабатываются общие, специальные, биометрические и иные категории персональных данных
Количество субъектов персональных данных	В ГИС «ОПК «Спецсвязьремонт»» предполагается обработка персональных данных более ста тысяч субъектов
Тип актуальных угроз	В ГИС «ОПК «Спецсвязьремонт»» не являются актуальными угрозы НДВ в прикладном и системном ПО (3 тип), поскольку используются сертифицированные версии прикладного и общесистемного ПО

	Общедоступные	Специальные	Биометрические	Иные
Сотрудники	1163	1163	1163	1163
Клиенты	214214	214214	214214	214214

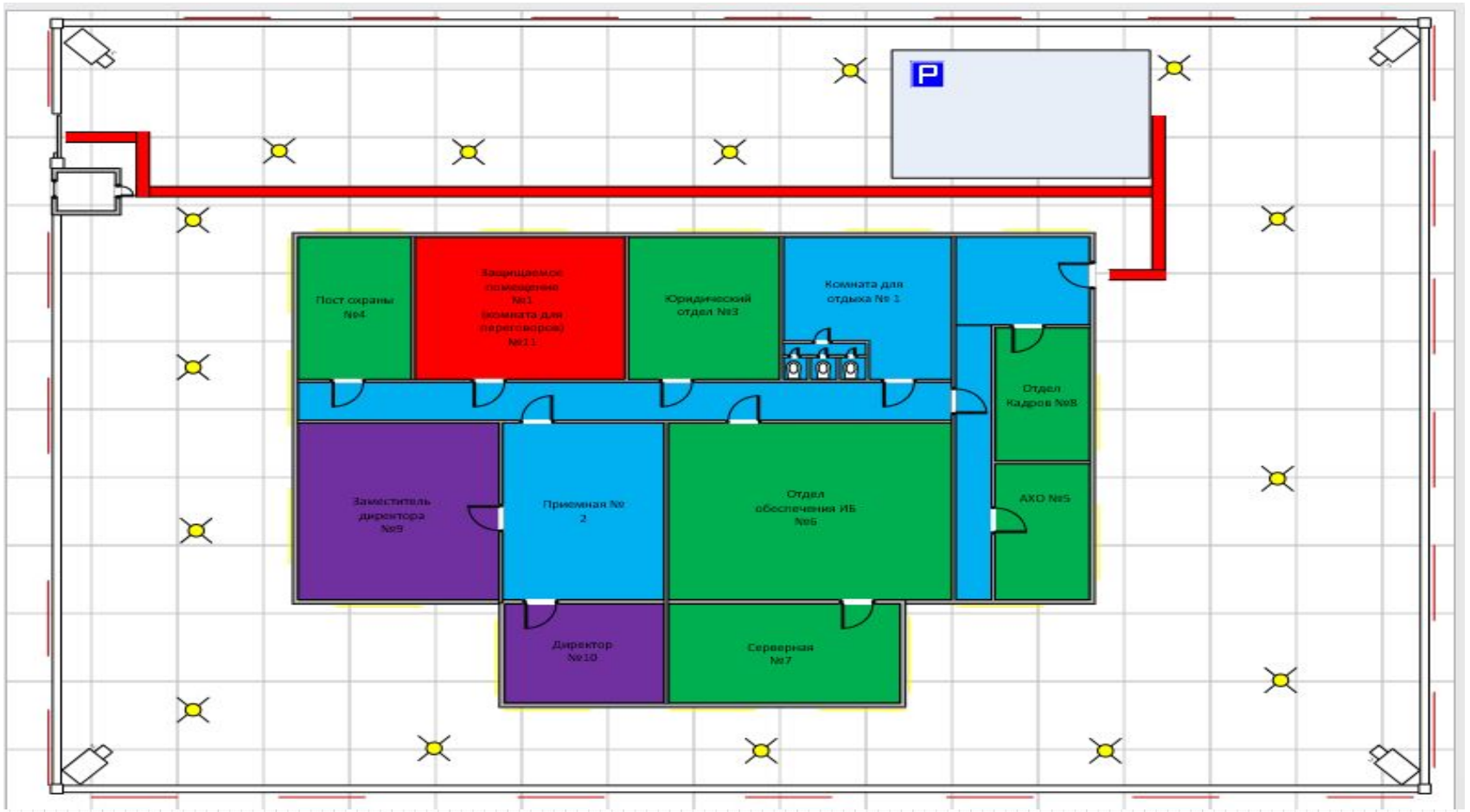
Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1 (НДВ ОС)	2 (НДВ ПО)	3 (Без НДВ)
ИСПДн-С (специальные)	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б (биометрические)			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И (иные)	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О (общедоступные)	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4

На основании полученных данных, согласно порядку определения уровня защищенности персональных данных, приведенному в Постановлении Правительства РФ № 1119 от 01.11.2012, комиссией **для персональных данных, обрабатываемых в ГИС «ОПК «Спецсвязьремонт»» установлена необходимость обеспечить по наивысшему уровню– второй уровень защищенности (УЗ-2)**.

Комиссией для ГИС «ОПК «Спецсвязьремонт»» установлен **итоговый средний уровень значимости информации (УЗ – 2).**

На основании полученных данных и согласно Приложению № 1 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России № 17 от 11 февраля 2013 года, **ГИС «ОПК «Спецсвязьремонт»» комиссией присвоен класс защищенности К2.**

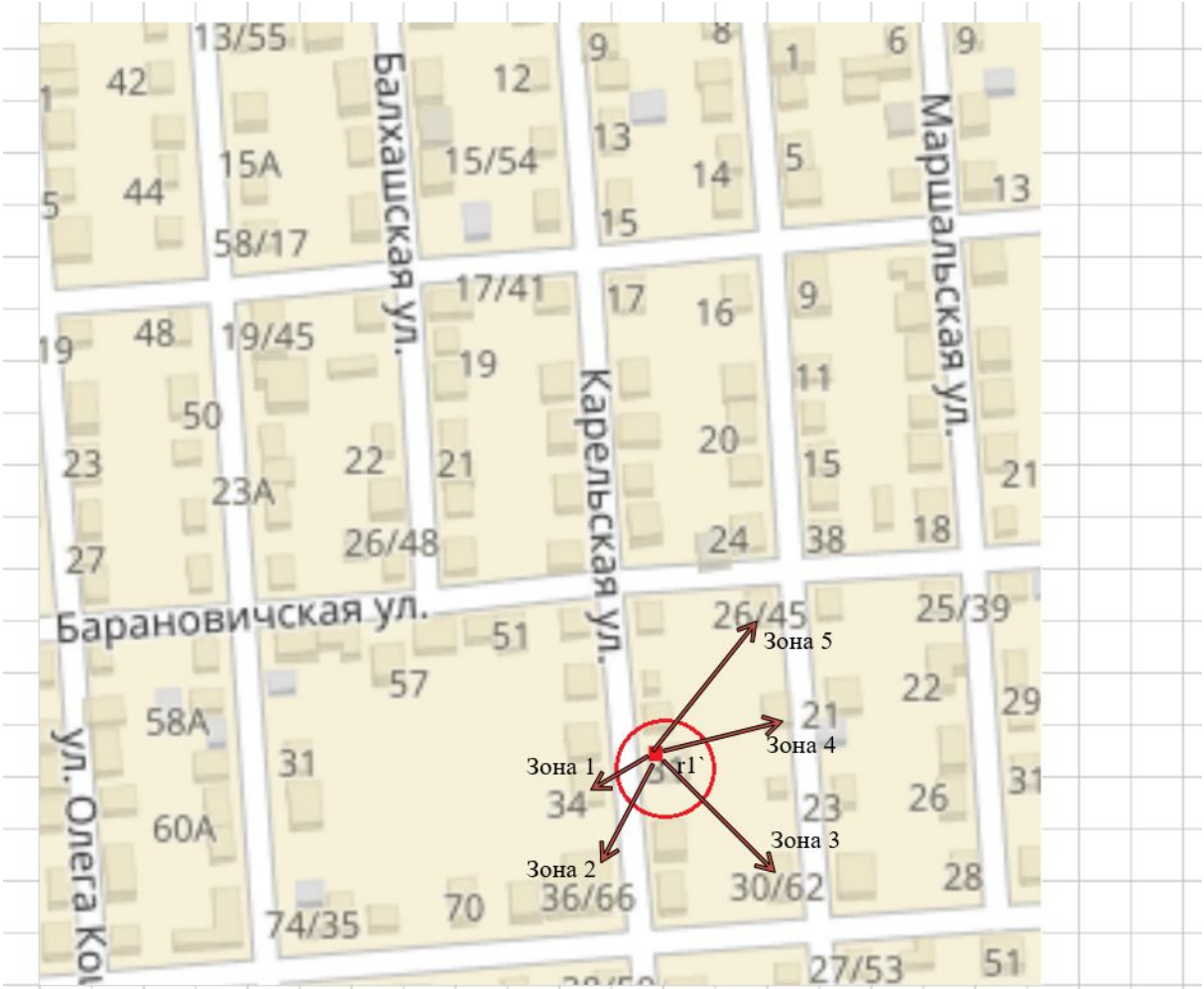
Схема территории объекта



В организации ОПК «Спецсвязьремонт» действует несколько отделов:

- IT – отдел;
- Отдел технической поддержки;
- Административно – хозяйственный отдел;
- Юридический отдел
- Отдел кадров;
- Финансовый отдел;
- Отдел информационной безопасности;
- Отдел информационного обеспечения;
- Бэк-офис (перационно-учётное подразделение, обеспечивающее работу подразделений, участвующих в управлении активами и пассивами организации).

Зоны разведки в ОПК «Спецсвязьремонт»



r1` - Зона показателя защищенности

- Защищаемое помещение

Зона 1 – Визуальная разведка

Зона 2 – Оптическая разведка

Зона 3 – Виброаккустическая разведка

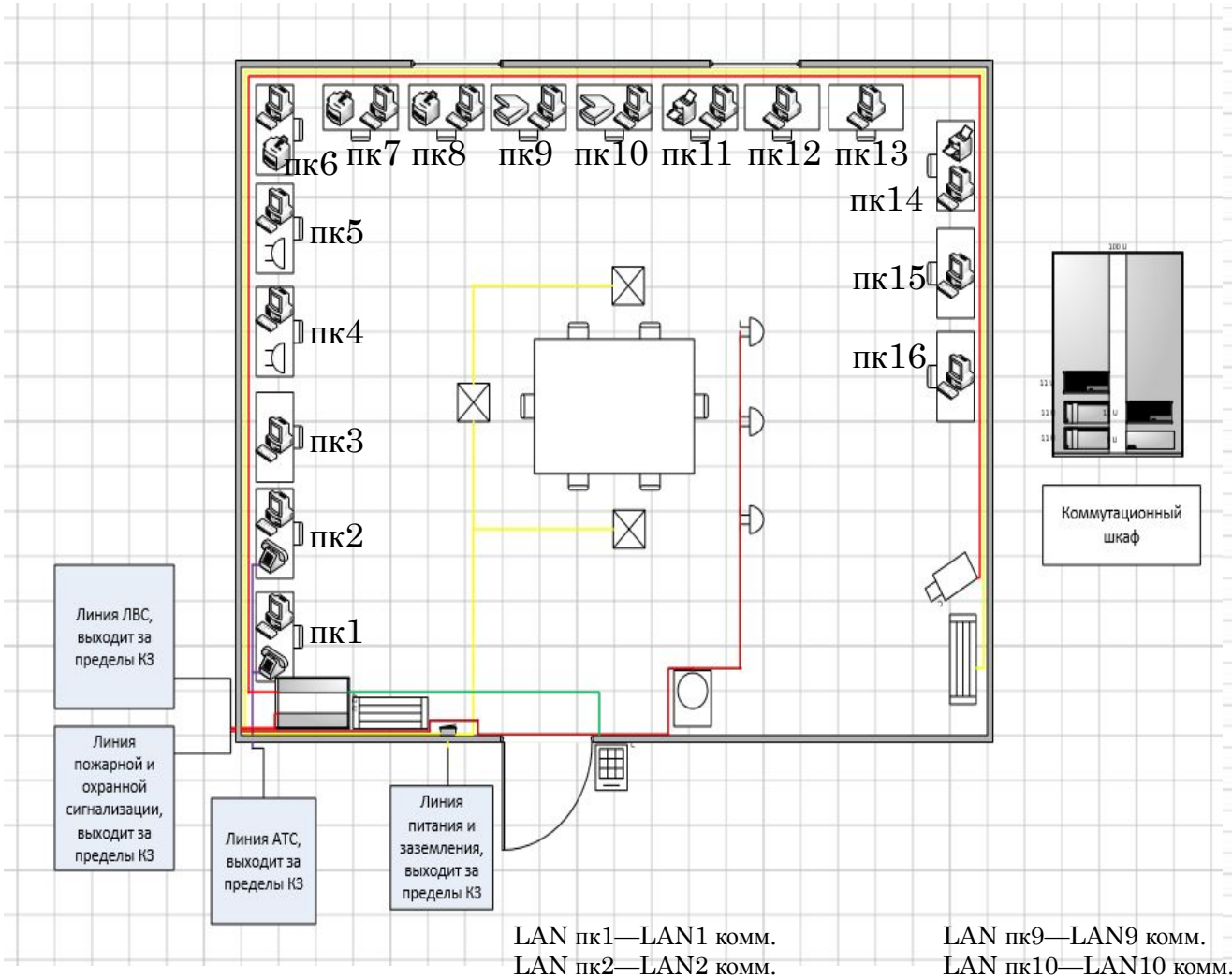
Зона 4 – НЧ АЭП

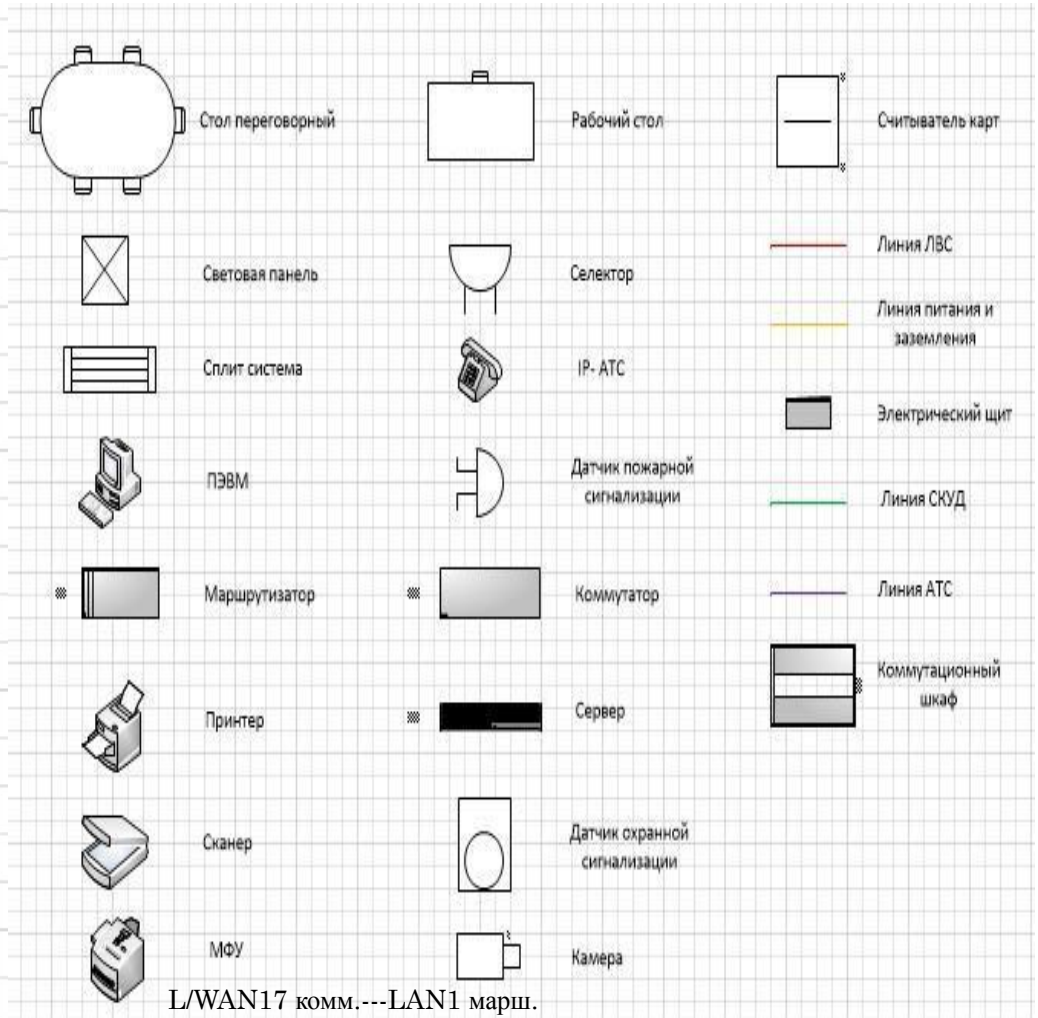
Зона 5 – Радиоразведка

В указанных зонах могут вести такую разведку, как:

1. Визуальную разведку;
2. Оптическую разведку;
3. НЧ АЭП;
4. Радиоразведку;
5. Виброаккустическую разведку.

Схема ОТСС и ВТСС защищаемого помещения Комната для переговоров)



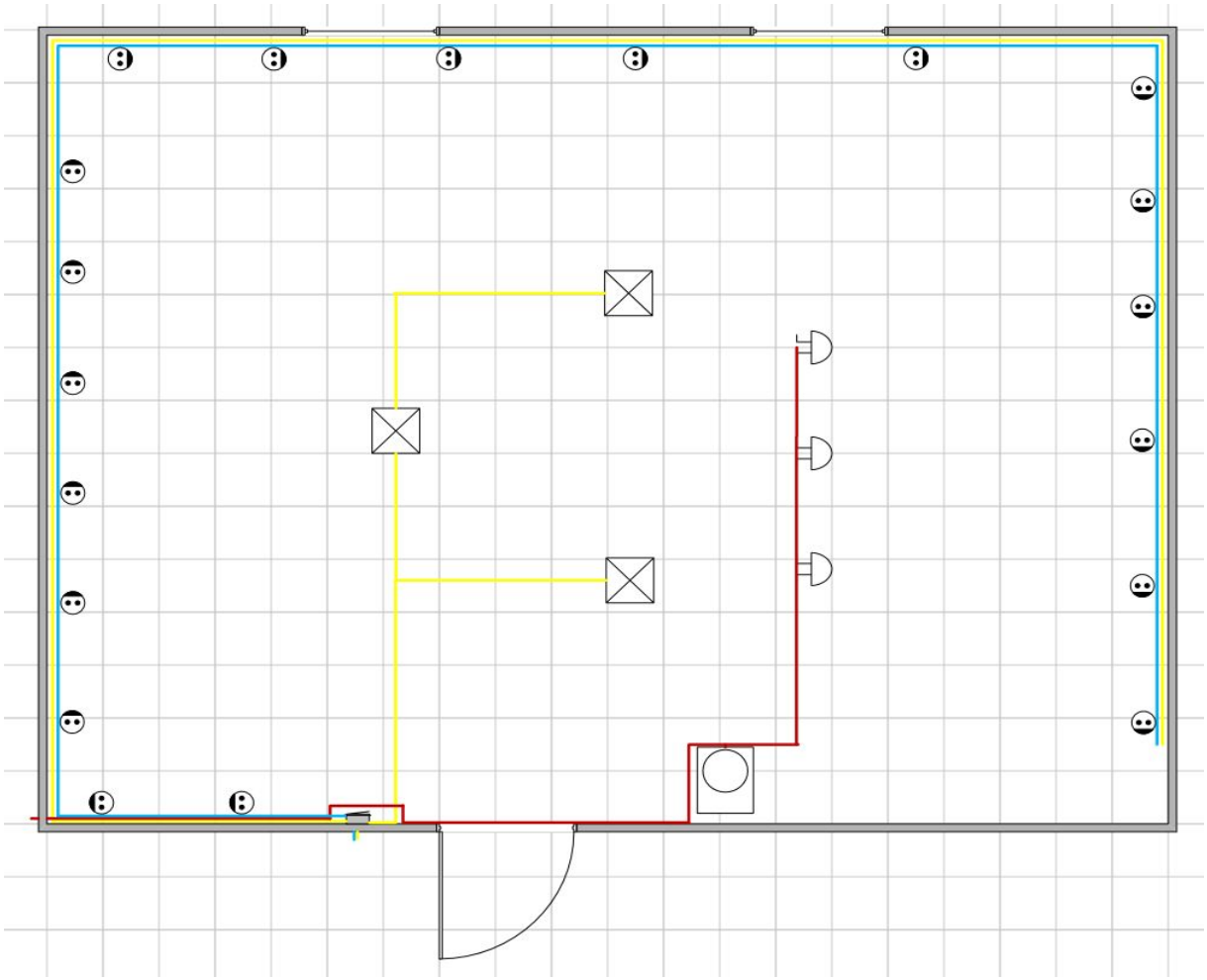


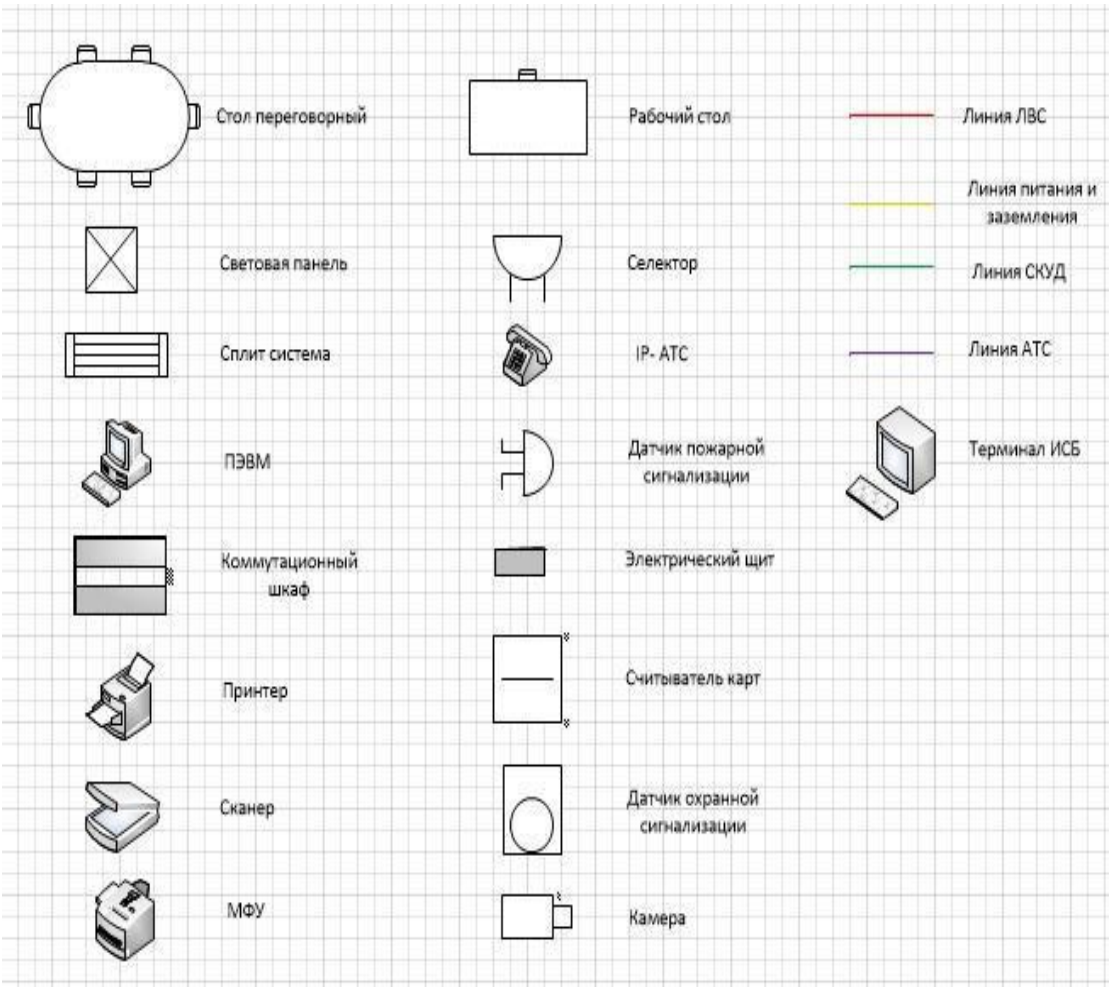
LAN пк1—LAN1 комм.
LAN пк2—LAN2 комм.
LAN пк3—LAN3 комм.
LAN пк4—LAN4 комм.
LAN пк5—LAN5 комм.
LAN пк6—LAN6 комм.
LAN пк7—LAN7 комм.
LAN пк8—LAN8 комм.

LAN пк9—LAN9 комм.
LAN пк10—LAN10 комм.
LAN пк11—LAN11 комм.
LAN пк12—LAN12 комм.
LAN пк13—LAN13 комм.
LAN пк14—LAN14 комм.
LAN пк15—LAN15 комм.
LAN пк16—LAN16 комм.

L/WAN17 комм.---LAN1 марш.
WAN марш.--- Internet

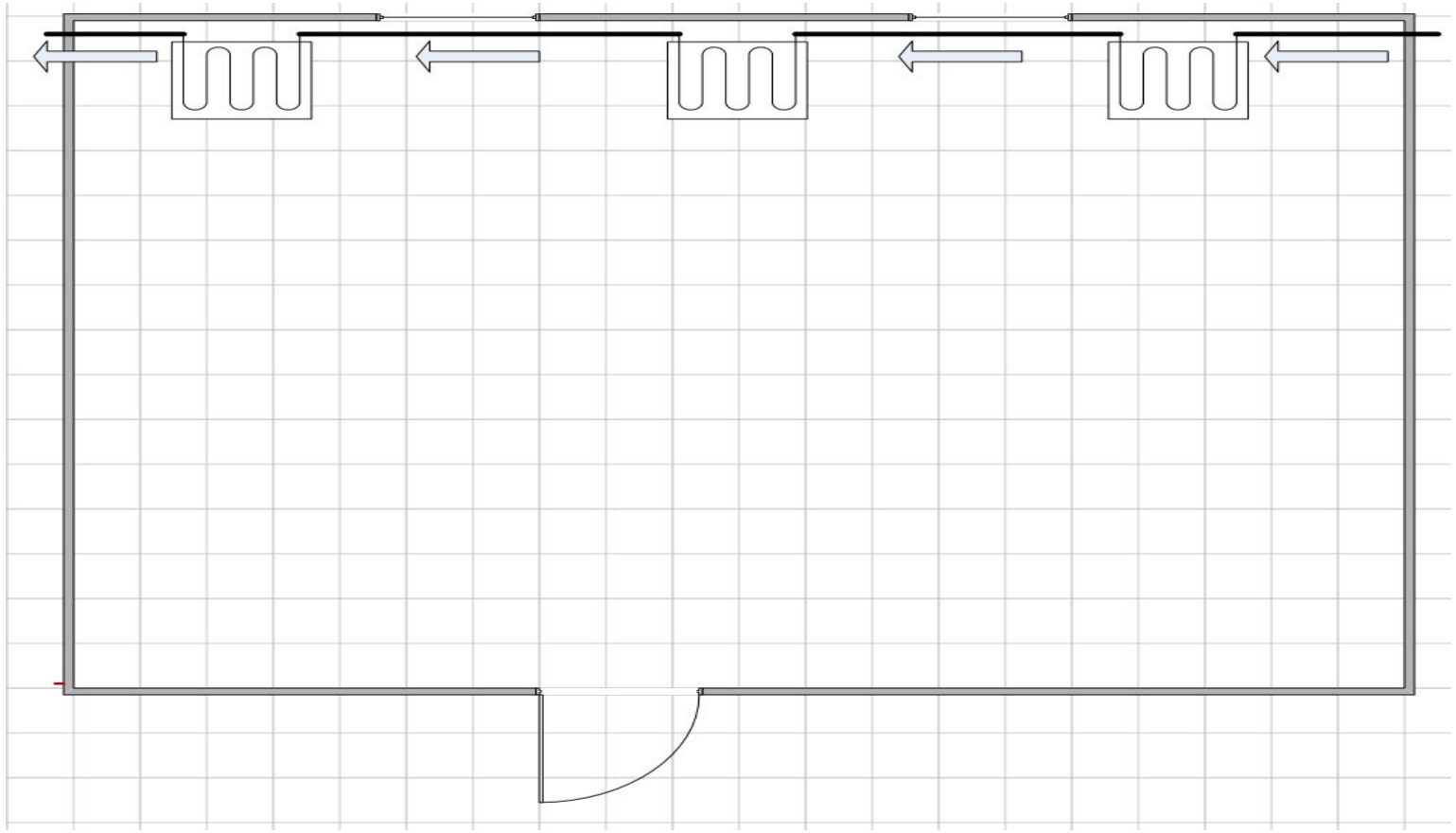
Схема электропитания защищаемого помещения (Комната для переговоров)





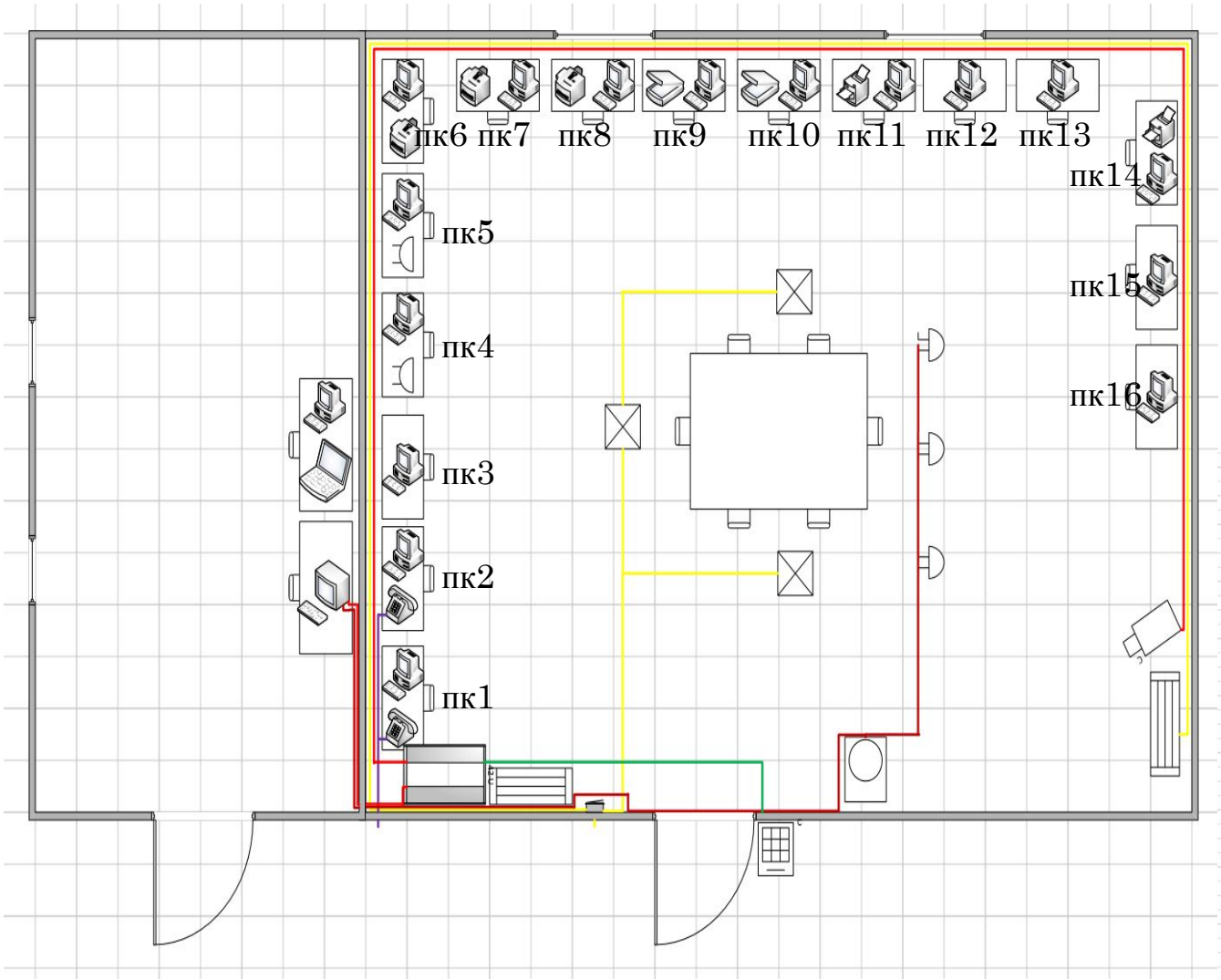
В защищаемом помещении используется 2 вида заземления: контурное заземление, на которое выведены все ОТСС, и заземление электрического щитка, которое тем самым заземляет всё электроснабжение в пределах КЗ. Подробная схема заземления и электроснабжения представлена на рис.

Схема коммуникаций защищаемого помещения (Комната для переговоров)



В защищаемом помещении система коммуникаций состоит из системы отопления в виде 3-х батарей в одном помещении. Подробная схема коммуникаций представлена на рис.

Схема комплексной системы безопасности (Комната для переговоров)



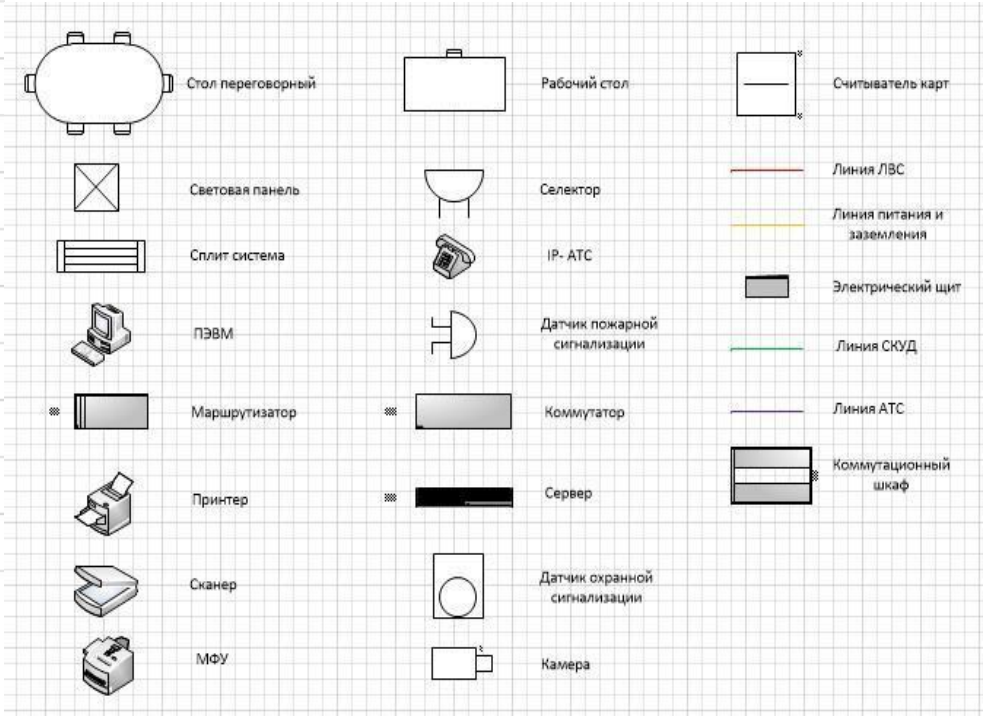


Схема ТКУИ защищаемых помещений (Комната для переговоров)

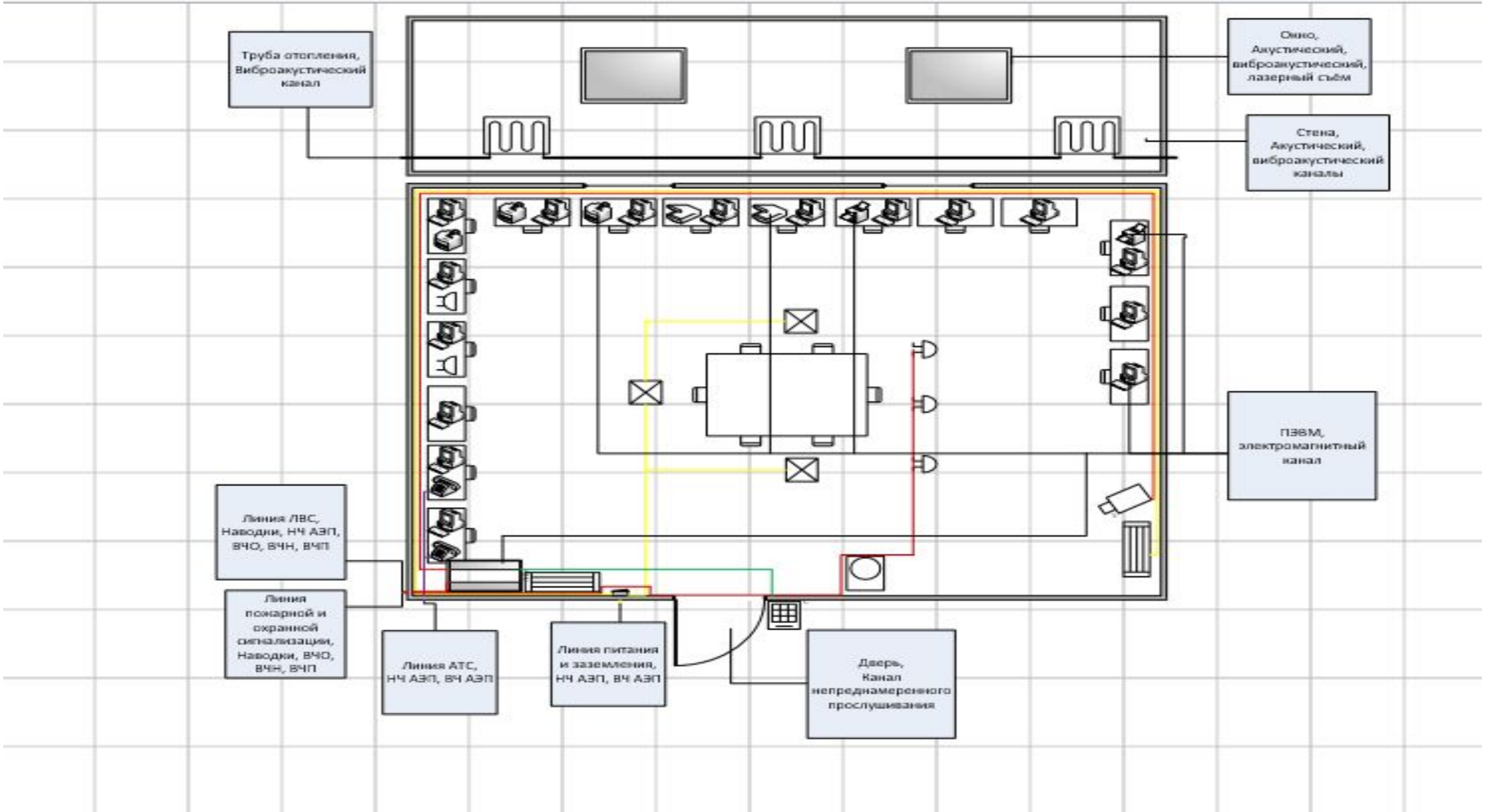
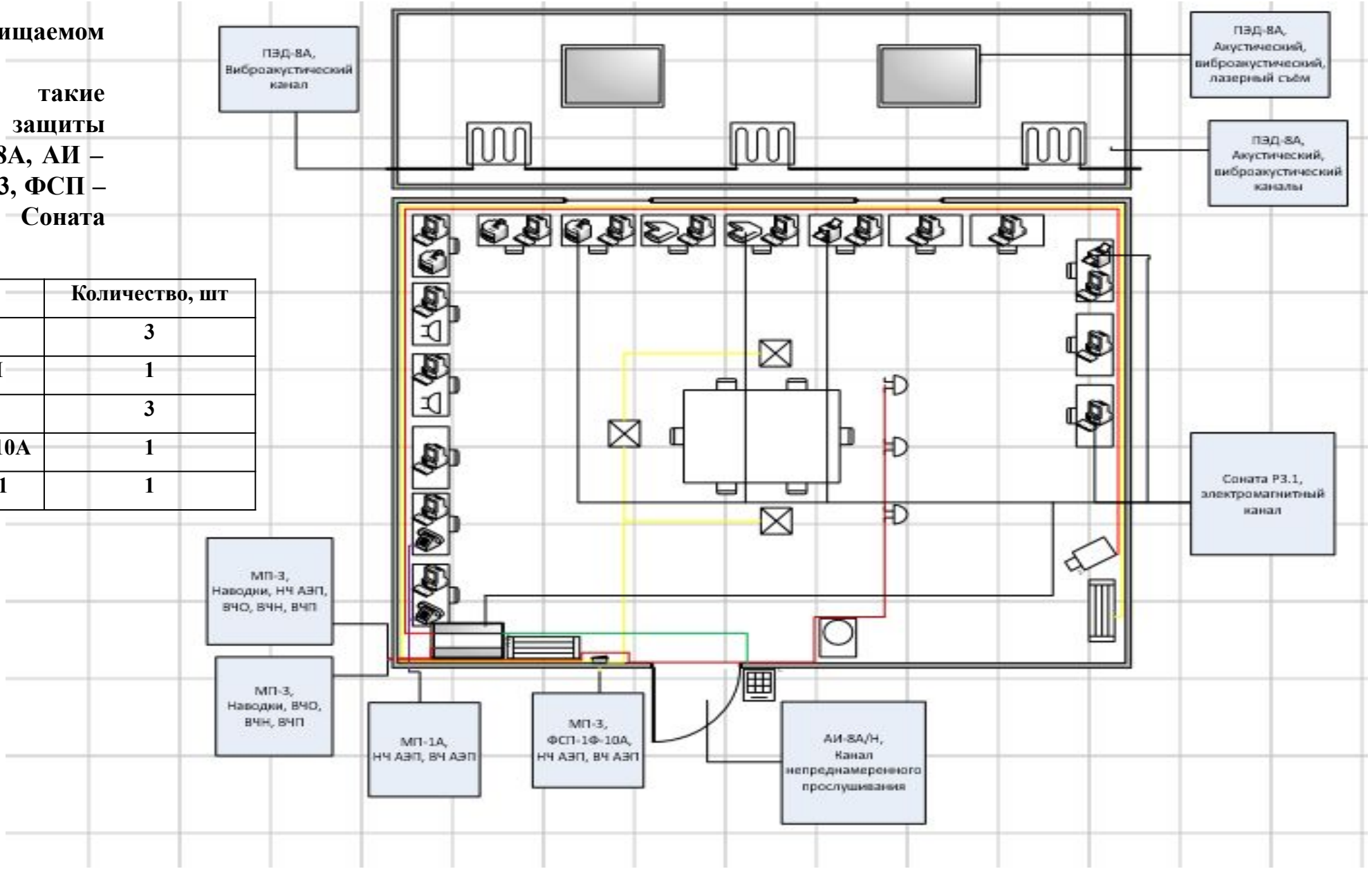


Схема СЗИ защищаемого помещения (Комната для переговоров)

В защищаемом помещении установили такие средства защиты как: ПЭД – 8А, АИ – 8Ф/Н, МП – 3, ФСП – 1Ф – 10А, Соната Р3.1.

№	Тип СЗИ	Количество, шт
1	ПЭД – 8А	3
2	АИ – 8Ф/Н	1
3	МП – 3	3
4	ФСП – 1Ф – 10А	1
5	Соната Р3.1	1



НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ, МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ, НАЦИОНАЛЬНЫЕ СТАНДАРТЫ, ИСПОЛЬЗУЕМЫЕ ДЛЯ ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И РАЗРАБОТКИ МОДЕЛИ УГРОЗ

—Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

— Постановления Правительства Российской Федерации от 6 июля 2015 года № 676 «О требованиях к порядку создания, развития, ввода в
эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;

— Постановления Правительства России от 01 ноября 2012 года № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;

— Банка данных угроз безопасности информации ФСТЭК России,

— Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

— Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— Приказа ФСБ России от 10 июля 2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

— Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8 Центра ФСБ России от 31.03.2015 № 149/7/2/6 432;

— Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 года;

— Методики оценки угроз безопасности информации, утвержденной ФСТЭК России 5 февраля 2021 года.

Описание информационной системы и её характеристика как объекта защиты

НАИМЕНОВАНИЕ ИС, ДЛЯ КОТОРОЙ РАЗРАБОТАНА ЧАСТНАЯ МОДЕЛЬ УГРОЗ:

Модель угроз разработана для ГИС «СПЕЦСВЯЗЬРЕМОНТ».

Состав ГИС «СПЕЦСВЯЗЬРЕМОНТ» состоит из следующих основных подсистем:

— телекоммуникационная подсистема;
— информационно-коммуникационная подсистема;
— подсистема консультативного обслуживания;
— подсистема мониторинга;
— подсистема обеспечения информационной безопасности.

КЛАСС ЗАЩИЩЕННОСТИ ИС, УРОВЕНЬ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ГИС «СПЕЦСВЯЗЬСЕРВИС»:

Для ГИС «СПЕЦСВЯЗЬРЕМОНТ» установлены:

—второй класс защищенности государственных информационных систем (К2) согласно приказу ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 года № 17;

—второй уровень защищенности персональных данных (УЗ2), обрабатываемых в информационных системах, согласно «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, В СООТВЕТСТВИИ С КОТОРЫМИ ФУНКЦИОНИРУЕТ ИС:

ГИС «СПЕЦСВЯЗЬРЕМОНТ» функционирует в соответствии со следующими нормативно-правовыми актами Российской Федерации:

— Конституция Российской Федерации;
— Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
— Федеральный закон от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности»;
— Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
— Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

НАЗНАЧЕНИЕ, ЗАДАЧИ (ФУНКЦИИ) ИС, СОСТАВ ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ И ЕЕ ПРАВОВОЙ РЕЖИМ

ГИС «СПЕЦСВЯЗЬРЕМОНТ» предназначена для разработки следующих работ:

- Производство электромонтажных работ
  - Прокладка внутренней проводки и наружных кабельных линий;
  - Установка распределительного защитного оборудования, приборов учета электроэнергии;
  - Монтаж электрического освещения;
  - Монтаж силового электрооборудования;
  - Монтаж, ввод в эксплуатацию слаботочных систем - все виды сигнализации, видеонаблюдение, СКУД.

Перечень обрабатываемой в ГИС «**СПЕЦСВЯЗЬРЕМОНТ**» информации:

Сведения, обрабатываемые в ГИС «СПЕЦСВЯЗЬРЕМОНТ»		**Категория информации/ персональных данных**	
Предприятие	Состав системы защиты	Служебная информация	
	Режимные мероприятия	Служебная информация	
	Должностные инструкции	Служебная информация	
	Технологии	Коммерческая тайна	
Сотрудники	ФИО	ПДн	Иные
	Дата рождения	ПДн	Иные
	Серия, номер паспорта	ПДн	Иные
	Номер телефона	ПДн	Иные
	Место регистрации	ПДн	Иные

СОСТАВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В состав ГИС «СПЕЦСВЯЗЬРЕМОНТ» в качестве функциональных объектов входят:

- Бухгалтерия;
- Отдел кадров;
- Отдел информационного обеспечения;
- Отдел информационной безопасности;
- Финансовый отдел;
- Планово-экономический отдел.

КАТЕГОРИИ ЛИЦ, ИМЕЮЩИХ ДОСТУП К РЕСУРСАМ СИСТЕМЫ

К категориям лиц, имеющих санкционированный доступ к компонентам и ресурсам ГИС «СПЕЦСВЯЗЬРЕМОНТ», относятся:

- пользователи - сотрудники «ПАРТНЕР» участвующие в информационном взаимодействии, занимающиеся обработкой защищаемой информации и имеющие доступ к части ресурсов ГИС «СПЕЦСВЯЗЬРЕМОНТ», в соответствии с наделёнными правами;
- пользователи - не являющиеся сотрудниками «ПАРТНЕР», участвующие в информационном взаимодействии, занимающиеся обработкой защищаемой информации и имеющие доступ к части ресурсов ГИС «СПЕЦСВЯЗЬРЕМОНТ», в соответствии с наделёнными правами;
- администратор информационной системы - сотрудник «ПАРТНЕР», участвующий в информационном взаимодействии, не занимающийся обработкой защищаемой информации;
- администратор информационной безопасности - назначается из состава сотрудников «ПАРТНЕР», осуществляет мониторинг и аудит СЗИ, используемых в ГИС «СПЕЦСВЯЗЬРЕМОНТ» при информационном взаимодействии.
- сотрудники обслуживающей организации, обеспечивающих техническое сопровождение ГИС «СПЕЦСВЯЗЬРЕМОНТ» в рамках заключенного договора (государственного контракта).

Также необходимо учитывать, что к категории лиц, не занимающихся обработкой защищаемой информации и не являющихся зарегистрированными пользователями ГИС «СПЕЦСВЯЗЬРЕМОНТ» (физические лица), но имеющих возможность санкционированного (в т.ч. разового) доступа к ресурсам ГИС «СПЕЦСВЯЗЬРЕМОНТ», следует отнести:

- лица, обеспечивающие функционирование систем или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
- лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ.

В связи с этим всех пользователей ГИС «СПЕЦСВЯЗЬРЕМОНТ» можно условно разделить на следующие классы пользователей ГИС «СПЕЦСВЯЗЬРЕМОНТ»:

- внутренние непривилегированные пользователи;
- внутренние привилегированные пользователи;
- внешние непривилегированые пользователи;
- внешние привилегированные пользователи.

В ГИС «СПЕЦСВЯЗЬРЕМОНТ» применяются следующие интерфейсы взаимодействия с информационной системой:

- сетевые интерфейсы - обеспечивающие взаимодействие с защищенной сетью ГИС «СПЕЦСВЯЗЬРЕМОНТ» и смежными (взаимодействующими) системами или сетями;
- интерфейсы для использования съемных машинных носителей информации;
- интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей.

Доступ внешних пользователей к ресурсам ГИС «СПЕЦСВЯЗЬРЕМОНТ» отсутствует.

ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ОТ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

На основе анализа основных процессов и особенностей области деятельности «ПАРТНЕР» и информации, представленной профильными подразделениями «ПАРТНЕР», выявлены возможные негативные последствия от реализации угроз безопасности, представленные в таблице

Виды риска (ущерба)	Возможные негативные последствия
У2 Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью.	• Нарушение законодательства Российской Федерации. • Потеря (хищение) денежных средств. • Недополучение ожидаемой (прогнозируемой) прибыли. • Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. • Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). • Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. • Срыв запланированной сделки с партнером. • Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.
У3 Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	• Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия). • Прекращение или нарушение функционирования сети связи. • Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации.

ВОЗМОЖНЫЕ ОБЪЕКТЫ ВОЗДЕЙСТВИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

№ п/п	Объект воздействия
1. Информационные ресурсы	
1.1	документы в файловом виде на АРМ пользователей (операторов ГИС «СПЕЦСВЯЗЬРЕМОНТ»)
1.2	базы данных, содержащие защищаемую информацию
1.3	электронные носители информации, содержащие защищаемую информацию
1.4	материальных носителях, содержащие защищаемую информацию (документы в бумажном виде)
1.5	каналы связи
2. Системное и прикладное программное обеспечение	
2.1	системное программное обеспечение
2.2	прикладное программное обеспечение общего назначения
2.3	прикладное программное обеспечение специализированного назначения
3. Средства вычислительной техники	
3.1	автоматизированные рабочие места пользователей (операторы ГИС «СПЕЦСВЯЗЬРЕМОНТ»)
3.2	автоматизированные рабочие места привилегированных пользователей
3.3	файловые сервера
3.4	сервера баз данных
3.5	системы хранения данных
3.6	системы резервного копирования
3.7	коммуникационное оборудование
3.8	электронные носители информации (флэш-накопители, жёсткие диски, CD/DVD-диски)
4. Средства защиты информации	
4.1	программные средства защиты информации
4.2	программно-аппаратные средства защиты информации

ОПИСАНИЕ ВИДОВ ВОЗДЕЙСТВИЯ НА КОМПОНЕНТЫ ИС, РЕАЛИЗАЦИЯ КОТОРЫХ НАРУШИТЕЛЕМ МОЖЕТ ПРИВЕСТИ К НЕГАТИВНЫМ ПОСЛЕДСТВИЯМ

Основными видами воздействий, приводящих к негативным последствиям, являются:

— утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);
— несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;
— отказ в обслуживании компонентов (нарушение доступности);
— несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);
— несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
— нарушение функционирования (работоспособности) программноаппаратных средств обработки, передачи и хранения информации.

Перечень УБИ и оценка их применимости

№ УБИ	Наименование УБИ	Объекты воздействия	Источник угрозы	Негативные последствия	Серверный сегмент (СС)	Пользов ательский сегмент (ПС)	Возможные сценарии
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	Системное программное обеспечение	Внутренний (Н1)	У1 У2	применима	применима	Закрепление (сохранение доступа) в системе или сети Повышение привилегий по доступу к компонентам систем и сетей Сокрытие действий и применяемых при этом средств от обнаружения Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз
			Внешний (Н1)	У1 У2	применима	применима	
УБИ.091	Угроза несанкционированного удаления защищаемой информации	Метаданные, объекты! файловой системы, реестр	Внутренний (Н1)	У1 У2	применима	применима	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям
			Внешний (Н1)	У1 У2	применима	применима	
УБИ.092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	Информационная система, аппаратное обеспечение	Внешний (Н4)	У2 У3	неприменима	неприменима	Возможные сценарии отсутствуют в связи с отсутствием объекта воздействия

Перечень актуальных угроз безопасности информации для серверного сегмента ГИС «СПЕЦСВЯЗЬРЕМОНТ»

№ УБИ	Наименование УБИ	Объект воздействия	Источник угрозы	Способ реализации	Негативные последствия	Актуальность угрозы	Примечания
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	+	Внутренний (H1) Внешний (H1)	+	У2	Актуальна	Угроза безопасности актуальна в связи с наличием источника угрозы, объекта воздействия и способа реализации угрозы, направленного на объект воздействия, а также наличия негативных последствий реализации угрозы безопасности
УБИ.091	Угроза несанкционированного удаления защищаемой информации	+	Внутренний (H1) Внешний (H1)	+	У2	Актуальна	Угроза безопасности актуальна в связи с наличием источника угрозы, объекта воздействия и способа реализации угрозы, направленного на объект воздействия, а также наличия негативных последствий реализации угрозы безопасности

Перечень актуальных угроз безопасности информации для пользовательского сегмента ГИС «СПЕЦСВЯЗЬРЕМОНТ»

№ УБИ	Наименование УБИ	Объект воздействия	Источник угрозы	Способ реализации	Негативные последствия	Актуальность угрозы	Примечания
УБИ.090	Угроза несанкционированного создания учётной записи пользователя	+	Внутренний (H1) Внешний (H1)	+	У2	Актуальна	Угроза безопасности актуальна в связи с наличием источника угрозы, объекта воздействия и способа реализации угрозы, направленного на объект воздействия, а также наличия негативных последствий реализации угрозы безопасности
УБИ.091	Угроза несанкционированного удаления защищаемой информации	+	Внутренний (H1) Внешний (H1)	+	У2	Актуальна	Угроза безопасности актуальна в связи с наличием источника угрозы, объекта воздействия и способа реализации угрозы, направленного на объект воздействия, а также наличия негативных последствий реализации угрозы безопасности

ОГРАНИЧЕНИЯ НА ИМЕЮЩУЮСЯ У НАРУШИТЕЛЯ ИНФОРМАЦИЮ ОБ ОБЪЕКТАХ

№ п/п	Информация	Ограничение	Обоснование ограничения
1	Содержание технической документации на технические и программные компоненты СФ	Доступна информация, находящаяся в свободном доступе. Доступна внутренним нарушителям частично в пределах компетенции согласно должностным функциям	В ГИС «СПЕЦСВЯЗЬРЕМОНТ» ограничен доступ к такой информации
2	Сведения о линиях связи, по которым передается защищаемая информация: линии связи, проходящие в КЗ; линии связи, проходящие за пределами КЗ	Потенциальному нарушителю могут быть доступны следующие сведения о линиях связи, проходящих в КЗ и за ее пределами: общая информация об архитектуре ЛВС; информация о типах используемого оборудования и кабелей. Более детальная информация о линиях связи нарушителю недоступна или доступна внутреннему нарушителю частично в пределах компетенции согласно должностным функциям	В ГИС «СПЕЦСВЯЗЬРЕМОНТ» ограничен доступ к такой информации
3	Все сети связи, работающие на едином ключе	Сведения недоступны	Информация доступна только привилегированным администраторам безопасности ГИС «СПЕЦСВЯЗЬРЕМОНТ»

ВЫВОДЫ

АКТУАЛЬНЫЕ КАТЕГОРИЙ НАРУШИТЕЛЯ

Потенциальным нарушителем безопасности информации могут быть нарушители категорий внешние и внутренние.

Потенциальными внешними нарушителями для ГИС «СПЕЦСВЯЗЬРЕМОНТ» могут быть:

— преступные группы (криминальные структуры);
— отдельные физические лица (хакеры);
— поставщики вычислительных услуг, услуг связи;
— бывшие (уволенные) работники (пользователи).

Потенциальными внутренними нарушителями для ГИС «СПЕЦСВЯЗЬРЕМОНТ» могут быть:

— лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы (администрация, охрана, уборщики и т.д.);
— авторизованные пользователи ИС;
— Администраторы ИС и Администраторы ИБ.

АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ СЕРВЕРНОГО СЕГМЕНТА ГИС «СПЕЦСВЯЗЬРЕМОНТ»

Для серверного сегмента ГИС «СПЕЦСВЯЗЬРЕМОНТ» актуальными являются следующие угрозы безопасности информации:

— УБИ.090 Угроза несанкционированного создания учётной записи пользователя;
— УБИ.091 Угроза несанкционированного удаления защищаемой информации;

АКТУАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ ПОЛЬЗОВАТЕЛЬСКОГО СЕГМЕНТА ГИС «СПЕЦСВЯЗЬРЕМОНТ»

Для пользовательского сегмента ГИС «СПЕЦМАШ» актуальными являются следующие угрозы безопасности информации:

— УБИ.090 Угроза несанкционированного создания учётной записи пользователя;
— УБИ.091 Угроза несанкционированного удаления защищаемой информации;

НЕОБХОДИМЫЙ КЛАСС СКЗИ

Для нейтрализация актуальных для ГИС «СПЕЦСВЯЗЬРЕМОНТ» угроз, при информационном взаимодействии, должны применяться СКЗИ класса не ниже КС2.