Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

Е.В. Каменева

ЗАЩИТА ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность

Оренбург
2019

УДК 004.056(076.5)
ББК 32.971.3я7
К 18

Рецензент – доцент, кандидат технически наук Р.Р. Галимов

К 18 **Каменева Е.В.**
Защита от утечки информации по техническим каналам : методические указания / Е.В. Каменева; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2019.

Методические указания содержат методику разработки системы защиты информации от утечки по техническим каналам.

Изложены цели выполнения, тематика и содержание курсового проекта, а также требования к оформлению и пояснения к процедуре защиты курсового проекта.

Методические указания к выполнению курсового проекта составлены на основе требований Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность и предназначены для выполнения курсового проекта студентами, изучающими дисциплину «Защита от утечки информации по техническим каналам».

УДК 004.056(076.5)
ББК 32.971.3я7

Содержание

Введение

Настоящие методические указания предназначены для выполнения курсового проекта по курсу «Защита от утечки информации по техническим каналам» предусмотренный учебным планом по направлению подготовки 10.03.01 Информационная безопасность в 6-ом семестре. Выполнение курсового проекта опирается на теоретические разделы курса и лабораторный практикум.

Целью выполнения курсового проекта является систематизация и закрепление знаний, полученных при изучении дисциплин «Техническая защита информации» и «Защита информации от утечки по техническим каналам», связанных с изучением теоретических аспектов и методологических основ защиты информации с помощью технических средств. Курсовой проект направлен на выработку системного подхода и развитие навыков самостоятельной работы при разработке системы защиты информации от утечки по техническим каналам.

Руководитель курсового проекта следит за процессом его выполнения, проводит консультации, намечает график контрольных мероприятий, помогает студенту решать принципиальные вопросы проводимого исследования и готовиться к защите курсового проекта. Студент, заканчивая очередной этап работы, представляет руководителю материалы курсового проекта для проверки правильности полученных промежуточных результатов и направления хода дальнейших работ.

1 Тема курсового проекта

В качестве основной темы курсового проекта предлагается следующая: «Проектирование системы технической защиты информации объекта информатизации». В виде объекта информатизации следует использовать подразделения промышленных предприятий, коммерческие фирмы, выделенные/защищаемые помещения, государственные учреждения. С целью проведения более полных и качественных исследований отдельным студентам могут быть выданы отдельные темы курсовых работ.

Область профессиональной деятельности бакалавров по направлению подготовки 10.01.03 Информационная безопасность включает в себя сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере.

В настоящее время для любой организации/предприятия актуальным является вопрос защиты информации. Деятельность и мероприятия по поддержанию требуемого уровня защищенности информации в организации должны быть поддержаны соответствующей системой ее защиты. Составной частью системы защиты информации является защита от утечки информации по техническим каналам. Защита информации от утечки по техническим каналам — это комплекс организационных, организационно - технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны. В связи с этим тема курсового проекта является актуальной для закрепления теоретических знаний и приобретения практических навыков студентов, обучающихся по направлению подготовки 10.03.01 Информационная безопасность.

2 Требования к оформлению курсового проекта

Расчетно-пояснительная записка курсового прокта должна быть оформлена в строгом соответствии с СТО 02069024.101 – 2015 «Работы студенческие. Общие требования и правила оформления».

Расчетно-пояснительная записка разделяется по составным разделам (главам) курсового проекта. Каждый раздел расчетно-пояснительной записки начинается с нового листа.

Успешное выполнение курсового проекта во многом зависит от четкого соблюдения установленных сроков. График выполнения работы устанавливается преподавателем – руководителем курсового проекта. Студенту необходимо предоставлять отчеты преподавателю о проделанной работе. Законченный курсовой проект, содержащий все требуемые элементы оформления, сдается на проверку научному руководителю. Студенты представляют курсовой проект в установленный срок (не позднее, чем за две недели до окончания текущего семестра). Если курсовой проект выполнен в соответствии с изложенными требованиями, руководитель подписывает её к защите и возвращает студенту. Если в проекте имеются ошибки, руководитель на полях или в рецензии делает соответствующие замечания. Если курсовой проект получает неудовлетворительную оценку со стороны руководителя, студент должен её переработать, устранив замечания руководителя. Подписанный руководителем курсовой проект защищается в назначенные сроки.

Расчетно-пояснительная записка курсового проекта (курсовой работы) содержит следующие структурные элементы:

– титульный лист;

– задание;

– аннотацию;

– содержание;

– введение;

– основную часть;

– список использованных источников;

– приложения.

Оформление текста курсового проекта выполняется в соответствии с требованиями раздела 6 СТО 02069024.101 – 2015 «Работы студенческие. Общие требования и правила оформления».

Титульный лист является первым листом курсового проекта, на котором указывают классификационный код (см. раздел 12).

Бланк задания следует помещать после титульного листа. Задание должно содержать исходные данные, объем и срок выполнения курсового проекта с подписями руководителя и исполнителя.

Аннотация является третьим листом курсового проекта и содержит краткую описательную характеристику курсового проекта по основным вопросам в целом и по его разделам с указанием того, что и каким образом сделано, какие каналы утечки информации установлены, какими способами и средствами они нейтрализованы

Изложение текста основной части, оформление иллюстраций, построение таблиц, оформление списка использованных источников, приложений должны соответствовать требованиям, указанным в разделах 7 и 8 СТО 02069024.101 – 2015 «Работы студенческие. Общие требования и правила оформления».

Заключение должно содержать выводы и предложения по проделанной работе.

В результате выполнения курсового проекта студент должен:

− обосновать актуальность выполнения работ по проектированию системы защиты информации от утечки по техническим каналам;

− представить характеристику предприятия;

− представить в виде схем и таблиц модель объекта защиты;

− определить технические каналы утечки информации;

− разработать методы и подобрать средства для предотвращения утечки информации;

− рассчитать затраты на покупку оборудования;

− разработать рекомендации по размещению средств предотвращения утечки информации.

3 Рекомендации по выполнению курсового проекта

Защита информации от утечки по техническим каналам представляет собой совокупность организационных и технических мероприятий, проводимых с целью исключения (существенного затруднения) добывания злоумышленником информации с помощью технических средств. Защита от этих средств достигается комплексным применением согласованных по цели, месту и времени мер защиты.

Согласно ФЗ №149 защите подлежит секретная информация (государственная тайна) и конфиденциальная информация. В зависимости от вида информации предъявляются требования по ее защите. В связи с этим, работу по созданию системы защиты информации от утечки по техническим каналам необходимо начинать с категорирования информации и моделирования объекта защиты, на котором эта информация обрабатывается.

Моделирование объектов защиты является одним из главных этапов разработки системы защиты от утечки информации по техническим каналам.

Моделирование объектов защиты предполагает решение следующих задач:

1) охарактеризовать организацию/предприятие и его деятельность;
2) структурировать защищаемую информацию;
3) разработать модели объектов защиты.

Характеристика организации/предприятия включает в себя:

− описание направления работы организации/предприятия;

− разработку организационной структуры организации/предприятия (пример организационной структуры приведен на рисунке 1);

− анализ основных функций главных структурных подразделений;

− разработку схемы информационных потоков (пример схемы информационные потоков приведен на рисунке 2).

Рисунок 1 – Пример организационной структуры организации/предприятия

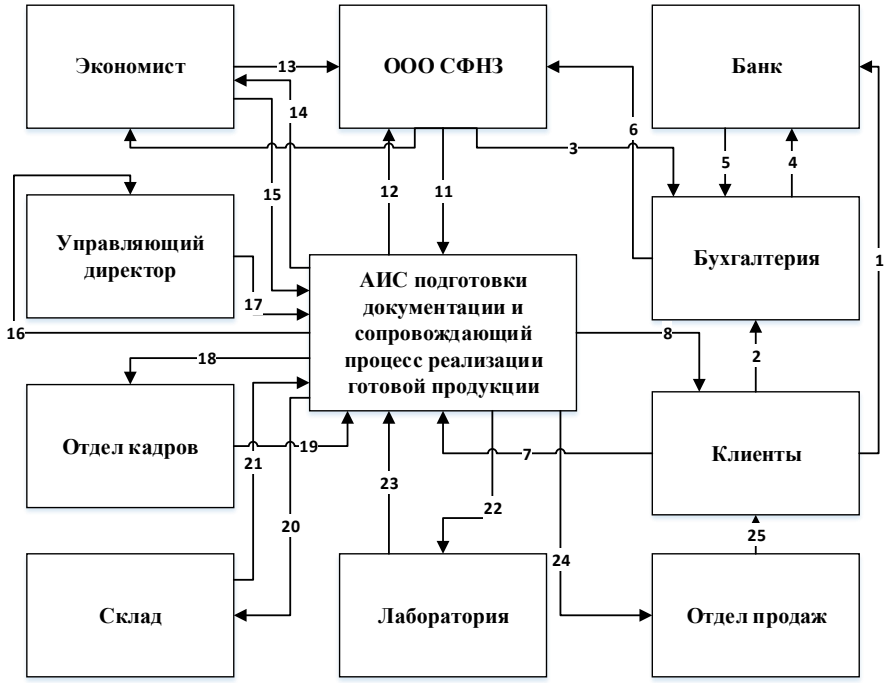

Рисунок 2 – Пример схемы информационных потоков организации/предприятия

Схема информационных потоков, в обязательном порядке, сопровождается таблицей (таблица 1), в которой приводится их описание и анализ.

Таблица 1 – Анализ информационных потоков организации/предприятия

Номер информационного потока	Наименование	Описание
1	Оплата услуг	Производится оплата услуг в Бухгалтерию ООО «СФНЗ» и в банк
2		
3	Запрос финансовой отчетности	Руководство ООО «СФНЗ» запрашивает финансовый отчет в Бухгалтерии
4	Запрос о состоянии счета	Бухгалтерия запрашивает отчет о состоянии счета
⋮	⋮	⋮
25	Продажа	Передача готовой продукции клиентам

Для ***структурирования информации*** в качестве исходных данных используются:

− перечень сведений, составляющих государственную, ведомственную или коммерческую тайну;

− перечень источников информации в организации.

Структурирование информации проводится путем классификации информации в соответствии со структурой, функциями и задачами организации с привязкой элементов информации к ее источникам.

Детализацию информации целесообразно проводить до уровня, на котором элементу информации соответствует один источник.

Схема классификации информации разрабатывается в виде графа-структуры, представленной на рисунке 3, нулевой (верхний) уровень иерархии который соответствует понятию «защищаемая информация», а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основное требование к схеме классификации – общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня, т. е. одна и та же информация (И) не должна указываться в разных элементах (Э) классификации.

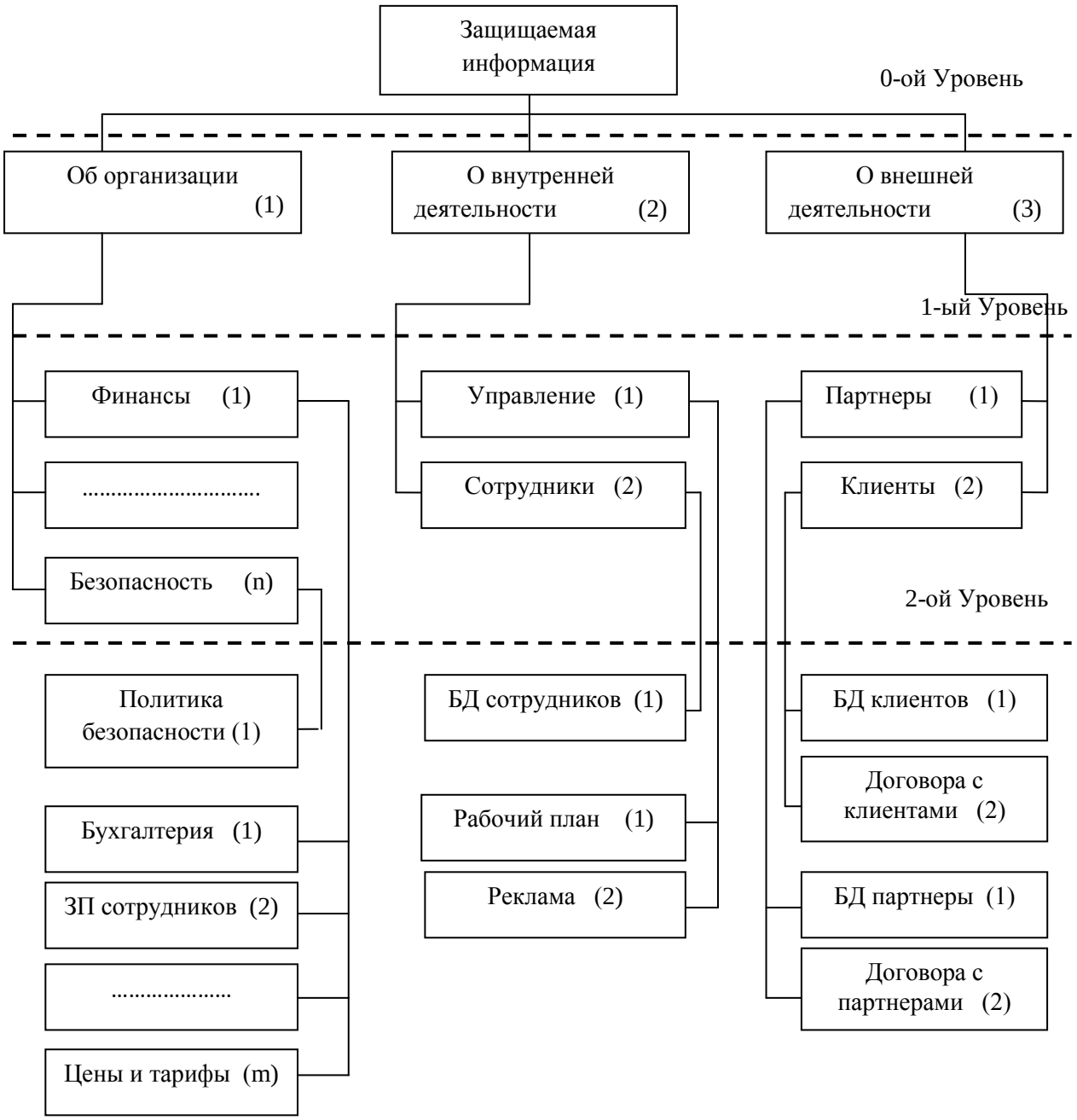

Рисунок 3 – Граф-структура защищаемой информации

На основе схемы классификации информации разрабатывается таблица 2, в первом столбце которой указывается номер элемента информации в схеме классификации. Во 2-м, 3-м и 4-м столбцах таблицы указываются наименование элемента информации (тематического вопроса) и его характеристики: гриф и цена. В столбце 5 указывается носитель информации (фамилия человека/название документа или его номер по книге учета, наименование и номер изделия и т.д.), а в

графе 6 —места размещения или хранения (возможные рабочие места людей-источников информации, места расположения, размещения или хранения других носителей).

Таблица 2 – Элементы информации, подлежащие защите

№ элемента информации	Элемент информации	Гриф конфиденциальности элемента информации	Цена	Носитель информации	Местонахождение источника информации
0111	Бухгалтерия	КТ	500000	HDD ПК, договоры, отчеты	Бухгалтерия /Серверная
0112	ЗП сотрудников	КТ	200000	HDD ПК, договоры, отчеты	Бухгалтерия /Серверная
…….	……	……	…..	…….	……
01n1	Политика безопасности	КИ	100000	Документы службы безопасности	Служба безопасности

Задача ***моделирования объектов защиты*** состоит в объективном описании и анализе источников конфиденциальной информации и существующей системы ее защиты. Для построения точной модели объекта защиты необходимо:

− определение источников защищаемой информации;

− описание пространственного расположения основных мест размещения источников защищаемой информации;

− выявление путей распространения носителей с защищаемой информации за пределы контролируемых зон (помещений, зданий, территории организации);

− описание с указанием характеристик существующих преград на путях распространения носителей с информацией за пределы контролируемых зон.

Моделирование проводится на основе пространственных моделей контролируемых зон с указанием мест расположения источников защищаемой информации – планов помещений, этажей зданий, территории в целом. На планах помещений указываются в масштабе места размещения ограждений, экранов, воздухопроводов, батарей и труб отопления, элементов интерьера и других

конструктивных элементов, способствующих или затрудняющих распространение сигналов с защищаемой информацией, а также места размещения и зоны действия технических средств охраны и телевизионного наблюдения. Их параметры целесообразно объединить в таблицу, вариант которой приведен в таблице 3.

Таблица 3 – Технический паспорт объекта информатизации

Название помещения	ООО «Банк»			
Этаж	1	Площадь, м2	333,5	
Количество окон, тип сигнализации. Наличие штор на окнах	36	Двойной стеклопакет, 18 окон выходит на проезжую часть, остальные 18 во внутренний двор, вертикальные жалюзи		
Двери, количество, одинарные , двойные	47	Одинарные,36 выходят в коридор,5 в тамбур, 4 в смежные помещения; двойные, 2 выходят на улицу		
Соседние помещения, название. Толщина стен	нет			
Помещение над потолком, название. Толщина перекрытий	Кровля. Толщина перекрытия – 220мм			
Помещение под полом, название. Толщина перекрытий.	Подвал. Толщина перекрытия – 220мм			
Наличие комнат с неконтролируемым доступом	нет			
Наличие хранилищ бумажных документов	13	Архив на 2-ом этаже, сейфы		
Вентиляционные отверстия, места размещения, размеры отверстий	В сантехузлах – принудительно обязательное 0,3м			
Батареи отопления, типы. Куда выходят трубы	Чугунные радиаторы. Выход - подвал			
Цепи электропитания, количество розеток	220 В, один входящий (исходящий) кабель в каждой кабинет. Источники бесперебойного питания в каждом кабинете			56
Телефон, количество	Стационарный. Места установки – стол. Тип кабеля – ТРП (2-х жильный)			33
Радиотрансляция	нет			
Бытовые электроприборы, количество	Электрочайник			17

Продолжение таблицы 3

АРМ, расположение, количество	Монитор и системный блок. Расположение – стол	37
Технические характеристики АРМ	Процессор AMD :Тип процессора - A9-9425, Количество ядер – 2, Частота процессора - 3.1 ГГц, Кэш-память - 1 МБ, Сокет - BGA (FT4), ОЗУ 8 Гб, объём жесткого диска 1 Тб, монитор Samsung SynsMaster 173s, ОС Windows 10	
Количество и тех. характеристики серверов	HPE ProLiant MicroServer Gen10	3
Количество коммутаторов ЛВС	Производитель D-Link, Промышленный управляемый коммутатор 2 уровня с 10 портами 10/100/1000Base-T и 2 портами 1000Base-X SFP (8 портов с поддержкой PoE 802.3af/802.3at (30 Вт), PoE□бюджет до 240 Вт)	4
Выход в Internet, тип подключения	через proxy-сервер	
Характеристика ПО	Информационное ПО: сетевое, СУБД Microsoft SQL Server 2013, 3 БД, объем БД 300 ГБ. Дополнительное ПО: Microsoft Office 2003, антивирусный пакет Kaspersky Internet Security	
Порядок доступа в помещения	Доступ в помещения в течение рабочего дня осуществляется с помощью контроллера доступа и(или) ключа, помещения закрываются на ключ в конце рабочего дня. Ключ и идентификатор доступа сдаются под роспись на КПП.	
Технические средства охраны, количество извещателей	Система охранной сигнализации реализована на базе интегрированной системы. магнитоконтакные извещатели (двери, окна); извещатель охранный объемный оптико- электронный; извещатель охранный поверхностный звуковой; извещатель охранный поверхностный емкостной.	 47 36 28 13
Телевизионные средства наблюдения	Телекамеры стационарные внутренние; телекамеры уличные;	20 9
Пожарная сигнализация	Пожарный извещатель дымовой. В каждом кабинете 2шт. Пожарный извещатель тепловой	 55 10
Другие средства	Контроллер системы доступа Оконные решетки (диаметр прутьев – 7мм., расстояние между прутьями -100 мм., глубина заделки – 100мм.). Расположены на всех окнах здания.	

На планах этажей здания указываются выделенные (с защищаемой информацией) и соседние помещения, схемы трубопроводов водяного отопления, воздухопроводов вентиляции, кабелей электропроводки, телефонной и

вычислительной сетей, радиотрансляции, заземления, зоны освещенности дежурного освещения, места размещения и зоны наблюдения телевизионных камер и т. д. На рисунках 4, 5, 6 и 7 представлены внутренний план помещения, схема освещения и отопления помещения, схема пожарной сигнализации помещения и схема расположения ТСПИ и телефонной линии в помещении соответственно. (Необходимо указать схемы всех этажей в отдельности).

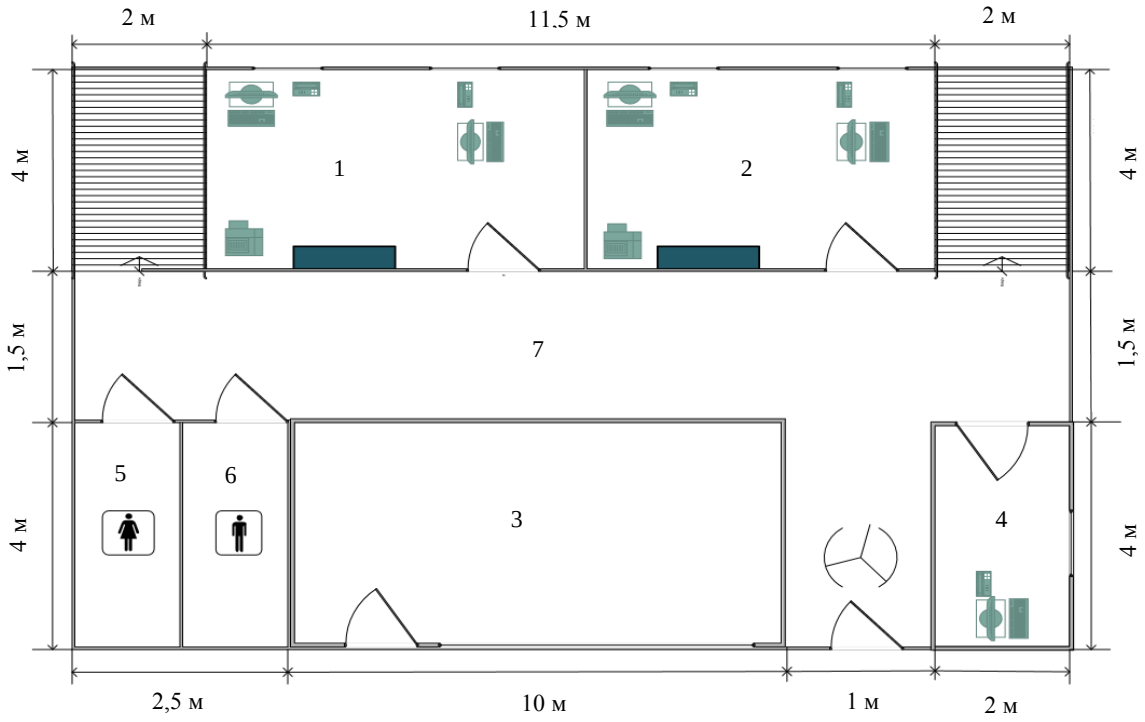

Рисунок 4 – Внутренний план помещения

На плане территории организации отмечаются места размещения здания (зданий), забора, контрольно-пропускного пункта, граничащие с территорией улицы и здания, места размещения и зоны действия технических средств охраны, телевизионной системы наблюдения и наружного освещения, места вывода из организации кабелей, по которым могут передаваться сигналы с информацией.

В процессе моделирования необходимо выполнить анализ возможных путей распространения информации за пределы контролируемой зоны и определить уровни сигналов на их границах на основе рассмотренных пространственных

моделей. В результате моделирования определяется состояние безопасности информации и слабые места существующей системы защиты. Результаты моделирования оформляются на планах и в таблицах.

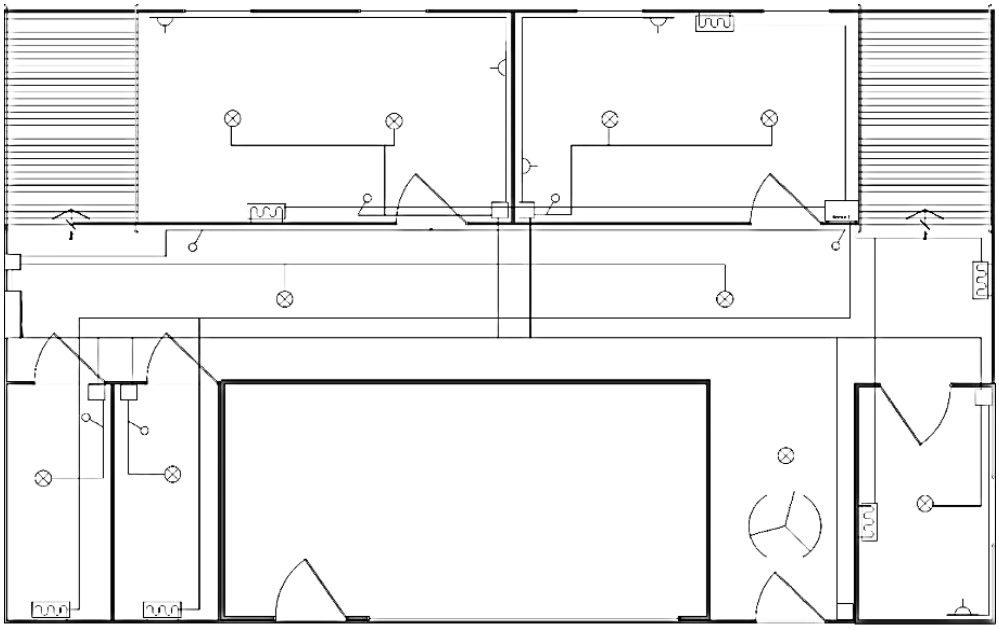

Рисунок 5 – Схема освещения и отопления помещения

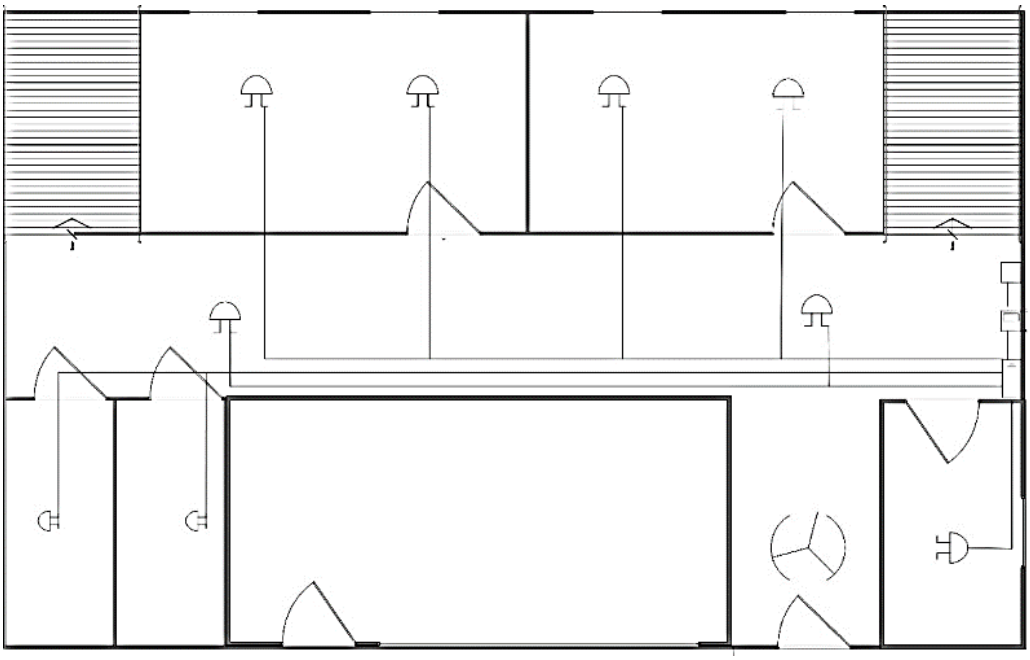

Рисунок 6 – Схема пожарной сигнализации помещения

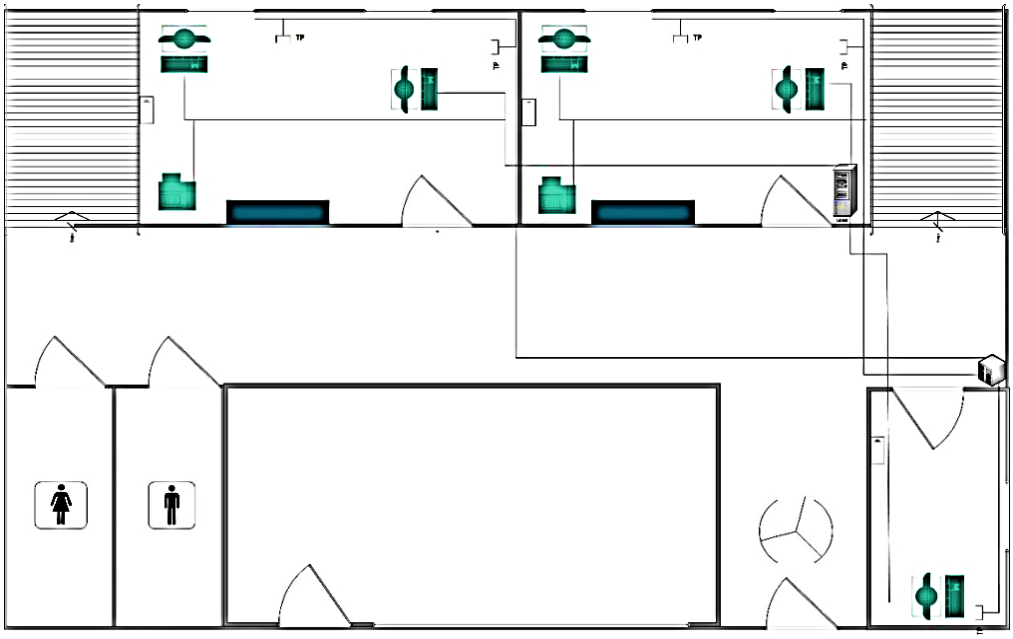

Рисунок 7 – Схема расположения ТСПИ и телефонной линии в помещении

Следующим этапом при разработке системы защиты информации от утечки является ***моделирование угроз безопасности информации***, которое предусматривает анализ способов ее хищения, изменения и уничтожения с целью оценки наносимого этими способами ущерба.

Моделирование угроз включает:

− моделирование способов физического проникновения злоумышленника к источникам информации;

− моделирование технических каналов утечки информации.

Действия злоумышленника по добыванию информации, как и других материальных ценностей, определяются поставленными целями и задачами, его мотивами, квалификацией и технической оснащенностью.

Для создания ***модели угрозы физического проникновения***, достаточно близкой к реальной, необходимо встать на место злоумышленника, т. е. попытаться мысленно проиграть с позиции злоумышленника варианты проникновения к источнику информации. Чем больше при этом будет учтено факторов, влияющих на эффективность проникновения, тем реальнее получится модель. Так как нам ничего

не известно о злоумышленнике, то для того, чтобы избежать ошибок, угрозу лучше переоценить, чем недооценить. Однако это может привести к увеличению затрат на защиту.

На основе такого подхода ***модель злоумышленника*** выглядит следующим образом:

– злоумышленник представляет собой серьезного противника, тщательно готовящего операцию проникновения, изучающего обстановку вокруг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;

– имеет в распоряжении современные технические средства проникновения и преодоления механических преград;

– всеми доступными способами добывает и анализирует информацию о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;

– проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

При моделировании действий злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, варианты их применения, слабые места и «мертвые» зоны диаграмм направленности активных средств охраны.

Возможные пути проникновения злоумышленника отмечаются линиями на планах (рисунок 8) территории, этажей и помещений зданий, а результаты анализа пути заносятся в таблицу.

При моделировании технических каналов утечки, помимо выявления самих каналов, определяется оценка реальности канала, величина и ранг угрозы.

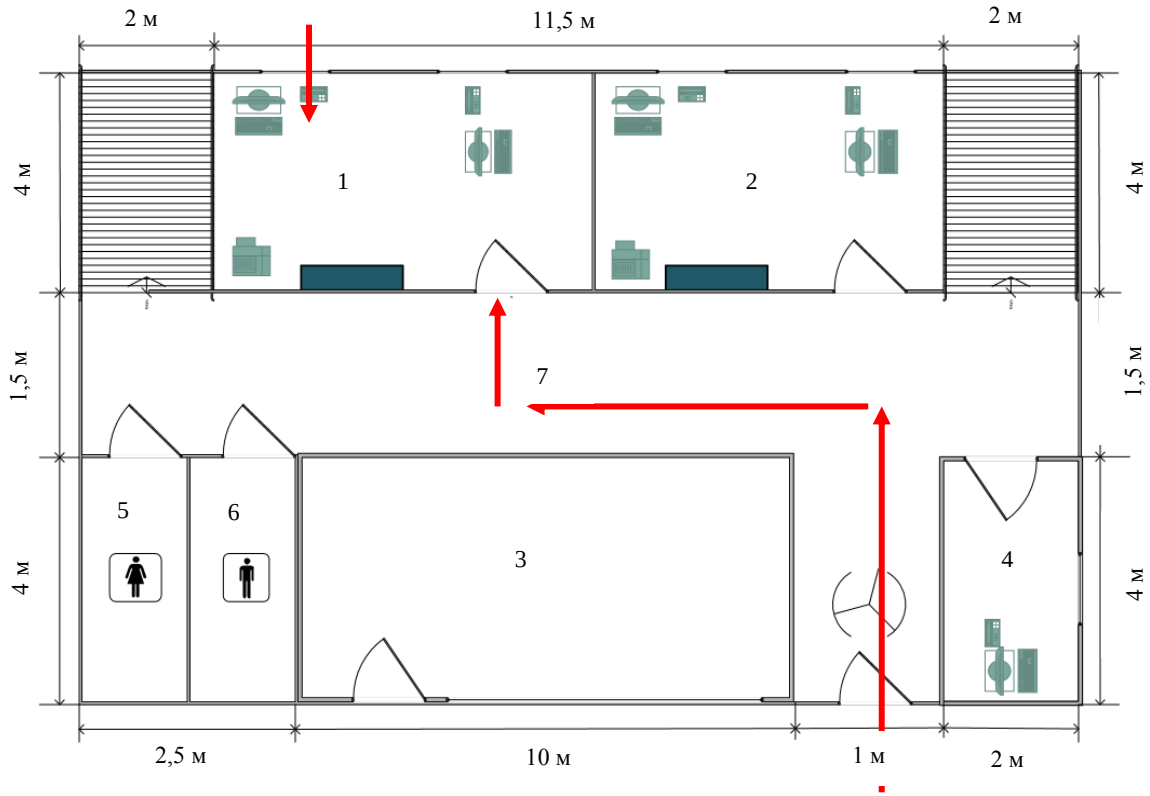

Рисунок 8 – Схема проникновения злоумышленника на объект защиты

Обнаружение и распознавание каналов утечки информации, как и любых объектов, производится по их демаскирующим признакам. В качестве общих индикаторов каналов утечки информации могут служить указанные в таблице 4 демаскирующие признаки.

Приведенные индикаторы являются лишь ориентирами при поиске потенциальных каналов утечки.

Таблица 4– Индикаторы технических каналов утечки информации

Вид канала	Индикаторы
Оптический	Окна, выходящие на улицу, близость к ним домов и деревьев. Отсутствие на окнах занавесок, штор, жалюзи. Читаемость содержания документов на столах. Читаемость содержания плакатов на стенах помещения. Малое расстояние между столами сотрудников в помещении. Читаемость экранов мониторов ПЭВМ на столах сотрудников со стороны окон, дверей или других сотрудников. Появление возле территории организации посторонних людей (в том числе в автомобилях) с биноклями, фотоаппаратами, кино и видеокамерами.

Продолжение таблицы 4

Радио-электронный	Наличие в помещении радиоэлектронных средств, ПЭВМ. ТА городской и внутренней АТС, громкоговорителей трансляционной сети и других предметов. Применение средств радиосвязи. Параллельное размещение кабелей в одном жгуте при разводке их внутри здания и на территории организации. Отсутствие заземления радио и электрических приборов.
Акустический	Малая толщина дверей и стен помещения. Наличие в помещении открытых вентиляционный отверстий. Отсутствие экранов на отопительных батареях. Близость окон к улице и ее домам. Появление возле организации людей с достаточно большими сумками, длинными и толстыми зонтами. Частая и продолжительная парковка возле организации чужих автомобилей.
Материально-вещественный	Наличие закрытых и опечатанных ящиков для бумаги и твердых отходов с демаскирующими веществами. Применение радиоактивных веществ. Неконтролируемый выброс газов с демаскирующими веществами, слив в водоемы и вывоз на свалку твердых отходов. Запись сотрудниками конфиденциальной информации на неучтенных листах бумаги.

Схемы использования технических каналов утечки информации злоумышленником оформляется в таблицу 5 модели угроз.

Таблица 5 – Модель угроз утечки информации по техническим каналам

№ элемента информации	Цена информации, руб, $С_и$	Источник сигнала, передатчик	Путь утечки	Вид канала	Оценка реальности пути, $Р_р$	Ущерб от реализации угрозы ,руб	Ранг угрозы
0111	500000	Электромагнитное поле с волнами видимого диапазона	Хищение информации путем видео- или фото-захвата, отображенной на мониторах, бумажных носителях	Оптический	0,2	100000	4
…	….	….	…..	……	……	…..	….
0112	200000	Монитор, системный блок, принтер, кабели, ПЭМИ	Сканирования ПЭМИ широкополосными приемниками	Электромагнитный	0,5	100000	4

Оценка угроз безопасности информации в результате проникновения злоумышленника к источнику конфиденциальной информации или ее утечки по

техническому каналу носят вероятностный характер. При этом рассматривается вероятность $P_р$ реализуемости рассматриваемого пути или канала, а также цены соответствующего элемента информации $С_и$.

Реальность пути связана с вероятностью выбора злоумышленником пути. Определяется с помощью метода экспертных оценок. Вероятность зависит от простоты реализации именно этого пути проникновения.

Угроза безопасности информации, выраженной в величине ущерба $C_{уи}$ от попадания ее к злоумышленнику, определяется для каждого пути или канала по формуле (1):

$$C_{уи} = C_и \times P_р \quad (1)$$

Разработка модели угроз безопасности информации заканчивается присваиванием им ранга. Ранг угроз каждая организация/предприятие устанавливает самостоятельно.

Ранжирование угроз в проекте провести по таблице 6.

Таблица 6 - Ранжирование угроз информации

Величина угрозы	Ранг угрозы
Более 5×10^5	1
$2\times10^5\ldots5\times10^5$	2
$5\times10^4\ldots2\times10^5$	3
$2\times10^4\ldots5\times10^4$	4
$10^2\ldots2\times10^4$	5

На следующем этапе курсового проекта необходимо разработать меры противодействия утечке информации и выбрать технические средства.

В общем случае защита информации от утечки по техническим каналам обеспечивается в следующих вариантах:

− источник и носитель информации локализованы в пределах границ объекта защиты и обеспечена механическая преграда от контакта с ними злоумышленника или дистанционного воздействия на них полей технических средств добывания;

− соотношение энергии носителя и помех на выходе приемника канала утечки такое, что злоумышленнику не удается снять информацию с носителя с необходимым для ее использования качеством;

− злоумышленник не может обнаружить источник или носитель информации;

− вместо истинной информации злоумышленник получает ложную, которую он принимает как истинную.

Эти варианты реализуют следующие методы защиты:

− исключение или существенное затруднение проникновения злоумышленника к источнику информации с помощью инженерных конструкций и технических средств охраны;

− скрытие достоверной информации;

− дезинформирование злоумышленника.

Классификация методов защиты информации от утечки по техническим каналам представлена на рисунке 9.

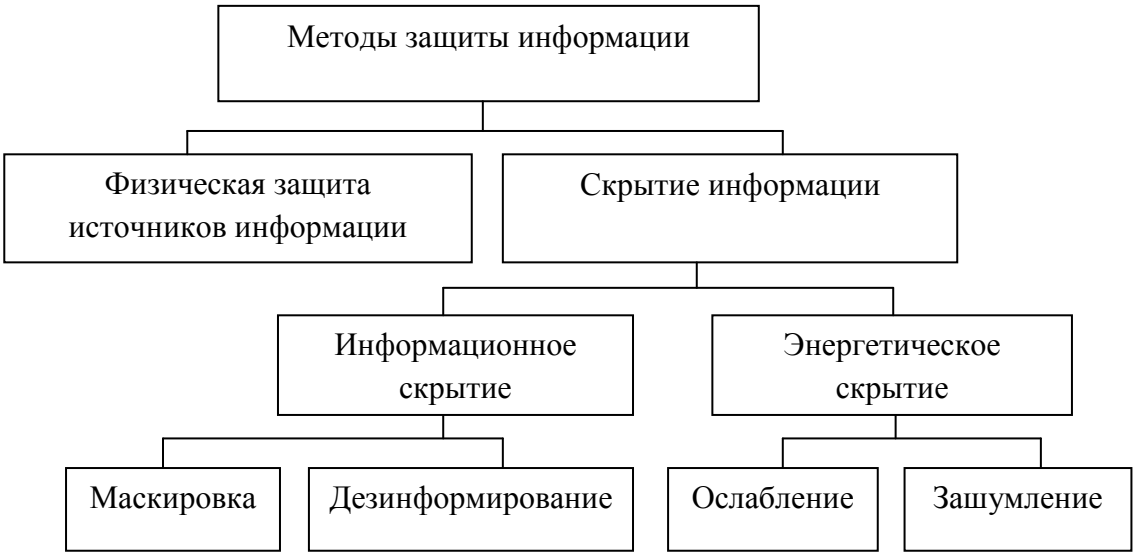

Рисунок 9 – Классификация методов защиты информации от утечки по техническим каналам

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение, далее – с меньшей угрозой и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит средств для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации. Перечень типовых способов и средств защиты информации приведены в таблице 7.

Таблица 7 - Типовые способы и средства защиты информации

Способы реализации угроз	Типовые способы и средства предотвращения угроз
Физический контакт злоумышленника с источником информации	Механические преграды (заборы. КПП, двери, взломостойкие стекла, решетки на окнах, хранилища, сейфы), технические средства охраны, телевизионные средства наблюдения, дежурное и охранное освещение, силы и средства нейтрализации угроз.
Воздействие огня	Технические средства пожарной сигнализации, средства пожаротушения. огнестойкие хранилища и сейфы.
Наблюдение	Маскировочное окрашивание, естественные и искусственные маски. ложные объекты, аэрозоли, пены. радиолокационные отражатели. Радио- и звукопоглощающие покрытия, теплоизолирующие материалы. Генераторы радио- и гидроакустических помех.
Подслушивание	Скремблирование и цифровое шифрование, звукоизолирующие конструкции, звукоизолирующие материалы, акустическое н вибрационное зашумление, обнаружение, изъятие и разрушение закладных устройств
Перехват	Выполнение требований по регламенту и дисциплине связи, отключение источников опасных сигналов, фильтрация и ограничение опасных сигналов, применение буферных устройств, экранирование. Пространственное и линейное зашумление.
Утечка информации по материально-вещественному каналу	Учет и контролируемое уничтожение черновиков, макетов, брака, сбор и очистка от демаскирующих веществ отходов.

Поскольку меры по защите информации для каждой угрозы рассматриваются отдельно, то в контролируемой зоне возможно их дублирование. Например, открытая дверь в служебное помещение может способствовать как наблюдению за документами с экранов персональных компьютеров в помещении, так и подслушиванию ведущихся в нем разговоров. Чтобы предотвратить утечку по этим

двум каналам необходимо установить на дверь устройство для автоматического ее закрытия и кодовый замок.

После объединения способов и средств защиты информации появятся свободные финансовые и/или технические ресурсы, которые могут быть использованы для предотвращения очередных по рангу угроз из таблицы 5. Следовательно, разработка мер по предотвращению представляет собой 2 этапа:

1. разработка локальных мер по предотвращению каждой из выявленных угроз;

2. интеграция (объединение) локальных мер.

Рекомендуемые способы и средства защиты информации заносятся в таблицу, вариант которой приведен в таблице 8.

Таблица 8 – Средства предотвращения угроз утечки информации

№ элемента информации	Тип угрозы	Величина угрозы	Способы предотвращения угроз	Средства предотвращения угроз
0111	Хищение информации путем видео- или фото-захвата, отображенной на мониторах, бумажных носителях	100000	Мониторы ПК и экранов должны быть размещены таким образом чтобы просмотр посторонними лицами был не возможен, использование	Жалюзи, Дверной доводчик, кодовый замок
…	…	…	…	…
0112	Сканирование ПЭМИ широкополосными приемниками	100000	Экранирование, Создание помех	Экранированные ПК, Генератор электромагнитного шума

После определения средств предотвращения угроз необходимо произвести их обзор и выбрать конкретную модель. Определяющими факторами при выборе являются наличие сертификата ФСТЭК, минимально достаточные технические характеристики и стоимость. Пример обзора средств предотвращения угроз представлен в таблице 9. После таблицы приводится вывод о выборе конкретного средства.

Таблица 9 – Обзор средств акустической защиты

Наименование	Характеристики			
	Диапазон рабочих частот Гц	Мощность Вт	Стоимость руб.	Сертификат ФСТЭК
Акустический маскиратор конфиденциальных переговоров «Букет»	100-11200	15	25000	+
Акустический маскиратор конфиденциальных переговоров в помещении Октава -А	90-11000	30	44300	+
Система комплексной акустической и виброакустической защиты помещения "Обертон"	90-11200	20	39800	+
Генератор акустического шума "RNG-01	100-15000	40	29100	-

После осуществления выбора средств защиты информации необходимо подсчитать общую стоимость финансовых затрат на их приобретение. Для этого целесообразно составить спецификацию средств защиты. Пример спецификации представлен в таблице 10.

Таблица 10 - Спецификация средств защиты информации от утечки по техническим каналам

Наименование товара	Тип	Цена, руб.	Количество, шт.	Сумма, руб.
Средство активной защиты информации "Соната-РС3"	Соната-РС3	18 880,00	1	18 880,00
Генератор шума ГНОМ-3	ГШ ГНОМ-3	7 680,00	3	23 040,00
Универсальный защитный модуль «Гром-ЗИ-4»	«Гром-ЗИ-4»	14 500,00	3	43 500,00
Всего				107 020,00

Последним этапом курсового проекта является разработка рекомендаций по размещению средств защиты информации от утечки по техническим каналам. Рекомендации необходимо изобразить на планах помещений, разработанных при моделировании объекта защиты. Пример рекомендаций по установке средств защиты представлен на рисунке 10.

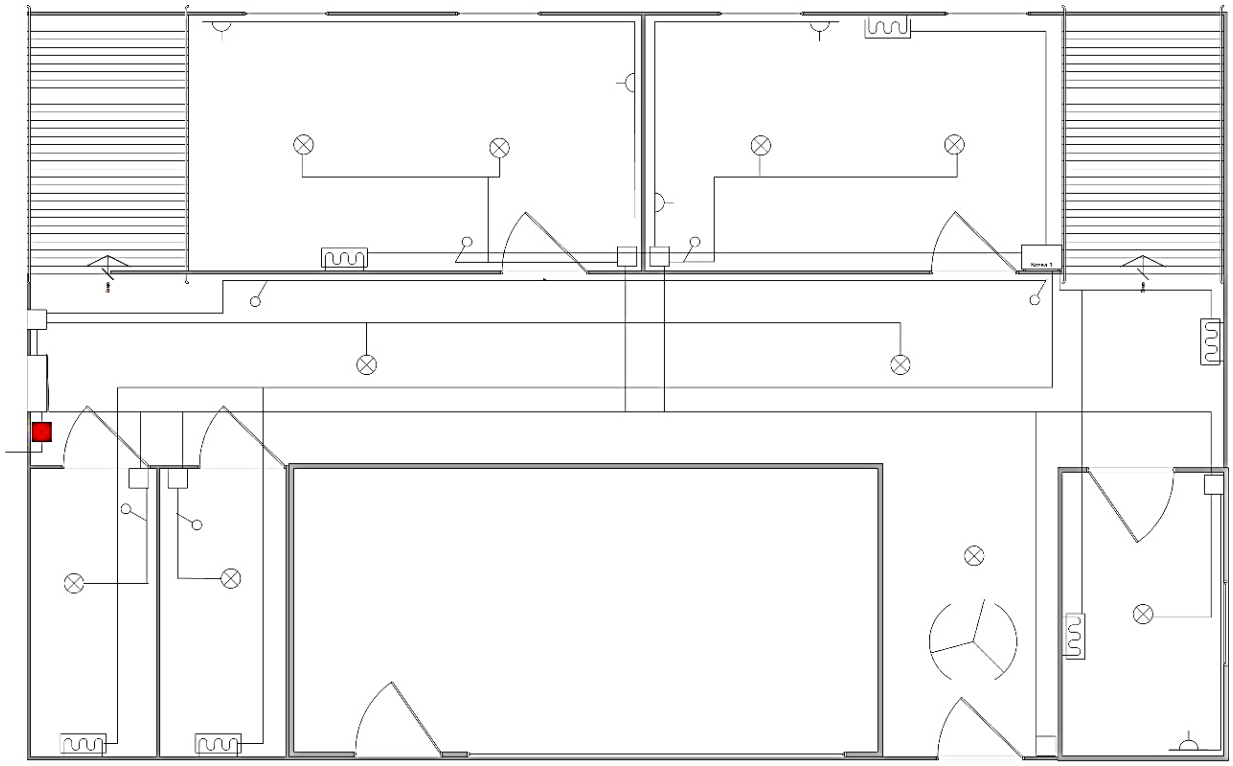

Рисунок 10 – Схема рекомендуемого места установки средства предотвращение утечки информации (название) через линии электропитания и заземления.

В заключении курсового проекта необходимо отразить основные выводы по работе.

4 Литература, рекомендуемая для изучения

4.1. Основная литература

1 ГОСТ Р 50922- 2006. Защита информации. Основные термины и определения. - Введ. 2008-02-01. - М.: Стандартинформ, 2007. - 12 с.

2 Аверченков, В.И. Разработка системы технической защиты информации : учеб. пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2-е изд., стереотип. – М. : ФЛИНТА, 2011. – 187 с.

3 Каторин, Ю.Ф., Защита информации техническими средствами: учебное пособие / под редакцией Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. – СПб: НИУ ИТМО, 2012. – 416 с.

4 Креопалов, В.В. Технические средства и методы защиты информации. Учебно-практическое пособие [Электронный ресурс] / В.В. Креопалов - Евразийский открытый институт, 2011. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book&id=90753

5 Рембовский, А.М., Выявление технических каналов утечки информации / А.М. Рембовский– М. : Вестник МГТУ, 2003. – 270 с.

6 Титов, А.А. Технические средства защиты информации: учебное пособие для студентов специальностей «Организация и технология защиты информации» и «Комплексная защита объектов информатизации». – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 77 с.

7 Хорев, А. А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники / А.А. Хорев // Специальная Техника. – 2010 - № 2. – С. 39-57.

8 Федеральная служба по техническому и экспортному контролю (ФСТЭК России). [Официальный сайт].Режим доступа: http://www.fstec.ru

4.2 Вспомогательная литература

1 Титов, А. А. Инженерно-техническая защита информации: учебное пособие [Электронный ресурс] / А. А. Титов. - Томский государственный университет систем управления и радиоэлектроники, 2010. ЭБС УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА. Режим доступа: http://biblioclub.ru/index.php?page=book&id=208567

2 Торокин, А. А. Инженерно-техническая защита информации: учеб. пособие для вузов / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 960 с.

3 Средства защиты информации. Каталог техники выявления и противодействия средствам разведки, антитеррора. Форум по вопросам защиты информации. Режим доступа: http://www.analitika.info

4 Бюро научно-технической информации. Техника для спецслужб. Режим доступа: http://www.bnti.ru/about.asp

5 Бузов Г.А. Защита от утечки информации по техническим каналам / Бузов Г.А., Калинин С.В., Кондратьев А.В. – М. : Горячая линия - Телеком, 2002. – 414 с.

6 Сидорин Ю.С. Технические средства защиты информации / Сидорин Ю.С. – СПб. : Политехнический университет, 2005. – 109 с.

7 Цымбалова А.А. Разработка модели распределения и использования ресурсов, выделяемых на защиту информации: учебник для вузов/ А. А. Цымбалова – М. : 2011 – 290 с.