МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Организация специальной экспертизы защищаемого помещения ООО «Газпром Интеренешнл»

Исполнитель Лубягов Даниил Владиславович
(фамилия,имя,отчество)

Руководитель Юрин Игорь Валентинович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой_____

(подпись)

_____
(ученаястепень,ученое звание)

_____ Бурлов В.Г._____
(фамилия,имя,отчество)

« » 20г

Санкт–Петербург

2023

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информационная безопасность в сегодняшние дни очень важна. Она защищает системы от проникновения и от атак со стороны потенциальных нарушителей. В эту сферу входят не только взлом, например, как DDoS-атаки, в результате которых может «лечь» сервер сайта, но и утечка данных по различным техническим каналам утечки информации. Злоумышленников в наше время огромное количество. И никто не хочет, чтобы их сервис потерял работоспособность, а данные оказались доступны всем вокруг. Для этого и нужна информационная безопасность.

В любой организации есть конфиденциальная информация, которая включает в себя как персональные данные сотрудников, так и пользователей. Так же в каждой организации есть коммерческая тайна и естественно никто не хочет, чтобы данные с предприятия утекали в общедоступные ресурсы. При утечке персональных данных организация получает проблемы с законодательском. Что бы этого избежать им требуется соблюдать меры безопасности.

Без мер по информационной безопасности кто угодно мог бы получить доступ к конфиденциальным сведениям или взломать любой сайт. Компьютерным пространством стало бы фактически невозможно пользоваться.

В информационной безопасности есть три принципа:

Конфиденциальность – он означает, что информация должна быть защищена от людей, не имеющих права ее просматривать.

Целостность – что информация, о которой идет речь, не повреждена, существует в полном объеме и не изменяется без ведома ее владельцев. Комментарий не сможет отредактировать посторонний человек — только автор или иногда модератор.

Доступность означает, что информация доступна для тех, кто имеет к ней доступ. Например, пользователь может войти в свою учетную запись и просмотреть весь ее контент. Покупатели могут зайти в каталог и просмотреть

товары. Сотрудники имеют доступ к внутренней базе данных на своем уровне доступа. Доступность иногда падает до полного отказа, если система подвергается атаке и система перестает работать.

Сфер в информационной безопасности довольно-таки много, в этой работе будет рассмотрена аппаратно-техническая защита информации от утечек по техническим каналам.

ГЛАВА 1 АНАЛИЗ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

1.1. Описание объекта защиты.

В данной работе будет рассмотрен объект информатизации – «Защищаемое помещение» Общества с ограниченной ответственностью «Газпром Интернешнл». Объект информатизации расположен по адресу: г. Санкт-Петербург, набережной реки Средней Невки, 24. Здание имеет три этажа, помещение находится на втором этаже (Рисунок 1), окна выходят на р. Большая Невка. Здание предприятия расположено на берегу реки Большой Невки. Схема защищаемого помещение изображена на рисунке 1.

Деятельность данного предприятия:

- Компания «Газпром Интернешнл» занимается разведкой и добычей за рубежом. Центр корпоративного обслуживания, расположенный в Санкт-Петербурге, Россия, оказывает консультационную поддержку компаниям, входящим в группу Gazprom EP International BV **.**
- Их основные направления деятельности включают управление проектами по разведке и добыче; поиск, оценка и приобретение новых нефтяных активов в крупнейших нефтегазовых регионах мира; представление «Газпрома» перед иностранными частными и государственными компаниями.

Обрабатываемая информация на объекте - конфиденциальная информация (далее – «КИ»).

Конфиденциальная информация - это информация, не относящаяся к государственной тайне, не подлежащей огласке, то есть секретной.

К КИ относятся также:

- Персональные данные
- Коммерческая тайна

Персональные данные согласно Федеральному закону от 27 июля 2006 года 152-ФЗ «О персональных данных» - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

К персональным данным относятся:

- Общие.

К ним законодательство относит базовые личные данные: ФИО, место регистрации, информация об образовании, о месте работы, номер телефона, e-mail;

- Специальные.

Информация о личности человека: расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, подробности интимной жизни, информация о судимостях;

- Биометрические.

Физиологические или биологические особенности человека, которые используют для установления его личности: фотографии, отпечатки пальцев, анализ ДНК, группа крови, рост, цвет глаз, вес и другие;

- Иные**.**

К ним относят все данные, которые нельзя отнести к другим видам: принадлежность к определенной социальной группе, корпоративные данные и так далее.

Коммерческая тайна согласно Федеральному закону "О коммерческой тайне" от 29.07.2004 N 98-ФЗ», коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

В качестве коммерческой информации следует считать следующие сведения:

- Знания и опыт в области продукции на рынке и предоставления услуг;
- Производственные сведения
- Технические сведения
- Экономические сведения

- Организационные сведения
- Результат интеллектуальной деятельности
- Знать сведения о рыночной конкуренции;

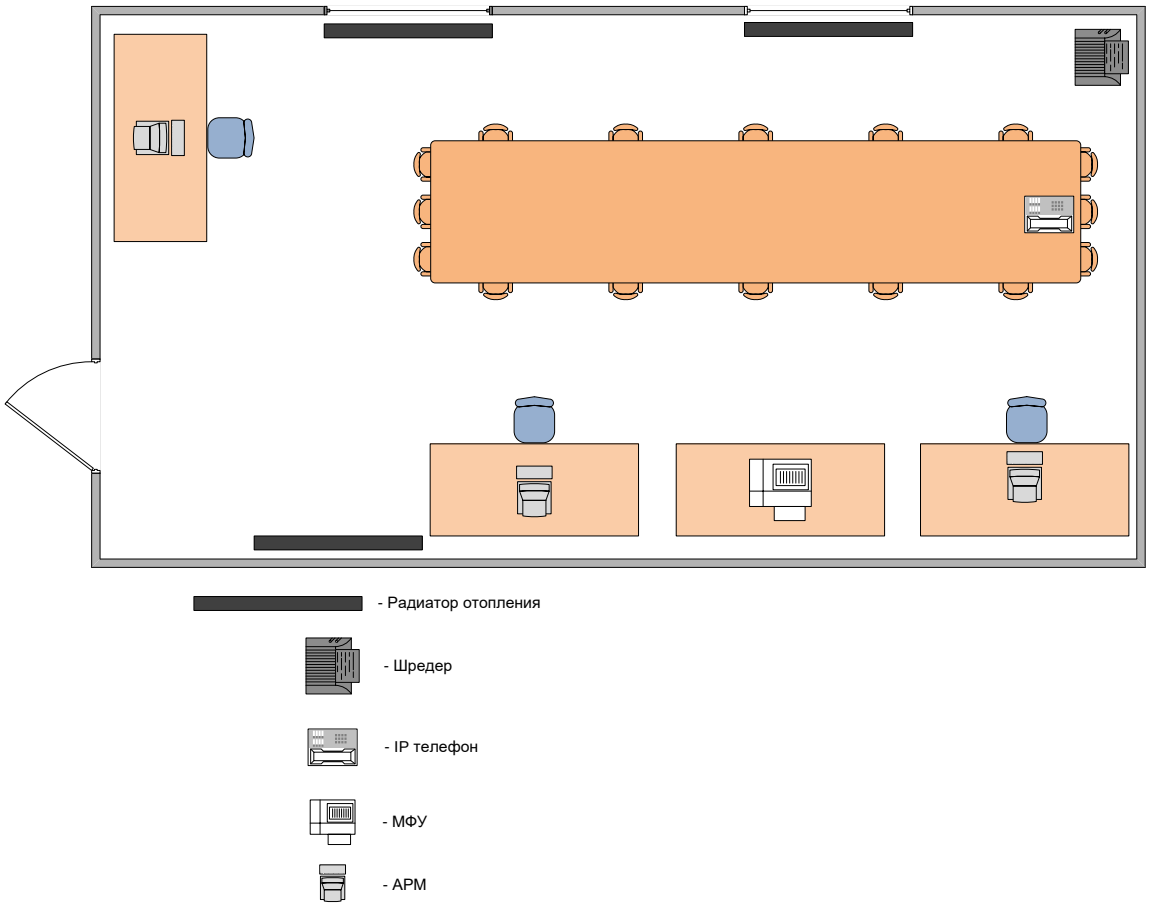
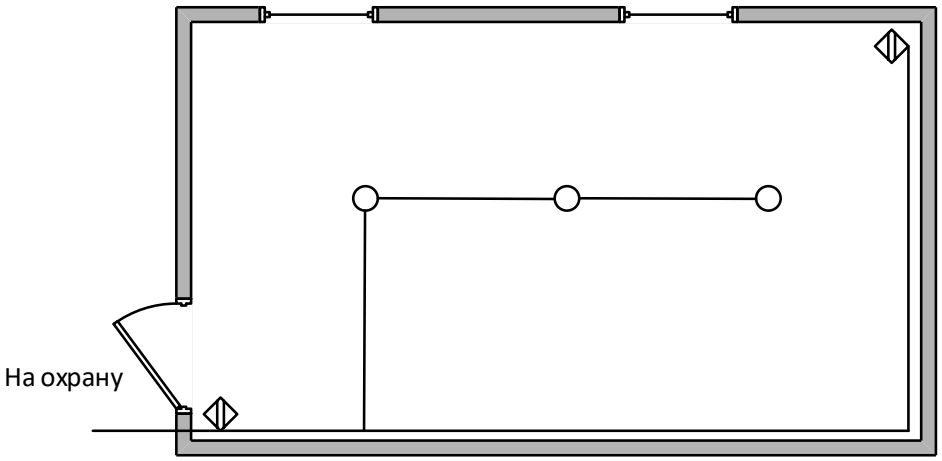


Рисунок 1 – Схема защищаемого помещения

Далее будут представлены схемы охранной и пожарной систем в ЗП на рисунке 2

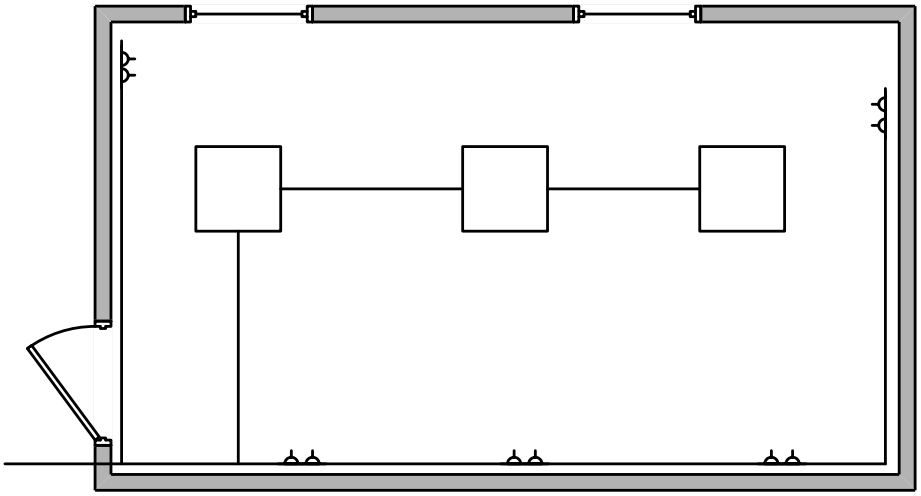


- Датчик движения

- Извещатель пожарный

Рисунок 2 - Схема охранной и пожарной системы

Также представлена схема электропитания в ЗП на рисунке 3



- Розетка 220 В

- Светильник

Рисунок 3 - Схема электропитания в ЗП

1.2. Анализ уязвимости объекта

Анализ уязвимости - это процесс выявления уязвимых мест объекта информатизации, реализуемого на нем производственно-технологического

процесса, существующей системы физической защиты; определения угроз, вероятных способов их осуществления и моделей нарушителей.

Требования и рекомендации направлены на исключение возможности перехвата конфиденциальной речевой информации, циркулирующей в защищаемом помещении, в системах звукоусиления (СЗУ), при осуществлении её магнитной звукозаписи и передачи по каналам связи.

При проведении мероприятий с использованием конфиденциальной речевой информации и технических средств ее обработки возможна утечка информации за счет следующих технических каналов:

- акустического излучения;
- виброакустических сигналов;
- прослушивания разговоров, ведущихся в ЗП;
- электрических сигналов;
- побочных электромагнитных излучений;
- радиоизлучений;

Также следует учитывать возможность хищения технических средств с хранящейся в них информацией или отдельных носителей информации.

Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях:

Ссылаясь на руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» (приказ Гостехкомиссии России от 30 августа 2002 г. № 282):

В организации должен быть документально определен перечень ЗП и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации, а также составлен технический паспорт на ЗП.

Защищаемые помещения следует размещать в пределах КЗ. Также рекомендуется размещать их на удалении от границ КЗ. Ограждающие конструкции не должны являться смежными с помещениями других учреждений. ЗП не рекомендуется располагать на первом этаже. Что бы

предотвратить просмотр через окна помещения нужно установить на них жалюзи или рольставни.

Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой связи, переносных аудио и видеозаписи. При установке в ЗП телефонных аппаратов следует отключать их из сети во время проведения мероприятий составляющую конфиденциальную информацию.

Для исключения возможных утечек информации за счет электроакустического преобразования рекомендуется использовать в ЗП сертифицированные СЗИ от утечки за счет электроакустического преобразования.

Системы пожарной и охранной сигнализации ЗП должны выходить на пульт охраны, который находиться в пределах КЗ.

Для обеспечения должного уровня звукоизоляции в помещении следует оборудовать дверные проемы тамбурами с двойными дверями, устанавливать дополнительные рамы в оконных проемах, уплотнительных прокладках в дверных и оконных.

В случае если, выше описанные методы, не обеспечивают должную безопасность, следует прибегнуть к организационно режимным мерам.

Что бы снизить вероятность перехвата информации по виброакустическому каналу должны быть приняты организационно режимные меры, которые исключают возможность установки посторонних предметов на внешней стороне ограждающих конструкций ЗП.

Что бы снизить уровень виброакустического сигнала следует системы отопления, вентиляции оборудовать звукоизолирующими экранами.

Если указанные меры защиты информации от утечки по акустическому и виброакустическому каналам недостаточны, следует применять метод активного акустического или виброакустического маскирующего зашумления.

Для этой цели применяются сертифицированные средства активной защиты

При использовании ЗП нужно предусматривать организационно-режимные меры, направленные на исключение несанкционированного доступа в помещение:

- двери ЗП, если в них ничего не проводится, необходимо закрывать на ключ;
- ключи от ЗП должны выдаваться только лицам ответственным за это помещение либо тем, кто в нем работает;
- установка и замена оборудования, мебели, ремонт ЗП должны производиться только под контролем специалиста по защите информации.

1.3. Модель угроз.

Модель угроз информационной безопасности (ИБ) — это описание существующих угроз, насколько они реалистичны, каковы шансы, что они воплотятся в жизнь, и, само собой, каковы последствия. С помощью грамотных МУ можно повысить уровень ИБ и даже затраты на защиту оптимизировать, сосредоточившись на самых вероятных угрозах.

Рассматривая данный объект информатизации можно описать вероятную модель угроз.

В первую очередь нужно рассмотреть контролируемую зону, в данном случае граница контролируемой зоны можно бы было считать ограждающие конструкции по периметру объекта информатизации, но смотря на план объекта можно заметить, что ограждение не смыкается по периметру объекта информатизации, этого нельзя сделать в связи с тем, что объект информатизации находиться рядом с водоемом.

Береговая линия — это общественный участок, располагающийся вдоль водоема. Для большинства водоемов его ширина составляет 20 м. Ширина береговой линии каналов, рек и ручьев, длина которых от истока до устья не превышает 10 км, составляет 5 м. Береговая линия – это береговая линия от

уреза воды – водохранилища. Ограничение доступа и приватизация участков, в том числе прибрежных полос, незаконны. Пункт 8 статьи 6 Водного кодекса Российской Федерации запрещает ограничение прохода вдоль береговой линии (исключения из этого запрета отсутствуют). Пункт 8 статьи 27 Земельного кодекса Российской Федерации запрещает приватизацию земель в прибрежной зоне. (в ред. Федерального закона от 13.07.2015 N 244-ФЗ).

Из выше сказанного закона невозможно установить ограждающие конструкции по периметру объекта информатизации. Исходя из этого можно предположить, что нарушитель сможет проникнуть на охраняемую территорию минуя ограждающие конструкции.

Так же из-за того, что окна помещения ООО «Газпром Интернешнл» выходят на р. Большая Невка, злоумышленники могут подойти в плотную к окнам для установки средств разведки информации, либо установить возимые средства разведки у берега реки.

К модели угроз также можно отнести следующие пункты:

- Кража носителей информации;
- Кража ключей и атрибутов доступа;
- Несанкционированное отключение средств защиты;
- Утрата ключей и атрибутов доступа;
- Непреднамеренное отключение средств защиты;
- Выход из строя аппаратно-программных средств;
- Сбой системы электроснабжения;
- Стихийное бедствие;
- Угрозы преднамеренных действий внутренних нарушителей.

1.4. Модель нарушителя.

Модель нарушителя – это предположения о возможных нарушениях, со стороны злоумышленника. Планирование того как можно предотвратить те или иные атаки.

Нарушитель (субъект атаки): лицо, проводящее атаку.

Все потенциальные нарушители подразделяются на:

- внешний нарушитель, атаки осуществляются за пределами КЗ;

В качестве внешнего нарушителями могут выступать:

- бывшие сотрудники Организации;
- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке;
- представители преступных организаций.

- внутренних нарушителей, атаки осуществляются в пределах КЗ;.

В качестве внутреннего нарушителями могут выступать все сотрудники предприятия. Виды нарушителей приведены в таблице № 1.

Таблица № 1 – Виды нарушителей. Угрозы и риски

Тип нарушителя	Категория	Угроза	Риск
Внутренний	Сотрудники, имеющие санкционированный доступ к материальным ценностям	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
	Сотрудники, имеющие доступ к финансовым ценностям	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
	Сотрудники, имеющие доступ к служебной информации	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
	Сотрудники, имеющие доступ к элементам системы защиты	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
	Обслуживающий персонал (охрана, инженерно-технические службы)	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
Внешний	Уполномоченный персонал разработчиков, который имеет право на техническое обслуживание	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
	Уволенный сотрудник	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов

	Недобросовестные партнеры	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
	Посетители	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов
	Конкуренты	Кража и распространение конфиденциальной информации.	Потеря денежных средств компании, персональных данных сотрудников клиентов

1.5. Контролируемая зона.

Контролируемая зона - пространство, в котором запрещено неконтролируемое нахождение посторонних лиц, транспортных и технических средств.

Границей контролируемой зоны может быть: периметр охраняемой территории, организации, ограждающие конструкции, части здания, защищаемого помещения.

Контролируемая зона может, быть периметром охраняемой территории частично, охраняемой территорией, охватывающей здания и сооружения, в которых проводятся конфиденциальные мероприятия, частью зданий, комнат, кабинетов, в которых проводятся конфиденциальные мероприятия. Контролируемая зона может устанавливаться размером больше, чем охраняемая территория, при этом она должна обеспечивать постоянный контроль за неохраняемой частью территории.

Рассматривая данный объект информатизации исходя из пункта 1.1(Модель угроз), контролируемой зоной являются ограждающие конструкции здания.

Схема расположения контролируемой зоны изображена на рисунке 4

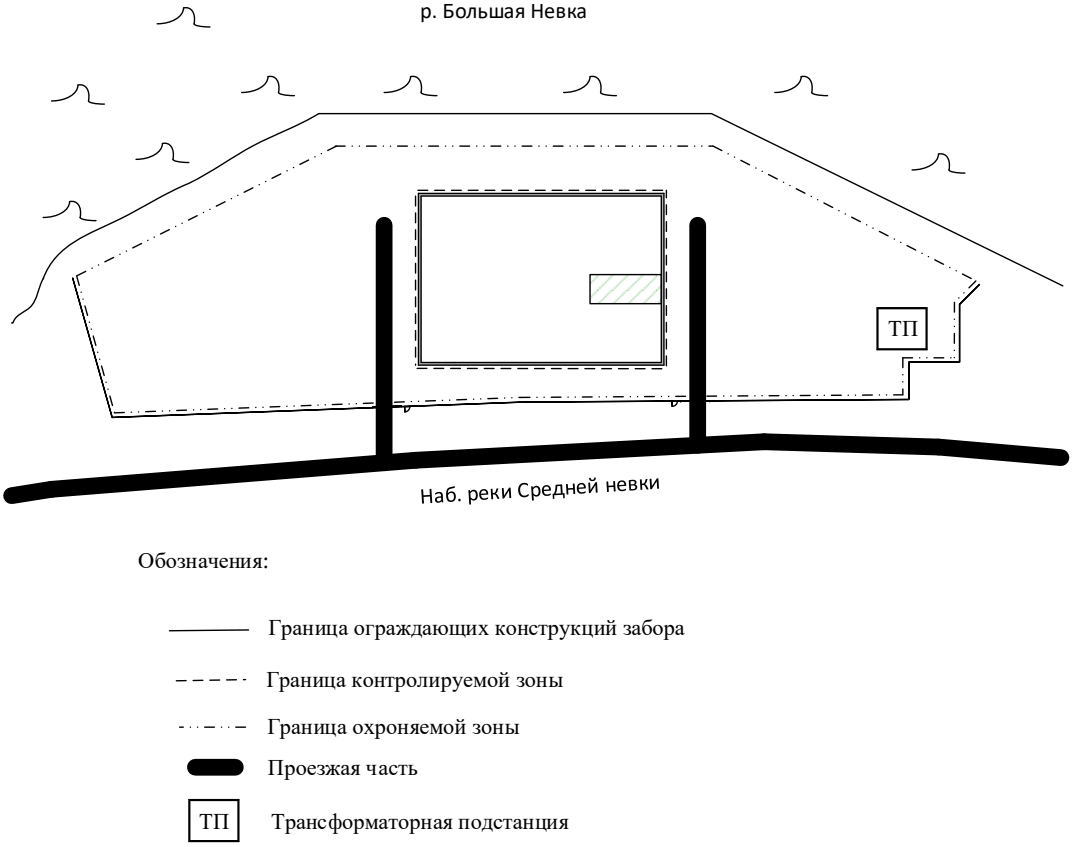


Рисунок 4 - Схема расположения контролируемой зоны

Так же у объекта информатизации имеется охраняемая зона.

Охраняемая зона - территория, в пределах которой устанавливается специальный режим охраны размещаемых объектов.

Охраняемой зоной принято считать ту зону, которая имеет:

1. Оградительные конструкции
2. Видеонаблюдение по периметру ограждающих конструкций
3. Круглосуточное дежурство как минимум одного охранника
4. Охранная сигнализация

Охраняемая зона изображена на рисунке 5

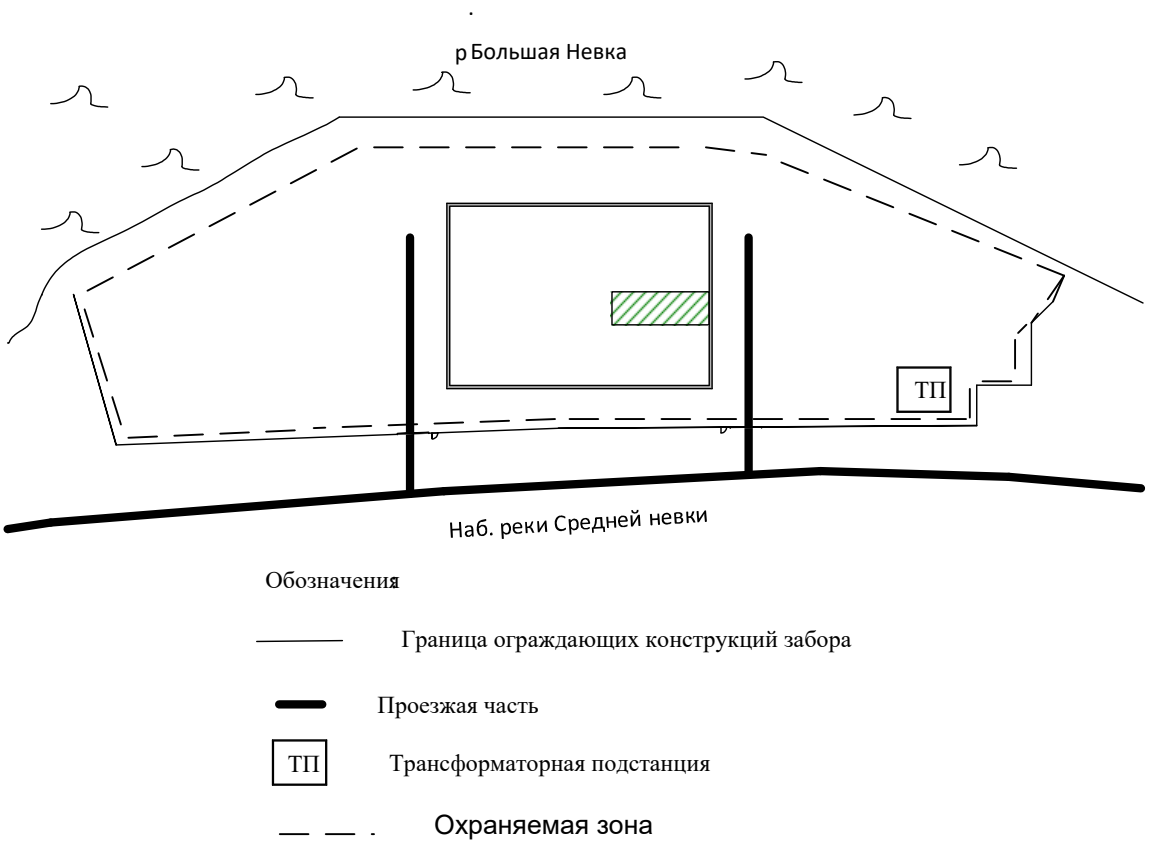


Рисунок 5 –Охраняемая зона.

1.6. Возможные технические каналы утечки информации.

Конфиденциальная информация объединяет различные виды конфиденциальной информации, которые в силу своей важности и ценности для правообладателя не могут быть раскрыты или переданы третьим лицам. В связи с этим статусом и для защиты такой информации введен в действие 149-ФЗ от 27 июля 2006 г., в котором указан перечень охраняемых данных и порядок обращения с ними. При согласовании и использовании технических средств обработки и передачи информации могут быть следующие каналы утечки и источники угроз информационной безопасности.

Определение понятия конфиденциальных данных не может быть обозначено точно из-за того, что в данную категорию попадает свыше десятка видов. Принято считать, что конфиденциальная информация – это сведения тайного характера, которые нельзя показать публично и находящиеся под

охраной закона. В первую очередь это личные данные людей, государственная, коммерческая тайны. Полный список обозначен в Указе Президента РФ от 13.07.2015 года за № 357.

Виды технических каналов утечки информации:

- Акустическое излучение информативного речевого сигнала
- Электрические сигналы, возникающие при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющийся по проводам, выходящим за пределы КЗ.
- Виброакустические сигналы, возникающие при преобразовании информативного акустического сигнала за счет воздействия его на строительные конструкции и инженерно-технические коммуникации ЗП
- Несанкционированный доступ к обрабатываемой в АС информации и несанкционированные действия с ней
- Воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедренных программных средств
- Побочные электромагнитные излучения информативных сигналов от технических и линий передачи информации
- Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ
- Радиоизлучения, модулированные информативным сигналом возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах технических средств
- Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных

устройств съема речевой информации (закладочные устройства), модулированные информативным сигналом

- Радиоизлучения или электрические сигналы от электронных устройств перехвата информации\. Подключенных к каналам связи или техническим средствам обработки информации
- Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств
- Прослушивание телефонных и радиопереговоров
- Хищение технических средств с хранящейся в них информацией или носителей информации

Перехват информации или воздействие на нее с использованием технических средств могут вестись:

- Из-за границы КЗ из близлежащих строений и транспортных средств
- Из смежных помещений, принадлежащих другим организациям и расположенных в том же здании, что и объект защиты
- При посещении организации посторонними лицами
- За счет несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС как с помощью технических средств АС, так и через сети

Для перехвата и воздействия на информацию могут использоваться портативные возимые и носимые устройства, которые размещаются рядом с объектом информатизации или подключаются к каналам связи или техническим средствам обработки конфиденциальной информации

Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, за счет следующих действий:

- Непреднамеренное прослушивание без использования технических средств конфиденциальных разговоров, из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем
- Некомпетентных или неправильных действий пользователей и администраторов.

Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств:

- Речевой информации, циркулирующей в ЗП
- Информации, выводимой на экраны видеомониторов
- Информации, хранящейся на физических носителях, в том числе выходящих в состав АС
- Информации, передаваемой по каналам связи, выходящим за пределы КЗ

Меры по обеспечению защиты информации выполняются подразделениями по защите информации либо же осуществляются другими компаниями, имеющими лицензию.

Исходя из пункта 1.1 видно, что контролируемая зона проходит по зданию. То есть нарушитель может проникнуть на охраняемую территорию и разместить различные типы средств разведки. Контролируемая зона изображена на рисунке 6.

Рисунок 6 – контролируемая зона

Например:

1. Перехват информации по акусто-вибрационному каналу утечки:

- Скрытое прослушивание(запись) разговоров. Для этого используют электронные стетоскопы;
- Установка закладных устройств в смежных помещениях;

2. Оптико-электронный (лазерный микрофон):

- Облучение оконных стекол ЗП лазерными акустическими система. Как правило эти системы устанавливаются за пределами КЗ, в ближайших зданиях или транспортных средствах;

3. Непреднамеренное прослушивание: данный канал утечки информации не рассматривается, так как потенциальных врагов в здании нет.

4. Акустический (микрофонный эффект)

- Направленные микрофоны, устанавливают в ближайших зданиях или транспортных средствах, которые находятся за пределами КХ;

Перехват информации с использованием технических средств ведутся:

- Из-за границы КЗ из близлежащих строений и транспортных средств
- При посещении организации посторонними лицами

1.7. Риски для каждого технического канала утечки информации.

- Акустическое излучение информативного речевого сигнала
- Электрические сигналы, возникающие при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющийся по проводам выходящим за пределы кз.
- Виброакустические сигналы, возникающие при преобразовании информативного акустического сигнала за счет воздействия его на строительные конструкции и инженерно-технические коммуникации ЗП
- Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации (закладочные устройства), модулированные информативным сигналом
- Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств.
- Прослушивание телефонных и радиопереговоров.

Ссылаюсь на методику ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России 14 февраля 2008 г»

Частота реализации угрозы определяется экспертным путем. Показатель характеризует насколько вероятным является реализация конкретной угрозы безопасности для ЗП. Вводятся четыре градации этого показателя:

- маловероятно – отсутствуют предпосылки для осуществления угрозы;

- низкая вероятность – предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию;
- средняя вероятность - предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;
- высокая вероятность - предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности не приняты.

При составлении перечня актуальных угроз, устанавливается соответствующий числовой коэффициент Y2:

1. 0 маловероятная угроза;
2. 2 низкая вероятность угрозы;
3. 5 средняя вероятность угрозы;
4. 10 высокая вероятность угрозы.

Угрозы и их характеристики рассмотрены в таблице № 2.

Таблица № 2 - Угроз и их характеристик приведена ниже

Наименование угрозы	Вероятность (Y2)	Реализуемость (Y)	Опасность	Актуальность
Угрозы утечки информации по техническим каналм				
Акустическое излучение информативного речевого сигнала	высокая вероятность (10)	высокая (0.75)	высокая	актуальная
Виброакустические сигналы	высокая вероятность (10)	средняя (0.75)	высокая	актуальная
Просмотр информации с различных носителей информации	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Прослушивание телефонных и радиопереговоров	средняя вероятность (5)	средняя (0.5)	средняя	актуальная
Снятие информации за счет оптико-электронного канал утечки	высокая вероятность (10)	высокая (0.75)	высокая	актуальная

Проведя анализ таблицы - Угроз и их характеристик, были выявлены три высоких вероятности опасности и две средних, исходя из этого был сделан вывод, что данный объект информатизации защищен на 25%.

Для расчета коэффициента реализуемости угроз Y применяется следующая формула:

Y=(Y1+Y2)/20**.**

Характеристики технических каналов утечки информации.

Акустический канал

- Воздушные

Перехват сигналов микрофонами.

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются специальные направленные микрофоны.

- Электроакустические

Перехват колебаний через ВТСС

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС.

- Вибрационные

Перехват сигналов электронными стетоскопами

В вибрационных ТКУИ средой распространения акустических сигналов являются конструкции зданий, сооружений, трубы водоснабжения, отопления. Для перехвата акустических колебаний в этом случае используются стетоскопы.

- Оптико-электронные

Перехват сигналов путем лазерного зондирования оконных стекол.

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле отражающих поверхностей. Отраженное лазерное излучение принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация.

Оптический канал

В оптическом канале получение информации возможно путём:

- визуального наблюдения,
- фото или видеосъемки,
- использования видимого и инфракрасного диапазонов для передачи информации от скрыто установленных микрофонов и других датчиков.

К утечке информации в оптических каналах относятся:

- безвоздушное пространство;
- атмосфера;
- оптические световоды.

1.8. Методика проведения аттестации

Ссылаясь на документ «положение по аттестации объектов информатизации и ГОСТ РО 0043-003-2012»

Аттестация – представляет из себя комплекс организационно-технических мероприятий, по итогам которых выдается специальный документ — «Аттестата соответствия» — подтверждается, соответствие объекта требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России».

Перечень работ при аттестации:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Аттестация защищаемого помещения обязательна при получении и осуществлении следующих работ:

1. Лицензии ФСТЭК России на техническую защиту КИ.
2. Лицензии ФСТЭК России на разработку и производство СЗИ для конфиденциальной информации.

Для того чтобы выполнить требования закона ФЗ-98 «О коммерческой тайне» и ФЗ-149 «Об информации, информационных технологиях и о защите информации» организации, в которой обрабатывается конфиденциальная информация, требуется обеспечить защиту.

Для проведения переговоров, составляющие конфиденциальную информацию, лучшим способом защиты является защищаемое помещение.

Проводить работы по аттестации ЗП могут только лицензиаты ФСТЭК России

В лицензии в обязательном порядке должны быть указаны следующие виды деятельности:

- Контроль защищенности КИ от утечки по техническим каналам в: ЗП;
- Аттестационные испытания и аттестация на соответствие требованиям по защите информации: защищаемых помещениях;

У лицензиата ФСТЭК обязательно должно быть в собственности следующее специальное контрольно-измерительное оборудование:

- низкочастотные генераторы сигналов,
- измерительные микрофоны,
- усилители мощности,
- акустические излучатели,
- измерители шума и вибраций,
- генераторы шумовых сигналов,
- селективные нановольтметры,
- вибродатчики (акселерометры),

Требования к оборудованию установлены ФСТЭК России следующим документом «Перечень контрольно-измерительного и испытательного оборудования, средств контроля защищенности, необходимых для выполнения работ и оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79».

Работы по проведению аттестационных испытаний в защищаемых помещениях довольно трудоемкие, так как нужно провести большое количество измерений. Часто измерения приходится осуществлять в труднодоступных местах. Также, данные работы требуют достаточное количество знаний в сфере защиты информации от утечки по техническим каналам информации.

Организационные меры защиты информации:

- Разработка систем и мероприятий по допуску посторонних лиц на объект
- Разработку и планирование мероприятий по обучению персонала, аттестации и контроля знаний в области работы с конфиденциальной информацией.
- Назначение ответственного за помещение;

- Инструкция по эксплуатации СЗИ;
- Назначить ответственного за организацию обработки ПДн – издание соответствующего приказа или распоряжения;
- Издать политику в отношении обработки ПДн;
- Ознакомить и (или) обучить работников, осуществляющих обработку ПДн, с требованиями по защите ПДн;
- Определить угрозы безопасности ПДн, то есть составить модель угроз;
- Установить правила доступа к персональным данным, например, вести журнал учета допущенных к обработке ПДн ;
- Обеспечить регистрацию и учет действий, совершаемых с персональными данными в информационной системе.
- ВТСС перед проведением аттестационных испытаний должны быть проверены на предмет отсутствия в них специальных электронных устройств несанкционированного перехвата информации.

1.9. Выводы по первой главе: в первой главе мы рассмотрели какие технические каналы утечки информации есть на рассматриваемом объекте информатизации, а также разобрались с понятием «Аттестация». Теперь мы имеем представление о различных технических каналах утечки информации и далее рассмотрим методы защиты от них.

ГЛАВА 2 АНАЛИЗ СОСТОЯНИЯ ИЗУЧАЕМОЙ ПРОБЛЕМЫ В ОРГАНИЗАЦИИ

2.1. Установка средств защиты информации для блокировки ТКУИ

1. Акустический канал изображен на рисунке 7;

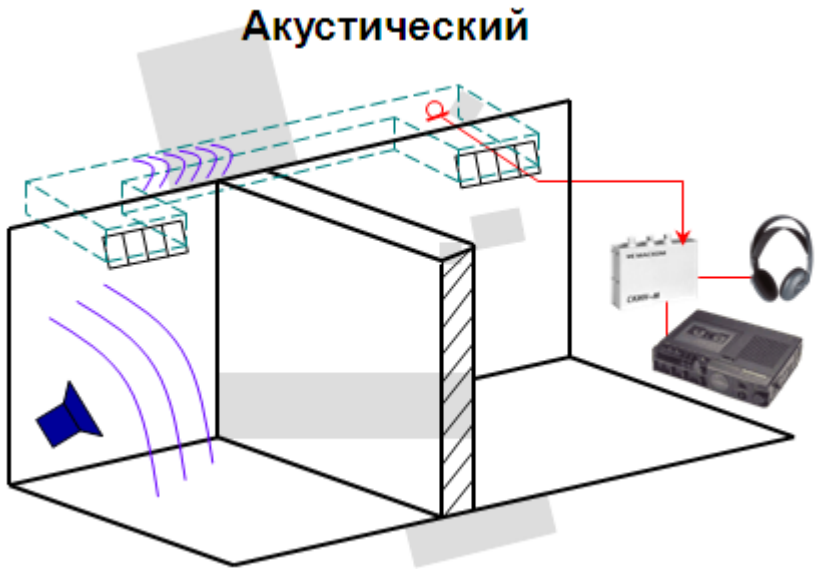


Рисунок 7 – Акустический канал

К акустическому каналу можно отнести следующие средства защиты информации:

- Акустические излучатели;
- Виброизлучатели.

2. Виброакустический канал изображен на рисунке 8;

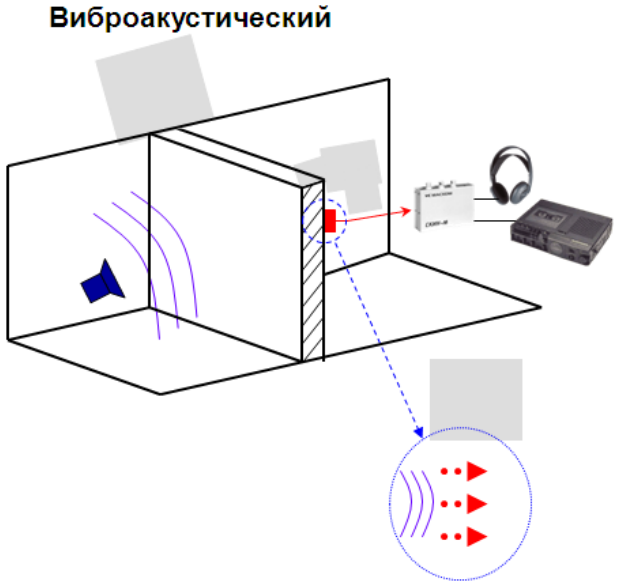


Рисунок 8 – Виброакустический канал

К акусто-вибрационному каналу можно отнести следующие средства защиты информации:

- Акустические излучатели;
- Виброизлучатели.

3. Оптико-электронный(лазерный) канал изображен на рисунке 9.

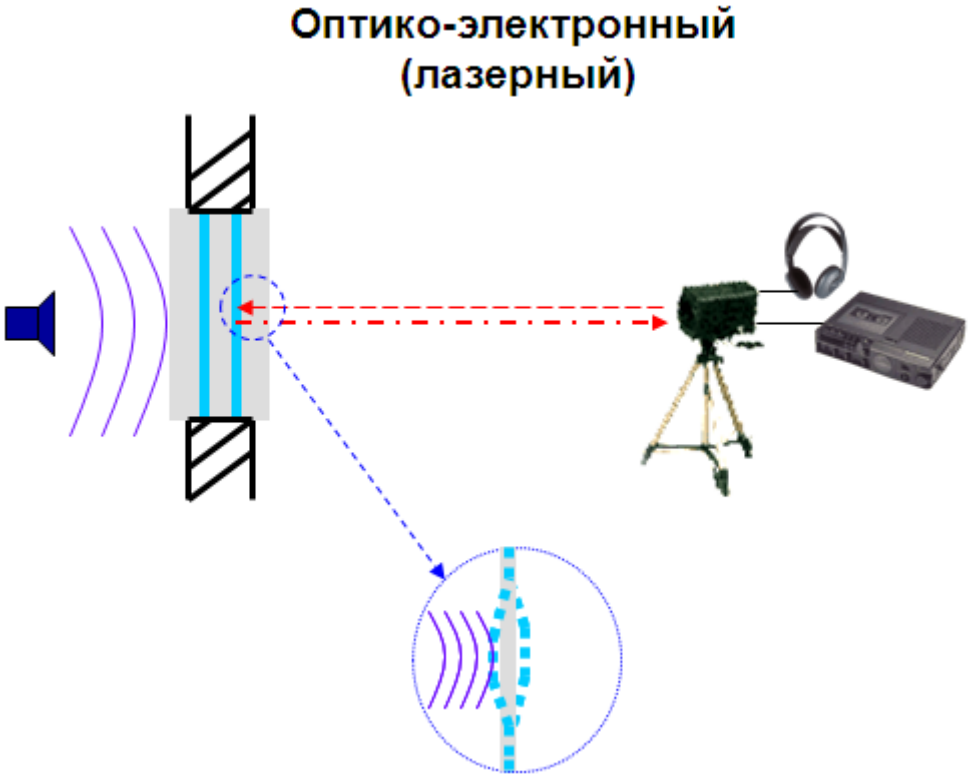


Рисунок 9 – Оптико-электронный канал

К оптико-электронному каналу можно отнести следующие средства защиты информации:

- Акустические излучатели;
- Виброизлучатели ;
- Жалюзи;
- Рольставни.

2.2. Виды средств защиты информации от утечки по ТКУИ.

Средства защиты информации – это различные технические, электронные устройства, которые устанавливаются в защищаемых помещениях для увеличения безопасности защиты информации, которая обрабатывается в этом помещении.

В соответствии с «Приказ 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» средства защиты информации должны пройти оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ «О техническом регулировании»

Средства защиты информации разделяются на следующие группы:

- Технические средства. Это различные типы средств защиты, которые решают задачи защиты информации. Они препятствуют физическому проникновению, и, если проникновение произошло, то блокируется доступу к информации. Эти задачи решают замки, решетки на окнах, защитная сигнализация и др. А также генераторы шума, сетевые фильтры, закрывающие технические каналы утечки информации. Технические средства достаточно надежны, устойчивы к модификациям. Из слабых сторон это относительно большие объем и масса и высокая стоимость.
- Программные СЗИ. К программным средствам защиты относятся такие программы, как идентификация пользователя, контроль доступа, шифрование информации, удаление остаточной информации Преимуществами программных средств являются универсальность, гибкость, надежность и простота использования. Минусы - ограниченные сетевые возможности, использует часть ресурсов файловых серверов.

Рассматривая данный объект информатизации, программные средства защиты информации не будут использоваться, так как в задачах не рассматриваются ОТСС.

- Смешанные аппаратно-программные средства у них те же функции, что у аппаратных и программных средств защиты по отдельности
- Организационные средства защиты складываются из организационно-технических и организационно-правовых. Преимущества организационных средств то что они позволяют решать множество различных

проблем, легки в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности улучшения и развития. Из недостатков — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

В данном случае будут рассматриваться технические(аппаратные) средства защиты информации.

Технические средства бывают активные и пассивные, и обеспечивают защиту нашей информации от какой-либо утечки по разным техническим каналам утечки, что возникают в связи с применением средств, необходимых для ее обработки.

устройства по источнику воздействия:

- электромеханические;
- электронные;
- механические и др.

Они решают проблему информационной защиты на срезе оборудования: или полностью предотвращают возможное проникновение, или, если такое случилось, становятся препятствием дальнейшей возможности свободного получения имеющихся данных.

Используется и различная маскировка такой информации. Одну часть такого задания могут выполнять:

- наличие защитной сигнализации;
- установка решеток на окнах;
- использование замков и др.

Другую часть выполняют:

- установленные сканирующие радиоприемники;
- различные сетевые фильтры; детекторы;
- антижучки;
- используемые генераторы шума, а также множество других разнообразных устройств.

Для защиты конфиденциальной информации используются сертифицированные по требованиям безопасности информации технические средства защиты информации. Порядок сертификации определятся законодательством РФ.

Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами Гостехкомиссии России и требованиям настоящего документа.

Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителей организаций, эксплуатирующих объекты информатизации.

Рекомендуются следующие стадии создания СЗИ**:**

- предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации;
- стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

На предпроектной стадии по обследованию объекта информатизации:

- устанавливается необходимость обработки конфиденциальной информации на данном объекте информатизации;
- определяется какая конфиденциальная информация, нуждается в защите от утечки по техническим каналам;
- определяются угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;

- определяются условия расположения объектов информатизации относительно границ КЗ;
- определяются конфигурация и топология автоматизированных систем и систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определяются технические средства и системы, предполагаемые к использованию в разрабатываемой АС и системах связи, условия их расположения, общесистемные и прикладные программные средства, имеющиеся на рынке и предлагаемые к разработке;
- определяются режимы обработки информации в АС в целом и в отдельных компонентах;
- определяется класс защищенности АС;
- определяется степень участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой и со службой безопасности;
- определяются мероприятия по обеспечению конфиденциальности информации в процессе проектирования объекта информатизации.

Аналитическое обоснование необходимости создания СЗИ содержит:

- информационную характеристику и организационную структуру объекта информатизации;
- характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;
- возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- перечень предлагаемых к использованию сертифицированных средств защиты информации;

- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;
- ориентировочные сроки разработки и внедрения СЗИ;

перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

2.3. Анализ рынка производителей СЗИ

ЗАО "АННА"

Основные направления деятельности Фирмы:

Научно-производственная деятельность:

- разработка систем быстрого немедленного информации на магнитных носителях;
- оборудование различных помещений техническими средствами защиты информации;
- разработка нестандартного радиоэлектронного оборудования.
- серийное производство средств защиты информации:
- технические средства защиты информации:
- по сети 220 В
- по виброакустическим каналам
- аппаратура дистанционного управления комплексами технических средств защиты информации.

ООО "Сюртель"

Их работа основана на научно-технической разработке и производстве технических средств защиты информации, комплексов регистрации и оповещения, специальных технических средств негласного контроля информации.

Компания проводит сертификацию информационных объектов, инспектирует объекты и технические средства на предмет наличия скрытно установленных средств перехвата информации, специализируется на исследованиях, по оценке защищенности информационных объектов.

Центр Безопасности Информации "Маском"

Центр безопасности информации "МАСКОМ", был онснован в 1991 году, сейчас является многопрофильным предприятием, оказывающим широкий спектр услуг в области обеспечения безопасности информации:

- научные разработки в области безопасности информации;
- проектирование ИС, зданий и объектов в информационно-защищенном исполнении;
- разработка и производство средств и систем безопасности информации;
- различные виды исследований и испытаний каналов утечки информации по техническим каналам;
- оснащение объектов инженерно-техническими средствами безопасности;

Лаборатория ППШ

Лаборатория ППШ одна из российских фирм, работающая в области защиты информации от несанкционированного доступа и от утечки по техническим каналам.

ООО "Газинформсервис"

Организация ООО «Газинформсервис» специализируется на разработке и внедрении комплексных систем защиты информации для предприятий всех форм собственности.

В структуре предприятия имеются подразделения, которые занимаются решением актуальных задач обеспечения информационной безопасности информационных систем и телекоммуникационных сетей.

ЗАО «ЦБИ-сервис»

ЗАО «ЦБИ-сервис» специализируется в области обеспечения безопасности информационных технологий.

Спектр выполняемых ЗАО «ЦБИ-сервис» работ и оказываемых услуг включает:

- разработка, производство и внедрение технических и программных систем защиты информации;
- Сертификация средств безопасности, средств и систем ограничения доступа к информации на соответствие требованиям информационной безопасности
- Идентификация каналов утечки информации, специальные исследования технических средств.

Помимо поставки покупных средств защиты информации, ЗАО «ЦБИ-сервис» также организует производство собственной продукции. К таким продуктам относятся программное обеспечение для управления безопасностью, защищенные ПК и другие средства обеспечения безопасности.

2.4. Разработка варианта внедрения СЗИ на объекте информатизации.

После проведения анализа рынка производителей СЗИ для сравнения были взяты две компании НПО «АННА» и «Лаборатория ППШ». Далее будет приведено сравнение двух организаций и вывод, чьи средства защиты информации лучше подойдут к данному объекту инфомратизации.

1)НПО «АННА», СЗИ «Соната-АВ-4Б».

1.Блоки электропитания и управления «Соната-ИП4.1»

Блоки электропитания и управления "Соната-ИП4.1", "Соната-ИП4.2" и "Соната-ИП4.3" предназначены для:

1)электропитания и управления подключаемыми к выходу "Нагрузка" элементами системы активной акустической и вибрационной защиты акустической речевой информации "Соната-АВ" модель 4Б (далее — Системы) в ходе ее эксплуатации;

2) управления подключаемыми к выходу "Нагрузка" средств активной защиты информации от утечки за счёт ПЭМИН ("Соната-Р3", "Соната-Р3.1", "Соната-РС3");

3) автоматический контроль исправности и режимов работы подключенных к нему устройств;

4) настройки (установки интегрального уровня, корректировки спектра и т.п.) изделий, перечисленных в п.1 и п.2, и считывания из них служебной информации (состояние счетчика наработки, код ошибки при отказе, индивидуальный адрес и т.п.), при инсталляции (проверке) комплекса технических средств защиты информации. «Соната-ИП4.1» представлена на рисунке 10. Параметры «Соната-ИП4.1» приведены в таблице №3

Соната-ИП4.1. Вид спереди

Рисунок 10 – «Соната-ИП4.1»

Цена: 26 400,00р.

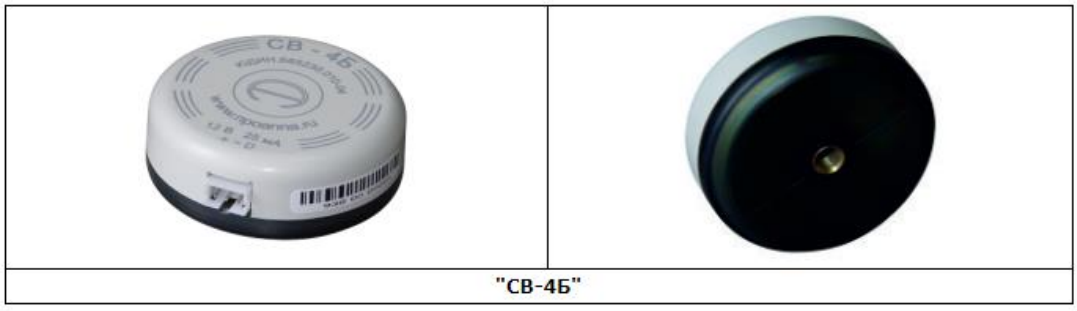
Таблица №3

Параметр	Значение	
	"Соната-ИП4.1"	"Соната-ИП4.3"
Количество "физических" выходов для подключения нагрузок	1	
Количество "логически" управляемых устройств, шт., не менее	239	
Выходное напряжение, В	12,5 ± 0,5	
Интерфейс/протокол управления подключаемыми к выходу "Нагрузка" устройствами	ReBus-3 (3-проводный)	
Нагрузочная способность[1)], мА, не более	1500	500
Мощность, потребляемая от сети, Вт, не более	40	8
Электропитание	сеть ~220В/50Гц	
Виды индикации (отображаемая информация)	световая, звуковая	
Интерфейс для подключения к управляющей ПЭВМ	USB 2.0	
Интерфейс удаленного мониторинга	Нет	Нет
Программное обеспечение для настройки подключаемых к выходу "Нагрузка" устройств	СПО "Камертон"	
Программное обеспечение для удаленного мониторинга элементов Системы	Нет	Нет
Габаритные размеры, мм, не более	Габариты и вес изделий	
Условия эксплуатации: температура окружающей среды	от +5 до +40 ˚С	

относительная влажность воздуха	до 80 % при температуре +25 ˚С

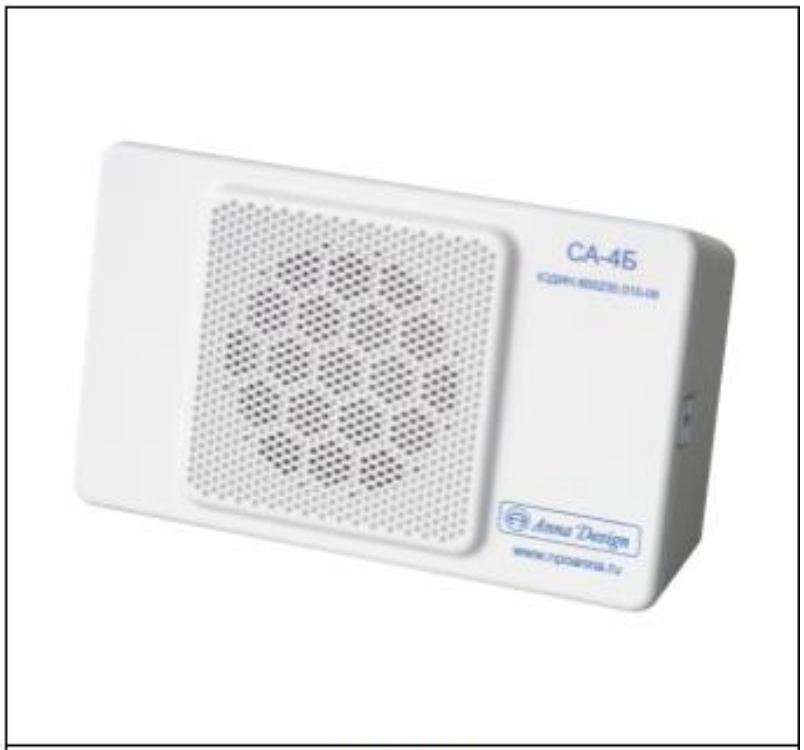
2.Генератор-акустоизлучатели «СА-4Б» и генератор-вибровозбудитель «СВ-4Б»

Генераторы-акустоизлучатели "СА-4Б", и генератор-вибровозбудитель "СВ-4Б" представляют собой электроакустические преобразователи со встроенными генераторами электрического шумового напряжения, предназначенные для построения систем защиты информации от утечки по акустическим и виброакустическим каналам и входят в состав системы виброакустической защиты "Соната-АВ4Б». Данные устройства приведены на рисунке 11 и рисунке 12. Технические характеристики приведены в таблице №4



"СВ-4Б"

Рисунок 11 – «СВ-4Б »



"СА-4Б"

Рисунок 12 – «СА-4Б »

Излучатели нового поколения ("СА-4Б", "СВ-4Б") позволяют динамически изменять настройки СВАЗ (т.е. изменение настроек в ходе эксплуатации системы). Это необходимо, для повышения комфорта многорежимного использования защищаемого помещения. Воспользоваться этой функцией возможно при использовании блока питания и управления "Соната-ИП4.1" и пульта дистанционного управления "Соната-ДУ4.3".

Цена:7 440,00руб.

Таблица №4 - Технические характеристики

Параметр	**"СА-4Б"**	**"СВ-4Б"**
Интерфейс управления	Rebus 3 (3 трехпроводный)	
Потребляемый ток, мА, не более	40	30
Электропитание, В, не менее	10	
Габариты изделия, мм, не более	Габариты и вес изделий	
Вес изделия, кг, не более		

Параметр	"СА-4Б"	"СВ-4Б"
Условия эксплуатации: - температура окружающей среды - относительная влажность воздуха	+5 ˚С ... +40 ˚С до 80 % при температуре +25 ˚С	

3.Пульт управления «Соната-ДУ4.3»

Он предназначен для управления системой, состоящей из генераторы-акустоизлучатель "СА-4Б", и генератор-вибровозбудитель "СВ-4Б" и блоком электропитания и управления «Соната-ИП4.1»

Взаимодействие с САЗ возможно только при наличии блока "Соната-ИП4.1". Пульт управления Соната – ДУ4.3 представлен на рисунке 13. Технические характеристики указаны в таблице № 5.

Рисунок 13 – Пульт управления Соната – ДУ4.3

Цена:7 680,00руб.

Таблица № 5 – Технические характеристики

Параметр	Значение
Интерфейс управления	ReBus-3
Напряжение электропитания, В, не менее	10
Ток, потребляемый от линии питания, мА, не более	60
Команды управления устройствами СВАЗ	переключение профилей защиты

Команды управления устройствами САЗ	включение / выключение
Виды индикации (отображаемая информация)	звуковая, визуальная
Габаритные размеры, мм, не более	Габариты и вес изделий
Условия эксплуатации: - температура окружающей среды - относительная влажность воздуха	от +5 до +40 ˚С до 80 % при температуре +25 ˚С

Размыкатели слаботочных линий "Соната-ВК4.1" предназначены для защиты информации от утечки за счет акустоэлектрических преобразований и ВЧ-навязывания по телефонным линиям и "Соната-ВК4.3" по линиям компьютерных сетей. "Соната-ВК4.1"и"Соната-ВК4.3"представлены на рисунке 14. Технические характеристики представлены в таблице № 6

"Соната-ВК4.1" "Соната-ВК4.3"

Рисунок 14 – "Соната-ВК4.1"и"Соната-ВК4.3"

Таблица № 6 – Технические характеристики

Параметр		**Соната-ВК4.1**	**Соната-ВК4.3**
Затухание сигнала в полосе частот, не менее	от 150 Гц до 150 кГц	60 дБ	
	от 150 кГц до 2 МГц	40 дБ	
	от 2 МГц до 10 МГц	30 дБ	
Контактное сопротивление, не более		200 мОм	
Проводность линии		4-х	8-ми
Параметры коммутируемой линии		Аналоговая телефонная линия	Кабельные линии (UTP и аналоги) компьютерной сети стандарта Ethernet 10/100

Параметр	Соната-ВК4.1	Соната-ВК4.3
Виды индикации (отображаемая информация)	Световая и звуковая	Световая: "Защита включена" и "Защита выключена"
Блок питания и управления	"Соната-ИП4.х"	
Электропитание, не менее	10 В	
Ток потребления, не более	50 мА	70 мА
Продолжительность непрерывной работы, не менее	8ч	
Условия эксплуатации: – температура окружающей среды – относительная влажность воздуха	+5 °С ... +40 °С до 80 % при температуре +25 °С	

Цена: 6 000,00руб.

Далее произведены расчеты средств защиты информации в таблице № 7

Таблица № 7 – расчет стоимости СЗИ НПО «АННА», «Соната-АВ-4Б»

Название СЗИ	Количество	Цена, за шт., руб.
Соната-ИП4.1	1	26 400,00
Соната-ДУ4.3	1	7 680,00
СА-4Б	2	7 440,00
СВ-4Б	5	7 440,00
Соната-ВК4.1	1	6000,00
Соната-ВК4.3	1	6000,00
Итог затраченных средств	11	98 160,00

2)«Лаборатория ППШ», СЗИ «ЛГШ-404».

Состав системы:

- Изделие «ЛГШ-404» - генераторный блок (35 700,00р.);
- Вибровозбудитель «ЛВП-10» - для установки на стены, трубы и окна (5 200,00р.);
- Акустический излучатель «ЛВП-2а» - для возбуждения маскирующих акустических помех (3 700,00р.);
- Размыкатель телефонных линий «ЛУР-4» (5 600,00р.);
- Размыкатель для Ethernet «ЛУР-8» (5 600,00р.).

Общая стоимость: 79 700,00 руб.

Исходя из выше описанного. выбор пал на систему защиты информации «Соната-АВ-4Б», так как она удовлетворяет предъявленным требованиям, более удобным способом установки, эксплуатации (параллельное подключение комплектующих) и ранее СЗИ была закуплена заказчиком.

2.5. Проверка наличия документации соответствующих требованиям на объекте.

Ссылаясь на Приказ ФСТЭК от 29 апреля 2021 г. №77 приведу список документов для проведения аттестационных испытаний.

«11. Для проведения работ по аттестации владелец объекта информатизации представляет в орган по аттестации следующие документы или их копии:

а) технический паспорт на объект информатизации по форме согласно приложениям N 1, 2 к настоящему Порядку;

б) акт классификации информационной (автоматизированной) системы по форме согласно приложению N 3 к настоящему Порядку, акт категорирования значимого объекта критической информационной инфраструктуры Российской Федерации (далее – акт категорирования значимого объекта);

в) модель угроз безопасности информации (в случае ее разработки в соответствии с требованиями по защите информации);

г) техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации объекта информатизации (для объекта информатизации, входящего в состав объекта капитального строительства, задание на проектирование (реконструкцию) объекта капитального строительства) (в случае их разработки в ходе создания объекта информатизации);

д) проектную документацию на систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации);

е) эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации;

ж) организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации (далее – документы по защите информации владельца объекта информатизации);

з) документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (в случае проведения анализа и испытаний в ходе создания объекта информатизации).

По решению владельца объекта информатизации, указанные в настоящем пункте документы (их копии) представляются в орган по аттестации в виде электронных документов.»

2.6. Анализ состояния ОТСС и ВТСС.

Рассматривая данный объект информатизации в помещении присутствуют следующие ОТСС и ВТСС, приведены в таблице №8.

Таблица № 8 – Описание состава ОТСС и ВТСС

	Название	Модель
№	ВТСС	
	Название	Модель
1.	АРМ №1 в составе	
1.1.	Системный блок	UNIVERSAL
1.2.	Монитор	Samsung 27V4L

1.3.	Клавиатура	Logitech K120
1.4.	Манипулятор «Мышь»	Logitech M90
1.5.	МФУ	HP MFP 135W
2.	АРМ №2 в составе	
2.1	Системный блок	UNIVERSAL
2.2	Монитор	Samsung 27V4L
2.3	Клавиатура	Logitech K120
2.4	Манипулятор «Мышь»	Logitech M90
3.	АРМ №3 в составе	
3.1.	Системный блок	UNIVERSAL
3.2.	Монитор	Samsung 27V4L
3.3.	Клавиатура	Logitech K120
3.4.	Манипулятор «Мышь»	Logitech M90
4.	Шредер	Deli Core E9954-EU
5.	IP телефон	Yealink
6.	МФУ	HP Laser MFP 135w
7.	Switch	D-Link DES-1005C
8.	Извещатель пожарный дымовой оптико-электронный	RUBEZH ИП 212-45
9.	Извещатель пожарный дымовой оптико-электронный	RUBEZH ИП 212-45
10.	Извещатель пожарный дымовой оптико-электронный	RUBEZH ИП 212-45
11.	Извещатель охранный объемный инфракрасный	Риелта Фотон-12 (ИО409-17/1)
	ОТСС	
12.	Отсутствуют в помещении	

В рассмотренном помещении отсутствуют ОТСС, так как в нем будут проводиться совещания, переговоры и другие виды мероприятий в ходе которых будет озвучиваться конфиденциальная информация.

2.7. Вывод по второй главе: в данной главе было рассмотрено что из себя представляют средства защиты информации. Были выбраны конкретные виды СЗИ по ТКУИ и произведены расчеты затраченных ресурсов.

ГЛАВА 3 ПРОВЕДЕНИЕ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ.

3.1. Методы проведения аттестации

Порядок аттестации защищаемого помещения

Общий порядок аттестации установлен двумя нормативно-методическими документами:

1. «Положение по аттестации объектов информатизации по требованиям безопасности информации» от 25.11.1994.
2. «ГОСТ РО 0043-003-2012 аттестация объектов информатизации. Общие положения» от 17.04.2012 (имеет гриф «ДСП», т.е. ограниченного распространения).

При аттестации защищаемого помещения (далее – ЗП) подвергаются оценке следующие обязательные технические каналы утечки информации:

- акустический (речевой);
- виброакустический (возникающий посредством преобразования речевого сигнала при его воздействии на строительные конструкции и инженерно-технические системы);
- Оптико-электронный (лазерный);
- прослушивания разговоров за счет скрытного подключения к различным видам связи;

Порядок проведения аттестации:

- обследование помещения,
- инструментальная оценка помещения без СЗИ,
- расчет закупаемых средств защиты информации,
- закупка СЗИ,
- установка и настройка СЗИ,
- повторная инструментальная оценка с наличием СЗИ в ЗП,
- оформление соответствующих документов.

По итогам аттестации оформляются следующий список документов:

- ПиМ – программа и методики аттестационных испытаний;

- протокол аттестационных испытаний;
- заключение по результатам аттестационных испытаний (общее для всех технических каналов утечки информации);
- аттестат соответствия ведётся по положительному заключению проведённых работ.

Стоимость аттестации защищаемого помещения составляет около 150 000,00 руб. вместе с поставкой, установкой и настройкой средств защиты информации. Цена в случае если помещение типовое.

В расчет цены также входят следующие работы:

- обследование помещения и разработка технического паспорта на помещение;
- инструментальная оценка (измерения контрольно-измерительным оборудованием);
- закупка, установка и настройка средств защиты;
- повторная инструментальная оценка;
- оформление отчетных документов.

Типовое помещение – это то помещение, которое включает в себя следующие пункты:

- 1 окно, 1 дверь, 1 батарея отопления, 1 вытяжка.
- Стены и перекрытия капитальные: бетонные или кирпичные.
- Отсутствие других компаний в том же здании, что и ЗП, то есть. потенциальных шпионов. Если есть соседи, то площадь помещения должна как можно меньше граничить с площадью потенциального врага.
- Входная дверь должна быть металлическая с уплотнительной резинкой. Если дверь деревянная, то ее толщина должна быть не менее 40 мм, а щели — как можно меньше.

Если рассматриваемое помещение не является типовым то стоимость будет рассчитана по другому, в большую сторону.

3.2. Цели и задачи проведения аттестации

Требования по защите конфиденциальной информации, обрабатываемой в защищаемых помещениях, установлены следующими нормативно-методическими документами ФСТЭК России:

1. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП.

2. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП.

3. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП.

4. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 N 282. ДСП.

Указанные документы имеют гриф «ДСП», то есть для служебного пользования и соответственно просто так к ним не получить доступ. Данные документы могут получить только соискатели лицензий или лицензиаты ФСТЭК России путем запроса указанных документов установленным порядком в самом ФСТЭК России.

3.3. Проведение аттестационных испытаний

Условия проведения измерений. Измерения следует проводить при минимальных уровнях акустической и вибрационной шумов в ЗП, персонал в это время не должен находится в помещении.

Измерение проводится следующим образом:

В самом помещении устанавливается тестовая акустическая система на высоте 1,5 м от пола и 1 м от контрольной точки с другой стороны контрольной точки устанавливается измеритель шума, либо же измеритель вибрации, на расстоянии 0.5 м, в зависимости от вида технического канала утечки информации.

Список аппаратуры, используемой при проведении измерений указан в таблице № 9.

Таблица № 9 – Перечень средств измерений и вспомогательного оборудования

№ п/п	Наименование средств измерений и вспомогательного оборудования	Тип	Диапазон частот, МГц
Средства измерений			
1.	Измеритель шума и вибрации в комплекте	ВШВ-003-М3	0,000002÷0,018
Вспомогательное оборудование и ПО			
1.	Вспомогательный генератор сигналов	Источник «ЗАВАНТ»	0,001÷10000
2.	Вспомогательный генератор сигналов	HP 8648C	0.1÷3200
3.	Вспомогательный генератор сигналов	SMA100B	0,008÷6000
4.	Тестовая акустическая система	АС-1 Лайт	0,00004÷0,016

Далее в таблице № 10 будут рассмотрены измеряемые контрольные точки (далее – «КТ»).

Таблица № 10 – описание контрольных точек

№ КТ	Описание КТ	Канал утечки информации
1	Батарея № 1, акселерометр установлен на приточной трубе радиатора батареи.	Виброакустический
2	Батарея № 2, акселерометр установлен на приточной трубе радиатора батареи.	Виброакустический
3	Батарея № 3, акселерометр установлен на приточной трубе радиатора батареи.	Виброакустический
4	Окно № 1, со стороны улицы левого окна	Акустический оптико-электронный
5	Окно № 2, со стороны улицы правого окна	Акустический оптико-электронный
6	У двери со стороны коридора	Акустический
7	Стена, у двери (рядом с пожарной кнопкой)	Виброакустический
8	Соседнее помещение, стена	Виброакустический
9	Стена, со стороны улицы	Оптико-электронный Акустический

№ КТ	Описание КТ	Канал утечки информации
10	Соседнее помещение, пол	Виброакустический
11	Стена, со стороны коридора	Виброакустический
12	Стена, со стороны р. Большая Невки	Виброакустический Оптико-электронный
13	Перекрытие, пол	Виброакустический
14	Перекрытие, потолок	Виброакустический

Контрольные точки обозначены на рисунке 15

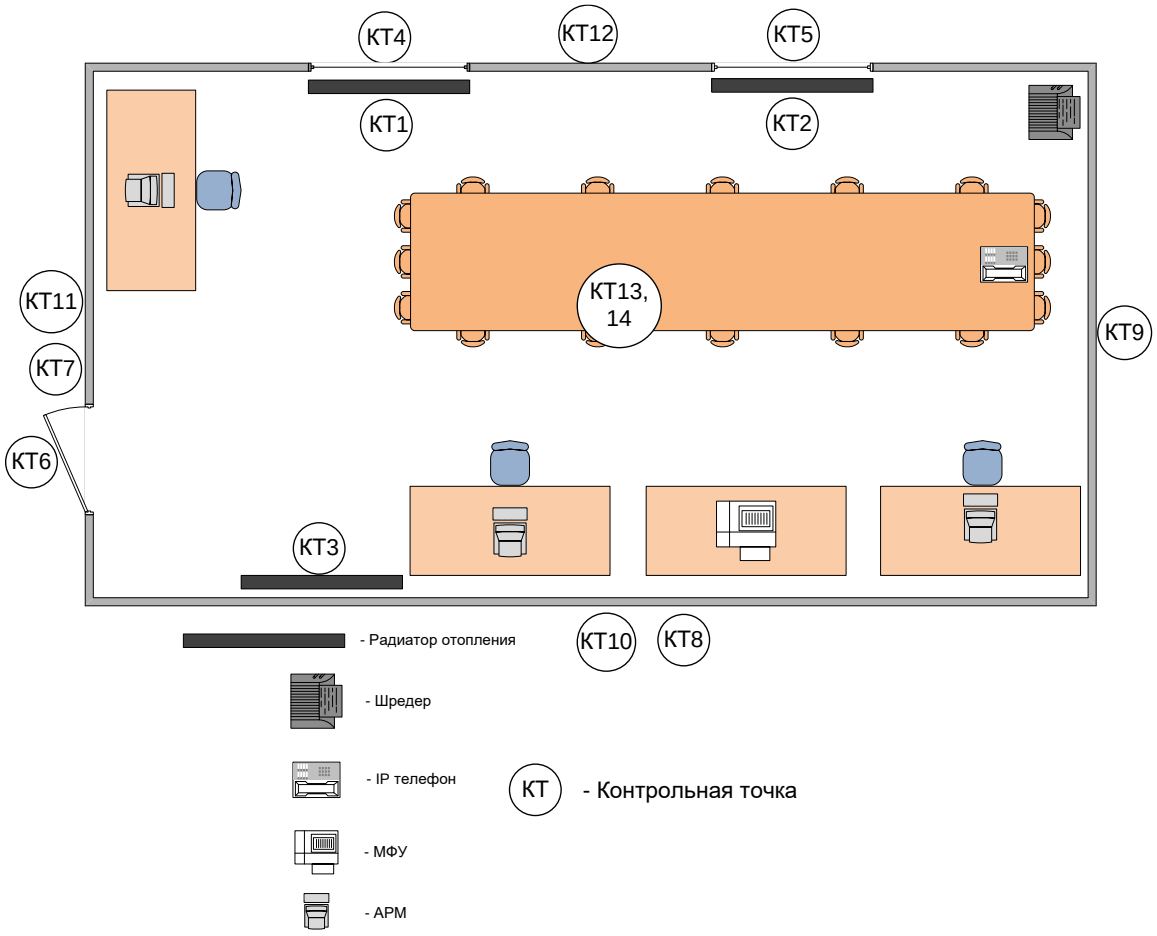


Рисунок 15 – Схема размещения контрольных точек в помещении № 215б.

Измерения проводились в соответствии с документом «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России 8 ноября 2001 г.

Далее приведена таблица № 11 измерений по контрольным точкам по акусто-речевой разведке

Таблица № 11 – Измерения акусто-речевой разведки.

Номер октавной полосы i	**Уровень излучения тестовой акустической системы**	**Сумма САЗ+шум в КТ**	**Уровень шума САЗ в КТ**
КТ 1			
1	87	50	60
2	88	55	60
3	91	50	61
4	92	50	68
5	95	47	64
КТ 2			
1	90	55	64
2	90	58	68
3	93	71	76
4	94	72	78
5	97	66	78
КТ 3			
1	90	53	62
2	90	55	65
3	93	68	76
4	94	70	78
5	97	64	76
КТ 4			
1	90	56	64
2	90	57	68
3	93	70	79
4	94	72	81
5	97	67	80
КТ 5			
1	90	59	76
2	90	66	83
3	93	69	86
4	94	73	80
5	97	69	77
КТ 6			
1	90	67	78
2	90	68	84
3	93	71	89
4	94	74	82
5	97	71	79
КТ 7			
1	90	20	31
2	90	20	28
3	93	21	28
4	94	18	26
5	97	17	21
КТ 8			
1	90	18	29
2	90	18	27
3	93	20	27

Номер октавной полосы i	**Уровень излучения тестовой акустической системы**	**Сумма САЗ+шум в КТ**	**Уровень шума САЗ в КТ**
4	94	20	25
5	97	19	20
КТ 9			
1	90	19	30
2	90	19	29
3	93	19	25
4	94	18	28
5	97	18	22
КТ 10			
1	90	19	30
2	90	18	30
3	93	19	28
4	94	20	28
5	97	20	24
КТ 11			
1	90	20	31
2	90	19	31
3	93	20	29
4	94	21	29
5	97	21	25
КТ 12			
1	90	17	32
2	90	17	32
3	93	18	30
4	94	19	30
5	97	18	26
КТ 13			
1	90	17	28
2	90	17	27
3	93	20	27
4	94	20	28
5	97	19	25
КТ14			
1	90	19	29
2	90	18	28
3	93	19	28
4	94	18	29
5	97	20	26

Особенностью акустической разведки является то, что анализ перехваченной с помощью технических средств разведки информации производит человек. Поэтому в качестве нормативного показателя оценки эффективности защиты ЗП от утечки речевой информации по техническим каналам используется словесная разборчивость речи **W**, под которой

понимается относительное количество (в процентах) правильно понятых человеком слов, перехваченных (зарегистрированных) средством разведки.

Практический опыт показывает, что невозможно составить подробную информацию о прослушанных разговорах с разборчивостью речи ниже 70-80%, а также невозможно составить краткую сводку прослушанных разговоров с разборчивостью речи ниже 70%. Более 40-60%. При разборчивости речи ниже 20-40% определить тему даже продолжающегося разговора сложно, а при разборчивости речи ниже 10-20% практически невозможно. Поскольку разборчивость речи ниже 10%, в перехваченных сообщениях трудно определить речевые символы.

Критерии эффективности защиты речевой информации приведены в таблице № 12

Таблица № 12 – Критерии эффективности защиты речевой информации

Цель защиты	Потенциальные технические каналы утечки информации	Критерий эффективности защиты W(%)
Скрыть ведение переговоров в ЗП	Прямой акустический, акустовибрационный, оптикоэлектронный	W ≤10
Скрыть предмет переговоров в ЗП	Прямой акустический, акустовибрационный, оптикоэлектронный	W ≤20
Скрыть содержание переговоров в ЗП	Прямой акустический, акустовибрационный, оптикоэлектронный	W ≤30
Скрыть содержание переговоров в ЗП	Прямой акустический без применения технических средств (непреднамеренное прослушивание)	W ≤50

Меры по защите речевой информации считаются эффективны, если рассчитанное по результатам измерения значение словесной разборчивости речи не превышает установленного нормированного значения: W ≤ Wn.

EΔi=V_{ci}-V_i-L_i(1)

Δi – отношение сигнал/шум в i-й октаве, вычисленное на основе измерений, дБ.

L_i- поправочный коэффициент (превышение тестового сигнала от нормали), (уровень звукового давления тестового сигнала минус нормированный октавный уровень);

$V_{\text{ш}i}$- шум САЗ или шум в помещении (измеренный);

$V_{\text{с}i}$-расчетные значения (октавный уровень сигнала);

$V_{(\text{с+ш})i}$-$V_{\text{ш}i}$= значение, смотря чему равна эта разность, $V_{\text{с}i}$ считается по разному;

$$Lc_i=\begin{cases}L_{(\text{с+ш})i} & \text{при} L_{(\text{с+ш})i}-L_{\text{ш}i}\geq 10\\ L_{(\text{с+ш})\,i}-\Delta & \text{при} L_{(\text{с+ш})i}-L_{\text{ш}i}<10\end{cases} \quad (2)$$

$$Vc_i=\begin{cases}V_{(\text{с+ш})i} & \text{при} V_{(\text{с+ш})i}-V_{\text{ш}i}\geq 10\\ V_{(\text{с+ш})\,i}-\Delta & \text{при} V_{(\text{с+ш})i}-V_{\text{ш}i}<10\end{cases} \quad (3)$$

Где Δ – поправка в дБ, определяемая из таблицы № 13

Таблица № 13

$V_{(\text{с+ш})i}-L_i$	10	6…10	4…6	3	2	1	0,5
Δ,дБ	0	1	2	3	4	7	10

exp(2) = e^2 = 2,7182818284

Словесная разборчивость речи W рассчитывается следующим образом:

$$W=\begin{cases}1{,}54R^{0{,}25}[1-\exp(-11R)], \text{ если } R<0{,}15;\\ 1-\exp\left[-\dfrac{11R}{1+0{,}7R}\right], \text{ если } R\geq 0{,}15,\end{cases} \quad (4)$$

где R – интегральный индекс артикуляции речи,

R =$\sum_{i=1}^{5}(r_i * k_i)$,(5)

$$r_i=\begin{cases}\dfrac{0{,}78+5{,}46\cdot\exp[-4{,}3\cdot 1{,}0^{-2}\cdot(27{,}3-|Q_i|)^2]}{1+10^{0{,}1\cdot|Q_i|}}, \text{ если } Q_i\leq 0;\\ 1-\dfrac{0{,}78+5{,}46\cdot\exp[-4{,}3\cdot 1{,}0^{-2}\cdot(27{,}3-|Q_i|)^2]}{1+10^{0{,}1\cdot|Q_i|}}, \text{ если } Q_i>0.\end{cases}$$

$$r_i=\{\frac{0{,}78+5{,}46*2{,}7182818284[-4{,}3*1{,}0^{-2}*(27{,}3-|Q|)^2}{1+10^{0{,}1*|-11-18|}}\} \quad (6)$$

ki – значение весового коэффициента в i-й октавной полосе;

Qi = Δi [дБ] – Ai;

Ai – значение формантного параметра спектра речевого сигнала в i-й октавной полосе, дБ;

Δi – отношение сигнал/шум в i-й октаве, вычисленное на основе измерений, дБ.

Числовые значения формантного параметра спектра речевого сигнала Ai и весового коэффициента Ki в октавных полосах представлены в таблице № 14

Таблица № 14 – Числовые значения формантного параметра спектра речевого сигнала Ai и весового коэффициента Ki в октавных полосах

Наименование параметров	Среднегеометрические частоты октавных полос Fcpi, Гц				
	250	500	1000	2000	4000
Ai, дБ	18	14	9	6	5
ki	0,03	0,12	0,20	0,30	0,26

Далее приведена таблица № 15 расчётов контрольных точек

Таблица № 15 – Расчет контрольных точек

Среднегеометрические частоты октавных полос	Октавный уровень контрольно-го сигнала	Октавный уровень вибр. шума в КТ	Октавный уровень смеси "в.сигнал + шум" в КТ	Октавный уровень вибр. сигнала в КТ	Октавный индекс виброизо-ляции	Значение показателя противо-действия АРР
fcp, Гц	*Lкi, дБ*	*Vшi, дБ*	*V(с+ш)i,дБ*	*Vсi, дБ*	*Q, дБ*	W
КТ1 - дверь						
250	87	50	60	60	27,5	0,06
500	88	55	60	58	29,7	
1000	91	50	61	61	30,4	
2000	92	50	68	68	24,1	
4000	95	47	64	64	31,1	
КТ2 - Батарея №1						
250	90	55	64	63	26,6	**0,01**
500	90	58	68	68	22,5	
1000	93	71	76	74	18,7	
2000	94	72	78	77	17,3	

Среднегеометрические частоты октавных полос	Октавный уровень контрольного сигнала	Октавный уровень вибр. шума в КТ	Октавный уровень смеси "в.сигнал + шум" в КТ	Октавный уровень вибр. сигнала в КТ	Октавный индекс виброизоляции	Значение показателя противодействия АРР
fср, Гц	*Lкi, дБ*	*Vшi, дБ*	*V(с+ш)i,дБ*	*Vсi, дБ*	*Q, дБ*	W
4000	97	66	78	78	19,3	
КТ3 - Батарея №2						
250	90	53	62	61	26,6	**0,02**
500	90	55	65	65	23,5	
1000	93	68	76	75	14,7	
2000	94	70	78	77	14,7	
4000	97	64	76	76	18,3	
КТ4 - Батарея №3						
250	90	56	64	63	28,7	**0,01**
500	90	57	68	68	23,4	
1000	93	70	79	78	13,6	
2000	94	72	81	80	13,6	
4000	97	67	80	80	18,2	
КТ5 - Окно №1						
250	90	58	78	76	12,1	**0,08**
500	90	63	83	83	5,1	
1000	93	69	86	86	5,1	
2000	94	73	82	79	13,0	
4000	97	69	80	76	18,7	
КТ6 - Окно №2						
250	90	67	78	78	12,4	**0,05**
500	90	68	84	84	6,1	
1000	93	71	89	89	4,1	
2000	94	74	82	81	12,7	
4000	97	71	79	78	18,7	
КТ7 - стена № 1						
250	90	20	31	31	54,4	**0,01**
500	90	20	28	27	58,7	
1000	93	21	29	27	63,0	
2000	94	18	27	25	65,7	
4000	97	17	25	19	73,2	
КТ8 - стена № 2						
250	90	18	31	29	55,4	**0,01**
500	90	17	29	26	57,6	
1000	93	18	27	26	71,0	

Среднегеометрические частоты октавных полос	Октавный уровень контрольного сигнала	Октавный уровень вибр. шума в КТ	Октавный уровень смеси "в.сигнал + шум" в КТ	Октавный уровень вибр. сигнала в КТ	Октавный индекс виброизоляции	Значение показателя противодействия АРР
fср, Гц	*Lкi, дБ*	*Vшi, дБ*	*V(с+ш)i,дБ*	*Vсi, дБ*	*Q, дБ*	W
2000	94	17	26	23	64,7	
4000	97	17	27	13	75,9	
КТ9 - стена № 3						
250	90	19	30	30	56,4	
500	90	19	29	29	58,5	
1000	93	19	25	24	71,3	**0,01**
2000	94	18	28	28	61,5	
4000	97	18	22	20	70,2	
КТ10 – пол у стены						
250	90	19	30	30	60,4	
500	90	18	30	30	60,3	
1000	93	19	28	27	65,6	**0,01**
2000	94	20	28	27	66,7	
4000	97	20	24	22	75,2	
КТ11 – пол у стены						
250	90	20	31	31	59,4	
500	90	19	31	31	59,3	
1000	93	20	29	28	64,6	**0,01**
2000	94	21	29	28	65,7	
4000	97	21	25	23	74,2	
КТ12 – пол у стены						
250	90	17	32	32	58,1	
500	90	17	32	32	58,1	
1000	93	18	30	30	63,3	**0,03**
2000	94	19	30	30	64,4	
4000	97	18	26	25	71,7	
КТ13 – Перекрытие, пол						
250	90	17	28	28	62,4	
500	90	17	27	27	63,5	
1000	93	20	27	26	67,0	**0,01**
2000	94	20	28	27	66,7	
4000	97	19	25	24	73,3	
КТ14 – Перекрытие, потолок						
250	90	19	29	29	61,5	
500	90	18	28	28	62,5	**0,01**
1000	93	19	28	27	65,6	

Среднегеометрические частоты октавных полос	Октавный уровень контрольного сигнала	Октавный уровень вибр. шума в КТ	Октавный уровень смеси "в.сигнал + шум" в КТ	Октавный уровень вибр. сигнала в КТ	Октавный индекс виброизоляции	Значение показателя противодействия АРР
fср, Гц	*Lкi, дБ*	*Vшi, дБ*	*V(с+ш)i,дБ*	*Vсi, дБ*	*Q, дБ*	W
2000	94	18	29	29	65,4	
4000	97	20	26	25	72,3	

Перечень документов, разработанных после проведения аттестационных испытаний:

- Программы и методики;
- Протокол аттестационных испытаний;
- Заключение по результатам аттестационных испытаний;
- Аттестат соответствия.

Анализ состояния объекта до внедрения СЗИ и после.

Для расчета итоговой вероятности утечки информации после внедрения СЗИ был проведён анализ защищенности объекта в таблице №16

Таблица № 16 - Угрозы и их характеристики после внедрения СЗИ

Наименование угрозы	Опасность до установки СЗИ	Опасность после установки СЗИ
УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ		
Акустическое излучение информативного речевого сигнала	высокая	низкая
Виброакустические сигналы	высокая	низкая
Просмотр информации с экранов дисплеев и других средств ее отображения	средняя	маловероятная
Прослушивание телефонных и радиопереговоров	средняя	маловероятная
Снятие информации за счет оптико-электронного канал утечки	высокая	низкая

Ссылаясь на таблицу 2 - Угроз и их характеристик, где защищенность объекта информатизации до внедрения средств защиты информации, составляло 25%, то исходя из таблицы 16 - Угроз и их характеристик после внедрения СЗИ, уровень защищенности объекта информатизации составляет

75%, то есть благодаря внедрению СЗИ, защищенность объекта была увеличена на 50%.

Так же ссылаясь на рассмотренные средства защиты информации, которые закупались для объекта информатизации и рассмотренные цены аттестационных испытаний можно сделать расчеты по стоимости всех проведённых работ, которые приведены в таблице № 17

Таблица № 17 – Стоимость всех проведенных работ

Наименование	Стоимость руб.
Проведение аттестационных испытаний	225 000,00
Закупка, установка и настройка средств защиты информации «Соната-АВ-4Б»	98 160,00
Итог затраченных средств	323 160,00

3.4. Стоимость информационных активов

Активы – это информация, технические средства, программное обеспечение и различная документация.

Информационные активы – это результат деятельности компании за определённый период времени.

Стоимость информационных активов выявляется внутри каждой организации персонально. Проводится сбор руководителей компании и по ГОСТ Р ИСО 22301-2021 «Надежность в технике. Системы менеджмента непрерывности деятельности. Требования» от 01.01.2022, производится расчет стоимости информационных активов организации.

После проведения расчета информационных активов организации было получено следующее значение: 157 млрд руб.

Исходя из выше сказанного, был проведен анализ стоимости потерь активов до внедрения и после внедрения средств защиты информации, проанализированный в таблице 18, а также объяснена актуальность закупленных и установленных средств защиты информации на объекте

информатизации. После таблицы приведён рисунок 16 в виде диаграммы в котором также указана стоимость потери активов организации.

Таблица 18 - Анализ стоимости потерь активов

Наименование	Количество в %	Количество в руб.
Информационные активы	100	157 000 000 000
Возможная потеря активов без установленных СЗИ	75	117 750 000 000
Возможная потеря активов с установленными СЗИ	25	39 250 000 000
Стоимость установки СЗИ	-	323 160,00

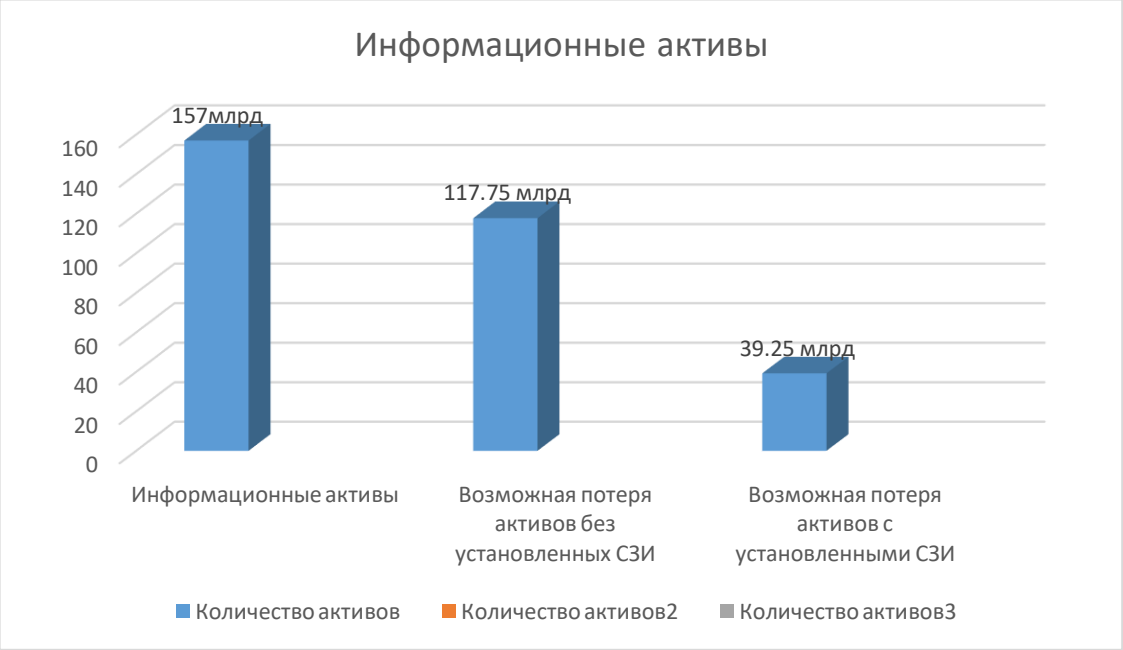


Рисунок 16 - Анализ стоимости потерь активов

3.5. Вывод по третьей главе: таким образом, в данной главе были рассмотрены методы проведения аттестации и соответственно проведены аттестационные испытания, в следствии которых были произведены расчеты по контрольным точкам технических каналов утечки информации, представленные в приложение А и выявлено процентное значение защиты информации на объект информатизации. А также проведён анализ потери информационных активов в зависимости от наличия или отсутствия средств защиты информации.

ЗАКЛЮЧЕНИЕ

В результате проведенных работ можно сделать следующие выводы:

1. Проведен анализ рассматриваемого объекта информатизации.
2. Рассмотрены модели угроз и модели нарушителя
3. Рассмотрены различные виды технических каналов утечки информации и выделены те каналы, которые рассматриваются на данном объекте информатизации.
4. Рассмотрены угрозы утечки информации по техническим каналам.
5. Рассмотрены различные виды средств защиты информации и выбраны подходящие к этому объекту информатизации, исходя из проведенного анализа организаций, занимающихся созданием средств защиты информации. Так же был проведен анализ различных средств защиты информации из разных организации, исходя из которого была выбрана и рассчитана стоимость комплекта СЗИ.
6. Были проведены аттестационные испытания в ходе которых был выпущен соответствующий методике комплект документов.
7. Были проведены расчеты по техническим каналам утечки информации в каждой контрольной точке. И получен коэффициент разборчивости речи.
8. После проведенного анализ угроз с установкой средств защиты информации, уровень защиты объекта информатизации был увеличен на 50%.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (Дата обращения 04.10.2022)

2. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ [Электронный ресурс]. Режим доступа:http://www.consultant.ru/document/cons_doc_LAW_48699/ (Дата обращения 06.10.2022)

3. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации" от 13.07.2015 N 244-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_182624/ (Дата обращения 07.10.2022)

4. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 [Электронный ресурс]. Режим доступа:https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (Дата обращения 20.11.2022)

5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год [Электронный ресурс]. Режим доступа:https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (Дата обращения 15.11.2022)

6. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 [Электронный ресурс]. Режим доступа:https://fstec.ru/normotvorcheskaya/akty/53-prikazy/2270-prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77 (Дата обращения 27.10.2022)

7. НПО «АННА» средства защиты информации. [Электронный ресурс]. Режим доступа: http://www.npoanna.ru/Content.aspx?name=models.sonata-ip41 (Дата обращения 17.10.2022)

8. ЦБИС РФ – Аттестационные испытания [Электронный ресурс]. Режим доступа:https://xn--90ao1ar.xn--p1ai/attestatsiya_fstek/attestatsiya-zashhishhaemyh-pomeshhenij/ (Дата обращения 17.10.2022)

ВЛОЖЕНИЕ А

Расчеты по контрольным точкам.

КТ1

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-11-18|^2}{1+10^{0,1*|-11-18|}}\} =0,0002$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-19-14|^2}{1+10^{0,1*|-19-14|}}\} =0,0004$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-19-9|^2}{1+10^{0,1*|-19-9|}}\} =0,0018$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-18-6|^2}{1+10^{0,1*|-18-6|}}\} =0,0070$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-25-5|^2}{1+10^{0,1*|-25-5|}}\} =0,0015$$

R =0,0002+0,0004+0,0018+0,0070+0,0015=0,0110

W =1,54*0,0110[1-2,7182818284(-11*0,0110)] =0,06

КТ2

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-16-18|^2}{1+10^{0,1*|-16-18|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-14-14|^2}{1+10^{0,1*|-14-14|}}\} =0,0011$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-29-9|^2}{1+10^{0,1*|-29-9|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-33-6|^2}{1+10^{0,1*|-33-6|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-32-5|^2}{1+10^{0,1*|-32-5|}}\} =0,0002$$

R =0,0001+0,0011+0,0001+0,0001+0,0002=0,0016

W =1,54*0,0016 [1-2,7182818284(-11*0,0016)] =0,01

КТ3

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-16-18|^2}{1+10^{0,1*|-16-18|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-14-14|^2}{1+10^{0,1*|-14-14|}}\} =0,0011$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-25-9|^2}{1+10^{0,1*|-25-9|}}\} =0,0005$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-31-6|^2}{1+10^{0,1*|-31-6|}}\} =0,0003$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-32-5|^2}{1+10^{0,1*|-32-5|}}\} =0,0002$$

R =0,0001+0,0011+0,0005+0,0003+0,0002=0,0021

W =1,54*0,0021 [1-2,7182818284(-11*0,0021)] =0,02

KT4

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-16-18|^2}{1+10^{0,1*|-16-18|}}\}$ =0,0001

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-14-14|^2}{1+10^{0,1*|-14-14|}}\}$ =0,0011

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-25-9|^2}{1+10^{0,1*|-25-9|}}\}$ =0,0005

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-31-6|^2}{1+10^{0,1*|-31-6|}}\}$ =0,0003

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-32-5|^2}{1+10^{0,1*|-32-5|}}\}$ =0,0002

R =0,0001+0,0011+0,0005+0,0003+0,0002=0,0027

W =1,54*0,0027 [1-2,7182818284(-11*0,0027)] =0,01

KT5

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-4-18|^2}{1+10^{0,1*|-4-18|}}\}$ =0,0010

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-4-14|^2}{1+10^{0,1*|-4-14|}}\}$ =0,0084

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-15-9|^2}{1+10^{0,1*|-15-9|}}\}$ =0,0047

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-30-6|^2}{1+10^{0,1*|-30-6|}}\}$ =0,0004

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-33-5|^2}{1+10^{0,1*|-33-5|}}\}$ =0,0002

R =0,0010+0,0084+0,0047+0,0004+0,0002=0,0147

W =1,54*0,0147 [1-2,7182818284(-11*0,0147)] =0,08

KT6

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-4-18|^2}{1+10^{0,1*|-4-18|}}\}$ =0,0001

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-4-14|^2}{1+10^{0,1*|-4-14|}}\}$ =0,0041

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-15-9|^2}{1+10^{0,1*|-15-9|}}\}$ =0,0057

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-30-6|^2}{1+10^{0,1*|-30-6|}}\}$ =0,0003

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-33-5|^2}{1+10^{0,1*|-33-5|}}\}$ =0,0001

R =0,0001+0,0041+0,0057+0,0003+0,0001=0,0103

W =1,54*0,0103 [1-2,7182818284(-11*0,0103)] =0,05

КТ7

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-13-18|^2}{1+10^{0,1*|-13-18|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-17-14|^2}{1+10^{0,1*|-17-14|}}\} =0,0006$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-25-9|^2}{1+10^{0,1*|-25-9|}}\} =0,0005$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-30-6|^2}{1+10^{0,1*|-30-6|}}\} =0,0004$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-37-5|^2}{1+10^{0,1*|-37-5|}}\} =0,0001$$

R =0,0001+0,0006+0,0005+0,0004+0,0001=0,0016

W =1,54*0,0016 [1-2,7182818284(-11*0,0016)] =0,01

КТ8

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-11-18|^2}{1+10^{0,1*|-11-18|}}\} =0,0002$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-12-14|^2}{1+10^{0,1*|-12-14|}}\} =0,0018$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-24-9|^2}{1+10^{0,1*|-24-9|}}\} =0,0006$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-30-6|^2}{1+10^{0,1*|-30-6|}}\} =0,0004$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-34-5|^2}{1+10^{0,1*|-34-5|}}\} =0,0001$$

R =0,0002+0,0018+0,0006+0,0004+0,0001=0,0031

W =1,54*0,0031 [1-2,7182818284(-11*0,0031)] =0,01

КТ9

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-13-18|^2}{1+10^{0,1*|-13-18|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-14-14|^2}{1+10^{0,1*|-14-14|}}\} =0,0011$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-27-9|^2}{1+10^{0,1*|-27-9|}}\} =0,0002$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-28-6|^2}{1+10^{0,1*|-28-6|}}\} =0,0006$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-36-5|^2}{1+10^{0,1*|-36-5|}}\} =0,0001$$

R =0,0001+0,0011+0,0002+0,0006+0,0001=0,0020

W =1,54*0,0020 [1-2,7182818284(-11*0,0020)] =0,01

KT10

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-13-18|^2}{1+10^{0,1*|-13-18|}}\}$ =0,0001

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-12-14|^2}{1+10^{0,1*|-12-14|}}\}$ =0,0018

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-24-9|^2}{1+10^{0,1*|-24-9|}}\}$ =0,0006

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-31-6|^2}{1+10^{0,1*|-31-6|}}\}$ =0,0003

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-38-5|^2}{1+10^{0,1*|-38-5|}}\}$ =0,0001

R =0,0001+0,0011+0,0002+0,0006+0,0001=0,0028

W =1,54*0,0028 [1-2,7182818284(-11*0,0028)] =0,01

KT11

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-13-18|^2}{1+10^{0,1*|-13-18|}}\}$ =0,0001

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-12-14|^2}{1+10^{0,1*|-12-14|}}\}$ =0,0018

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-24-9|^2}{1+10^{0,1*|-24-9|}}\}$ =0,0006

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-31-6|^2}{1+10^{0,1*|-31-6|}}\}$ =0,0003

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-38-5|^2}{1+10^{0,1*|-38-5|}}\}$ =0,0001

R =0,0001+0,0011+0,0002+0,0006+0,0001=0,0028

W =1,54*0,0028 [1-2,7182818284(-11*0,0028)] =0,01

KT12

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-13-18|^2}{1+10^{0,1*|-13-18|}}\}$ =0,0004

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-12-14|^2}{1+10^{0,1*|-12-14|}}\}$ =0,0034

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-24-9|^2}{1+10^{0,1*|-24-9|}}\}$ =0,0014

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-31-6|^2}{1+10^{0,1*|-31-6|}}\}$ =0,0008

$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-38-5|^2}{1+10^{0,1*|-38-5|}}\}$ =0,0001

R =0,0004+0,0034+0,0014+0,0008+0,0001=0,0060

W =1,54*0,0060 [1-2,7182818284(-11*0,0060)] =0,03

КТ13

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-13-18|^2}{1+10^{0,1*|-13-18|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-14-14|^2}{1+10^{0,1*|-14-14|}}\} =0,0011$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-26-9|^2}{1+10^{0,1*|-26-9|}}\} =0,0003$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-31-6|^2}{1+10^{0,1*|-31-6|}}\} =0,0003$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-39-5|^2}{1+10^{0,1*|-39-5|}}\} =0,0001$$

R =0,0001+0,0011+0,0003+0,0003+0,0001=0,0018

W =1,54*0,0018 [1-2,7182818284(-11*0,0018)] =0,01

КТ14

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-14-18|^2}{1+10^{0,1*|-14-18|}}\} =0,0001$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-14-14|^2}{1+10^{0,1*|-14-14|}}\} =0,0011$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-24-9|^2}{1+10^{0,1*|-24-9|}}\} =0,0006$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-27-6|^2}{1+10^{0,1*|-27-6|}}\} =0,0008$$

$$r_i = \{\frac{0,78+5,46*2,7182818284[-4,3*1,0^{-2}*(27,3-|-39-5|^2}{1+10^{0,1*|-39-5|}}\} =0,0001$$

R =0,0001+0,0011+0,0003+0,0003+0,0001=0,0026

W =1,54*0,0018 [1-2,7182818284(-11*0,0018)] =0,01

ПРИОЖЕНИЕ Б

Разработанные документы после проведения аттестационных испытаний.

ГРИФ

Экз. №____

УТВЕРЖДАЮ

_____

_____

_____ФИО

«____»_____202_ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

защищаемого помещения
«№ 215б»

Составил: _____ _____

Ознакомлен: _____ _____

1. Общие сведения об объекте.

1.1. Наименование: защищаемое помещение «№ 215б».

1.2. Расположение: г. Санкт-Петербург, наб. р. Большой Невки, д. 24с1, помещение №215б).

1.3. В помещении обсуждается информации конфиденциального характера.

1.4. Сведения о вводе объекта в эксплуатацию:

_____

_____

2. Состав оборудования объекта.

2.1 Перечень основных и вспомогательных технических средств, и систем, установленных в защищаемом помещении «№ 215б» приведен в таблице 1:

Таблица 1 – Вспомогательные средства

№ п/п	Наименование средств измерений и вспомогательного оборудования	Тип	Диапазон частот, МГц
Средства измерений			
2.	Измеритель шума и вибрации в комплекте	ВШВ-003-М3	0,000002÷0,018
Вспомогательное оборудование и ПО			
5.	Вспомогательный генератор сигналов	Источник «ЗАВАНТ»	0,001÷10000
6.	Вспомогательный генератор сигналов	HP 8648C	0.1÷3200
7.	Вспомогательный генератор сигналов	SMA100B	0,008÷6000
8.	Тестовая акустическая система	АС-1 Лайт	0,00004÷0,016

2.2 Состав средств защиты используемых в ЗП «№ 215б» приведен в п. 3 настоящего Технического паспорта.

2.3 Меры защиты применяемые в ЗП «№ 215б» приведены в п. 4 настоящего Технического паспорта.

2.4 Размещение ВТСС в помещении № 215б приведено в п. 5 настоящего Технического паспорта.

2.5 Схема размещения ЗП «№ 215б» относительно границы контролируемой зоны приведена в п. 6 настоящего Технического паспорта.

2.6 Схема кабельных соединений в ЗП «№ 215б» приведена в п. 7 настоящего Технического паспорта.

3. Состав средств защиты используемых в ЗП.

3.1 Перечень средств защиты используемых в ЗП «№ 215б» приведен в таблице 2:

Таблица 2

№ п/п	Наименование и тип ТС	Заводской номер	Сведения о сертификате	Акт установки

	Соната-ИП4.1			
	Соната-ДУ4.3			
	СА-4Б			
	СВ-4Б			
	Соната-ВК4.1			
	Соната-ВК4.3			

4. **Меры защиты, применяемые в ЗП «**№ 215б**».**

- двери помещения должны быть закрыты;
- трубки телефонных аппаратов должны лежать на рычагах;
- установленная система акустического и виброакустического зашумления «Соната-ИП4.1-_» должна быть включена и приведена в активный режим;
- Требования из Протоколов СИ (АВАК и АЭП); - если есть.

Меры по обеспечению режима секретности выполняются в соответствии с Памяткой по обеспечению режима безопасности и эксплуатации оборудования в защищаемом помещении «№ 215б» .

5. **Схема размещения ЗП «**№ 215б**»**

6. **Схема размещения ЗП «**№ 215б**» относительно границы контролируемой зоны**

СХЕМА

Учитывая расположение ЗП «№ 215б» на 2 этаже административного здания минимальное расстояние от ВТСС ЗП до границы контролируемой зоны составляет __ м.

7. **Схема кабельных соединений в ЗП «**№ 215б**»**

1. Линии электропитания имеют выход за пределы контролируемой зоны.
2. Система телефонной связи имеет выход за пределы контролируемой зоны (на городскую АТС).
3. Линии осветительной сети имеют выход за пределы контролируемой зоны.
4. Линии пожарной сигнализации не имеют выход за пределы контролируемой зоны.

8. **. Учет проведения регламентных проверок**

№ п/п	**Наименование организации проводившей проверку**	**Дата проведения проверки**	**Номер протокола**	**Примечание**
1.				
2.				

3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				

9. Лист регистрации изменений.

Порядковый № и дата внесения изменений	**Наименование документа, фиксирующего изменения**	**№№ замененных (исправленных) листов формуляра**	**Подпись лица внесшего изменения**

ГРИФ

Экз. №____

УТВЕРЖДАЮ

_____

_____

_____ФИО

«____»_____200_ г.

АКТ

установки системы защиты информации в защищаемом помещении

«№215б»

1. В _____ 202_ года проведены работы по установке в защищаемом помещении «_____» системы акустического и виброакустического зашумления в составе:
   - «Соната-АВ-4Б» (зав. №_____);
   - вибропреобразователи СВ-4Б (5 шт.);
   - акустический излучатель СА-4Б (2 шт.),
2. Работы проведены специалистами _____ (лицензия ФСТЭК России №____ от _____г.).
3. Установленная система виброакустического зашумления «Соната-АВ-4Б» имеет сертификат ФСТЭК России №___ от __.__.____г.
4. Сотруднику _____ (название организации) _____ (ФИО) передан Паспорт системы виброакустического зашумления «Соната-АВ-4Б».
5. По окончании установки системы защиты информации проведены ее испытания специалистами _____ (лицензия ФСТЭК России №____ от _____г.).

Приложение. Сертификат ФСТЭК России №___ от __.__.____г.

Представитель Заказчика _____ (ФИО)

Представитель Исполнителя _____ (ФИО)

_____

ГРИФ

Экз. №____

УТВЕРЖДАЮ

_____

_____

_____ФИО

«____»_____202_ г.

Перечень лиц, имеющих право самостоятельного доступа в защищаемое помещение «№215б» и работающих в нем

№	Фамилия, имя, отчество	Должность
1		
2		
3		

_____ (должность) _____

(ФИО)

ГРИФ

Экз. №____

УТВЕРЖДАЮ

_____

_____

_____ФИО

«____»_____200_ г.

ПАМЯТКА

по обеспечению режима безопасности и эксплуатации оборудования в защищаемом помещении «№ 215 б»

1. Ответственность за режим безопасности в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет ответственный за режим безопасности в защищаемом помещении, назначенный соответствующим распоряжением.

2. Ответственность за наличие и сохранность имущества, установленного в ЗП и указанного в техническом паспорте на помещение, несет ответственный за режим безопасности.

3. Установка нового оборудования, мебели, и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с лицом, ответственным за режим безопасности и органом по аттестации.

4. Установка новых или замена старых технических средств и систем может осуществляться только при наличии заключения о специальной проверке, выданного организацией, имеющей лицензию ФСБ на проведение проверки. – если проводилось СП.

5. В нерабочее время помещение должно закрываться на ключ и сдаваться под охрану.

6. Уборка помещения и все регламентные работы должны проводиться под контролем должностного лица, имеющего право самостоятельного

доступа в защищаемое помещение «№ 215б», согласно Перечня… (№___ от __.__.____г.).

7. Категорически запрещается изменение настроек системы акустической и виброакустической защиты «Соната АВ-4Б».

8. Все работы по обслуживанию технических средств связи и распределенных коммуникаций проводятся только под контролем должностного лица, ответственного за режим безопасности.

9. В рабочее время в помещении обязательно должно присутствовать должностное лицо, имеющее право самостоятельного доступа в защищаемое помещение «№ 215б», согласно Перечня… (№___ от __.__.____г.). При отсутствии такового лица нахождение кого-либо в ЗП запрещается и помещение должно закрываться на ключ.

10. При проведении закрытых мероприятий:

- двери и окна помещения должны быть закрыты;
- трубки телефонных аппаратов должны лежать на рычагах;
- установленная система акустического и виброакустического зашумления «Соната АВ-4Б» должна быть включена и приведена в активный режим;
- Требования из Протоколов СИ (АВАК и АЭП) – если есть;

11. В случае выхода из строя системы акустического и виброакустического зашумления «Соната АВ-4Б» проводить закрытые мероприятия на конфиденциальные темы **запрещается.**

12. Все технические средства, установленные в помещении, должны иметь протокол испытаний по результатам их специальных исследований. Импортные технические средства, бытовые приборы и оборудование должны пройти специальную проверку на отсутствие в них специальных электронных устройств перехвата информации («закладок»). – если проводились СИ.

13. В помещение запрещается вносить все виды радиотелефонов, оконечные устройства сотовой, микросотовой, транковой и пейджинговой связи, а также средства звукозаписи. При установке в ЗП телефонных и

факсимильных аппаратов с автоответчиком, спикерфоном и имеющих выход в городскую АТС, следует отключать эти аппараты на время проведения конфиденциальных мероприятий.

14. Повседневный контроль за выполнением требований по защите помещения осуществляют должностные лица, имеющие право самостоятельного доступа в защищаемое помещение «№ 215б», согласно Перечня… (№___ от __.__.____г.). Периодический контроль эффективности мер защиты помещения осуществляется должностным лицом, ответственным за режим безопасности.

_____ (должность) _____ (ФИО)

Данные по уровню подготовки кадров, обеспечивающих защиту информации

№ п/п	Фамилия, имя отчество специалиста	Образование (учебное заведение, специальность)	Должность	Стаж работы в области защиты информации
1.				
2.				
3.				
4.				

должность подпись

ПРИКАЗ

__.__.202_ №____

О назначении ответственного за режим безопасности в защищаемом помещении **«**№ 215б**»**

В связи с аттестацией защищаемого помещения «№ 215б» по требованиям по безопасности для конфиденциальной информации

ПРИКАЗЫВАЮ:

1. Назначить ответственным за режим безопасности в защищаемом помещении «№ 215б» – (должность) _____ (ФИО)

В своей работе ответственному за режим безопансоти руководствоваться документами:

- Специальные требования и рекомендация по технической защите конфиденциальной информации (СТР-К);
- Памятка по обеспечению режима безопасности и эксплуатации оборудования в защищаемом помещении «№ 215б».

_____ (должность) _____

(ФИО)