

Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬ-
НОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
(УНИВЕРСИТЕТ ИТМО)
ФАКУЛЬТЕТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
(ФБИТ)

КУРСОВАЯ РАБОТА

По дисциплине:

«Инженерно-технические средства защиты информации»

На тему:

«Проектирование системы защиты от утечки информации по различным ка-
налам»

Выполнил:

студент группы N34511 И. К. Золотников



Проверил:

Преподаватель ФБИТ И. Ю. Попов

Санкт-Петербург

2023

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
(УНИВЕРСИТЕТ ИТМО)

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

| | |
|--------------------------------|---|
| Студент | Золотников И. К. (Фамилия И.О.) |
| Факультет | ФБИТ |
| Группа | N34511 |
| Направление (специальность) | 10.03.01 Информационная безопасность |
| Руководитель | Попов И. Ю. (Фамилия И.О., должность, ученое звание, степень) |
| Дисциплина | Инженерно-технические средства защиты информации |
| Наименование темы | Проектирование системы защиты от утечки информации по различным каналам |
| Задание | Анализ возможных каналов утечки, средств их предотвращения и создание плана расположения средств на основании плана помещения |

Краткие методические указания

Содержание пояснительной записки

Рекомендуемая литература

Руководитель

(Подпись, дата)

Студент

Золотников И. К. 15.12.2023 

(Подпись, дата)


ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
(УНИВЕРСИТЕТ ИТМО)

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

| | |
|--------------------------------|---|
| Студент | Золотников И. К. (Фамилия И.О.) |
| Факультет | ФБИТ |
| Группа | N34511 |
| Направление (специальность) | 10.03.01 Информационная безопасность |
| Руководитель | Попов И. Ю. (Фамилия И.О., должность, ученое звание, степень) |
| Дисциплина | Инженерно-технические средства защиты информации |
| Наименование темы | Проектирование системы защиты от утечки информации по различным каналам |

| № п/п | Наименование этапа | Дата завершения | | Оценка и подпись руководителя |
|----------|---------------------------------|-----------------|-------------|----------------------------------|
| | | Планируемая | Фактическая | |
| 1 | Создание плана КР | 08.11.2023 | 08.11.2023 | |
| 2 | Анализ литературы | 08.11.2023 | 08.11.2023 | |
| 3 | Составление основного текста КР | 20.11.2023 | 20.11.2023 | |
| 4 | Создание презентации | 8.12.2023 | 8.12.2023 | |
| 5 | Презентация КР перед аудиторией | 19.12.2023 | 19.12.2023 | |

Руководитель _____
(Подпись, дата)

Студент Золотников И. К. 15.12.2023  _____
(Подпись, дата)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВА-
ТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
(УНИВЕРСИТЕТ ИТМО)

АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

| | |
|--------------------------------|--|
| Студент | Золотников И. К. <hr/> (Фамилия И.О.) |
| Факультет | ФБИТ |
| Группа | N34511 |
| Направление (специальность) | 10.03.01 Информационная безопасность |
| Руководитель | Попов И. Ю. <hr/> (Фамилия И.О., должность, ученое звание, степень) |
| Дисциплина | Инженерно-технические средства защиты информации |
| Наименование темы | Проектирование системы защиты от утечки информации по различным каналам |

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и за- ☒ Предложены студен- ☐ Сформулированы при участии сту-
дачи работы том дента
☐ Определены руководителем
2. Характер ра- ☐ Расчет ☐ Конструирование
боты ☒ Моделирование ☐ Дру-
гое: _____

3. Содержание работы

Рассмотрены возможные каналы утечки информации и средства защиты.

Создан план размещения средств защиты в здании.


4. Выводы

Был создан план размещения средств защиты и подсчитаны примерные затраты.

Руководитель

(Подпись, дата)

Студент

Золотников И. К. 15.12.2023 

(Подпись, дата)

СОДЕРЖАНИЕ

| | |
|---|----|
| Введение | 6 |
| 1 Общие положения..... | 8 |
| 1.1 Общие сведения о защищаемой организации | 8 |
| 1.2 Общие сведения о технических каналах утечки информации .. | 11 |
| 1.3 Перечень руководящих документов | 12 |
| 2 Анализ помещений объекта..... | 26 |
| 2.1 Обоснование необходимости защиты информации | 26 |
| 2.2 Описание помещения | 26 |
| 2.3 Анализ технических каналов утечки информации и выбор средств защиты | 27 |
| 3 Анализ технических средств защиты | 29 |
| 3.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации..... | 30 |
| 3.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации.. | 33 |
| 3.3 Защита от побочного электромагнитного излучения и наводок | 34 |
| 3.4 Защита от утечек по оптическому каналу | 35 |
| 4 Описание расстановки технических средств защиты | 36 |
| Заключение..... | 39 |
| Список использованных источников..... | 40 |

ВВЕДЕНИЕ

Отрасль атомной энергетики является одной из самых важных для любого государства. Благодаря использованию атомной энергии у государств есть возможность поддерживать и развивать свой промышленный потенциал и поддерживать достаточно высокий уровень жизни людей за счет поставок электроэнергии. Поэтому для любого государства одной из важнейших задач является обеспечение безопасности своего атомного комплекса.

Для обеспечения безопасности необходимо противостоять различным угрозам информационной безопасности. В частности, одной из наиболее актуальных проблем всегда была возможность преднамеренной и непреднамеренной утечки информации. Для ее избежания необходимо обеспечить надлежащую защиту для всех каналов передачи информации. Для обеспечения безопасности могут быть использованы различные технические средства, которые позволят предотвратить распространение информации дальше контролируемых зон и перекрыть возможные каналы утечки информации.

В данной работе будет рассмотрен процесс разработки комплекса инженерно-технической защиты информации для офиса администрации, то есть людей, занимающихся управлением работой атомной электростанции. В офисе находятся рабочие кабинеты, переговорная, помещение архива, уборная, общее место для отдыха. Так как это администрация атомной электростанции, необходимо обеспечить защиту информации, составляющей государственную тайну уровня «секретно».

ЦЕЛИ И ЗАДАЧИ

Целью данной курсовой работы является разработка комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем секретности «секретно».

Для осуществления цели работы необходимо решить ряд задач:

- Предоставить общие сведения об организации и ее информационных потоках;
- Рассмотреть общие сведения о технических канал утечки информации и обосновать важность защиты информации в организации;
- Предоставить план помещения организации и проанализировать возможность утечек информации;
- Провести анализ рынка активных и пассивных технических средств защиты информации и выбрать наиболее подходящие;
- Составить план расположения выбранных средств.

1 Общие положения

1.1 Общие сведения о защищаемой организации

Наименование организации: «СПбАЭС».

Область деятельности: Электроэнергетика и производство ядерной энергии.

Прибыль (месячная/годовая): 0.5 млрд руб/мес, 6 млрд руб/год.

Расходы:

- Топливо - 5 млрд руб/год.
- Утилизация отходов - 1 млрд руб/год.
- Обслуживание и ремонт - 5 млрд руб/год.
- Безопасность - 0.5 млрд руб/год.
- Вывод из эксплуатации - до 100 млрд руб.
- Оплата труда - 0.5 млрд руб/год.
- Страхование, лицензирование - 50 млн руб/год.
- Прочие административные расходы - 10 млн руб/год.

Стоимость информационных активов:

- Информационные системы - 80 млн руб.
- ПО - 90 млн руб.
- Базы данных - 300 млн руб.
- Коммуникационные системы - 50 млн руб.
- Информационная безопасность - 80 млн руб.

Персонал организации:

- административно-управленческий и общецеховой персонал (начальник цеха или отдела, его заместители, экономист, кладовщик, технологи);
- оперативный персонал (имеется в составе подразделений, непосредственно связанных с реализацией и обеспечением непрерывного круглосуточного технологического процесса на АЭС);
- ремонтный персонал;

- службы, производственные участки и бригады;
- лаборатории, состоящие иногда из нескольких групп.

Численность персонала АЭС, как правило, связана с ее установленной мощностью и колеблется от одного до двух человек на МВт.

Установленная мощность СПбАЭС - 4000 МВт. Численность персонала - 5000 человек.

На рисунках ниже представлена схема информационных потоков предприятия (рисунок 1) и план защищаемого объекта – административного офиса (рисунок 3).

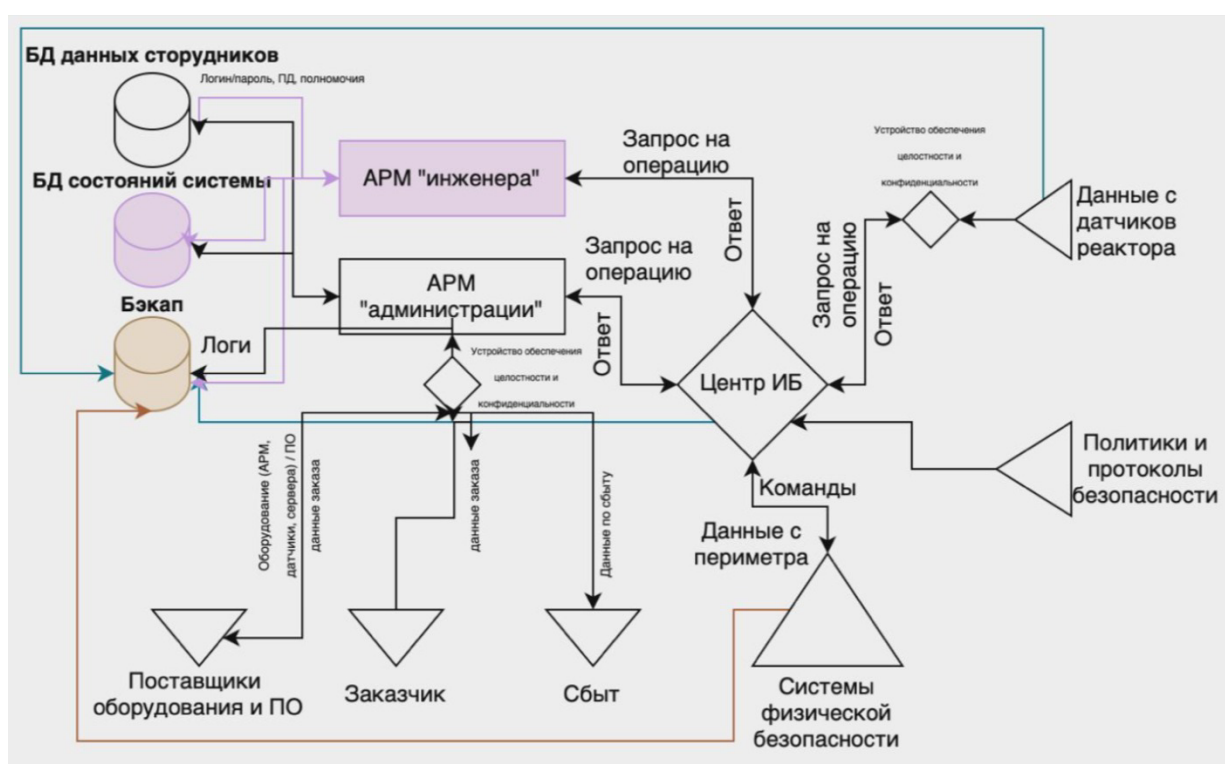


Рисунок 1 – Схема информационных потоков

Так как информация в системе относится к категории государственной тайны уровня «секретно», необходимо обезопасить все информационные потоки, то есть нужно обеспечить полную защиту и внутренних, и внешних информационных потоков.

На рисунке 2 представлена организационная структура предприятия.

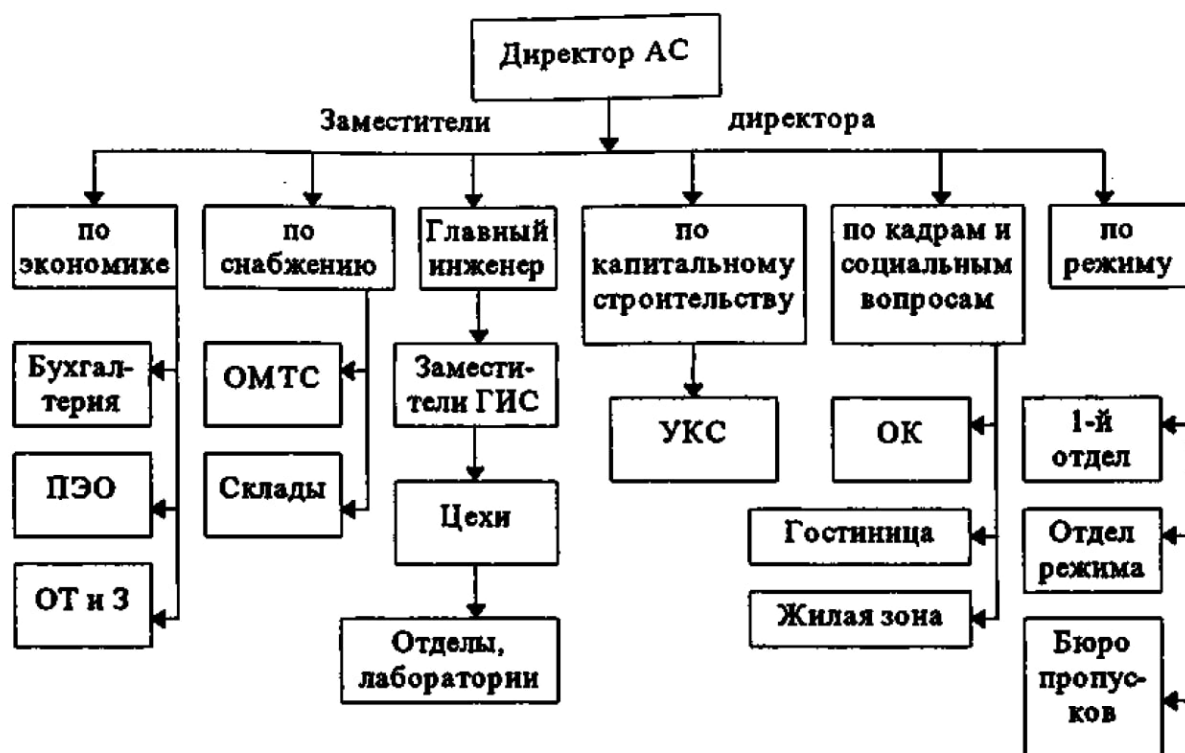


Рисунок 2 – Организационная структура

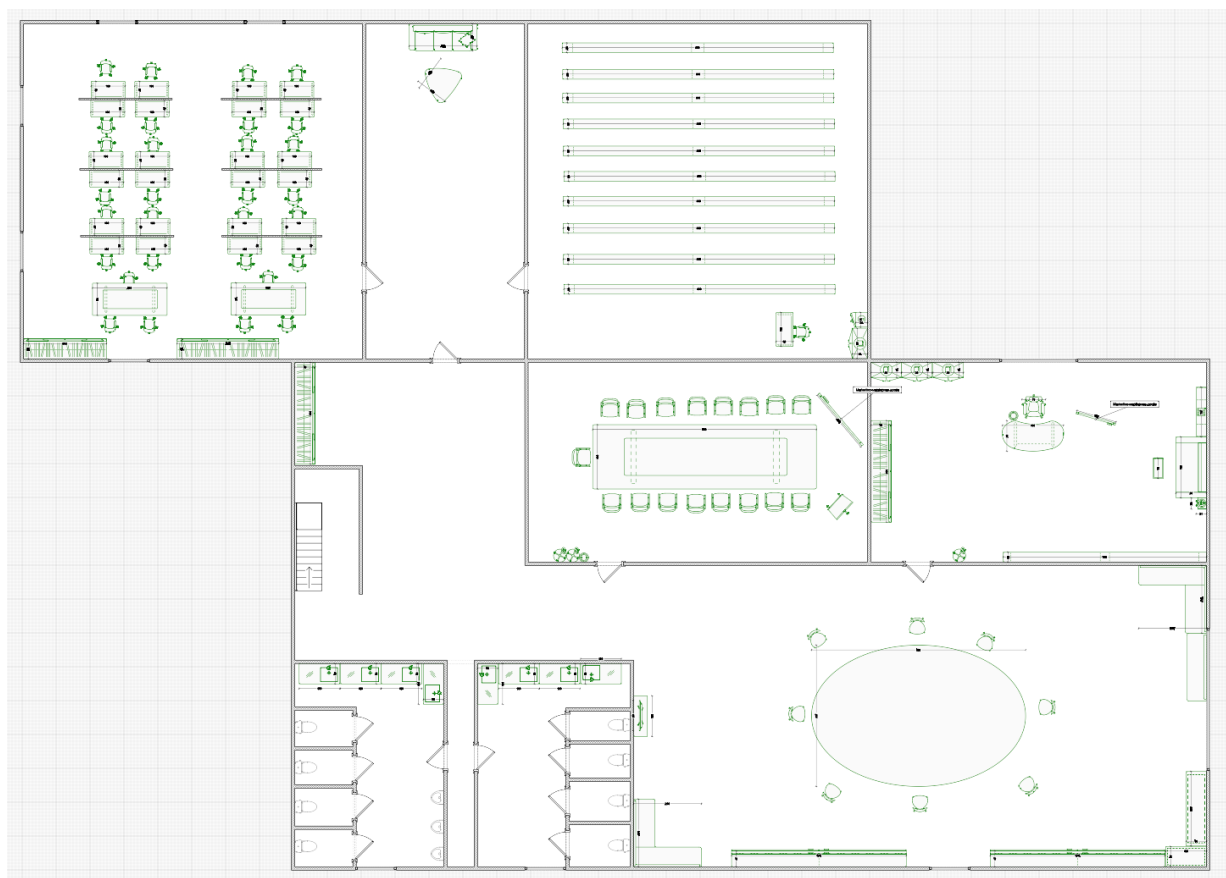


Рисунок 3 – План административного офиса

1.2 Общие сведения о технических каналах утечки информации

Утечка информации — это бесконтрольный выход информации за пределы организации или предприятия, которым она была доверена по службе или стала известна в процессе работы.

Утечка информации может быть следствием добровольного или принудительного разглашения информации, ухода информации по различным каналам или же несанкционированного доступа к информации. В данной работе будет рассмотрена утечка информации по техническим каналам.

Технический канал утечки информации (ТКУИ) — совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается информация.

Утечка по техническому каналу — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

На вход ТКУИ поступает информация в виде первичного сигнала, источниками которого могут быть:

- отраженные электромагнитные и акустические волны;
- собственные электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.

Информация от источника поступает на вход канала на языке источника, проходит через среду распространения и записывается на носитель информации после преобразования передатчиком. Среда распространения сигнала в таком случае — это физическая среда, внутри которой сигнал может распространяться и регистрироваться.

Основными параметрами среды являются:

- наличие физических препятствий;

- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

На рисунке 4 представлена общая классификация технических каналов утечки информации.



Рисунок 4 – Классификация ТКУИ

1.3 Перечень руководящих документов

В данном списке находятся основные документы, регулирующие деятельность в области предотвращения утечки информации по техническим каналам:

- «Вопросы Государственной технической комиссии при Президенте Российской Федерации» от 19 февраля 1999 г. №212.
- «Вопросы защиты государственной тайны» от 30.03.1994 г. №614.
- «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. №1203.
- «О межведомственной комиссии по защите государственной тайны» от 8 ноября 1995 г. №1108.
- «Вопросы Межведомственной комиссии по защите государственной тайны» от 20 января 1996 г. №71 с изменениями, внесенными

Указами Президента Российской Федерации от 21 апреля 1996 г. No573, от 14 июня 1997 г. No594.

- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. No644.
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. No188.
- Инструкция No0126–87.

Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. No921– 51.

- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. No1233.
- «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15 апреля 1995 г. No333.
- «О внесении дополнения в Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 30 апреля 1997 г. No513.

- «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. No870.
- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. No973.
- «О сертификации средств защиты информации» от 26 июня 1995 г, No608.

Ниже представлены законы Российской Федерации, которые необходимо учитывать в работе:

- «О государственной тайне» от 21 июля 1993 г. No5151–1.
- «Об информации, информатизации и защите информации» от 20 февраля 1995 г. No24-ФЗ.
- «О безопасности» от 5 марта 1992 г. No2446–1.
- «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. No4524–1.
- «О связи» от 16 февраля 1995 г. No15-ФЗ.
- «Об участии в международном информационном обмене» от 4 июля 1996 г. No85-ФЗ.

Ниже представлен перечень распорядительных документов ФСТЭК:

- СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам.
- СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации.
- Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров.
- Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации.

- Временный порядок аттестации объектов информатизации по требованиям безопасности информации.
- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
- Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования.
- Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей.
- Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам.

Требования по защите информации на объектах типа АЭС сформулированы на основе следующих документов:

1. Федеральный закон № 170 от 21 ноября 1995 г. «Об использовании атомной энергии»
 - a. Глава V. Государственное регулирование безопасности при использовании атомной энергии
 - i. Статья 23. Государственное регулирование безопасности при использовании атомной энергии
 - ii. Статья 25. Полномочия органов государственного регулирования безопасности
 - iii. Статья 26. Разрешения (лицензии) на право ведения работ в области использования атомной энергии
 - iv. Статья 27. Разрешения на право ведения работ в области использования атомной энергии, выдаваемые работникам объектов использования атомной энергии
2. Федеральный закон № 187 от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»
 - a. Статья 3. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры
 - b. Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры
 - c. Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры
 - d. Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры

- e. Статья 12. Оценка безопасности критической информационной инфраструктуры
 - f. Статья 13. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры
- 3. Федеральный закон № 5485-1 от 21 июля 1993 г. «О государственной тайне»
 - a. Раздел VI. Защита государственной тайны
 - i. Статья 21. Допуск должностных лиц и граждан к государственной тайне
 - ii. Статья 21.1. Особый порядок допуска к государственной тайне
 - iii. Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне
 - iv. Статья 23. Условия прекращения допуска должностного лица или гражданина к государственной тайне
 - v. Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне
 - vi. Статья 25. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну
 - vii. Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне
 - viii. Статья 27. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну

ix. Статья 28. Порядок сертификации средств защиты информации

4. Постановление Правительства РФ № 669 от 12 июля 2016 г. «Об утверждении Положения о стандартизации в отношении продукции (работ, услуг), для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, а также процессов и иных объектов стандартизации, связанных с такой продукцией»
 - a. Обеспечение средствами стандартизации необходимого уровня безопасности объектов использования атомной энергии
 - b. Обеспечение единой технической политики в сфере стандартизации в отношении обеспечения безопасности объектов использования атомной энергии
 - c. Внедрение средствами стандартизации передовых технологий в области использования атомной энергии с учетом того, что технические и организационные решения, принимаемые для обеспечения безопасности объекта использования атомной энергии, должны быть апробированы прежним опытом, испытаниями, исследованиями, опытом эксплуатации прототипов
5. Постановление Правительства РФ № 749 от 26 июня 2017 г. «Об установлении зон безопасности с особым правовым режимом объекта использования атомной энергии»
 - a. Пункт 2. Ограничения на въезд и пребывание граждан на территории зоны безопасности
 - b. Пункт 3. Ограничения на полеты летательных аппаратов
6. Приказ ФСТЭК № 31 от 14 марта 2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизирован-

ных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

а. Пункт 2. Требования к организации защиты информации в автоматизированной системе управления

- i. Разработка системы защиты автоматизированной системы управления
- ii. Внедрение системы защиты автоматизированной системы управления и ввод ее в действие
- iii. Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления
- iv. Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления

б. Пункт 3. Требования к мерам защиты информации в автоматизированной системе управления

7. Приказ ФСТЭК № 235 от 21 декабря 2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

а. Пункт 3. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры

б. Пункт 4. Требования к организационно-распорядительным документам по безопасности значимых объектов

с. Пункт 5. Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры

8. Приказ ФСТЭК № 239 от 25 декабря 2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

а. Пункт 2. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

- i. Установление требований к обеспечению безопасности значимого объекта
- ii. Разработка организационных и технических мер по обеспечению безопасности значимого объекта
- iii. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
- iv. Обеспечение безопасности значимого объекта в ходе его эксплуатации
- v. Обеспечение безопасности значимого объекта при выводе его из эксплуатации

б. Пункт 3. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

с. Пункт 4. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов

9. Федеральные нормы и правила в области использования атомной энергии «Общие положения обеспечения безопасности атомных станций» (НП-001-15)

а. Пункт 3. Основные принципы безопасности, реализуемые в проекте атомной станции и ее систем

10. Федеральные нормы и правила в области использования атомной энергии «Правила устройства и эксплуатации локализирующих систем безопасности атомных станций» (НП-010-16)

а. Пункт 2. Общие требования к локализирующим системам безопасности атомных станций

б. Пункт 10. Эксплуатация локализирующих систем безопасности и их элементов

Регламенты и нормативные документы госкорпорации «Росатом» (11-13):

11. Приказ Государственной корпорации по атомной энергии «Росатом» от 30.10.2018 № 1/31-НПА «Об утверждении Административного регламента Государственной корпорации по атомной энергии «Росатом» по предоставлению государственной услуги «Аккредитация органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, обязательным требованиям»»

12. ИСО 50001-2023 «Системы энергетического менеджмента. Требования и руководство по применению»

а. 9.1 Требование бизнеса по управлению доступом

б. 9.2 Процесс управления доступом пользователей

с. 9.3 Ответственность пользователей

д. 9.4 Управление доступом к системам и приложениям

е. 10.1 Средства криптографической защиты информации

f. 13.1 Менеджмент информационной безопасности сетей

g. 13.2 Передача информации

13.ГОСТ Р ИСО/МЭК 13335-1-2006. «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1.

14.Приказ Государственной корпорации по атомной энергии «Росатом» от 03.10.2017 № 1/31-НПА «Об утверждении Требований к обозначению зоны безопасности с особым правовым режимом объекта использования атомной энергии»

15.Приказ Государственной корпорации по атомной энергии «Росатом» от 28.09.2017 № 1/29-НПА «Об утверждении порядка взаимодействия подразделений ведомственной охраны Государственной корпорации по атомной энергии "Росатом" с территориальными органами федерального органа исполнительной власти в сфере обеспечения безопасности, органами внутренних дел Российской Федерации, войсками национальной гвардии Российской Федерации»

16.ГОСТ Р МЭК 61513-2011 Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования

a. 5 Общий жизненный цикл безопасности систем контроля и управления

i. 5.2 Получение требований систем контроля и управления из проектных основ безопасности атомной станции

ii. 5.3 Выходная документация

iii. 5.4 Проектирование общей архитектуры систем контроля и управления и назначение функций систем контроля и управления

iv. 5.5 Общее планирование

v. 5.6 Выходная документация

b. 6 Жизненный цикл системы безопасности

- i. 6.2 Требования
 - ii. 6.3 Планирование системы
 - iii. 6.4 Выходная документация
 - iv. 6.5 Квалификация системы
- c. 7 Общая интеграция и ввод в эксплуатацию
 - i. 7.2 Цели, которые должны быть достигнуты
 - ii. 7.3 Выходная документация
- d. 8 Общая эксплуатация и техническое обслуживание
 - i. 8.2 Цели, которые должны быть достигнуты
 - ii. 8.3 Выходная документация

17.МЭК ТО 63415-2023 «Атомные станции. Системы контроля и управления. Применение формальных моделей киберзащищенности для проектирования и оценки архитектуры киберзащищенности контроля и управления»

И другие стандарты международной электротехнической комиссии (МЭК/IEC) – IEC 60880:2006, IEC 62645:2014, IEC 62859:2016, проект IEC 63096

18.Документы международного агентства по атомной энергии – NSS 17, NST036, NST037, NST038, NST045, NST047

19.ГОСТ Р МЭК 61226-2011. «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»

- a. 6 Процедура классификации
 - i. 6.2 Определение основ проекта
 - ii. 6.3 Идентификация и классификация функций
- b. 7 Установление технических требований по категориям
 - i. 7.2 Требования, относящиеся к функциям
 - ii. 7.3 Требования, относящиеся к системам контроля и управления
 - iii. 7.4 Требования к оборудованию

iv. 7.5 Требования, связанные с аспектами качества

20.ГОСТ Р ИСО/МЭК 27001-2021 «Системы менеджмента информационной безопасности. Требования»

a. 5 Руководство

i. 5.2 Политика

ii. 5.3 Роли, обязанности и полномочия в организации

b. 6 Планирование

i. 6.1 Действия по рассмотрению рисков и возможностей

ii. 6.2 Цели информационной безопасности и планы по их достижению

c. 7 Обеспечение и поддержка

i. 7.1 Ресурсы

ii. 7.2 Квалификация

iii. 7.3 Осведомленность

iv. 7.4 Взаимодействие

v. 7.5 Документированная информация

d. 8 Функционирование

i. 8.1 Оперативное планирование и контроль

ii. 8.2 Оценка рисков информационной безопасности

iii. 8.3 Обработка рисков информационной безопасности

e. 9 Оценивание исполнения

i. 9.1 Мониторинг, оценка защищенности, анализ и оценивание

ii. 9.2 Внутренний аудит

iii. 9.3 Проверка со стороны руководства

21.ГОСТ Р ИСО/МЭК 27002-2021 «Свод норм и правил применения мер обеспечения информационной безопасности»

a. 5 Политики информационной безопасности

- i. 5.1 Руководящие указания в части информационной безопасности
- b. 6 Организация деятельности по информационной безопасности
 - i. 6.1 Внутренняя организация деятельности по обеспечению информационной безопасности
- c. 8 Менеджмент активов
 - i. 8.1 Ответственность за активы
 - ii. 8.2 Категорирование информации
 - iii. 8.3 Обращение с носителями информации
- d. 9 Управление доступом

22.ГОСТ Р ИСО/МЭК 13335-1-2006 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

- a. 3 Концепции безопасности и взаимосвязи
 - i. 3.2 Активы
 - ii. 3.3 Угрозы
 - iii. 3.4 Уязвимости
 - iv. 3.5 Воздействие
 - v. 3.6 Риск
 - vi. 3.7 Защитные меры
 - vii. 3.8 Ограничения
 - viii. 3.9 Взаимосвязь компонентов безопасности

23.ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009. «Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели»

- a. 5 Базовые концепции
 - i. 5.6 Оценка угроз и рисков
 - ii. 5.7 Степень завершенности программ безопасности
 - iii. 5.8 Политики безопасности

2 Анализ помещений объекта

2.1 Обоснование необходимости защиты информации

Объектом защиты является офис администрации атомной электростанции. Согласно Практическому руководству по обеспечению безопасности ядерной информации, созданному Международным агентством по атомной энергии (МАГАТЭ), наивысшим уровнем секретности для предприятий данного типа является уровень «секретно».

В таком случае, определим класс защищенности автоматизированной системы как 1В согласно классам защищенности, представленным в Руководящем документе Государственной технической комиссии при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта до 1992 года.

В класс 1В выделяются многопользовательские АС, в которых одновременно обрабатывается и хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС. Также в таких системах обрабатывается информация не выше «секретной».

В нашем случае, в автоматизированной системе присутствуют как административные руководящие работники, так и их подчиненные, сотрудники архива, экономического и научного отделов, которые не должны иметь доступа к информации других отделов и личным данным других сотрудников.

2.2 Описание помещения

Рассматриваемые помещения имеют следующую площадь:

- Кабинет директора: 58,41 м²;
- Переговорная: 59,10 м²;
- Рабочая зона: 98,10 м²;
- Архив: 99,20 м²;
- Общее пространство: 264,82 м²;
- Уборная (суммарно): 55,85 м².

Для ведения переговоров выделено специальное помещение, в котором находятся стол для переговоров и стулья вокруг него, проектор с экраном, доски для записей.

В кабинете директора находятся различные шкафы для хранения, столы, кресло, рабочий стол и диван для отдыха.

В рабочей зоне расположены столы для работы, стулья, АРМы сотрудников.

В архиве располагаются шкафы для хранения, рабочее место сотрудника архива из стола и стула.

В общей зоне находится различный гарнитур для отдыха – диваны, столы, стулья, шкафы и столешницы.

2.3 Анализ технических каналов утечки информации и выбор средств защиты

Так как практически в каждом помещении есть декоративные или малозаметные элементы, где можно спрятать закладное устройство. Помимо этого, в каждом помещении имеются розетки, что приводит к наличию электрического и электромагнитного канала утечки информации. Присутствуют угрозы снятия по вибрационному, оптическому и акустическим каналам.

Материально-вещественный канал утечки исключается, так как он регулируется политикой компании об учете физических носителей информации.

В таблице 1 приведены средства защиты информации, необходимые для обеспечения комплексной безопасности согласно типу информации — государственная тайна уровня «секретно».

Таблица 1 – Различные каналы утечек

| Каналы | Источники | Пассивная за- щита | Активная защита |
|--------|-----------|-----------------------|-----------------|
| | | | |

| | | | |
|----------------------------------|---------------------------------------|--|---|
| Акустический/акустоэлектрический | Окна, двери, проводка | Звукоизоляция переговорной комнаты, фильтры для сетей электропитания | Устройства акустического зашумления |
| Вибрационный/виброакустический | Твердые поверхности, особенно батареи | Изолирующие звук и вибрацию обшивки стен | Устройства вибрационного зашумления |
| Электромагнитный/электрический | АРМы, розетки и прочая техника | Фильтры для сетей электропитания | Устройства электромагнитного зашумления |
| Оптический | Окна и двери | Жалюзи или шторы, тонирующие пленки, доводчики на дверях | Бликующие устройства |

К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного способа – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен звукопоглощающими материалами или экранирования технических средств.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

3 Анализ технических средств защиты

Согласно требованиям «Типовых норм и правил проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними», утвержденных Решением Межведомственной комиссии по защите государственной тайны от 21.01.2011 N 199, защита рассматриваемых помещений должна удовлетворять следующим критериям:

1. В помещениях для работы с государственной тайной и хранилищах секретных документов устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери с двух сторон обшиваются металлическим листом не менее 2 мм толщиной, внутри — звукоизоляционный материал, сама дверь должна иметь толщину не менее 4 сантиметров. Дверь устанавливается на металлический каркас.
2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
3. По требованиям безопасности режимных помещений, если окна комнат и хранилищ находятся рядом с водостоком, эвакуационной лестницей, крышами стоящих вблизи зданий, на первом или последнем этаже, каждое окно оборудуется выдвижными ставнями или створками с металлической решеткой, которая крепится к железным конструкциям оконного проема в стене.
4. Все режимные помещения оборудуются аварийным освещением.
5. Оборудование помещений для работы с государственной тайной по требованиям технической безопасности, вся аппаратура, периферия и ПО должны быть сертифицированы и соответствовать требованиям ФСТЭК, предъявляемым к оснащению защищенных и выделенных помещений.

6. Перед началом эксплуатации необходимо проверить выделенные и иные режимные помещения проверить на предмет наличия «жучков» и иных средств несанкционированного получения информации. В дальнейшем такие проверки желательно проводить периодически, чтобы исключить возможность утечки.

3.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита акустического и виброакустического каналов утечки информации представляет собой:

- усиленные двери;
- тамбурное помещение перед переговорной;
- дополнительная отделка переговорной звукоизолирующими материалами.

Активная защита представляет собой систему виброакустического шумления. В таблице 2 приведен сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу.

Таблица 2 – Характеристики устройств

| Устройство | Цена, руб. | Диапазон частот, Гц | Состав |
|------------|------------|---------------------|---|
| КАМЕРТОН-5 | 46000 | 90-11200 | Блок управления и контроля системой; Блок генерации и генератор маскирующих шумов, создающий помехи в речевом диапазоне частот; Виброизлучатели разных типов, блокирующие вибрационные каналы утечки информации (стены, перекрытия, оконные |

| | | | |
|-------|-------|-----------|---|
| | | | <p>рамы, прочие элементы строительной конструкции); Акустоизлучатели разных типов, создающие помехи в акустических каналах Блок управления и контроля системой; Блок генерации и генератор маскирующих шумов, создающий помехи в речевом диапазоне частот; Виброизлучатели разных типов, блокирующие вибрационные каналы утечки информации (стены, перекрытия, оконные рамы, прочие элементы строительной конструкции); Акустоизлучатели разных типов, создающие помехи в акустических каналах.</p> |
| БУРАН | 67500 | 100-11200 | <p>Имеет четыре канала формирования помех, к каждому из которых могут подключаться вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование электрического сигнала, формируемого прибором, в механические колебания в ограждающих конструкциях защищаемого помещения, а также в акустические колебания воздуха.</p> |

| | | | |
|----------------|-------|-----------|--|
| Соната «АВ» 4Б | 44000 | 175-11200 | Блок электропитания и управления, генератор- акустоизлучатель, генератор- вибровозбудитель, размыкатель телефонной линии, размыкатель слаботочной линии, размыкатель линии Ethernet, пульт управления, блок сопряжения с внешними устройствами, техническое средство защиты речевой информации от утечки по оптоэлектронному (лазерному) каналу. |
| Гамма СВАЗ-01 | 28600 | 90-11200 | Имеет четыре канала формирования помех, к каждому из которых могут подключаться вибропреобразователи пьезоэлектрического или электромагнитного типа, а также акустические системы, обеспечивающие преобразование электрического сигнала, формируемого прибором, в механические колебания в ограждающих конструкциях защищаемого помещения, а также в акустические колебания воздуха. |

По результатам анализа была выбрана система Соната «АВ» 4Б.

У этой модели наиболее удобный монтаж, есть возможность индивидуальной регулировки интегрального уровня и корректировки спектра каждого генератора. Также эта модель обладает приемлемой ценой.

3.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

Пассивная защита основывается на установке фильтров для сетей электропитания во всех помещениях. Активная защита основывается на создании в сети белого шума, который скрывает колебания порождаемые воздействием звуковой волны или работающей электрической техникой.

В таблице 3 представлены подходящие средства активной защиты.

Таблица 3 – Характеристики устройств

| Устройство | Цена, руб. | Состав |
|--------------------------------|------------|---|
| Соната-РСЗ | 32400 | Диапазон частот до 2 ГГц, диапазон регулировки. Возможность регулирования уровня излучаемых электромагнитных шумов; возможность блокировки прибора от несанкционированного доступа; световой и звуковой индикаторы работы и контроля уровня излучения; совместимость с проводными пультами ДУ СОНАТА. |
| Сетевой генератор шума ЛГШ-221 | 36400 | Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Световой индикатор работы в стандартном режиме; световая и звуковая сигнализация в случае отказа и перехода в аварийный режим работы; счетчик отработанных часов; возможность интеграции в программно-аппаратный комплекс ДУ и контроля «Паутина». |
| Двухканальный ге- | 24000 | Диапазон частот 10 кГц – 400 МГц, диапазон регулировки уровня шума не менее 20 ДБ. Ге- |

| | | |
|---------------------------------|--|--|
| генератор шумления SEL SP-44 | | генератор регулируемого шума. Индикация нормального / аварийного режима работы. Электропитание от сети переменного тока 220В 50 Гц. Устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания. |
|---------------------------------|--|--|

В результате рассмотрения перечня устройств был выбран генератор шума Соната-РСЗ. Данная модель совместима с выбранной ранее системой Соната «АВ» 4Б, что облегчает установку системы. Данное устройство является эффективным и недорогим решением.

3.3 Защита от побочного электромагнитного излучения и наводок

Защита от ПЭМИН осуществляется методом радиомаскировки, то есть использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации.

В таблице 4 представлены возможные варианты используемых решений.

Таблица 4 – Характеристики устройств

| Устройство | Цена, руб. | Состав |
|------------|------------|--|
| СКИТ-МШ | 16800 | Широкополосный генератор электромагнитных помех. |
| СОНАТА-РЗ | 97200 | Изделие обеспечивает защиту от утечки за счет побочных электромагнитных излучений и наводок путем излучения в окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индицирования в них маскирующих шумовых напряжений. |

| | | |
|-------------------------------------|--------|--|
| Генератор шума SEL SP-21B2 «Спектр» | 112000 | Генератор шума переносной портативный, диапазон частот 0,1–1000 МГц. |
|-------------------------------------|--------|--|

Из-за совместимости с другими устройствами линейки СОНАТА и средней цены выбрано устройство СОНАТА-РЗ.

3.4 Защита от утечек по оптическому каналу

Для прекращения действия оптического канала утечки информации достаточно ликвидировать оптический контакт.

Подобное можно сделать при помощи закрытия окон кабинета шторами или тонированными пленками, что не является самым разумным решением при наличии существенного минуса раскрытия защиты информации.

Наиболее оптимальным вариантом будет применение жалюзи.

Для предотвращения наблюдения через дверь применяется доводчик двери.

4 Описание расстановки технических средств защиты

Оценим необходимое количество устройств и приведем план их размещения на объекте.

Согласно руководству по эксплуатации системы Соната «АВ», существуют нормы предварительного оценивания количества излучателей:

- стены - один на каждые 3...5 метров периметра для капитальной стены при условии установки излучателей на уровне половины высоты помещения;
- потолок, пол - один на каждые 15...25 м² перекрытия;
- один на окно (при установке на оконный переплет);
- один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Пьезоизлучатели устанавливаются в расчете по одному ПИ на каждое окно.

Аудиоизлучатели устанавливаются по одному на каждый вентиляционный канал или дверной тамбур и по одному на каждые 8...12 м³ надпотолочного пространства или других пустот.

В таблице 5 приведена ожидаемая смета на выбранные средства защиты на выбранном объекте.

Таблица 5 – Смета

| Средство защиты | Цена, руб. | Количество, шт. | Стоимость, руб. |
|--|------------|-----------------------|-----------------|
| Соната-СА-4Б1 (генератор-акустоизлучатель) | 3540 | 6 (кабинет директора) | 212400 |
| | | 6 (переговорная) | |
| | | 9 (рабочая | |

| | | | |
|---|-------|--|---------|
| | | зона) 9 (архив) 5 (уборная) 25 (общее пространство) | |
| Соната-СВ-4Б (генератор-вибровозбудитель) | 7440 | 27 (окна и двери) 5 (трубопровод) 48 (стены) 58 (пол и потолок) | 1026720 |
| Соната «АВ» 4Б | 44000 | 1 | 44000 |
| Соната-РСЗ | 32400 | 1 | 32400 |
| Соната-РЗ | 97200 | 1 | 97200 |
| Рычажная тяга | 1000 | 7 | 7000 |
| Жалюзи | 2000 | 10 | 20000 |
| Дверь звукоизолирующая | 78000 | 3 | 234000 |

Итоговая стоимость 1673720 рублей.

Жалюзи устанавливаем на каждом окне. Доводчики устанавливаем на каждой двери. Соната-РЗ и Соната-РСЗ подключены согласно рекомендациям производителя к другим устройствам и отдельно не выделены. Установка остальных элементов системы показана на рисунке 5 ниже.

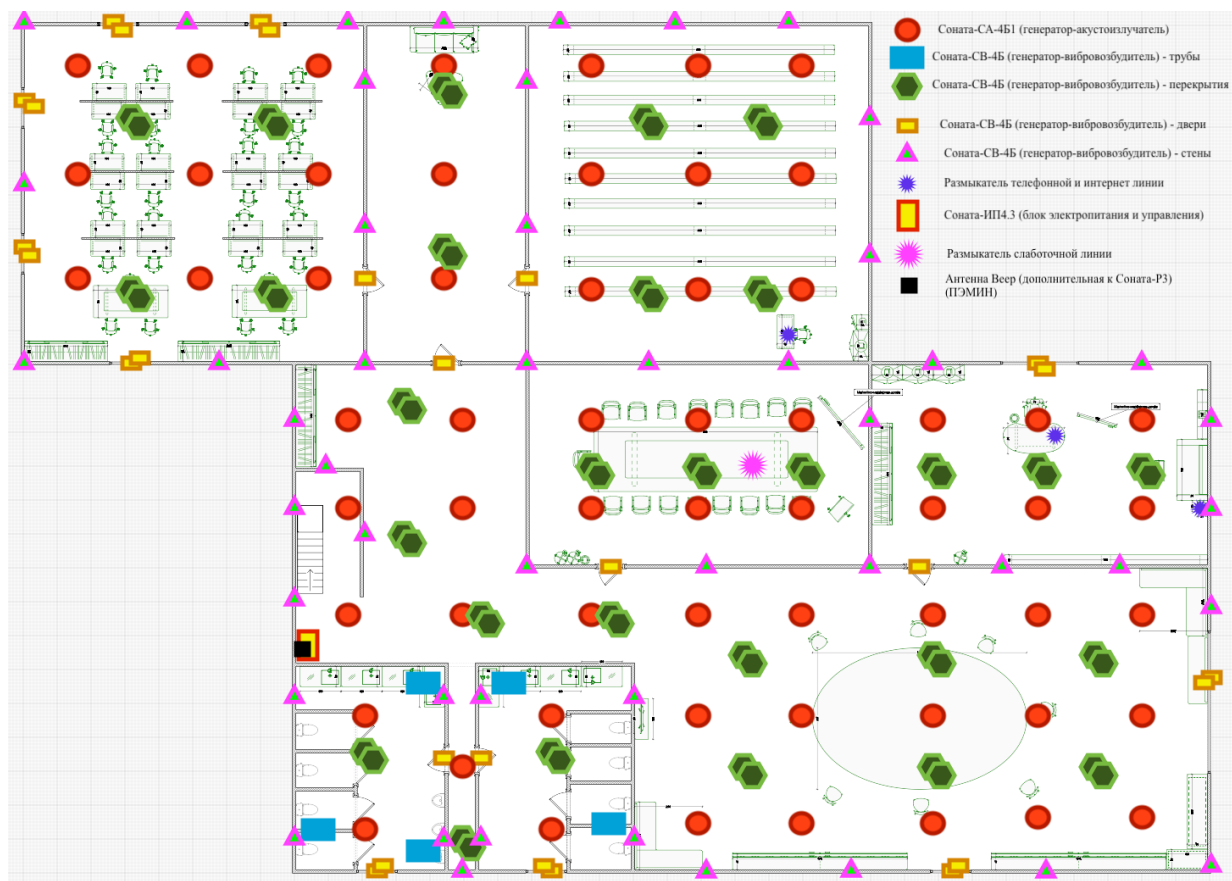


Рисунок 5 – План установки устройств

ЗАКЛЮЧЕНИЕ

В результате выполнения данной работы был проведен теоретический анализ технических каналов утечки информации. Далее были определены руководящие документы, а также проведен анализ защищаемых помещений, проведена оценка каналов утечки информации и выбраны меры пассивной и активной защиты информации.

По итогам работы была составлена смета на основе действующих цен на технические средства защиты информации, итоговое значение суммы затрат составило 1673720 рублей. Также, была нарисована схема расстановки устройств.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. «Система виброакустической и акустической защиты «Соната-АВ». Руководство по эксплуатации» — URL: <http://www.cbi-info.ru/files/sonata-av3m.pdf> (дата обращения: 15.12.2023)
2. РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ. Р 50.1.056–2005. Техническая защита информации. Основные термины и определения. — Москва: Стандартинформ, 2006. — 16 с.
3. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации — Текст : электронный // ФСТЭК России : сайт. — URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3?ysclid=lqbe5zk5v3801711409> (дата обращения: 15.12.2023)
4. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждено 30.08.2002 приказом Председателя Гостехкомиссии России № 282. — URL: <https://wikisec.ru/images/2/2c/Str-k-.pdf> (дата обращения: 15.12.2023)
5. СРЕДСТВА ЗАЩИТЫ ПЕРЕГОВОРОВ ОТ ПРОСЛУШИВАНИЯ — Текст : электронный // Системы комплексной безопасности — Detector Systems : сайт. — URL: https://detsys.ru/catalog/sredstva_zashchity_peregovorov/ (дата обращения: 15.12.2023)
6. Требования к режимным помещениям и их оборудованию — Текст : электронный // Получить лицензию ФСБ: помощь с лицензированием ФСБ и ФСТЭК в Москве и Санкт-Петербурге, цены : сайт. — URL: <https://licenziya-fsb.com/trebovaniya-k-rezhimnym-pomeshheniyam?ysclid=lqbefj9gm6940142668> (дата обращения: 15.12.2023)

ПРИЛОЖЕНИЕ А

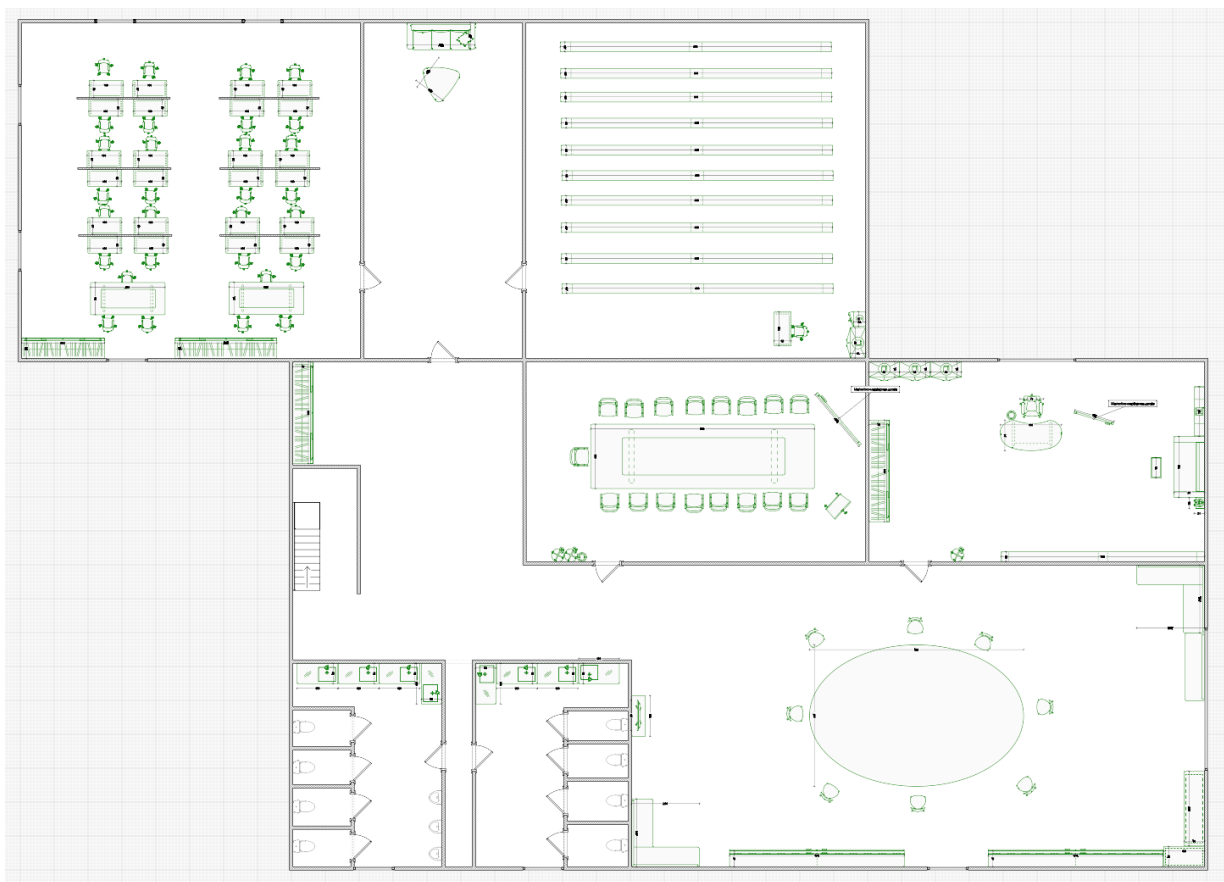


Рисунок 6 – План всего помещения

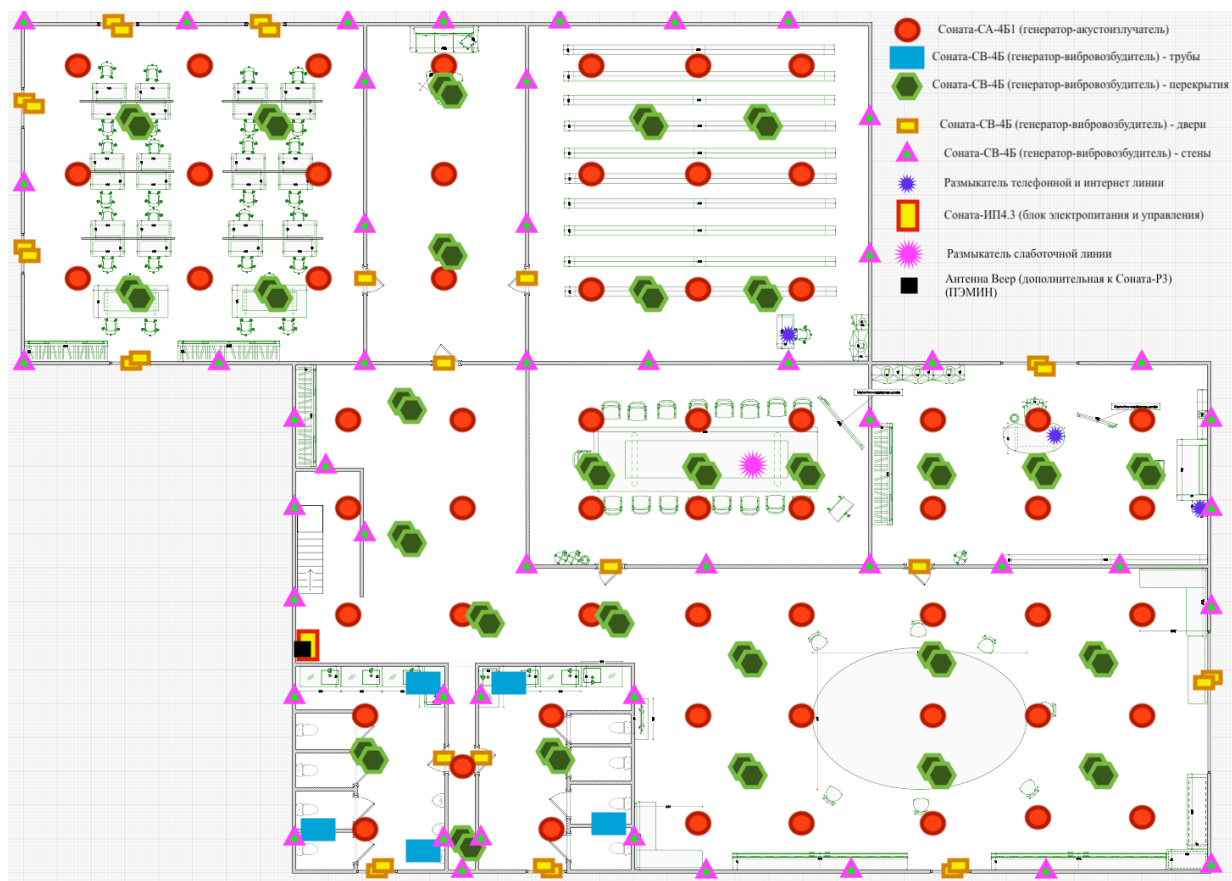


Рисунок 7 – План расположения средств