

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

КУРСОВАЯ РАБОТА

По дисциплине:

**«Инженерно-технические средства защиты
информации»**

На тему:

**Проектирование инженерно-технической защиты
информации на предприятии**

Вариант 27

Выполнил:

Давыдов М.А., гр. N34471


(подпись)

Проверил преподаватель:

Попов И. Ю., доцент ФБИТ

(подпись)

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Давыдов Марк Анатольевич
	(Фамилия И.О.)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	Информационная безопасность
Руководитель	Попов Илья Юрьевич, к.т.н., доцент ФБИТ
	(Фамилия И.О., должность, ученое звание, степень)
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
Задание	Разработать систему инженерно-технической защиты информации на предприятии

Краткие методические указания

- Курсовая работа выполняется в рамках изучения дисциплины «Инженерно-технические средства защиты информации».
- Порядок выполнения и защиты курсовой работы представлен в методических указаниях, размещенных на коммуникационной площадке дисциплины.
- Объект исследований курсовой работы ограничивается заданным помещением.

Содержание пояснительной записки

- Введение.
- Организационная структура предприятия.
- Обоснование защиты информации.
- Анализ защищаемых помещений.
- Анализ рынка технических средств.
- Описание расстановки технических средств.
- Заключение.
- Список литературы.

Рекомендуемая литература

Руководитель		(Подпись, дата)
Студент	Давыдов Марк Анатольевич	21.12.2023
		(Подпись, дата)

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

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Давыдов Марк Анатольевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируема я	Фактически я	
1	Разработка и утверждение задания и календарного плана на курсовую работу	24.10.2023	24.10.2023	
2	Анализ теоретической составляющей	26.11.2023	26.11.2023	
3	Разработка комплекса инженерно-технической защиты информации в заданном помещении	01.12.2023	02.12.2023	
4	Представление выполненной курсовой работы	19.12.2023	21.12.2023	

Руководитель _____

(Подпись, дата)

Студент Давыдов Марк Анатольевич

21.12.2023

(Подпись, дата)

Студент Давыдов Марк Анатольевич

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) Информационная безопасность

Руководитель Попов Илья Юрьевич, к.т.н., доцент ФБИТ

(Фамилия И.О., должность, ученое звание, степень)

Дисциплина Инженерно-технические средства защиты информации

Наименование темы	Проектирование инженерно-технической системы защиты информации на предприятии
--------------------------	---

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

Цель данного исследования заключается в усилении безопасности рассматриваемого объекта. Основное задание включает в себя не только выявление существующих угроз и потенциальных уязвимостей, но и разработку комплекса мер для улучшения как пассивных, так и активных методов обеспечения безопасности. Предлагаемый подход стремится не только к укреплению физической защиты помещения, но и к созданию гибких, адаптивных решений, способных эффективно противостоять современным вызовам в сфере безопасности. Важным компонентом работы над проектом является интеграция новейших технологий и инновационных методов, чтобы обеспечить высокую эффективность и надежность в области обеспечения безопасности.

□ Расчет

□ Конструирование

□ Моделирование

☒ Другое Проектирование

1. Введение.
2. Организационная структура предприятия.
3. Обоснование защиты информации.
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы.

В ходе проведения исследования были выявлены универсальные стратегии по предотвращению является в

потенциальных утечек важной информации через различные технические каналы на предприятии.

Проведенный анализ областей кибер- и физической безопасности подчеркнул важность постоянного

совершенствования стратегий защиты и интеграции передовых методов предотвращения. Выводом

необходимость не только технологических решений, но и формирования внутренней культуры

безопасности в организации. Это включает систематическое обучение сотрудников и их активное участие

обеспечении безопасности. Разработка такого всестороннего адаптивного подхода становится

неотъемлемой частью эффективной стратегии защиты в современном информационном обществе, где

динамичность и непредсказуемость являются неотъемлемыми аспектами.

Руководитель _____

(Подпись, дата)

Студент Давыдов Марк Анатольевич

21.12.2023

(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	7
1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ	8
1.1 Анализ технических каналов утечки информации	8
1.2 Информационные потоки.....	13
1.3 Перечень руководящих документов.....	14
1.4 Структура информационных потоков на предприятии	17
2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ	19
3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	22
3.1 Схема помещения	22
3.2 Анализ возможных каналов утечки информации	23
4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ	24
4.1 Выбор средств защиты.....	24
4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам	25
4.3 Защита от утечки информации по (вибро-) акустическим каналам.....	28
4.4 Защита от ПЭМИН.....	31
4.5 Защита от утечек информации по оптическим каналам	33
5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ	34
ЗАКЛЮЧЕНИЕ	39
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	40

ВВЕДЕНИЕ

Информационная безопасность предприятий в условиях современных технологических вызовов требует тщательного проектирования инженерно-технической защиты. Данная курсовая работа посвящена исследованию и разработке мероприятий, направленных на обеспечение безопасности информации.

Средства защиты информации (СЗИ) представляют собой комплекс технических, программных и организационных мер, направленных на предотвращение, выявление и противодействие угрозам информационной безопасности. Технические средства включают в себя системы криптографической защиты, биометрические устройства, системы антивирусной защиты, а также противоаварийные и противопожарные системы. Программные средства включают в себя антивирусные программы, программы мониторинга и аудита. Организационные меры включают в себя разработку политик безопасности, обучение персонала и управление доступом.

В рамках курсовой работы будет уделено внимание обеспечению инженерно-технической безопасности от утечек по техническим каналам. Рассмотрение этого вопроса позволит подобрать эффективные меры и лучшие на рынке устройства для предотвращения утечек данных, обеспечивая тем самым полноценную инженерно-техническую защиту информации на предприятии.

1 ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1 Анализ технических каналов утечки информации

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

Эта утечка может быть следствием:

- разглашения конфиденциальной информации;
- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Согласно теме курсовой работы, рассматриваться будет только утечка информации по техническим каналам.

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

Утечка (информации) по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. На рисунке 1 приведена структура технического канала утечки информации.



Рисунок 1 – Структура технического канала утечки информации

На вход ТКУИ поступает информация в виде первичного сигнала,

представляющего собой носитель с информацией от её источника.

Источниками сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) 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, поэтому полученную информацию передатчик преобразует в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Среда распространения сигнала - физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником. Она характеризуется набором физических параметров, определяющих условия перемещения сигнала. Основными параметрами, которые надо учитывать при описании среды распространения, являются:

- физические препятствия для субъектов и материальных тел;
- мера ослабления сигнала на единицу длины;
- частотная характеристика;
- вид и мощность помех для сигнала.

Приемник после этого производит следующие действия:

- выбор носителя с нужной получателю информацией;
- усиление принятого сигнала до значений, обеспечивающих съём информации;
- съём информации с носителя;
- преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Классификация технических каналов утечки информации приведена на рисунке 2.



Рисунок 2 – Классификация технических каналов утечки информации

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по металлическим проводам. Акустические ТКУИ в свою очередь делятся на акустоэлектрическом, виброакустическом и акустические.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Снятие информации возможно с помощью наблюдения, например, через подсматривание в окно или приоткрытую дверь. Альтернативой является использование закладного устройства с возможностью фото или видеозаписи. Данный канал утечки актуален для графической формы представления информации, защита осуществляется методом установки жалюзи или другой формой непрозрачного покрытия на все просматриваемые снаружи поверхности (окна, стеклянные двери и т. д.), а также использованием доводчиков для дверей.

В радиоэлектронном канале утечки информации в качестве носителей

используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового.

Электромагнитный ТКУИ связан с перехватом электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию. Данный канал утечки актуален при наличии в помещении электронной вычислительной техники, компьютеров или других средств обработки информации. Создаваемое при работе технических устройств электромагнитное излучение называют побочным электромагнитным излучением и наводками (ПЭМИН); защита осуществляется посредством специальных технических устройств, создающих электромагнитный шум, скрывающий это электромагнитное излучение.

Электрический ТКУИ связан со съемом информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Электрические колебания, появляющиеся при работе электрических приборов, содержат информацию о подключенных устройствах. Защита осуществляется посредством специальных фильтров для сетей электропитания, которые скрывают электрические колебания, вызываемые вычислительной техникой.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Снятие информации возможно либо с помощью подслушивания из-за пределов помещения (при отсутствии звукоизоляции), либо с помощью закладных устройств с

функциями аудиозаписи. Данный канал утечки актуален при передаче информации в звуковой форме (диалог, совещание, др.); защита осуществляется посредством использования звукоизолирующих материалов, мешающих звуку выйти за пределы помещения, а также использованием специальных программных и аппаратных средств, позволяющих выявить закладки.

В акустоэлектрическом канале информация представлена в виде акустических колебаний, которые далее воздействуют на сети электропитания, вызывая электрические колебания. При снятии этих колебаний есть возможность восстановить исходный акустический сигнал. Данный канал утечки информации актуален, когда в контролируемом помещении есть электрические сети, связанные с внешней территорией. Например, телефонная сеть – подав небольшое напряжение на входящую телефонную линию и сняв его на входе, мы сможем получить распространяющуюся в помещение звуковую информацию. Защита осуществляется посредством использования специальных фильтры для сетей электропитания, скрывающих колебания, вызванные воздействием на электрические сети.

В виброакустическом канале информация изначально представлена в виде акустических колебаний, которые воздействуют на некоторую твердую поверхность, превращаясь в вибрационные колебания. Данный канал утечки информации актуален практически всегда, так как связан с наличием твёрдых поверхностей в контролируемом помещении, в т. ч. стен, потолка и пола, батарей отопления, оконных стёкол. Защита осуществляется путём использования специальных технических устройства, которые передают на защищаемую твердую поверхность белый шум, который скрывает вибрационные колебания, вызванные акустическими волнами.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве

вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага, портативные носители информации (HHD, SSD, проч. карты памяти). С кражей или копированием информации, зафиксированной на материальных носителях борются в первую очередь организационными мерами, вводя строгий порядок учета и работы с данными видами носителей.

Отдельной угрозой является возможность проникновения злоумышленника на территорию охраняемого помещения, так что не менее актуальным вопросом является рассмотрение контроля доступа на охраняемую территорию.

1.2 Информационные потоки

Информационный поток представляет собой совокупность передаваемых сообщений в логистической системе, служащих для эффективного управления, анализа и контроля логистических операций на предприятии. Корректное управление и обеспечение безопасности информационных потоков играют важную роль в обеспечении конфиденциальности, целостности и доступности данных.

Эти потоки могут представляться разнообразными формами, включая бумажные и электронные документы, аудиозаписи, символы и сигналы. Основное деление информационных потоков на открытые и закрытые производится в зависимости от их цели.

Открытые информационные потоки доступны всем сотрудникам и заинтересованным сторонам в пределах предприятия без ограничений. Эти потоки включают в себя информацию, не содержащую чувствительных данных и не требующую дополнительных уровней доступа. Открытые потоки способствуют эффективному внутреннему обмену информацией, создавая атмосферу открытости и прозрачности.

В свою очередь, закрытые информационные потоки содержат

конфиденциальную и чувствительную информацию, требующую повышенного уровня защиты. Эти потоки включают в себя финансовые данные, персональные записи, интеллектуальную собственность и другую конфиденциальную информацию, которая при попадании в неправильные руки может повлечь серьезные последствия для предприятия. Защита закрытых потоков включает строгие политики доступа, шифрование данных и другие меры безопасности, направленные на обеспечение безопасности конфиденциальной информации.

1.3 Перечень руководящих документов

Основными указами Президента Российской Федерации в области предотвращения утечки информации по техническим каналам являются:

- «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. №573, от 14 июня 1997 г. №594;
- «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 8 мая 1993 г. №644;
- «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. №188.

Основными постановлениями Правительства Российской Федерации в области предотвращения утечки информации по техническим каналам

являются:

- инструкция №0126–87;
- 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. №921–51;
- «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» от 3 ноября 1994 г. №1233;
- «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. №333;
- «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. №513;
- «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» от 4 сентября 1995 г. №870;
- «Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам» от 2 августа 1997 г. №973;
- «О сертификации средств защиты информации» от 26 июня 1995 г. №608.

Также на сайте ФСТЭК существует отдельный раздел, содержащий специальные нормативно-технические документы ФСТЭК России –

нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации:

- 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;
- 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.

Также, необходимо обратить внимания на законы Российской Федерации:

- «О государственной тайне» от 21 июля 1993 г. №5151–1;
- «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ;
- «О безопасности» от 5 марта 1992 г. №2446–1;
- «О федеральных органах правительственной связи и информации» от 19 февраля 1993 г. №4524–1;
- «О связи» от 16 февраля 1995 г. №15-ФЗ;
- «Об участии в международном информационном обмене» от 4 июля 1996 г. №85-ФЗ.

1.4 Структура информационных потоков на предприятии

На схеме информационных потоков (рисунок 3) синим цветом обозначены открытые потоки, включающие в себя бухгалтерскую и финансовую отчетность, а также налоговые сведения. Закрытые потоки, выделенные красным цветом, содержат важную защищаемую информацию, такую как персональные данные клиентов и сотрудников, служебная и коммерческая тайны, а также сведения о разрабатываемом программном продукте, включая программный код, его назначение и другие характеристики.

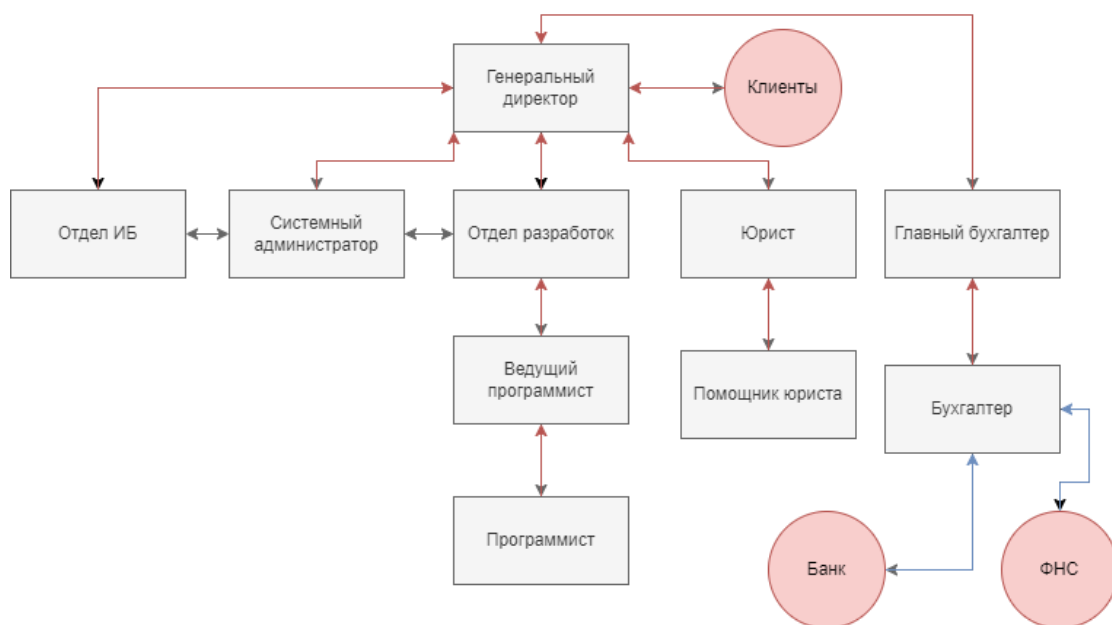


Рисунок 3 – Схема информационных потоков на предприятии

2 ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

В соответствии с поставленной задачей для курсовой работы, разрабатываемая система защиты информации предназначена для данных, классифицированных как государственная тайна уровня «совершенно секретно». 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, обеспечение защиты предполагаемых помещений должно соответствовать следующим критериям:

1. Для помещений, предназначенных для работы с государственной тайной, а также для хранилищ секретных документов, устанавливаются усиленные двери, обеспечивающие надежное закрытие. Двери оснащаются двусторонней обшивкой из металлического листа толщиной не менее 2 мм, внутренняя часть заполняется звукоизоляционным материалом. Толщина двери составляет не менее 4 сантиметров, а ее установка производится на металлический каркас.

2. Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными помещениями в здании;

3. Согласно требованиям безопасности для 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, крепящейся к железным конструкциям оконного проема в стене;

4. Все режимные помещения оснащаются аварийным освещением;

5. Оборудование помещений для работы с государственной тайной должно соответствовать требованиям технической безопасности. Вся используемая аппаратура, периферийные устройства и программное обеспечение должны быть сертифицированы и соответствовать стандартам

безопасности, установленным ФСТЭК;

6. Перед вводом в эксплуатацию выделенных и других режимных помещений необходимо провести проверку на наличие "жучков" и других средств несанкционированного получения информации. Подобные проверки следует проводить периодически для исключения возможности утечки информации.

Согласно Руководящему документу Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» от 30 марта 1992 г.: «При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники.

Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В» (таблица 1).

Таблица 1 – Классы защищенности автоматизированных систем

<p>Первая группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)</p>	1А	В случае обработки секретной информации с грифом «особая важность»
	1Б	В случае обработки секретной информации с грифом не выше «совершенно секретно»
	1В	В случае обработки секретной информации с грифом не выше «секретно»
	1Г	АС, в которых циркулирует служебная информация
	1Д	АС, в которых циркулируют персональные данные
<p>Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)</p>	2А	Информация, составляющая гостайну
	2Б	Служебная тайна или персональные данные

Продолжение таблицы 1

<p>Третья группа (многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС)</p>	3А	Информация, составляющая гостайну
	3Б	Служебная тайна или персональные данные

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1 Схема помещения

Для размещения технических средств защиты на объекте необходимо провести анализ защищаемого помещения, представленного на плане офисного типа предприятия (рисунок 4).

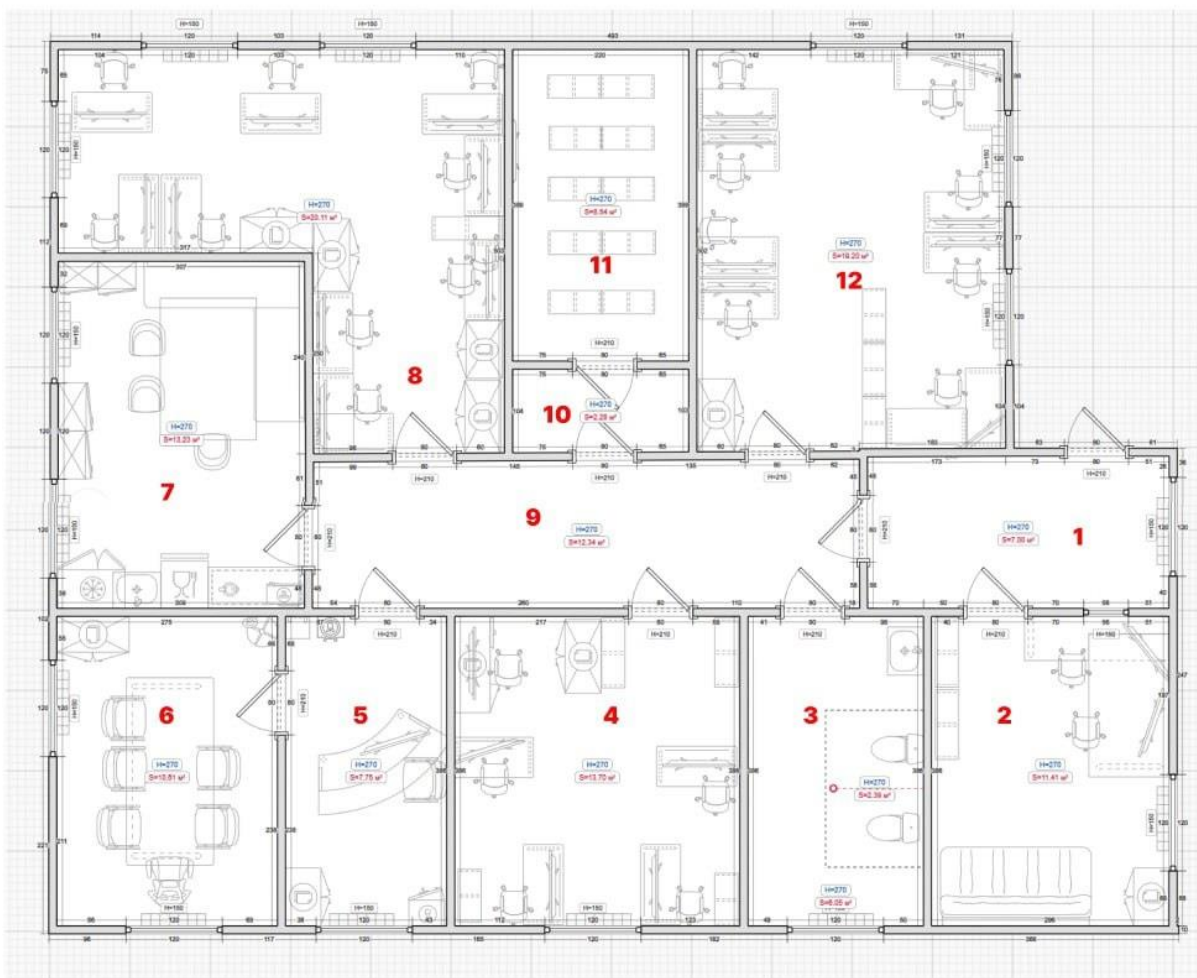


Рисунок 4 – План защищаемого помещения

3.2 Анализ возможных каналов утечки информации

В каждом помещении существуют потенциальные маршруты для нежелательной утечки информации, связанные с электромагнитными и электрическими протечками, такими как использование компьютеров и розеток. Декоративные элементы, вроде комнатных растений, могут служить средствами для установки подслушивающих устройств, которые способны передавать информацию через акустический канал.

Существует также риск утечки информации через оптические каналы, например, из-за незакрытых окон или незащищенных дверей. Необходимо также учитывать виброакустический канал, который может использоваться для передачи информации через твердые поверхности, такие как стены или батареи отопления.

Существует возможность вещественно-материального канала утечки информации из-за наличия материальных носителей данных, однако этот канал не может быть полностью заблокирован с использованием технических средств защиты.

4 АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

4.1 Выбор средств защиты

Для обеспечения высокого уровня комплексной безопасности информации, которая отнесена к категории «совершенно секретно» в зависимости от её типа, требуется оснащение помещения специальными средствами и устройствами, перечисленными в таблице 2. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 2 – Активная и пассивная защита информации

Каналы	Источники	Активная защита	Пассивная защита
Акустический Электроакустический	Стены, двери, окна, электрические сигналы	Устройства акустического зашумления	Защитные экраны и фильтры для сетей электропитания, изоляция особо важных помещений

Продолжение таблицы 2

Виброакустический	Стекла, стены и иные твердые поверхности	Устройства вибрационного зашумления	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов
Визуально-оптический	Окна и стеклянные поверхности, двери	Жалюзи, бликующие устройства	Защитные экраны и фильтры для сетей электропитания
Электрический Электромагнитный	Компьютеры, сервера, бытовая техника, розетки	Устройства электромагнитного зашумления	Защитные экраны и фильтры для сетей электропитания

4.2 Защита от утечки информации по электрическим, акустоэлектрическим и электромагнитным каналам

Пассивная защита в данном контексте включает в себя установку фильтров в электропитании всех помещений, направленных на минимизацию возможных электромагнитных и электрических утечек информации.

Система активной защиты основана на использовании белого шума в сети. Эта система генерирует постоянный фоновый шум, который маскирует колебания, возникающие от звуковых волн или работы электронных устройств. Для более детального анализа представлены модели устройств и их характеристики в таблице 3. Эти меры активной защиты направлены на

обеспечение дополнительного уровня безопасности и предотвращение возможных технических каналов утечки информации в защищаемых помещениях.

Таблица 3 – Активная защита от утечек информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Особенности
ФП-15М	174 900	<p>Ток нагрузки – 70 А. Уровень шума/затухания – 95 дБ. Напряжение – при постоянном токе 500В / при переменном токе с частотой 50Гц 220В / при переменном токе с частотой 400Гц 115В. Частотный диапазон – 1ГГц - 1,8ГГц.</p> <p>Количество фаз – 3. Тип соединения – экранированный кабель (2шт) в комплекте</p>	<p>Предназначен для подавления побочных электромагнитных излучений и наводок (ПЭМИН) в цепях электропитания, сигнализации, контроля, а также организации ввода этих цепей в защищаемые и экранированные сооружения, помещения, камеры, контейнеры. Для трехфазной сети. Сертификат ФСТЭК.</p>

Продолжение таблицы 3

Модель	Цена, руб.	Характеристики	Особенности
ФСП-1Ф-7А	54 920	<p>Ток нагрузки – 10 А. Уровень шума/затухания – 80 дБ. Напряжение – 220 В. Частотный диапазон – 0,125 - 1000 МГц.</p> <p>Количество фаз – 1. Тип соединения – подключение к однофазным цепям электропитания с заземляющим проводом.</p>	<p>Фильтр высокочастотных и импульсных помех, скачков напряжения на входе.</p> <p>Предназначен для встраивания в сеть с силой тока 7А, напряжением 220В, частотой 50Гц. Имеет небольшой вес и компактные размеры.</p> <p>Сертифицирован ФСТЭК, соответствует нормам ИСО и ГОСТ.</p>
Генератор шума SEL SP-44	26 000	<p>Уровень шума затухания 12–90 дБ. Напряжение 220 В ± 10% 50 Гц. Диапазон частот 10 кГц – 400 МГц.</p> <p>Количество фаз – 1 с заземлением.</p>	<p>Наличие сертификата ФСТЭК, разрешающего использование устройства в выделенных помещениях 3–1 категорий. Функция самодиагностики для оперативного выявления неисправностей и сбоев в работе</p>

На основании анализа, проведенного в таблице 4, был выбран генератор шума ФСП-1Ф-7А. Оптимальный вариант, так как устройство имеет достаточно небольшой вес – 1500 г – и компактный размер – 172 мм x 172 мм x 42 мм.

4.3 Защита от утечки информации по (вибро-) акустическим каналам

Пассивные меры безопасности охватывают установку тамбурной зоны перед переговорной комнатой и усиление дверей для дополнительной защиты. Для обеспечения звукоизоляции переговорной комнаты и офиса руководителя применяются специализированные материалы, способствующие снижению звуковой проницаемости стен и, таким образом, повышению конфиденциальности обсуждаемой информации.

Активные меры безопасности включают в себя систему виброакустической маскировки. Для обеспечения безопасности помещения, где обрабатывается информация с уровнем секретности "совершенно секретно", рассматриваются технические средства активной защиты информации, соответствующие категории не ниже 1Б (таблица 4). Эти меры направлены на предотвращение возможных технических каналов утечки информации, обеспечивая дополнительный уровень безопасности в защищаемых помещениях.

Таблица 4 – Активная защита от утечек информации по (вибро-)акустическим каналам

Модель	Цена, руб.	Характеристики	Особенности
SEL SP-157 Шагрень	47 400	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Защита паролем настроек системы. Отсчёт времени наработки генерации шума по каждому каналу с выводом на экран. Непрерывный контроль состояния системы и каждого отдельного излучателя.
Генератор шума ЛГШ-304	47 400	Диапазон воспроизводимого шумового сигнала 90–11200 Гц. Максимальное количество излучателей – 64. Электропитание 220В/50Гц.	Соответствует требованиям «Требования к средствам активной акустической и вибрационной защиты акустической речевой информации» (ФСТЭК России, 2015) – по 1 классу защиты. Оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима.

Продолжение таблицы 4

Модель	Цена, руб.	Характеристики	Особенности
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175–11200 Гц. Выходное напряжение В $12,5 \pm 0,5$. Электропитание сеть ~ 220 В/50 Гц.	Комплект состоит из блоков электропитания и управления, генераторов-акустоизлучателей, генераторов-вибровозбудителей, размыкателя телефонной линии, размыкателя слаботочной линии, размыкателя линии Ethernet, пульта управления, блоков сопряжения из внешних устройств. Технического средства защиты речевой информации от утечки по оптико-электронному (лазерному) каналу и прочих аксессуаров.

Исходя из анализа, представленного в таблице 4, было принято решение о выборе системы Соната АВ-4Б. По сравнению с альтернативными системами, предназначенными для защиты от утечек информации через акустические и вибрационные каналы, данная система считается наиболее востребованной и получила множество положительных отзывов.

4.4 Защита от ПЭМИН

ПЭМИН – побочные электромагнитные излучения и наводки. Вариант защиты компьютерной информации методом зашумления (радиомаскировки) предполагает использование генераторов шума в помещении, где установлены средства обработки конфиденциальной информации. Зашумление обеспечивается типами генераторов, представленными в таблице 5.

Таблица 5 – Активная защита от ПЭМИН

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ЛГШ-516 СТАФ	51 000	Наличие регулировки уровня шума. Диапазон частот – 0,01–6000 МГц (для изделия, выпускаемого по ВСЦТ.464214.003 ТУ). Электропитание – выполнен в виде сетевого удлинителя с 5 розетками типа F. Мощность – 15 Вт. Режим работы – круглосуточно.	Прибор может быть использован в целях защиты информации, содержащей сведения, составляющие государственную тайну (сертификат ФСТЭК по 2 классу защиты). Может устанавливаться в ВП до 2 категории включительно. Пять уровней регулировки выходного сигнала

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
СТИКС-4	62 400	<p>Диапазон частот – 0,01–1800 МГц (с возможностью расширения полосы до 2500 МГц).</p> <p>Уровень шума – не создает акустического шума.</p> <p>Электропитание – $\sim(187\div 242)\text{В}/50\text{ Гц}$.</p> <p>Мощность – не более 8 ВА. Режим работы – при температуре окружающей среды ниже 35°C не менее 8 ч, при температуре окружающей среды выше 35°C не менее 4 ч, перерыв перед продолжением работы 1 час</p>	<p>Предназначена для активной защиты объектов вычислительной техники от утечки информации за счет побочных электромагнитных излучений и наводок на объектах до 2-й категории включительно. За счет наведения шумового маскирующего электрического сигнала в отходящие от СЗИ «Стикс-4» линии электропитания и заземления, а также в токопроводящие линии и инженерно-технические коммуникации в диапазоне частот 0,01–400 МГц</p>

Продолжение таблицы 5

Модель	Цена, руб.	Характеристики	Особенности
Генератор шума ГНОМ-3М	57 200	<p>Диапазон частот 10 кГц - 1800 МГц.</p> <p>Уровень шума от -26 дБ (мкА/м*√кГц) до 50 дБ(мкВ/м*√кГц).</p> <p>Мощность – 45 Вт.</p>	<p>Предназначен для активной защиты информации, обрабатываемой на электронно-вычислительной технике.</p> <p>Имеет 4 выхода для подключения к цепям электропитания и к антенным контурам.</p> <p>Прост в эксплуатации и не требует дополнительных настроек. Имеет сертификат ФСТЭК</p>

В качестве средства активной защиты от ПЭМИН был выбран генератор шума СТИКС-4. Этот выбор обоснован широким диапазоном частот (от 0,01 до 1800 МГц) и устройство обеспечивает защиту от ПЭМИН до 2-й категории включительно.

4.5 Защита от утечек информации по оптическим каналам

Для предотвращения возможности использования оптического канала для утечки информации можно воспользоваться следующими средствами:

- шторы;
- жалюзи;
- тонированные пленки на стеклах.

Среди предложенных вариантов защиты от оптического канала утечки

информации использование жалюзи выделяется как наиболее эффективное решение. Жалюзи не только препятствуют визуальному наблюдению, но также успешно защищают от солнечных лучей. При выборе таких средств важно учитывать их адаптивность к конкретным потребностям и особенностям окружающей среды, чтобы обеспечить максимальный уровень безопасности.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

В предыдущей главе был проанализирован рынок инженерно-технических средств и были выбраны лучшие средства защиты информации из них, которые включает в себя:

- сетевой генератор шума «Соната РС3»;
- система виброакустической защиты «Соната АВ-4Б»;
- генератор шума «СТИКС-4» от ПЭМИН
- жалюзи на пятнадцать окон;
- четыре усиленные двери с толщиной 4 мм, обшитые металлическим листом не менее 2 мм, внутри – звукоизоляционный материал.

Для каждого помещения оптимальное количество акустоизлучателей и вибровозбудителей зависит от различных факторов, таких как звукоизоляция, форма, материалы стен, местоположение, уровень фонового шума и другие подобные аспекты.

Согласно информации на официальном веб-сайте производителя НПО «АННА» для выбранной системы виброакустической защиты, предварительную оценку необходимого количества вибровозбудителей «Соната СВ-4Б» можно провести, руководствуясь следующими стандартами:

- 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;
- окна – один на окно (при установке на оконный переплет);
- двери – 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.

Предварительная оценка необходимого количества акустоизлучателей «Соната СВ-4Б» может быть выполнена из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м³ над потолочного пространства или других пустот.

В таблице 6 содержится список мер защиты, предназначенных для применения во всех помещениях, а также конечная стоимость.

Таблица 6 – Необходимое оборудование

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Сетевой генератор шума ФСП-1Ф-7А	54 920	1	54 920
Генератор шума СТИКС-4	64 200	1	64 200
Блок электропитания и управления «Соната- ИП4.3»	21 600	1	21 600

Продолжение таблицы 7

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Генератор- акустоизлучатель «Соната СА-4Б1»	3 540	25	88 500

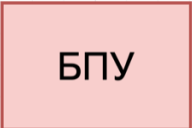
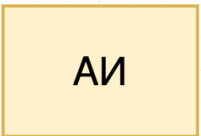
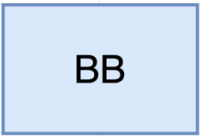
Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Генератор-вибровозбудитель «Соната СА-4Б»	7 440	107	796 080
Размыкатель телефонной линии «Соната ВК4.1»	6 000	2	12 000
Размыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6 000
Размыкатель линии «Ethernet» «Соната ВК4.1»	6 000	1	6 000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7 680
Шторы-плиссе Blackout	4 900	15	73 500
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	83 619	4	334 476
Итого			1 464 956

В трех помещениях установлены усиленные звукоизолирующие двери, как показано на рисунке 5. На каждом окне установлены шторы. Системы «Соната СА-4Б1» и «Соната СВ-4Б» размещены в соответствии с указаниями производителя. ФСП-1Ф-7А и СТИКС-4 находятся рядом с «Соната-ИП4.3» и подключены к ней. Все выключатели установлены в соответствии с рекомендациями производителя. В таблице 7 приведены описание обозначений устройств.


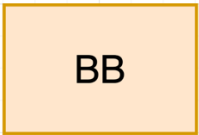

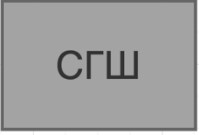


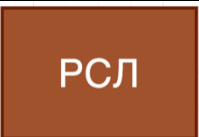

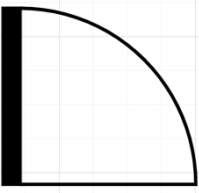



Рисунок 5 – Схема расстановки устройств

Таблица 7 – Описание обозначений устройств

Обозначение	Устройство	Количество, шт.
	Блок электропитания и управления «Соната-ИП4.3»	1
	Генератор-акустоизлучатель «Соната СА-4Б1»	25
	Генератор-вибровозбудитель «Соната СВ-4Б» (стены)	43

Продолжение таблицы 7

Обозначение	Устройство	Количество, шт.
	Генератор-вибровозбудитель «Соната СВ-4Б» (потолок, пол)	22
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	42
	Генератор-вибровозбудитель «Соната СВ-4Б» (трубопровод)	3
	Сетевой генератор шума ФСП-1Ф- 7А	1
	Генератор шума «СТИКС-4»	1
	Размыкатель линии «Ethernet» «Соната-ВК4.3»	1
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	2
	Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	4
	Шторы-плиссе BlackOut	15

ЗАКЛЮЧЕНИЕ

В ходе работы над этой курсовой был осуществлен тщательный анализ информационных потоков в предприятии, охватывая как открытые, так и закрытые каналы передачи данных. Очевидна неотложная необходимость обеспечения надежной защиты информации, включая государственную тайну класса "совершенно секретно". В результате анализа безопасности помещений были выделены ключевые потенциальные угрозы и каналы утечки.

В ходе данной курсовой работы был проведен анализ проблемы обеспечения информационной безопасности на предприятии через проектирование инженерно-технической защиты. Также были проанализированы как закрытые, так и открытые информационные потоки на предприятии, в которой циркулирует государственная тайна типа «совершенно секретно».

Рассмотрение технических каналов утечки информации, что представляет особую актуальность в современных условиях угроз информационной безопасности, позволило выявить потенциальные угрозы и подобрать универсальные средства для перекрытия разного рода технических каналов по физической природе их носителя. Однако, в условиях быстрого развития технологий и появления новых угроз, необходимо постоянное обновление и совершенствование стратегий защиты информации на предприятии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
2. Хорев А. А. Техническая защита информации: учебное пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. – 436 с.
3. Detector Systems: Системы комплексной безопасности [Электронный ресурс]. – Режим доступа: <https://detsys.ru/> (дата обращения: 01.11.2023).