

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

Факультет безопасности информационных технологий

Дисциплина:


«Инженерно-технические средства защиты информации»

ОТЧЕТ ПО КУРСОВОЙ РАБОТЕ

«Разработка комплекса инженерно-технической защиты информации в
помещении»

Выполнил:

Нгуен Хоанг Хиеп, студент группы N34471


(подпись)

Проверил:

К.т.н., доцент фБИТ

Попов Илья Юрьевич

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ**

Студент	Нгуен Хоанг Хиеп
	(Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	10.03.01 Технологии защиты информации (2020)
Руководитель	Попов Илья Юрьевич
	(Фамилия И.О)
Должность, ученое звание, степень	К.т.н., доцент факультета безопасности информационных технологий
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты
Задание	Разработка комплекса инженерно-технической защиты информации в Помещении.


Краткие методические указания

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

Содержание пояснительной записки

1. Введение.
2. Анализ технических каналов утечки информации.
3. Руководящие документы
4. Анализ защищаемых помещений.
5. Анализ рынка технических средств.
6. Описание расстановки технических средств.
7. Заключение.
8. Список литературы

Рекомендуемая литература

Руководитель	
	(Подпись, дата)
Студент	
	(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ**

Студент Нгуен Хоанг Хиеп
(Фамилия И.О)

Факультет Безопасность информационных технологий

Группа N34471

Направление (специальность) 10.03.01 Технологии защиты информации (2020)

Руководитель Попов Илья Юрьевич
(Фамилия И.О)


Должность, ученое звание, степень К.т.н., доцент факультета безопасности информационных технологий

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Разработка комплекса инженерно-технической защиты информации в помещении

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1.	Разработка и утверждение задания и календарного плана на курсовую работу	15.11.2023	15.11.2023	
2.	Анализ теоретической составляющей	02.12.2023	02.12.2023	
3.	Разработка комплекса инженерно-технической защиты информации в заданном помещении	11.12.2023	11.12.2023	
4.	Представление выполненной курсовой работы	19.12.2023	19.12.2023	

Руководитель _____
(Подпись, дата)


Студент 
(Подпись, дата)

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ**

Студент	Нгуен Хоанг Хиеп
	(Фамилия И.О)
Факультет	Безопасность информационных технологий
Группа	N34471
Направление (специальность)	10.03.01 Технологии защиты информации (2020)
Руководитель	Попов Илья Юрьевич
	(Фамилия И.О)
Должность, ученое звание, степень	К.т.н., доцент факультета безопасности информационных технологий
Дисциплина	Инженерно-технические средства защиты информации
Наименование темы	Разработка комплекса инженерно-технической защиты информации в помещении

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы	Целью работы является повышение защищенности рассматриваемого помещения. Задачами является анализ защищаемого помещения, оценка каналов утечки информации и выбор мер пассивной и активной защиты информации.
2. Характер работы	Отчетная курсовая работа
3. Содержание работы	1. Введение. 2. Анализ технических каналов утечки информации. 3. Руководящие документы 4. Анализ защищаемых помещений. 5. Анализ рынка технических средств. 6. Описание расстановки технических средств. 7. Заключение. 8. Список литературы
4. Выводы	По итогам проделанной работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель	
	(Подпись, дата)
Студент	
	(Подпись, дата)

СОДЕРЖАНИЕ

Содержание	5
Введение	6
1 Анализ технических каналов утечки информации.....	8
1.1 Физические каналы утечки информации	9
1.2 Технические каналы утечки информации.....	10
1.2.1 Акустические технические каналы утечки информации.....	10
1.2.2 Визуально-оптические технические каналы утечки информации.....	11
1.2.3 Радиоэлектронные технические каналы утечки информации.....	11
1.2.4 Материально-вещественные технические каналы утечки информации	11
1.3 Информационные каналы утечки	11
2 Руководящие документы.....	13
3 Анализ защищаемых помещений.....	15
3.1 Описание помещений.....	16
3.2 Анализ возможных утечек информации	17
3.3 Выбор средств защиты информации	18
4 Анализ технических средств защиты информации.....	19
4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации	19
4.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации	22
4.3 Защита от ПЭМИН	23
4.4 Защита от утечек по оптическому каналу	23
5 Описание расстановки технических средств	24
Заключение.....	27
Список использованных источников.....	28

ВВЕДЕНИЕ

Обеспечение информационной безопасности любой организации включает в себя управление инцидентами информационной безопасности. Существует ряд методик, определяющих основные параметры управления ими. Эти методики внедряются на уровне национальных и международных стандартов. События или инциденты ИБ в рамках этих регламентов выявляются и регистрируются, их последствия устраняются, а на основании анализа причин их возникновения положения и методики дорабатываются.

Целью данной работы является разработка процесса управления инцидентами информационной безопасности объекта.

Деятельность любого современного предприятия основана на обладании и управлении информацией. В связи с этим защита информации становится предметом пристального внимания, так как повсеместно внедряемые технологии и компоненты без соответствующих предосторожностей быстро становятся источниками проблем. Средства защиты информации (СЗИ) обеспечивают защиту информации в информационных системах, по сути, представляющих собой совокупность хранимой в базах данных информации, информационных технологий, обеспечивающих ее обработку, и технических средств. Они позволяют предотвратить несанкционированный доступ злоумышленника к ресурсам и данным предприятия, тем самым снизив риск несанкционированных утечки, утраты, искажения, уничтожения, копирования и блокирования информации и, как следствие, нанесения экономического, репутационного или других видов ущерба предприятию. Разработка эффективного комплекса мер для выполнения данной задачи является одной из наиболее актуальных современных проблем. Технические средства защиты информации являются важной частью комплекса мер по обеспечению режима конфиденциальности на предприятии.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «секретно» на объекте информатизации. Защищаемый объект состоит из десяти помещений и представляет собой офис предприятия, занимающегося продажей недвижимости со следующими помещениями:

- кабинет руководителя;
- переговорная;
- кабинет сотрудников;
- приемная;

- склад;
- комната отдыха;
- входная зона,
- кухня,
- туалет.

Данная работа состоит из пяти глав. В первой главе произведен анализ технических каналов утечки информации. Во второй приведён перечень управляющих документов. В третьей – анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств. Четвертая глава представляет собой анализ рынка технических средств защиты информации разных категорий. Пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.

1 АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Утечкой информации считают неправомерное распространение набора сведений, выходящее за пределы круга доверенных лиц или организаций, которые хранили эти сведения. Утечкой называют противоправное овладение чужой информацией вне зависимости от того, каким способом достигается получение данных.

Утечка информации происходит при сопутствующих условиях, которые допускают ее возникновение:

- Некомпетентность сотрудников, которые занимаются защитой данных, их непонимание важности процесса и халатное отношение к информации;
- Использование нелегальных средств или не прошедших сертификацию программ по защите конфиденциальной информации;
- Низкая степень контроля над средствами охраны сведений;
- Постоянная смена сотрудников, которые занимаются защитой конфиденциальной информации.

Канал утечки информации – совокупность источника сигнала, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации, оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и вспомогательные технические средства и системы, такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

Канал утечки данных, которыми владеет компания, может быть физическим, техническим или информационным.

Физический канал возникает из-за недостаточной защиты бумажных или электронных носителей информации в процессе их перевозки, хранения, использования для работы. Появление такого канала позволяет злоумышленникам подслушивать служебные разговоры, скрытно изучать и копировать информацию ограниченного доступа.

Техническим называют канал, в котором источниками информации служат шумовые сигналы, излучения и вибрации, исходящие от интересующих объектов. Распространение сигналов происходит через определенную физическую среду (волновую или электрическую). Для улавливания и расшифровки информационных сигналов используется специальная техника.

В информационных каналах происходит потеря компьютерных данных. Угрозы перехвата могут возникать из-за несоблюдения правил обработки, хранения и передачи информации или в результате использования слабозащищенного программного обеспечения.

1.1 Физические каналы утечки информации

Физическими называют каналы утечки информации, возникающие из-за слабой организации физической защиты данных от несанкционированного изучения и копирования, а также от похищения.

Канал подобных утечек может возникать в процессе:

- Передачи сотрудникам документов из хранилища, обмена данными между работниками, знакомства клиентов и поставщиков с деятельностью предприятия;
- Распечатки и тиражирования данных с помощью устройств общего пользования;
- Перевозки документов без должной охраны;
- Размещения документов в архивах и хранилищах;
- Уничтожения данных с несоблюдением правил и требований безопасности.

Каналы утечки информации могут появиться из-за непродуманной организации рабочих мест сотрудников (тесного расположения столов, отсутствие перегородок между ними, хранения документации не в сейфах, а в обычных шкафах).

Причиной утечки графической информации может быть использование в дизайне помещений стеклянных перекрытий, сквозь которые можно визуально проследить за работой сотрудников и изучить обрабатываемые данные.

Для утечки акустической информации достаточно подслушивания разговоров между сотрудниками. Злоумышленники могут подслушать разговоры сотрудников, в которых оглашается конфиденциальная информация. Нередко происходят ситуации, в которых сотрудники обсуждают рабочие проблемы, находясь в общественных местах, провоцируя случайную утечку важной коммерческой информации.

1.2 Технические каналы утечки информации

Происхождение технического канала утечки информации (ТКУИ) может быть естественным и искусственным.

– Естественный технический канал утечки информации появляется в результате способности физических объектов излучать тепло и свет, производить шумы, испускать радиоактивные лучи. Информация об интересующем объекте может быть получена путем косвенного изучения его физических характеристик и состава.

– Искусственный канал утечки создается путем внедрения в линии связи закладных устройств, установки в рабочих помещениях малогабаритных приборов перехвата.

ТКУИ подразделяют на:

- Акустические;
- Оптические;
- Радиоэлектронные;
- Материально-вещественные.

1.2.1 Акустические технические каналы утечки информации

Акустическими называют ТКУИ, которые образуются при прохождении звуковых волн через воздух, жидкие или твердые материалы.

Выделяют следующие разновидности акустического канала утечки информации:

- Воздушный (перехват речевой информации производится с помощью чувствительных направленных микрофонов);
- Виброакустический (злоумышленники используют устройства для улавливания вибрационных колебаний, вызываемых давлением звуковых волн на строительные конструкции зданий);
- Электроакустический (утечка информации происходит из-за преобразования звукового сигнала в электрический при прохождении акустических волн через ВТСС);
- Параметрический (поле, создаваемое источником акустического сигнала, может изменять параметры электромагнитных устройств, используемых злоумышленниками);
- Оптико-акустический (причиной потери данных является «микрофонный» эффект).

1.2.2 Визуально-оптические технические каналы утечки информации

В оптических ТКУИ производится перехват видовой информации с помощью оптических приборов.

По способу перехвата информации визуально-оптические ТКУИ подразделяют на оптические каналы:

- визуального наблюдения (невооруженным глазом или через бинокль);
- фотографирования и видеосъемки;
- перехвата видимого и ИК-излучения, исходящего от объекта информации, с помощью скрытно установленных датчиков.

1.2.3 Радиоэлектронные технические каналы утечки информации

Источниками информационных сигналов в радиоэлектронном канале утечки информации могут быть:

- устройства передачи радиочастотных сигналов, установленные в функциональных каналах связи;
- побочные электромагнитные излучения и наводки;
- аппараты, испускающие тепловые электромагнитные волны;
- объекты, способные отражать радиосигналы.

1.2.4 Материально-вещественные технические каналы утечки информации

В материально-вещественных ТКУИ источниками информации становятся материальные объекты, выносимые за пределы рабочей зоны.

Материально-вещественные ТКУИ классифицируют, учитывая:

- физическое состояние информационных объектов (твердое, жидкое или газообразное);
- природу объектов перехвата (химическую, биологическую, радиоактивную, механическую);
- виды носителей (воздух, земля, вода).

1.3 Информационные каналы утечки

Информационный канал может быть разделен на следующие каналы:

- канал коммутируемых линий связи;
- канал выделенных линий связи;

- канал локальной сети;
- канал машинных носителей информации;
- канал терминальных и периферийных устройств.

В последнее время наиболее динамично развиваются методы съема компьютерной информации. В этом направлении используются:

- аппаратные закладки;
- вредоносные программы.

Основные возможности несанкционированного доступа связаны с использованием специального математического обеспечения, включающего в себя такие составляющие, как компьютерные вирусы, «логические бомбы», «троянские кони», программные закладки и т. п.

В настоящее время известно большое количество программных закладок, основные функции которых следующие:

- слежение за пользователем;
- раскрытие паролей, ключей;
- изучение обрабатываемой информации.

2 РУКОВОДЯЩИЕ ДОКУМЕНТЫ

Основными документами в области защиты информации являются:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».
- Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
- Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
- Указ Президента РФ от 30.11.1995 N 1203 (ред. от 25.03.2021) «Об утверждении Перечня сведений, отнесенных к государственной тайне».
- Постановление Правительства РФ от 26.06.1995 N 608 (ред. От 21.04.2010) «О сертификации средств защиты информации».
- Федеральный закон от 27 июля 2006 г. No 152-ФЗ «О персональных данных».
- Постановление Правительства РФ от 1 ноября 2012 г. No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Закон РФ «О государственной тайне» от 21.07.1993 N 5485–1.
- Межведомственная комиссия по защите государственной тайны решение No 199 от 21.01.2011г. "О Типовых нормах и правилах проектирования помещений для хранения носителей сведений, составляющих государственную тайну, и работы с ними".

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.

- 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.

3 АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

Для перехода к проектированию технических средств защиты на объекте проведем анализ защищаемых помещений. На рисунке 1 информационных потоков сплошной зеленой линией обозначены открытые потоки, а красным пунктиром обозначены закрытые потоки.

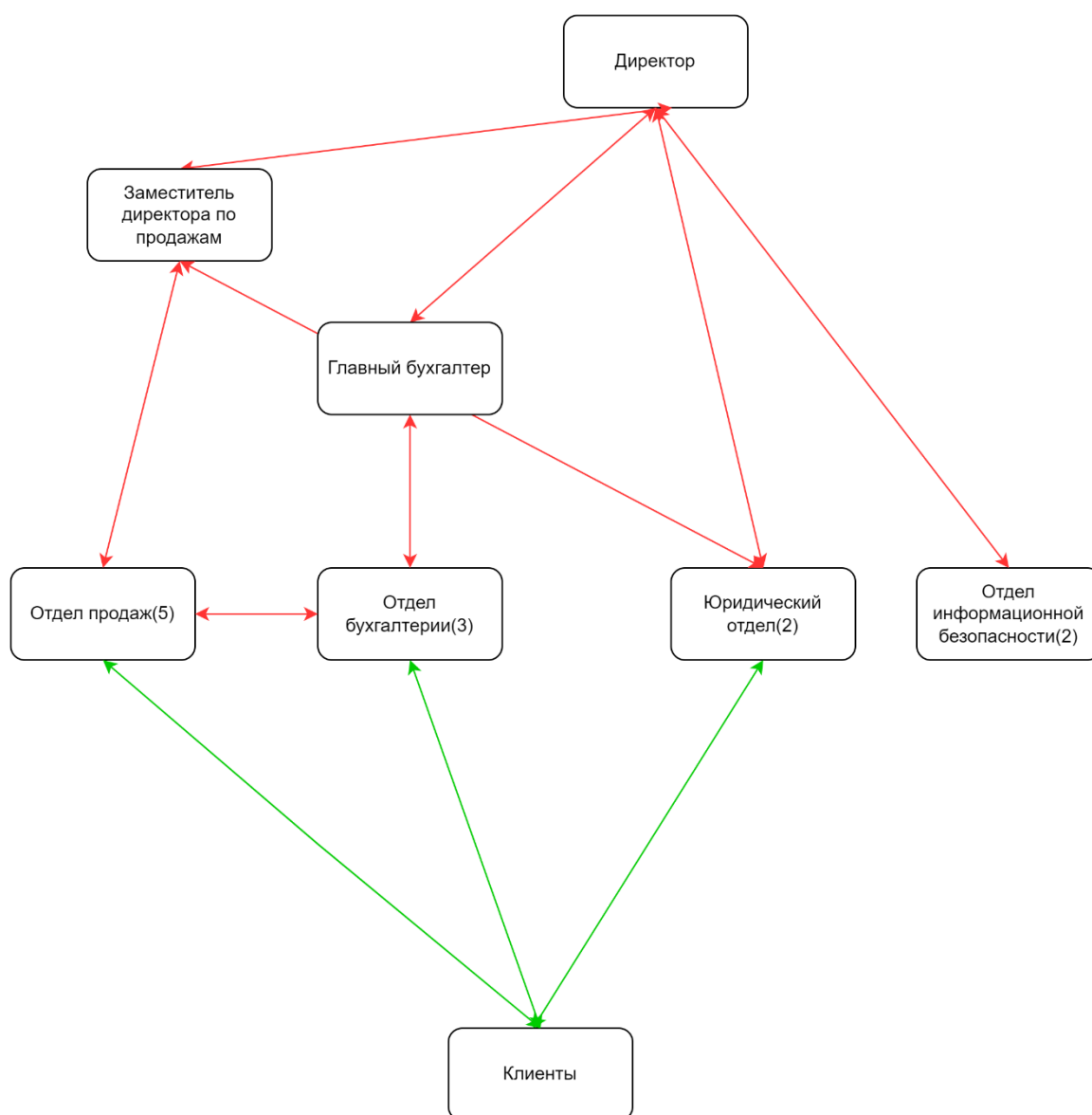


Рисунок 1 – Информационные потоки организации

По открытым потокам передается: информация о продаже недвижимости, информация о состоянии платежей, юридическая информация для клиентов.

По закрытым потокам передается: информация, составляющая служебную тайну, персональные данные сотрудников и клиентов, внутренняя юридическая информация,

финансовая информация, информация о настройке программного обеспечения, информация о мероприятиях по обеспечению ИБ, информация о состоянии системы.

3.1 Описание помещений

На рисунке 2 представлен план защищаемого помещения с учетом мебелировки. Помещение расположено на 1 этаже одноэтажного здания, окна выходят в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и прочими элементами, с которых в помещения могут проникнуть посторонние лица. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см.

Номера на плане здания соответствуют следующим помещениям:

1. Вход и помещение охраны
2. Приёмная: Имеет системы АРМ с диванами для клиентов.
3. Кабинет сотрудников: 70м². В помещении есть два окна, одно находится в кабинете замесителя директора по продажам. Имеет 8 АРМ сотрудников с ТВ, принтером.
4. Склад: 22,5м². В помещении расположены 3 серверов и документы. Окон в помещении нет.
5. Кабинет директора 25м². В помещении есть одно окно. Кабинет директора имеет диван, АРМ, ТВ, настольный телефон, стол и стулья.
6. Переговорная: 45м². В помещении есть одно окно. Имеет большое стол с стульями, ТВ и книжкой шкаф.
7. Комната отдыха: 40м². В помещении есть одно окно. Имеет стол с стульями, ТВ, фортепиано и диваны.
8. Гардеров
9. Туалет
10. Кухня



Рисунок 2 – План защищаемого помещения

3.2 Анализ возможных утечек информации

В помещениях присутствуют декоративные элементы, где можно спрятать закладное устройство. В каждом помещении имеются розетки, а значит, актуальны электрического и электромагнитного каналов утечки информации. Также присутствует угроза снятия информации по вибрационному и оптическому каналам, а также акустическому, виброакустическому, акустоэлектрическому.

Материально-вещественный канал утечки информации регулируется строгой политикой компании в отношении физических носителей информации, и в рамках курсовой работы не рассматривается.

3.3 Выбор средств защиты информации

Для обеспечения комплексной безопасности согласно типу конфиденциальной информации – государственная тайна типа «секретно» требуется оснастить помещение средствам защиты (Таблица 1).

Таблица 1 – Активная и пассивная защита информации

Канал утечки	Источник	Пассивная защита	Активная защита
Акустический, акустоэлектрический	Окна, двери, электрические сети, проводка	Звукоизоляция переговорной, фильтры для сетей электропитания	Устройства акустического зашумления
Вибрационный, виброакустический	Все твердые поверхности помещения, батареи	Изолирующие звук и вибрацию обшивки стен, дополнительное помещение перед переговорной,	Устройства вибрационного зашумления
Оптический	Окна, двери	Жалюзи на окнах, доводчики на дверях	Бликующие устройства
Электромагнитный, электрический	Розетки, АРМ, бытовая техника	Фильтры для сетей электропитания	Устройства электромагнитного зашумления

4 АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В соответствии с заданием на курсовую работу, создаваемая система защиты информации предназначена для информации, составляющей государственную тайну с грифом «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, защита рассматриваемых помещений должна удовлетворять следующим критериям:

- 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 см. Дверь устанавливается на металлический каркас.
- Обязательно устанавливается противопожарное перекрытие между блоком режимных помещений и остальными комнатами в здании.
- 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.
- Все режимные помещения оборудуются аварийным освещением.
- 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.
- 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.

4.1 Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивная защита представляет собой:

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

Активная защита представляет собой систему виброакустического зашумления. Для защиты помещения для работы с государственной тайной уровня «секретно» рассматриваются технические средства активной защиты информации для объектов информатизации категории не ниже 1В. Проведем сравнительный анализ подходящих средств активной защиты помещений по виброакустическому каналу (Таблица 2).

Таблица 2 – Сравнительный анализ средств активной защиты от утечки информации по виброакустическому каналу

Модель	Цена, руб.	Характеристики	Состав
Соната АВ-4Б	44 200	Диапазон воспроизводимого шумового сигнала 175 - 11200 Гц	Блоки электропитания и управления - Соната-ИП4.1, Соната-ИП4.2, Соната-ИП4.3; Генераторы акустоизлучатели – СА-4Б, СА-4Б1; Генератор-вибровозбудитель – СВ-4Б Размыкатель телефонной линии – Соната-ВК4.1; Размыкатель слаботочной линии – Соната-ВК4.2; Размыкатель линии Ethernet – Соната ВК4.3; Пульт управления – Соната ДУ4.3; Блоки сопряжения с внешними устройствами – Соната СК4.1, Соната-СК4.2; Техническое средство защиты речевой информации от утечки по оптико электронному (лазерному) каналу - "Соната-АВ4Л": Генераторный блок "АВ-4Л" + вибровозбудитель "СП4Л"; Аксессуары – фиксатор труба, фиксатор стена, кабель.

ЛГШ-404	35 100	Диапазон рабочих частот 175 - 11200 Гц	Изделие «ЛГШ-404» – генератор шума; Вибровозбудитель «ЛВП-10» – для установки на стены, трубы и окна; Акустический излучатель «ЛВП-2а» - для возбуждения маскирующих акустических помех; Виброэкран «ЛИСТ-1» – для защиты от наблюдения и акустических микрофонов; Размыкатель «ЛУР» – для размыкания слаботочных линий.
Шорох-5Л	15 300	Диапазон частот 80 - 11300	Блок питания и управления «БПУ-1» с активными вибровозбудителями «ПЭД-8А» и активными акустическими излучателями «АИ-8А/Н» и «АИ-8А/Мини»
SEL SP-157 «Шагренъ»	31 200	Диапазон частот 90 - 11200 Гц	Центральный генераторный блок помех SEL SP-157G, вибрационный преобразователь SEL SP-157VP, акустический излучатель SEL SP-157AS, вибрационный преобразователь повышенной мощности SEL SP-157VPS, акустический излучатель повышенной мощности SEL SP-157ASP.

По результатам проведенного анализа средств защиты, в качестве системы виброакустической и акустической защиты была выбрана «Соната АВ-4Б». Данное средство имеет сертификат ФСТЭК и обладает следующими преимуществами:

- возможность построения системы автоматического контроля всех элементов
- снижение трудозатрат на конфигурирование и тестирование системы при инсталляции и контроле
- возможность изменения настроек генераторов-излучателей
- снижение затрат на создание единого комплекса ТСЗИ

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

Пассивная защита заключается в установке фильтров для сетей электропитания во всех помещениях.

Активная защита заключается в создании в сети белого шума, который скрывает колебания, порождаемые воздействием звуковой волны или работающей электрической техникой.

Таблица 3 – Сравнительный анализ средств активной защиты от утечки информации по электрическим каналам

Модель	Цена, руб.	Характеристики	Примечания
ЛГШ-513	39 000	Присутствует регулировка уровня шума; Диапазон частот 0,01 – 1800 МГц	Генератор шума по цепям электропитания, заземления и ПЭМИН
СОНАТА РЗ.1	33 120	Присутствует регулировка уровня шума; Диапазон частот до 2 ГГц	Предназначено для защиты информации от утечки информации за счет побочных электромагнитных излучений и наводок на линии электропитания и заземления, линии проводной связи и токоведущие инженерные коммуникации
ГАММА ГШ-18	29 400	Присутствует регулировка уровня шума; Диапазон частот 0,01 – 1800 МГц	Генератор шума ПЭМИН. Есть регулировка уровня шума, управление осуществляется аттеньюаром, есть возможность увеличить уровень шума за счет подключения внешней антенны

ГНОМ-3М	57 200	Отсутствует регулировка уровня шума; Диапазон частот 0,15 – 1800 МГц	Генератор шум по цепям электропитания, заземления и ПЭМИН. Дистанционное управление отсутствует. Есть возможность подключать внешние антенны.
---------	--------	--	---

В результате проведенного анализа в качестве средства защиты от утечки по электрическим каналам была выбрана «Соната-Р3.1». Данное средство имеет сертификат ФСТЭК. ПЭМИН «Соната-Р3.1» обеспечивает защиту информации 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 индуцирования в них маскирующих шумовых напряжений.

4.3 Защита от ПЭМИН

Для организации активной защиты от ПЭМИН было выбрано средство защиты «Соната-Р3.1». Данный выбор обоснован тем, что устройство совместимо со средством защиты Соната АВ-4Б, которое было выбрано ранее. Также у устройства приемлемая цена, есть возможность регулировать уровень шума, есть возможность управления пультом, и есть удобная индикация исправности устройства.

4.4 Защита от утечек по оптическому каналу

Чтобы обеспечить защиту помещения от визуального наблюдения, необходимо установить на окно шторы, жалюзи или любое другое решение, блокирующее вид снаружи комнаты. Были выбраны жалюзи, так как это наиболее выгодный вариант с точки зрения удобства и затрат на содержание.

5 ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ

Согласно информации, приведённой в 4 главе, выбранные средства защиты информации включают в себя:

- Усиленные двери (толщина не менее 4 см), обшитые металлом (толщина не менее 2 мм) со звукоизолирующей прокладкой на металлическом каркасе – 4 шт.;
- «Соната АВ-4Б»;
- «Соната-РЗ»;
- «Соната-РС2»;
- Жалюзи на 4 окон.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. «Соната АВ-4Б» содержит генераторы-акустоизлучатели «СА-4Б1» и генераторы-вибровозбудители «СВ-4Б1».

Согласно официальному сайту НПО «Анна», необходимое количество генератороввибровозбудителей «СВ-4Б1» можно предварительно оценить из следующих норм:

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 газоснабжения - один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Необходимое количество генераторов-акустоизлучателей «СА-4Б1» можно предварительно оценить из следующих норм:

один на каждый вентиляционный канал или дверной тамбур;

один на каждые 8–12 м³ надпотолочного пространства или других пустот.

Составим смету по результатам выбора средств защиты информации от утечки.

Таблица 4 – Смета

Мера защиты	Цена, руб.	Количество , шт.	Стоимость, руб.
Блок электропитания и управления «Соната-ИП4.3»	21 600	1	21 600
Генератор акустоизлучатель «СА-4Б1»	6 500	15	97 500

Генератор вибровозбудитель «СВ-4Б1»	6 500	34	221 000
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 ВК4.3»	6 000	1	6 000
Усиленные звукоизолирующие двери UltimatumNext	75 283	5	376 415
Жалюзи «Эскар»	2 632	4	10 528
ЛГШ-513	39 000	4	156 000
Средство активной защиты информации от утечки за счет ПЭМИН «Соната Р3»	32 100	1	32 100
Пульт управления «Соната-ДУ4.3»	7 700	1	7 700
Генераторный блок «АВ-4Л»	10 320	1	10 320
Итого:			957 163

Жалюзи установлены на каждом окне. Средством защиты от ПЭМИН является устройство «Соната-Р3». «Соната-РС2» подключена к системе электроснабжения согласно рекомендациям производителя, на схеме отдельно не обозначена.



- | | | | | | | |
|------------|---|------------|--|----------------|--|-------------------------|
| БЛУ | Блок электропитания и управления «Соната-ИП4.3» | ВВ | Генератор вибровозбудитель «СВ-4Б1» (стены) | РСП | Размыкатель слаботочной линии «Соната-ВК4.2» | |
| АИ | Генератор акустоизлучатель «СА-4Б1» | ВВ | Генератор вибровозбудитель «СВ-4Б1» (потолок, пол) | РЛЕ | Размыкатель линии Ethernet «Соната ВК4.3» | |
| ВВ | Генератор вибровозбудитель «СВ-4Б1» (двери, окна) | РТЛ | Размыкатель телефонной линии «Соната-ВК4.1» | | Усиленные звукоизолирующие двери UltimatumNext | |
| | | | | Жалюзи «Эскар» | ЛГШ | Генератор шумов ЛГШ-513 |

Рисунок 3 – Схема расстановки технических средств

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы был проведен анализ потенциальных каналов утечки информации в защищаемом помещении и разобраны необходимые меры их защиты. Были выбраны подходящие для защищаемого объекта средства защиты путем анализа существующих на рынке технических средств противодействия рассматриваемым каналам утечки информации. Также был разработан план установки средств защиты и подсчитана смета расходов.

В результате работы была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, акустоэлектрическому, электрическому, электромагнитному, оптико-электронному техническим каналам защиты информации, а также была обеспечена защита от ПЭМИН.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2010. - 436 с.
2. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст : непосредственный // Молодой ученый. — 2016 — No 3 (107). — С. 69-72. — URL: <https://moluch.ru/archive/107/25842/>
3. Мещеряков Р. В., Шелупанов А. А., Зайцев А. П. Технические средства и методы защиты информации. – 2007. - 507 с
4. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с.