

**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 системы защиты информации на
предприятии»**

Выполнил:

Студент гр. N34532

Дамов Родион Павлович



Проверил преподаватель:

Попов Илья Юрьевич,

доцент ФБИТ, к. т. н.

Отметка о выполнении:

Санкт-Петербург

2023 г.

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

ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент Дамов Родион Павлович
(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34532

Направление (специальность) 11.03.03 – Технологии защиты информации (2020)

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 Проанализировать всевозможные каналы утечки данных в помещении, провести анализ рынка технических средств защиты информации разных категорий, разработать схему расстановки выбранных технических средств в защищаемом помещении

Краткие методические указания

Содержание пояснительной записки

Курсовая работа содержит введение, организационную структуру предприятия, обоснование защиты информации, описание помещения, анализ рынка технических средств, рекомендации по организации защиты, заключение, список источников

Рекомендуемая литература

Руководитель _____
(Подпись, дата)


Студент  06.12.2023
(Подпись, дата)

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

(Фамилия И.О.)

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

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

(Подпись, дата)

(Подпись, дата)

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

Студент Дамов Родион Павлович

(Фамилия И.О.)

Факультет Безопасность информационных технологий

Группа N34532

Направление (специальность) 11.03.03 – Технологии защиты информации (2020)

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

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

Дисциплина Инженерно-технические средства защиты информации

Наименование темы Проектирование инженерно-технической системы защиты информации на предприятии

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

**1. Цель и задачи
работы**

☐ Предложены студентом

☐ Сформулированы при участии студента

☒ Определены руководителем

Цель: разработать инженерно-техническую систему защиты информации на предприятии, обеспечивающую надежную защиту данных и минимизацию рисков утечки, повреждения или несанкционированного доступа к информации.

Задачи: рассмотреть организационную структуру предприятия; обосновать необходимость защиты информации; провести анализ защищаемых помещений; выбрать инженерно-технические средства защиты информации в соответствии с существующим рынком предлагаемых решений; спроектировать систему защиты информации на основе выбранных средств.

**2. Характер
работы**

☐ Расчет

☐ Конструирование

☒ Моделирование

Другое _____

3. Содержание работы

Курсовая работа содержит введение, организационную структуру предприятия, обоснование защиты информации, анализ защищаемых помещений, анализ рынка предлагаемых решений, описание расстановки технических мер защиты информации, заключение, список источников.

4. Выводы

В результате работы был произведен комплексный анализ возможных технических каналов утечки информации в предложенных помещениях, предложены меры пассивной и активной защиты информации.

Руководитель _____

(Подпись, дата)

Студент _____



06.12.2023

(Подпись, дата)

«__» _____ 20__ г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ	7
1.1. Описание организационной структуры предприятия	7
1.2. Информационные потоки.....	7
1.3. Структура информационных потоков на предприятии.....	7
2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ	10
3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ	13
3.1. Схема помещения	13
3.2. Описание помещений	16
3.3. Анализ потенциальных каналов утечек информации	17
4. АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ.....	18
4.1. Выбор средств защиты	18
4.2. Устройства для перекрытия акустического и виброакустического каналов утечки информации	19
4.3. Защита от утечек информации по оптическим каналам	22
4.4. Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации.....	22
5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ	23
ЗАКЛЮЧЕНИЕ	28
СПИСОК ИСПОЛЪЗУЕМЫХ ИСТОЧНИКОВ	29
ПРИЛОЖЕНИЕ 1	30

ВВЕДЕНИЕ

В современном мире, где информационные технологии стремительно развиваются, а организации все более зависят от электронной обработки, хранения и передачи данных, обеспечение безопасности информации становится одной из наиболее актуальных и важных задач. Особенно это важно для компаний, которые оперируют конфиденциальной и важной информацией, такой как персональные данные клиентов, финансовые отчеты, коммерческие секреты и другие чувствительные данные. В этом контексте проектирование системы защиты информации на предприятии играет фундаментальную роль в обеспечении безопасности данных и предотвращении различных угроз.

Средства защиты информации (СЗИ) предназначены для обеспечения безопасности информации в информационных системах, которые включают в себя базы данных, технологии обработки информации и соответствующее оборудование. Они помогают предотвратить несанкционированный доступ злоумышленников к ресурсам и данным предприятия, тем самым снижая риск утечки, потери, искажения, уничтожения, копирования или блокирования информации, что в свою очередь может привести к экономическому, репутационному или иным видам ущерба для предприятия. Разработка эффективного набора мер для решения этой задачи является одной из наиболее актуальных проблем современности. Технические средства защиты информации играют важную роль в комплексе мер по обеспечению конфиденциальности на предприятии.

В данной работе рассмотрен процесс разработки комплекса инженерно-технической защиты информации, составляющей государственную тайну с уровнем «совершенно секретно» на объекте информатизации. Объект имеет 7 помещений, в которые входят кабинет генерального директора, кабинет для совещаний и переговоров, кабинет директора по развитию и бухгалтерии, открытое рабочее пространство, комната отдыха, кухонная зона и ресепшн.

Данная работа состоит из пяти глав. В первой главе произведен анализ организационной структуры предприятия и технических каналов утечки информации. Во второй приведено обоснование необходимости защиты информации и перечень управляющих документов, в третьей произведён анализ защищаемых помещений с точки зрения возможных утечек информации и требуемых для защиты технических средств. Четвертая глава произведён выбор средств ЗИ на основе анализа рынка технических средств защиты информации разных категорий, и пятая глава посвящена разработке схем расстановки выбранных технических средств в защищаемом помещении.

1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

1.1. Описание организационной структуры предприятия

Предприятие – объект, обрабатывающий материальные или информационные потоки.

Организационная структура предприятия – это формальная система, которая определяет, как управляются и координируются различные функциональные направления, подразделения и индивиды в организации.

Схема организационной структуры защищаемого предприятия представлена на рисунке 1.

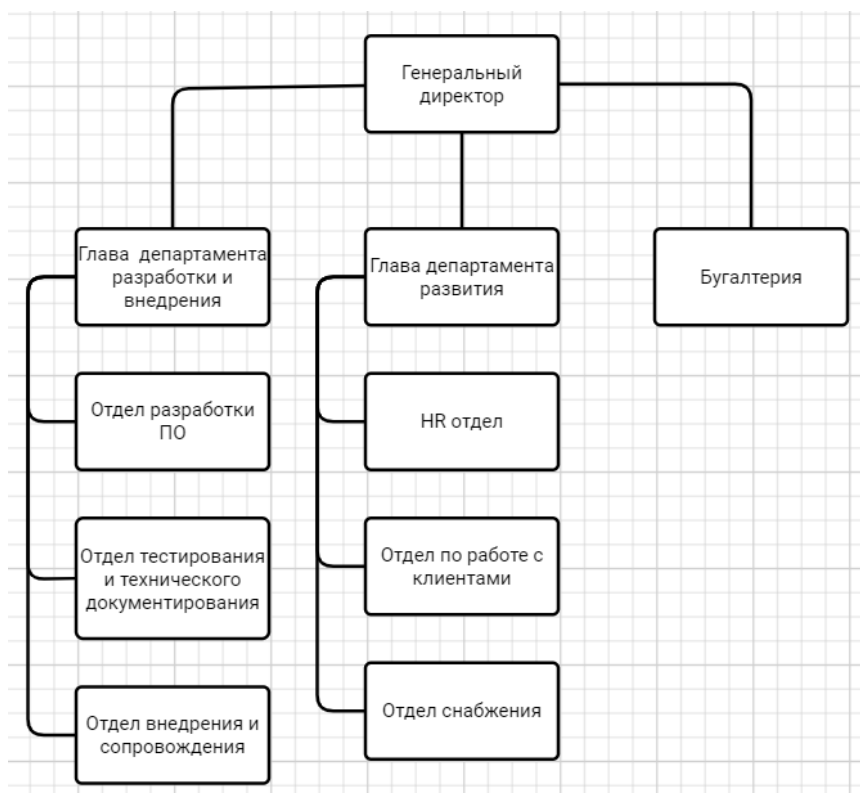


Рисунок 1 – Организационная структура предприятия

1.2. Информационные потоки

Информационные потоки представляют собой ключевую составляющую системы передачи данных в организации или процессе. Схема информационных потоков позволяет визуализировать и описать обмен информацией между различными участниками системы. Она помогает выявить и проанализировать все этапы передачи и обработки информации, идентифицировать узкие места и возможные проблемы в потоке данных, а также оптимизировать процессы коммуникации и обработки информации.

1.3. Структура информационных потоков на предприятии

Схема информационных потоков предприятия представлена на рисунке 2.

Пунктирной линией на схеме обозначены открытые информационные потоки – к ним относятся данные о предприятии от генерального директора в пожарную инспекцию и СанПиН, налоговая отчетность в налоговую службу, связи между отделом снабжения и поставщиками, а также между отделом по работе с клиентами и рекламой.

Остальные информационные потоки являются закрытыми, поскольку содержат в себе один (или несколько) видов защищаемых активов:

- Персональные данные сотрудников и клиентов;
- Секретные сведения, содержащие государственную тайну;
- Конфиденциальная информация, содержащая коммерческую тайну.

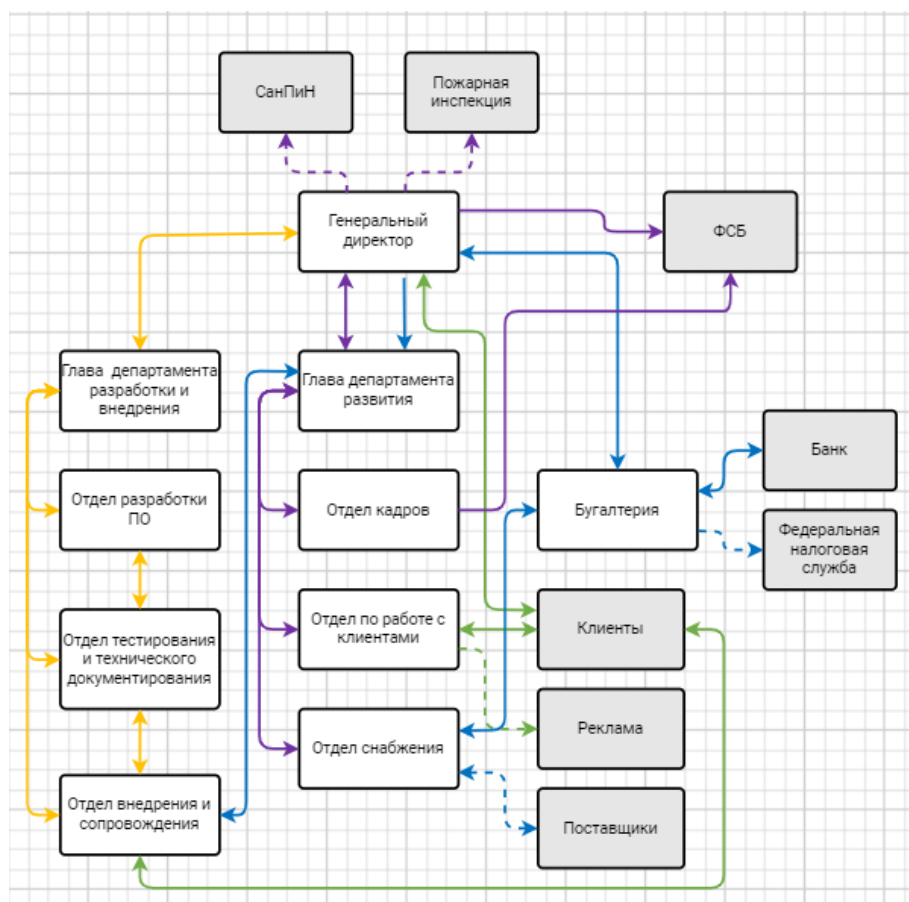








Рисунок 2 – Информационные потоки предприятия

Пояснения к цветовым обозначениям на схеме информационных потоков предприятия представлены в таблице 1.

Таблица 1 – Цветовые обозначения на рисунке 2

Обозначение	Пояснение
	Информация, связанная с основной деятельностью предприятия – разработкой ПО
	Информация, связанная с обеспечением оптимального функционирования основной деятельности предприятия

	Информация, связанная с внешним взаимодействием предприятия на рынке
	Информация, связанная с финансовой деятельностью предприятия
	Внутренние субъекты информационного обмена предприятия
	Внешние субъекты информационного обмена предприятия

2. ОБОСНОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

В информации, хранящейся и обрабатываемой защищаемым объектом, содержатся сведения, содержащие:

1. Коммерческую тайну – информацию, которая относится к бизнесоперациям, процессам, методологиям и стратегиям предприятия, и которая дает ей конкурентное преимущество на рынке. Это могут быть конфиденциальные данные о продуктах, клиентах, партнерах, сделках, финансовых показателях, исследованиях и разработках.
2. Персональные данные – предприятие обрабатывает персональные данные сотрудников, клиентов и сторонних лиц, работающих с проектами. Это может включать личную информацию, такую как имена, адреса, номера телефонов, электронные адреса, финансовые данные, данные о физической и медицинской характеристиках и другие личные сведения.
3. Государственную тайну – это сведения политического, экономического, военного и научно-технического характера, утрата или разглашение которых создает угрозу безопасности и независимости государства или наносит ущерб его интересам.

Подробнее остановимся на государственной тайне. Установлены три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений:

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

В рассматриваемом предприятии фигурируют сведения второй степени секретности (гриф «совершенно секретно»). Предприятие занимается разработкой программного обеспечения для государственных организаций на основе операционной системы Аврора.

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 см. 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.

Согласно закону РФ "О государственной тайне" от 21.07.1993 N 5485-1, статье 28, средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 1, пункту 4, защита информации осуществляется путем

выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Советом Министров – Правительством Российской Федерации.

Согласно Постановлению Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51, статье 3, пункту 26, защита информации осуществляется путем:

...

2) предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований;

...

5) выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

б) предотвращения перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Выявление возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок по выявлению этих устройств.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

3. АНАЛИЗ ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЙ

3.1. Схема помещения

Необходимо провести анализ защищаемого помещения, чтобы разместить технические средства защиты на объекте. План помещений с меблировкой предприятия представлен на рисунке 3.

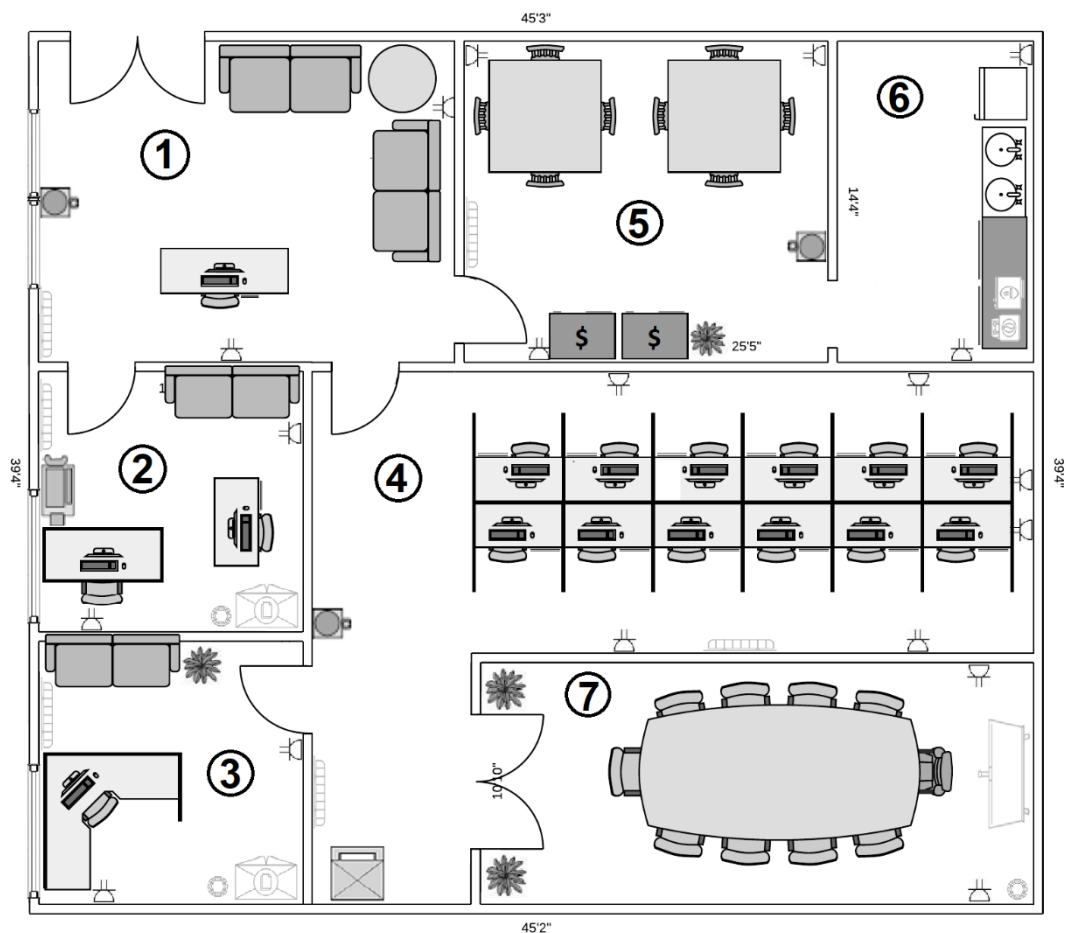
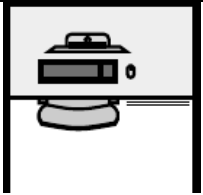
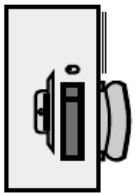
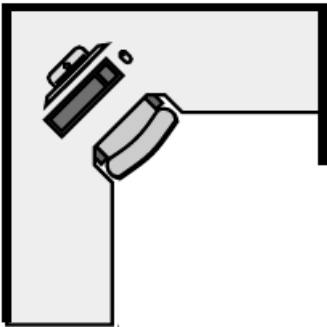
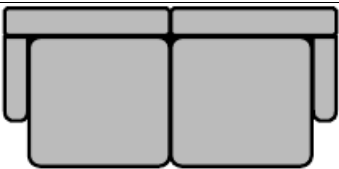
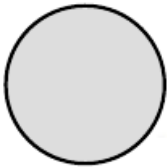
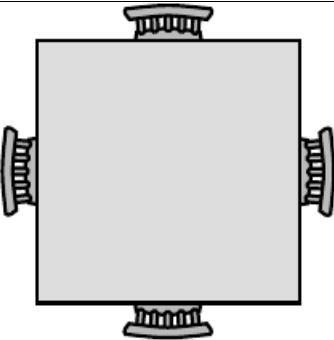

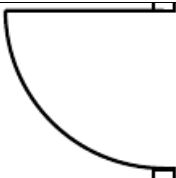







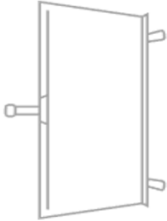





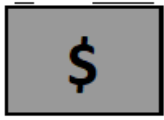
Рисунок 3 – План защищаемого помещения


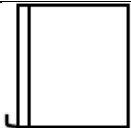
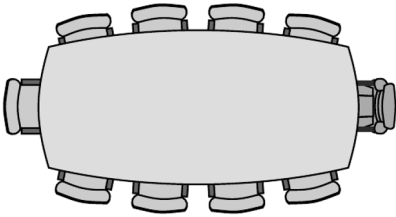
В таблице 2 представлены описание обозначений, изображенных на плане.

Таблица 2 – Описание обозначений.

Обозначение	Описание
	Закрытое с 3 сторон стенкой рабочее место сотрудника (стол с полочками, стул, ПК с монитором, мышью и клавиатурой)
	Рабочее место сотрудника (стол с полочками, стул, ПК с монитором, мышью и клавиатурой)

	<p>Рабочее место генерального директора (стол, стул, ПК с монитором, мышью и клавиатурой)</p>
	<p>Диван</p>
	<p>Журнальный столик</p>
	<p>Обеденный стол</p>
	<p>Оконный проём</p>
	<p>Дверной проём (с указанием направления раскрытия двери)</p>
	<p>Принтер</p>

	Сканер
	Радиатор отопления
	Растение комнатное
	Мусорное ведро для бумаги
	Интерактивная доска с проектором
	Шкаф для документов
	Кулер с водой
	СВЧ-печь
	Кофемашина
	Розетка
	Вендомат

	Раковины
	Холодильник
	Стол для переговоров с 10 стульями

3.2. Описание помещений

На рассматриваемом предприятии в рамках курсовой работы имеются следующие помещения, подлежащие инженерно-технической защите:

1. Ресепшн при входе в офис 4.5м × 6м (27м²)
2. Кабинет бухгалтерии 4м × 4м (16м²)
3. Кабинет директора 4м × 4м (16м²)
4. Общая рабочая зона (45.6м²)
5. Комната отдыха 5.2м × 4.2м (22м²)
6. Кухня 2.6м × 4.2м (11м²)
7. Переговорная комната 7.6м × 4м (30.4м²)

Комната ресепшна включает в себя: одно рабочее место сотрудника (см. таблицу 2), два дивана, журнальный столик, кулер, радиатор, два оконных проёма, входные двери и три дверных проёма в помещения 2, 4, 5, помещение оснащено 2 розетками.

Комната бухгалтерии включает в себя: два рабочих места сотрудника (см. таблицу 2), диван, сканер, шкаф для документов, мусорное ведро, оконный проём, радиатор, дверной проём в помещение 1, помещение оснащено 2 розетками.

Кабинет директора включает в себя: рабочее место генерального директора (см. таблицу 2), диван, растение, шкаф для документов, мусорное ведро, оконный проём, радиатор, дверной проём в помещение 4, помещение оснащено 2 розетками.

Общая рабочая зона включает в себя: 12 закрытых с 3 сторон стенкой рабочих мест сотрудника (см. таблицу 2), принтер, кулер, два радиатора, три дверных проёма в помещения 1, 3, 7, помещение оснащено 6 розетками.

Комната отдыха включает в себя: два обеденных стола (см. таблицу 2), два

вендомата, растение, кулер, оконный проём, дверной проём в помещение 1, помещение оснащено 3 розетками.

Кухня включает в себя: холодильник, 2 раковины, комод, микроволновка, кофеварка, помещение оснащено 2 розетками.

Переговорная комната включает в себя: стол для переговоров (см. таблицу 2), два растения, ведро для мусора, интерактивная доска с проектором, дверной проём в помещение 4, помещение оснащено 2 розетками.

Офис расположен на шестом этаже бизнес-центра, окна помещения выходят в закрытый двор, который находится под постоянным наблюдением и не имеет смежности с пожарными и эвакуационными лестницами, крышами пристроек, выступами на стенах, балконами и другими элементами, которые могли бы использоваться посторонними лицами для доступа в помещение. Остальные 3 стены граничат с другими офисными помещениями и холлом бизнес-центра с установленными противопожарными перекрытиями. Стены здания и внутренние перегородки железобетонные, толщиной не менее 10 см. Все помещения оборудованы аварийным освещением.

3.3. Анализ потенциальных каналов утечек информации

В каждом помещении существуют потенциальные пути для нежелательной утечки информации, связанные с электромагнитными и электрическими утечками информации, то есть с использованием компьютеров и розеток. Декоративные элементы, такие как комнатные растения, могут использоваться для установки закладных устройств, которые могут использоваться для передачи информации через акустический канал.

Существуют также риски утечки информации через оптические каналы, например, из-за незакрытых окон и незащищенных дверей. Важно учитывать также виброакустический канал, который может быть использован для передачи информации из-за наличия твердых поверхностей, таких как стены или батареи отопления.

Материально-вещественный канал в рамках данной работы не рассматривается, поскольку его защита регламентируется внутренней политикой информационной безопасности компании.

4. АНАЛИЗ РЫНКА ТЕХНИЧЕСКИХ СРЕДСТВ

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.
- Все режимные помещения оборудуются аварийным освещением.
- 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. 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 3. Это позволит обеспечить надежную защиту от несанкционированного доступа и утечки такой конфиденциальной информации.

Таблица 3 – Активная и пассивная защита информации

Каналы	Источники	Пассивная защита	Активная защита
Электрический Электромагнитный	Компьютеры, сервера, бытовая техника, розетки	Защитные экраны и фильтры для сетей электропитания	Устройства электромагнитного зашумления
Акустический Электроакустический	Стены, двери, окна, электрические сигналы	Защитные экраны и фильтры для сетей электропитания, изоляция особо	Устройства акустического зашумления

		важных помещений	
Виброакустический	Стекла, стены и иные твердые поверхности	Изоляция переговорной, использование антивибрационных материалов и звукозащитных экранов	Устройства вибрационного зашумления
Визуально- оптический	Окна и стеклянные поверхности, двери	Защитные экраны и фильтры для сетей электропитания	Жалюзи, бликующие устройства

4.2. Устройства для перекрытия акустического и виброакустического каналов утечки информации

Пассивные меры безопасности включают в себя создание тамбурной зоны перед переговорной комнатой и установку усиленных дверей. Для обеспечения звукоизоляции переговорной комнаты и кабинета руководителя используются специальные материалы для звукоизоляции стен.

Активные меры безопасности представляют собой систему виброакустической маскировки. Для обеспечения безопасности помещения, в котором обрабатывается информация, отнесенная к категории «совершенно секретно», рассматриваются технические средства активной защиты информации для объектов информатизации, имеющих категорию не ниже 1Б (см. приложение 1).

В таблице 4 приведен сравнительный анализ решений, предлагаемых на современном рынке, и удовлетворяющих указанным требованиям для защиты объекта от утечек по виброакустическому каналу.

Таблица 4 – Средства активной защиты от утечек по виброакустическому каналу

Модель	Производитель	Описание/особенности	Цена
ЛГШ-304	Лаборатория ППШ	Предназначено для защиты акустической речевой информации, путем формирования акустических маскирующих шумовых помех. Диапазон рабочих частот - 175- 11200 Гц. Интервал давления - 28 дБ.	25 220 руб.
ЛВП-2а (В	Лаборатория	Акустический излучатель предназначен для	5 200 руб.

Модель	Производитель	Описание/особенности	Цена
составе ЛГШ-404)	ППШ	возбуждения маскирующих акустических помех в различных закрытых пространствах (таких, как междверные проемы, воздуховоды и т.д.)	(35 100 руб.
Виброзкран «ЛИСТ-1»	Лаборатория ППШ	Виброзкран - это специальное устройство или материал, созданное для защиты от вибраций или для снижения передачи вибраций через поверхности или конструкции. Оно используется для уменьшения уровня шума, подавления вибраций или предотвращения передачи вибраций из одной среды в другую.	16 380 – 45 240 руб в зависимости от размера
Бубен-Ультра	ИНФОСЕКЬЮР	Прибор предназначен для полного и (или) частичного подавления полезного звукового сигнала при попытке записи на мобильные или стационарные записывающие устройства, радио и проводные специальные технические средства, выносные микрофоны посредством генерации двух типов помех. А именно: <ul style="list-style-type: none"> - помехи в ультразвуковом диапазоне, воздействующей непосредственно на мембрану микрофона; - акустический псевдослучайный сигнал типа «речевой хор», для затруднения ее выделения из полезного сигнала. 	48 000 руб.
Соната АВ-4Б	НПО Анна	“Соната-АВ” модель 4Б построена по принципу "единый источник электропитания + генераторы-электроакустические преобразователи (излучатели)" Благодаря этому построению проявляется высокая стойкость защиты информации. Имеет ряд преимуществ перед "классическим" подходом - "центральный генератор + электроакустические преобразователи": <ol style="list-style-type: none"> 1. Есть возможность подключения к одному питающему шлейфу. Это делает легче процесс проектирования и монтажа 2. Индивидуальная регулировка интегрального уровня и корректировка спектра каждого генератора улучшает действие системы Улучшенная аппаратная настройка	44 200 руб.

Модель	Производитель	Описание/особенности	Цена
		<p>элементов модели 4Б позволяет связывать источник электропитания с другими для обмена информацией. Это дает возможность:</p> <ul style="list-style-type: none"> • Создать систему автоматического контроля всех элементов • Снизить время на конфигурирование и тестирование системы • Изменить настройки генераторов и построить гибкую систему виброакустической защиты • Уменьшить затраты благодаря использованию единой линии связи и электропитания 	
Буран	ИНФОСЕКБЮР	<p>Средство активной акустической и вибрационной защиты акустической речевой информации. Частота 100 – 11 200 Гц. Интервал давления - 30 дБ. + преобразователь (2000 руб.)</p>	67 500 руб.
Бекар	ЗАО “СНТК”	<p>Система активной акустической и вибрационной защиты речевой информации. Частота 175 - 11200 Гц. Интервал давления - 20 дБ. Идет в системе с блоком питания, блоком контроля целостности (18800 руб.) + программатором (цена по запросу).</p>	4 600 руб.

В результате сравнения, в качестве применяемого решения была выбрана аппаратура защиты от акустической разведки «Соната АВ» модель 4Б. Данный выбор обоснован оптимальным соотношением цены и выдаваемых характеристик системы. Система предоставляет возможность построения системы автоматического контроля всех элементов при минимально возможной стоимости оборудования и монтажа, а также возможность изменения настроек генераторов-излучателей "на лету" и, как следствие – возможность построения адаптивной ("многопрофильной") системы виброакустической защиты, обеспечивающей выполнение требований по защищенности при различных вариантах использования помещения. Кроме того, усовершенствованная настройка аппаратных элементов модели 4Б позволяет интегрировать источник электропитания с другими для обмена информацией.

4.3. Защита от утечек информации по оптическим каналам

Для прекращения функционирования оптического канала утечки информации необходимо установить на окно жалюзи, шторы или тонирующие пленки. Также решением, которое может обеспечить дополнительную защиту от утечек по виброакустическому каналу, может являться виброзкран «Лист-1», рассмотренный в пункте 4.2. Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

4.4. Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации

Для пассивной защиты объекта используются сетевые фильтры для цепей электропитания, экранирование металлическим материалом. В качестве средств для активной защиты используется генератор пространственного зашумления для создания в сети белого шума, который скрывает колебания, порождаемые работающей электрической техникой или воздействием звуковой волны. В таблице 5 приведен сравнительный анализ решений, предлагаемых на современном рынке, и удовлетворяющих требованиям класса защиты для предотвращения утечек по электрическим каналам.

Таблица 5 – Средства активной защиты от утечек по электрическим каналам

Модель	Производитель	Описание/особенности	Цена
ЛГШ 503	Лаборатория ППШ	Оснащен визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Оснащен счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы в режиме формирования маскирующих помех. Прибор имеет возможность подключения проводного дистанционного управления и контроля, в качестве которого может использоваться программно-аппаратный комплекс «Паутина».	44 200 руб.
Соната- РЗ.1	НПО Анна	Обеспечивает защиту информации от утечки за счет побочных электромагнитных излучений и наводок путем излучения в	39 000 руб.

		окружающее пространство электромагнитного поля шума, а также наводок на линии сети электропитания и заземления путем индуцирования в них маскирующих шумовых напряжений.	
ЛГШ-513	Лаборатория ППШ	Изделие «ЛГШ-513» оснащено визуальной системой индикации нормального режима работы и визуально-звуковой системой индикации аварийного режима (отказа). Изделие «ЛГШ-513» оснащено счетчиком учета времени наработки, учитывающим и отображающим в часах и минутах суммарное время работы Изделия в режиме формирования маскирующих помех.	33 120 руб
Генератор шума Пульсар	Эшелон технологии	Имеет защиту регулятора уровня выходного шумового сигнала от нелегального доступа (и сигнализирует об этом). Индикаторы нормального режима работы (диод) и аварийного режима (свет и звук).	24 525 руб.

В результате сравнения, в качестве применяемого решения было выбрано устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Соната-РЗ.1». ПЭМИН «Соната-РЗ.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. Преимуществом данного решения можно назвать возможность комбинирования нескольких устройств с целью потенциального повышения класса защищенности. Также, что немаловажно, данное устройство имеет сертификат ФСТЭК и приемлемую стоимость. Ещё один фактор, говорящий в пользу данного устройства – выбор средства защиты от акустических утечек от этого же производителя, что дает нам возможность встроить его в систему «Соната АВ4Б».

5. ОПИСАНИЕ РАССТАНОВКИ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

На основе информации, приведенной в главе 4, выбранные технические средства защиты информации включают в себя:

- Усиленные двери (от 4 мм), обшитые металлом (от 2 мм) со звукоизолирующей прокладкой на металлическом каркасе – 4 шт., в кабинет генерального директора, переговорную и кабинет бухгалтерии.
- Аппаратура защиты от акустической разведки «Соната АВ» модель 4Б;
- Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН «Соната-РЗ.1».
- Жалюзи на четыре окна.

Оценим количество компонентов и расстановку выбранных технических средств.

Соната АВ-4Б содержит генераторы-акустоизлучатели СА-4Б и генераторы-вибровозбудители ЛГШ-503.

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;
- Один на окно (при установке на оконный переплет);
- Один на дверь (при установке на верхнюю перекладину дверной коробки);
- Трубы систем ЦО – 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 надпотолочного пространства или других пустот.

Итоговое количество требуемых технических средств для рассматриваемого объекта защиты и их расчетная стоимость представлены в таблице 6.

Меры защиты	Цена, руб.	Количество, шт.	Итоговая стоимость
Блок электропитания и управления «СонатаИП4.3»	21 600	1	21600
Генератор-акустоизлучатель «Соната СА-4Б»	3 540	9	31860
Генератор-вибровозбудитель «Соната СВ-4Б»	7 440	14	104160
Размыкатель телефонной линии «Соната ВК4.1»	6 000	2	12000
Размыкатель слаботочной линии «Соната ВК4.2»	6 000	1	6000
Размыкатель линии «Ethernet» «Соната ВК4.3»	6 000	2	12000
Пульт управления «Соната-ДУ 4.3»	7 680	1	7680
Соната-РЗ.1	31 120	6	186720
Рулонные шторы Blackout	4 900	6	29400
Усиленные звукоизолирующие двери «Ultimatum Next ПВХ»	86 886	3	260658
Итого			672078

План помещения с установленными средствами технической защиты представлен на рисунке 4.






Рисунок 4 – План объекта с техническими СЗИ

Условные обозначения описаны в таблице 6.

Таблица 6 – Условные обозначения к рисунку 4.

Обозначение	Устройство	Количество, шт.
	Усиленные звукоизолирующие двери «Ultimatum Next PBX»	4
	Рулонные шторы BlackOut	6
	Генератор-вибровозбудитель «Соната СВ-4Б» (окна, двери, батареи)	14
	Генератор-акустоизлучатель СА-4Б (запотолочное пространство, вентиляция)	9

	Размыкатель линии «Ethernet» «Соната-ВК4.3»	2
	Размыкатель слаботочной линии «Соната-ВК4.2»	1
	Размыкатель телефонной линии «Соната-ВК4.1»	2
	Блок электропитания и управления «Соната-ИП4.3»	1
	Соната-РЗ.1	6

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы был произведен теоретический обзор технических каналов утечки информации, анализ защищаемого предприятия, включая описание структуры предприятия, составление подробного плана помещений, описание информационных каналов.

Для выбора необходимых средств технической защиты информации был проведен анализ рынка существующих решений для противодействия рассматриваемым каналам утечки и выбраны наиболее подходящие для объекта решения. На основе выбранных средств был разработан план установки и произведен расчет финансовых затрат, которые указаны в разделе 5 данной работы.

В результате была предложена защита от утечек информации по акустическому, виброакустическому, оптическому, электрическому, акустоэлектрическому, электромагнитному, оптико-электронному каналам. Расчетная стоимость требуемых технических средств составит ориентировочно 672 078 руб. без учёта затрат на установку и соединение элементов системы, что можно считать достаточно оправданной суммой для объекта, который хранит и обрабатывает информацию, составляющую государственную тайну с грифом уровня «совершенно секретно».

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие/Н. С. Кармановский, О. В. Михайличенко, С. В. Савков. — Санкт-Петербург: НИУ ИТМО, 2013. — 148 с. — Текст : электронный // Лань: электроннобиблиотечная система. — URL: <https://e.lanbook.com/book/43579> — Режим доступа: для авториз. пользователей.
2. Титов А. А. Инженерно-техническая защита информации: учебное пособие. Томск: ТУСУР, 2010. — 195 с.
3. Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 — URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=454091>
4. ПОЛОЖЕНИЕ «О ГОСУДАРСТВЕННОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ ИНОСТРАННЫХ ТЕХНИЧЕСКИХ РАЗВЕДОК И ОТ ЕЕ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ» (утв. Постановлением Совета Министров – Правительства РФ от 15 сентября 1993 г. № 912-51)
5. РУКОВОДСТВО АДМИНИСТРАТОРА Операционная система Аврора релиз 4.0.2 update 5 — URL: http://docs.auroraos.ru/files/4.0.2_update_5/Rukovodstvo_administratora_OS_Avrora_4.0.2_update_5.pdf

ПРИЛОЖЕНИЕ 1

Классы защищенности автоматизированных систем

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)	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
Вторая группа (АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности)	2А	Информация, составляющая гостайну
	2Б	Служебная тайна или персональные данные
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)	3А	Информация, составляющая гостайну
	3Б	Служебная тайна или персональные данные