

**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:

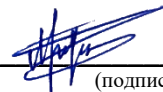
«Инженерно-технические средства защиты информации»

На тему:

«Проектирование инженерно-технической системы защиты информации на предприятии»

Выполнил:

Чернякова Л. В., студент группы N34511



(подпись)

Проверил:

Попов И. Ю., к.т.н., доцент ФБИТ

(отметка о выполнении)

(подпись)

(подпись)

Санкт-Петербург

2023 г.

Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО
ЗАДАНИЕ НА КУРСОВУЮ РАБОТУ

Студент	Чернякова Лилия Владиславовна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34511
Направление (специальность)	10.03.01. - Технологии защиты информации
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
Задание	Разработать инженерно-техническую систему защиты информации на предприятии

Краткие методические указания

Рекомендуемая литература

Руководитель	Попов Илья Юрьевич
	(Подпись, дата)
Студент	Чернякова Лилия Владиславовна
	(Подпись, дата)

Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО
ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Студент Чернякова Лилия Владиславовна
(Фамилия И.О.)

Факультет Безопасности Информационных Технологий

Группа N34511

Направление (специальность) 10.03.01. - Технологии защиты информации


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

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	Создание плана КР	08.12.2023	08.12.2023	
2	Анализ литературы	08.12.2023	08.12.2023	
3	Составление основного текста КР	13.12.2023	13.12.2023	
4	Создание презентации	16.12.2023	16.12.2023	
5	Презентация КР перед аудиторией	19.12.2023	19.12.2023	

Руководитель Попов Илья Юрьевич
(Подпись, дата)

Студент Чернякова Лилия Владиславовна
(Подпись, дата) 

Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО
АННОТАЦИЯ НА КУРСОВУЮ РАБОТУ

Студент	Чернякова Лилия Владиславовна
	(Фамилия И.О.)
Факультет	Безопасности Информационных Технологий
Группа	N34511
Направление (специальность)	10.03.01. - Технологии защиты информации
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 данной работы – разработать систему инженерно-технической защиты предприятия

2. Характер работы


- ☐ Расчет ☐ Конструирование
☐ Моделирование ☒ Другое
(Проектирование)

3. Содержание работы

1. Информация о предприятии;
2. Необходимость внедрения системы защиты;
3. Исследование помещения;
4. Проектирование системы защиты.

4. Выводы

Исследованы организационная структура, план помещений организации, проанализирован рынок средств защиты, сформирована система защиты организации, спроектирован план помещения с учетом средств защиты.

Руководитель	Попов Илья Юрьевич	(Подпись, дата)
Студент	Чернякова Лилия Владиславовна	(Подпись, дата) 

СОДЕРЖАНИЕ

Введение.....	6
1 Информация о предприятии	8
2 Необходимость внедрения средств защиты.....	10
3 Исследование помещения	13
4 Проектирование системы инженерно-технической защиты	16
4.1 Каналы утечки информации	16
4.2 Выбор средств защиты.....	20
4.2.1 Устройства для перекрытия акустического и виброакустического канала утечки информации	20
4.2.2 Устройства для перекрытия электрического, акустоэлектрического и электромагнитного каналов утечки информации.....	23
4.2.3 Устройства для перекрытия оптического канала защиты информации.....	26
4.2.4 Устройства для перекрытия канала ПЭМИН.....	26
4.3 Подсчет стоимости выбранных средств.....	26
4.4 Расстановка средств защиты	28
Заключение.....	31
Список использованной литературы	32

ВВЕДЕНИЕ

Компьютеризация и развитие интернет-технологий ускорили и оптимизировали бизнес-процессы. Однако современные технические средства используют также в целях промышленного шпионажа и недобросовестной конкуренции. Наличие инженерно-технической защиты информации стало необходимым требованием для безопасной работы многих предприятий. Комплексная система защиты приобрела ведущую роль в предотвращении утечек важных технических данных, поэтому компании выделяют значительную часть средств на ее постоянное совершенствование.

Инженерно-техническая защита – это совокупность технических средств и мероприятий, нацеленных на предотвращение утечек, разглашения информации, и несанкционированного доступа в сетевые ресурсы организации. Актуальность защиты информации обуславливается наличием большого числа потенциальных конкурентов, а также недоброжелателей, которые могут навредить компании. Попадая в чужие руки, ценная информация становится товаром. Ее искажение, порча или плагиат могут навредить репутации и финансам компании, причинить вред и способствовать выходу с рынка.

Защита конфиденциальности информации для многих предприятий стала первостепенной задачей, от качества решения которой зависит конкурентоспособность и возможность успешно выводить на рынок технологические новинки. Используя современные инженерно-технические средства можно обеспечить защиту сведений, относящихся к категории секретных или конфиденциальных.

Чем вызвана необходимость в инженерно-технической защите информации?

- Активным развитием средств добычи информации, которые, в том числе, позволяют получать несанкционированный доступ к данным на расстоянии.
- Оснащением жилых, производственных и служебных помещений радио- и электроаппаратурой, неполадки в работе которых нередко способствуют утечке конфиденциальной информации.
- Достижениями микроэлектроники (аудиожучки, миникамеры), которые стали доступны обычным пользователям и могут быть использованы для нелегальной добычи информации из скрытых источников.

Использование надежных технических средств защиты информации становится единственным способом предотвратить утечку данных. Именно поэтому будет полезным узнать, какие методы защиты информации являются наиболее надежными и целесообразными в применении.

Цель курсовой работы: повышение безопасности предприятия за счет внедрения системы инженерно-технической защиты информации.

Задачи курсовой работы:

1. Анализ организационной структуры предприятия;
2. Обоснование необходимости разработки инженерно-технической системы защиты информации;
3. Анализ плана помещения предприятия;
4. Анализ рынка средств инженерно-технической защиты информации;
5. Проектирование инженерно-технической системы защиты предприятия.

1 ИНФОРМАЦИЯ О ПРЕДПРИЯТИИ

Полное наименование организации: ОАО «Банк поддержки Вооруженных сил и оборонной промышленности».

Банк обслуживает финансовые операции, связанные с экспортом оружия, проведением военных кампаний. Помимо этого, банк предоставляет кредиты для научных исследований и разработок в области военных технологий. Также банк начисляет зарплату и пенсии военнослужащим.

Департамент организации:

- операционно-кассовый отдел;
- кредитный отдел;
- юридический отдел;
- бухгалтерия и отдел кадров;
- отдел автоматической обработки данных;
- переговорная;
- кабинет директора.

На рисунке 1 представлена организационная структура департамента.



Рисунок 1 – Структура департамента

Информация ограниченного доступа организации:

- государственная тайна;
- коммерческая тайна;
- персональные данные;
- служебная информация;
- банковская тайна.

На рисунке 2 представлена схема перемещения информационных потоков между отделами организации. Зеленым цветом обозначены внешние открытые потоки, красным – внутренние закрытые.

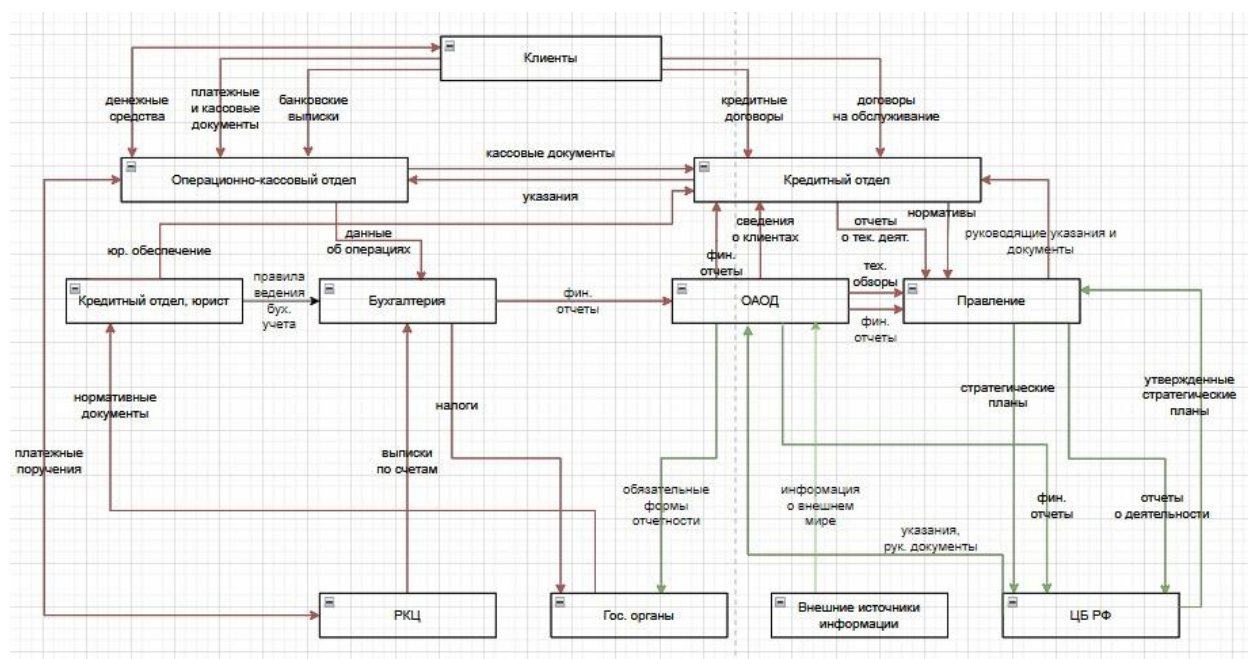


Рисунок 2 – Схема перемещения информационных потоков организации

2 НЕОБХОДИМОСТЬ ВНЕДРЕНИЯ СРЕДСТВ ЗАЩИТЫ

Внедрение системы инженерно-технической защиты информации должно обосновываться не только масштабами обслуживаемых средств и операций, но и повышенной чувствительностью информации, циркулирующей в организации.

Согласно ст. 5 Закона РФ от 21.07.1993 N 5485-1 (ред. от 04.08.2023) "О государственной тайне", к перечню сведений, составляющих государственную тайну, относятся:

1) сведения в военной области:

о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом "Об обороне", об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники:

о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) сведения в области внешней политики и экономики:

о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

Согласно Постановлению Правительства РФ от 04.09.1995 N 870 (ред. от 30.10.2021) "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности":

4. К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб интересам государственного органа или отрасли экономики Российской Федерации в одной или нескольких из указанных областей.

Существует три категории выделенных помещений (то есть помещений, специально предназначенных для проведения совещаний по вопросам, содержащим сведения, составляющие государственную тайну Российской Федерации):

- 1 категория: разрешается обсуждать информацию с грифом до «особой важности» включительно;*
- 2 категория: с грифом до «совершенно секретно» включительно;*
- 3 категория: с грифом до «секретно» включительно.*

Таким образом, информация, циркулирующая внутри ОАО «Банк поддержки Вооруженных сил и оборонной промышленности» относится к сведениям с грифом «совершенно секретно», а помещение можно отнести ко 2 категории. Внедрение системы инженерно-технической защиты информации обосновано.

3 ИССЛЕДОВАНИЕ ПОМЕЩЕНИЯ

Для проектирования инженерно-технической системы защиты предприятия исследуем план помещения (рисунок 3).

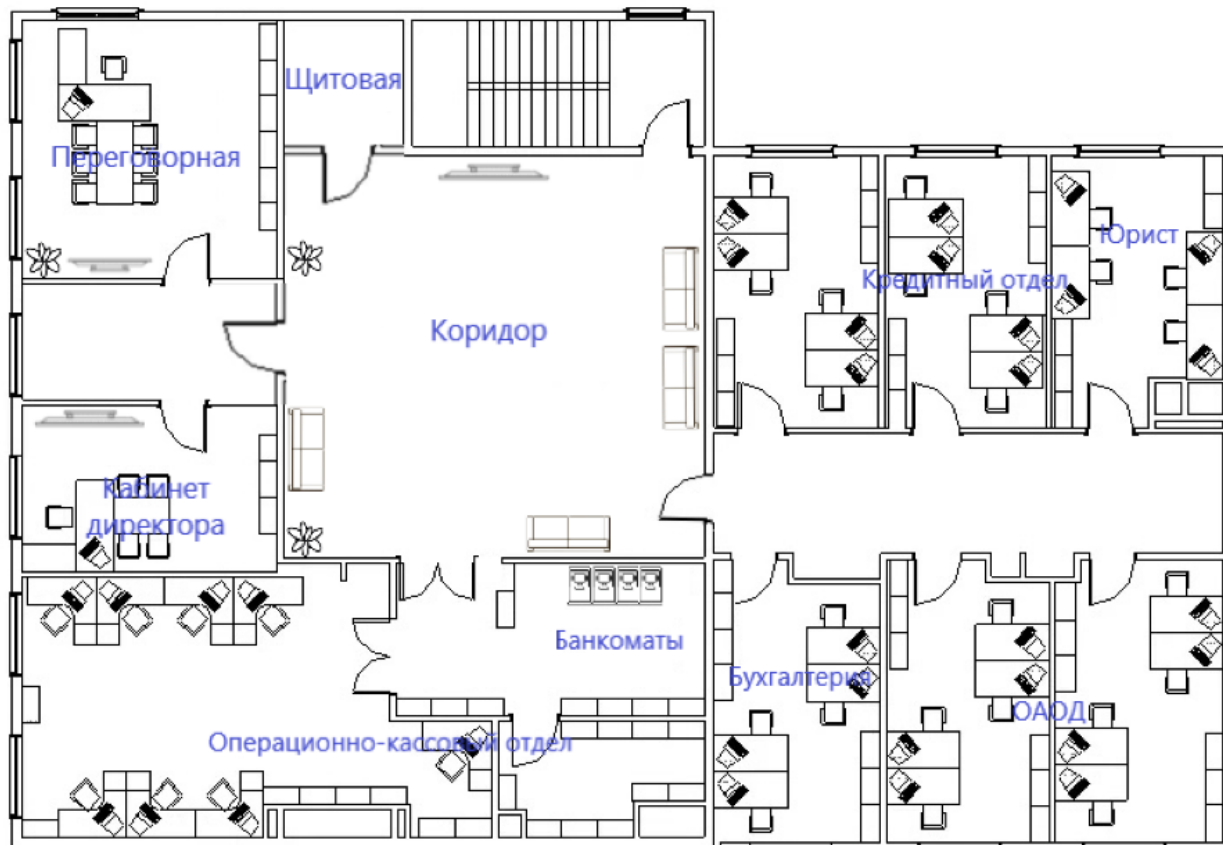



Рисунок 3 – План помещения

Условные обозначения элементов, изображенных на плане, представлены в таблице 1.

Таблица 1 – Условные обозначения элементов помещения

Обозначение	Элемент
	Стол
	Стул
	Диван
	Стеллаж (шкаф)
	ПК
	Телевизор
	Цветок

Окончание таблицы 1

Обозначение	Элемент
	Банкомат

Площадь комнат:

- переговорная (20 кв. м.);
- кабинет директора (15 кв. м.);
- операционно-кассовый отдел (50 кв. м.);
- банкоматы (15 кв. м.);
- кредитный отдел (30 кв. м.);
- юрист (15 кв. м.);
- бухгалтерия (15 кв. м.);
- ОАОД (15 кв. м.);
- коридор (70 кв. м.);
- щитовая (7 кв. м.).

Подробное описание вышеперечисленных помещений представлено в таблице 2.

Таблица 2 – Описание помещений

Комната	Предназначение	Электроника	Прочее
Переговорная	Проведение переговоров	1 ПК, 1 телевизор без выхода в сеть, 2 розетки	Мебель, 3 окна и 3 батареи
Кабинет директора	Управление	1 ПК, 1 телевизор без выхода в сеть, 2 розетки	Мебель, 1 окно и 1 батарея
Операционно-кассовый отдел	Проведение банковских операций	9 ПК, 9 розеток	Мебель, 2 окна и 2 батареи
Банкоматы	Проведение банковских операций	4 банкомата, 4 розетки	Отсутствует
Кредитный отдел	Проведение кредитных операций	8 ПК, 8 розеток	Мебель, 2 окна и 2 батареи
Юрист	Юридическое обеспечение	4 ПК, 4 розетки	Мебель, 1 окно и 1 батарея

Окончание таблицы 2

Комната	Предназначение	Электроника	Прочее
Бухгалтерия	Бухгалтерское обеспечение	4 ПК, 4 розетки	Мебель, 1 окно и 1 батарея
ОАОД	Автоматизированная обработка документов	4 ПК, 4 розетки	Мебель, 1 окно и 1 батарея
Коридор	Место ожидания	1 телевизор, 1 розетка	Мебель

Офис банка расположен на втором этаже, окна ведут в закрытый контролируемый двор. Окна не соседствуют с пожарными и эвакуационными лестницами, балконами и прочими элементами, с которых в помещения могут проникнуть. Помещение расположено в угловой части здания, которая редко используется инженерами или муниципальными сотрудниками при выполнении каких-либо видов работ. Все двери с доводчиками.

4 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ

4.1 Каналы утечки информации

Утечка – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена. Утечка информации может осуществляться по различным каналам. Каналом утечки информации называют канал коммуникации, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

Существует три формы утечки информации:

- разглашение информации;
- несанкционированный доступ к информации;
- 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.

Структура канала утечки представлена на рисунке 4.



Рисунок 4 – Структура канала утечки

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.

Далее полученная информация преобразуется 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. Приемник после этого снимает информацию с носителя, обрабатывает полученный сигнал (усиление) и преобразует информацию в форму сигнала, доступную получателю (человеку или техническому устройству).

По физической природе носителя и виду канала связи ТКУИ делятся на:

- оптические;
- радиоэлектронные;
- электрические;
- электромагнитные;
- индукционные;
- акустические;
- акустоэлектрические;
- виброакустические;
- материально-вещественные.

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.

Индукционный ТКУИ связан с бесконтактным съемом информации с кабельных линий связи. Возможность такого съема информации возникает за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это поле перехватывается специальным индукционным датчиком, далее усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что бесконтактные закладные устройства обнаружить труднее всего, так как они не изменяют характеристик канала связи. Защита осуществляется посредством использования специальных программных и аппаратных средств, позволяющих выявить закладки.

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 технические 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.

Помимо вышеперечисленного, также выделяют оптико-электронные ТКУИ, связанные с перехватом акустических сигналов путём лазерного зондирования оконных стекол.

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

Внутри помещений существует потенциальная угроза утечки информации. Декоративные элементы предоставляют возможность скрыть устройства для незаметного слежения. Розетки, присутствующие в каждом помещении, могут использоваться для электрической и электромагнитной передачи данных. Утечка информации также может

происходить через вибрационные, оптические, акустические, виброакустические и акустоэлектрические каналы.

Для обеспечения безопасности ОАО «Банк поддержки Вооруженных сил и оборонной промышленности» необходимо оснастить помещения элементами пассивной и активной защиты.

К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации.

4.2 Выбор средств защиты

4.2.1 Устройства для перекрытия акустического и виброакустического канала утечки информации

Пассивная защита акустического и виброакустического каналов утечки информации представляет собой:

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

Активная защита акустического и виброакустического каналов утечки информации реализуется с помощью систем акустических и виброакустических помех. Сравнение систем приведено в таблице 3.

Таблица 3 – Сравнение систем

Наименование системы	Диапазон частот	Характеристики	Сертификат	Стоимость
«Буран»	100 – 11 200 Гц	<ul style="list-style-type: none"> • высокое качество шумовой помехи; • коррекция спектра помехового сигнала; • мониторинг уровня нагрузки каналов; • контроль аварийных ситуаций и визуально-звуковую сигнализацию при отключении одного и более излучателей, коротком замыкании в канале помех, неисправности собственной системы вибрационного зашумления; • защиту от несанкционированного изменения настроек. 	ФСТЭК	60 000 р.

Окончание таблицы 3

Наименование системы	Диапазон частот	Характеристики	Сертификат	Стоимость
«Соната АВ-4Б»	175 – 11200 Гц	<ul style="list-style-type: none"> • есть возможность подключения к одному питающему шлейфу; • корректировка спектра каждого генератора; • автоматический контроль элементов; • гибкая система защиты; • легкая конфигурация. 	ФСТЭК	45 000 р.
«Камертон 5»	90 – 11200 Гц	<ul style="list-style-type: none"> • в систему входит вспомогательное оборудование; • проста в эксплуатации; • сигнализирует о сбоях; • надежное зашумление; • подходит для помещений разной планировки и площади; • гибкая настройка. 	ФСТЭК	46 000 р.

По совокупности характеристик в качестве системы защиты акустических и виброакустических каналов выбрана система «Соната АВ-4Б».

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

Пассивная защита электрического, акустоэлектрического и электромагнитного каналов утечки информации представляет собой фильтры для сетей электропитания.

Активная защита электрического, акустоэлектрического и электромагнитного каналов утечки информации реализуется с помощью сетевых генераторов шума. Сравнение приведено в таблице 5.

Таблица 4 – Сравнение систем

Наименование системы	Диапазон частот	Характеристики	Сертификат	Стоимость
ЛГШ-221	0,01 – 400 МГц	<ul style="list-style-type: none"> • визуальная система индикации нормального режима работы; • визуально-звуковая система индикации аварийного режима (отказа); • счетчик учета времени работы в режиме формирования маскирующих помех (ЖК-дисплей); • защита органов регулировки уровня выходного шумового сигнала; • проводное дистанционное управление и контроль (через программно-аппаратный комплекс «Паутина»). 	ФСТЭК	36 400 р.

Продолжение таблицы 4

Наименование системы	Диапазон частот	Характеристики	Сертификат	Стоимость
SEL SP-44	0,01 – 300 МГц	<ul style="list-style-type: none"> • основные узлы прибора – формирователи шума, регуляторы уровня и выходные усилители представляют собой полностью цифровые устройства. • наличие независимых регуляторов уровня для низкочастотного и высокочастотного диапазонов. • устройство имеет высший класс устойчивости к импульсным помехам и допускает длительную работу в условиях эквивалентного короткого замыкания. • во время работы прибор постоянно осуществляет самотестирование • управление включением помехи может осуществляться с панели управления или дистанционно. 	ФСТЭК	24 000 р.

Окончание таблицы 4

Наименование системы	Диапазон частот	Характеристики	Сертификат	Стоимость
«Соната-РЗ»	0,01 – 200 МГц	<ul style="list-style-type: none"> • исполнение в виде моноблока со встроенной в него антенной; • наличие регулятора уровня излучаемого электромагнитного шума; • наличие специальной проверки; • возможность увеличения уровня излучаемого электромагнитного шума в диапазоне 0.01-100 МГц за счет использования дополнительной антенны (поставляется опционально); • наличие встроенной системы контроля уровня излучения с визуальной и звуковой сигнализацией; • возможность проводного дистанционного управления. 	ФСТЭК	97 000 р.

По совокупности характеристик в качестве средства защиты электрического, акустоэлектрического и электромагнитного каналов утечки информации выбран генератор шума «Соната-РЗ».

4.2.3 Устройства для перекрытия оптического канала защиты информации

Для защиты от утечки информации по оптическому каналу следует снизить освещенность защищаемого объекта и его отражательные свойства, использовать различные пространственные ограждения (ширмы, экраны, шторы, ставни, темные стекла), применять специальную маскировку и средства сокрытия защищаемых объектов (аэрозольные завесы, сетки, краски, укрытия).

Наиболее простой вариант защиты – шторы.

4.2.4 Устройства для перекрытия канала ПЭМИН

Для защиты от утечки информации за счет побочных электромагнитных излучений и наводок будем использовать средство «Соната-РЗ.1», так как оно будет легко совместимо с другими средствами.

4.3 Подсчет стоимости выбранных средств

Таким образом, для защиты предприятия выбраны следующие средства активной и пассивной защиты:

- усиленные двери (в переговорную, кабинет директора, кабинет юриста);
- система акустических и виброакустических помех «Соната АВ-4Б»;
- генератор шума «Соната-РЗ»;
- средство активной защиты информации от утечки за счёт ПЭМИН «Соната-РЗ.1»;
- жалюзи на все окна.

Перейдём к оценке количества компонентов и расстановке выбранных технических средств. Согласно руководству по эксплуатации «Система виброакустической и акустической защиты «Соната-АВ». Руководство по эксплуатации» для предварительной оценки необходимого количества излучателей необходимо исходить 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 м. кв. перекрытия;

- один на окно (при установке на оконный переплет);
- один на дверь (при установке на верхнюю перекладину дверной коробки);
- трубы систем водо- (тепло- и газо-) снабжения – один на каждую вертикаль (отдельную трубу) вида коммуникаций.

Ориентировочное количество пьезоизлучателей может быть определено из расчета: один ПИ-45 на каждое стекло.

Необходимое количество аудиоизлучателей можно предварительно оценить из следующих норм:

- один на каждый вентиляционный канал или дверной тамбур;
- один на каждые 8...12 м. куб. надпотолочного пространства или др. пустот.

Основным правилом, которым следует руководствоваться при выборе мест установки излучателей в каждом конкретном помещении, является обеспечение максимального уровня вибрационного и акустического шума в предполагаемом канале утечки информации при обеспечении приемлемого уровня мешающего акустического шума в защищаемом помещении. Контроль вибрационного и акустического зашумления помещений рекомендуется производить в соответствии с методиками и рекомендациями ФСТЭК (Гостехкомиссии) РФ.

В таблице 5 приведен расчет затрат на все средства защиты.

Таблица 5 – Расчет затрат

Наименование	Цена, руб.	Количество, шт.	Стоимость, р.
Усиленная дверь ДС 9	63 000	3	189 000
Жалюзи	5 000	14	70 000
Генератор шума «Соната-РЗ»	97 000	1	97 000
Средство активной защиты информации от утечки за счёт ПЭМИН «Соната-РЗ.1»	33 000	1	33 000
Система акустических и виброакустических помех «Соната АВ-4Б»	45 000	1	45 000
Блок электронного управления «Соната-ИП4.3»	21 000	1	21 000
Генератор вибровозбудитель «Соната-САВ-4Б»	7 400	38 + 17 + 30	629 000

Окончание таблицы 5

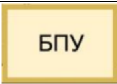
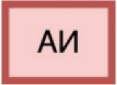

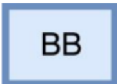

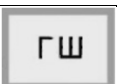
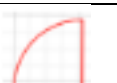
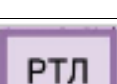
Наименование	Цена, руб.	Количество, шт.	Стоимость, р.
Генератор акустоизлучатель «Соната-СА-4Б1»	3 500	16	56 000
Итого			1 140 000

4.4 Расстановка средств защиты

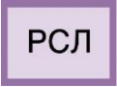
Жалюзи установлены на каждом окне. Элементы комплексной системы Соната «АВ» модель 4Б расположены так же, как и на рисунке 4. «Соната-РЗ» подключена напрямую к «Соната-ИП4.3» и на схеме отдельно не обозначена. «Соната-РЗ.1» подключена к системе электроснабжения согласно рекомендациям производителя, на схеме отдельно не обозначена.

Условные обозначение элементов приведены в таблице 6.

Таблица 6 – Условные обозначения элементов защиты

Элемент	Условное обозначение
«Соната-ИП4.3» блок электронного управления	
«Соната-СВ-4Б1» генератор-акустоизлучатель	
«Соната-СВ-4Б» генератор-вибровозбудитель (двери, окна, батареи)	
«Соната-СВ-4Б» генератор-вибровозбудитель (стены)	
«Соната-СВ-4Б» генератор-вибровозбудитель (пол, потолок)	
«Соната-РЗ.1» генератор шума	
Дверь звукоизолирующая	
Размыкатель телефонной линии	

Окончание таблицы 6

Элемент	Условное обозначение
Размыкатель слаботочной линии	
Размыкатель линии Интернета	

Размещение элементов представлено на рисунке 5.

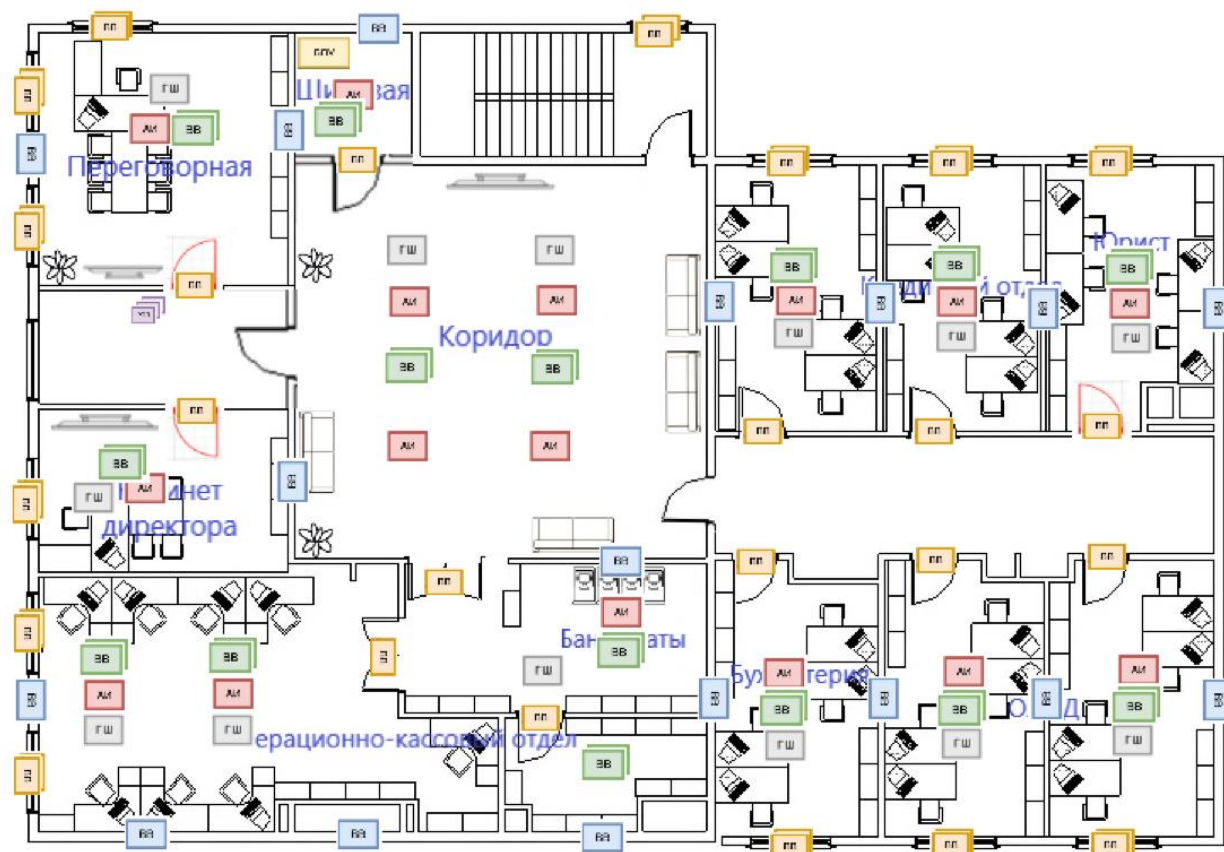


Рисунок 5 – Размещение средств инженерно-технической защиты

ЗАКЛЮЧЕНИЕ

Исследованы организационная структура, план помещений организации ОАО «Банк поддержки Вооруженных сил и оборонной промышленности» на наличие каналов утечки информации.

Проанализирован рынок средств активной и пассивной защиты информации от утечек по каналам связи и сформирована система защиты организации.

В результате работы спроектирован план помещения с учетом средств инженерно-технической защиты информации. Общая сумма затрат составила 1 140 000 рублей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

6. 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.
7. Трунова, А. А. Анализ каналов утечки конфиденциальной информации в информационных системах предприятий / А. А. Трунова. — Текст: непосредственный // Молодой ученый. — 2016. — No3 (107). — С. 69–72. — URL: <https://moluch.ru/archive/107/25842/> (дата обращения: 19.01.2022).
8. Каторин Ю. Ф., Разумовский А. В., Спивак А. И. Защита информации техническими средствами. Учебное пособие - Санкт-Петербург: НИУ ИТМО, 2012. - 416 с. - экз.
9. Скрипник Д. Техническая защита информации. [Интернет-ресурс] URL: <https://intuit.ru/studies/courses/3649/891/info> (дата обращения: 15.01.2022)