



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(Дипломная работа)

На тему «Организация защиты информации в строительной компании от
утечки по техническим каналам»

Исполнитель

(подпись)

Карпенкова Дарья Андреевна

(фамилия, имя, отчество)

Руководитель

(подпись)

Юрин Игорь Валентинович

(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой

(подпись)

Бурлов Вячеслав Георгиевич

(фамилия, имя, отчество)

«____» _____ 2024 г.

Санкт-Петербург

2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
ГЛАВА 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ.....	7
1.1. Классификация технических каналов утечки информации.....	7
1.2. Угрозы реализации технических каналов утечки информации	8
1.3. Защита информации от утечки по техническим каналам	13
1.4. Выводы по 1 главе	16
ГЛАВА 2. АНАЛИЗ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	17
2.1. Определение информационных потоков компании.....	24
2.2. Классификация обрабатываемой информации	28
2.3. Анализ потенциальных технических каналов утечки информации	34
2.4. Разработка модели угроз безопасности информации.....	36
2.5. Разработка модели нарушителя	37
2.6. Класс защищенности автоматизированной системы.....	38
2.7. Аналитическое обоснование необходимости повышения эффективности системы технической защиты информации	40
2.8. Выводы по 2 главе	44
ГЛАВА 3. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ПРИ ЕЕ ОБРАБОТКЕ, ХРАНЕНИИ И ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ.....	45
3.1. Средства защиты информации от утечки по техническим каналам	45
3.1.1. Организационные меры по защите информации.....	45
3.1.2. Технические средства защиты информации.....	46
3.2. Оценка защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от ее утечки по каналу побочных электромагнитных излучений и наводок	50
3.3. Обеспечение защиты информации от хищения, утраты, уничтожения, искажения, подделки и блокирования доступа к ней в результате НСД	60
3.4. Оценка эффективности применяемых мер и средств защиты информации	61
3.5. Выводы по 3 главе	66
ЗАКЛЮЧЕНИЕ	68
СПИСОК ЛИТЕРАТУРЫ	70
Приложение А.....	71

Приложение Б	104
Приложение В	111
Приложение Г	114

ВВЕДЕНИЕ

В современном информационном обществе защита информации является одной из наиболее актуальных и значимых проблем. Строительная компания, как и любая другая компания, имеет дело с большим объемом конфиденциальных данных, которые становятся объектом интереса для злоумышленников. Технические каналы утечки информации представляют собой большую угрозу для общественной жизни и развития бизнеса.

В последние годы цифровая трансформация показывает потенциал для преобразования различных отраслей экономики, и строительная индустрия не является исключением. Вместе с использованием новейших технологий, таких как искусственный интеллект, интернет вещей и автоматизация, цифровая трансформация открывает множество возможностей для улучшения эффективности и производительности в строительстве.

Одним из главных преимуществ цифровой трансформации в строительной отрасли является упрощение процесса проектирования и планирования. С помощью 3D-моделирования и виртуальной реальности, инженеры и архитекторы могут создать точные и детализированные модели зданий и сооружений, что позволяет выявить потенциальные проблемы заранее и сэкономить время и ресурсы при строительстве.

В целом, цифровая трансформация в строительной отрасли предлагает огромные возможности для повышения эффективности, снижения затрат и улучшения качества работ. С развитием новых технологий и инструментов, будущее строительства становится все более связанным с цифровым миром. Использование этих инноваций открывает новые горизонты для строительства и помогает преодолеть традиционные ограничения этой отрасли.

В условиях цифровой трансформации, строительные компании сталкиваются с новыми вызовами в области информационной безопасности. Несмотря на все преимущества, которые предоставляют современные технологии, они приносят с собой и ряд угроз, которые способны нанести ущерб бизнесу.

Строительные компании часто работают с конфиденциальными данными, такими как финансовая информация клиентов, контракты, стратегии развития компании, маркетинговые данные, техническая документация, планы строительства. Злоумышленники и конкуренты могут попытаться получить доступ к этим данным, чтобы использовать их в своих корыстных целях. Киберпреступники могут использовать социальную инженерию, фишинг, вредоносные программы, техническую компьютерную разведку, кибершпионаж и другие техники, чтобы провести успешную атаку. Ущерб от подобного рода инцидентов исчисляется сотнями миллионов рублей.

Организации в строительной индустрии работают с персональными данными сотрудников и клиентов, включая их личные сведения, финансовые данные и другую конфиденциальную информацию. Если компания не защищает такие данные должным образом, то она рискует подвергнуться утечкам, что может привести к негативным последствиям, таким как большие издержки материального характера, ущерб для имиджа компании, штрафные санкции.

Утечка информации по техническим каналам является одной из основных угроз безопасности информации ограниченного доступа. Этот вид утечки предполагает неконтролируемое распространение информационного сигнала от его источника через физическую среду до технического средства, осуществляющего прием информации.

Эффективная техническая защита информации информационных ресурсов играет важную роль в современном мире, где информация стала одним из самых ценных активов. Эти меры являются неотъемлемой частью комплексной системы обеспечения информационной безопасности и способствуют оптимизации финансовых затрат на организацию защиты информации.

На сегодняшний день, одной из наиболее важных задач является организация защиты информации в компании от утечки по техническим каналам. Цифровая трансформация строительных компаний является актуальным трендом в современной индустрии. Внедрение цифровых технологий позволяет оптимизировать процессы проектирования, строительства и управления,

повышая эффективность работы, сокращая затраты и сроки проектов. Однако, вместе с преимуществами, цифровая трансформация также вносит новые вызовы в области информационной безопасности.

Объектом выпускной квалификационной работы является система защиты информации строительной компания, занимающаяся комплексным проектированием от градостроительного консалтинга и концепций застройки до рабочей документации объектов строительства, включая инженерные решения, с их авторским и техническим сопровождением до полного введения объекта «под ключ».

Предметом выпускной квалификационной работы является техническая защита информации в строительной компании.

Целью дипломного проекта является разработка и внедрение эффективных мер защиты информации в строительной компании от утечки по техническим каналам.

ГЛАВА 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

1.1. Классификация технических каналов утечки информации

Утечка информации – это процесс несанкционированного переноса информации от ее источника к злоумышленнику по каналу утечки информации.

Утечка информации по техническим каналам является одной из ключевых угроз безопасности конфиденциальной информации. Под этим термином понимается неконтролируемый процесс распространения информативного сигнала от его источника через физическую среду до технических устройств, которые осуществляют прием и обработку этой информации.

Основные технические средства и системы (ОТСС) представляют собой технические средства и построенные на их базе системы, которые непосредственно обрабатывают, принимают, хранят и передают конфиденциальную информацию. В состав таких средств входят электро-вычислительная техника, режимные автоматические телефонные станции, системы оперативно-командной и громкоговорящей связи, звукоусиления, звукового сопровождения и звукозаписи, а также другие средства, которые используются для проведения конфиденциальных переговоров и обработки другой конфиденциальной информации.

Часто вместе с основными техническими средствами и системами устанавливаются вспомогательные технические средства и системы (ВТСС), которые не прямо учувствуют в обработке конфиденциальной информации, но используются совместно с ними. К таким средствам и системам относятся открытые телефонные линии, громкоговорящая связь, системы пожарной и охранной сигнализации, системы электропитания, освещения, заземления, радиодиффузии, электробытовые и электроизмерительные приборы и другие. При этом важной задачей является обеспечение безопасности информации путем минимизации размещения вспомогательных технических средств и систем относительно основных технических средств. Информация в ОТСС защищается различными мерами, включая инженерно-технические, программно-аппаратные, криптографические, режимные и другие [1].

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды, через которую они распространяются. На рисунке 1 показана общая классификация технических каналов утечки информации, которая включает следующие виды каналов.



Рисунок 1 – Классификация технических каналов утечки информации

1.2. Угрозы реализации технических каналов утечки информации

Выявление и предотвращение утечки данных по техническим каналам является важной задачей в области информационной безопасности. Одной из распространенных причин утечки информации является наличие закладных электронных устройств, таких как микрофоны, видеокамеры, стетоскопы. Эти устройства могут быть смонтированы в оборудование, линии электропередачи, строительные конструкции и предметы быта.

При обработке данных возможно возникновение угроз безопасности за счет реализации следующих технических каналов утечки информации, которые показаны на рисунке 2:

- угроз утечки акустической (речевой) информации;

- угроз утечки видовой информации;
- угроз утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

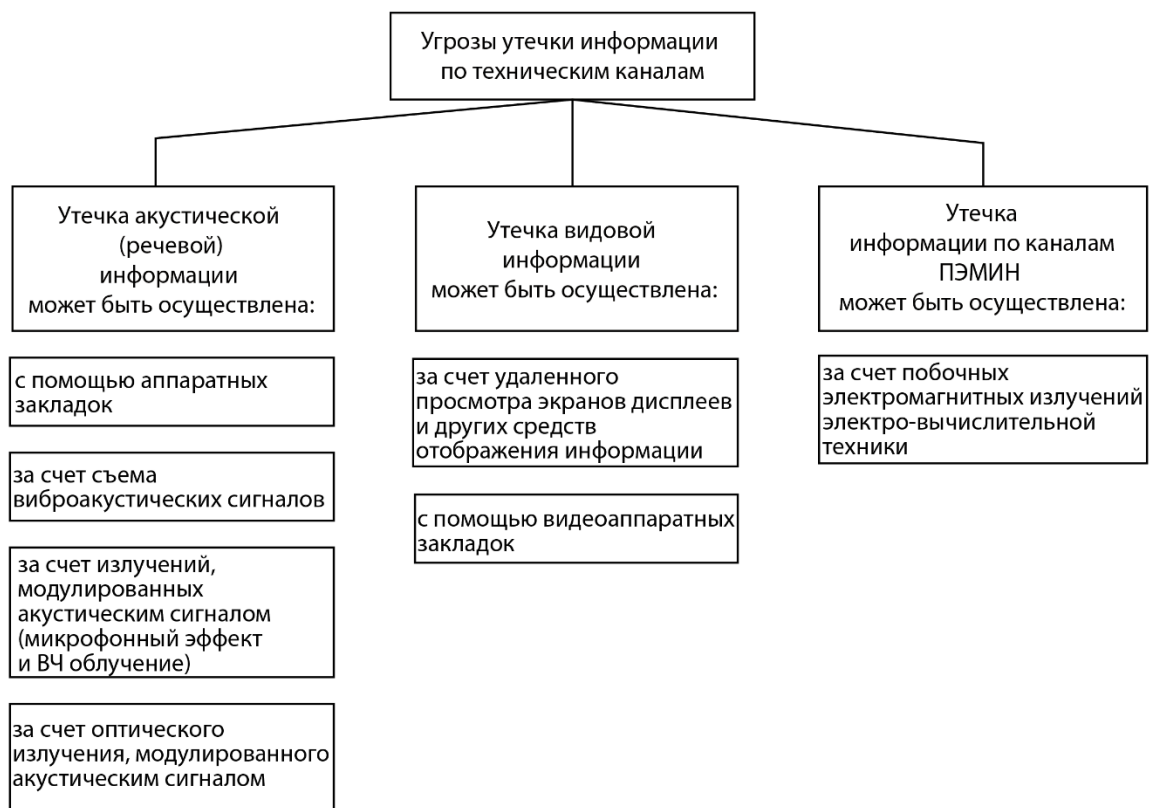


Рисунок 2 – Реализации технических каналов утечки информации

Акустический сигнал представляет собой колебания частиц акустической среды, которые распространяются в виде звуковых волн различной формы и продолжительности. Эти колебания могут быть инициированы механическими колебаниями систем, такими как органы речи человека, а также могут быть преобразованы с помощью различных устройств, включая электроакустические преобразователи.

Таковыми устройствами могут быть пьезоэлементы, микрофоны, телефоны, громкоговорители и другие подобные устройства. Они выполняют функцию преобразования акустических колебаний в электрические и обратно.

В зависимости от того, как информационные сигналы возникают физически, как они распространяются в среде и как они могут быть перехвачены, технические каналы утечки акустической (речевой) информации можно классифицировать на несколько типов: акустические, виброакустические,

виброакустические (лазерные), акустоэлектрические, высокочастотные навязывания и параметрические каналы. Характеристики основных каналов утечки акустической (речевой) информации и основные характеристики средств ее перехвата приведены в таблице 1.

Таблица 1 – Характеристики технических каналов утечки речевой информации и характеристики аппаратуры перехвата речевой информации по техническим каналам

Название технических каналов утечки информации	Название аппаратуры	Виды аппаратуры	Дальность перехвата акустической (речевой) информации
Акустический	Направленные микрофоны	Стационарная, портативная носимая, портативная возимая	до 150 м
	Ненаправленные микрофоны	Портативная носимая, портативная возимая	до 50 м
Виброакустический	Вибродатчики (контактные микрофоны)	Автономная автоматическая (совместно со средствами приема ретранслируемого сигнала)	до 10 м (на поверхностях 200 см и более)
Виброакустический (лазерный)	Лазерные микрофоны	Стационарная, портативная носимая, портативная возимая	до 600 м
Акустоэлектрический	Средства съема электрических сигналов с гальваническим подключением	Стационарная, портативная возимая	до 250 м

Название технических каналов утечки информации	Название аппаратуры	Виды аппаратуры	Дальность перехвата акустической (речевой) информации
Высокочастотное навязывание	Средства съема электрических сигналов с гальваническим подключением	Стационарная, портативная, возимая	до 250 м
Высокочастотное облучение (параметрический)	Приемники электромагнитного излучения	Стационарная, портативная, возимая	до 1500 м

Общая классификация портативной (носимой и возимой) аппаратуры перехвата речевой информации показана ниже на рисунке 3.

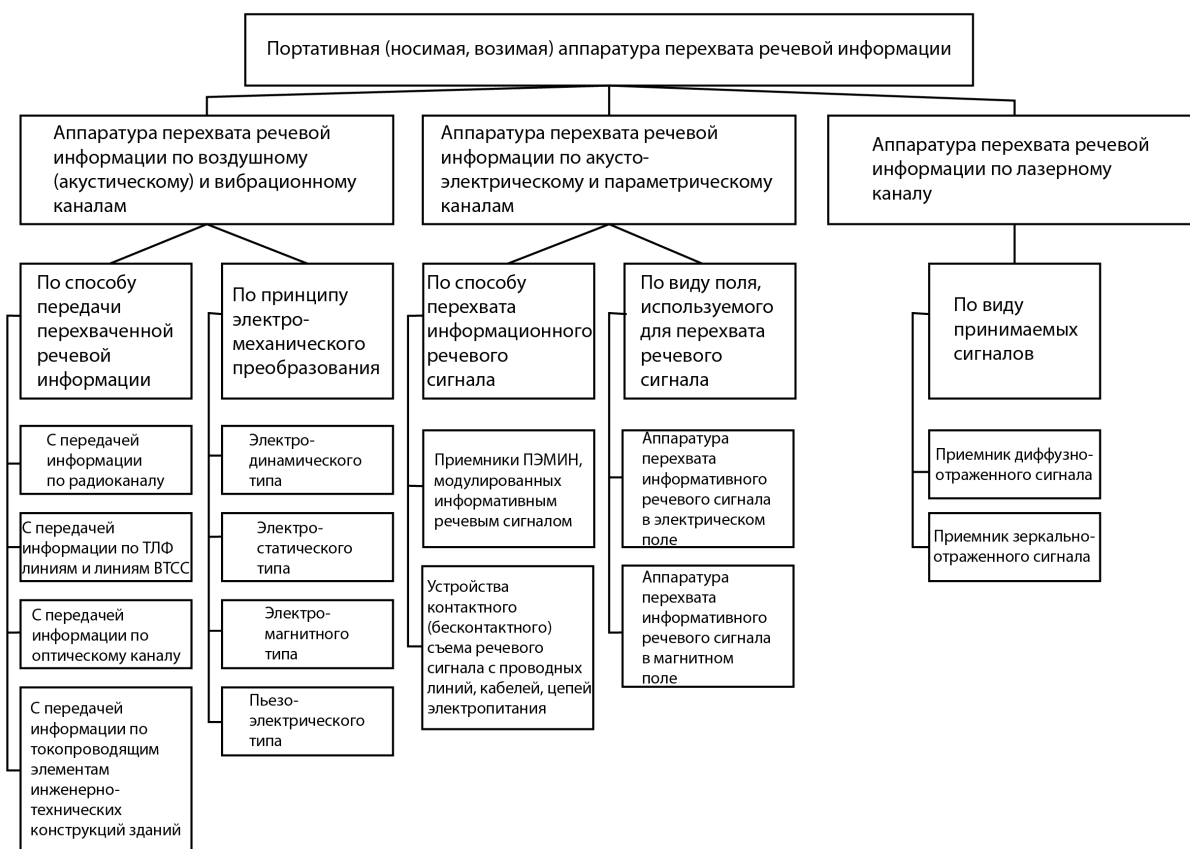


Рисунок 3 – Общая классификация портативной (носимой, возимой) аппаратуры перехвата речевой информации по техническим каналам утечки информации

Посторонние лица могут перехватывать или просматривать защищаемую видовую информацию, как непосредственно, при несанкционированном доступе в помещение объекта информатизации, так и на расстоянии прямой видимости

за пределами объекта информатизации, используя оптические и/или оптико-электронные устройства.

Для перехвата защищаемой видовой информации могут быть использованы следующие виды портативных (носимых, возимых) средств перехвата видовой информации, которые показаны на рисунке 4.

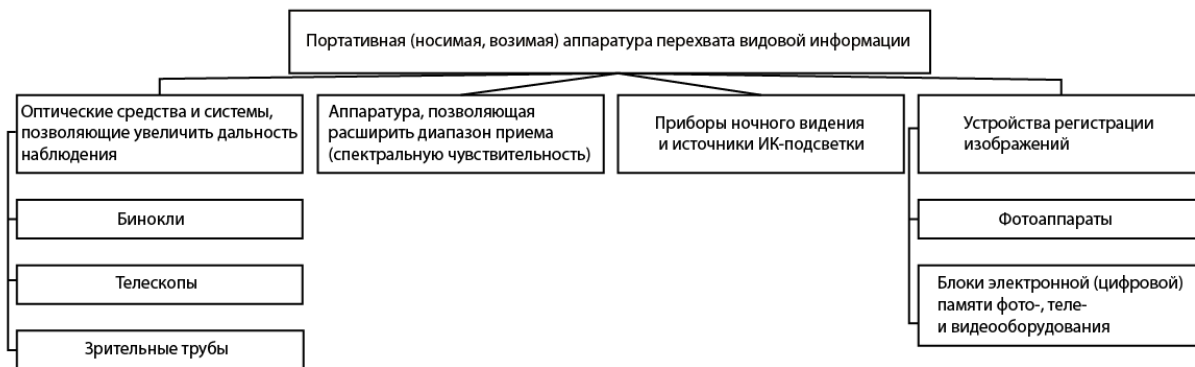


Рисунок 4 – Обобщенная классификация портативной (носимой, возимой) аппаратуры перехвата видовой (графической) информации

Побочные электромагнитные излучения и наводки (ПЭМИН) относятся к электромагнитным помехам или электромагнитным воздействиям, которые могут возникать в различных технических системах.

Побочные электромагнитные излучения возникают как результат работы электронных устройств и оборудования, таких как компьютеры, мобильные телефоны, радиостанции, телевизоры и другие подобные устройства. Они могут испускать электромагнитные волны, которые распространяются в окружающую среду.

Наводки, с другой стороны, возникают в результате внешнего электромагнитного воздействия на систему или устройство. Это может быть вызвано близким расположением других электронных устройств, сильными электромагнитными источниками (например, высоковольтными линиями электропередачи) или другими внешними факторами.

Основные каналы утечки информации за счет ПЭМИН приведены на рисунке 5.



Рисунок 5 – Основные каналы утечки информации за счет ПЭМИН

1.3. Защита информации от утечки по техническим каналам

Число утечек информации возрастает ежегодно. Если говорить об общих цифрах, то эксперты подсчитали, что количество скомпрометированных записей за 2022 год в 4,5 раза превысило население России. Компания InfoWatch, лидер российского рынка систем защиты корпоративной информации, представила исследование случаев утечек информации ограниченного доступа.

После стабильного увеличения числа зарегистрированных случаев утечки информации с 2017 по 2019 годы и их снижения во время пандемии, в 2022 году произошел резкий скачок. На рисунке 6 показано как по сравнению с предыдущим годом количество случаев утечки информации выросло более чем в 2,1 раза (на 112,6%).

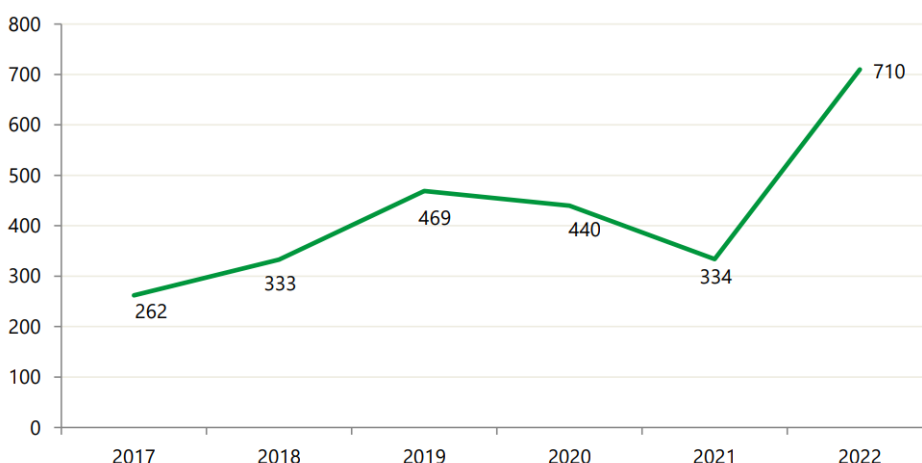


Рисунок 6 – Количество утечек данных (Россия, 2017-2022 гг.)

Действительно, с каждым годом риск утечки информации становится все более серьезной проблемой. В свете растущего количества кибератак, взломов и

других угроз безопасности данных, защита информации является важной задачей для компаний.

В целом, защита информации – это непрерывный процесс, требующий постоянного мониторинга, обновления и улучшения. Своевременные и эффективные меры по защите информации помогут снизить риск утечек и обеспечить конфиденциальность, целостность и доступность данных.

Защита информации от утечки по техническим каналам является приоритетной задачей, требующей использования разнообразных подходов и технических средств. В данном контексте возможны несколько вариантов, которые могут быть применены:

- источник и носитель информации могут физически находиться внутри контролируемой зоны объекта и предоставлять барьер от контакта с злоумышленниками или от удаленного воздействия на них с использованием технических средств сбора информации;

- соотношение энергии носителя и уровня помех на выходе приемника в канале утечки может быть организовано таким образом, что злоумышленнику будет затруднительно или невозможно получить информацию с носителя с требуемым качеством для ее использования;

- злоумышленнику не обнаружить источник или носитель информации;

- злоумышленник получает умышленно ложную информацию, которую воспринимает как истинную.

На рисунке 7 представлена классификация методов защиты информации от утечки по техническим каналам.

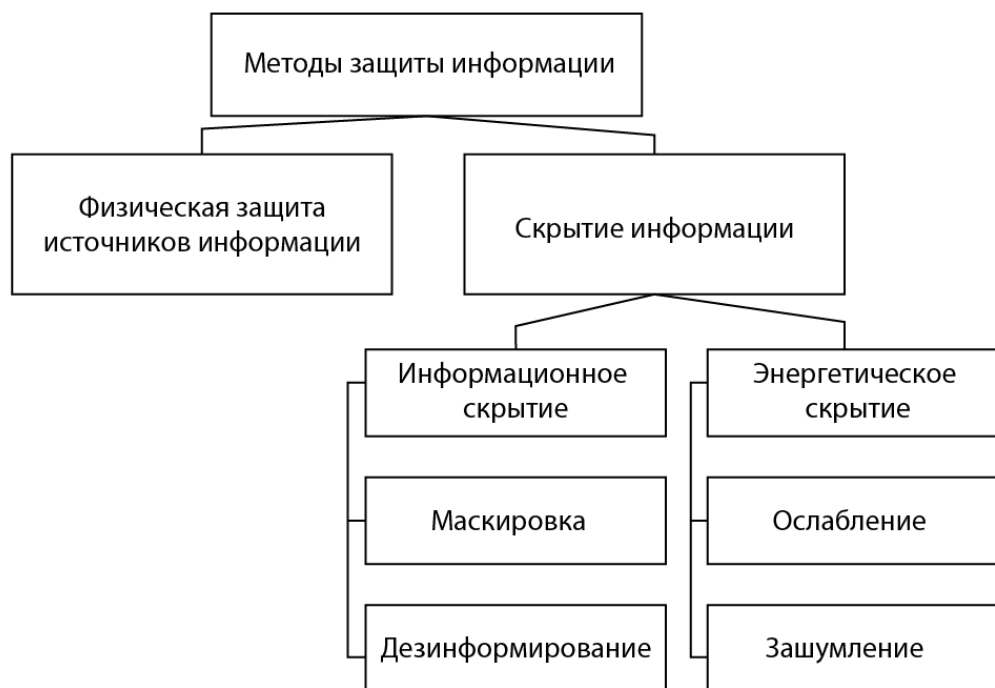


Рисунок 7 – Классификация методов защиты информации от утечки по техническим каналам

Суть процесса скрывания информации заключается в изменении структуры и энергетических характеристик информационных носителей с целью предотвратить или существенно затруднить возможность извлечения информации злоумышленником напрямую или с использованием технических средств для собственных целей.

Энергетическое скрывание представляет собой использование способов и средств защиты, препятствующих выполнению энергетического условия разведывательного контакта. Данный метод сокрывания информации обеспечивается применением способов и средств, уменьшающих энергию носителя или увеличивающих энергию помех.

Звукоизоляция направлена на ограничение распространения звуковых волн внутри определенного пространства и снижение воздействия внешних источников шума.

Звукопоглощение достигается с помощью преобразования кинетической энергии акустической волны в тепловую энергию в звукопоглощающем материале.

Для эффективной борьбы с каналами утечки используются различные методы, направленные на снижение уровня информационных сигналов или снижения соотношения сигнал/шум в процессе передачи до такого значения, при котором исключается возможность перехвата информации за пределами контролируемой зоны.

1.4. Выводы по 1 главе

Проведя анализ технических каналов утечки информации, можно прийти к выводу, что эффективная защита информации требует комплексного подхода и применения разнообразных методов защиты.

Для защиты информации от утечки по техническим каналам на объектах информатизации внедряются различные организационно-режимные мероприятия и специальные технические средства защиты технических средств приема, обработки, хранения и передачи информации (ТСПИ) и выявления электронных устройств перехвата информации (закладных устройств), внедренных в ТСПИ.

ГЛАВА 2. АНАЛИЗ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

В выпускной квалификационной работе рассмотрен объект информатизации – Строительная компания, расположенная по адресу: г. Санкт-Петербург, Малый проспект Васильевского острова, 6. Здание двухэтажное, офис компании находится на втором этаже, окна выходят на Малый проспект Васильевского острова и во двор. На рисунке 8 представлено картографическое расположение компании. На рисунке 9 изображена карта входа в строительную компанию. На рисунке 10 изображено расположение контролируемой зоны и трансформаторной подстанции.

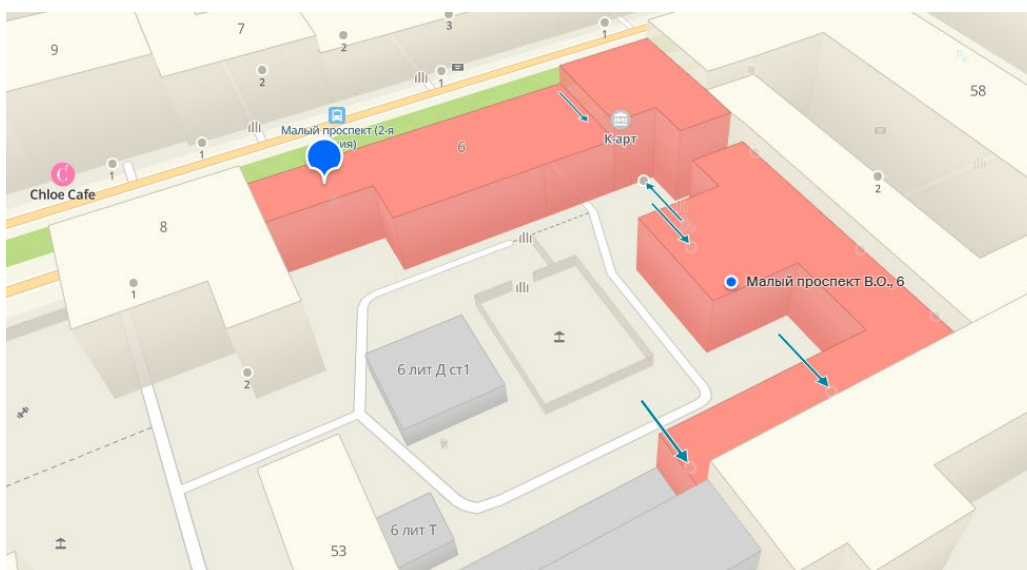


Рисунок 8 – Картографическое изображение здания

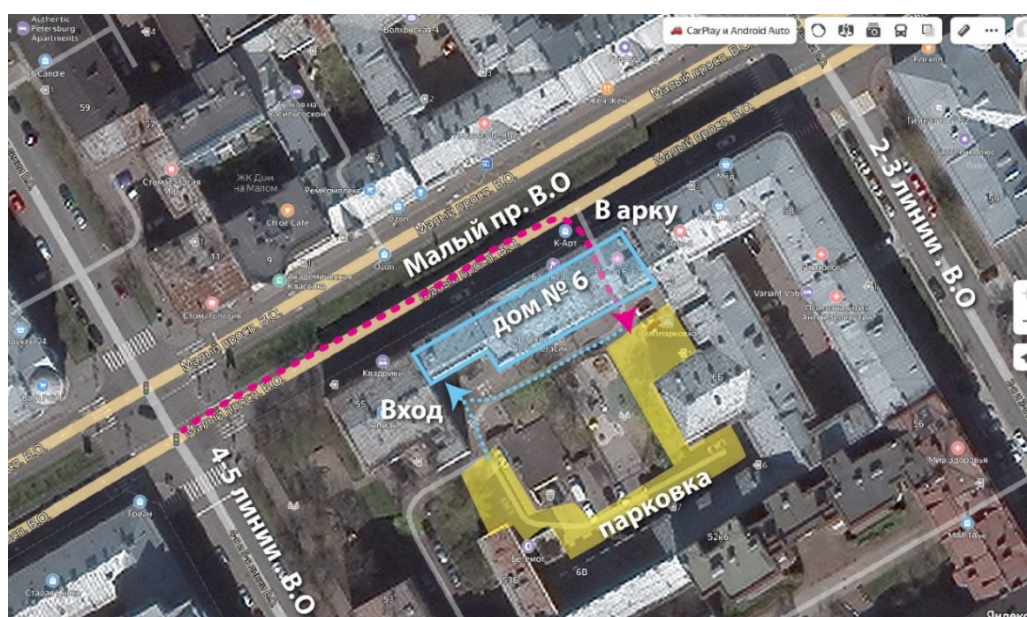


Рисунок 9 – Карта входа в строительную компанию

На рисунке 10 показана граница контролируемой зоны и расположение трансформаторной подстанции.

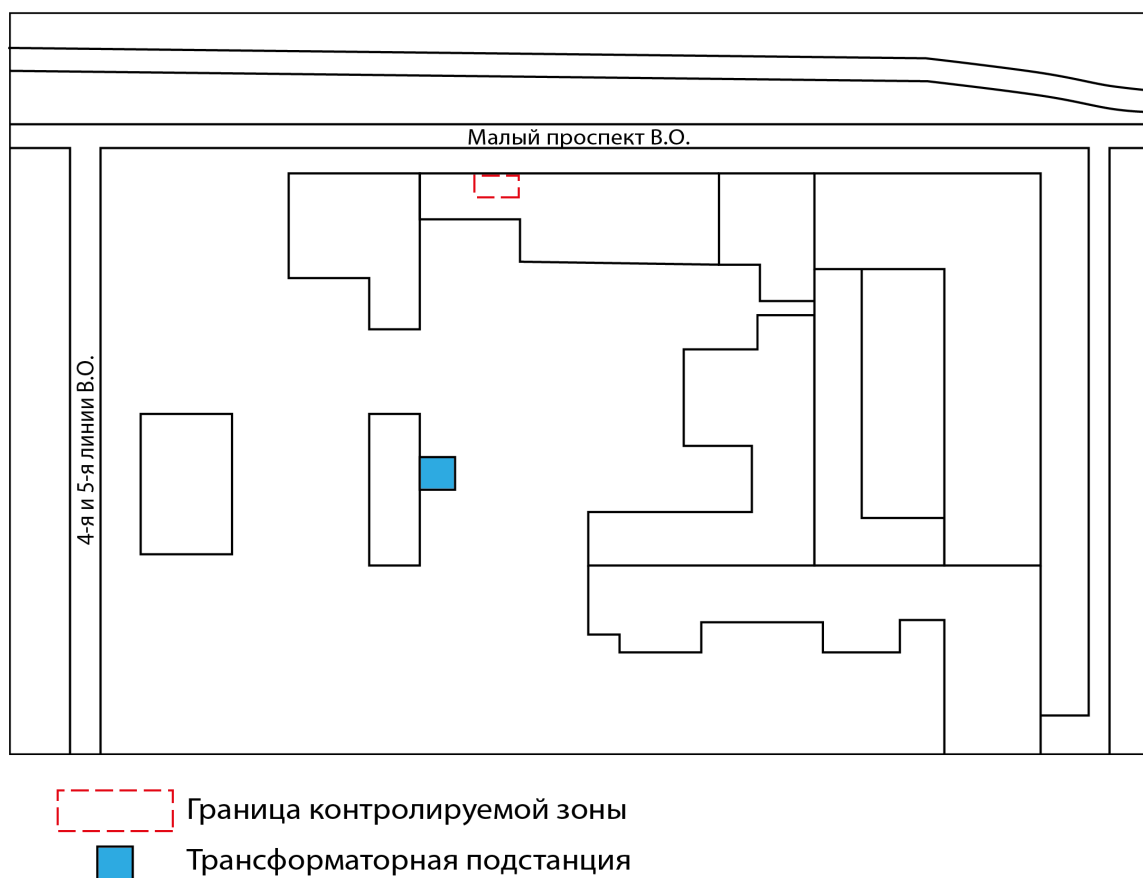


Рисунок 10 – Схема расположения контролируемой зоны и трансформаторной подстанции

Граница контролируемой зоны – это граница, которая обозначает переход от свободно доступной территории в зону, контролируемую системой безопасности.

Для строительной компании граница контролируемой зоны проходит по периметру офисного помещения.

На рисунке 11 показаны фотографии из окон близлежащих зданий.



Рисунок 11 – Фотографии из окон близлежащих зданий. Вид на Малый проспект В.О. (справа), вид во двор здания (слева)

На рисунке 12 показана 3D схема офисного пространства строительной компании.

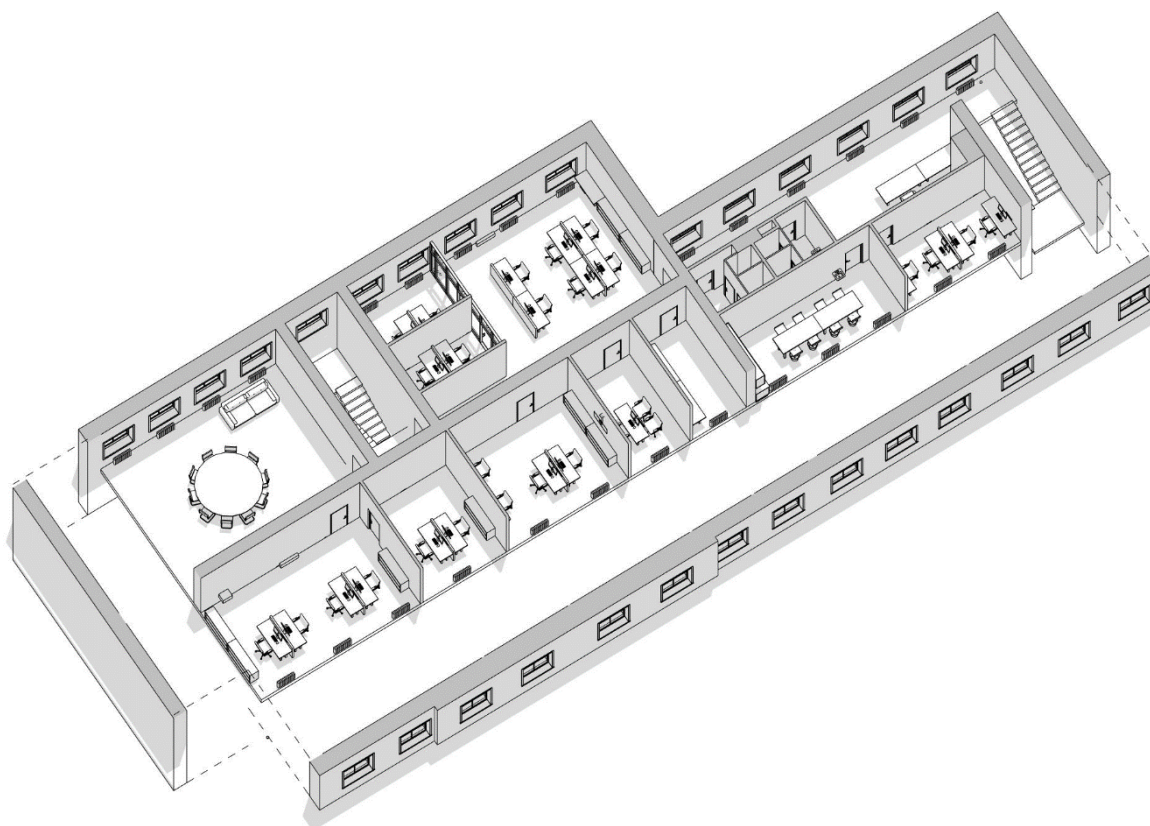


Рисунок 12 – 3D схема расположения офисного пространства

На рисунке 13 показана схема расположения автоматизированной системы в строительной компании. Площадь контролируемой зоны шириной 6 м и длиной 12 м составляет 72 м², высота потолка 4 м.

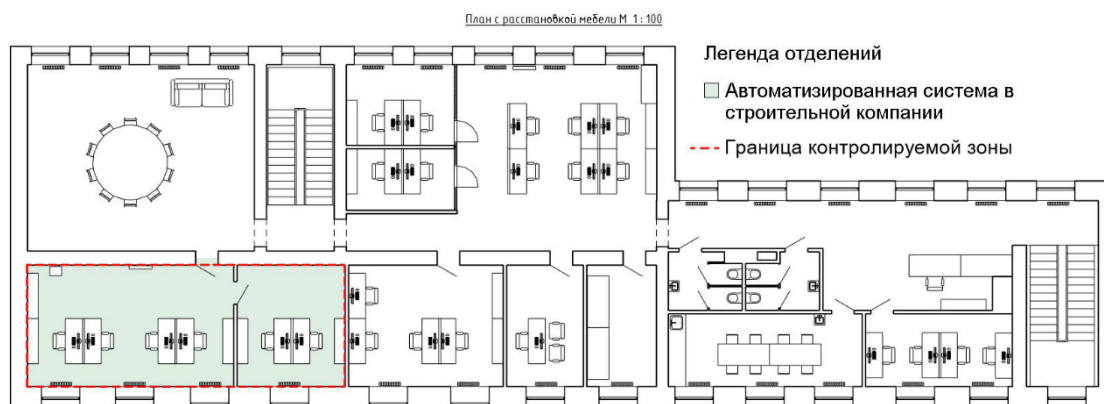


Рисунок 13 – Схема расположения автоматизированной системы в строительной компании

На рисунке 14 показана схема расположения оборудования автоматизированной системы.

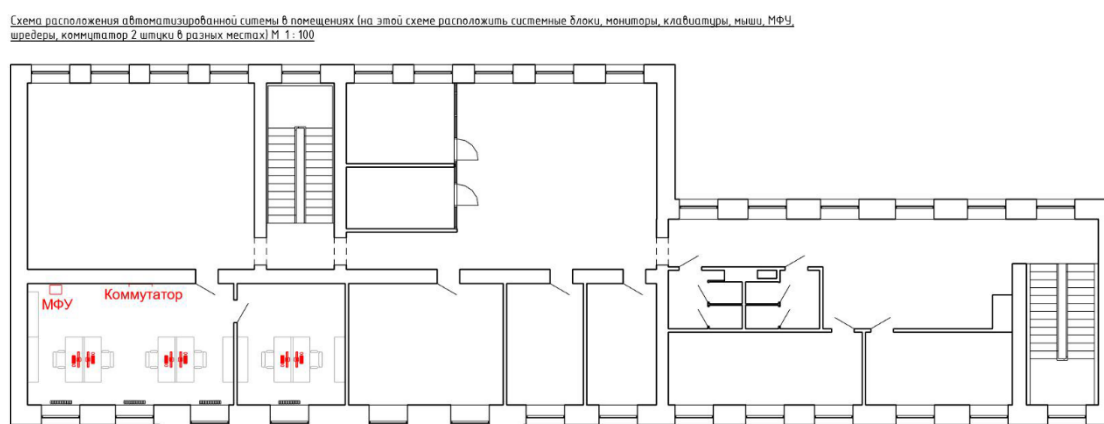


Рисунок 14 – Схема расположения оборудования автоматизированной системы

В таблице 2 приведен список оборудования автоматизированной системы.

Таблица 2 – Список оборудования автоматизированной системы

Наименование	Модель
ОТСС	
АРМ №1	
Системный блок	ПК MSI MAG Infinite S3
Монитор	27" Монитор Philips 273V7QDSB

Наименование	Модель
Манипулятор (Мышь)	Logitech M90
Клавиатура	ExeGate LY-331L5
APM №2	
Системный блок	ПК MSI MAG Infinite S3
Монитор	27" Монитор Philips 273V7QDSB
Манипулятор (Мышь)	Logitech M90
Клавиатура	ExeGate LY-331L5
APM №3	
Системный блок	ПК ASUS S500MC-51140F0090
Монитор	27" Монитор Philips 273V7QDSB
Манипулятор (Мышь)	Logitech M90
Клавиатура	ExeGate LY-331L5
МФУ лазерное	Kyocera ECOSYS M2040dn
APM №4	
Системный блок	ПК ASUS S500MC-51140F0090
Монитор	27" Монитор Philips 273V7QDSB
Манипулятор (Мышь)	Logitech M90
Клавиатура	ExeGate LY-331L5
APM №5	
Системный блок	ПК ASUS S500MC-51140F0090
Монитор	27" Монитор Philips 273V7QDSB
Манипулятор (Мышь)	Logitech M90
Клавиатура	ExeGate LY-331L5
APM №6	
Системный блок	ПК ASUS ROG Strix G10DK G10DK-53600X0190
Монитор	27" Монитор Philips 273V7QDSB
Манипулятор (Мышь)	Logitech M90
Клавиатура	ExeGate LY-331L5
BTCC	
Уничтожитель бумаг	ГЕЛЕОС АП55-5
Извещатель пожарный дымовой	ИП 212-187 W1.04
Оптический оповещатель	Schneider Electric XVR13B05
Громкоговоритель настенный	iSpeak 5 (AMC)
Сетевое оборудование	
Коммутатор	TP-Link TL-SG2428P

На рисунке 15 показана схема расположения охранной и пожарной сигнализации.

Схема расположения охранной и пожарной сигнализации с указанием установки и типов датчиков М 1:100

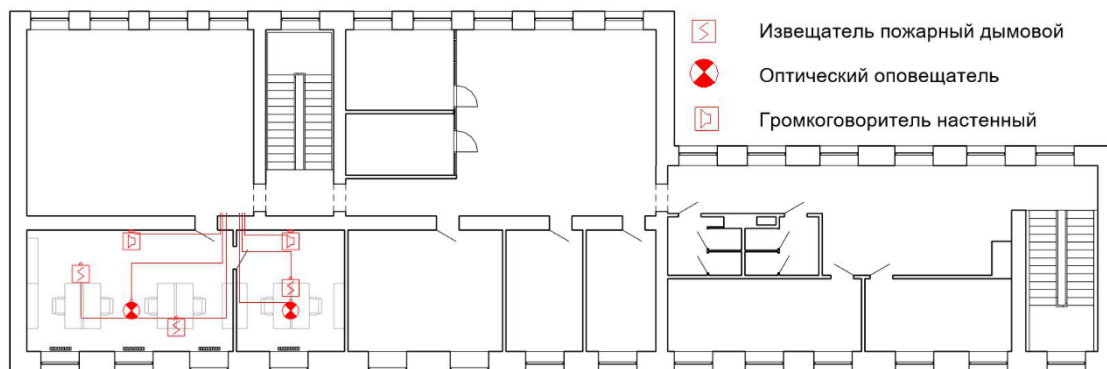


Рисунок 15 – Схема расположения охранной и пожарной сигнализации
На рисунке 16 показана схема электропитания в помещениях.

Схема электропитания в помещении М 1:100

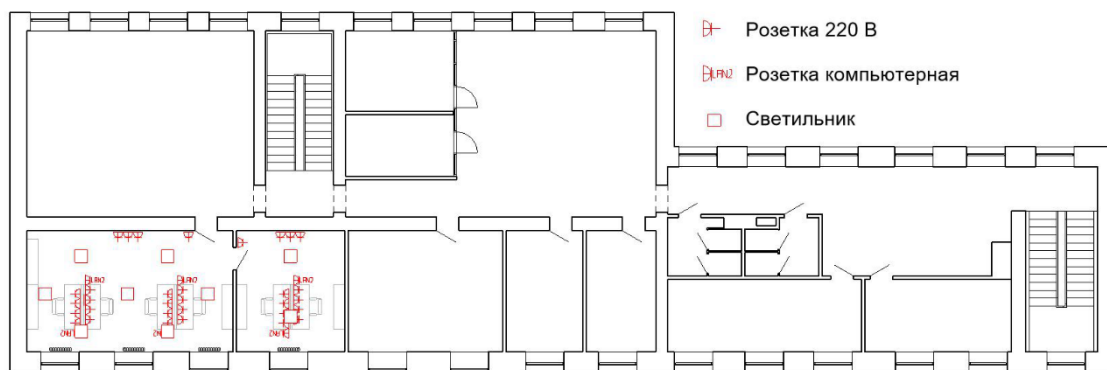


Рисунок 16 – Схема электропитания в помещении
На рисунке 17 показано размещение камер видеонаблюдения.

Схема видеонаблюдения М 1:100

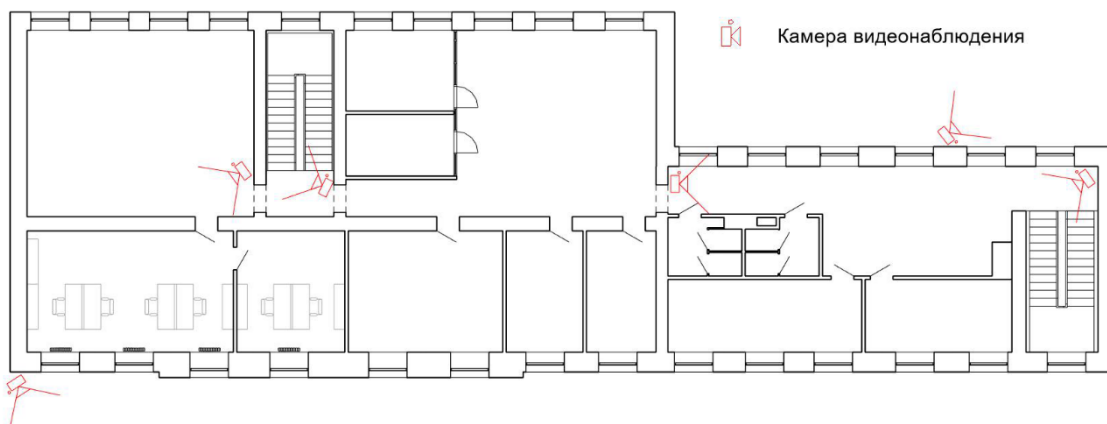


Рисунок 17 – Схема размещения камер видеонаблюдения

Общая схема системы контроля и управления доступом показана на рисунке 18.

Система контроля и управления доступом офисного помещения М 1:100



Рисунок 18 – Общая схема СКУД

На рисунке 19 представлена схема организационной структуры строительной компании. Данная схема определяет иерархическую и функциональную организацию компании, включая роли, ответственности и связи между различными отделами и сотрудниками.

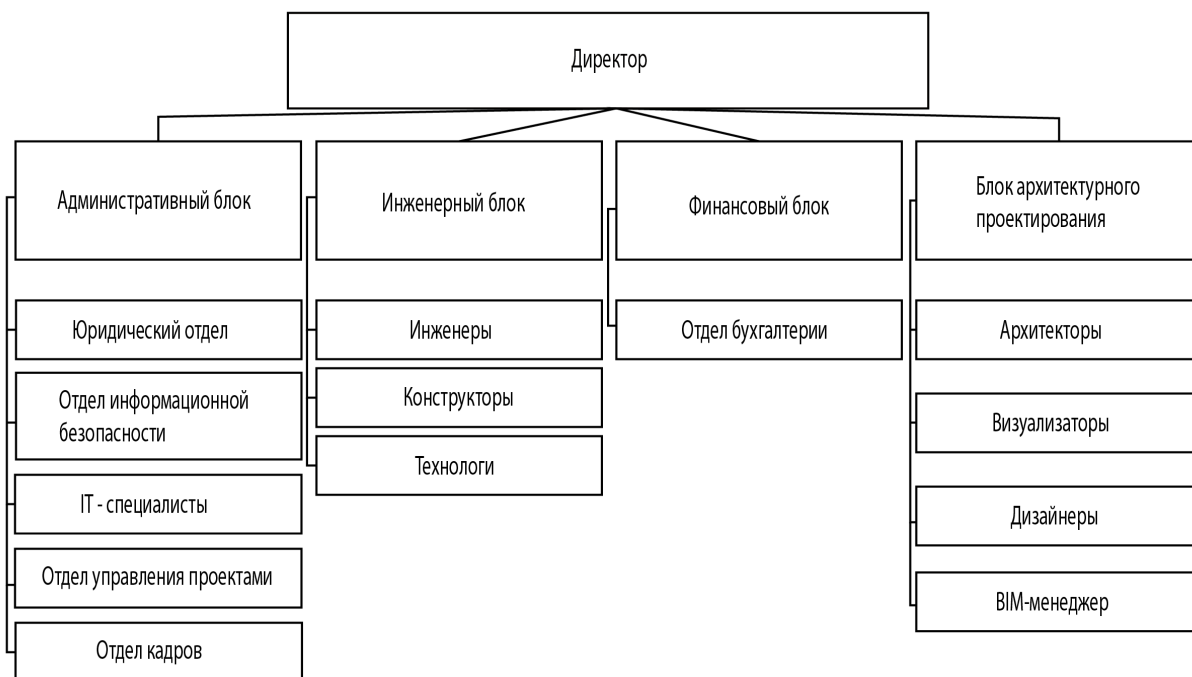


Рисунок 19 – Схема организационной структуры строительной компании

2.1. Определение информационных потоков компании

Информационные потоки в компании – это передача информации между различными отделами, сотрудниками и структурными единицами внутри организации. Они играют важную роль в обеспечении эффективного функционирования компании и принятии решений.

Информационные потоки могут иметь различные формы и направления, они могут быть формальными, так и неформальными. Формальные потоки информации определены официальными процедурами и стандартами компании. Неформальные потоки информации являются менее структурированными и могут включать в себя переговоры, электронные письма и другие неофициальные каналы коммуникации.

Цель информационных потоков в компании – обеспечить своевременную и точную передачу информации, содействовать принятию решений, повысить эффективность и координацию работы.

Итак, из анализа строительной компании можно выявить основные потоки информации, представленные в таблице 3.

Таблица 3 – Основные информационные потоки в строительной компании

Номер информационного потока	Вид информационного потока
1	Согласование о принятии на работу сотрудников, выход в отпуск
2	Информация о оформлении на работу, отбор персонала, анализ текучести кадров, личные дела сотрудников, аттестация сотрудников
3	Информация о сотрудниках, заработная плата, документы приказов об зачислении/увольнении, о командировках, отпусках, поощрениях/штрафных санкциях для сотрудников
4	Снабжение информацией об последних изменениях в действующем законодательстве
8	Информация о заключении/расторжении договоров и их оценка, информация о контрагентах
9	Информация о факте заключения/расторжения договоров
10	Информация по оплате договоров

Номер информационного потока	Вид информационного потока
11	Информация о проекте, управленческие решения, распоряжения, согласования, информация о контрольных точках
12	Информация о ресурсной базе, отчетность, временные планы, информация о сроках достижения целей
13	Информация о коммерческом предложении, согласование ключевых параметров проекта
14	Информация о рисках и возможностях проекта
15	Информация о трудовых и стоимостных затратах на реализацию проект
16	Информация о потенциальных угрозах и уязвимостях, информация о затратах, связанных с реализацией мер по защите информации, отчеты об инцидентах, проведенные расследования, результаты аудита информационных систем и процессов, а также отчеты о текущем уровне защищенности объектов информатизации - все это является важными документами, необходимыми для оценки эффективности и состояния системы защиты информации, информация о планировании и реализации мероприятий по защите информации, информация о регистрации и хранении данных о событиях информационной безопасности, информация о деятельности подразделений в целях защиты коммерческой тайны и персональных данных
17	Распоряжения о внедрении средств защиты информации, определение перечня информации, составляющей коммерческую тайну, приказ об утверждении перечня лиц, допущенных к работе с документами и информацией, отнесенной к коммерческой тайне, информация о согласовании плана текущей деятельности отдела, информация о согласовании установленного режима конфиденциальности при обсуждении или при обработке с использованием средств вычислительной техники информации, составляющей коммерческую тайну, а также персональные данные
18	Информация об обеспечении информационной безопасности, использования вычислительной

Номер информационного потока	Вид информационного потока
	техники и технической поддержки средств связи и программного обеспечения при проектировании, создании и эксплуатации автоматизированных систем и информационных ресурсов
19	Информация об обслуживании вычислительной техники и сетевого оборудования
20	Информация о выделении бюджета на обеспечении информационной безопасности
21	Информация о необходимости добавления в штат высококвалифицированных сотрудников, информация о обработке и защиты персональных данных сотрудников (политики, инструкции, приказы, должностные инструкции)
22	Информация о подборе персонала, программы обучения и развития сотрудников, обработка персональных данных, оплата труда, отпуска и больничные
23	Информация о планировании и использовании финансовых ресурсов, информация о соблюдении нормативных документов, регулирующих обработку персональных данных и коммерческой тайны, информация о передаче приказов ответственным лицам, имеющим доступ к коммерческой тайне
24	Информация, связанная с подготовкой документов (организационно-распорядительная документация, соглашения о конфиденциальности, согласие на обработку персональных данных и других документов, связанных с конфиденциальным документооборотом
25	Информация о неисправности компьютерной техники или программного обеспечения
26	Информация о необходимости подписания соглашений о конфиденциальности с контрагентами, ее соблюдении режима коммерческой тайны и работе с документацией, содержащей коммерческую тайну. Также стоит отметить информацию о контрагентах, с которыми ведется деловое взаимодействие
27	Информация о необходимости подписания соглашений о конфиденциальности с контрагентами, ее соблюдении режима

Номер информационного потока	Вид информационного потока
	коммерческой тайны и работе с документацией, содержащей коммерческую тайну. Также стоит отметить информацию о контрагентах, с которыми ведется деловое взаимодействие
28	Информация о техническом задании, информация о ходе работы, соглашение о конфиденциальности
29	Информация о сроках реализации проект
30	Информация о ходе работ, сдача проектного решения, согласование проектных решений с заказчиком, согласования, пожелания
31	Информация об оплате счета
32	Информация о факте оплаты, реквизиты
33	Информация о оформлении договоров и иных документов
34	Информация о предоставлении BIM среды в соответствии с техническими требованиями
35	Информация о неисправностях компьютерной техники или программного обеспечения
36	Информация о решении ремонта и настройки техники
37	Информация о заработной плате и отпуске
38	Информация о соблюдении режима коммерческой тайны
39	Информация об интерьерных решениях
40	Информация об планировочных решениях
41	Информация о работы в BIM среды
42	Информация о нововведениях в технологию работы с информационной моделью
43	Информация о конструкторских решениях
44	Информация об инженерных решениях
45	Информация о технологических решениях
46	Информация о согласовании принятых инженерных решений
47	Информация от заказчика, внесение изменений и правок
48	Информация о проекте, сроки реализации, постановка задач
49	Информация об администрировании корпоративной сети

Таблицу 3 сопровождаю схемой основных информационных потоков в строительной компании, которая показана на рисунке 20.

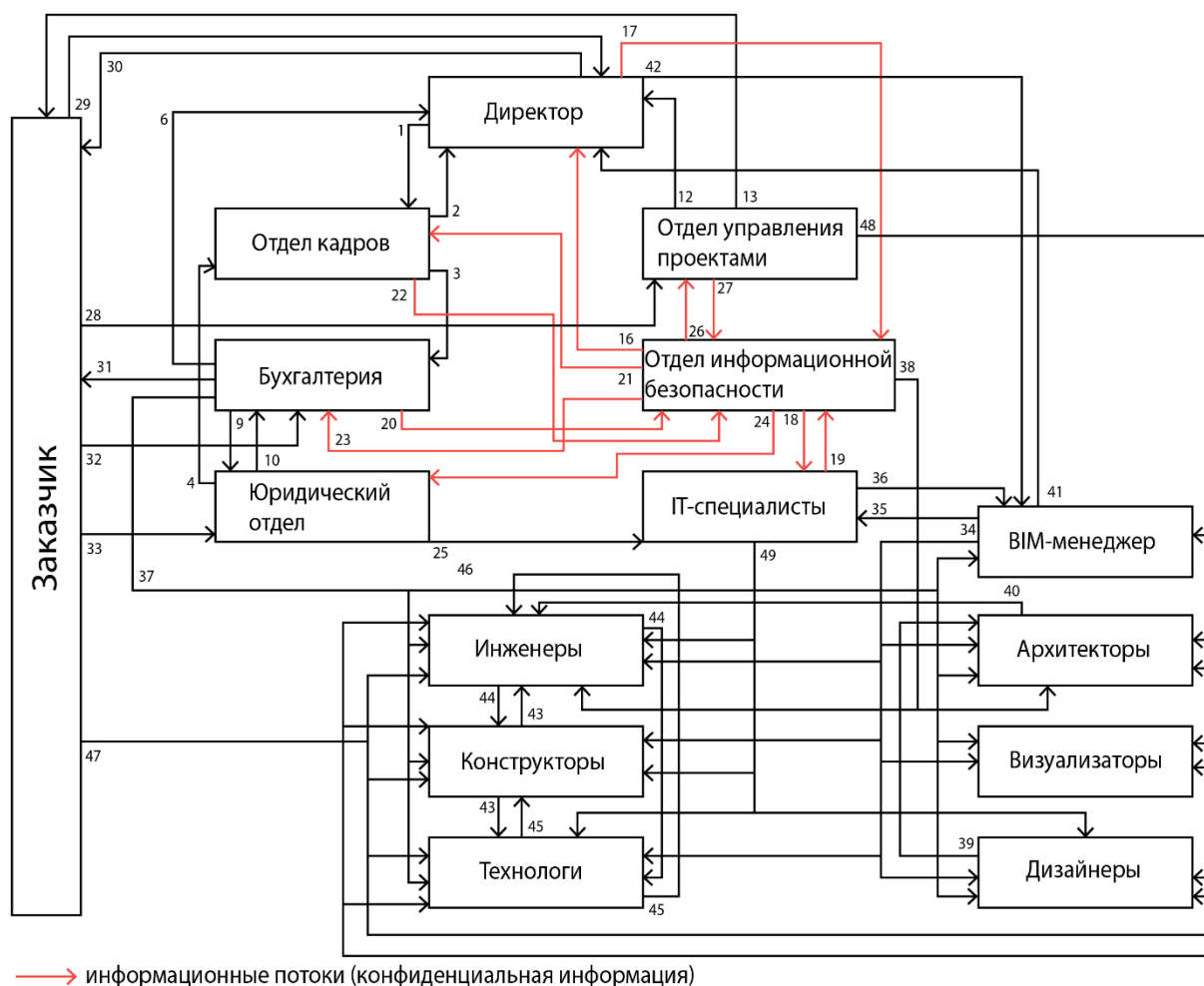


Рисунок 20 – Схема основных информационных потоков в строительной организации

Определение информационных потоков позволяет специалистам по информационной безопасности более точно анализировать риски и разрабатывать эффективные стратегии для защиты компании от угроз.

2.2. Классификация обрабатываемой информации

В строительной компании обрабатывается коммерческая тайна и персональные данные.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [2].

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [3].

К информации, составляющей коммерческую тайну, относятся:

- Внутренние стандарты проектирования в Обществе;
- Методики и инструменты проектирования, используемые в Обществе;
- Файлы информационных и иных моделей (.FBX, .3DS, .MAX, .DWG) Общества;
- Проектно-сметная документация Общества;
- Сведения в области финансовой деятельности Общества;
- Информация о ценовой политике Общества, методики ценообразования (порядок, способы);
- Текущие и планируемые показатели по организации финансовой деятельности (внутренняя финансовая отчетность);
- Сведения о финансовых операциях Общества и о доходах по этим операциям.
- Информация о проведении деловых переговоров с контрагентами и информация о содержании данных переговоров, включая материалы, подготовленные к проведению переговоров, либо составленные в ходе переговоров или после окончания – по результатам переговоров;
- Деловая переписка, включая информацию, содержащуюся в документах, поступивших от контрагентов Общества, информация, поступающая по электронной почте на адрес Общества и на корпоративные электронные адреса работников Общества, имеющая гриф «Коммерческая тайна».
- Сведения в области управленческой деятельности Общества;
- Информация о системе делопроизводства и документооборота Общества;

– Информация о составе и состоянии технических и программных средств Общества;

– Иная информация, за исключением информации, которая в соответствии с законодательством не может быть отнесена к коммерческой тайне, может быть отнесена к коммерческой тайне по решению Директора Общества.

К информации, составляющей персональные данные, относятся:

- Паспорт или иной документ, удостоверяющий личность;
- Трудовая книжка;
- Страховое свидетельство государственного пенсионного страхования;
- Свидетельство о постановке на учёт в налоговый орган и присвоения ИНН;
- Военный билет;
- Документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- Документы, содержащие сведения о заработной плате, доплатах и надбавках;
- Приказы о приеме лица на работу, об увольнении, а также о переводе лица на другую должность;
- Другие документы, содержащие сведения, предназначенные для использования в служебных целях.

Классификация субъектов деятельности по защите конфиденциальной информации, представлена в таблице 4.

Таблица 4 – Классификация субъектов деятельности по защите конфиденциальной информации

Субъект автоматизированной системы	Описание	Роль
Администратор безопасности	Специалисты, ответственный за	Эксперт

Субъект автоматизированной системы	Описание	Роль
	настройку, мониторинг и обеспечение безопасности информационных систем. Он имеют прямой доступ к конфиденциальной информации и отвечает за ее защиту от несанкционированного доступа	
Владелец приложений	Ответственное лицо, которое отвечает за управление, разработку, использование, обновление и обеспечение защиты приложения	Определяет стратегию развития приложения, управление его функциональностью и дизайном, согласование требований пользователей, управление бюджетом, развертывание обновлений и обеспечение соответствия целям бизнеса
Владелец базы данных (БД)	Ответственное лицо, которое управляет базой данных, имеет право на доступ к данным и несет ответственность за их сохранность и использование	Эксперт
Администратор СУБД	Специалист, ответственный за установку, настройку, обновление, мониторинг и обслуживание баз данных	Эксперт
Пользователи конфиденциальной информации	Сотрудники организации, которым предоставлен доступ к конфиденциальной	Пользователи

Субъект автоматизированной системы	Описание	Роль
	информации в соответствии с их должностными обязанностями. Они должны быть обучены правилам обращения с конфиденциальной информацией и соблюдать установленные процедуры безопасного обращения с данными	
Владельцы информации	Лица, ответственные за определение конфиденциальности информации, ее классификацию и установление правил доступа. Они принимают решения о том, какая информация считается конфиденциальной и какие меры защиты необходимо применять	Эксперты
Внешние стороны	Могут быть партнеры, подрядчики, клиенты и другие внешние участники, которым предоставлен доступ к конфиденциальной информации. Для них также устанавливаются правила обработки конфиденциальной информации и контролируется их соответствие	Пользователи

Сводная таблица экспертной оценки показателей стоимости конфиденциальной информации представлена в таблице 5.

Таблица 5 – Элементы информации, подлежащие защите

Элемент информации	Гриф конфиденциальности элемента информации	Оценочный эксперт	Цена, рубли	Носитель информации
Стандарты проектирования, методики и инструменты проектирования	Коммерческая тайна	Владелец информации	100.000.000	SDD ПК, договоры, регламентирующая документация
Проектно-сметная документация			100.000.000	SSD ПК, договоры, документы инженерного отдела
Бухгалтерия			150.000.000	SSD ПК, договоры, отчеты
Информация о контрагентах			15.000.000	SSD ПК, договоры, отчеты
Информация о составе и состоянии технических и программных средств		Администратор безопасности	10.000.000	SSD ПК, документы службы безопасности
Организационно-распорядительная документация ИБ			5.000.000	SSD ПК, документы службы безопасности
Паспорт или иной документ, удостоверяющий личность, трудовая книжка, страховое свидетельство государственного пенсионного страхования, свидетельство о	Персональные данные	Администратор безопасности, владелец БД, администратор СУБД	5.000.000	SSD ПК, бумажные носители

Элемент информации	Гриф конфиденциальности элемента информации	Оценочный эксперт	Цена, рубли	Носитель информации
постановке на учёт в налоговый орган и присвоения ИНН, документы воинского учёта, документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки, документы, содержащие сведения о заработной плате, доплатах и надбавках, приказы о приеме лица на работу, об увольнении, а также о переводе лица на другую должность, другие документы, содержащие сведения, предназначенные для использования в служебных целях				
Итого стоимость активов, рубли			385.000.000	

2.3. Анализ потенциальных технических каналов утечки информации

При сохранении информации особенно важно определить и оценить потенциальные каналы утечки информации. Это позволяет принять

соответствующие меры по защите данных и предотвратить возможные угрозы безопасности.

У каждого технического канала есть свои уникальные особенности, которые требуют учета, чтобы обеспечить эффективную защиту информации от утечек и возможных угроз.

Выявление и распознавание каналов утечки информации основано на обнаружении и анализе демаскирующих признаков. Демаскирующие признаки являются общими индикаторами, которые помогают идентифицировать потенциальные каналы утечки информации. В таблице 6 приведены основные потенциальные технические каналы утечки данных.

Таблица 6 – Потенциальные технические каналы утечки информации

Вид канала	Способ кражи информации
Оптический канал	Нарушители способны получить информацию путем визуального слежения, фото- и видеофиксации.
Радиоэлектронный канал	Нарушители способны получить информацию путем перехвата электрических радиотепловых и радиолокационных сигналов.
Акустический канал	Нарушители способны получить информацию путем подслушивания разговоров с применением встроенных или портативных микрофонов и диктофонов.
Виброакустический канал	Злоумышленники способны получить информацию путем прослушивания разговоров с использованием телефонно-локационного способа, путем бесконтактного съема индуктивным или емкостным способом.
Параметрический канал	Нарушители способны получить информацию путем перехвата сигналов и детектирования побочных электромагнитных излучений с помощью технических средств приема информации.

Вид канала	Способ кражи информации
Каналы утечки информации за счет паразитных связей	Злоумышленники способны получить информацию путем прямого физического подключения к линии связи.
Материально-вещественный канал	Нарушители способны получить информацию путем хищения или нелегального доступа к носителям информации: флешкам, дискам, бумажным документам, черновикам.

Представленная классификация технических каналов утечки информации демонстрирует очевидность того факта, что проблему утечки информации нельзя решить с помощью одного способа или метода. Утечка информации – сложная и многогранная проблема, которая требует комплексного подхода и сочетания различных стратегий и мероприятий.

В ходе рассмотрения здания и офисного помещения, где находится автоматизированная система (АС), следует обратить внимание на следующие возможные технические каналы утечки информации:

1. Перехват побочных электромагнитных излучений;
2. Перехват наведенных электрических сигналов;
3. Высокочастотное облучение технических средств обработки информации;
4. Внедрение в технические средства обработки информации электронных устройств перехвата информации.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [4].

2.4. Разработка модели угроз безопасности информации

Модель угроз безопасности информации – документ, определяющий основные исходные условия для проверки соответствия средств защиты автоматизированной системе заданным к ней требованиям. При разработке модели угроз для автоматизированной системы используется нормативная база и методология ФСТЭК России.

Разработка модели угроз необходима коммерческим организациям для того, чтобы точно и четко определить требования к системе защиты информации. Модель позволяет организовать надежную защиты персональных данных и всего, что относится к категории «Коммерческой тайны».

В ходе анализа автоматизированной системы строительной компании была разработана модель угроз безопасности информации и рассчитаны вероятности реализации угроз безопасности (Приложение А).

При разработке модели угроз безопасности информации была применена обновленная Методика оценки угроз безопасности информации (ФСТЭК России, 2021 г.).

Методика устанавливает новую систему моделирования угроз безопасности, которая состоит из трех этапов:

- Определение негативных последствий от реализации (возникновения) угроз безопасности информации;
- Определение возможных объектов воздействия угроз безопасности информации;
- Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

2.5. Разработка модели нарушителя

Нарушитель безопасности информации - физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах [5].

Вероятный нарушитель информационной безопасности может быть:

- внешним;
- внутренним.

Атаки внешнего нарушителя, направленные на каналы связи, являются серьезной угрозой для безопасности информации. Такие атаки могут включать перехват, анализ, уничтожение, модификацию или блокирование передаваемой

информации. Одна из наиболее распространенных таких атак — это с использованием уязвимостей программной среды, которые могут быть эксплуатированы злоумышленниками для преодоления системы защиты конфиденциальной информации.

В целом, чтобы нейтрализовать атаки внешнего нарушителя на каналы связи, необходимо принять комплекс мер, включая организационные и режимные мероприятия, обновления программного обеспечения, шифрование данных и мониторинг сетевой активности.

Возможности внутреннего нарушителя зависят от ограничительных факторов, которые действуют в пределах контролируемой зоны. Один из основных факторов — это комплекс режимных и организационно-технических мер, принятых для обеспечения безопасности. Эти меры включают в себя подбор, расстановку и обеспечение высокой профессиональной подготовки персонала, контроль доступа физических лиц внутрь контролируемой зоны и контроль за выполнением работ, направленных на предотвращение и пресечение несанкционированных действий.

Модель нарушителя информационной безопасности представляет собой совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения.

Модель нарушителя разработана с целью анализа и понимания потенциальных угроз (Приложение Б).

2.6. Класс защищенности автоматизированной системы

Автоматизированная система — это система, в которой процессы и операции, которые ранее выполнялись вручную, теперь выполняются с помощью компьютерных программ и технологий. Такая система позволяет автоматизировать и оптимизировать различные бизнес-процессы, улучшая скорость, эффективность и точность работы.

Автоматизированные системы могут включать в себя различные компоненты, такие как программное обеспечение, оборудование, сенсоры, базы

данных и сетевые ресурсы. Они могут включать в себя функции планирования, управления, мониторинга, анализа данных, управления ресурсами и другие.

Цель автоматизированной системы - улучшить производительность, снизить риски ошибок и оптимизировать использование ресурсов. Она может помочь ускорить выполнение задач, улучшить качество работы, упростить процессы и улучшить уровень обслуживания.

Однако, важно также обеспечить безопасность автоматизированной системы, включая защиту данных, обеспечение конфиденциальности, целостности и доступности, а также предотвращение несанкционированного доступа и угроз безопасности.

Согласно руководящему документу ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г., все действующие и проектируемые автоматизированные системы (АС) учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию подлежат классификации.

Для эффективной системы безопасности строительной компании необходимо определить класс защищенности автоматизированной системы. Для этого был проведен анализ автоматизированной системы и получены следующие результаты:

- Система обрабатывает информацию на носителях различного уровня конфиденциальности;
- В АС обрабатывается и хранится информация ограниченного доступа (конфиденциальная информация);
- АС является многопользовательской;
- Пользователи имеют одинаковые права доступа (полномочия).

Проанализировав полученные результаты, можно сделать вывод, что автоматизированная система относится к классу защищенности «2Б». На основании этого в соответствии Руководящим документом ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к

информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г. в таблице 7 представлены требования к системе.

Таблица 7 – Подсистемы и требования к классу защищенности 2Б

Подсистемы и требования	Класс защищенности 2Б
1. Подсистема управления доступом	
1.1 Идентификация, проверка подлинности и контроль доступа субъектов: при входе в систему	+
1.2 Управление потоками информации	+
2. Подсистема регистрации и учета	
2.1 Регистрация и учет: входа (выхода) субъектов доступа в (из) систему (узел сети)	+
2.2 Учет носителей информации	+
3. Криптографическая система	
3.1 Шифрование конфиденциальной информации	-
3.2 Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-
3.3 Использование аттестованных (сертифицированных) криптографических средств	-
4. Подсистема обеспечения целостности	
4.1 Обеспечение целостности программных средств и обрабатываемой информации	+
4.2 Физическая охрана средств вычислительной техники и носителей информации	+
4.3 Наличие администратора (службы) защиты информации в АС	-
4.4 Периодическое тестирование СЗИ НСД	+
4.5 Наличие средств восстановления СЗИ НСД	+
4.6 Использование сертифицированных средств защиты	-

2.7. Аналитическое обоснование необходимости повышения эффективности системы технической защиты информации

Аналитическое обоснование необходимости повышения эффективности технической защиты информации (ТЗИ) основывается на анализе объекта информатизации, на оценке угроз, связанных с безопасностью информации, и на

определении потенциальных уязвимостей, которые могут быть использованы злоумышленниками.

Для конкретизации обоснования необходимости повышения эффективности системы технической защиты информации приведу реестр информационных активов в виде таблицы 8.

Таблица 8 – Реестр информационных активов

Информационный актив	Тип информационного актива	Свойства информационного актива			Стоимость актива, рубли
		Целостность	Доступность	Конфиденциальность	
Стандарты проектирования, методики и инструменты проектирования	Коммерческая тайна	Ц1	Д1	К1	100.000.000
Проектно-сметная документация		Ц1	Д1	К1	100.000.000
Бухгалтерия		Ц1	Д1	К1	150.000.000
Информация о контрагентах		Ц2	Д1	К2	15.000.000
Информация о составе и состоянии технических и программных средств		Ц1	Д2	К1	10.000.000
Организационно-распорядительная документация ИБ		Ц2	Д2	К1	5.000.000
Паспорт или иной документ, удостоверяющий личность, трудовая книжка, страховое свидетельство государственного пенсионного страхования, свидетельство о постановке на учёт в	Персональные данные	Ц2	Д2	К1	5.000.000

Информационный актив	Тип информационного актива	Свойства информационного актива			Стоимость актива, рубли
		Целостность	Доступность	Конфиденциальность	
налоговый орган и присвоения ИНН, документы воинского учёта, документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки, документы, содержащие сведения о заработной плате, доплатах и надбавках, приказы о приеме лица на работу, об увольнении, а также о переводе лица на другую должность, другие документы, содержащие сведения, предназначенные для использования в служебных целях					

Критерии оценивания представлены в таблице 9.

Таблица 9 – Критерии оценивания

Доступность	Целостность	Конфиденциальность
Д1 – критическая — это такое состояние или ситуация, когда отсутствие чего-то приводит к полной остановке работы субъекта	Ц1 – критическая — это такое состояние или ситуация, где любое несанкционированное изменение может привести к неправильной работе всего субъекта или его значительной части, а	К1 – критическая — это такое состояние или ситуация, где любое разглашение информации может привести к полному краху работы субъекта или вызвать

Доступность	Целостность	Конфиденциальность
	последствия такой модификации будут необратимыми	значительные материальные потери
Д2 – важная — это такое состояние или ситуация, когда отсутствие чего-то не приведет к полной остановке работы субъекта, но рано или поздно понадобится	Ц2 – важная — это такое состояние или ситуация, где любое несанкционированное изменение может привести к неправильной работе части субъекта через некоторое время, если не будут предприняты некоторые действия, а последствия такой модификации будут обратимы	К2 – важная — это такое состояние или ситуация, где любое разглашение информации может привести к моральным потерям
Д3 – незначительная — это такое состояние или ситуация, когда отсутствие чего-то не влияет на работу субъекта	Ц3 – незначительная — это такое состояние или ситуация, где любое несанкционированное изменение не скажется на работе системы	К3 – незначительная — это такое состояние или ситуация, где любое разглашение информации не влияет на работу субъекта

Основные аргументы, подкрепляющие необходимость повышения эффективности системы технической защиты информации:

1. Защита конфиденциальности. Техническая защита информации обеспечивает конфиденциальность данных, защищая их от утечки или несанкционированного распространения. Это особенно важно в случае хранения или обработки конфиденциальной информации, такой как персональные данные и коммерческая тайна.

2. Защита целостности. Защита целостности информации является важным аспектом безопасности. Несанкционированные изменения или модификации данных могут привести к искажению информации и принятию ошибочных решений.

3. Обеспечение доступности. Система технической защиты информации также направлена на обеспечение непрерывной доступности информации. Отказ или нарушение доступности конфиденциальной

информации может нанести серьезный ущерб бизнесу или нарушить работу организации.

Система технической защиты информации должна:

1. Предотвращать утечки информации через технические каналы утечки информации;
2. Предотвращать несанкционированный доступ к информации.

2.8. Выводы по 2 главе

Анализ объекта информатизации является основой для дальнейшей разработки системы защиты информации.

В ходе проведенной работы мной обозначены основные направления защиты информации в автоматизированной системе:

- Обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- Обеспечение защиты информации от хищения, утраты, уничтожения, искажения, подделки и блокирования доступа к ней в результате несанкционированного доступа (НСД).

ГЛАВА 3. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ПРИ ЕЕ ОБРАБОТКЕ, ХРАНЕНИИ И ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ

3.1. Средства защиты информации от утечки по техническим каналам

Защита конфиденциальной информации от утечки по техническим каналам является неременным условием для обеспечения информационной безопасности организации. Для достижения этой цели необходимо применять комплекс организационных и технических мероприятий, которые в совокупности формируют систему технической защиты информации на защищаемом объекте.

3.1.1. Организационные меры по защите информации

Организационная защита конфиденциальной информации представляет собой комплекс мер, основанных на процедурных и административных методах, которые регулируют процессы работы с важными данными, включая их хранение, передачу и обработку.

Для данного объекта информатизации используются следующие организационные меры защиты информации:

- Утверждена модель угроз и модель нарушителя;
- Утвержден и введен журнал учета машинных носителей;
- Утвержден и введен журнал регистрации и учета входящей и исходящей конфиденциальной информации;
- Утверждена политика информационной безопасности в компании;
- Утверждено положение о парольной защите;
- Утвержден перечень информации, составляющей коммерческую тайну;
- Утвержден перечень обрабатываемых персональных данных;
- Утвержден перечень лиц, допущенных к коммерческой тайне;
- Утвержден перечень лиц, допущенных к обработке персональных данных;
- Утверждены и введены должностные обязанности;

- Утвержден договор о неразглашении коммерческой тайны для сотрудников;
- Утверждено соглашение о неразглашении информации;
- Назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по защите информации, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением требований по безопасности;
- Утвержден порядок разграничения прав доступа к информационным ресурсам;
- Утверждена инструкция о порядке обращения с информацией, составляющей коммерческую тайну;
- Организована физическая защита помещений (вход в компанию осуществляется посредством пропуска и ключа, установлены видеокамеры, помещение оборудовано охранной и пожарной сигнализацией).

3.1.2. Технические средства защиты информации

Технические средства защиты информации – это специальные устройства, которые обеспечивают безопасность информации при помощи аппаратных средств.

Эффективная техническая защита информации является крайне важным элементом комплексной системы обеспечения информационной безопасности и способствует оптимизации финансовых затрат на организацию защиты информации.

Для эффективного решения задач технической защиты информации необходимо иметь квалифицированных специалистов в области защиты информации и специальные устройства, способные обнаруживать и блокировать потенциальные каналы утечки информации. Выбор специальных устройств определяется на основе анализа актуальных угроз и степени защищенности объекта информатизации.

Исходя из настоящей Модели угроз, была выявлена актуальная угроза безопасности информации, реализация (возникновение) которой может привести

к нарушению безопасности, обрабатываемой в автоматизированной системе и сетях информации:

- Угроза утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Утечка информации за счет перехвата ПЭМИН является одной из наиболее вероятных и скрытых угроз в системах обработки данных. Частотный диапазон ПЭМИН, сопровождающих информативные сигналы, находится в диапазоне от 10 кГц до 2 ГГц и определяется тактовой частотой используемого средства обработки информации [6]. Дальность распространения ПЭМИН может достигать до 1000 метров. Потенциально опасными источниками ПЭМИН являются компьютерные мониторы, проводные линии связи и накопители на магнитных дисках.

С точки зрения утечки информации опасным режимом работы средства вычислительной техники (СВТ) является вывод на экран монитора информации, которую можно перехватить специальным оборудованием на удалении до 1000 метров.

Средства вычислительной техники – это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [7].

Источниками побочных электромагнитных излучений в автоматизированной системе являются все линии и СВТ, в которых присутствуют электрические сигналы.

На рисунке 21 показаны технические средства разведки побочных электромагнитных излучений (ТСР ПЭМИ), которые могут быть находиться в близлежащих зданиях или в автомобилях, расположенных за пределами контролируемой зоны.

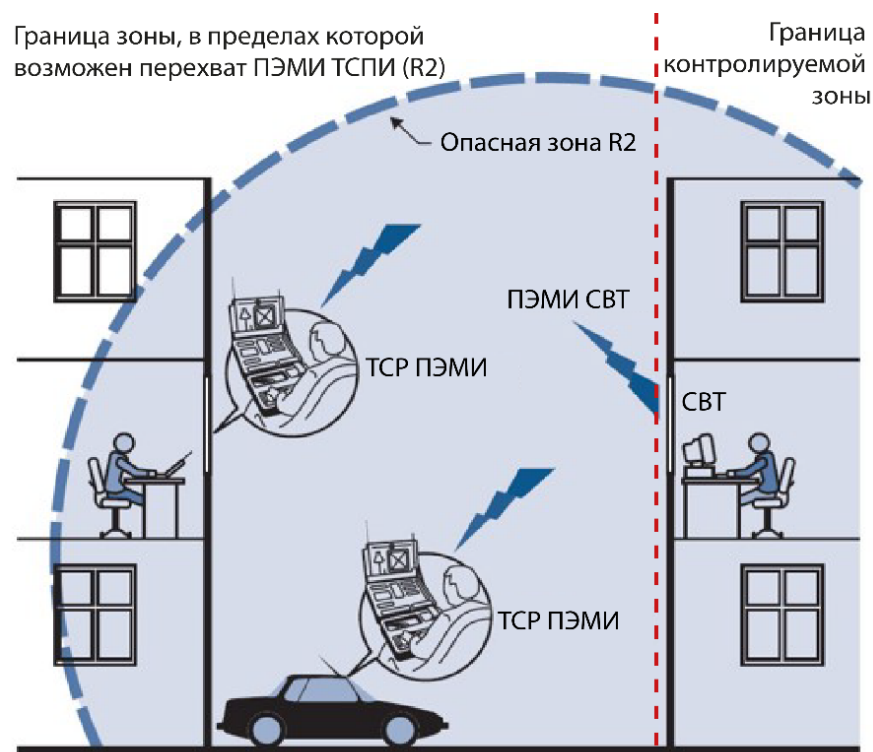


Рисунок 21 – Перехват побочных электромагнитных излучений ТСПИ средствами разведки ПЭМИН

Для перехвата побочных электромагнитных излучений СВТ используются специальные стационарные, перевозимые и переносимые приёмные устройства, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок.

Побочные электромагнитные излучения ТСПИ являются причиной возникновения электромагнитных и параметрических каналов утечки информации, а также могут оказаться причиной возникновения наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому снижению уровня побочных электромагнитных излучений уделяется большое внимание.

Эффективность системы защиты основных и вспомогательных технических средств от утечки информации по техническим каналам представляет собой многогранный анализ, основанный на различных критериях. Один из важных критериев — это отношение сигнал/шум, которое определяется физическими характеристиками информационного сигнала.

Защита информации от утечки через ПЭМИН осуществляется с помощью пассивных и активных методов и средств. Классификация методов защиты информации от утечки по каналу ПЭМИН представлена на рисунке 22.

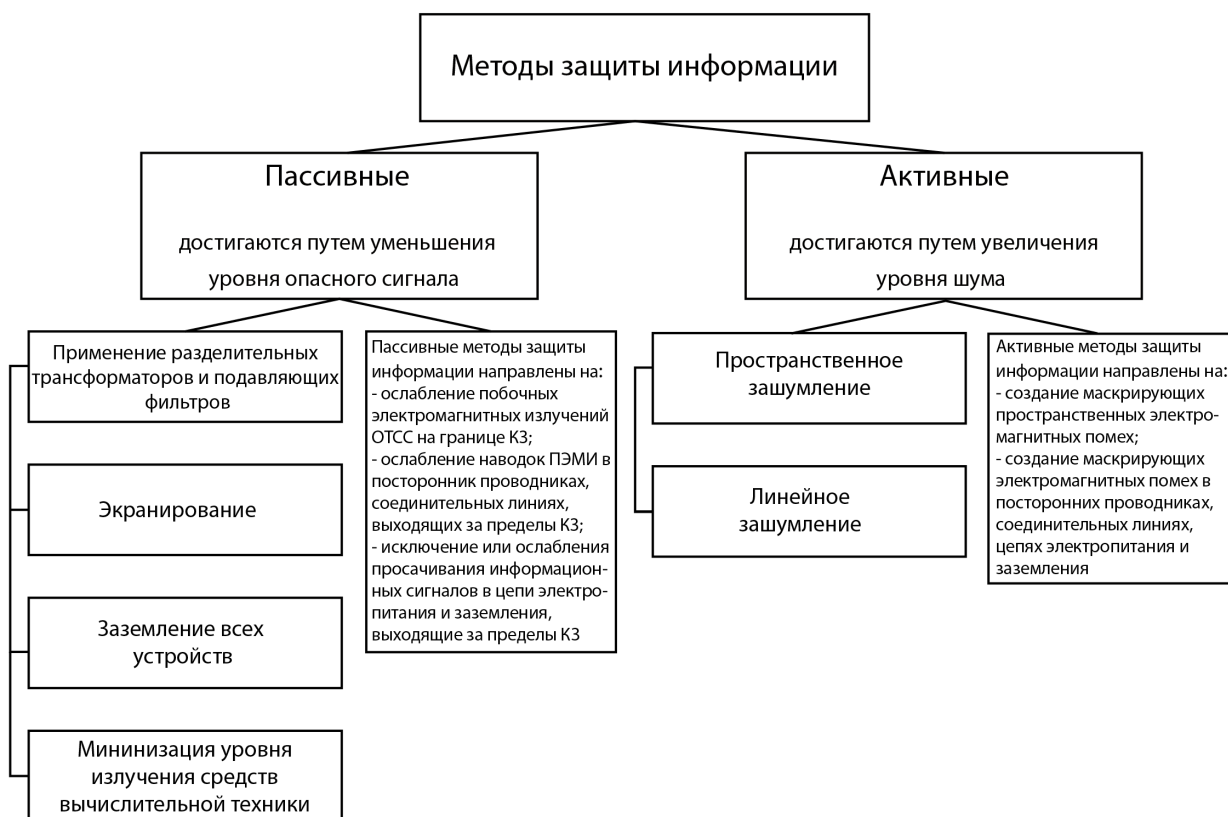


Рисунок 22 – Классификация методов защиты информации от утечки по каналу ПЭМИН

Активный метод защиты информации достигается путем перекрытия полезного сигнала более мощным шумом. Генератор шума специально создает мощные электромагнитные излучения, которые не имеют никакой информативной ценности и делают практически невозможным съём полезного сигнала. Стоит обратить внимание, что генератор шума имеет свои недостатки, такие как:

- Мощный источник излучения вреден для здоровья;
- Присутствие маскирующих средств защиты говорит о наличии конфиденциальной информации.

Пассивный метод защиты информации достигается путем уменьшения мощности излучаемого сигнала.

Таким образом, наиболее оптимальным решением в соотношении цена/качество является комбинированный подход, с использованием активного и пассивного метода защиты информации.

На рисунке 23 показана наглядная схема работы активных и пассивных методов защиты от утечки информации по каналу ПЭМИН.

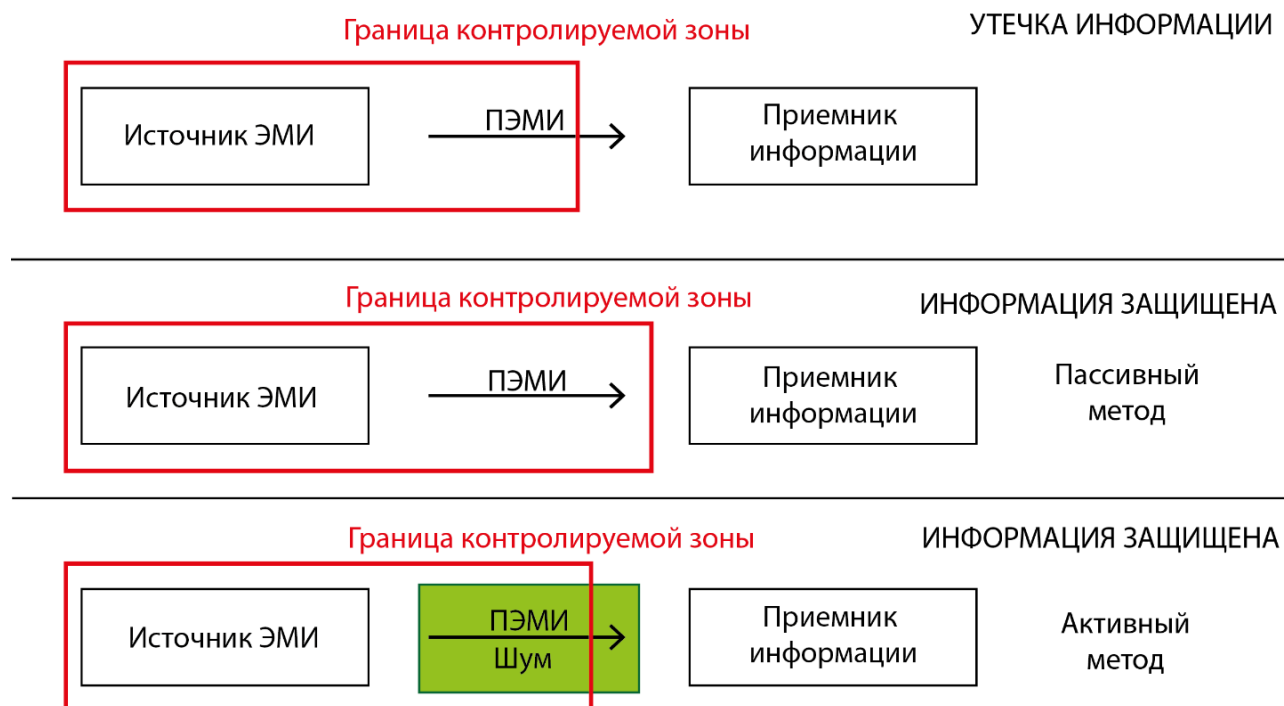


Рисунок 23 – Схема работы методов защиты от утечки информации по каналу ПЭМИН

3.2. Оценка защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от ее утечки по каналу побочных электромагнитных излучений и наводок

Для выбора оптимальных средств технической защиты информации необходимо провести оценку защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от ее утечки по каналу побочных электромагнитных излучений.

Для проведения оценки защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы в своей работе, буду использовать методику оценки защищённости конфиденциальной информации от утечки по техническим каналам.

Опасная зона R2 представляет собой область вокруг СВТ, где напряженность электрической или магнитной составляющей электромагнитного поля информативного сигнала превышает допустимое значение.

Опасная зона r1 представляет собой область вокруг СВТ, где на границе и за пределами которого уровень наведенного от СВТ информативного сигнала в сосредоточенных антеннах не превышает допустимого (нормированного) значения [8].

При проведении оценки защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от ее утечки по каналу побочных электромагнитных излучений необходимо произвести измерения следующих физических величин:

- напряженность электромагнитного поля по электрической составляющей (E);
- напряжение в линиях и токоведущих конструкциях (U);
- тактовые частоты работы технических средств (f).

Для оценки защищенности информации, обрабатываемой на ОТСС в составе, АС от утечки по каналу ПЭМИ необходимо убедиться, что требуемый радиус контролируемой зоны – R, меньше чем существующий радиус контролируемой зоны — Rкз. Если данное условие выполняется, ОТСС можно считать защищенным от утечки информации по каналу ПЭМИ.

Для проведения оценки защищенности использовалось следующее измерительное оборудование, которое представлено в таблице 10.

Таблица 10 – Перечень оборудования для проведения оценки защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от ее утечки по каналу побочных электромагнитных излучений и наводок

№	Названия средств измерений и вспомогательного оборудования	Диапазон частот
Измерительное оборудование		

№	Названия средств измерений и вспомогательного оборудования	Диапазон частот
1.	R&S®Spectrum Rider FPH Портативный анализатор спектра	5 кГц – 44 ГГц
2.	Осциллограф цифровой запоминающий ADS-2102	До 100 МГц
3.	Антенна измерительная рамочная АИР 3-2	9 кГц – 30 МГц
4.	Многофункциональное поисковое устройство ST-031 «ПИРАНЬЯ»	-
4.1.	Основной блок	
4.2.	Программное обеспечение «ST131.S ANALYZER – PRO»	-
4.3.	СВЧ антенна – детектор «ST131.S.SHF»	4000 – 18000 МГц
4.4.	Датчик магнитного поля «ST131.S.MF»	770 – 16нМ (полоса 0,001 – 5 МГц)
Вспомогательное оборудование		
5	Соната – РК1	0,01 – 1000 МГц

Многофункциональный поисковый прибор ST-031 «Пиранья» предназначен для эффективного обнаружения и локализации специальных технических средств (СТС), которые могут быть использованы для негласного сбора информации. Этот прибор также способен выявлять естественные и искусственно созданные каналы утечки информации, а также осуществлять контроль качества защиты информации. ST-031 представляет собой инновационное устройство, объединяющее в себе широкий спектр функций и возможностей. Несмотря на свою компактность, прибор обладает высокой чувствительностью и точностью обнаружения, что позволяет эффективно выполнять контрольно-поисковые задачи. На рисунке 24 показан общий вид ST-031 «Пиранья».



Рисунок 24 – Общий вид ST-031 «Пиранья»

На рисунке 25 изображена типовая схема расчетно-инструментального метода оценки защищенности СВТ от утечки информации, возникающей за счет ПЭМИ.

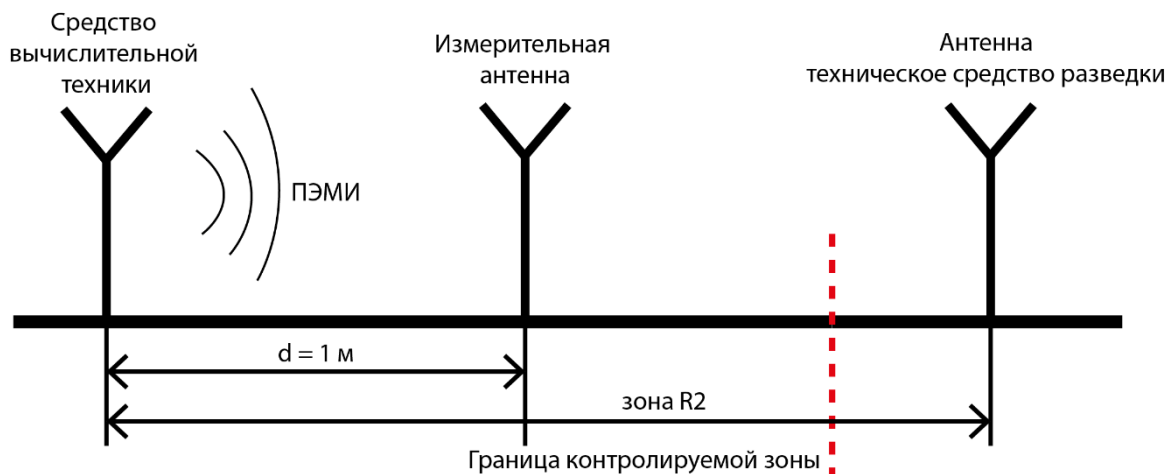


Рисунок 25 – Типовая схема расчетно-инструментального метода оценки защищенности СВТ от утечки информации, возникающей за счет ПЭМИ

Для расчета зон перехвата побочных электромагнитных излучений и наводок средств в данной работе используются методические документы в открытом доступе, позволяющие провести расчет в учебных целях [9].

Перехват ПЭМИ СВТ возможен при наличии следующих условий:

– расстояние от СВТ до границы контролируемой зоны должно быть менее зоны R2

$$R_{кз} \leq R2, \quad (1)$$

где $R_{кз}$ – длина исследуемого отрезка до граница контролируемой зоны, м;

– в пределах опасной зоны R2 возможно размещение средств разведки ПЭМИН.

Максимально возможный уровень напряженности поля информативного сигнала ПЭМИ рассчитывается по формуле

$$E_{ci} = \sqrt{E_{вкл.i}^2 - E_{выкл.i}^2}, \quad (2)$$

Где E_{ci} – максимально возможный уровень напряженности поля информативного сигнала ПЭМИ за период измерения на i -й частоте, мкВ/м; $E_{вкл.i}$ – измеренное значение напряженности поля информативного сигнала ПЭМИ на i -й частоте ОТСС в включенном состоянии при нагрузке, мкВ/м; $E_{выкл.i}$ – измеренное значение напряженности поля на i -й частоте ОТСС в выключенном состоянии, мкВ/м.

При измерении уровней напряженности поля сигналов ПЭМИ в зависимости от длины волны, используется понятие ближней, средней и дальней зон. Это связано с различной характеристикой распространения сигнала и взаимодействия антенны с полем.

Ближняя зона ограничена расстоянием от излучателя $R = \lambda_i/2\pi$, где $\lambda_i = \frac{300}{f_i}$. Дальняя зона начинается с расстояния $R_i > 6 \lambda_i$. Промежуточная зона ограничена расстоянием $\lambda_i/2\pi < R_i < 6 \lambda_i$.

Расстояние R_i для каждой частоты рассчитывается по формуле

$$R_i = \frac{L_i}{t \sqrt{\frac{k * E_{выкл.i}}{E_{ci}}}}, \quad (3)$$

Где R_i – максимальная длина исследуемого отрезка, на котором возможно выделение информативного сигнала, м; L_i – расстояние от ОТСС до границы

ближней, промежуточной или дальней зоны, м; t – коэффициент значения зоны; k – константное значение.

Расчет наводок на линии ОТСС проводится по следующей формуле

$$U_{ci} = 20 \lg \sqrt{10^{U(c+\text{ш})_i/10}} - 10^{U_{\text{ш}i}/10}, \quad (4)$$

Где U_{ci} – значение напряженности в точке присоединения измерительного прибора, дБ; $U(c + \text{ш})_i$ – значение смешанного напряжения обнаруженных компонентов нагрузки и шума, дБ; $U_{\text{ш}i}$ – значение напряженности шума в линии.

В таблицах 11 и 12 приведены оценочные значения ПЭМИН. Приведенные данные необходимы для определения значений радиусов зоны R2 и r1.

Протокол измерений и расчетов показателей ПЭМИН представлен в приложении Г.

Таблица 11 – Оценка ПЭМИ

№ п/п	f, МГц	Ес, дБ	Е _{выкл} , дБ	Е _{с+выкл} , дБ	R, м
АРМ №1					
1	51,4	67,7	58,5	67,7	10,54
2	254,31	54,3	28,7	54,3	9,6
3	311,2	57,4	39,7	68,4	14,9
4	568,8	49,7	48,5	49,7	5,7
АРМ №2					
1	51,4	68,5	68,2	67,5	10,52
2	254,31	47,3	28,9	47,3	9,21
3	311,2	52,6	47,4	52,6	13,8
4	568,8	44,9	25,4	44,9	5,1
АРМ №3					
1	51,4	71,6	36,5	61,6	9,6
2	254,31	29,5	23,8	30,5	10,1
3	311,2	38,4	26,1	38,6	13,2
4	568,8	41,6	22,4	41,8	4,9
АРМ №4					
1	51,4	55,8	27,7	55,8	10,7
2	254,31	33,2	25,6	33,6	10,2
3	311,2	41,2	28,9	41,6	13,7
4	568,8	48,1	29,4	48,1	5,6
АРМ №5					
1	51,4	62,4	41,2	62,4	10,8
2	254,31	46,8	22,4	49,0	10,1
3	311,2	33,5	31,8	33,5	12,6

№ п/п	f, МГц	E _c , дБ	E _{выкл} , дБ	E _{c+выкл} , дБ	R, м
4	568,8	36,4	29,3	36,4	5,4
АРМ №6					
1	51,4	57,2	36,5	57,2	9,48
2	254,31	38,5	26,6	39,1	5,7
3	311,2	36,4	24,5	36,4	10,5
4	568,8	46,9	33,8	47,2	3,6

Таблица 12 – Оценка наводок ПЭМИ

№	f, МГц	U(c+ш) _i , дБ	Uш _i , дБ	U _c _i , дБ	U _{1изм} _i , мкВ	U _{2изм} _i , мкВ	K _p _i , дБ/м	R _i , м
АРМ №1								
1	51,4	48	12	13,55	201,5	6,8	2	5,75
2	254,31	61	16	17,4	167,4	5,7	2,5	5,7
АРМ №2								
1	51,4	54	22	13,54	241,6	6,2	2,6	5,8
2	254,31	60	18	21,7	111,8	5,2	1,6	10,9
АРМ №3								
1	51,4	48	20	21,8	195,8	7,5	1,9	4,7
2	254,31	63	24	26,2	223,7	7,1	2,2	5,5
АРМ №4								
1	51,4	65	14	17,4	184,6	5,1	2,5	5,3
2	254,31	62	15	16,87	267,2	6,6	1,9	6,2
АРМ №5								
1	51,4	61	17	19,2	154,3	7,6	1,75	7,1
2	254,31	59	24	27,7	198,6	5,9	2,5	5,48
АРМ №6								
1	51,4	54	20	26,3	297,2	5,2	2,1	7,8
2	254,31	62	18	19,7	125,9	7,6	2,5	4,68

На рисунке 26 показано выполнение практической части работы.

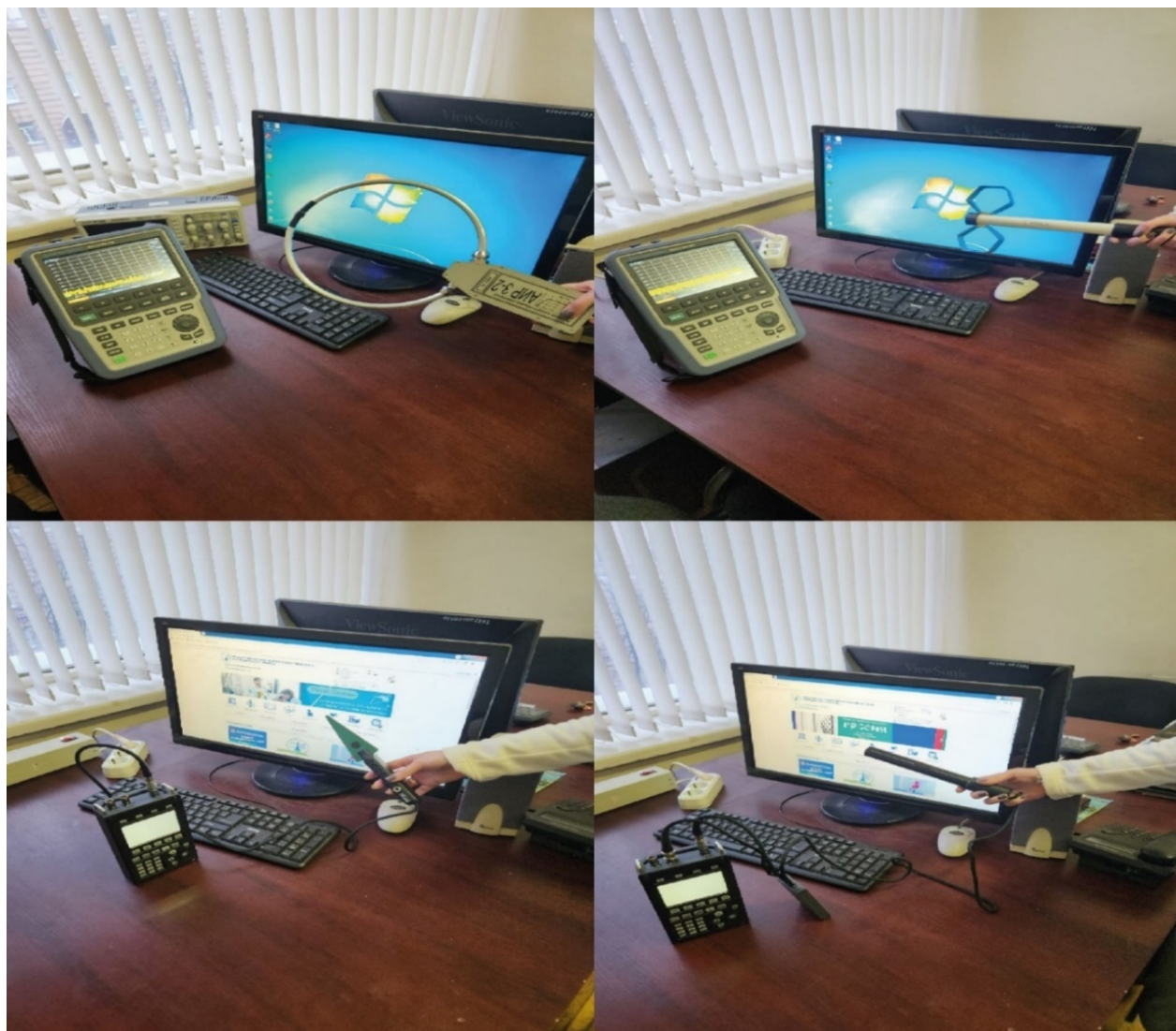


Рисунок 26 – Практическое выполнение измерений ПЭМИН

По результатам измерений радиус зоны $R_2 = 14,9$ метров. Радиус зоны $r_1 = 10,9$ метров. Минимальное расстояние от СВТ объекта до границы контролируемой зоны составляет $R_{кз} = 10$ метров. Данные показатели удовлетворяют соотношению (1). Другими словами, полученные значения говорят о том, что условия защищенности информации от утечки по каналу ПЭМИН не выполняются.

Вывод: условия защищенности информации от утечки по каналу ПЭМИН не выполняются, так как рассчитанный требуемый радиус контролируемой зоны больше минимального расстояния от ОТСС до существующей границы контролируемой зоны. Необходимо применение средств защиты.

Таким образом, предложенная математическая модель обнаружения побочных электромагнитных излучений СВТ позволила оценить возможность перехвата ПЭМИ СВТ средствами разведки и обосновать использование на объекте информатизации технических средств защиты информации.

Технические средства защиты информации (ТСЗИ) – это различные аппаратные устройства, включающие в себя инженерные, механические или электронные компоненты, которые предназначены для решения задач по защите информации. Они либо исключают возможность утечки информации через различные каналы, либо обеспечивают ее защиту с помощью различных технических методов.

Определяющими факторами при выборе ТСЗИ являются минимально достаточные технические характеристики и стоимость. Характеристики ТСЗИ от ПЭМИН представлены в таблице 13.

Таблица 13 – Характеристики ТСЗИ от ПЭМИН

Технические характеристики	СОНАТА – РК1	ЛГШ – 501
Диапазон частот	0,01 – 1000 МГц	0,01 – 1800 МГц
Электропитание	220 В, 50 Гц	220 В, 50 Гц
Габаритные размеры	142×60×167	230×100×45
Режим работы	Круглосуточно	Круглосуточно
Стоимость	14 000 руб.	18 880 руб.

Таким образом, из числа рассмотренных технических средств защиты от ПЭМИН, преимуществом обладает ТСЗИ от ПЭМИН СОНАТА – РК1. Определяющие факторы – наименьшая стоимость и достаточные технические характеристики.

Устройство комбинированной защиты «Соната-РК1» предназначено для защиты информации, обрабатываемой основными техническими средствами и системами, от утечки по каналу ПЭМИН путем постановки маскирующих помех в линиях электропитания и заземления, а также путем пространственного

зашумления и частичного поглощения информативных сигналов, распространяющихся по линиям электропитания и заземления.

На рисунке 27 показано выполнение практической части работы с применением технического средства защиты информации «СОНАТА – РК1».



Рисунок 27 – Практическое выполнение измерений ПЭМИН с применением технического средства защиты информации «СОНАТА – РК1»

По результатам измерений и расчетам зон с применением «СОНАТА – РК1» радиус требуемой контролируемой зоны $R_2 = 5$ метров. Минимальное расстояние от СВТ объекта до границы контролируемой зоны составляет $R_{кз} = 10$ метров. Полученные значения говорят о том, что требуемый радиус контролируемой зоны меньше минимального расстояния от ОТСС до существующей границы контролируемой зоны.

Вывод: Зоны активного зашумления, рассчитанные для устройства «СОНАТА – РК1», превышают требуемый радиус контролируемой зоны для всех

составляющих спектра информативного сигнала. Условия защищенности информации от утечки по каналу ПЭМИН выполняются.

3.3. Обеспечение защиты информации от хищения, утраты, уничтожения, искажения, подделки и блокирования доступа к ней в результате НСД

Несанкционированный доступ (НСД) — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

На основании предпроектного обследования, в рамках данной работы были выявлены следующие угрозы, связанные с несанкционированным доступом:

1. Несанкционированный доступ лиц к объекту информатизации;
2. Несанкционированный доступ к каналам связи.

От угрозы, связанной с несанкционированным доступом лиц к объекту информатизации, был разработан комплекс мероприятий, направленных на минимизацию вероятности реализации выявленных угроз:

- Разработана матрица доступа субъектов автоматизированной системы к ее защищаемым информационным ресурсам (Приложение В);
- Внедрена система видеонаблюдения (рис.17);
- Внедрена система контроля управления доступом (рис.18);
- Установлено средство защиты информации (СЗИ) от НСД.

Сертифицированные СЗИ от НСД на российском рынке пользуются высоким спросом. Это связано с необходимостью выполнения действующего законодательства и нормативных актов в области защиты информации:

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и другие.

Характеристики СЗИ от НСД представлены в таблице 14.

Таблица 14 – Характеристики СЗИ от НСД

Критерии сравнения	СЗИ от НСД «Secret Net Studio 8.10»	СЗИ от НСД «Dallas Lock 8.0-K»	СЗИ от НСД «Блокхост-Сеть 4»
Класс АС	до 1Г включительно	До 1Г включительно	До 1Г включительно
Совместимость в Windows 10	+	+	+
Наличие сертификата соответствия ФСТЭК	№ 3745 от 16 мая 2017 г., срок действия продлен до 16 мая 2025 г.	№ 2720 от 25 сентября 2012 г., срок действия продлен до 25 сентября 2026 г.	№ 4374 от 11 марта 2021 г., действителен до 11 марта 2026 г.
Цена	6700 руб.	7500 руб.	8650 руб.

Подводя итог, из числа рассмотренных средств защиты информации от НСД, преимуществом обладает СЗИ от НСД «Secret Net Studio 8.10». Определяющие факторы – наименьшая стоимость и достаточные технические характеристики.

3.4. Оценка эффективности применяемых мер и средств защиты информации

Эффективность принятых мер, обеспечивающих безопасность информации определяется по следующим критериям:

1. Уровень надежности: основным условием сохранения данных является эффективно выстроенные уровни ее защиты, которые последовательно обеспечивают предотвращения несанкционированного доступа, атак и прочих незаконных действий.

2. Эффективность системы: зависит от нескольких ключевых факторов, включая скорость и эффективность в предотвращении атак, возможность оперативно реагировать на потенциальные атаки и минимизировать воздействие на конфиденциальную информацию.

3. Соблюдение нормативно-правовой базы: юридическая защита данных.

4. Соотношение стоимости и эффективности: оно подразумевает, что система должна быть признана целесообразной, принимая во внимание как стоимость реализации и внедрения системы, так и затраты на поддержку и

обслуживание. Система безопасности должна достигать баланса между затратами и достигаемыми результатами.

Для эффективного применения технических средств защиты информации от утечки по техническим каналам, необходимо производить оценку и контроль защищенности информации, обрабатываемой на ОТСС в составе АС от утечки по каналу ПЭМИ и за счет наводок информативного сигнала на цепи электропитания и заземления, выходящие за пределы КЗ.

После проведения оценки защищенности информации, которая обрабатывается на ОТСС в составе АС от утечки по каналу ПЭМИ, выяснилось, что требуемый радиус КЗ превышает реальное расстояние до границы контролируемой зоны при:

- просмотре информации на экран монитора с интерфейсом DVI на частоте 311,2 МГц – 68,4 дБ.

В результате проведения оценки защищенности информации, которая обрабатывается на ОТСС в составе АС от утечки за счет наводок информативного сигнала на цепи электропитания и заземления, выходящие за пределы КЗ, было определено, что максимальная длина пробега линии электропитания и заземления, на которой возможно выделение информативного сигнала больше длины реального пробега линий электропитания и заземления до ближайшей границы КЗ при:

- наводках информативного сигнала на цепь электропитания во время просмотра информации на экран монитора с интерфейсом DVI на частоте 254 МГц – 21 дБ.

Для защиты информации, обрабатываемой на объекте информатизации было применено устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН «СОНАТА – РК1».

После применения ТСЗИ от утечки по ТКУИ — устройства комбинированной защиты «Соната-РК1», в электромагнитном поле уровень шума стал равен 70 дБ. Все ОТСС в составе защищаемой АС находятся в пределах зоны электромагнитного поля шума, созданного генератором шумового

электромагнитного излучения. Это значит, что все сигналы, при которых защищенность информации, обрабатываемой в ОТСС, от утечек по каналу ПЭМИ и за счет наводок на токопроводящие цепи не выполняется будут замаскированы электромагнитным сигналом шума.

В результате использования ТСЗИ от утечки по ТКУИ, информация, которая обрабатывается на ОТСС в составе АС, считается защищенной от утечки по каналу ПЭМИ и за счет наводок информативного сигнала на цепи электропитания и заземления, выходящие за пределы КЗ, так как напряжение шума, созданного устройством комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН «СОНАТА – РК1», больше напряжения создаваемого смесью тест-сигнала и шума в линиях, что соответственно больше напряжения создаваемого тест-сигналом, что показано в таблицах 15 и 16, где:

- $E(c + \text{ш})_{\max}$ – максимальное значение смешанного напряжения обнаруженных компонентов нагрузки и шума, дБ;
- $U(c + \text{ш})_{\max}$ – максимальное смешанное напряжение обнаруженных компонентов нагрузки и шума, дБ;
- $E_{\text{ш}}$ – напряженность электромагнитного поля, созданная за счет шума, дБ.

Таблица 15 – Результат оценки защищенности информации обрабатываемой ОТСС в составе АС от утечки по каналу ПЭМИ

Режим обработки информации на техническом средстве	f, МГц	$E(c + \text{ш})_{\max}$, дБ	$E_{\text{ш}}$, дБ
Просмотр информации на экран монитора (интерфейс DVI)	51,4	64	70
	254,31	38	
	311,2	68	
	568,8	55	

Таблица 16 – Результат оценки защищенности информации, обрабатываемой на ОТСС в составе АС от утечки за счет наводок информативного сигнала на цепи электропитания и заземления

Режим обработки информации на техническом средстве	f, МГц	Цепь	$U(c + ш)_{max}$, дБ	Еш, дБ
Просмотр информации на экран монитора (интерфейс DVI)	51,4	Электропитания	23	70
		Заземления	21	
	254,31	Электропитания	47	
		Заземления	59	
	311,2	Электропитания	62	
		Заземления	49	
	568,8	Электропитания	68	
		Заземления	56	

Для наглядного представления оценки эффективности применяемых мер и средств защиты информации на рисунке 28 представлен график результатов оценки защищенности информации обрабатываемой ОТСС в составе АС от утечки по каналу ПЭМИН. На графике отображаются максимальные значения уровня шума без применения специального технического средства защиты информации от утечек по каналу ПЭМИН и значения уровня шума после внедрения устройства комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН «СОНАТА – РК1».

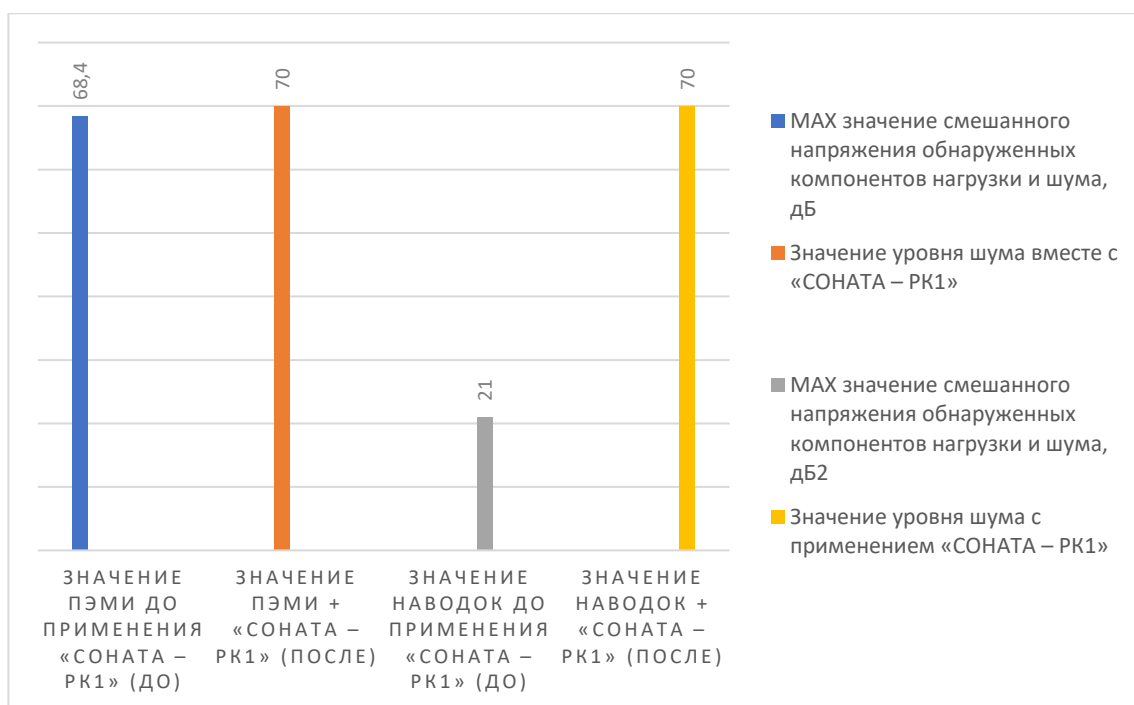


Рисунок 28 – График результатов оценки защищенности информации обрабатываемой ОТСС в составе АС от утечки по каналу ПЭМИН

Таким образом, вместе с технической защитой потенциальных каналов утечки информации, для повышения эффективности системы защиты информации в строительной компании были установлены и внедрены следующие средства:

- СЗИ от НСД «Secret Net Studio 8.10»;
- разработана матрица доступа субъектов автоматизированной системы к ее защищаемым информационным ресурсам;
- внедрена система видеонаблюдения и система контроля управления доступом.

Спецификация выбранных средств защиты информации от утечки по техническим каналам представлена в таблице 17.

Таблица 17 – Спецификация выбранных средств защиты информации от утечки по техническим каналам

Наименование товара	Тип	Цена, руб.	Количество, шт.	Сумма, руб.
Устройство комбинированной защиты объектов	«СОНАТА – РК1»	14 000 руб.	6	84 000 руб.

Наименование товара	Тип	Цена, руб.	Количество, шт.	Сумма, руб.
информатизации от утечки информации за счет ПЭМИН				
СЗИ от НСД	«Secret Net Studio 8.10»	6700 руб.	6	40 200 руб.
Пакет расширенной технической поддержки на 1-год	«Secret Net Studio 8.10»	1320 руб.	1	1320 руб.
Итого				125 520 руб.

На рисунке 29 показана схема рекомендуемого расположения средств защиты информации.



Рисунок 29 – Схема рекомендуемого расположения средств защиты информации

3.5. Выводы по 3 главе

В главе представлены результаты оценки защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от ее утечки по каналу побочных электромагнитных излучений и результаты оценки эффективности применяемых мер и средств защиты информации. По результатам оценки установлено, что

защищенность информации от утечки по каналу ПЭМИН выполняется, так как требуемый радиус контролируемой зоны меньше минимального расстояния от ОТСС до существующей границы контролируемой зоны.

Исходя из полученных результатов, была проведена оценка эффективности применяемых мер и средств защиты информации, которая позволила оценить защищенность информации, обрабатываемой в технических средствах в составе автоматизированной системы от утечек по техническим каналам. В результате оценки эффективность подтвердилась.

Для повышения эффективности системы защиты информации было применено устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН «СОНАТА – РК1» и установлено СЗИ от НСД «Secret Net Studio 8.10», также были определены необходимые организационные меры по защите информации.

ЗАКЛЮЧЕНИЕ

Выпускная квалификационная работа посвящена повышению эффективности системы защиты информации в строительной компании от утечки по техническим каналам за счет применения специальных технических средств защиты. По результатам исследований, проведенных в рамках поставленной задачи, были получены следующие результаты.

В ходе работы был проведен детальный анализ объекта информатизации, в результате чего были определены и подробно описаны потенциальные технические каналы утечки информации в защищаемой автоматизированной системе. На основе проведенного анализа было принято решение о выборе определенных средств обнаружения технических каналов утечки конфиденциальной информации, которые были применены с целью оценки защищенности обрабатываемой информации в основных технических средствах, входящих в состав автоматизированной системы.

Для проведения оценки защищенности информации, обрабатываемой техническими средствами в составе автоматизированной системы, в настоящей работе была использована методика оценки защищённости конфиденциальной информации от утечки по техническим каналам.

Таким образом, для повышения эффективности системы защиты информации в строительной компании от утечки по техническим каналам были определены необходимые организационные меры по защите информации и выбраны технические средства защиты информации – устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН «СОНАТА – РК1» и СЗИ от НСД «Secret Net Studio 8.10».

После применения защитных мер была выполнена оценка эффективности использованных мер и средств защиты информации, в результате которой определено, что защищенность информации, обрабатываемой в технических средствах в составе автоматизированной системы от утечек по техническим каналам, выполняется.

Защита информации от утечки по техническим каналам является одной из наиболее значимых задач в современном информационном обществе. Работа строительных организаций тесно связана с обработкой и хранением конфиденциальных данных, поэтому эффективная организация защиты информации является необходимостью.

Подводя итог по проделанной работе, можно прийти к следующим выводам о том, что задачи, поставленные мною в начале работы, были решены, цель исследования достигнута.

Результаты исследования могут использоваться в практической деятельности строительных компаний для обеспечения безопасного обращения с конфиденциальной информацией.

СПИСОК ЛИТЕРАТУРЫ

1. Соколов, А. И. Технические средства защиты информации: технические каналы утечки информации : учеб. пособие / А. И. Соколов, М. Ю. Монахов ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2006. – 71 с. (Комплексная защита объектов информатизации. Кн. 13 / под ред. М. Ю. Монахова).
2. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 20.10.2023).
3. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 20.10.2023).
4. ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения (с Поправкой) : официальное издание М.: Стандартинформ, 2009.
5. Банк данных угроз безопасности информации Список терминов // <https://bdu.fstec.ru/ubi/terms/terms/index> (дата обращения: 24.10.2023).
6. Бузов Г.А. Защита от утечки информации по техническим каналам / Бузов Г.А., Калинин С.В., Кондратьев А.В. – М.: Горячая линия - Телеком, 2002. – 415 с.
7. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования : официальное издание М.: Издательство стандартов, 1995.
8. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники. [Электронный ресурс]. – Режим доступа: <http://www.bnti.ru/showart.asp?aid=954&lvl=04.03> (дата обращения 04.12.2023).
9. Хорев А.А. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера // Доклады ТУСУР. 2014. №2 (32). [Электронный ресурс]. – Режим доступа: <http://cyberleninka.ru/article/n/otsenka-vozmozhnosti-obnaruzheniya-pobochnyh-elektromagnitnyh-izlucheniyyvideosistemy-kompyuter> (дата обращения 04.12.2023).

Приложение А
УТВЕРЖДАЮ

Директор

ООО «Строительная компания»

_____/И.И. Иванов

« » _____ 2022 г.

Модель угроз безопасности информации

Санкт-Петербург

2022

1. Общие положения

Модель угроз описывает уровень исходной защищенности информационной системы, в которой производится обработка информации, составляющей коммерческую тайну и персональные данные, описание угроз информационной безопасности и определяет актуальные угрозы.

Данная модель угроз разработана на основании:

- Методика оценки угроз безопасности информации (ФСТЭК России, 2021 г.);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.);
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»;
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Основные виды угроз безопасности

2.1 Угрозы утечки по техническим каналам

В процессе обработки персональных данных (далее - ПДн) и коммерческой тайны (далее - КТ) в Автоматизированной системе (далее - АС) существует возможность нарушения безопасности ПДн и КТ за счет реализации следующих угроз:

- 1) угрозы утечки акустической (речевой) информации;
- 2) угрозы утечки видовой информации;
- 3) угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (далее – ПЭМИН).

2.2 Угрозы несанкционированного доступа

Угрозы несанкционированного доступа (далее – НСД) в АС с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного, доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн и КТ, и включают в себя:

- 1) угрозы НСД, связанные с действиями нарушителей, имеющих доступ к АС;
- 2) угрозы, осуществляемые с использованием протоколов сетевого взаимодействия, реализуемые внутри распределенной сети;

- 3) угрозы внедрения (в том числе по сети) вредоносных программ.

3. Источники угроз безопасности ПДн и КТ

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Источниками угроз НСД в АС могут быть:

- носитель вредоносной программы;
- аппаратная закладка;
- нарушитель.

4. Определение уровня исходной защищенности

При составлении перечня актуальных угроз безопасности ПДн и КТ каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1 , а именно:

- 0 для высокой степени исходной защищенности;
- 5 для средней степени исходной защищенности;
- 10 для низкой степени исходной защищенности.

Таблица 1 – Уровень исходной защищенности

Технические и эксплуатационные характеристики системы	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению			
Система, развернутая в пределах одного здания в пределах контролируемой зоны	+	–	–
2. По наличию соединения с сетями общего пользования			
Система, физически отделенная от сети общего пользования	–	+	–
3. По встроенным операциям со сведениями и разграничению прав доступа			
Чтение, поиск	+	–	–
Запись, удаление, сортировка	–	+	–
Модификация, передача	–	–	+
4. По разграничению доступа к ПДн и КТ			
Система, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем АС, либо субъект ПДн	–	+	–
Характеристики системы защиты	30%	60%	10%

Таким образом, система имеет средний ($Y_1=5$) уровень исходной защищенности, т.к. более 75% характеристик соответствуют уровню защищенности не ниже «среднего».

5. Определение актуальных угроз безопасности информации

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн и КТ для данной АС в складывающихся условиях обстановки.

Вводятся четыре вербальных градации этого показателя:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие СЗИ);

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2 , а именно:

- 0 для маловероятной угрозы;
- 2 для низкой вероятности угрозы;
- 5 для средней вероятности угрозы;
- 10 для высокой вероятности угрозы.

С учетом всего вышеизложенного коэффициент реализуемости угрозы Y будет определяться соотношением:

$$Y = (Y_1 + Y_2) / 20.$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признается низкой;
- если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признается средней;
- если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признается высокой;
- если $Y > 0,8$, то возможность реализации угрозы признается очень высокой.

Определение вероятности реализации угроз безопасности системы обработки информации представлено в таблице 2.

Таблица 2 – Модель угроз безопасности системы обработки информации

Тип угроз безопасности	Анализ угроз	Вероятность реализации (Y2)	Коэффициент реализуемости угрозы	Возможность реализации
1. Угрозы утечки по техническим каналам				
1.1 Угрозы утечки акустической информации	В системе отсутствует голосовое управление средствами обработки конфиденциальных сведений	Маловероятна (0)	0,25	Низкая
1.2 Угрозы утечки видовой информации	Проход в помещения, в которых ведется обработка конфиденциальных сведений организован по электронным пропускам. Лицам иных отделов в случае производственной необходимости разрешен проход в эти помещения в сопровождении уполномоченных сотрудников	Маловероятна (0)	0,25	Низкая
1.3 Угрозы утечки по каналам ПЭМИН	Имеются ВТСС и линии связи, выходящие за пределы помещений. А также линии связи,	Средняя (5)	0,5	Средняя

Тип угроз безопасности	Анализ угроз	Вероятность реализации (Y2)	Коэффициент реализуемости угрозы	Возможность реализации
	выходящие за пределы контролируемой зоны.			
2. Угрозы несанкционированного доступа к информации				
2.1 Кража ПЭВМ	Вынос ПЭВМ разрешен только техническим специалистом в сопровождении соответствующей документации	Маловероятна (0)	0,25	Низкая
2.2 Кража носителей информации	Доступ в помещения, в которых ведется обработка конфиденциальных сведений, ограничен организационными мерами	Маловероятна (0)	0,25	Низкая
2.3 Действия вредоносных программ (вирусов)	На АРМ установлено антивирусное ПО «Kaspersky». Пользователям запрещено производить отключение системы антивирусной защиты. Обновление баз выполняется регулярно	Маловероятно (0)	0,25	Низкая

Тип угрозы безопасности	Анализ угроз	Вероятность реализации (Y2)	Коэффициент реализуемости угрозы	Возможность реализации
2.4 Утрата атрибутов доступа	Доступ к информационным ресурсам в ЛВС организации ограничен логином и паролем ранее зарегистрированных пользователей. Пользователи проинструктированы о порядке действий в случае утраты или компрометации паролей.	Низкая (2)	0,35	Средняя
2.5 Непреднамеренная модификация, уничтожение информации сотрудниками	Резервное копирование осуществляется раз в неделю	Средняя (5)	0,5	Средняя
2.6 Сбой системы электроснабжения	Отсутствуют источники бесперебойного питания для каждого ключевого элемента	Средняя (5)	0,5	Средняя
2.7 Стихийное бедствие	План восстановления работы системы после сбоев регламентирован в нормативных документах	Низкая (2)	0,35	Средняя

Тип угрозы безопасности	Анализ угроз	Вероятность реализации (Y2)	Коэффициент реализуемости угрозы	Возможность реализации
2.8 Доступ лиц к модификации, уничтожению информации, не допущенных к ее обработке	Доступ в помещения, в которых ведется обработка конфиденциальных сведений, ограничен организационными мерами.	Низкая (2)	0,35	Средняя
2.9 Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	Сотрудники, допущенные к обработке сведений конфиденциального характера, ознакомлены о порядке работы и подписали Договор о неразглашении.	Средняя (5)	0,5	Средняя

Опасность угроз определяется по методическим в документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. приказом ФСТЭК России от 15.02.2008 г.). Оценка опасности угроз представлена в таблице 3.

Таблица 3 – Оценка опасности угроз

Тип угрозы безопасности	Опасность угрозы
1.1 Угрозы утечки акустической информации	Низкая
1.2 Угрозы утечки видовой информации	Низкая
1.3 Угрозы утечки по каналам ПЭМИН	Средняя
2.1 Кража ПЭВМ	Низкая
2.2 Кража носителей информации	Низкая
2.3 Действия вредоносных программ (вирусов)	Низкая
2.4 Утрата атрибутов доступа	Низкая

Тип угроз безопасности	Опасность угрозы
2.5 Непреднамеренная модификация, уничтожение информации сотрудниками	Средняя
2.6 Сбой системы электроснабжения	Средняя
2.7 Стихийное бедствие	Низкая
2.8 Доступ лиц к модификации, уничтожению информации, не допущенных к ее обработке	Низкая
2.9 Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	Средняя

Для определения угрозы как «актуальной», уровни ее опасности и возможности реализации, должны быть не ниже «среднего». Определение актуальности угрозы представлено в таблице 4.

Таблица 4 – Определение актуальности угрозы

Показатель опасности угрозы Возможность реализации угрозы	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Параметр актуальности рассмотренных угроз представлен в таблице 5.

Таблица – 5 Актуальность угроз

Тип угроз безопасности	Актуальность угрозы
1.1 Угрозы утечки акустической информации	Неактуальная
1.2 Угрозы утечки видовой информации	Неактуальная
1.3 Угрозы утечки по каналам ПЭМИН	Актуальная
2.1 Кража ПЭВМ	Неактуальная
2.2 Кража носителей информации	Неактуальная
2.3 Действия вредоносных программ (вирусов)	Неактуальная

Тип угроз безопасности	Актуальность угрозы
2.4 Утрата атрибутов доступа	Неактуальная
2.5 Непреднамеренная модификация, уничтожение информации сотрудниками	Актуальная
2.6 Сбой системы электроснабжения	Актуальная
2.7 Стихийное бедствие	Неактуальная
2.8 Доступ лиц к модификации, уничтожению информации, не допущенных к ее обработке	Неактуальная
2.9 Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	Актуальная

6. Основные угрозы безопасности информации

Таблица – 6 Основные угрозы безопасности информации

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
1	Осуществление несанкционированного доступа (ознакомления) с целевой информацией при ее обработке и хранении в АС	Пользователи АС	Осуществление доступа к целевой информации с использованием штатных средств, предоставляемых АС	Недостатки механизмов разграничения доступа к целевой информации, связанные с возможностью предоставления доступа к целевой информации	Целевая информация (в том числе персональные данные и коммерческая тайна)	Конфиденциальность	Несанкционированное ознакомление и разглашение коммерческой тайны и персональных данных, используемых в АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
				неуполномоченн ым на это лицам			
2	Осуществление несанкционирова нного копирования (хищения) информации, содержащей конфиденциальн ые сведения (в том числе баз данных АС)	Пользователи АС	Осуществление действий с использованием штатных средств (предоставляемы х АС), направленных на копирование (выгрузку) информации из баз данных АС	Недостатки механизмов безопасного взаимодействия АРМ пользователей с серверами АС	Целевая информаци я (в том числе персональн ые данные и коммерческ ая тайна)	Конфиденциаль ность	Несанкциониро ванное ознакомление и разглашение персональных данных и коммерческой тайны, используемых в АС
3	Осуществление необнаруженной	Пользователи АС	Осуществление необнаруженной	Недостатки механизмов	Целевая информаци	Целостность	Навязывание должностным

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	несанкционированной модификации (подмены) целевой информации (прежде всего, персональных данных и коммерческой тайны)		модификации (подмены) целевой информации с использованием штатных средств, предоставляемых АС	разграничения доступа к целевой информации и механизмов аудита, связанные с возможностью необнаруженной модификации (подмены) целевой информации неуполномоченн	я (в том числе персональн ые данные и коммерческ ая тайна)		лицам модифицирован ной (ложной) информации; передача по запросам модифицирован ной (ложной) информации и нарушение режимов функционирова ния АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
				ыми на это лицами			
4	Осуществление необнаруженного несанкционированного блокирования (нарушения доступности) целевой информации	Пользователи АС	Осуществление необнаруженного блокирования доступности целевой информации с использованием штатных средств АС, предоставляемых АС, а также с использованием специализирован	Недостатки механизмов безопасного администрирования сервисов, предоставляемых АС, а также механизмов аудита, связанные с возможностью бесконтрольного несанкциониров	Целевая информация (в том числе персональные данные и коммерческая тайна)	Доступность	Непредставление целевой информации заинтересованным лицам в отведенные временные интервалы; нарушение штатного режима функционирования АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
			ных инструментальны х средств	анного блокирования доступности целевой информации			
5	Перехват защищаемой информации в каналах связи (каналах передачи данных) с использованием специально разработанных технических	пользователи АС; уполномоченн ый персонал разработчиков АС, который на договорной основе имеет право на техническое	Перехват целевой и технологической информации с использованием специально разработанных технических средств и программного	Недостатки механизмов защиты передаваемой информации, связанные с возможностью ее перехвата из каналов связи и последующего с	Целевая информация (в том числе персональн ые данные и коммерческ ая тайна)	Конфиденциаль ность	Несанкциониро ванное ознакомление и разглашение персональных данных и коммерческой информации, используемых в АС;

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	средств и программного обеспечения (специализированных программно-технических средств)	обслуживание и модификацию компонентов АС	обеспечения, не входящих в состав АС	ней ознакомления			несанкционированное ознакомление с принципами функционирования механизмов защиты в АС, создание предпосылок к подготовке и проведению атак на информационные ресурсы АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
6	Внедрение в АС компьютерных вирусов	Пользователи АС; уполномоченн ый персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС	Внедрение компьютерных вирусов при взаимодействии с внешними системами (выгрузка баз данных, файловый обмен и т.п.), а также при использовании съемных носителей информации на	Недостатки механизмов защиты информационны х ресурсов АС от компьютерных вирусов	Программн ое обеспечени е	Целостность	Нарушение режимов функционирова ние АС; реализация различного рода негативных информационн ых воздействий на целевую, технологическу ю информацию и программное обеспечение АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
			автоматизирован ных рабочих местах пользователей АС				
7	Осуществление необнаруженных несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию	Пользователи АС	Несанкционированные информационные воздействия (направленные на «отказ в обслуживании» для сервисов, модификацию конфигурационн ых данных	Недостатки механизмов защиты программно-аппаратных элементов АС от несанкционированных внешних воздействий	Программное обеспечение	Конфиденциальность, целостность	Нарушение режимов функционирования АС; снижение уровня защищенности АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	конфигурационн ых данных программно-аппаратных средств, подбор аутентификацион ной информации и т.п.) на программно-аппаратные элементы АС		программно-аппаратных средств, подбор аутентификацион ной информации и т.п.) с использованием специализирован ного программно-аппаратного обеспечения				
8	Осуществление несанкционирова нного доступа к	Пользователи АС, уполномоченн	Использование необнаруженных уязвимостей и	Наличие недокументиров анных	Целевая информаци я (в том	Конфиденциаль ность, целостность	Несанкциониро ванное ознакомление и

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	информационным активам, основанное на использовании СЗИ, телекоммуникационного оборудования с уязвимостями и недокументированными (недекларированными) возможностями, внесенными на	ый персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС	недокументированных (не декларированных) возможностей СЗИ, телекоммуникационного оборудования	(недекларированных) возможностей, внесенных на этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и	числе персональные данные и коммерческая тайна), технологическая информация, программное обеспечение		разглашение защищаемой информации; нарушение режимов функционирования АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	этапах разработки, производства, хранения, транспортировки, ввода в эксплуатацию, ремонта и обслуживания программных и технических средств			технических средств АС			
9	Осуществление несанкционированного доступа к	Пользователи АС, уполномоченн	Восстановление остаточной информации на	Недостатки механизмов гарантированног	Целевая информация (в том	Конфиденциальность	Несанкционированное ознакомление и

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	защищаемой информации, основанное на восстановлении (в том числе фрагментарном) остаточной информации путем анализа выведенных из употребления, сданных в ремонт, на обслуживание, переданных для использования	ый персонал разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС	носителях защищаемой информации с использованием специализированных инструментальны х средств	о уничтожения защищаемой информации, связанные с возможностью ее последующего несанкционированного восстановления	числе персональн ые данные и коммерческ ая тайна)		разглашение защищаемой информации

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	другим пользователям или для использования за пределами АС носителей информации						
10	Целенаправленно е искажение, навязывание ложной (специально сформированной нарушителем) защищаемой	Пользователи АС; пользователи других АИТС, являющихся внешними по отношению к АС; персонал	Осуществление целенаправленног о искажения, навязывание ложной (специально сформированной нарушителем)	Недостатки механизмов защиты информации, передаваемой по каналам связи, связанные с возможностью	Целевая информаци я (в том числе персональн ые данные и коммерческ ая тайна)	Целостность	Навязывание должностным лицам искаженной, ложной (специально сформированно й нарушителем)

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	информации в каналах связи (каналах передачи данных), с использованием специально разработанных технических средств и программного обеспечения (специализированных программно-технических средств)	разработчиков АС, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов АС	защищаемой информации с использованием специально разработанных технических средств и программного обеспечения (специализированных программно-технических средств), не входящих в состав, АС	ее искажения и навязывания ложной информации			информации; нарушение режимов функционирования АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
11	Целенаправленно е блокирование защищаемой информации в каналах связи (каналах передачи данных), с использованием специально разработанных технических средств и программного обеспечения (специализирован	Пользователи АС	Осуществление целенаправленног о блокирования защищаемой информации с использованием специально разработанных технических средств и программного обеспечения (специализирован ных программно-технических	Недостатки механизмов защиты передаваемой информации, связанные с возможностью ее блокирования в каналах связи	Целевая информаци я (в том числе персональн ые данные и коммерческ ая тайна)	Доступность	Непредставлени е целевой информации заинтересованн ым лицам в отведенные временные интервалы; нарушение штатного режима функционирова ния АС; срыв выполнения

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	ных программно-технических средств)		средств), не входящих в состав АС				поставленных задач
12	Внедрение в АС вредоносного программного обеспечения	Пользователи АС	Внедрение вредоносного программного обеспечения при взаимодействии с внешними системами (выгрузка баз данных, файловый обмен и т.п.), а также при	Недостатки механизмов защиты информационных ресурсов АС от вредоносного программного обеспечения	Программное обеспечение	Конфиденциальность, целостность, доступность	Несанкционированное ознакомление и разглашение коммерческой тайны и персональных данных; создание предпосылок к подготовке и проведению

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
			использовании съемных носителей информации на автоматизирован ных рабочих местах пользователей и администраторов АС				атак на информационн ые ресурсы АС; нарушение режимов функционирова ние АС; реализация различного рода негативных воздействий на целевую, технологическу ю информацию

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
							и программное обеспечение АС
13	Хищение производственных отходов (распечаток, записей, списанных носителей) с целью последующего анализа и несанкционированного ознакомления с	Сотрудники, имеющие санкционированный доступ в служебных целях в помещениях, в которых размещаются активы АС, но не имеющие права доступа к активам;	Осуществление прямого хищения производственных отходов (распечаток, записей, списанных носителей	Недостатки организационно-технических мер, обеспечивающих гарантированное уничтожение производственных отходов в АС, связанные с возможностью их	Целевая информация (в том числе персональные данные и коммерческая тайна)	Конфиденциальность	Несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и проведению атак на информационные ресурсы АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	целевой и технологической информацией	обслуживающ ий персонал (охрана, работники инженерно–технических служб и т.д.)		несанкциониров анного хищения и последующего использования для проведения аналитических исследований			
14	Осуществление несанкционирова нного визуального просмотра защищаемой информации, отображаемой на	Сотрудники, имеющие санкциониров анный доступ в служебных целях в помещениях, в которых	Осуществление несанкционирова нного визуального просмотра защищаемой информации, отображаемой на	Недостатки реализации необходимых организационно-режимных мероприятий на объектах АС, связанные с	Целевая информаци я (в том числе персональн ые данные и коммерческ ая тайна)	Конфиденциаль ность	Несанкциониро ванное ознакомление и разглашение защищаемой информации, создание предпосылок к

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
	средствах отображения (экранах мониторов), а также несанкционированное ознакомление с распечатываемым и документами, содержащими защищаемую информацию	размещаются активы АС, но не имеющие права доступа к активам; обслуживающ ий персонал (охрана, работники инженерно технических служб и т.д.)	средствах отображения (экранах мониторов), несанкционирова нного ознакомления с распечатываемым и документами, содержащими защищаемую информацию	возможностью несанкциониров анного визуального просмотра защищаемой информации на средствах отображения (экранах мониторов), а также несанкциониров анного ознакомления с			подготовке и проведению атак на информационн ые ресурсы АС

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
				распечатываемы ми документами, содержащими защищаемую информацию			
15	Преднамеренное осуществление сбоев, внесение неисправностей, уничтожение технических и программнотехнических компонентов АС	Пользователи АС; уполномоченн ый персонал разработчиков АС, который на договорной основе имеет право на техническое	Осуществление сбоев, внесение неисправностей, уничтожение технических и программно-технических компонентов АС путем непосредственног	Недостатки механизмов физической защиты компонентов АС, связанные с возможностью осуществления сбоев, внесения неисправностей,	Целевая информаци я (в том числе персональн ые данные и коммерческ ая тайна), программно е	Доступность, целостность	Непредоставлен ие целевой информации заинтересованн ым лицам в отведенные временные интервалы; нарушение штатного

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
		обслуживание и модификацию компонентов АС	о физического воздействия	уничтожения технических, и программно-технических компонентов АС	обеспечени е		режима функционирования АС; срыв выполнения поставленных задач
16	Осуществление несанкционированного доступа к оставленным без присмотра функционирующ им штатным средствам	Сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются	Осуществление несанкционированного доступа к оставленным без присмотра функционирующ им штатным средствам	Недостатки реализации необходимых организационно-режимных мероприятий на объектах АС, связанные с возможностью	Целевая информация (в том числе персональн ые данные и коммерческ ая тайна)	Конфиденциальность	Несанкционированное ознакомление и разглашение защищаемой информации, создание предпосылок к подготовке и

Идентификатор угрозы	Аннотация угрозы	Источник	Способ реализации угрозы	Используемые уязвимости	Вид активов, потенциал но подверженн ых угрозе	Нарушаемые характеристики безопасности активов	Возможные последствия реализации угрозы
		активы АС, но не имеющие права доступа к активам; обслуживающ ий персонал (охрана, работники инженерно–технических служб и т.д.)		несанкциониров анного доступа к оставленным без присмотра функционирую щим штатным средствам			проведению атак на информационн ые ресурсы АС

Приложение Б
УТВЕРЖДАЮ

Директор

ООО «Строительная компания»

_____/И.И. Иванов

« » _____ 2022 г.

Модель нарушителя

Санкт-Петербург

2022

1. Общие положения

Модель нарушителя информационной безопасности представляет собой совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения.

Данная модель нарушителя разработана на основании:

- Методика оценки угроз безопасности информации (ФСТЭК России, 2021 г.);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.);
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Определение модели вероятного нарушителя

Все угрозы безопасности информации автоматизированных систем (далее - АС) подразделяются на два класса:

- непреднамеренные угрозы (угрозы, не связанные с деятельностью человека; угрозы социально-политического характера; ошибочные действия персонала и пользователей АС; угрозы техногенного характера);
- атаки.

Непреднамеренные угрозы по своей природе не связаны со злонамеренными действиями человека по отношению к АС. Но эти угрозы могут не только привести к потере, искажению или компрометации информационных активов АС, но и создать условия, которые может использовать в своих целях нарушитель.

Предполагается, что защита от непреднамеренных угроз в основном регламентируется инструкциями, разработанными и утвержденными подразделениями, эксплуатирующими различные компоненты АС с учетом особенностей эксплуатации этих компонентов и действующей нормативной базы.

Угрозы безопасности информации могут быть реализованы нарушителями за счет:

- несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне;

- несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, операционные системы);
- несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web- приложения, иные прикладные программы общего и специального назначения);
- несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);
- несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства;
- воздействия на пользователей, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

3. Описание возможных нарушителей

Угрозы безопасности информации в информационной системе могут быть реализованы следующими видами нарушителей:

- внешние субъекты (физические лица);
- разработчики, производители, поставщики программных, технических и программно-технических средств;
- лица, обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);
- пользователи автоматизированной системы;
- системные администраторы;
- бывшие работники (пользователи).

Таблица 1 – Виды нарушителей и их цели (мотивации)

Вид нарушителя	Тип нарушителя	Возможные цели (мотивации) реализации угроз безопасности
Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
Разработчики, производители программных, технических и	Внешний	Внедрение дополнительных функциональных возможностей в ПО на этапе разработки. Непреднамеренные,

Вид нарушителя	Тип нарушителя	Возможные цели (мотивации) реализации угроз безопасности
программно-технических средств		неосторожные или неквалифицированные действия
Лица, обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия
Пользователи автоматизированной системы	Внутренний	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
Системные администраторы, администраторы безопасности	Внутренний	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения иной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.
Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации.

Потенциал нарушителей и их возможности приведены в таблице 2.

Таблица 2 – Потенциал нарушителей

Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица), лица, обслуживающие инфраструктуру оператора, пользователи автоматизированной системы, бывшие работники	Имеют возможность получить информацию об уязвимостях отдельных компонент автоматизированной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на автоматизированную систему
Нарушители с базовым повышенным (средним) потенциалом	Разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в

Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
		автоматизированной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент автоматизированной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно - функциональных характеристиках и особенностях функционирования автоматизированной системы
Нарушители с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами.

Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
		Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами)

Противодействие техническим средствам разведки (ПД ТСР) входит в общую систему мер по защите государственной тайны и конфиденциальной информации и представляет собой совокупность согласованных мероприятий, предназначенных для исключения или существенного затруднения добывания противником охраняемых сведений с помощью технических средств разведки.

Особая роль ПД ТСР обусловлена принципиальной открытостью системы управления конкурентов и противников в части каналов получения информации о наших силах и средствах, т.е. добывание информации о противоборствующей стороне предполагает наличие информационных потоков от физических носителей охраняемых сведений к системе управления противника. Кроме того, искажение или снижение качества получаемой информации непосредственно влияет на принимаемые противником решения и, через его систему управления, на способы и приемы исполнения решения, т.е. непосредственный контакт противоборствующих сторон принципиально необходим на этапах добывания информации и исполнения решения, причем добывание информации должно предшествовать принятию решения и его исполнению. Поэтому ПД ТСР должно носить предупреждающий характер.

Приложение В
УТВЕРЖДАЮ

Директор

ООО «Строительная компания»

_____/И.И. Иванов

« » _____ 2022 г.

МАТРИЦА ДОСТУПА

пользователей к техническим, программным средствам и информационным ресурсам автоматизированной системы

1. Список субъектов доступа.

№ п/п	Инициалы, фамилия	Учетная запись	Вид выполняемых функций	Уровень допуска учетной записи
1.	Смирнов В.А.	Smirnov.v	Администратор безопасности	Конфиденциально
2.	Кузнецов А.А.	Kuznetsov.a	Пользователь	Конфиденциально
3.	Попов Т.Д.	Popov.t	Пользователь	Конфиденциально
4.	Иванов Д.С.	Ivanov.d	Пользователь	Конфиденциально
5.	Петров С.А.	Petrov.s	Пользователь	Конфиденциально
6.	Михайлов П.А.	Mihailov.p	Пользователь	Конфиденциально

2. Список средств, информационных ресурсов автоматизированной системы (объектов доступа).

№ п/п	Наименование информационного ресурса	Категория информационного ресурса	Место хранения информационного ресурса
АРМ №1-№6			
1.	Средства ОС для запуска и работы ПЭВМ	Конфиденциально	C:\WINDOWS\
2.	Основные конфигурационные файлы операционной системы	Конфиденциально	C:\WINDOWS\
3.	Прикладное программное обеспечение	Конфиденциально	C:\Program Files\

№ п/п	Наименование информационного ресурса	Категория информационного ресурса	Место хранения информационного ресурса
4.	Драйверы средств защиты информации	Конфиденциально	C:\Program Files\Secret Net Studio\
5.	Средства настройки и управления средств защиты информации	Конфиденциально	C:\Program Files\Secret Net Studio\
6.	Основные конфигурационные файлы средств защиты информации	Конфиденциально	C:\Program Files\Secret Net Studio\
7.	Антивирусные средства	Конфиденциально	C:\Program Files\
8.	Многофункциональное устройство	Устройство печати и сканирования	USB-порт
9.	Съемный носитель	CD-диск	D:\
10.	Обрабатываемые, хранимые данные	Конфиденциально	C:\ПД\

3. Установленные права доступа к средствам, информационным ресурсам.

Объе кт досу па	Субъекты доступа					
	1	2	3	4	5	6
1.	Полный доступ	Выполне ние, чтение	Выполне ние, чтение	Выполне ние, чтение	Выполне ние, чтение	Выполне ние, чтение
2.	Полный доступ	Чтение	Чтение	Чтение	Чтение	Чтение
3.	Полный доступ	Выполне ние, чтение	Выполне ние, чтение	Выполне ние, чтение	Выполне ние, чтение	Выполне ние, чтение
4.	Полный доступ	-	-	-	-	-
5.	Полный доступ	-	-	-	-	-
6.	Полный доступ	-	-	-	-	-

Объект доступа	Субъекты доступа					
	1	2	3	4	5	6
7.	Полный доступ	-	-	-	-	-
8.	Печать, сканирование	Печать, сканирование	Печать, сканирование	Печать, сканирование	Печать, сканирование	Печать, сканирование
9.	Полный доступ	Удаление, чтение, запись	Удаление, чтение, запись	Удаление, чтение, запись	Удаление, чтение, запись	Удаление, чтение, запись
10.	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ	Полный доступ

Протокол измерений и расчетов показателей ПЭМИН

В таблицах 1 и 2 приведены оценочные значения ПЭМИН. Приведенные данные необходимы для определения значений радиусов зоны R2 и r1.

Таблица 1 – Оценка ПЭМИ

№ п/п	f, МГц	E _c , дБ	E _{выкл} , дБ	E _{c+выкл} , дБ	R, м
АРМ №1					
1	51,4	67,7	58,5	67,7	10,54
2	254,31	54,3	28,7	54,3	9,6
3	311,2	57,4	39,7	68,4	14,9
4	568,8	49,7	48,5	49,7	5,7
АРМ №2					
1	51,4	68,5	68,2	67,5	10,52
2	254,31	47,3	28,9	47,3	9,21
3	311,2	52,6	47,4	52,6	13,8
4	568,8	44,9	25,4	44,9	5,1
АРМ №3					
1	51,4	71,6	36,5	61,6	9,6
2	254,31	29,5	23,8	30,5	10,1
3	311,2	38,4	26,1	38,6	13,2
4	568,8	41,6	22,4	41,8	4,9
АРМ №4					
1	51,4	55,8	27,7	55,8	10,7
2	254,31	33,2	25,6	33,6	10,2
3	311,2	41,2	28,9	41,6	13,7
4	568,8	48,1	29,4	48,1	5,6
АРМ №5					
1	51,4	62,4	41,2	62,4	10,8

№ п/п	f, МГц	E _c , дБ	E _{выкл} , дБ	E _{c+выкл} , дБ	R, м
2	254,31	46,8	22,4	49,0	10,1
3	311,2	33,5	31,8	33,5	12,6
4	568,8	36,4	29,3	36,4	5,4
АРМ №6					
1	51,4	57,2	36,5	57,2	9,48
2	254,31	38,5	26,6	39,1	5,7
3	311,2	36,4	24,5	36,4	10,5
4	568,8	46,9	33,8	47,2	3,6

Расчет границы промежуточной зоны рассчитывается по формуле:

$$L_1 = \frac{150}{\pi * f_i},$$

Расчет границы ближней и промежуточной рассчитывается по формуле:

$$L_2 = \frac{1800}{\pi * f_i},$$

Ближняя зона ограничена расстоянием от излучателя $R = \lambda_i/2\pi$, где $\lambda_i = \frac{300}{f_i}$. Дальняя зона начинается с расстояния $R_i > 6 \lambda_i$.

Промежуточная зона ограничена расстоянием $\lambda_i/2\pi < R_i < 6 \lambda_i$.

Расстояние R_i для каждой частоты рассчитывается по формуле:

$$R_i = \frac{L_i}{t \sqrt{\frac{k * E_{\text{выкл},i}}{E_{ci}}}},$$

Где R_i – максимальная длина исследуемого отрезка, на котором возможно выделение информативного сигнала, м; L_i – расстояние от ОТСС до границы ближней, промежуточной или дальней зоны, м; t – коэффициент значения зоны; k – константное значение.

$t = 1$ при дальней зоне ($R_i > 6 \lambda_i$); $t = 2$ при промежуточной зоне ($\lambda_i/2\pi < R_i < 6 \lambda_i$); $t = 3$ при ближней зоне ($\lambda_i/2\pi$), где $\lambda_i = \frac{300}{f_i}$.

Значение L_1 выбирается из условий:	Значение E_{ci} выбирается из условий:
$L_1 = R_0$ – для ближней зоны;	$E_i = E_{ci}$ – для ближней зоны;
$L_1 = \begin{cases} L_{1i}, & \text{если } L_{1i} > R_0 \\ R_0, & \text{если } L_{1i} \leq R_0 \end{cases}$ – для промежуточной зоны	$E_1 = \begin{cases} E_{1i}, & \text{если } L_{1i} > R_0 \\ E_{ci}, & \text{если } L_{1i} \leq R_0 \end{cases}$ – для промежуточной зоны, где $E_{1i} = E_{ci} \left(\frac{R_0}{L_{1i}}\right)^3$ – значение напряженности поля информативного сигнала на границе ближней и промежуточной зон
$L_2 = \begin{cases} L_{2i}, & \text{если } L_{2i} > R_0 \\ R_0, & \text{если } L_{2i} \leq R_0 \end{cases}$ – для дальней зоны	$E_2 = \begin{cases} E_{2i}, & \text{если } L_{2i} > R_0 \\ E_{ci}, & \text{если } L_{2i} \leq R_0 \end{cases}$ – для дальней зоны

Определение зоны R_2 для АРМ №1	
1) $f_1 = 51,4$ МГц $L_1 = \frac{150}{3,14 \cdot 51,4} = 0,92939 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 51,4} = 11,15269 \text{ м}$ $E_{\text{с+выкл}} = 10^{38 + \frac{23}{24,3}} = 2441,6 \text{ мкВ}$ $E_{\text{выкл}} = 10^{11,5 + \frac{23}{24,3}} = 58,521 \text{ дБ}$ $E_c = \sqrt{2441,6^2 - 58,521^2} = 2440,05 \text{ мкВ}$ $E_c = 20 * \log_{10} 2440,05 = 67,747 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 58,52}{2440}}} = 4,21 \text{ м}$ $E_6 = 2440,05 * \left(\frac{1}{0,92939}\right)^3 = 8973,24 \text{ мкВ}$	2) $f_2 = 254,31$ $L_1 = \frac{150}{3,14 \cdot 254,31} = 0,47874 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 254,31} = 7,546 \text{ м}$ $E_{\text{с+выкл}} = 10^{31,4 + \frac{17}{24,3}} = 498,45 \text{ мкВ}$ $E_{\text{выкл}} = 10^{7,1 + \frac{17}{24,3}} = 28,74 \text{ дБ}$ $E_c = \sqrt{498,45^2 - 28,74^2} = 301,4 \text{ мкВ}$ $E_c = 20 * \log_{10} 301,4 = 54,34 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 28,74}{301,4}}} = 5,2 \text{ м}$ $E_6 = 301,4 * \left(\frac{1}{0,47874}\right)^3 = 25658,88 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 \cdot 28,74}{301,4}}} = 8,6 \text{ м}$

$R_{\Pi} = \frac{1}{2\sqrt{\frac{0,3*58,52}{2440}}} = 10,54 \text{ м}$ $E_{\Pi} = 2440,05 * (\frac{1}{11,152})^2 = 2,879 \text{ мкВ}$ $R_{\Delta} = \frac{11,152}{\frac{0,3*58,521}{2,879}} = 4,5 \text{ м}$	$E_{\Pi} = 301,4 * (\frac{1}{7,546})^2 = 2,21 \text{ мкВ}$ $R_{\Delta} = \frac{7,546}{\frac{0,3*28,74}{2,21}} = 9,6 \text{ м}$
3) $f_3 = 311,2$ $L_1 = \frac{150}{3,14*311,2} = 0,3111 \text{ м}$ $L_2 = \frac{1800}{3,14*311,2} = 5,21 \text{ м}$ $E_{\text{с+выкл}} = 10^{5,8+\frac{16,6}{24,3}} = 68,49 \text{ мкВ}$ $E_{\text{выкл}} = 10^{4,1+\frac{16,6}{24,3}} = 39,774 \text{ дБ}$ $E_c = \sqrt{68,49^2 - 39,774^2} = 51,9 \text{ мкВ}$ $E_c = 20 * \log_{10} 51,9 = 57,4 \text{ дБ}$ $R_6 = \frac{1}{3\sqrt{\frac{0,3*39,774}{51,9}}} = 5,2 \text{ м}$ $E_6 = 51,9 * (\frac{1}{0,3111})^3 = 10458,11 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2\sqrt{\frac{0,3*39,774}{51,9}}} = 3,6 \text{ м}$ $E_{\Pi} = 51,9 * (\frac{1}{5,21})^2 = 7,66 \text{ мкВ}$ $R_{\Delta} = \frac{5,21}{\frac{0,3*39,744}{7,66}} = 14,9 \text{ м}$	4) $f_1 = 568,8 \text{ МГц}$ $L_1 = \frac{150}{3,14*568,8} = 0,014 \text{ м}$ $L_2 = \frac{1800}{3,14*568,8} = 5,68 \text{ м}$ $E_{\text{с+выкл}} = 10^{17,6+\frac{16,4}{24,3}} = 48,91 \text{ мкВ}$ $E_{\text{выкл}} = 10^{4,9+\frac{16,4}{24,3}} = 48,52 \text{ дБ}$ $E_c = \sqrt{48,91^2 - 48,52^2} = 88,4 \text{ мкВ}$ $E_c = 20 * \log_{10} 88,4 = 49,72 \text{ дБ}$ $R_6 = \frac{1}{3\sqrt{\frac{0,3*48,52}{88,4}}} = 7,59 \text{ м}$ $E_6 = 88,4 * (\frac{1}{0,0014})^3 = 9655,32 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2\sqrt{\frac{0,3*48,52}{88,4}}} = 5,7 \text{ м}$ $E_{\Pi} = 88,4 * (\frac{1}{5,68})^2 = 5,62 \text{ мкВ}$ $R_{\Delta} = \frac{5,68}{\frac{0,3*48,52}{5,62}} = 5,5 \text{ м}$
Определение зоны R_2 для АРМ №2	
1) $f_1 = 51,4 \text{ МГц}$ $L_1 = \frac{150}{3,14*51,4} = 0,92939 \text{ м}$ $L_2 = \frac{1800}{3,14*51,4} = 11,15269 \text{ м}$ $E_{\text{с+выкл}} = 10^{44+\frac{12,4}{24,3}} = 3625,2 \text{ мкВ}$ $E_{\text{выкл}} = 10^{12,5+\frac{22}{24,3}} = 68,21 \text{ дБ}$	2) $f_2 = 254,31$ $L_1 = \frac{150}{3,14*254,31} = 0,47874 \text{ м}$ $L_2 = \frac{1800}{3,14*254,31} = 7,546 \text{ м}$ $E_{\text{с+выкл}} = 10^{42+\frac{12,3}{24,3}} = 4045,2 \text{ мкВ}$ $E_{\text{выкл}} = 10^{7,1+\frac{23}{24,3}} = 75,2 \text{ дБ}$

$E_c = \sqrt{3625,2^2 - 68,21^2} =$ $2906,11 \text{ мкВ}$ $E_c = 20 * \log_{10} 2906,11 = 68,52 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 68,21}{2906,11}}} = 5,48 \text{ м}$ $E_6 = 2906,11 * (\frac{1}{0,92939})^3 = 17847,3$ мкВ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 68,21}{2906,11}}} = 10,52 \text{ м}$ $E_{\Pi} = 2906,11 * (\frac{1}{11,15269})^2 = 2,879 \text{ мкВ}$ $R_{\Delta} = \frac{11,15269}{\frac{0,3 * 68,21}{2,879}} = 7,48 \text{ м}$	$E_c = \sqrt{4045,2^2 - 75,2^2} =$ $2463,1 \text{ мкВ}$ $E_c = 20 * \log_{10} 2463,8 = 49,68 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 75,2}{2463,1}}} = 8,1 \text{ м}$ $E_6 = 2463,1 * (\frac{1}{0,47874})^3 = 15477,3 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 75,2}{2463,1}}} = 9,21 \text{ м}$ $E_{\Pi} = 2463,1 * (\frac{1}{7,546})^2 = 4,11 \text{ мкВ}$ $R_{\Delta} = \frac{7,546}{\frac{0,3 * 75,2}{4,11}} = 8,9 \text{ м}$
3) $f_3 = 311,2$ $L_1 = \frac{150}{3,14 * 311,2} = 0,151 \text{ м}$ $L_2 = \frac{1800}{3,14 * 311,2} = 1,82 \text{ м}$ $E_{\text{с+выкл}} = 10^{7,8 + \frac{16,7}{24,3}} = 59,34 \text{ мкВ}$ $E_{\text{выкл}} = 10^{5,1 + \frac{16,7}{24,3}} = 43,77 \text{ дБ}$ $E_c = \sqrt{59,34^2 - 43,77^2} = 52,3 \text{ мкВ}$ $E_c = 20 * \log_{10} 52,3 = 57,2 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 43,77}{52,3}}} = 5,2 \text{ м}$ $E_6 = 52,3 * (\frac{1}{0,3111})^3 = 1115,8 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 43,77}{52,3}}} = 11,2 \text{ м}$ $E_{\Pi} = 52,3 * (\frac{1}{5,21})^2 = 7,5 \text{ мкВ}$ $R_{\Delta} = \frac{52,3}{\frac{0,3 * 43,77}{7,5}} = 13,8 \text{ м}$	4) $f_1 = 568,8 \text{ МГц}$ $L_1 = \frac{150}{3,14 * 568,8} = 0,083 \text{ м}$ $L_2 = \frac{1800}{3,14 * 568,8} = 1,00 \text{ м}$ $E_{\text{с+выкл}} = 10^{17,6 + \frac{15,7}{24,3}} = 44,9 \text{ мкВ}$ $E_{\text{выкл}} = 10^{4,9 + \frac{15,7}{24,3}} = 41,6 \text{ дБ}$ $E_c = \sqrt{44,9^2 - 41,6^2} = 45,2 \text{ мкВ}$ $E_c = 20 * \log_{10} 45,2 = 44,9 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 25,4}{45,2}}} = 4,9 \text{ м}$ $E_6 = 45,2 * (\frac{1}{0,0014})^3 = 8541,32 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 25,4}{45,2}}} = 5,1 \text{ м}$ $E_{\Pi} = 45,2 * (\frac{1}{5,68})^2 = 4,88 \text{ мкВ}$ $R_{\Delta} = \frac{5,68}{\frac{0,3 * 25,4}{4,88}} = 4,9 \text{ м}$

Определение зоны R_2 для АРМ №3	
1) $f_1 = 51,4$ МГц $L_1 = \frac{150}{3,14 \cdot 51,4} = 0,92939 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 51,4} = 11,15269 \text{ м}$ $E_{\text{с+выкл}} = 10^{24 + \frac{14,4}{24,3}} = 73,6 \text{ мкВ}$ $E_{\text{выкл}} = 10^{12,5 + \frac{11,9}{24,3}} = 36,5 \text{ дБ}$ $E_c = \sqrt{73,6^2 - 36,5^2} = 1185,2 \text{ мкВ}$ $E_c = 20 * \log_{10} 1185,2 = 71,6 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 36,5}{1185,2}}} = 5,36 \text{ м}$ $E_6 = 1185,2 * \left(\frac{1}{0,92939}\right)^3 = 15845,8 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 \cdot 36,5}{1185,2}}} = 9,56 \text{ м}$ $E_{\Pi} = 1185,2 * \left(\frac{1}{11,15269}\right)^2 = 36,4 \text{ мкВ}$ $R_d = \frac{11,15269}{\frac{0,3 \cdot 36,5}{36,4}} = 7,48 \text{ м}$	2) $f_2 = 254,31$ $L_1 = \frac{150}{3,14 \cdot 254,31} = 0,47874 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 254,31} = 7,546 \text{ м}$ $E_{\text{с+выкл}} = 10^{18,3 + \frac{17,6}{24,3}} = 30,5 \text{ мкВ}$ $E_{\text{выкл}} = 10^{7,2 + \frac{17,3}{24,3}} = 23,8 \text{ дБ}$ $E_c = \sqrt{30,5^2 - 23,8^2} = 9254,2 \text{ мкВ}$ $E_c = 20 * \log_{10} 9254,2 = 29,5 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 23,8}{9254,2}}} = 7,3 \text{ м}$ $E_6 = 9254,2 * \left(\frac{1}{0,47874}\right)^3 = 8477,7 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 \cdot 23,8}{9254,2}}} = 10,1 \text{ м}$ $E_{\Pi} = 9254,2 * \left(\frac{1}{7,546}\right)^2 = 13,5 \text{ мкВ}$ $R_d = \frac{7,546}{\frac{0,3 \cdot 2,8}{13,5}} = 6,5 \text{ м}$
3) $f_3 = 311,2$ $L_1 = \frac{150}{3,14 \cdot 311,2} = 0,3111 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 311,2} = 5,21 \text{ м}$ $E_{\text{с+выкл}} = 10^{5,8 + \frac{16,7}{24,3}} = 38,6 \text{ мкВ}$ $E_{\text{выкл}} = 10^{7,1 + \frac{12,7}{24,3}} = 26,1 \text{ дБ}$ $E_c = \sqrt{38,6^2 - 26,1^2} = 39,1 \text{ мкВ}$ $E_c = 20 * \log_{10} 52,3 = 38,4 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 26,1}{39,1}}} = 7,3 \text{ м}$	4) $f_1 = 568,8$ МГц $L_1 = \frac{150}{3,14 \cdot 568,8} = 0,014 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 568,8} = 5,68 \text{ м}$ $E_{\text{с+выкл}} = 10^{12,4 + \frac{18,9}{24,3}} = 41,8 \text{ мкВ}$ $E_{\text{выкл}} = 10^{6,3 + \frac{18,9}{24,3}} = 22,4 \text{ дБ}$ $E_c = \sqrt{44,9^2 - 25,4^2} = 42,4 \text{ мкВ}$ $E_c = 20 * \log_{10} 45,2 = 41,6 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 22,4}{42,4}}} = 3,2 \text{ м}$

$E_6 = 39,1 * (\frac{1}{0,3111})^3 = 12547,8 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2\sqrt{\frac{0,3*26,1}{39,1}}} = 9,4 \text{ м}$ $E_{\Pi} = 39,1 * (\frac{1}{5,21})^2 = 11,3 \text{ мкВ}$ $R_{\Delta} = \frac{39,1}{\frac{0,3*26,1}{11,3}} = 13,2 \text{ м}$	$E_6 = 42,4 * (\frac{1}{0,0014})^3 = 6544,2 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2\sqrt{\frac{0,3*22,4}{42,4}}} = 3,81 \text{ м}$ $E_{\Pi} = 42,4 * (\frac{1}{5,68})^2 = 4,9 \text{ мкВ}$ $R_{\Delta} = \frac{5,68}{\frac{0,3*22,4}{44,9}} = 5,5 \text{ м}$
Определение зоны R_2 для АРМ №4	
1) $f_1 = 51,4 \text{ МГц}$ $L_1 = \frac{150}{3,14*51,4} = 0,92939 \text{ м}$ $L_2 = \frac{1800}{3,14*51,4} = 11,15269 \text{ м}$ $E_{\text{с+выкл}} = 10^{36+\frac{22,9}{24,3}} = 55,8 \text{ мкВ}$ $E_{\text{выкл}} = 10^{12,6+\frac{22,8}{24,3}} = 27,7 \text{ дБ}$ $E_c = \sqrt{55,8^2 - 27,7^2} = 6952,6 \text{ мкВ}$ $E_c = 20 * \log_{10} 6952,6 = 55,8 \text{ дБ}$ $R_6 = \frac{1}{3\sqrt{\frac{0,3*27,7}{6952,6}}} = 5,33 \text{ м}$ $E_6 = 6952,6 * (\frac{1}{0,92939})^3 = 11441,8 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2\sqrt{\frac{0,3*27,7}{6952,6}}} = 10,7 \text{ м}$ $E_{\Pi} = 6952,6 * (\frac{1}{11,15269})^2 = 14,754 \text{ мкВ}$ $R_{\Delta} = \frac{11,15269}{\frac{0,3*68,21}{2,879}} = 8,8 \text{ м}$	2) $f_2 = 254,31$ $L_1 = \frac{150}{3,14*254,31} = 0,47874 \text{ м}$ $L_2 = \frac{1800}{3,14*254,31} = 7,546 \text{ м}$ $E_{\text{с+выкл}} = 10^{16,3+\frac{24}{24,3}} = 33,6 \text{ мкВ}$ $E_{\text{выкл}} = 10^{2,1+\frac{24}{24,3}} = 25,6 \text{ дБ}$ $E_c = \sqrt{33,6^2 - 25,6} = 14365,2 \text{ мкВ}$ $E_c = 20 * \log_{10} 14365,2 = 33,2 \text{ дБ}$ $R_6 = \frac{1}{3\sqrt{\frac{0,3*25,6}{14356,2}}} = 9,6 \text{ м}$ $E_6 = 14365,2 * (\frac{1}{0,47874})^3 = 6522,3 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2\sqrt{\frac{0,3*25,6}{6522,3}}} = 9,55 \text{ м}$ $E_{\Pi} = 14365,2 * (\frac{1}{7,546})^2 = 64,21 \text{ мкВ}$ $R_{\Delta} = \frac{7,546}{\frac{0,3*25,6}{64,21}} = 10,2 \text{ м}$
3) $f_3 = 311,2$ $L_1 = \frac{150}{3,14*311,2} = 0,3111 \text{ м}$ $L_2 = \frac{1800}{3,14*311,2} = 5,21 \text{ м}$ $E_{\text{с+выкл}} = 10^{11,8+\frac{24,2}{24,3}} = 41,6 \text{ мкВ}$	4) $f_1 = 568,8 \text{ МГц}$ $L_1 = \frac{150}{3,14*568,8} = 0,014 \text{ м}$ $L_2 = \frac{1800}{3,14*568,8} = 5,68 \text{ м}$ $E_{\text{с+выкл}} = 10^{8+\frac{14,3}{24,3}} = 48,3 \text{ мкВ}$

$E_{\text{ВЫКЛ}} = 10^{6,1 + \frac{24,1}{24,3}} = 28,9 \text{ дБ}$ $E_c = \sqrt{41,6^2 - 28,9^2} = 1455,9 \text{ мкВ}$ $E_c = 20 * \log_{10} 1455,9 = 41,2 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 28,9}{1455,9}}} = 11,5 \text{ м}$ $E_6 = 1455,9 * \left(\frac{1}{0,3111}\right)^3 = 2114,3 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 28,9}{1455,9}}} = 13,7 \text{ м}$ $E_{\Pi} = 1455,9 * \left(\frac{1}{5,21}\right)^2 = 8,6 \text{ мкВ}$ $R_d = \frac{52,3}{\frac{0,3 * 1455,9}{8,6}} = 12,8 \text{ м}$	$E_{\text{ВЫКЛ}} = 10^{5,2 + \frac{14,7}{24,3}} = 29,4 \text{ дБ}$ $E_c = \sqrt{48,3^2 - 29,4^2} = 45,6 \text{ мкВ}$ $E_c = 20 * \log_{10} 45,6 = 48,1 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 29,4}{45,6}}} = 5,6 \text{ м}$ $E_6 = 45,6 * \left(\frac{1}{0,0014}\right)^3 = 7466,3 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 29,4}{45,6}}} = 4,5 \text{ м}$ $E_{\Pi} = 45,6 * \left(\frac{1}{5,68}\right)^2 = 5,3 \text{ мкВ}$ $R_d = \frac{5,68}{\frac{0,3 * 29,4}{5,3}} = 5,5 \text{ м}$
Определение зоны R_2 для АРМ №5	
1) $f_1 = 51,4 \text{ МГц}$ $L_1 = \frac{150}{3,14 * 51,4} = 0,92939 \text{ м}$ $L_2 = \frac{1800}{3,14 * 51,4} = 11,15269 \text{ м}$ $E_{\text{с+ВЫКЛ}} = 10^{14,6 + \frac{18,2}{24,3}} = 62,5 \text{ мкВ}$ $E_{\text{ВЫКЛ}} = 10^{12,5 + \frac{18,2}{24,3}} = 41,2 \text{ дБ}$ $E_c = \sqrt{62,5^2 - 41,2^2} = 2544,3 \text{ мкВ}$ $E_c = 20 * \log_{10} 2544,3 = 62,4 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 41,2}{2544,3}}} = 10,8 \text{ м}$ $E_6 = 2544,3 * \left(\frac{1}{0,92939}\right)^3 = 109,322 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 41,2}{2544,3}}} = 4,6 \text{ м}$ $E_{\Pi} = 2544,3 * \left(\frac{1}{11,15269}\right)^2 = 365,2 \text{ мкВ}$ $R_d = \frac{11,15269}{\frac{0,3 * 41,2}{365,2}} = 7,2 \text{ м}$	2) $f_2 = 254,31$ $L_1 = \frac{150}{3,14 * 254,31} = 0,47874 \text{ м}$ $L_2 = \frac{1800}{3,14 * 254,31} = 7,546 \text{ м}$ $E_{\text{с+ВЫКЛ}} = 10^{10,6 + \frac{19,1}{24,3}} = 49,0 \text{ мкВ}$ $E_{\text{ВЫКЛ}} = 10^{6,1 + \frac{19,1}{24,3}} = 22,4 \text{ дБ}$ $E_c = \sqrt{49^2 - 22,4^2} = 1544,69 \text{ мкВ}$ $E_c = 20 * \log_{10} 1544,69 = 46,8 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 * 22,4}{1544,69}}} = 8,6 \text{ м}$ $E_6 = 1544,69 * \left(\frac{1}{0,47874}\right)^3 = 2741,1 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 * 22,4}{1544,69}}} = 5,2 \text{ м}$ $E_{\Pi} = 1544,69 * \left(\frac{1}{7,546}\right)^2 = 1063,1 \text{ мкВ}$ $R_d = \frac{7,546}{\frac{0,3 * 22,4}{1063,1}} = 10,1 \text{ м}$

3) $f_3 = 311,2$ $L_1 = \frac{150}{3,14 \cdot 311,2} = 0,3111 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 311,2} = 5,21 \text{ м}$ $E_{\text{с+выкл}} = 10^{12,1 + \frac{15,7}{24,3}} = 33,5 \text{ мкВ}$ $E_{\text{выкл}} = 10^{3,1 + \frac{15,7}{24,3}} = 31,8 \text{ дБ}$ $E_c = \sqrt{33,5^2 - 31,8^2} = 34,6 \text{ мкВ}$ $E_c = 20 * \log_{10} 34,6 = 54,1 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 31,8}{34,6}}} = 11,8 \text{ м}$ $E_6 = 34,6 * \left(\frac{1}{0,3111}\right)^3 = 8547,2 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 \cdot 31,8}{34,6}}} = 12,6 \text{ м}$ $E_{\Pi} = 34,6 * \left(\frac{1}{5,21}\right)^2 = 17,1 \text{ мкВ}$ $R_d = \frac{52,3}{\frac{0,3 \cdot 31,8}{17,1}} = 4,8 \text{ м}$	4) $f_1 = 568,8 \text{ МГц}$ $L_1 = \frac{150}{3,14 \cdot 568,8} = 0,014 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 568,8} = 5,68 \text{ м}$ $E_{\text{с+выкл}} = 10^{8,6 + \frac{23}{24,3}} = 44,9 \text{ мкВ}$ $E_{\text{выкл}} = 10^{4,9 + \frac{23}{24,3}} = 29,3 \text{ дБ}$ $E_c = \sqrt{44,9^2 - 29,3^2} = 45,2 \text{ мкВ}$ $E_c = 20 * \log_{10} 45,2 = 36,4 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 29,3}{45,2}}} = 5,4 \text{ м}$ $E_6 = 45,2 * \left(\frac{1}{0,0014}\right)^3 = 8541,32 \text{ мкВ}$ $R_{\Pi} = \frac{1}{\sqrt[2]{\frac{0,3 \cdot 29,3}{45,2}}} = 5,1 \text{ м}$ $E_{\Pi} = 45,2 * \left(\frac{1}{5,68}\right)^2 = 4,88 \text{ мкВ}$ $R_d = \frac{5,68}{\frac{0,3 \cdot 29,3}{4,88}} = 3,2 \text{ м}$
Определение зоны R_2 для АРМ №6	
1) $f_1 = 51,4 \text{ МГц}$ $L_1 = \frac{150}{3,14 \cdot 51,4} = 0,92939 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 51,4} = 11,15269 \text{ м}$ $E_{\text{с+выкл}} = 10^{44 + \frac{12,4}{24,3}} = 3625,2 \text{ мкВ}$ $E_{\text{выкл}} = 10^{12,5 + \frac{22}{24,3}} = 36,5 \text{ дБ}$ $E_c = \sqrt{3625,2^2 - 36,5^2} = 4113 \text{ мкВ}$ $E_c = 20 * \log_{10} 4113 = 57,2 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 36,5}{4113}}} = 8,1 \text{ м}$	2) $f_2 = 254,31$ $L_1 = \frac{150}{3,14 \cdot 254,31} = 0,47874 \text{ м}$ $L_2 = \frac{1800}{3,14 \cdot 254,31} = 7,546 \text{ м}$ $E_{\text{с+выкл}} = 10^{42 + \frac{12,3}{24,3}} = 404,2 \text{ мкВ}$ $E_{\text{выкл}} = 10^{7,1 + \frac{23}{24,3}} = 26,6 \text{ дБ}$ $E_c = \sqrt{404,2^2 - 75,2^2} = 485,2 \text{ мкВ}$ $E_c = 20 * \log_{10} 485,2 = 38,5 \text{ дБ}$ $R_6 = \frac{1}{\sqrt[3]{\frac{0,3 \cdot 26,6}{485,2}}} = 2,9 \text{ м}$

$E_6 = 4113 * (\frac{1}{0,92939})^3 = 1632,4 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2 \sqrt{\frac{0,3*36,5}{4113}}} = 5,41 \text{ м}$ $E_{\Pi} = 4113 * (\frac{1}{11,15269})^2 = 3,166 \text{ мкВ}$ $R_{\Delta} = \frac{11,15269}{\frac{0,3*36,5}{3,166}} = 9,48 \text{ м}$	$E_6 = 485,2 * (\frac{1}{0,47874})^3 = 4117,5 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2 \sqrt{\frac{0,3*26,6}{485,2}}} = 3,4 \text{ м}$ $E_{\Pi} = 485,2 * (\frac{1}{7,546})^2 = 513,4 \text{ мкВ}$ $R_{\Delta} = \frac{7,546}{\frac{0,3*26,6}{513,4}} = 5,7 \text{ м}$
3) $f_3 = 311,2$ $L_1 = \frac{150}{3,14*311,2} = 0,3111 \text{ м}$ $L_2 = \frac{1800}{3,14*311,2} = 5,21 \text{ м}$ $E_{\text{с+выкл}} = 10^{6,3+\frac{24,2}{24,3}} = 45,21 \text{ мкВ}$ $E_{\text{выкл}} = 10^{1,1+\frac{24,2}{24,3}} = 24,5 \text{ дБ}$ $E_c = \sqrt{45,21^2 - 24,5^2} = 46,25 \text{ мкВ}$ $E_c = 20 * \log_{10} 46,25 = 36,4 \text{ дБ}$ $R_6 = \frac{1}{3 \sqrt{\frac{0,3*24,5}{46,25}}} = 5,8 \text{ м}$ $E_6 = 46,25 * (\frac{1}{0,3111})^3 = 3214,6 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2 \sqrt{\frac{0,3*24,5}{46,25}}} = 7,7 \text{ м}$ $E_{\Pi} = 46,25 * (\frac{1}{5,21})^2 = 81,3 \text{ мкВ}$ $R_{\Delta} = \frac{52,3}{\frac{0,3*24,5}{81,3}} = 13,8 \text{ м}$	4) $f_1 = 568,8 \text{ МГц}$ $L_1 = \frac{150}{3,14*568,8} = 0,014 \text{ м}$ $L_2 = \frac{1800}{3,14*568,8} = 5,68 \text{ м}$ $E_{\text{с+выкл}} = 10^{15,6+\frac{20}{24,3}} = 47,2 \text{ мкВ}$ $E_{\text{выкл}} = 10^{5,9+\frac{20}{24,3}} = 25,4 \text{ дБ}$ $E_c = \sqrt{47,2^2 - 25,4^2} = 46,1 \text{ мкВ}$ $E_c = 20 * \log_{10} 46,1 = 46,9 \text{ дБ}$ $R_6 = \frac{1}{3 \sqrt{\frac{0,3*25,4}{46,1}}} = 2,1 \text{ м}$ $E_6 = 46,1 * (\frac{1}{0,0014})^3 = 154,2 \text{ мкВ}$ $R_{\Pi} = \frac{1}{2 \sqrt{\frac{0,3*25,4}{46,1}}} = 3,6 \text{ м}$ $E_{\Pi} = 46,1 * (\frac{1}{5,68})^2 = 3,1 \text{ мкВ}$ $R_{\Delta} = \frac{5,68}{\frac{0,3*25,4}{3,1}} = 5,5 \text{ м}$

Расчет наводок на линии ОТСС проводится по следующим формулам

$$U_{ci} = 20 \lg \sqrt{10^{U(c+\text{ш})_i/10}} - 10^{U_{\text{ш}i}/10},$$

Где U_{ci} – значение напряженности в точке присоединения измерительного прибора, дБ; $U(c + \text{ш})_i$ – значение смешанного напряжения

обнаруженных компонентов нагрузки и шума, дБ; $U_{шi}$ – значение напряженности шума в линии.

Показатель защищенности в точке проведения измерений рассчитывается по формуле

$$P_i = U_i - U_{шi},$$

Где P_i – показатель защищенности, дБ; U_i – значение напряжения сигнала в линии, дБ; $U_{шi}$ – значение напряжения шума в линии, дБ.

Величина коэффициента погонного затухания K_{Pi} наведенных сигналов в исследуемой линии рассчитывается по формуле

$$K_{Pi} = \frac{U_{1 \text{ изм } i} - U_{2 \text{ изм } i}}{l},$$

Где $U_{1 \text{ изм } i}$ – напряжение специально созданного сигнала, измеренное на частоте fi исследуемой линии в непосредственной близости от ОТСС, мкВ; $U_{2 \text{ изм } i}$ – напряжение специально созданного сигнала, измеренное на частоте fi исследуемой линии на некотором удалении от ОТСС, мкВ; l – значение напряженности линии ВТСС.

Максимальная длина пробега R_i – исследуемой линии рассчитывается по формуле

$$R_i = \frac{P_i + 10}{K_{Pi}}.$$

Таблица 11 – Оценка наводок ПЭМИ

№	f, МГц	U(c+ш) _i , дБ	U _{шi} , дБ	U _{ci} , дБ	U _{1измi} , мкВ	U _{2измi} , мкВ	K _{pi} , дБ/м	R _i , м
АРМ №1								
1	51,4	48	12	13,55	201,5	6,8	2	5,75
2	254,31	61	16	17,4	167,4	5,7	2,5	5,7
АРМ №2								
1	51,4	54	22	13,54	241,6	6,2	2,6	5,8
2	254,31	60	18	21,7	111,8	5,2	1,6	10,9
АРМ №3								
1	51,4	48	20	21,8	195,8	7,5	1,9	4,7
2	254,31	63	24	26,2	223,7	7,1	2,2	5,5
АРМ №4								
1	51,4	65	14	17,4	184,6	5,1	2,5	5,3
2	254,31	62	15	16,87	267,2	6,6	1,9	6,2

№	f, МГц	U(c+ш)і, дБ	Uші, дБ	Uсі, дБ	U _{1измі} , мкВ	U _{2измі} , мкВ	K _{pi} , дБ/м	R _i , м
АРМ №5								
1	51,4	61	17	19,2	154,3	7,6	1,75	7,1
2	254,31	59	24	27,7	198,6	5,9	2,5	5,48
АРМ №6								
1	51,4	54	20	26,3	297,2	5,2	2,1	7,8
2	254,31	62	18	19,7	125,9	7,6	2,5	4,68

Определение зоны r_1 для АРМ № 1	
1) $f_1 = 51,4$ $U_{c1} = 20 * \lg \sqrt{10^{\frac{28}{10}} - 10^{\frac{12}{10}}} = 13,548 \text{ дБ}$ $P_1 = 13,548 - 12 = 1,548$ $K_{pi} = \frac{39-15}{12} = 2$ $r_1 = \frac{1,548+10}{2} = 5,75 \text{ м}$	2) $f_2 = 254,31$ $U_{c2} = 20 * \lg \sqrt{10^{\frac{21}{10}} - 10^{\frac{16}{10}}} = 17,4 \text{ дБ}$ $P_2 = 17,4 - 16 = 1,4$ $K_{pi} = \frac{47-17}{12} = 2,5$ $r_2 = \frac{1,4+10}{2,5} = 5,7 \text{ м}$
Определение зоны r_1 для АРМ № 2	
1) $f_1 = 51,4$ $U_{c1} = 20 * \lg \sqrt{10^{\frac{24}{10}} - 10^{\frac{22}{10}}} = 27,32 \text{ дБ}$ $P_1 = 27,32 - 22 = 5,32$ $K_{pi} = \frac{49-17}{12} = 2,6$ $r_1 = \frac{5,32+10}{2,6} = 5,8 \text{ м}$	2) $f_2 = 254,31$ $U_{c2} = 20 * \lg \sqrt{10^{\frac{20}{10}} - 10^{\frac{18}{10}}} = 21,7 \text{ дБ}$ $P_2 = 21,7 - 18 = 3,7$ $K_{pi} = \frac{39-15,5}{12} = 1,6$ $r_2 = \frac{6,7+10}{1,6} = 10,9 \text{ м}$
Определение зоны r_1 для АРМ № 3	
1) $f_1 = 51,4$ $U_{c1} = 20 * \lg \sqrt{10^{\frac{18}{10}} - 10^{\frac{20}{10}}} = 21,8 \text{ дБ}$ $P_1 = 21,8 - 20 = 1,8$ $K_{pi} = \frac{42-19}{12} = 1,9$ $r_1 = \frac{1,8+10}{1,9} = 4,7 \text{ м}$	2) $f_2 = 254,31$ $U_{c2} = 20 * \lg \sqrt{10^{\frac{23}{10}} - 10^{\frac{24}{10}}} = 26,2 \text{ дБ}$ $P_2 = 26,2 - 24 = 2,2$ $K_{pi} = \frac{39-12,7}{12} = 2,2$ $r_2 = \frac{2,2+10}{2,2} = 5,5 \text{ м}$
Определение зоны r_1 для АРМ № 4	
1) $f_1 = 51,4$ $U_{c1} = 20 * \lg \sqrt{10^{\frac{25}{10}} - 10^{\frac{14}{10}}} = 17,4 \text{ дБ}$ $P_1 = 17,4 - 14 = 3,4$ $K_{pi} = \frac{47-17}{12} = 2,5$	2) $f_2 = 254,31$ $U_{c2} = 20 * \lg \sqrt{10^{\frac{22}{10}} - 10^{\frac{15}{10}}} = 16,87 \text{ дБ}$ $P_2 = 16,87 - 15 = 1,87$

$r_1 = \frac{3,4+10}{2,5} = 5,3 \text{ м}$	$K_{pi} = \frac{49-26}{12} = 1,9$ $r_2 = \frac{1,87+10}{1,9} = 6,2 \text{ м}$
Определение зоны r_1 для АРМ № 5	
1) $f_1 = 51,4$ $U_{c1} = 20 * \lg \sqrt{10^{\frac{21}{10}} - 10^{\frac{17}{10}}} = 19,2 \text{ дБ}$ $P_1 = 19,2 - 17 = 2,2$ $K_{pi} = \frac{40-19}{12} = 1,75$ $r_1 = \frac{2,2+10}{1,75} = 7,1 \text{ м}$	2) $f_2 = 254,31$ $U_{c2} = 20 * \lg \sqrt{10^{\frac{19}{10}} - 10^{\frac{24}{10}}} = 27,7 \text{ дБ}$ $P_2 = 27,7 - 24 = 3,7$ $K_{pi} = \frac{43-13}{12} = 2,5$ $r_2 = \frac{3,7+10}{2,5} = 5,48 \text{ м}$
Определение зоны r_1 для АРМ № 6	
1) $f_1 = 51,4$ $U_{c1} = 20 * \lg \sqrt{10^{\frac{24}{10}} - 10^{\frac{20}{10}}} = 26,3 \text{ дБ}$ $P_1 = 26,3 - 20 = 6,3$ $K_{pi} = \frac{42-16}{12} = 2,1$ $r_1 = \frac{6,3+10}{2,1} = 7,8 \text{ м}$	2) $f_2 = 254,31$ $U_{c2} = 20 * \lg \sqrt{10^{\frac{22}{10}} - 10^{\frac{18}{10}}} = 19,7 \text{ дБ}$ $P_2 = 19,7 - 18 = 1,7$ $K_{pi} = \frac{49-19}{12} = 2,5$ $r_2 = \frac{1,7+10}{2,5} = 4,68 \text{ м}$