МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 ООО «Газпром Интернешнл» от утечек по техническим каналам»

Исполнитель _____ Яковлев Георгий Алексеевич
(подпись) (фамилия, имя, отчество)

Руководитель _____ Юрин Игорь Валентинович
(подпись) (фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой_____ Бурлов В.Г.
(подпись) (фамилия, имя, отчество)

«____»_____2023 г.

Санкт–Петербург

2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время индустрия информационных технологий развиваются с большой скоростью, с этим развитием приходит как благо, так и вред. Такое развитие увеличивает доступность к большому количеству информации, что побуждает не только улучшать и совершенствовать текущее положение, но и к краже, уничтожению или изменению этой информации.

С этими растущими угрозами человечество борется на протяжении всего своего существования. Когда создают оружие, разрабатывают и щит, с помощью которого можно отбить атаку. Так и в нынешнее время, разрабатывают средства разведки, которые могут перехватить информацию и создаются средства по ее защите.

Таким образом, данная тема работы актуальная по сей день, так как разрабатываются новые средства снятия информации, повышается уровень информационной грамотности и растет конкуренция между компаниями. Для противодействия этим угрозам следует разрабатывать новые или совершенствовать средства защиты информации.

В данной работе рассмотрен процесс организации системы защиты автоматизированных систем на предприятии ООО «Газпром Интернешнл», подобраны средства защиты информации и проведены аттестационные испытания в соответствии с требованиями и рекомендациями по защите информации.

ГЛАВА 1. АНАЛИЗ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

В данной работе будет рассмотрен объект информатизации – «Автоматизированная система» Общества с ограниченной ответственностью «Газпром Интернешнл», расположенное по адресу: г. Санкт-Петербург, наб. реки Средней Невки, 24, стр. 1. Здание трехэтажное, помещение находится на втором этаже, окна выходят на р. Большая Невка. Здание предприятия расположено на берегу реки Большой Невки. На рисунках 1 представлена общая схема расположения помещения в здании. На рисунке 2, представлено расположение автоматизированных систем и предметов мебели в помещении. На рисунке 3, представлена схема расположения линий слаботочных систем, пожарной системы и пожарной системы в помещении. На рисунке 4, представлена схема, расположения линий электропитания в помещении.

Автоматизированная система (далее - «АС») - система, включающая средства по автоматизации и реализующего информационную технологию выполнения установленных задач, и персонала для поддержки его работы.

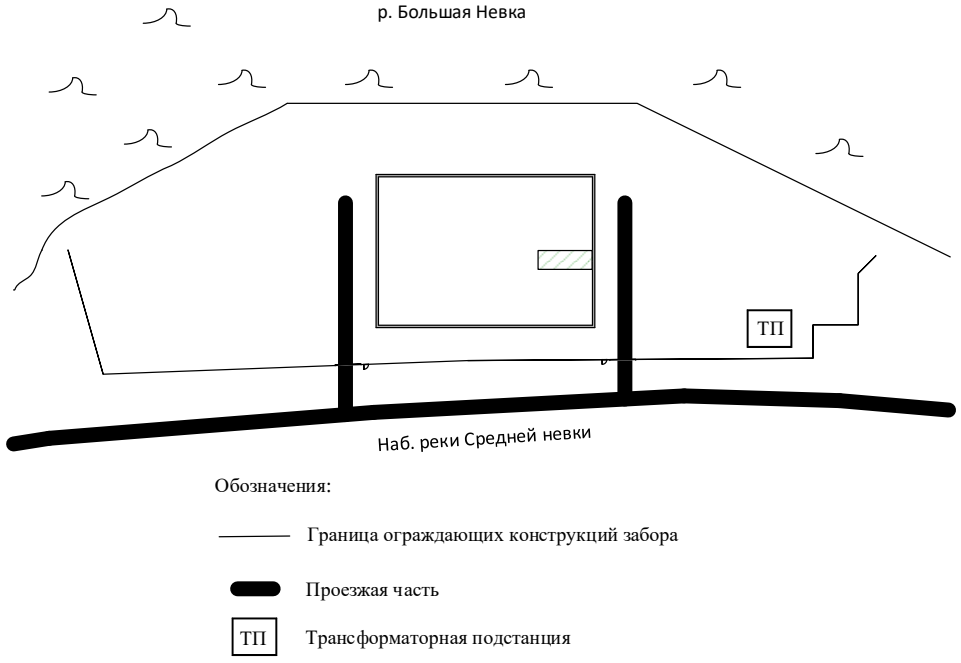


Рисунок 1 – Схема расположения помещения в здании

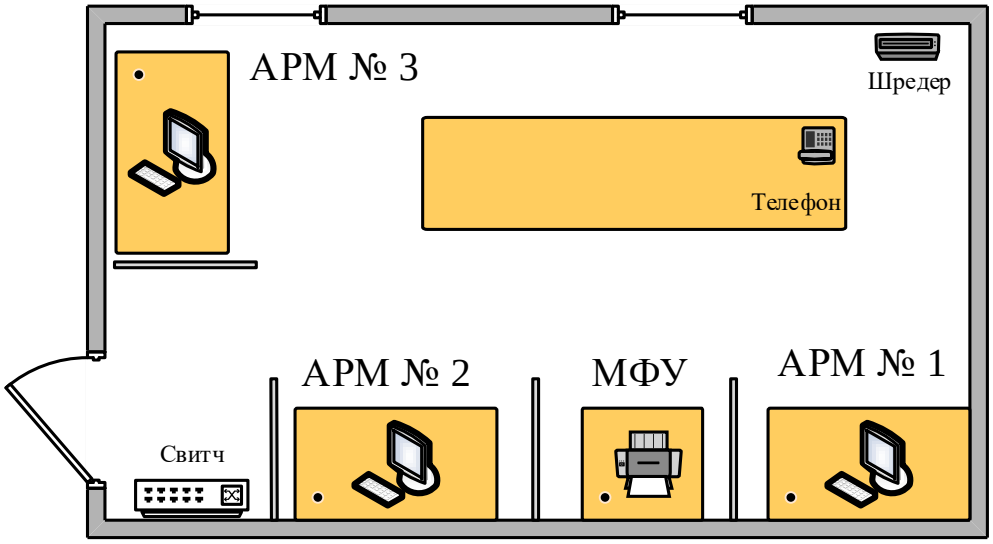
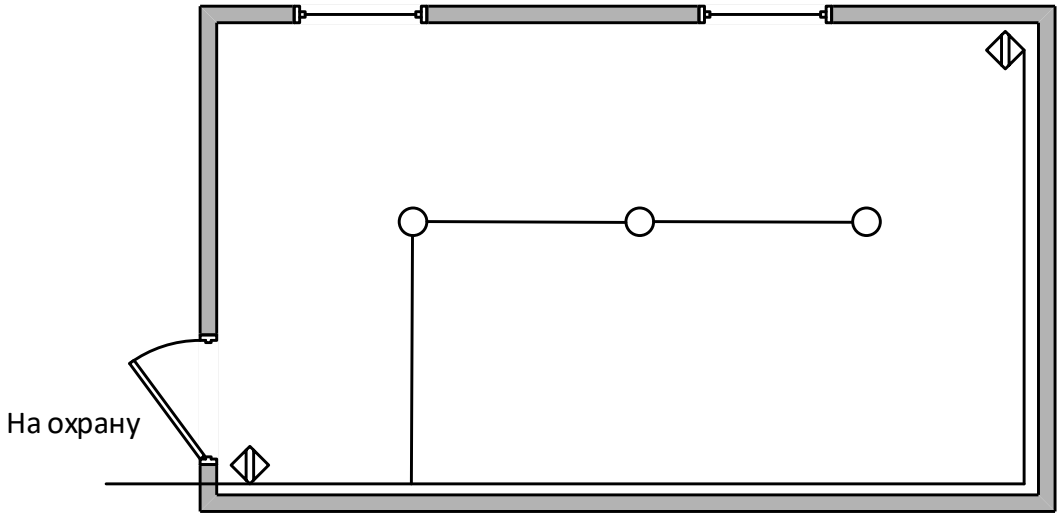


Рисунок 2 – Схема расположения автоматизированных систем в помещении № 215б



- Датчик движения

- Извещатель пожарный

Рисунок 3 – Схема расположения линий слаботочных систем

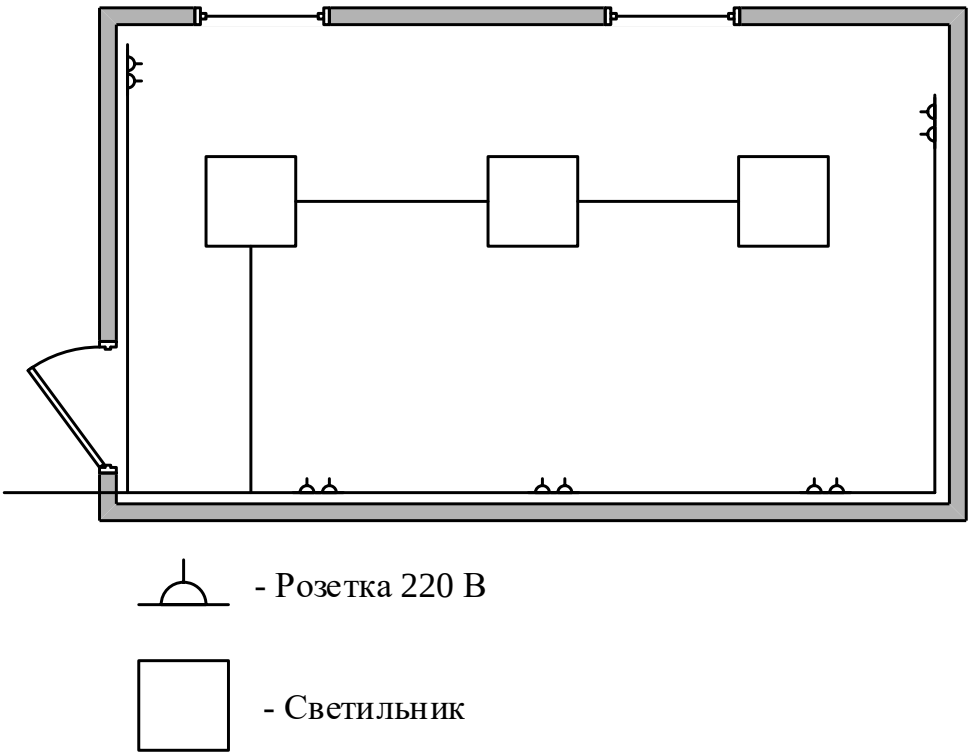


Рисунок 4 – Схема электропитания помещения № 215б

Перечень оборудования, которое расположено в помещении № 215б, представлено в таблице 1.

Таблица 1 – Перечень оборудования

Наименование	Модель
ОТСС	
АРМ № 1	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
МФУ	HP MFP 135W
АРМ № 2	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
АРМ № 3	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120

Наименование	Модель
Манипулятор «Мышь»	Logitech M90
Сетевое оборудование	
Свитч	D-LINK DES1005C
ВТСС	
Шредер	Deli Core E9954-EU
IP телефон	Yealink
Датчик движения	Риелта Фотон-12 (ИО409-17/1)
Датчик движения	Риелта Фотон-12 (ИО409-17/1)
Извещатель пожарный	RUBEZH ИП 212-45
Извещатель пожарный	RUBEZH ИП 212-45
Извещатель пожарный	RUBEZH ИП 212-45

1.1. Вид обрабатываемой информации на объекте

На объекте циркулирует как коммерческая тайна, так и персональные данные.

Исходя из этого, коммерческая тайна – это режим конфиденциальности информации, позволяющий обладателю повысить свои доходы, избежать расходов, сохранить положение на рынке, работ, услуг или получить иную коммерческую выгоду.

К информации, составляющую коммерческую тайну относятся следующие сведения:

- Информация о материальном положении фирмы;
- Сведения о новых разработках компании;
- Данные о клиентах;
- Информация об имуществе предприятия и его стоимости.

Персональные данные– это вся информация, по которой можно определить человека используя его фамилию, адрес проживания, возраст, место работы и др.

К видам персональных данных относятся:

- ФИО;
- Место жительства;
- Заработная плата;

- Биометрические данные;
- Информация из паспорта;
- Паспортные данные;
- СНИЛС.

1.2. Анализ уязвимостей объекта

При анализе информации о состоянии объекта информатизации ООО «Газпром Интернешнл», были обнаружены следующие уязвимости:

1) На рисунке 1 показано что ограждения здания ООО «Газпром Интернешнл» не смыкаются по периметру контролируемой зоны, это связано с тем, что участок попадает под действия законов, согласно нему, береговая линия не может быть ограничена для общего пользования;

«Земельный кодекс Российской Федерации» ст. 27, п. 8 – согласно этому пункту, запрещается приватизировать береговые земельные участки и территории общего пользования.

Из этих законов можно сделать вывод: установка забора к береговой линии невозможна. Следовательно, летом - возможно проникновение посторонних лиц на территорию в обход ограждающих конструкции забора, а зимой – злоумышленник может пройти по замерзшей реке Большая Невка и проникнуть на территорию ООО «Газпром Интернешнл».

2) Так, как окна помещения ООО «Газпром Интернешнл» выходят на р. Большая Невка, то есть возможность для съёма информации с экранов мониторов, с помощью оптических устройств.

3) Исходя и того, что контролируемая зона проходит по периметру ограждающих конструкций здания, злоумышленник может проникнуть на охраняемую территорию и установить средства разведки по каналу ПЭМИ вплотную к зданию, а возимые средства разведки у ворот здания ООО «Газпром Интернешнл».

1.3. Контролируемая зона

Контролируемая зона – это та территория, на которой не допускает неконтрольное пребывание посторонних лиц или транспортных средств без сопровождения ответственного сотрудника.

Границей контролируемой зоны могут служить ограждающие конструкции здания или часть здания, забор и периметр охраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите персональных данных.

Для ООО «Газпром Интернешнл» граница контролируемой зоны проходит по ограждающим конструкциям здания, рисунок 5.

Охраняемая зона – это зона, в которой происходит круглосуточное дежурство охранной организации, видеосъемка и невозможно пребывание лиц без пропуска или без сопровождения ответственного сотрудника ООО «Газпром Интернешнл».

Исходя из выше изложенным пункта, контролируемая зона не может проходить по ограждающим конструкция забора, вместо этого устанавливается охраняемая зона, которая проходит по ограждающим конструкциям забора и береговой линии, схема расположения представлена на рисунке 5.

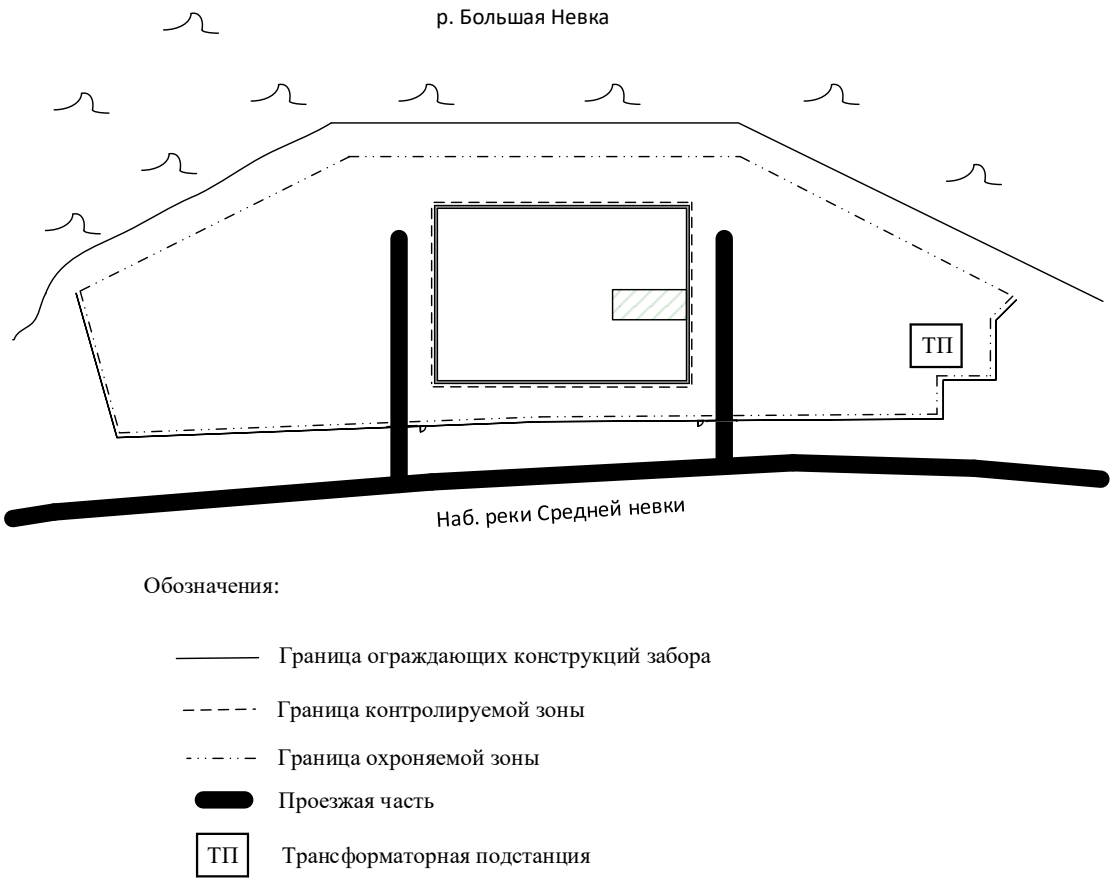


Рисунок 5 – Схема расположения контролируемой и охраняемой зоны

1.4. Анализ возможных технических каналов утечки информации

При рассмотрении здания и помещения где находятся АС, были обнаружены возможные каналы:

- несанкционированный доступ и несанкционированные действия по отношению к информации в АС;
- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации;
- побочные электромагнитные излучения информативного сигнала от технических средств,
- наводки информативного сигнала, обрабатываемого ОТСС и ВТСС, на цепи электропитания и линии, выходящие за пределы КЗ;

- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав ОТСС и ВТСС, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- просмотр информации с дисплеев, бумажных носителей и иных средств отображения информации;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- некомпетентные или ошибочные действия пользователей или администраторов АС при работе.

1.5. Классификация автоматизированной системы

Из руководящим документам автоматизированные системы должны быть классифицированы по:

Типу автоматизированной системы:

1) Многопользовательская;

2) Однопользовательская.

Правам допуска к информации:

1) Допуск к части информации;

2) Допуск ко всей информации.

Размещению на носителях:

1) Одноуровневая конфиденциальность;

2) Многоуровневая конфиденциальность.

Виду обрабатываемой информации:

1) Несекретно;

2) Конфиденциально;

3) Секретно;

4) Совершенно секретно;

5) Особой важности.

В соответствии с этими категориями для автоматизированной системы определяется ее класс. Согласно руководящими документами был проведен анализ исходя из которого была определена. В таблице 24 приложение Е показаны характеристики рассматриваемой автоматизированной системы.

В ходе анализа таблицы 24 в приложении Е, можно сделать вывод, что для автоматизированной системы установленной в помещении № 215б, соответствует класс защищенности «2Б».

1.6. Модель угроз

Порядок описания и разработки модели угроз регламентируются руководящих документах ФСТЭК России.

В данных документах сказано, что нужно:

- Определить угрозы персональных данных при их обработке в информационной системе;
- Примененные средства защиты информации;
- Выявить угрозы, которые могут нанести вред информационной системе;
- Проанализировать угрозы безопасности информации или уточнить.

Из выше изложенного можно сделать вывод, что для любых информационных систем необходимо разработать модель угроз.

Угроза – набор условий и факторов, которые создают потенциальный или фактический риск нарушения информационной безопасности.

Источник угроз безопасности – субъект, являющийся непосредственной причиной возникновения угрозы безопасности информации.

Уязвимость – это такое состояние системы, при которой созданы условия для угроз безопасности информации.

Несанкционированный доступ к информации (далее - «НСД») – это доступ к информации, нарушающий правила контроля доступа при помощи СВТ или автоматизированной системы.

При рассмотрении объекта информатизации ООО «Газпром Интернешнл», была разработана модель угроз и рассчитаны вероятности угроз безопасности информации согласно руководящим документам: «Базовая модель угроз безопасности персональных данных при их обработки в информационных системах персональных данных» (утв. ФСТЭК РФ от 15 февраля 2008г) и «Методика определения актуальных угроз безопасности персональных данных при их обработки в информационных системах персональных данных» (утв. ФСТЭК РФ от 14 февраля 2008г).

Для рассмотрения угроз безопасности информации определяется ее актуальность. Актуальной угрозой считается, которая может быть реализована и представляет угрозу для персональных данных.

Исходной уровень защищенности объекта понимается под его техническим и эксплуатационным характеристикам, в таблице 23 (приложение Е) приведен анализ объекта информатизации ООО «Газпром Интернешнл».

Согласно таблице 23 значению уровня защищенности «Высокий» соответствуют 1 характеристика, значению уровня «Средний» - 3 характеристики, значению уровня «Низкий» - 1 характеристика. Таким образом, числовой коэффициент исходной защищенности ИСПДн Оператора соответствует значению 5 (средняя).

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

- маловероятно – реализация или потенциальная угроза (модификации, изменения, хищения) информации отсутствует;

- низкая вероятность – имеется угроза (модификации, изменения, хищения) информации, но приняты меры, затрудняющие ее реализацию;
- средняя вероятность – имеется угроза информации, принятых мер защиты информации недостаточно для обеспечения безопасности персональных данных;
- высокая вероятность – имеется угроза безопасности информации, меры для защиты персональных не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно:

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

Таблице 2 описаны угрозы и их характеристики для данного объекта информатизации.

Таблица 2 – Актуальности угроз безопасности информации на АС

Наименование угрозы	Вероятность угрозы (Y2)	Вероятность реализации угрозы (Y)	Возможность реализации угрозы	Актуальность
Угрозы утечки информации по техническим каналам				
Угрозы утечки информации со средств ее отображения	средняя вероятность (5)	0,5	средняя	актуальная
Угрозы утечки информации по каналу ПЭМИН	средняя вероятность (5)	0,5	средняя	актуальная
Угрозы НСД к ПДн, обрабатываемым на АРМ				
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой	средняя вероятность (5)	0,5	средняя	актуальная

Наименование угрозы	Вероятность угрозы (Y2)	Вероятность реализации угрозы (Y)	Возможность реализации угрозы	Актуальность
системы ввода/вывода (BIOS), перехват управления загрузкой				
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ	средняя вероятность (5)	0,5	средняя	актуальная
Угрозы внедрения вредоносных программ	средняя вероятность (5)	0,5	средняя	актуальная
Предоставление пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам ИСПДн сверх необходимого для работы	высокая вероятность (10)	0,75	высокая	актуальная
Неумышленная (случайная) отправка ПДн по ошибочным адресам электронной почты	низкая вероятность (2)	0,35	средняя	актуальная
Преднамеренное копирование	низкая вероятность	0,35	средняя	актуальная

Наименование угрозы	Вероятность угрозы (Y2)	Вероятность реализации угрозы (Y)	Возможность реализации угрозы	Актуальность
доступных ПДн на неучтённые (в том числе отчуждаемые) носители в том числе печать неучтённых копий документов с ПДн на принтерах	(2)			
Неумышленное (случайное) добавление (фальсификация) ПДн	низкая вероятность (2)	0,35	средняя	актуальная
Неумышленное (случайное) уничтожение доступных ПДн (записей, файлов, форматирование диска)	высокая вероятность (10)	0,6	высокая	актуальная
Преднамеренное уничтожение доступных ПДн (записей, файлов, форматирование диска)	низкая вероятность (2)	0,6	высокая	актуальная
Покинуть рабочее место с не заблокированной рабочей станцией	высокая вероятность (10)	0,6	высокая	актуальная
Подкючение к ИСПДн стороннего оборудования (компьютеров, дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи)	средняя вероятность (5)	0,5	средний	актуальная
Использование оборудования, оставленного без присмотра, паролей	низкая вероятность (2)	0,35	средняя	актуально
Внедрение	высокая	0,75	высокая	актуально

Наименование угрозы	Вероятность угрозы (Y2)	Вероятность реализации угрозы (Y)	Возможность реализации угрозы	Актуальность
вредоносных программ	вероятность (10)			
Доступ к информации ИСПДн, выходящей за пределы контролируемой зоны вследствие списания (утилизации) носителей информации, содержащих ПДн	низкая вероятность (2)	0,35	средняя	актуально
Игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации	высокая вероятность (10)	0,75	высокая	актуально
Нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации(в частности, ключевой, парольной и аутентифицирующей информации)	высокая вероятность (10)	0,75	высокая	актуально
Не информирование о факте утраты (ключевой, парольной, аутентифицирующей а также любой другой информации ограниченного доступа)	высокая вероятность (10)	0,75	высокая	актуально
Сетевые угрозы				
Угрозы "Анализа сетевого трафика" с	средняя вероятность	0,5	средняя	актуально

Наименование угрозы	Вероятность угрозы (Y2)	Вероятность реализации угрозы (Y)	Возможность реализации угрозы	Актуальность
перехватом передаваемой по сети информации	(5)			
Угрозы выявления паролей	средняя вероятность (5)	0,35	средняя	актуально
Угрозы удаленного запуска приложений	средняя вероятность (5)	0,35	средняя	актуально
Угрозы внедрения по сети вредоносных программ	средняя вероятность (5)	0,5	средняя	актуальная
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	средняя вероятность (5)	0,5	средняя	актуально
Угрозы типа "Отказ в обслуживании"	средняя вероятность (5)	0,35	средняя	актуально

Для расчета коэффициента реализуемости угроз Y применяется следующее соотношение:

$$Y = (Y_1 + Y_2)/20 \ (1)$$

1.7. Модель нарушителя

Нарушитель – это лицо или объект, случайно или преднамеренно выполняет действие, которое приводит к нарушению информационной безопасности.

Исходя из анализов и оценки экспертов, был сделан вывод что нарушители делятся на два типа:

- внешние нарушители – это постороннее лицо, не сотрудник предприятия, которое не может находиться на территории без сопровождения ответственного;
- внутренние нарушители – это работник предприятия, который имеет доступ на территории предприятия и может свободно передвигаться.

После анализа документов и оценки нарушителей, были описаны категории таких нарушителей:

- Криминальные структуры;
- Потенциальные нарушители, хакеры;
- Недобросовестные партнеры;
- Технический персонал провайдера услуг;
- Представители охраны и аварийных структур;
- Внешние субъекты (физические лица).

Таким образом, были выделены внешние нарушители со следующими способностями:

- осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений;
- осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена;
- осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
- осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИСПДн, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны.

После анализа выше перечисленного, была разработана модель нарушителя для объекта информатизации ООО «Газпром Интернешнл», в таблице 3 это показано.

Таблица 3 – Предполагаемый нарушитель

№	Описание нарушителя	Тип нарушителя	Описание возможностей нарушителя
1	Лица, которые обладают доступом к ИСПДн, но они не имеют доступ к ПДн (вспомогательный персонал).	Внутренний	-Имеют доступ к части информации хранящейся в информационной системе; -Имеют представление о характеристиках объекта и топологию строения системы; -Знает данные учетных записей и может достать от пароли зарегистрированных учетных записей; -Может изменить состав системы (устанавливать, удалять или изменять программы, производить съем информации, модификацию информации и (или) уничтожать информацию).
2	Пользователи зарегистрированные в информационной системе персональных данных, имеющие к ней допуск и осуществляющий доступ к ресурсам с рабочего места (основной	Внутренний	-Данный нарушитель имеет представление о топологии информационной структуре ИСПДн и ее характеристиках; -Имеет легальный доступ к ПДн; -Располагает именами учетных записей и возможность выявления паролей зарегистрированных пользователей; -Возможность изменять конфигурацию системы (устанавливать программно-аппаратные закладки, производить съем

№	Описание нарушителя	Тип нарушителя	Описание возможностей нарушителя
	персонал).		информации, модификацию информации и (или) уничтожать информацию).
3	Пользователи зарегистрированные в информационной системе персональных данных, имеющие к ней допуск и осуществляющий доступ к ресурсам через удаленный доступ (основной персонал).	Внутренний	-Данный нарушитель имеет такие же возможности, что и предыдущие нарушители № 1 и № 2; -Имеет представление о топологии информационной структуре ИСПДн и ее характеристиках; -Имеет легальный доступ к ПДн; -Располагает именами учетных записей и возможность выявления паролей зарегистрированных пользователей; -Возможность изменять конфигурацию системы (устанавливать программно-аппаратные закладки, производить съем информации, модификацию информации и (или) уничтожать информацию).
4	Зарегистрированные пользователи имеющие права системного администратора информационной системы персональных данных (основной персонал).	Внутренний	-Данный вид нарушителя обладает всеми возможностями предыдущий типов нарушителей № 1, 2 и 3; -Имеет полную информацию о информационной системе персональных данных; -Обладает информацией о техническом и программно-прикладном обеспечении; -Обладает информацией конфигурации информационной системы персональных

№	Описание нарушителя	Тип нарушителя	Описание возможностей нарушителя
			данных; -Имеет доступ ко всем техническим средствам информационной системы персональных данных и ее данным; -Обладает легальными правами конфигурирования и администрирования системой.
5	Разработчики-программисты, поставщики прикладного программного обеспечения.	Внешний	-Внедрение программно-аппаратных закладок; -Внесение ошибок в программный код продукта, недекларированные возможности продукта, вредоносных программ; -Обладание информации о топологии, технических средствах или любых данных о информационной системы персональных данных;
6	Лица, без легитимного допуска к системе персональных данных, поставляющие услуги.	Внешний	-Обладает возможностью внедрения программно-аппаратных закладок; -Обладание информации о топологии, технических средствах или любых данных о информационной системы персональных данных;

Таким образом, из описанных нарушителей из таблицы 24 «Описание нарушителя» можно сделать вывод, что опасным для объекта информатизации ООО «Газпром Интернешнл» являет внутренний

нарушитель, имеющий допуск к обработке, сопровождению или техническому обслуживанию информационной системы персональных данных.

1.8. Вывод по результатам анализа объекта

В результате анализа объекта информатизации ООО «Газпром Интернешнл», были выявлены уязвимости и каналы утечки информации. Это было необходимо для дальнейшей работы по разработке и внедрению системы защиты информации на данном объекте. Таким образом, мы узнали слабые места объекта, которым стоит уделить пристальное внимание.

Данный объект имеет «особенности», которые стоит учитывать при разработке системы защиты информации. Это и то, что в зимнее время нарушитель может проникнуть на охраняемую территорию по льду, так и не возможность установки забора по периметру занимаемого земельного участка.

ГЛАВА 2. АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

После анализа предприятия, помещения и средств, на которых будет обрабатываться конфиденциальная информация, необходимо рассмотреть средства защиты для устранения уязвимых аспектов АС.

Для устранения данных уязвимостей используют меры защиты информации:

- Организационные;
- Технические;
- Организационно-технические.

2.1. Организационные меры защиты информации

Перед применением технических мер защиты информации реализуют организационные меры. Для данного объекта информатизации используются следующие меры защиты информации:

- Составлены инструкции для исполнителей;
- Определен перечень лиц, допущенных в помещение где обрабатывается конфиденциальная информация;
- Назначен администратор безопасности и люди ответственные за данное помещение;
- В нерабочее время помещение, где обрабатывается конфиденциальная информация, закрывается и встает под охранную сигнализацию;
- Установлен запрет на пронос: папок, телефонов и других предметов, с помощью которых возможно пронести из помещения конфиденциальную информацию.

2.2. Виды технических средств защиты информации

Прежде чем выбирать какими устройствами стоит закрывать те или иные уязвимости, необходимо определить, какие бывают и для чего их применяют.

Средства защиты информации — это средства предназначенные для устранения перехвата, изменения или уничтожения информации.

1) Технические средства - один из основных видов защиты информации. К данному виду относятся механические, электромеханические, электронные и другие аппаратные устройства. Эти устройства либо препятствуют проникновению в защищаемое помещение, либо скрывают информацию. К таким средствам относятся: сигнализации, генераторы шума, сетевые фильтры и сканирующие радиоприемники.

2) Программные средства – данный вид включает в себя программы, которые идентификацию пользователей, контроля доступа, шифрования информации, удаления временных файлов, тестового контроля системы защиты и др. К таким средствам защиты относятся DLP-системы, средства защиты от НСД, криптографические средства и антивирусные программы.

3) Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

4) Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия).

2.3. Производители средств защиты информации

Для подбора средств защиты необходимо проанализировать рынок по их производству, какие имеются производители, что они предоставляют и

как это можно использовать для объекта. На рынке средств защиты наиболее распространёнными производителями являются:

1) ООО «АННА» - является научно-производственным предприятием, осуществляющим разработку и серийное производство технических средств защиты информации. Основные виды их продукции:

- технические средства защиты информации, реализующие функцию экстренного гарантированного уничтожения программного и информационного обеспечения на магнитных носителях посредством магнитного воздействия (серия "Стек-НСxxx"). На рисунке 6 представлено устройство для утилизации жестких дисков.

Рисунок 6 – Утилизатор для жестких дисков компьютеров

- технические средства защиты от утечки по каналам ПЭМИН (серии "Соната-Р3", "Соната-Р3.1" и "Соната-РСх"). На рисунке 7 представлен внешний вид средства защиты информации «Соната-Р3.1».

Рисунок 7 – Внешний вид Сонаты-Р3.1

- технические средства защиты от утечки по акустическому и виброакустическому каналам (серия "Соната-АВхх"). На рисунке 8 представлен внешний вид «Соната АВ».

Рисунок 8 – Внешний вид генераторного блока «Соната АВ»

2) АО «Лаборатория противодействия промышленному шпионажу» - осуществляет исследования и разработки в области создания новых технических средств защиты информации. Виды продукции:

- Система постановки виброакустических и акустических помех (ЛГШ-404, Виброэкран ЛИСТ-1, ЛВП-10). На рисунке 9 представлен внешний вид ЛГШ-404.

Рисунок 9 – Внешний вид ЛГШ-404

3) Лаборатория «ППШ» разрабатывает защищённые кабинки (КПЗИ-1) – это кабинки, предназначенные для проведения закрытых мероприятий и разговоров по телефонам спецсвязи. На рисунке 10 представлено, как выглядит кабинка для переговоров.

Рисунок 10 – Внешний вид защищенной кабинки

- Персональные электронно-вычислительные машины в защищенном исполнении. Эти устройства используют для проведения совещаний или обсуждения конфиденциальной информации. Данный вид устройства разработан в формате моноблока, таким образом, устройство защищено от перехвата информации по каналу ПЭМИН. Один из защищенных ПЭВМ представлен на рисунке 11.

Рисунок 11 – Внешний вид ПЭВМ «ЛИС-40.1»

4) Группа компаний «Конфидент» - Центр защиты информации ГК «Конфидент» разрабатывает линейку сертифицированных средств защиты информации Dallas Lock для защиты конфиденциальной информации на рабочих станциях и серверах под управлением ОС Windows и Linux; разграничения; контроля доступа; межсетевого экранирования; доверенной загрузки; централизованного управления и мн. др. На рисунке 12 представлен внешний вид коробочного издания.

Рисунок 12 – Внешний вид коробочного издания Dallas Lock

5) ООО «Код Безопасности» - разрабатывает средства защиты от несанкционированного доступа, антивирус, межсетевые экраны. Один и продуктов - СЗИ Secret Net Studio — это комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Продукт объединяет в себе функционал нескольких средств защиты «Кода Безопасности» (СЗИ от НСД Secret Net, межсетевой экран TrustAccess, СЗИ Trusted Boot Loader, СКЗИ «Континент-АП»).

2.4. Сравнение средств защиты информации

В результате анализа объекта были получены каналы утечки информации, которые будут разделены на две группы:

- Несанкционированный доступ к информации, хищение, удаление и изменение;
- ПЭМИН.

Для группы Несанкционированный доступ к информации, хищение, удаление и изменение, соответствуют следующие каналы утечки информации:

- несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах;
- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации.

Для группы ПЭМИН, соответствуют следующие каналы утечки информации:

- побочные электромагнитные излучения информативного сигнала от технических средств,
- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации.

Для выбора подходящих средств защиты информации нужно сравнить средства защиты от разных производителей. Далее в таблице 4 будут рассмотрены средства защиты информации для первой группы - Несанкционированный доступ к информации, хищение, удаление и изменение.

Таблица 4 – Сравнение СЗИ от НСД

Критерии сравнения	Dallas Lock 8.0-К	Secret Net Studio 8.8	Страж NT
Класс защищенности	5	5	5
Уровень контроля НДВ	4	4	4
Класс защиты межсетевого экрана	4	4	-
Класс автоматизированных систем	До класса 1Г	До класса 1Г	До класса 1Г
Совместимость с Windows 7 Professional	+	-	+
Наличие сертификата ФСТЭК	ФСТЭК России № 2720 от 25 сентября 2012 г. Действителен до 25 сентября 2026 г.	ФСТЭК России № 3745 от 16 мая 2017 г. Действителен до 16 мая 2020 г. Продлен до 16 мая 2025 г.	ФСТЭК России № 3553 от 20 апреля 2016 г. Действителен до 20 апреля 2024 г.
Стоимость, руб.	8 826.00	10 500.00	6 000.00
Стоимость технической поддержки, руб.	1 500.00	-	-

Таким образом, на основании данного анализа средств защиты информации от НСД было выбрано СЗИ «Dallas Lock 8.0-К». Данный выбор был сделан на основе средней стоимости СЗИ и функционалу, который удовлетворяет все предъявленные требования.

Далее в таблице 5, буду рассмотрены антивирусные программы.

Таблица 5 – Сравнение антивирусный программ

Критерии сравнения	Dr.Web Enterprise Security Suite	Kaspersky Endpoint Security 11 для Windows
Уровень доверия	2	-
Профиль защиты средств антивирусной защиты	2А, 2Б, 2В, 2Г	2Б, 2В, 2Г
Совместимость с Windows 7 Professional	+	+
Наличие сертификата ФСТЭК	ФСТЭК России № 3509 от 27 января 2016 г. Действителен до 27 января 2019 г. Продлен до 27 января 2024 г.	ФСТЭК России № 4068 от 22 января 2019 г. Действителен до 22 января 2024 г.
Стоимость, руб.	7 260.00	11 015.00

Таким образом, на основании данного анализа средств защиты от вредоносных программ, выбор пал на СЗИ «Dr.Web Enterprise Security Suite». Данный выбор был сделан на основе низкой стоимости СЗИ и функционалу, который удовлетворяет все предъявленные требования.

Последним рассмотренным средством защиты информации будет каналы группы ПЭМИН, в таблице 6 это рассмотрено.

Таблица 6 – Сравнение средств защиты по каналу ПЭМИН

Характеристика	Соната-Р3.1	ЛГШ-513
Виды индикации (отображаемая информация)	Световая, звуковая (исправность/отказ)	Световая, звуковая (исправность/отказ)
Дистанционное управление	1) пульт управления "Соната-ДУ4.3" в	Проводное дистанционное

Характеристика	Соната-Р3.1	ЛГШ-513
	комплексе с блоком питания и управления "Соната-ИП4.х"; 2) пульт управления "Соната-ДУ4.4"	управление и контроль (через программно-аппаратный комплекс «Паутина»)
Электропитание	сеть 220 В +10%/-15%, 50 Гц	187÷242
Продолжительность непрерывной работы, часов, не менее	8	круглосуточно
Габаритные, мм не более	500, 330, 65	230, 110, 50
Наличие сертификата ФСТЭК	ФСТЭК России № 3539 от 24 марта 2016 г. Действителен до 24 марта 2024 г.	ФСТЭК России № 3521 от 12 февраля 2016 г. Действителен до 12 февраля 2024 г.
Стоимость, руб.	33 000.00	39 000.00

Таким образом, на основании данного анализа средств защиты информации от побочно-электромагнитных излучений и наводок было выбрано СЗИ «Соната-Р3.1». Данный выбор был сделан на основе низкой стоимости СЗИ и функционалу, который удовлетворяет все предъявленные требования.

2.5. Выбор средств защиты информации для объекта

После сравнительного анализа средств защиты информации для автоматизированных систем были выбраны следующее оборудование: от НСД- СЗИ Dallas Lock 8.0-К. Внешний вид коробочного издания представлен на рисунке 12.

Рисунок 12 – Выбранное СЗИ от НСД

От вредоносных программ- антивирусная программа «Dr.Web Enterprise Security Suite». На рисунке 13 представлен логотип компании «Dr. Web».

Рисунок 13 – Выбранная компания антивирусной программы

От побочно-электромагнитных излучений и наводок – СЗИ НПО «АННА» «Соната-Р3.1». На рисунке 14 представлен установленное устройство в помещении.

Рисунок 14 – Установленная «Соната-Р3.1» в помещении № 215б

Исходя из выше сказанного, для помещения, где обрабатывается конфиденциальная информация были выбраны подходящие средства защиты информации, которые закрывают все обнаруженные каналы утечки информации. Перед установкой средств защиты информации следует закупить их у производителя, в таблице 7 показана итоговая стоимость закупки оборудования.

Таблица 7 – Стоимость закупки СЗИ у производителя

Название	Количество, шт.	Цена, за шт., руб.
СЗИ от НСД «Dallas Lock 8.0-К»	3	10 326.00

Название	Количество, шт.	Цена, за шт., руб.
СЗИ от вредоносных программ «Dr.Web Enterprise Security Suite»	3	7 260.00
СЗИ от ПЭМИН «Соната-Р3.1»	1	33 000.00
	Итог	85 758.00

2.6. Вывод результатам выбранных средств защиты информации

Таким образом, анализ производителей и рынка средств защиты информации на помог определится с наиболее подходящими устройствами, которые помогут в защите автоматизированной системе в помещении.

На основе этих анализов был проведен сравнительный анализ средств защиты информации и были выбраны те, которые удовлетворяют таким требованиям как: низкая стоимость, легкость в установки и простота в эксплуатации.

После закупки средств защиты информации, были установлены на автоматизированных системах, на рисунке 15 показано их расположение.

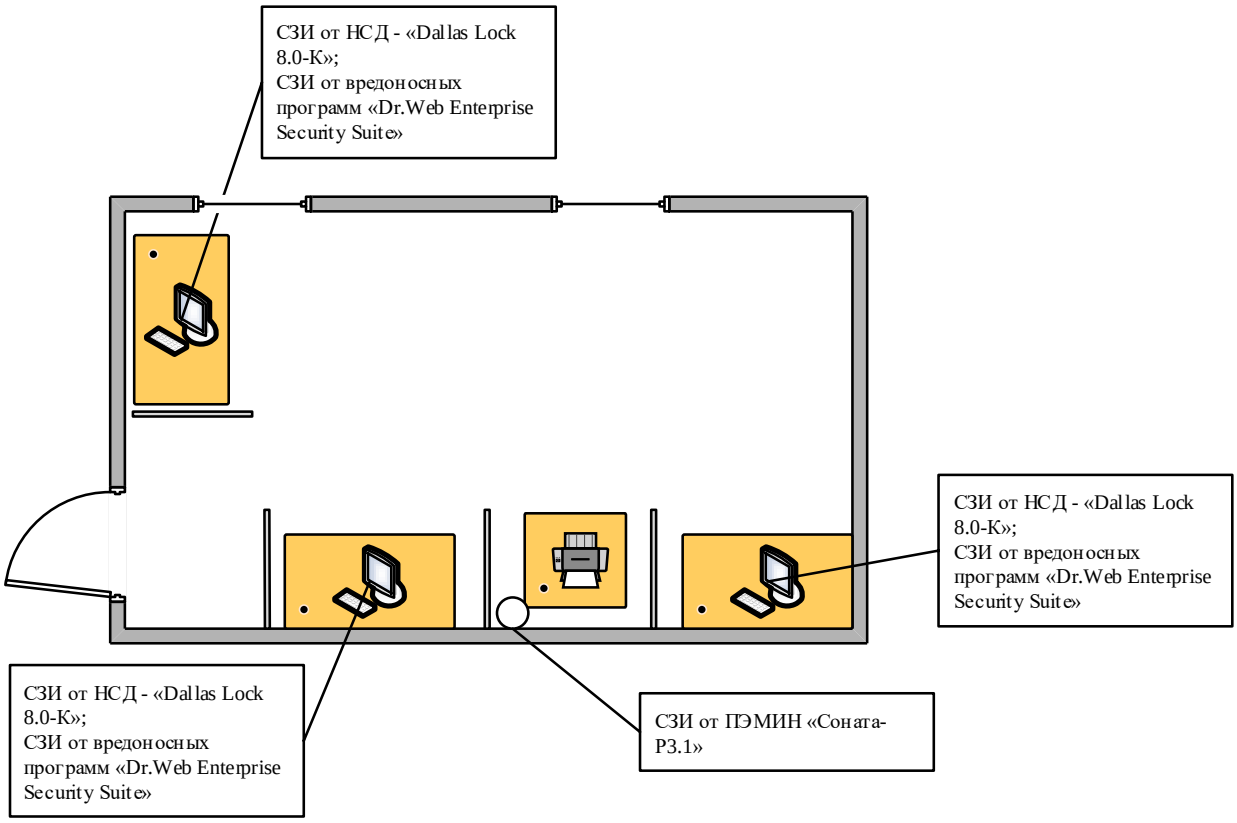


Рисунок 15 – Схема расположения средств защиты информации в помещении

В результате применяемые средства защиты информации закрыли обнаруженные уязвимые каналы утечки информации для автоматизированных систем.

ГЛАВА 3. ПРОВЕДЕНИЕ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

3.1. Разработка документов

После установки программ антивирусной защиты, средств от несанкционированного доступа и генератора шума на объекте информатизации следует документальное оформление следующих документов:

- Технический паспорт (приложение Б);
- Акт классификации;
- Инструкция по эксплуатации средств защиты информации для персонала;
- Разрешительная система доступа (приложение А);
- Список лиц, допущенных к работе.

3.2. Определение и описание

Аттестация представляет собой процесс проверки объектов информатизации на соответствия требованиям по защите информации лицензиатами – это организации, которые получили сертификат на осуществление работ в данной области от ФСТЭК.

Аттестация автоматизированных систем представляет собой комплексную подготовку АС и ее оценка соответствия требованиям безопасности информации. Результатом аттестационных испытаний является заключение, по результатам которого выдается или не выдается аттестат соответствия.

В данной работе был описан процесс со стороны разработчика системы защиты информации, в этой главе будет рассмотрен процесс аттестации автоматизированной системы со стороны лицензиата.

Аттестационные испытания проводятся для:

- Автоматизированных систем;
- Защищаемых помещений.

3.3. Порядок аттестации

Порядок и действия при проведении аттестационных испытаний описан проходит в следующем порядке:

1) Перед аттестацией заказчик предоставляет органу лицензиату следующие документы:

- Акт классификации;
- Модель угроз;
- Модель нарушителя;
- ТЗ на реализацию разработки СЗИ;
- Технический паспорт разработанный на каждый АРМ;
- Документация на систему защиты;
- Организационно-распорядительные документы;
- Акты установки средств защиты информации;
- Документы, содержащие результаты описания уязвимостей объекта информатизации.

2) Что необходимо сделать при аттестации:

1. Программа и методика аттестационных испытаний

На основе анализа предоставленных документов от заказчика, лицензиат разрабатывает программу и методики аттестационных испытаний. В данный документ входят следующие данные: наименование и краткое описание архитектуры, класс защищенности информационной системы, категорию значимого объекта, ФИО экспертов органа по аттестации (которые проводят аттестационные испытания), наименование и реквизиты документов ФСТЭК России на основании которых проводились аттестационные испытания, актуальные угрозы информационной безопасности для данного объекта информатизации.

В документе «Программа и методика аттестационных испытаний» описан процесс обследования объекта информатизации в условиях его эксплуатации, проведение аттестационных испытаний, сроки проведения испытаний и ответственного за проведение каждой работы. В частях,

описывающих аттестационные испытания, должны быть указаны: порядок, условия и методы испытаний, применяемы для испытания СЗИ установленных на объекте информатизации (приложение Г).

Программа и методика аттестационных испытаний согласовывается с органом аттестации и владельцем объекта информатизации.

2. Аттестационные испытания включают следующие мероприятия и работы:

- Оценка сведений, предоставленных владельцем объекта информатизации и отправленных документов в орган по аттестации на соответствие требованиям по защите информации;
- Обследование объекта информатизации на соответствие предоставленным сведениям содержащихся в документах владельца.
- Проверка наличия: документа о анализе уязвимостей объекта, сведений о установленных СЗИ и наличии их в реестре ФСТЭК;
- Проверка наличия у владельца объекта информатизации, ответственных за защиту информации, в ходе эксплуатации объекта информатизации;
- Оценка уровня подготовки и знаний работников объекта информатизации;
- Оценка принятых организационных мер защиты информации и оценка достаточности принятых таких мер для защиты от актуальных угроз информационной безопасности;
- Оценка принятых технических средств защиты информации и оценка достаточности принятых таких мер для защиты от актуальных угроз информационной безопасности;
- Для проведения работ по испытаниям СЗИ от НСД, эксперты органа по аттестации осуществляют тестирование ее функции безопасности, анализ эффективности, а также совершают попытки обхода СЗИ при помощи средств тестирования.

3) В ходе проведения аттестационных испытаний владелец может изменять состав и архитектуру объекта информатизации, для выполнения требований по защите информации.

4) По результатам аттестационных испытаний оформляется заключение (приложение Д), в этом документе входят следующие данные:

- Наименование объекта информатизации, состав программно-технических средств, программных средств и средств защиты информации;
- Класс защищенности АС;
- ФИО эксперта, проводившего аттестационные испытания;
- Дата утверждения программы и методик аттестационных мероприятий;
- Сроки проведения аттестационных испытаний;
- Наименование и реквизиты документов ФСТЭК России, на соответствие которых проводились аттестационные испытания;
- Результаты аттестационных испытаний с описанием: проведенных работ в соответствии с программой и методикой аттестационных испытаний, указанием сроков работ, экспертов, проводивших аттестационные испытания, заключение о соответствии или несоответствии требованиям по защите информации каждой проделанной работы;
- В случаи обнаружения, в ходе проведения аттестационных испытаний несоответствий, дают рекомендации по устранению недостатков;
- Выводы о выдачи или не выдачи аттестата соответствия по результатам аттестационных испытаний или необходимость доработки средств защиты информации.

5) Заключение и протоколы, после проведения аттестационных испытаний, отправляются в течение 5 рабочих дней с момента утверждения органом по аттестации владельцу объекта информатизации.

Таким образом, в данной работе по выше описанным требованиям будет проходить аттестация автоматизированной системы.

Согласно «Временной методики оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации» Гостехкомиссия России, измерения по каналу ПЭМИ проводились на расстоянии 1 метра от ОТСС, на рисунке показано размещения аппаратуры измерения.

3.4. Проведенные работы по аттестации объекта информатизации

Данные аттестационные испытания и оформление соответствующих документов о прохождении таких испытании имеют право только органы по аттестации.

Аттестация проходит в следующем порядке:

- Анализ объекта на соответствие описанному в документах, присланных от заказчика;
- Составить программы и методики аттестационных испытаний;
- Определить уязвимые направления;
- Определить границу контролируемой зоны;
- Провести оценку защищенности объекта информатизации, при выявлении разведопасных направлениях, требуется установка СЗИ и последующей оценки защищенности примененных средств защиты информации;
- Оформление заключения о прохождении или не прохождении аттестационных испытаний;
- В случае, положительного прохождения аттестационных испытаний, оформляется аттестат соответствия.

Согласно этому плану и были выполнены работы:

1) Программа и методики аттестационных испытаний составляется для определения методов, оценки и сроков проводимых испытаний на объекте информатизации.

2) Протокол оценки защищенности проводится для

3) В конце оформляется заключение, в которой описывается весь перечень состава ОТСС, ВТСС, программного обеспечения, средств защиты и результат аттестационных испытаний.

4) Аттестат соответствия

3.5. Оценка защищенности автоматизированной системы

Для оценки защищенности автоматизированной системы по каналам ПЭМИН, проводятся мероприятия и расчеты описанные ранее во «Временной методике…», определяются зоны, в которых возможен съем конфиденциальной информации (R_2 и r_1) с автоматизированной системы. Для проведения данных исследований необходимо специальное оборудование, в таблице 8 оно приведено.

Таблица 8 – Перечень контрольно-измерительного оборудования

№ п/п	Наименование средств измерений и вспомогательного оборудования	Тип	Диапазон частот, МГц
1.	Токосъемник	ТИ 2-4	0,009-400
2.	Анализатор спектра	FPH13 (с опцией FPH-K43)	0,005-13600
3.	Антенна биконическая измерительная	НБА-02	0,009-2500
4.	Комплект антенный измерительный	АИК 1-40/10	0,9-12400
5.	Антенна рамочная измерительная	НРА-02	0,009-30
6.	Пробник напряжения	П-400	0,0001-400
7.	Эквивалент сети для проведения специсследований	ЭС-1000СИ	0,009-500
8.	Логопериодическая измерительная антенна	ПИРАМИДА	1000-12500
9.	Селективный нановольтметр	Unipan-233	0,0000015-0,15
1.	Осциллограф	С1-112А	До 10
2.	Специализированные тестирующие программы ЗАО «ЦБИ-сервис»	-	-
3.	Антенна передающая для проведения объектовых специсследований	КУБ-М	0,009-1000
4.	Вспомогательный генератор сигналов	Источник	0,001-10000
5.	Индуктор магнитный	ИМ-2	0,00002-600

На рисунке 16 представлена схема расположения контрольно-измерительного оборудования, с помощью которого проводились исследования.

С помощью этих исследований, на автоматизированной системе определялись зоны, в пределах которой возможен съем информации, зоны наводок на линии питания и слаботочных систем.

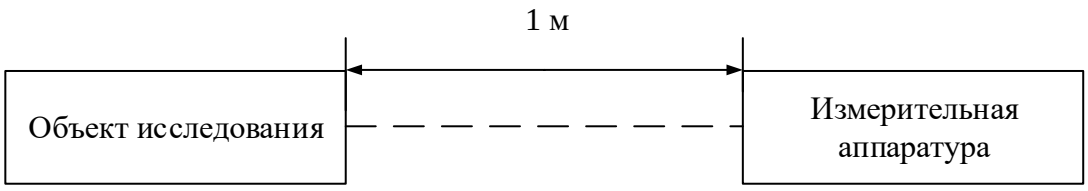


Рисунок 16 – Схема расположения объекта исследования и измерительной аппаратуры

Согласно рисунку 16, были исследованы автоматизированные системы. Результаты определения зоны R_2 в таблице 9, рассчитывается зона r_1 таблице 10 описаны результаты.

Где:

- F - частота;
- K - общее число спектральных составляющих;
- R_0 – рекомендуемое расстояние установки измерительного оборудования;
- ρH_i – напряженность электромагнитного поля по магнитной составляющей, мкВ/м;
- E_i - напряженность электромагнитного поля по электрической составляющей, мкВ/м;
- $E_{\text{ш}}(\rho H_{\text{ш}i})$ - напряженность электромагнитного поля по электрической (магнитной) составляющей за счет шума, мкВ/м;

- L_1 – расстояние от ОТСС до границы ближней и промежуточной зон, м;
- L_2 – расстояние от ОТСС до границы промежуточной и дальней зон, м;
- f_i – частотный -й спектральной составляющей информативного сигнала;
- R_{2_i} – радиус контролируемой зоны для -й составляющей спектра информативного сигнала, м;
- E_{0_i} – уровень напряженности электромагнитного поля при работе ОТСС в тестируемом режиме;
- $E_{ш_i}$ – уровень напряженности электромагнитного поля при выключенном ОТСС;
- $E_{c_i}(\rho H_{c_i})$ - напряженность электромагнитного поля по электрической (магнитной) составляющей, созданная информативным сигналом, мкВ/м;
- $E_{1_i}(\rho H_{1_i})$ – значение напряженности информативного сигнала на границе ближней и промежуточной зон, мкВ/м;
- $E_{2_i}(\rho H_{2_i})$ – значение напряженности информативного сигнала на границе промежуточной и дальней зон, мкВ/м;
- $E_{0_i}(\rho H_{0_i})$ – измеренный уровень напряженность электромагнитного поля при работе ОТСС в тестируемом режиме, мкВ/м;
- ρ= 377 Ом – волновое сопротивление свободного пространства.

Таблица 9 – Расчет зоны R_2

№ fi	F, МГц	$E_{с+ш}$, дБ	$E_{ш}$, дБ	$E_{с}$, дБ	R, м
АРМ № 1					
1	74,26	68,9	33,7	68,9	13,85
2	222,76	49,4	24,6	49,4	7,60
3	371,28	27,2	23,4	24,9	1,99
4	519,8	36,7	22,4	36,5	4,90
АРМ № 2					
1	74,26	70,9	36,5	70,9	13,23

№ fi	F, МГц	$E_{с+ш}$, дБ	$E_{ш}$, дБ	$E_{с}$, дБ	R, м
2	222,76	52,3	26,4	52,3	8,13
3	371,28	29	23,9	27,4	2,23
4	519,8	38,3	23,4	38,2	5,26
АРМ № 3					
1	74,26	67,9	34,9	67,9	12,20
2	222,76	46,9	29,4	46,8	4,98
3	371,28	33,8	30,3	31,2	1,93
4	519,8	41,5	33,1	40,8	2,85

При проведении исследовании на автоматизированной системе было обнаружено 4 частоты, на которых был обнаружен сигнал. Таким образом, при расчете зоны R_2 для автоматизированной системы был получен результат 13,85 м.

После расчет зоны R_2 следует определись и зону r_1, в таблице показаны расчеты, полный расчет па частотам представлен в приложении В.

Где:

- $U_{(с+ш)_i}$ – напряжение смеси обнаруженных компонент тест-сигнала и шума, дБ;
- l – протяженность линии ВТСС между точками А и Б, м;
- $U_{ш_i}$ – шум в линии, дБ;
- $U_{с_i}$ – напряжение сигнала в линии, дБ;
- $П_i$ – показатель защищенности, дБ;
- $К_{П_i}$ – коэффициент погонного затухания наведенных сигналов в исследуемой линии, дБ/м;
- $U_{1изм_i}$ – напряжение специально созданного сигнала, измеренное на частоте f_i исследуемой линии в непосредственной близости от ОТСС, мкВ;
- $U_{2изм_i}$ – напряжение специально созданного сигнала, измеренное на частоте f_i исследуемой линии на некотором удалении от ОТСС, мкВ;
- R_i – максимальная длина пробега исследуемой линии, на которой возможно выделение информативного сигнала, м;

- $R_{КЗ}$ – реальный пробег исследуемой линии до границы контролируемой зоны, м.

На рисунке 17 представлена принципиальная схема измерения наводок от автоматизированной системы.

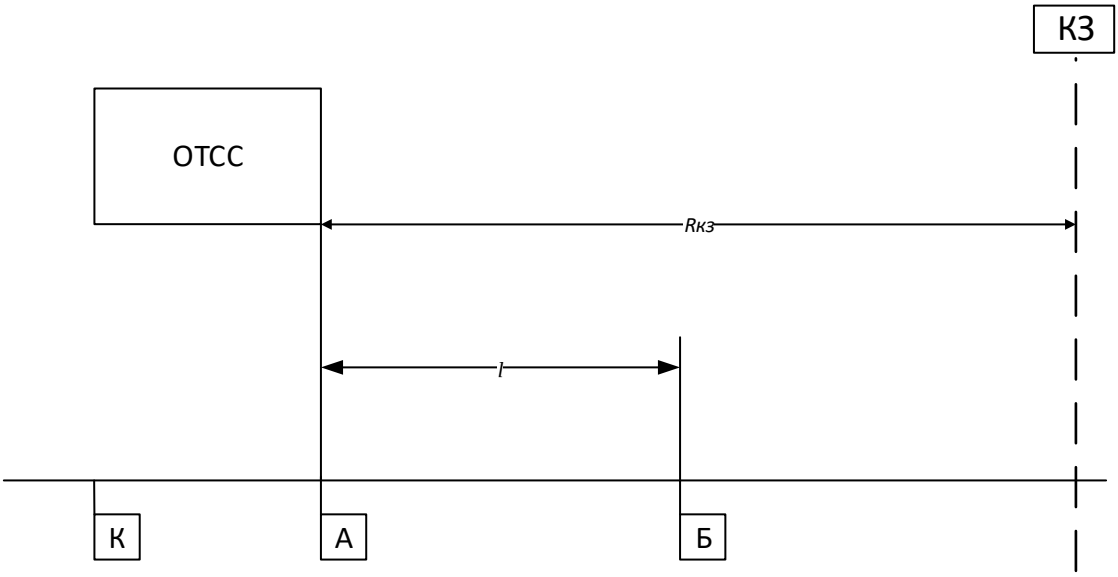


Рисунок 17 – Схема проведения исследований линий наводок

Где:

l= 12 м;

$R_{кз}$=50 м;

Таблица 10 – Расчет наводок на линии

№ fi	fi, МГц	U(с+ш)i, дБ	Uшi, дБ	Uci, дБ	U1 измi. мкВ	U2 измi, мкВ	Кпi, дБ/м	Ri, м	Rкз, м
АРМ № 1									
1	74,26	25	15	24,54	281,8	6,3	2,75	7,1	50
2	222,76	22	16	20,74	89,1	5,6	2	7,4	50
АРМ № 2									
1	74,26	28	24	25,80	223,9	7,1	2,5	4,7	50
2	222,76	23	19	20,80	125,9	7,9	2	5,9	50
АРМ № 3									
1	74,26	24	20,2	21,66	158,5	5,3	2,458333	4,7	50
2	222,76	22	18,5	19,43	199,5	7,5	2,375	4,6	50

По результатам расчет зоны в пределах которой осуществляются наводки на линии питания и слаботочных систем, была получена зон 7,4 м, в пределах которой это будет возможно, полный расчет па частотам представлен в приложении В.

После проведенных исследований на автоматизированной системе по каналу ПЭМИН, были получены результаты, по которым можно сделать вывод что автоматизированная система имеет зону R_2 – 13,85 м, а r_1 – 7,4 м.

Таким образом, на основе полученных данных о автоматизированной системе проверяется следующее соотношение:

$$R_2 \leq R_{\text{кз}} \quad (1).$$

Где:

R_2 – это зона в пределах которой возможен съем информации;

$R_{\text{кз}}$ – это зона контролируемой зоны.

Для рассматриваемого объекта информатизации расстояние до ближайшего места съема информации по каналу ПЭМИ составляет $R_{\text{кз}} = 5$ м., следовательно соотношение (1) не выполняется, требуется применение средств защиты информации.

Вывод: защищенность АС от утечки информации по каналу ПЭМИН не обеспечивается, так как зона $R_2 = 13{,}85$ м. превышает зону $R_{\text{кз}} = 5$ м.

3.6. Оценка эффективности принятых мер защиты

Данная оценка проводится для анализа применяемых средств защиты информации. Если при оценке защищенности обнаружено, что имеются каналы утечки информации, то устанавливаются средства защиты информации и проводят оценку эффективности принятых мер защиты информации.

Оценка эффективности защиты информации проводилась, для:

1) Канала от НСД

Для проверки технических средств от несанкционированного доступа применяют следующие:

- Тестируют систему с помощью обхода или других способов проникновения;
- Используют программы для снятия контрольных сумм, для проверки целостности системы.

Для определения уровня принятых мер защиты вводятся значения от 1 до 4. Уровень 1 соответствует применением средств защиты информации не ниже 4 класса, 4 уровня доверия, а также СВТ не ниже 5 класса. Уровень 2 соответствует применением средств защиты информации не ниже 5 класса, 5 уровня доверия, а также СВТ не ниже 5 класса. Уровень 3 соответствует применением средств защиты информации не ниже 6 класса, 6 уровня доверия, а также СВТ не ниже 5 класса. Уровень 4 соответствует применением средств защиты информации не ниже 6 класса, 6 уровня доверия, а также СВТ не ниже 6 класса.

Согласно выше описанным уровням, определяется эффективность средств защиты, установленных на АС.

По результатам проверки средств защиты информации на установленных автоматизированной системе, уровень эффективности защит информации соответствует 2 уровню.

2) Для канала ПЭМИН

Для определения защищённости автоматизированной системы по каналам ПЭМИН, проводятся оценка защищенности и расчет зоны R_2, в предыдущем пункте был расписан весь процесс расчетов и измерений.

Таким образом, были проведены мероприятия, в ходе которых проверялись требования по защите информации. Порядка проведения испытаний прописаны в документе – программа и методики аттестационных испытаний, которые согласовывались с заказчиком.

В ходе проверки автоматизированной системы были рассчитаны зоны, и обосновали необходимость применения генератора шума в помещении от

утечек по каналу ПЭМИН. Так, как с применением сертифицированного генератора шума выполняются требования по защите информации по каналу ПЭМИН для автоматизированной системы (приложение В).

3.7. Заключение по результатам аттестационных испытаний

По результатам проведенных аттестационных испытаний автоматизированной системы, оформляется заключение, где описан: состав техники, средств защиты информации и итоги испытаний (приложение).

При успешно прохождении аттестационных испытаний оформляется аттестат соответствия (приложение).

3.8. Анализ рисков

После проведения: анализа угроз конфиденциальной информации, установки средства защиты информации и проведения аттестационных испытаний были рассчитаны риски утечки информации по ранее выявленным каналам утечки информации, в таблице 11 они показаны.

Таблица 11 - Расчеты рисков после проведения аттестационных испытаний

Наименование угрозы	Возможность реализации угрозы	Достигнутый уровень реализации рисков
Угрозы утечки информации по техническим каналам		
Угрозы утечки видовой информации	средняя	малая вероятность
Угрозы утечки информации по каналу ПЭМИН	средняя	малая вероятность
Угрозы НСД к ПДн, обрабатываемым на АРМ		
Угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой	средняя	малая вероятность
Угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение,	средняя	малая вероятность

Наименование угрозы	Возможность реализации угрозы	Достигнутый уровень реализации рисков
форматирование и т.п.) операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ		
Угрозы внедрения вредоносных программ	средняя	малая вероятность
Предоставление пользователям прав доступа (в том числе по видам доступа) к ПДн и другим ресурсам ИСПДн сверх необходимого для работы	высокая	низкая
Неумышленная (случайная) отправка ПДн по ошибочным адресам электронной почты	средняя	малая вероятность
Преднамеренное копирование доступных ПДн на неучтённые (в том числе отчуждаемые) носители в том числе печать неучтённых копий документов с ПДн на принтерах	средняя	малая вероятность
Неумышленное (случайное) добавление (фальсификация) ПДн	средняя	малая вероятность
Неумышленное (случайное) уничтожение доступных ПДн (записей, файлов, форматирование диска)	высокая	низкая
Преднамеренное уничтожение доступных ПДн (записей, файлов, форматирование диска)	высокая	низкая
Покинуть рабочее место с не заблокированной рабочей станцией	высокая	низкая
Подкючение к ИСПДн стороннего оборудования (компьютеров, дисков и иных устройств, в том числе имеющих выход в беспроводные сети связи)	средний	малая вероятность
Использование оборудования, оставленного без присмотра, паролей	средняя	малая вероятность
Внедрение вредоносных программ	высокая	низкая
Доступ к информации ИСПДн, выходящей за пределы контролируемой зоны вследствие списания (утилизации) носителей информации, содержащих ПДн	средняя	малая вероятность
Игнорирование организационных ограничений (установленных правил) при работе с ресурсами АСЗИ, включая средства защиты информации	высокая	низкая

Наименование угрозы	Возможность реализации угрозы	Достигнутый уровень реализации рисков
Нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации(в частности, ключевой, парольной и аутентифицирующей информации)	высокая	низкая
Не информирование о факте утраты (ключевой, парольной, аутентифицирующей а также любой другой информации ограниченного доступа)	высокая	низкая
Сетевые угрозы		
Угрозы "Анализа сетевого трафика" с перехватом передаваемой по сети информации	средняя	малая вероятность
Угрозы выявления паролей	средняя	малая вероятность
Угрозы удаленного запуска приложений	средняя	малая вероятность
Угрозы внедрения по сети вредоносных программ	средняя	малая вероятность
Угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации	средняя	малая вероятность
Угрозы уровня "Отказ в обслуживании"	средняя	малая вероятность

Таким образом, из анализа данной таблицы можно сделать вывод, что проведенные мероприятия по защите информации выполнили поставленные задачи. Данные автоматизированные средства ООО «Газпром Интернешнл» были защищены по выявленным каналам утечки информации.

3.9. Достигнутый уровень безопасности информации на предприятии

Исходя из таблицы 11, для каналов утечки с уровнем – низкая вероятность соответствует 7 каналов, с уровнем – малая вероятность соответствует 16. Таким образом, достигнутый уровень защищенности составляет 85,25%, итоговый полученный процент защищенности по внедрению средств защиты информации составляет 50,25%.

По результатам внедрения средств защиты информации можно сказать, что уровень безопасности объекта информатизации соответствует высокому.

3.10. Анализ экономики проведенных работ

Для экономической оценки проделанных работ по закупке, установке и проведении аттестационных испытаний необходимо произвести расчет затраченных ресурсов.

По результатам второй главы, были взяты следующие средства защиты информации:

- СЗИ от НСД «Dallas Lock 8.0-К»;
- СЗИ от вредоносных программ «Dr.Web Enterprise Security Suite»;
- СЗИ от ПЭМИН «Соната-Р3.1».

Еще следует учитывать в стоимость проведение аттестационных испытаний для автоматизированной системы. Для оптимального выбора органа по аттестации, будут рассмотрены организации в таблице 12.

Таблица 12 – Итоговой расчет закупок

Наименование	ООО «Центр безопасности информационных систем»	ООО «Единый центр аттестации и сертификации»	ООО «АСТ»
Количество АС, шт.	3	3	3
Цена, руб.	300 000,00	180 000,00	240 000,00

Исходя из приведенных цен и организаций, которые занимаются аттестацией, можно понять, что цена на аттестацию АС начинается от 180 тыс. рублей. Эти данные дают понять, к каким затратам следуют быть готовым при аттестации автоматизированной системы.

Выше были описана стоимость проведения аттестационных испытаний, за выбранный вариант была взята организация – ООО «Единый центр аттестации и сертификации», так как эта цена была низкой среди других представленных организаций. Для итогового расчета затраченных средств, для реализации системы защиты на АС и проведении АИ на соответствие требований по безопасности, в таблице 13 это показано.

Таблица 13 – Расчет итоговых затрат

№	Наименование СЗИ	Количество, шт.	Стоимость, руб.
1	СЗИ от НСД Dallas Lock 8.0-К	3	30 978.00
2	Антивирусная программа Dr.Web Enterprise Security Suite	3	21 780.00
3	СЗИ от ПЭМИН «Соната-Р3.1»	1	33 000.00
4	Аттестационные испытания	для 3 АС	180 000,00
		Итог	265 758,00

По результатам расчетов экономической составляющей данной работы: закупка, установка и проведение аттестации, для трех автоматизированных систем в помещении ООО «Газпром Интернешнл», будет составлять 265 758 рублей 00 копеек.

3.11. Вывод по результатам выполненных работ

По итогам аттестационных испытаний автоматизированной системы, было получено положительное заключение, оформлен аттестат соответствия по требования защиты информации.

Была проведена оценка защищенности, которая выявила не соответствие требованиям по защите информации, следовательно, были применены средства защиты информации. Данные каналы утечки информации были закрыты.

Рассчитана итоговая стоимость всех произведенных работ, включая подбор средств защиты информации и проведения аттестационных испытаний органом по аттестации.

Благодаря проведенным мероприятиям уровень объекта информатизации был повышен до высокого уровня защищенности.

ЗАКЛЮЧЕНИЕ

В ходе выполнения ВКР был произведен анализ помещения и автоматизированных систем ООО «Газпром Интернешнл». В результате были обнаружены угрозы и уязвимости, которые необходимо устранить.

Благодаря установке средств защиты информации, данные каналы были устранены. После проведения работ по установке защиты информации были проведены аттестационные испытания автоматизированных систем на соответствие требований по защите информации. Испытания показали полное соответствие данным требованиям.

Таким образом была повышена защищенность конфиденциальной информации, обрабатываемой на автоматизированных системах, все поставленные цели и задачи были выполнены в данной работе.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон Российской Федерации от 29 июля 2004 №98-ФЗ «О коммерческой тайне» // ГАРАНТ – 2011. №3543. – 168 с.

2. ФСТЭК России [Электронный ресурс]. Режим доступа: https://fstec.ru/ (дата обращения: 05.10.2022).

3. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка)». Утверждена ФСТЭК Российской Федерации 15.02.2008 [Электронный ресурс]. Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114spetsialnye-normativnye-dokumenty/379bazovaya-model-ugroz-bezopasnosti-perso-nalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii2008god (дата обращения: 20.10.2022).

4. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждена ФСТЭК Российской Федерации 14.02.2008.

5. Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных».

6. Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» // РГ – 2006. №4131. – 197 с.

7. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей Государственную тайну, содержащейся в Государственных информационных системах».

8. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9. DallasLock система защиты информации от несанкционированного доступа [Электронный ресурс]. Режим доступа: http://www.dallaslock.ru/ (дата обращения: 05.10.2022).

10. SecretNet система защиты информации от несанкционированного доступа [Электронный ресурс]. Режим доступа: http://www.securitycode.ru/products/secret_net/ (дата обращения: 05.10.2022).

11. «Об утверждении Перечня сведений конфиденциального характера». Указ от 23 сен. 2005 г. №1111 // – РГ – 2006. №4531 – 3 с.

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ

Генеральный директор

ООО «Газпром Интернешнл»

_____

«____»_____2023г.

Матрица доступа субъектов автоматизированной системы к ее защищаемым информационным ресурсам:

Таблица 14 - Список субъектов

Имя пользователя	Учетная запись	Тип учетной записи	Уровень допуска
АРМ № 1			
Иванов	Admin	Администратор	Конфиденциально
Петров	Petrov	Пользователь	Конфиденциально
АРМ № 2			
Иванов	Admin	Администратор	Конфиденциально
Семенов	Semenov	Пользователь	Конфиденциально
АРМ № 3			
Иванов	Admin	Администратор	Конфиденциально
Артемьев	Artemev	Пользователь	Конфиденциально

Таблица 15 -Установленные права доступа

Объекты доступа	Субъекты доступа			
	Admin	Petrov	Semenov	Artemev
Средства ОС для запуска и работы ПЭВМ	Полный доступ	Чтение, запись	Чтение, запись	Чтение, запись
Основные конфигурационные файлы операционной системы	Полный доступ	Чтение	Чтение	Чтение
Прикладное программное обеспечение	Полный доступ	Чтение, запись	Чтение, запись	Чтение, запись
Драйверы средств защиты информации	Полный доступ	Чтение, запись	Чтение, запись	Чтение, запись

Объекты доступа	Субъекты доступа			
	Admin	Petrov	Semenov	Artemev
Средства настройки и управления средств защиты информации	Полный доступ	Чтение, запись	Чтение, запись	Чтение, запись
Основные конфигурационные файлы средств защиты информации	Полный доступ	-	-	-
Антивирусные средства	Полный доступ	Чтение, запись	Чтение, запись	Чтение, запись
Многофункциональное устройство	Полный доступ	Печать, сканирование	-	-
Обрабатываемые, хранимые данные	Полный доступ	Полный доступ	Полный доступ	Полный доступ

должность ФИО

ПРИЛОЖЕНИЕ Б

УТВЕРЖДАЮ

Генеральный директор

ООО «Газпром Интернешнл»

_____

«____»_____2023г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

автоматизированной системы № 1,2 и 3

1. Перечень основных технических средств и систем (ОТСС), входящих в состав автоматизированной системы.

Таблица 16

Наименование	Модель
АРМ № 1	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
МФУ	HP MFP 135W
АРМ № 2	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
АРМ № 3	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
Сетевое оборудование	
Свитч	D-LINK DES1005C

2. Перечень вспомогательных технических средств и систем (ВТСС), входящих в АС.

Наименование	Модель
Шредер	Deli Core E9954-EU
IP телефон	Yealink
Датчик движения	Риелта Фотон-12 (ИО409-17/1)
Датчик движения	Риелта Фотон-12 (ИО409-17/1)
Извещатель пожарный	RUBEZH ИП 212-45
Извещатель пожарный	RUBEZH ИП 212-45
Извещатель пожарный	RUBEZH ИП 212-45

3. Перечень средств защиты информации, установленных на объекте информатизации.

Таблица 17

№ п/п	Наименование и тип ТС	Сведения о сертификате
1.	Средство защиты информации от несанкционированного доступа «Dallas Lock 8.0-К»	ФСТЭК России № 2720 от 25 сентября 2012 г. Действителен до 25 сентября 2026 г.
2.	Антивирусная программа Dr.Web Enterprise Security Suite	ФСТЭК России № 3509 от 27 января 2016 г. Действителен до 27 января 2019 г. Продлен до 27 января 2024 г.
3	Генератор шума «Соната – Р3.1»	ФСТЭК России № 3539 от 24 марта 2016 г. Действителен до 24 марта 2024 г

ПРИЛОЖЕНИЕ В

ПРОТОКОЛ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

автоматизированной системы

Таблица 18 Измерительное оборудование

№ п/п	Наименование средств измерений и вспомогательного оборудования	Тип	Диапазон частот, МГц
1.	Токосъемник	ТИ 2-4	0,009-400
2.	Анализатор спектра	FPH13 (с опцией FPH-K43)	0,005-13600
3.	Антенна биконическая измерительная	НБА-02	0,009-2500
4.	Комплект антенный измерительный	АИК 1-40/10	0,9-12400
5.	Антенна рамочная измерительная	НРА-02	0,009-30
6.	Пробник напряжения	П-400	0,0001-400
7.	Эквивалент сети для проведения специсследований	ЭС-1000СИ	0,009-500
8.	Логопериодическая измерительная антенна	ПИРАМИДА	1000-12500
9.	Селективный нановольтметр	Unipan-233	0,0000015-0,15
1.	Осциллограф	С1-112А	До 10
2.	Специализированные тестирующие программы ЗАО «ЦБИ-сервис»	-	-
3.	Антенна передающая для проведения объектовых специсследований	КУБ-М	0,009-1000
4.	Вспомогательный генератор сигналов	Источник	0,001-10000
5.	Индуктор магнитный	ИМ-2	0,00002-600

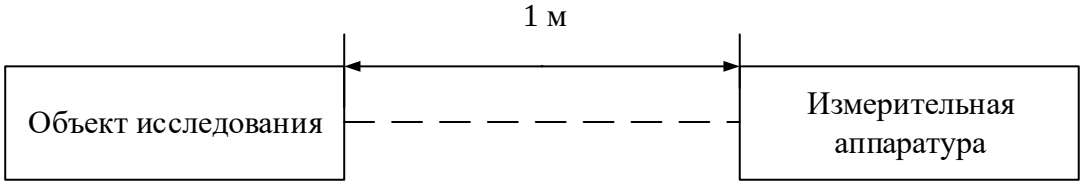


Рисунок 18 – Схема расположения измерительного оборудования

Согласно описанным действиям были проведены исследования автоматизированной системы, в таблицах описаны данные результаты.

где:

F - частота;

K - общее число спектральных составляющих;

R_0 – рекомендуемое расстояние установки измерительного оборудования;

ρH_i – напряженность электромагнитного поля по магнитной составляющей, мкВ/м;

E_i - напряженность электромагнитного поля по электрической составляющей, мкВ/м;

$E_{\text{ш}}(\rho H_{\text{ш}i})$ - напряженность электромагнитного поля по электрической (магнитной) составляющей за счет шума, мкВ/м;

L_1 – расстояние от ОТСС до границы ближней и промежуточной зон, м;

L_2 – расстояние от ОТСС до границы промежуточной и дальней зон, м;

f_i – частотный -й спектральной составляющей информативного сигнала;

R_{2_i} – радиус контролируемой зоны для -й составляющей спектра информативного сигнала, м;

E_{0_i} – уровень напряженности электромагнитного поля при работе ОТСС в тестируемом режиме;

$E_{\text{ш}_i}$ – уровень напряженности электромагнитного поля при выключенном ОТСС;

$E_{c_i}(\rho H_{c_i})$ - напряженность электромагнитного поля по электрической (магнитной) составляющей, созданная информативным сигналом, мкВ/м;

$E_{1_i}(\rho H_{1_i})$ – значение напряженности информативного сигнала на границе ближней и промежуточной зон, мкВ/м;

$E_{2_i}(\rho H_{2_i})$ – значение напряженности информативного сигнала на границе промежуточной и дальней зон, мкВ/м;

$E_{0_i}(\rho H_{0_i})$ – измеренный уровень напряженность электромагнитного поля при работе ОТСС в тестируемом режиме, мкВ/м;

ρ= 377 Ом – волновое сопротивление свободного пространства.

Расчеты проводились в соответствии с формулами:

Радиус контролируемой зоныR_{2_i} для -й составляющей спектра информативного сигнала определяется из условия:

$$R_{2_i} = R_i, \text{ (1)}$$

Для расчёта границы промежуточной зоны производятся следующие расчеты:

$$L_1 = \frac{150}{\pi * f_i} \text{ (2).}$$

Для расчета границы ближней и промежуточной зоны производятся следующие расчеты:

$$L_2 = \frac{1800}{f_i} \text{ (3).}$$

Для расчета возможного расстояния R_i для каждой частоты рассчитывается по формуле:

$$R_i = \frac{L_1}{\sqrt[\Pi]{\frac{k * E_{\text{ш}_i}}{E_i}}} \text{ м. (4)}$$

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

Значение L_1 выбирается из условий:

$L_1 = R_0$ - для ближней зоны;

$L_1 = \begin{cases} L_{1_i}, если\ L_{1_i} > R_0 \\ R_0, если\ L_{1_i} \leq R_0 \end{cases}$ - для промежуточной зоны;

$L_1 = \begin{cases} L_{2_i}, если\ L_{2_i} > R_0 \\ R_0, если\ L_{2_i} \leq R_0 \end{cases}$ - для дальней зоны;

Значение E_{c_i} – выбирается из условий:

$E_i = E_{c_i}$ - для ближней зоны;

$E_1 = \begin{cases} E_{1_i}, если\ L_{1_i} > R_0 \\ E_{c_i}, если\ L_{1_i} \leq R_0 \end{cases}$ - для промежуточной зоны;

$E_1 = \begin{cases} E_{2_i}, если\ L_{2_i} > R_0 \\ E_{c_i}, если\ L_{2_i} \leq R_0 \end{cases}$ - для дальней зоны;

где $E_{1_i} = E_{c_i}(R_0/L_{1_i})^3$ (5)

– значение напряженности поля информативного сигнала на границе ближней и промежуточной зон;

$$E_{2_i} = \begin{cases} E_{1_i}(L_{1_i}/L_{2_i})^2, если\ R_0 < L_{1_i} \\ E_{c_i}(R_0/L_{2_i})^2, если\ R_0 \geq L_{1_i} \end{cases} \quad (6)$$

- значение напряженности поля информативного сигнала на границе промежуточной и дальней зон.

$$E_{c_i} = \sqrt{{E_{0_i}}^2 - {E_{ш_i}}^2}\ \text{мкВ/м}; \quad (7)$$

Значение *k= 0,3* потому что ОТСС имеет в составе монитор.

1. Определение зоны R_2 для АРМ № 1:

1) $f_1 = 74.26$ МГц

$$L_1 = \frac{150}{3{,}14 * 74{,}26} = 0{,}6433 \text{ м}$$

$$L_2 = \frac{1800}{74{,}26} = 24{,}2 \text{ м}.$$

$$E_{с+ш} = 10^{48+20{,}9/20} = 2786{,}1 \text{ мкВ}.$$

$$E_{ш} = 10^{12{,}8+20{,}9/20} = 48{,}4172 \text{ мкВ}.$$

$$E_{с} = \sqrt{2786{,}1^2 - 48{,}4^2} = 2785{,}7 \text{ мкВ}.$$

$$E_{с} = 20 * \log_{10} 2785{,}7 = 68{,}9 \text{ дБ}.$$

$$R_{б} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 48{,}4}{2785{,}7}}} = 5{,}76 \text{ м}.$$

$$E_б = 2785{,}7 * \left(\frac{1}{0{,}64}\right)^3 = 10\ 464{,}402 \text{ мкВ}.$$

$$R_п = \frac{1}{\sqrt[2]{\frac{0{,}3 * 48{,}4}{2785{,}7}}} = 13{,}85 \text{ м}.$$

$$E_п = 2785{,}7 * \left(\frac{1}{24{,}2}\right)^2 = 4{,}741 \text{ мкВ}.$$

$$R_д = \frac{24{,}2}{\frac{0{,}3 * 48{,}4}{4{,}741}} = 7{,}9 \text{ м}.$$

2) $f_2 = 222.76$ МГц

$$L_1 = \frac{150}{3{,}14 * 222{,}76} = 0{,}2144 \text{ м}$$

$$L_2 = \frac{1800}{222{,}76} = 8{,}08 \text{ м}.$$

$$E_ш = 10^{4{,}7+19{,}9/20} = 16{,}9824 \text{ мкВ}.$$

$$E_{с+ш} = 10^{29{,}5+19{,}9/20} = 295{,}12 \text{ мкВ}.$$

$$E_с = \sqrt{295{,}12^2 - 16{,}9824^2} = 294{,}62 \text{ мкВ}.$$

$$E_с = 20 * \log_{10} 294{,}62 = 49{,}39 \text{ дБ}.$$

$$R_б = \frac{1}{\sqrt[3]{\frac{0{,}3 * 16{,}9824}{294{,}62}}} = 3{,}867 \text{ м}.$$

$$E_б = 294{,}62\ * \left(\frac{1}{0{,}2144}\right)^3 = 29\ 874{,}907 \text{ мкВ}.$$

$$R_п = \frac{1}{\sqrt[2]{\frac{0{,}3 * 16{,}9824}{294{,}62}}} = 7{,}6 \text{ м}.$$

$$E_п = 294{,}62 * \left(\frac{1}{8{,}08}\right)^2 = 4{,}512 \text{ мкВ}.$$

$$R_д = \frac{8{,}08}{\frac{0{,}3 * 16{,}9824}{4{,}512}} = 7{,}157 \text{ м}.$$

3) $f_3 = 371.28$ МГц

$$L_1 = \frac{150}{3{,}14 * 371{,}28} = 0{,}1287 \text{ м}$$

$$L_2 = \frac{1800}{371{,}28} = 4{,}85 \text{ м.}$$

$$E_{\text{ш}} = 10^{4{,}6+18{,}8/20} = 14{,}7911 \text{ мкВ.}$$

$$E_{\text{с+ш}} = 10^{8{,}4+18{,}8/20} = 22{,}909 \text{ мкВ.}$$

$$E_{\text{с}} = \sqrt{22{,}909^2 - 14{,}7911^2} = 17{,}494 \text{ мкВ.}$$

$$E_{\text{с}} = 20 * \log_{10} 17{,}494 \ = 24{,}86 \text{ дБ.}$$

$$R_{\text{б}} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 14{,}7911}{17{,}494}}} = 1{,}58 \text{ м.}$$

$$E_{\text{б}} = 17{,}494 \ * \left(\frac{1}{0{,}1287}\right)^3 = 8\,213{,}0176 \text{ мкВ.}$$

$$R_{\text{п}} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 14{,}7911}{17{,}494}}} = 1{,}986 \text{ м.}$$

$$E_{\text{п}} = 17{,}494 * \left(\frac{1}{0{,}1287}\right)^2 = 0{,}744 \text{ мкВ.}$$

$$R_{\text{д}} = \frac{4{,}85}{\frac{0{,}3 * 14{,}7911}{0{,}744}} = 0{,}813 \text{ м.}$$

4) $f_4 = 519.8$ МГц

$$L_1 = \frac{150}{3{,}14 * 519.8} = 0{,}0919 \text{ м}$$

$$L_2 = \frac{1800}{519.8} = 3{,}46 \text{ м.}$$

$$E_{\text{ш}} = 10^{3{,}9+18{,}5/20} = 13{,}1826 \text{ мкВ.}$$

$$E_{\text{с+ш}} = 10^{18{,}2+18{,}5/20} = 68{,}391 \text{ мкВ.}$$

$$E_{\text{с}} = \sqrt{68{,}391^{\ 2} - 13{,}1826^2} = 67{,}109 \text{ мкВ.}$$

$$E_{\text{с}} = 20 * \log_{10} 67{,}109 \ = 36{,}54 \text{ дБ.}$$

$$R_{\text{б}} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 13{,}1826}{67{,}109}}} = 2{,}57 \text{ м.}$$

$$E_б = 67{,}109 * \left(\frac{1}{0{,}0919}\right)^3 = 8\ 6457{,}469 \text{ мкВ}.$$

$$R_п = \frac{1}{\sqrt[2]{\frac{0{,}3 * 13{,}1826}{67{,}109}}} = 4{,}119 \text{ м}.$$

$$E_п = 67{,}109 * \left(\frac{1}{3{,}46}\right)^2 = 5{,}596 \text{ мкВ}.$$

$$R_д = \frac{3{,}46}{\frac{0{,}3 * 13{,}1826}{5{,}596}} = 4{,}9 \text{ м}.$$

2. Определение зоны R_2 для АРМ № 2:

1) $f_1 = 74.26$ МГц

$$L_1 = \frac{150}{3{,}14 * 74{,}26} = 0{,}6433 \text{ м}$$

$$L_2 = \frac{1800}{74{,}26} = 24{,}2 \text{ м}.$$

$$E_{с+ш} = 10^{50+12{,}8/20} = 3\ 507{,}5 \text{ мкВ}.$$

$$E_ш = 10^{15{,}6+20{,}9/20} = 66{,}8344 \text{ мкВ}.$$

$$E_с = \sqrt{3\ 507{,}5^2 - 66{,}8344^2} = 3\ 506{,}9 \text{ мкВ}.$$

$$E_с = 20 * \log_{10} 3\ 506{,}9 = 70{,}9 \text{ дБ}.$$

$$R_б = \frac{1}{\sqrt[3]{\frac{0{,}3 * 66{,}8344}{3\ 506{,}9}}} = 5{,}592 \text{ м}.$$

$$E_б = 3\ 506{,}9 * \left(\frac{1}{0{,}6433}\right)^3 = 13\ 173{,}499 \text{ мкВ}.$$

$$R_п = \frac{1}{\sqrt[2]{\frac{0{,}3 * 66{,}8344}{3\ 506{,}9}}} = 13{,}23 \text{ м}.$$

$$E_п = 3\ 506{,}9\ * \left(\frac{1}{24{,}2}\right)^2 = 5{,}969 \text{ мкВ}.$$

$$R_д = \frac{24{,}2}{\frac{0{,}3 * 66{,}8344}{5{,}969}} = 7{,}216 \text{ м}.$$

2) $f_2 = 222.76$ МГц

$$L_1 = \frac{150}{3{,}14 * 222{,}76} = 0{,}2144 \text{ м}$$

$$L_2 = \frac{1800}{222{,}76} = 8{,}08 \text{ м.}$$

$$E_{\text{ш}} = 10^{6{,}5+19{,}9/20} = 20{,}893 \text{ мкВ.}$$

$$E_{\text{с+ш}} = 10^{32{,}4+19{,}9/20} = 412{,}1 \text{ мкВ.}$$

$$E_{\text{с}} = \sqrt{412{,}1^2 - 20{,}893^2} = 411{,}57 \text{ мкВ.}$$

$$E_{\text{с}} = 20 * \log_{10} 411{,}57 = 52{,}29 \text{ дБ.}$$

$$R_{\text{б}} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 20{,}893}{411{,}57}}} = 4{,}034 \text{ м.}$$

$$E_{\text{б}} = 411{,}57 \ * \left(\frac{1}{0{,}2144}\right)^3 = 41\,731{,}877 \text{ мкВ.}$$

$$R_{\text{п}} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 20{,}893}{411{,}57}}} = 8{,}103 \text{ м.}$$

$$E_{\text{п}} = 411{,}57 * \left(\frac{1}{8{,}08}\right)^2 = 6{,}303 \text{ мкВ.}$$

$$R_{\text{д}} = \frac{8{,}08}{\frac{0{,}3 * 20{,}893}{6{,}303}} = 8{,}126 \text{ м.}$$

3) $f_3 = 371.28$ МГц

$$L_1 = \frac{150}{3{,}14 * 371{,}28} = 0{,}1287 \text{ м}$$

$$L_2 = \frac{1800}{371{,}28} = 4{,}85 \text{ м.}$$

$$E_{\text{ш}} = 10^{5{,}1+18{,}8/20} = 15{,}6675 \text{ мкВ.}$$

$$E_{\text{с+ш}} = 10^{10{,}2+18{,}8/20} = 28{,}184 \text{ мкВ.}$$

$$E_{\text{с}} = \sqrt{28{,}184^2 - 15{,}6675^2} = 23{,}428 \text{ мкВ.}$$

$$E_{\text{с}} = 20 * \log_{10} 23{,}428 \ = 27{,}39 \text{ дБ.}$$

$$R_{б} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 15{,}6675}{23{,}428}}} = 1{,}708 \text{ м.}$$

$$E_{б} = 23{,}428 \ * \left(\frac{1}{0{,}1287}\right)^{3} = 10\,998{,}908 \text{ мкВ.}$$

$$R_{п} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 15{,}6675}{23{,}428}}} = 2{,}233 \text{ м.}$$

$$E_{п} = 23{,}428 * \left(\frac{1}{0{,}1287}\right)^{2} = 0{,}997 \text{ мкВ.}$$

$$R_{д} = \frac{4{,}85}{\frac{0{,}3 * 15{,}6675}{0{,}997}} = 1{,}028 \text{ м.}$$

4) $f_4 = 519.8$ МГц

$$L_1 = \frac{150}{3{,}14 * 519.8} = 0{,}0919 \text{ м}$$

$$L_2 = \frac{1800}{519.8} = 3{,}46 \text{ м.}$$

$$E_{ш} = 10^{4{,}9+18{,}5/20} = 14{,}7911 \text{ мкВ.}$$

$$E_{с+ш} = 10^{19{,}8+18{,}5/20} = 82{,}224 \text{ мкВ.}$$

$$E_{с} = \sqrt{82{,}224^{\ 2} - 14{,}7911^{2}} = 80{,}883 \text{ мкВ.}$$

$$E_{с} = 20 * \log_{10} 80{,}883 \ = 38{,}16 \text{ дБ.}$$

$$R_{б} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 14{,}7911}{80{,}883}}} = 2{,}632 \text{ м.}$$

$$E_{б} = 80{,}883 * \left(\frac{1}{0{,}0919}\right)^{3} = 104\,203{,}2 \text{ мкВ.}$$

$$R_{п} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 14{,}7911}{80{,}883}}} = 4{,}269\text{м.}$$

$$E_{п} = 80{,}883 * \left(\frac{1}{0{,}0919}\right)^{2} = 6{,}745 \text{ мкВ.}$$

$$R_{д} = \frac{3{,}46}{\frac{0{,}3 * 14{,}7911}{6{,}745}} = 5{,}2 \text{ м.}$$

3. Определение зоны R_2 для АРМ № 3:

1) $f_1 = 74.26$ МГц

$$L_1 = \frac{150}{3{,}14 * 74{,}26} = 0{,}6433 \text{ м}$$

$$L_2 = \frac{1800}{74{,}26} = 24{,}2 \text{ м.}$$

$$E_{ш} = 10^{14+20{,}9/20} = 55{,}5904 \text{мкВ.}$$

$$E_{с+ш} = 10^{47+20{,}9/20} = 2\,483{,}1 \text{ мкВ.}$$

$$E_{с} = \sqrt{2\,483{,}1^2 - 55{,}5904^2} = 2\,482{,}5 \text{ мкВ.}$$

$$E_{с} = 20 * \log_{10} 2\,482{,}5 = 67{,}9 \text{ дБ.}$$

$$R_{б} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 55{,}5904}{2\,482{,}5}}} = 5{,}3 \text{ м.}$$

$$E_{б} = 2\,482{,}5 * \left(\frac{1}{0{,}6433}\right)^3 = 9\,325{,}4789 \text{ мкВ.}$$

$$R_{п} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 55{,}5904}{2\,482{,}5}}} = 12 \text{ м.}$$

$$E_{п} = 2\,482{,}5 \ * \left(\frac{1}{24{,}2}\right)^2 = 4{,}225 \text{ мкВ.}$$

$$R_{д} = \frac{24{,}2}{\frac{0{,}3 * 55{,}5904}{4{,}225}} = 6{,}141 \text{ м.}$$

2) $f_2 = 222.76$ МГц

$$L_1 = \frac{150}{3{,}14 * 222{,}76} = 0{,}2144 \text{ м}$$

$$L_2 = \frac{1800}{222{,}76} = 8{,}08 \text{ м.}$$

$$E_{ш} = 10^{9{,}5+19{,}9/20} = 29{,}5121 \text{ мкВ.}$$

$$E_{с+ш} = 10^{27+19{,}9/20} = 221{,}31 \text{ мкВ.}$$

$$E_{\text{с}} = \sqrt{221{,}31^2 - 29{,}5121^2} = 219{,}33 \text{ мкВ}.$$

$$E_{\text{с}} = 20 * \log_{10} 219{,}33 = 46{,}82 \text{ дБ}.$$

$$R_{\text{б}} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 29{,}5121}{219{,}33}}} = 2{,}915 \text{ м}.$$

$$E_{\text{б}} = 219{,}33 \ * \left(\frac{1}{0{,}2144}\right)^3 = 22\,239{,}784 \text{ мкВ}.$$

$$R_{\text{п}} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 29{,}5121}{219{,}33}}} = 4{,}977 \text{ м}.$$

$$E_{\text{п}} = 219{,}33 * \left(\frac{1}{8{,}08}\right)^2 = 3{,}359 \text{ мкВ}.$$

$$R_{\text{д}} = \frac{8{,}08}{\frac{0{,}3 * 29{,}5121}{3{,}359}} = 3{,}066 \text{ м}.$$

3) $f_3 = 371.28$ МГц

$$L_1 = \frac{150}{3{,}14 * 371{,}28} = 0{,}1287 \text{ м}$$

$$L_2 = \frac{1800}{371{,}28} = 4{,}85 \text{ м}.$$

$$E_{\text{ш}} = 10^{11{,}5+18{,}8/20} = 32{,}7341 \text{ мкВ}.$$

$$E_{\text{с+ш}} = 10^{15+18{,}8/20} = 48{,}978 \text{ мкВ}.$$

$$E_{\text{с}} = \sqrt{48{,}978^2 - 32{,}7341^2} = 36{,}432 \text{ мкВ}.$$

$$E_{\text{с}} = 20 * \log_{10} 36{,}432 \ = 31{,}23 \text{ дБ}.$$

$$R_{\text{б}} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 32{,}7341}{36{,}432}}} = 1{,}548 \text{ м}.$$

$$E_{\text{б}} = 36{,}432 * \left(\frac{1}{0{,}1287}\right)^3 = 17\,104{,}351 \text{ мкВ}.$$

$$R_{\text{п}} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 32{,}7341}{36{,}432}}} = 1{,}926 \text{ м}.$$

$$E_{\text{п}} = 36{,}432 * \left(\frac{1}{0{,}1287}\right)^2 = 1{,}55 \text{ мкВ}.$$

$$R_{\text{д}} = \frac{4{,}85}{\frac{0{,}3 * 32{,}7341}{1{,}55}} = 0{,}765 \text{ м}.$$

4) $f_4 = 519.8$ МГц

$$L_1 = \frac{150}{3{,}14 * 519.8} = 0{,}0919 \text{ м}$$

$$L_2 = \frac{1800}{519.8} = 3{,}46 \text{ м}.$$

$$E_{\text{ш}} = 10^{14{,}6+18{,}5/20} = 45{,}1856 \text{ мкВ}.$$

$$E_{\text{с+ш}} = 10^{23+18{,}5/20} = 117{,}85 \text{ мкВ}.$$

$$E_{\text{с}} = \sqrt{117{,}85^{\,2} - 45{,}1856^2} = 109{,}93 \text{ мкВ}.$$

$$E_{\text{с}} = 20 * \log_{10} 109{,}93 = 40{,}82 \text{ дБ}.$$

$$R_{\text{б}} = \frac{1}{\sqrt[3]{\frac{0{,}3 * 45{,}1856}{109{,}93}}} = 2 \text{ м}.$$

$$E_{\text{б}} = 109{,}93 * \left(\frac{1}{0{,}0919}\right)^3 = 141\,619{,}43 \text{ мкВ}.$$

$$R_{\text{п}} = \frac{1}{\sqrt[2]{\frac{0{,}3 * 45{,}1856}{109{,}93}}} = 2{,}848\text{м}.$$

$$E_{\text{п}} = 109{,}93 * \left(\frac{1}{0{,}0919}\right)^2 = 9{,}167 \text{ мкВ}.$$

$$R_{\text{д}} = \frac{3{,}46}{\frac{0{,}3 * 45{,}1856}{9{,}167}} = 2{,}342\text{м}.$$

Таблица 19 – Расчет зоны R_2

№ fi	F, МГц	$E_{с+ш}$, дБ	$E_{ш}$, дБ	$E_{с}$, дБ	R, м
АРМ № 1					
1	74,26	68,9	33,7	68,9	13,85
2	222,76	49,4	24,6	49,4	7,60

3	371,28	27,2	23,4	24,9	1,99
4	519,8	36,7	22,4	36,5	4,90
АРМ № 2					
1	74,26	70,9	36,5	70,9	13,23
2	222,76	52,3	26,4	52,3	8,13
3	371,28	29	23,9	27,4	2,23
4	519,8	38,3	23,4	38,2	5,26
АРМ № 3					
1	74,26	67,9	34,9	67,9	12,20
2	222,76	46,9	29,4	46,8	4,98
3	371,28	33,8	30,3	31,2	1,93
4	519,8	41,5	33,1	40,8	2,85

При проведении исследовании на автоматизированной системе было обнаружено 4 частоты, на которых был обнаружен сигнал. Таким образом, при расчете зоны R_2 для автоматизированной системы был получен результат 13,85 м.

После расчет зоны R_2 следует определись и зону r_1, в таблице показаны расчеты.

где:

$U_{(с+ш)_i}$ – напряжение смеси обнаруженных компонент тест-сигнала и шума, дБ;

l – протяженность линии ВТСС между точками А и Б, м;

$U_{ш_i}$ – шум в линии, дБ;

$U_{с_i}$ – напряжение сигнала в линии, дБ;

$П_i$ – показатель защищенности, дБ;

$К_{П_i}$ – коэффициент погонного затухания наведенных сигналов в исследуемой линии, дБ/м;

$U_{1изм_i}$ – напряжение специально созданного сигнала, измеренное на частоте f_i исследуемой линии в непосредственной близости от ОТСС, мкВ;

$U_{2изм_i}$ – напряжение специально созданного сигнала, измеренное на частоте f_i исследуемой линии на некотором удалении от ОТСС, мкВ;

R_i – максимальная длина пробега исследуемой линии, на которой возможно выделение информативного сигнала, м;

$R_{КЗ}$ – реальный пробег исследуемой линии до границы контролируемой зоны, м.

Для расчета наводок на линии ОТСС, берутся следующие формулы:

1) Расчет значения напряженности в точке подсоединения измерительного пробника:

$$U_{c_i} = 20 * lg\sqrt{10^{U_{(с+ш)i}/10} - 10^{U_{ш_i}/10}} \text{ дБ. (8)}$$

2) Расчет показателя защищенности в точке проведения измерений:

$$П_i = U_{c_i} - U_{ш_i}, \text{ дБ. (9)}$$

3) Расчет величины коэффициента погонного затухания $К_{П_i}$ наведенных сигналов в исследуемой линии:

$$К_{П_i} = \frac{U_{1изм_i} - U_{2изм_i}}{l} \text{ дБ/м. (10)}$$

4) Для расчёта максимальной длины пробега R_i исследуемой линии, проводится по формуле:

$$R_i = \frac{П_i + 10}{К_{П_i}} \text{ м.}$$

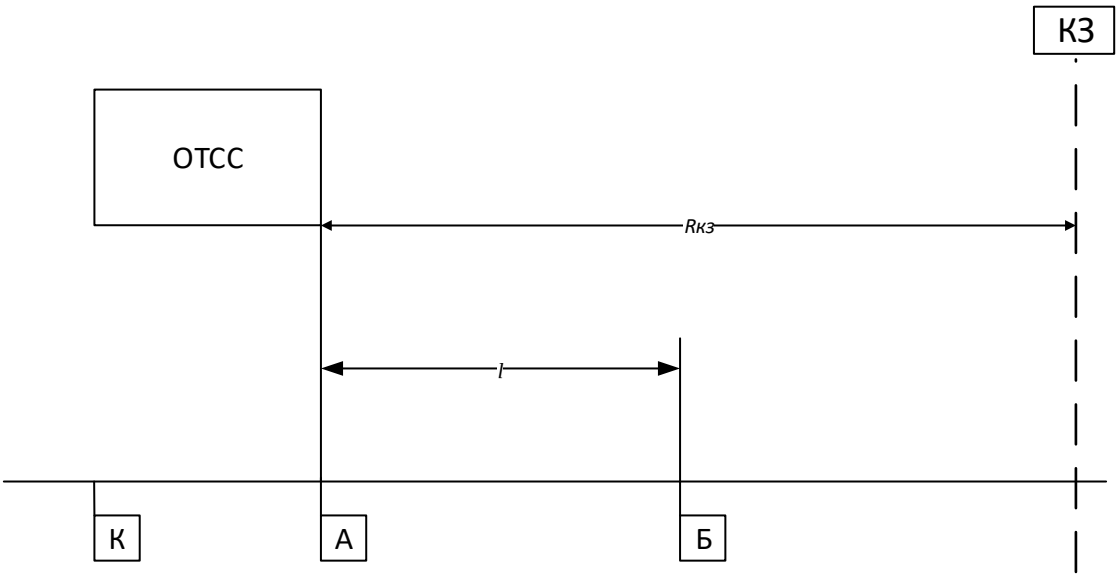


Рисунок 19 – Схема расположения измерительного оборудования

Определение зоны r_1 для АРМ № 1:

1) $f_1 = 74{,}26$ МГц

$$U_{c_1} = 20 * lg\sqrt{10^{\frac{25}{10}} - 10^{\frac{15}{10}}} = 24{,}54243 \text{ дБ.}$$

$$\text{П}_1 = 24{,}54243 - 15 = 9{,}542425$$

$$\text{К}_{\text{П}_i} = \frac{49 - 16}{12} = 2{,}75$$

$$R_1 = \frac{9{,}542425 + 10}{2{,}75} = 7{,}106336 \text{ м.}$$

2) $f_1 = 222{,}76$ МГц

$$U_{c_2} = 20 * lg\sqrt{10^{\frac{22}{10}} - 10^{\frac{16}{10}}} = \text{ дБ.}$$

$$\text{П}_2 = 20{,}74372 - 16 = 4{,}74372$$

$$\text{К}_{\text{П}_i} = \frac{39 - 15}{12} = 2$$

$$R_2 = \frac{4{,}74372 + 10}{2} = 7{,}371862 \text{ м.}$$

Определение зоны r_1 для АРМ № 2:

1) $f_1 = 74{,}26$ МГц

$$U_{c_1} = 20 * lg\sqrt{10^{\frac{28}{10}} - 10^{\frac{24}{10}}} = \ 25{,}79519 \text{ дБ.}$$

$$\text{П}_1 = 25{,}79519 - 24 = 1{,}79519$$

$$\text{К}_{\text{П}_i} = \frac{47 - 17}{12} = 2{,}5$$

$$R_1 = \frac{1{,}79519 + 10}{2{,}5} = 4{,}718077 \text{ м.}$$

2) $f_2 = 222{,}76$ МГц

$$U_{c_2} = 20 * lg\sqrt{10^{\frac{22}{10}} - 10^{\frac{16}{10}}} = \text{ дБ.}$$

$$\text{П}_2 = 20{,}74372 - 16 = 4{,}74372$$

$$\text{К}_{\text{П}_i} = \frac{39 - 15}{12} = 2$$

$$R_2 = \frac{4{,}74372 + 10}{2} = 7{,}371862 \text{ м.}$$

Определение зоны r_1 для АРМ № 3:

1) $f_1 = 74{,}26$ МГц

$$U_{c_1} = 20 * lg\sqrt{10^{\frac{24}{10}} - 10^{\frac{20{,}5}{10}}} = 21{,}65766 \text{ дБ.}$$

$$\text{П}_1 = 21{,}65766 - 20{,}5 = 1{,}4576584415$$

$$\text{К}_{\text{П}_i} = \frac{44 - 14{,}5}{12} = 2{,}458333333$$

$$R_1 = \frac{1{,}4576584415 + 10}{2{,}458333333} = 4{,}660742417 \text{ м.}$$

2) $f_1 = 222{,}76$ МГц

$$U_{c_2} = 20 * lg\sqrt{10^{\frac{22}{10}} - 10^{\frac{18{,}5}{10}}} = 19{,}42973549 \text{ дБ.}$$

$$\text{П}_2 = 19{,}42973549 \ - 18{,}5 = 0{,}929735488$$

$$\text{К}_{\text{П}_i} = \frac{46 - 17{,}5}{12} = 2{,}375$$

$$R_2 = \frac{0{,}929735488 + 10}{2{,}375} = 4{,}60199389 \text{ м.}$$

Таблица 20 – Расчет наводок на линии

№ fi	fi, МГц	U(с+ш)i, дБ	Uшi, дБ	Uci, дБ	U1 измі. мкВ	U2 измі, мкВ	Кпі, дБ/м	Ri, м	Rкз, м
АРМ № 1									
1	74,26	25	15	24,54	281,8	6,3	2,75	7,1	
2	222,76	22	16	20,74	89,1	5,6	2	7,4	
АРМ № 2									
1	74,26	28	24	25,80	223,9	7,1	2,5	4,7	
2	222,76	23	19	20,80	125,9	7,9	2	5,9	
АРМ № 3									
1	74,26	24	20,2	21,66	158,5	5,3	2,458333	4,7	
2	222,76	22	18,5	19,43	199,5	7,5	2,375	4,6	

ПРИЛОЖЕНИЕ Г

СОГЛАСОВАНО УТВЕРЖДАЮ

_____ _____

«___» _____ «___» _____

ПРОГРАММА И МЕТОДИКА

проведения аттестационных испытаний автоматизированной системы

Объект испытаний.

Объектом испытаний является объект информатизации автоматизированная система, предназначенный для обработки информации с конфиденциальной информации.

Таблица 21

Наименование	Модель
АРМ № 1	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
МФУ	HP MFP 135W
АРМ № 2	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
АРМ № 3	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
Сетевое оборудование	
Свитч	D-LINK DES1005C

1 Средства защиты объекта информатизации «АРМ»:

- СЗИ от НСД «Dallas Lock 8.0-К»;
- СЗИ от вредоносных программ «Dr.Web Enterprise Security Suite»
- СЗИ от ПЭМИН «Соната-Р3.1» генератор шума

2 Цель и виды испытаний.

2.1 Целью АИ объекта информатизации определение соответствия требования защите информации.

2.2 При АИ объекта проводится оценка его соответствия требованиям по защите информации:

- от утечки за счет невыполнения организационно мер защиты информации;
- от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) технических средств и систем объекта;
- от утечки за счет электронных устройств перехвата информации;
- от несанкционированного доступа (НСД) к информации, в том числе от компьютерных вирусов, а также иных разрушающих программных воздействий, нарушающих целостность информации или работоспособность технических средств автоматизированной системы (АС) объекта информатизации.

3 Условия и порядок проведения аттестационных испытаний объекта информатизации.

Программа испытаний разрабатывается на основе анализа исходных данных об объектах на этапе предварительного ознакомления.

Для проведения испытаний заявитель предоставляет аттестационной комиссии следующие исходные данные и документацию:

- Технический паспорт на объект информатизации;
- Список лиц, допущенных в помещение, где ведется обработка конфиденциальной информации с использованием АС ОИ;
- Список лиц допущенных к обработке конфиденциальной информации на ОИ;
- Состав программного обеспечения, используемого при обработке конфиденциальной информации в АС в составе ОИ;

- Перечень защищаемых ресурсов с документальным подтверждением уровней конфиденциальности каждого ресурса;
- Схема информационных потоков АС;
- Инструкции по обеспечению защиты конфиденциальной информации, обрабатываемой на ОИ;
- Эксплуатационная документация на применяемые средства защиты информации в составе ОИ;
- Схема размещения основных (ОТСС) и вспомогательных (ВТСС) технических средств и систем в помещении, прокладки линий и коммуникаций, выходящих из помещения за границы контролируемой зоны;
- Схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны;
- Схема прокладки коммуникаций, не выходящих за пределы контролируемой зоны;
- Схема электроснабжения и заземления ОТСС;
- Схема электропитания силовой и осветительной сетей;
- Сведения об измерении сопротивления заземляющего устройства;
- Данные по уровню подготовки кадров, обеспечивающих защиту информации;
- Данные о наличии и расположении постоянных представительств иностранных государств, обладающих правом экстерриториальности;
- Акты установки на объекте систем защиты информации.

Методика испытаний.

При проведении аттестационных испытаний применяются следующие методы проверок и испытаний:

- экспертно - документальный метод;
- измерение побочного излучения опасного сигнала от основных технических средств и систем ОИ и оценка защищенности;
- проверка отдельных функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем

пробного запуска средств защиты информации от НСД и наблюдения за их выполнением:

- «Terrier» версия 3.0;
- «ФИКС» версия 3.0;
- «Ревизор 1 XP»;
- «Ревизор 2 XP».

Экспертно-документальный метод предусматривает проверку соответствия объекта информатизации требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов, по обеспечению необходимых мер защиты информации в АС, а также соответствия реальных условий эксплуатации требованиям по размещению, монтажу и эксплуатации технических средств АС.

Измерение побочного излучения опасного сигнала и оценка защищенности проводится в соответствии с действующими нормативными и методическими документами по защите информации от ее утечки по каналам ПЭМИН.

Проверка и испытания функций или комплекса функций зашиты информации от НСД с помощью тестирующих средств, проводятся для отдельных средств АС (технических и программных) по выбору аттестационной комиссии.

На основе исходных данных по технологии обработки и передачи информации, разрешительной системы доступа персонала к защищенным ресурсам АС, анализируется обобщенная технологическая схема АС с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации, устанавливаются опасные факторы и угрозы, критические места АС, снижающие уровень защиты, комплектность и характеристики средств защиты.

По результатам изучения уточняется схема технологического процесса с привязкой к конкретным средствам обработки и передачи информации, и штатному персоналу.

Производится выборочная проверка соответствия размеров контролируемой зоны (КЗ) в представленных документах (планы объектов, планы размещения ОТСС, акты обследования и др.) фактическим размерам контролируемой зоны. Определяются минимальные значения расстояний от источников информативных сигналов до границы КЗ.

Инструментальная оценка защищенности информации от утечки за счет ПЭМИН ОТСС производится для ОТСС в соответствии с действующими нормами эффективности защиты от утечки за счет ПЭМИН, методикой контроля защищенности объекта информатизации, методиками специальных исследований ОТСС. По результатам оформляются протоколы испытаний.

ПРИЛОЖЕНИЕ Д

УТВЕРЖДАЮ

_____

«____»_____2023г.

ЗАКЛЮЧЕНИЕ

по результатам испытаний в рамках аттестации объекта информатизации

При проведении аттестационных испытаний было представлены автоматизированные системы в таблице 1

Таблица 22– Состав средств ОТСС и ВТСС

Наименование	Модель
ОТСС	
АРМ № 1	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
МФУ	HP MFP 135W
АРМ № 2	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
АРМ № 3	
Системный блок	UNIVERSAL
Монитор	Samsung 27V4L
Клавиатура	Logitech K120
Манипулятор «Мышь»	Logitech M90
Сетевое оборудование	
Свитч	D-LINK DES1005C
ВТСС	
Шредер	Deli Core E9954-EU
IP телефон	Yealink
Датчик движения	Риелта Фотон-12 (ИО409-17/1)
Датчик движения	Риелта Фотон-12 (ИО409-17/1)
Извещатель пожарный	RUBEZH ИП 212-45
Извещатель пожарный	RUBEZH ИП 212-45
Извещатель пожарный	RUBEZH ИП 212-45

По утвержденной и согласованной с заявителем Программе и методике проведения аттестации проведены следующие проверки:

- проверка достаточности и соблюдения организационно-режимных мер на объекте информатизации;
- испытания на соответствие требованиям по защите информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) основных технических средств объекта;
- испытания на соответствие требованиям по защите систем электропитания и заземления технических средств объекта;
- испытания объекта на соответствие требованиям по защите информации от несанкционированного доступа к обрабатываемой информации;
- проверка основных технических средств объекта для выявления возможно внедренных электронных устройств перехвата информации.

1. Результаты изучения технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки секретной информации технических средств.

По результатам изучения описания технологического процесса обработки информации, анализа схемы информационных потоков, определения состава используемых для обработки технических средств, выявлены следующие возможные угрозы для защищаемой информации в автоматизированной системе (АС) ОИ:

- утечка информации вследствие несоблюдения организационно-режимных мер;
- несанкционированный доступ к защищаемой информации в АС, включая воздействие на АС вредоносных программ;
- утечка информации за счет побочных электромагнитных излучений и наводок (ПЭМИН);

- утечка информации за счет специальных электронных устройств съема информации, возможно внедренных в основные технические средства и системы (ОТСС) ОИ.

2. Результаты аттестационной проверки организационно-режимных мер по защите информации.

2.2 Представленные документы достаточны и их содержание соответствует требованиям стандартов и руководящих документов по безопасности информации

2.3 Состав и структура программно-аппаратных средств объекта информатизации (ОИ), включенных в реальный технологический процесс обработки защищаемой информации, а также их размещение в помещении № 215б, соответствуют представленной документации. Существующая на объекте практика обработки и хранения конфиденциальной информации соответствует представленному описанию технологического процесса. Пользователь АС объекта информатизации имеет оформленное установленным порядком разрешение на допуск информации.

2.4 Сотрудники осуществляющий эксплуатацию ОИ, имеет определённый опыт и стаж работы с информацией и её защитой

2.5 Имеются документы о разрешительной системе доступа персонала к ОИ:

– Перечень лиц, обслуживающих автоматизированную систему объекта информатизации;

– Перечень лиц, имеющих право самостоятельного доступа в помещение;

– Перечень лиц, имеющих право самостоятельного доступа к штатным средствам автоматизированной системы объекта информатизации и уровень их полномочий;

2.6 Объект информатизации оснащен лицензионными копиями программного обеспечения, согласно Состава программного обеспечения автоматизированной системы объекта информатизации.

2.7 Объект информатизации оснащен сертифицированными средствами защиты информации:

-программно-аппаратным комплексом защиты информации от несанкционированного доступа «Dallas Lock 8.0-К» (Сертификат ФСТЭК России № 2720 от 25 сентября 2012 г. Действителен до 25 сентября 2026 г.);

-генератором шума «Соната – Р3.1» (Сертификат ФСТЭК России № 3539 от 24 марта 2016 г. Действителен до 24 марта 2024 г.);

-антивирусная программа «Dr.Web Enterprise Security Suite» (Сертификат ФСТЭК России № 3509 от 27 января 2016 г. Действителен до 27 января 2019 г. Продлен до 27 января 2024 г.).

2.8 Представленные аттестационной комиссии протоколы и предписания соответствуют требованиям нормативных документов.

2.9 Помещение №215б, в котором находится объект информатизации «АРМ», расположено на 2-ем этаже трехэтажного здания ООО «Газпром Интернешнл» и отвечает требованиям режима, обеспечивающего обработку данных:

- дверь оборудована специальным замком;
- по окончании работы помещение №215б запирается, опечатывается и сдается под охрану;
- выдача ключа от входной двери производится только сотрудникам, имеющим право самостоятельного доступа в помещение №215б, согласно Перечня лиц, имеющих право самостоятельного доступа в помещение №215б с объектом информатизации;
- уборка помещения производится в присутствии лиц, имеющих право самостоятельного доступа в помещение, согласно Перечня лиц, имеющих право самостоятельного доступа в помещение № 215б с объектом информатизации;
- в случае ухода из помещения в рабочее время, помещение закрывается на ключ;

- исключена возможность несанкционированного просмотра информации с монитора, с распечаток принтера лицами, не имеющими права доступа к обрабатываемой информации;

3. Результаты аттестационных испытаний на соответствие требованиям по защите информации от утечки по каналам ПЭМИН.

3.1. В определено минимальное расстояние от ОТСС ОИ «АРМ» до границы контролируемой зоны (R=5м). Реальное расположение ОТСС ОИ «АРМ» соответствует представленной документации.

3.2. По результатам исследований определены значения радиусов зоны 2 для ОТСС ОИ «АРМ» (R=13,8м) средств разведки без использования системы активного зашумления. Указанные значения превышают минимальное расстояние до границы контролируемой зоны, приведенное в Техническом паспорте объекта информатизации.

3.3. По результатам исследований определены значения радиусов зон 1 ОТСС ОИ «АРМ». Указанные значения превышают минимальные расстояния до вспомогательных ТСС, имеющих линии, выходящие за пределы контролируемой зоны, и линий, имеющих выход за пределы контролируемой зоны.

3.4. На объекте в рамках аттестационных испытаний введена в эксплуатацию система активного зашумления на базе генератора шума «Соната – Р3.1».

3.5. При использовании, настоящего заключения, системы активного зашумления на базе генератора шума «Соната – Р3.1» требования к расположению ОТСС ОИ «АРМ» относительно вспомогательных ТСС, имеющих линии, выходящие за пределы контролируемой зоны, и линий, имеющих выход за пределы контролируемой зоны, не предъявляются.

3.6. Использованные при проведении испытаний методики исследований, измерительные средства и измерительная аппаратура соответствуют требованиям нормативных документов. Полнота и схема

проведенных измерений соответствуют требованиям нормативных документов.

4. Результаты испытаний на соответствие требованиям по защите систем электропитания и заземления.

4.1. Трансформаторная подстанция, питающая ОТСС ОИ «АРМ», расположена за пределами контролируемой зоны. При использовании, согласно системы активного зашумления на базе генератора шума «Соната – Р3.1» и неизменности схемы электропитания ОТСС ОИ «АРМ» защита сети электропитания эффективна.

4.2. Заземлитель, используемый для ОТСС ОИ «АРМ», расположен в пределах контролируемой.

4.3. Использованные при проведении испытаний методики исследований, измерительные средства и измерительная аппаратура соответствуют требованиям нормативных документов. Полнота и схема проведенных измерений соответствуют требованиям нормативных документов.

5. Результаты аттестационных испытаний на соответствие требованиям по защите информации от НСД.

5.1. Для обеспечения уровня защищенности по классу 2Б в АС ОИ «АРМ» установлена и настроена система защиты информации (СЗИ) от несанкционированного доступа (НСД) «Dallas Lock 8.0-К».

5.2. В соответствии с комплексными испытаниями автоматизированной системы объекта информатизации «АРМ» на соответствие требованиям по защите от несанкционированного доступа к обрабатываемой информации соответствует требованиям к АС класса защищенности 2Б.

6. Выводы и рекомендации

1. Комплексная система защиты объекта информатизации «АРМ» соответствует нормативным требования по безопасности информации,

предъявляемым к объекту информатизации, в состав которого входит АС класса защищенности 2Б.

2. Рекомендовать выдачу «Аттестата соответствия» объекту информатизации «АРМ» «Газпром Интернешнл» сроком на 3 года при условии обеспечения заявителем неизменности условий функционирования и технологии обработки информации, установленных в процессе аттестационных испытаний.

Члены аттестационной комиссии

_____

ПРИЛОЖЕНИЕ Д

Таблица 23 – Определение класса

Подсистемы и выполненные требования	
1. Подсистема управления доступом	
Идентификация, проверка подлинности и контроль доступа субъектов:	
через вход в систему	+
2. Подсистема регистрации и учета	
При прохождении регистрации и учета:	
регистрируется вход и выход из системы	+
Учет носителей информации	+
3. Криптографическая подсистема	
Шифрование конфиденциальной информации	+
Использование аттестованных (сертифицированных) криптографических средств	+
4. Подсистема обеспечения целостности	
Обеспечение целостности программных средств и обрабатываемой информации	+
Физическая охрана средств вычислительной техники и носителей информации	+
Периодическая проверка средств защиты от НСД	+
Наличие средств восстановления средств защиты от НСД	+

Таблица 24 - Характеристики исходной степени защищенности

№	Параметр	Назначение	Уровень защищенности
1	Расположение	локальная ИСПДн, развернутая в пределах одного здания	высокий
2	Подключенные лини с сетями общего пользования	ИСПДн, имеющая одноточечный выход в сеть общего пользования	средний
3	Проведение операций с записями персональных данных	модификация, передача	низкий

№	Параметр	Назначение	Уровень защищенности
4	Определение уровня допуска к персональным данным	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5	Подключенные линии передачи данных с другими базами ПДн	ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	высокий
6	Показатели обработки персональных данных при обезличивании их	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	средний
7	Объем персональных данных доступный для обработки третьими лицами	ИСПДн, не предоставляющие никакой информации	высокий
Y1 объекта информатизации равен			5