МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(Дипломная работа)

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

Исполнитель _____ Симонов Никита Константинович
(подпись) (фамилия,имя,отчество)

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

«К защите допускаю»

Заведующий кафедрой _____ Бурлов Вячеслав Георгиевич
(подпись) (фамилия,имя,отчество)

«____»_____ 2024 г.

Санкт-Петербург

2024

Оглавление

ВВЕДЕНИЕ

В современном мире, информация приобретает все большее значение, а защита информации становится одной из важнейших и актуальных проблем. ООО «Кравт», как и любая компания работает с большим количеством конфиденциальных данных, которые привлекают злоумышленников. А технические каналы утечки информации представляют большую угрозу не только для бизнеса, но и для общества.

Утечка конфиденциальной информации может привести к значительным финансовым потерям, ущербу репутации и даже к правовым последствиям. В связи с этим возникает необходимость в организации надежной системы защиты информации, способной предотвратить несанкционированный доступ и утечку данных по техническим каналам.

Цель работы – разработка и внедрение эффективных мер защиты информации в компании от утечки по техническим каналам

Задачи которые необходимо решить в работе для достижения дели:

- Произвести анализ объекта информатизации
- Проанализировать угрозы реализации технических каналов утечки информации
- Провести анализ текущего состояния системы защиты информации, идентификацию уязвимостей, определение и анализ потенциальных рисков утечки
- Разработать модель угроз безопасности информации и модель угроз
- Разработать комплекс мер по обеспечению защиты информации от утечки по техническим каналам
- Провести оценку эффективности принятых мер и средств защиты информации

Ожидаемые результаты исследования:

- Повышение эффективности системы защиты информации в компании от утечки по техническим каналам
- Практическое внедрение специальных средств технической защиты информации
- Проведение оценки эффективности применяемых мер, обеспечивающих безопасность информации

ГЛАВА 1. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

1.1Технические каналы утечки информации, их классификация

Утечка информации – это процесс несанкционированной передачи данных от источника к злоумышленнику через канал утечки информации. Одной из основных угроз безопасности конфиденциальной информации является её распространение по техническим каналам. Этот термин обозначает неконтролируемое распространение информативного сигнала от источника через физическую среду к техническим устройствам, которые принимают и обрабатывают эти данные.

Основные технические средства и системы (ОТСС) включают в себя устройства и системы, которые непосредственно обрабатывают, принимают, хранят и передают конфиденциальную информацию. К ним относятся электронно-вычислительная техника, специализированные телефонные станции, системы оперативной и громкоговорящей связи, звукоусиления, звукового сопровождения и записи, а также другие средства, используемые для конфиденциальных переговоров и обработки секретных данных.

Часто вместе с ОТСС используются вспомогательные технические средства и системы (ВТСС), которые не участвуют напрямую в обработке конфиденциальной информации, но применяются совместно с ними. К таким средствам относятся открытые телефонные линии, громкоговорящая связь, системы пожарной и охранной сигнализации, системы электропитания, освещения, заземления, радиофикации, бытовые и измерительные электроприборы и другие. Важно минимизировать размещение ВТСС относительно ОТСС для обеспечения безопасности информации.

Информация в ОТСС защищается различными мерами, такими как инженерно-технические, программно-аппаратные, криптографические, режимные и другие[1].

Особенности технических каналов утечки информации зависят от физической природы информационных сигналов и характеристик среды, через которую они распространяются. На рисунке 1 представлена общая классификация таких каналов, включающая различные виды утечек.

Рисунок 1 – Классификация технических каналов утечки информации

1.2 Угрозы реализации технических каналов утечки информации

Обнаружение и предотвращение утечек данных по техническим каналам — важная задача в сфере информационной безопасности. Одной из частых причин утечки информации является использование закладных электронных устройств, таких как микрофоны, видеокамеры и стетоскопы. Эти устройства могут быть установлены в оборудование, линии электропередачи, строительные конструкции и бытовые предметы.

При обработке данных возможны угрозы безопасности через следующие технические каналы утечки информации, представленные на рисунке 2:

- угрозы утечки акустической (речевой) информации;

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

Рисунок 2 – Реализации технических каналов утечки информации

Акустический сигнал — это колебания частиц в акустической среде, распространяющиеся в виде звуковых волн различной формы и продолжительности. Эти колебания могут возникать из-за механических движений систем, таких как органы речи человека, а также могут быть преобразованы различными устройствами, включая электроакустические преобразователи.

К таким устройствам относятся пьезоэлементы, микрофоны, телефоны, громкоговорители и другие подобные приборы, которые выполняют функцию преобразования акустических колебаний в электрические и обратно.

В зависимости от способа возникновения, распространения в среде и возможности перехвата информационных сигналов, технические каналы утечки акустической (речевой) информации можно разделить на несколько

типов: акустические, виброакустические, виброакустические (лазерные), акустоэлектрические, высокочастотные навязывания и параметрические каналы.

Характеристики основных каналов утечки акустической (речевой) информации и основные параметры средств её перехвата представлены в таблице 1.

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

Название технических каналов утечки информации	Название аппаратуры	Виды аппаратуры	Дальность перехвата акустической (речевой) информации
Акустический	Направленные микрофоны	Стационарная, портативная носимая, портативная возимая	до 150 м
	Ненаправленные микрофоны	Портативная носимая, портативная возимая	до 50 м
Виброакустический	Вибродатчики (контактные микрофоны)	Автономная автоматическая (совместно со средствами приема ретранслируемого сигнала)	до 10 м (на поверхностях 200 см и более)
Виброакустический (лазерный)	Лазерные микрофоны	Стационарная, портативная носимая, портативная возимая	до 600 м
Акустоэлектрический	Средства съема электрических сигналов с гальваническим подключением	Стационарная, портативная возимая	до 250 м
Высокочастотное навязывание	Средства съема электрических сигналов с гальваническим подключением	Стационарная, портативная возимая	до 250 м
Высокочастотное облучение (параметрический)	Приемники электромагнитного излучения	Стационарная, портативная возимая	до 1500 м

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

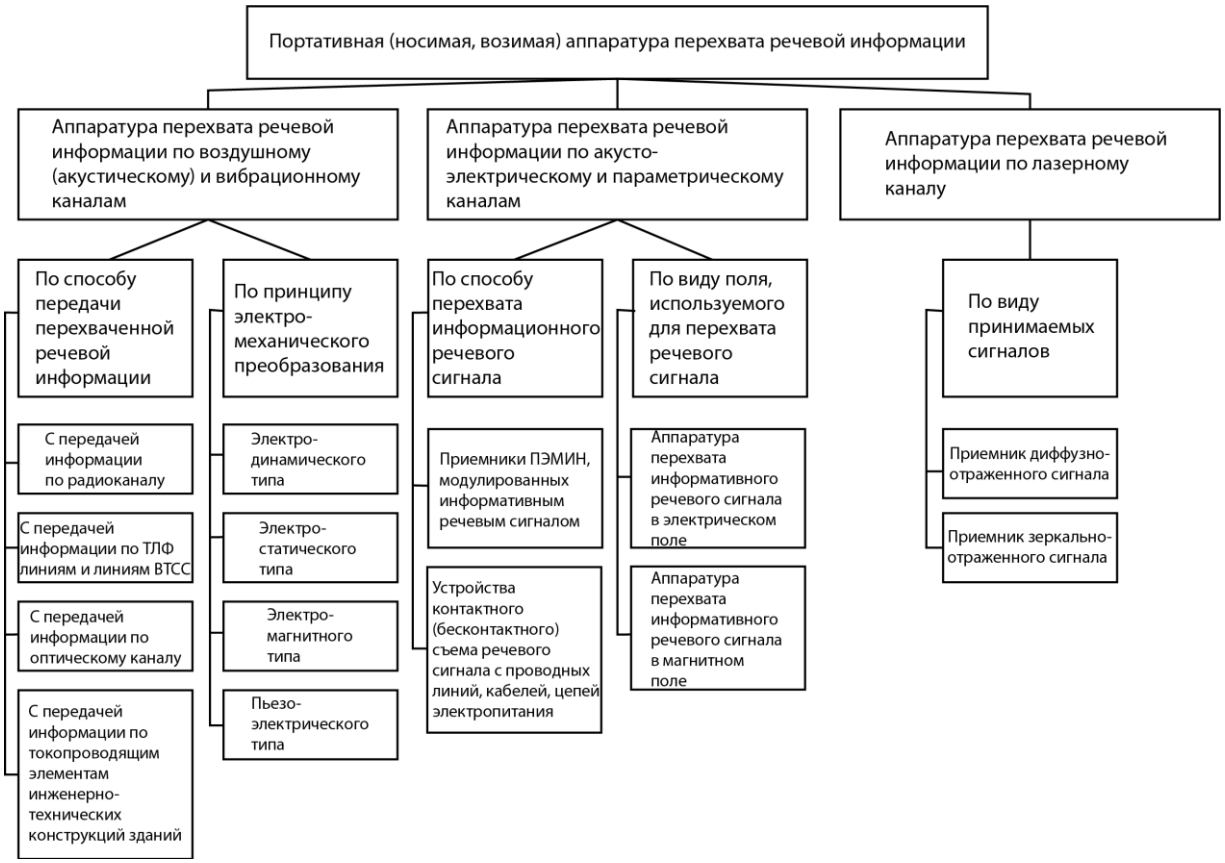

Рисунок 3 – Общая классификация портативной (носимой, возимой) аппаратуры перехвата речевой информации по техническим каналам утечки информации

Посторонние лица могут получать доступ к защищаемой видовой информации двумя способами: непосредственно при несанкционированном проникновении в помещение объекта информатизации или на расстоянии прямой видимости за пределами объекта, используя оптические и/или оптико-электронные устройства.

Для перехвата видовой информации могут применяться различные виды портативных (носимых, возимых) средств, как показано на рисунке 4.

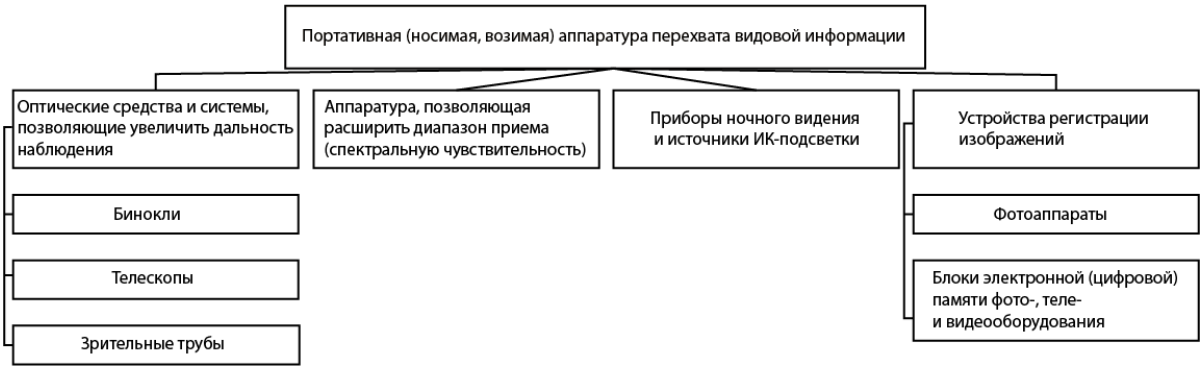

Рисунок 4 – Обобщенная классификация портативной (носимой, возимой) аппаратуры перехвата видовой (графической) информации

Побочные электромагнитные излучения и наводки (ПЭМИН) представляют собой электромагнитные помехи или воздействия, которые могут возникать в различных технических системах.

Побочные электромагнитные излучения появляются в процессе работы электронных устройств и оборудования, таких как компьютеры, мобильные телефоны, радиостанции, телевизоры и другие подобные приборы. Эти устройства могут излучать электромагнитные волны в окружающую среду.

Наводки возникают вследствие внешнего электромагнитного воздействия на систему или устройство. Это может быть вызвано близким расположением других электронных устройств, наличием сильных электромагнитных источников (например, высоковольтных линий электропередачи) или другими внешними факторами.

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

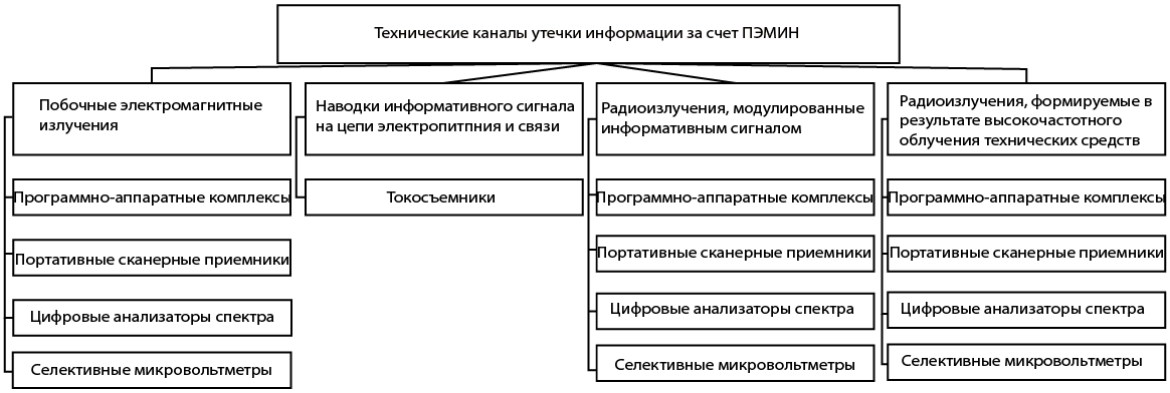

Рисунок 5 – Основные каналы утечки информации за счет ПЭМИН

1.3 Защита информации от утечки по техническим каналам

Число утечек информации возрастает ежегодно. Если говорить об общих цифрах, то эксперты компании InfoWatch подсчитали, что количество скомпрометированных записей Всего за I полугодие 2024г.Скомпрометировано без малого миллиард записей ПДн 986 млн Это на 33,8% больше, чем в I полугодии 2023 г.

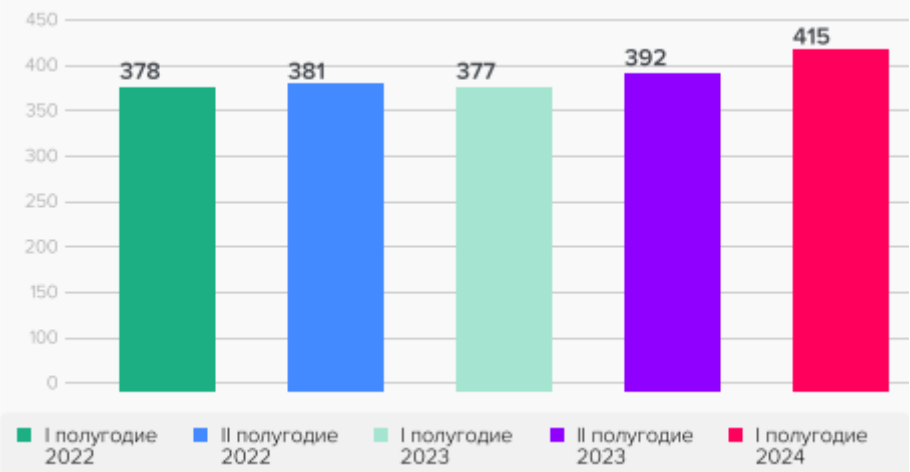

Рисунок 6 – Количество утечек данных

Действительно, с каждым годом риск утечки информации становится всё более значимой проблемой. В условиях роста числа кибератак, взломов и других угроз безопасности данных, защита информации приобретает критическое значение для компаний.

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

Защита информации от утечки по техническим каналам является приоритетной задачей, требующей применения разнообразных подходов и технических средств.

В этом контексте возможны несколько вариантов:

- Источник и носитель информации могут находиться внутри контролируемой зоны объекта, создавая барьер от контакта с

злоумышленниками или удалённого воздействия с использованием технических средств сбора информации.

- Соотношение энергии носителя и уровня помех на выходе приёмника в канале утечки может быть организовано так, что злоумышленнику будет сложно или невозможно получить информацию с требуемым качеством для её использования.
- Злоумышленнику может быть не удастся обнаружить источник или носитель информации.
- Злоумышленник может получить намеренно ложную информацию, воспринимая её как истинную.

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

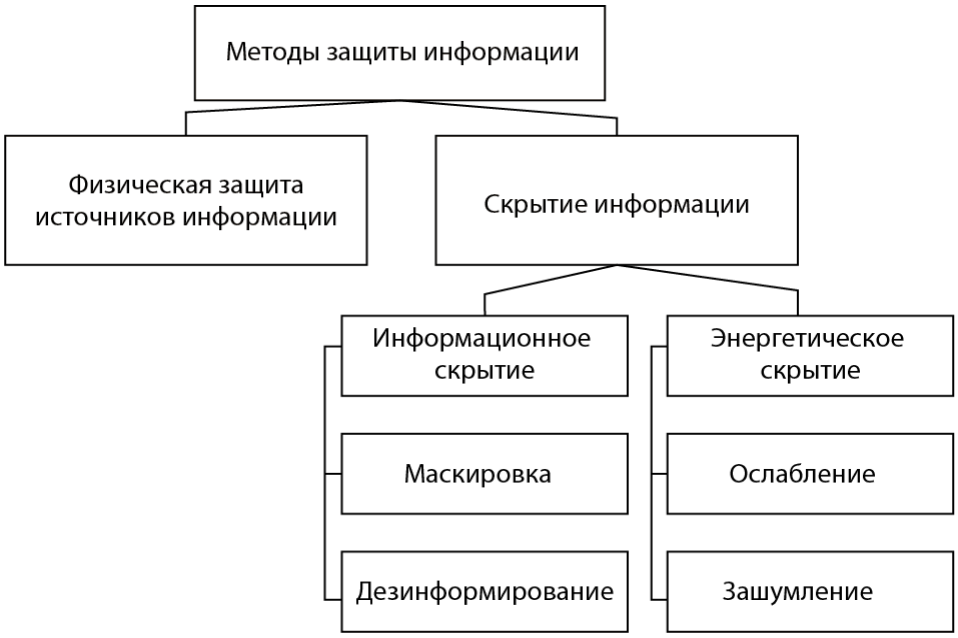

Рисунок 7 – Классификация методов защиты информации от утечки по техническим каналам

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

Энергетическое скрытие включает применение методов и средств защиты, которые препятствуют выполнению энергетического условия разведывательного контакта. Этот метод достигается использованием способов и средств, уменьшающих энергию носителя или увеличивающих энергию помех.

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

Звукопоглощение достигается за счет преобразования кинетической энергии акустической волны в тепловую энергию в звукопоглощающем материале.

Для эффективной защиты с каналами утечки применяются различные методы, цель которых — снизить уровень информационных сигналов или уменьшить соотношение сигнал/шум в процессе передачи до такого значения, при котором исключается возможность перехвата информации за пределами контролируемой зоны.

1.4. Выводы по первой главе

Проведя анализ технических каналов утечки информации, можно заключить, что эффективная защита информации требует комплексного подхода и использования разнообразных методов защиты.

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

ГЛАВА 2. АНАЛИЗ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

В выпускной квалификационной работе рассмотрен объект информатизации – ООО «Кравт», которая занимается контрактной разработкой

IT и мехатронных систем, комплексных решений и автоматизированных встраиваемых технологий, расположенная по адресу г. Санкт-Петербург, Кантемировская 39, офис находится на 3 этаже здания. Окна выходят во двор,и на Кантемировскую улицу. Компания имеет два офиса, 90 сотрудников.

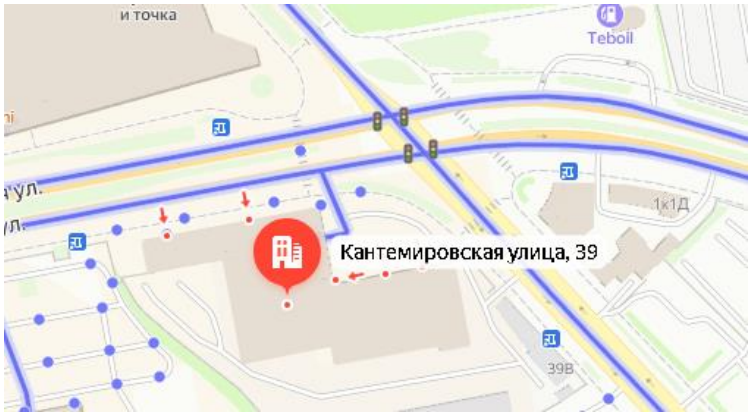

Рисунок 8 Расположение объекта защиты на карте

На рисунке 9,10,11,12 изображены фотографии из окон ближайших зданий. Стоит отметить, что окна офисных помещений выходят на улицу:

Рисунок 9. Вид от входа в здание

Рисунок 10. Здание напротив – виз. Контакт

Рисунок 11. Вид из окна с дальней части офиса

Рисунок 12. Вид из окна с дальней части офиса

2.1. Краткое описание информационной системы:
Все имеющиеся информационные системы размещены на едином сервере и включают в себя следующие компоненты:

1. Easy Redmine – система для управления проектами, в которой ведется учет заявок на закупку, оплаченных счетов, а также мониторинг прогресса работы по проектам и распределение задач между сотрудниками.

2. 1С (Унифицированная налоговая форма, Зарплата и управление персоналом, Корпоративные решения) – используется для учета и управления финансовыми потоками и персоналом.

3.GitLab – система для хранения и управления исходным кодом проектов.

4.Виртуальные машины с гипервизором VMware, обеспечивающие гибкость и масштабируемость вычислительных ресурсов.

5.Сетевой диск, функционирующий без аутентификации пользователей, что может представлять собой потенциальный риск для безопасности.

6.Удаленный доступ через OpenVPN, при котором каждому пользователю предоставляется персональный именной сертификат.

7.3D-моделирование изделий – инструмент для разработки трехмерных моделей.

8.Проектирование печатных плат – специализированные решения для проектирования электронных компонентов.

По информации с сайта руспрофи, на 6.10.2024:, стоимость активов, выручка и финансы представлены на рисунке 13.

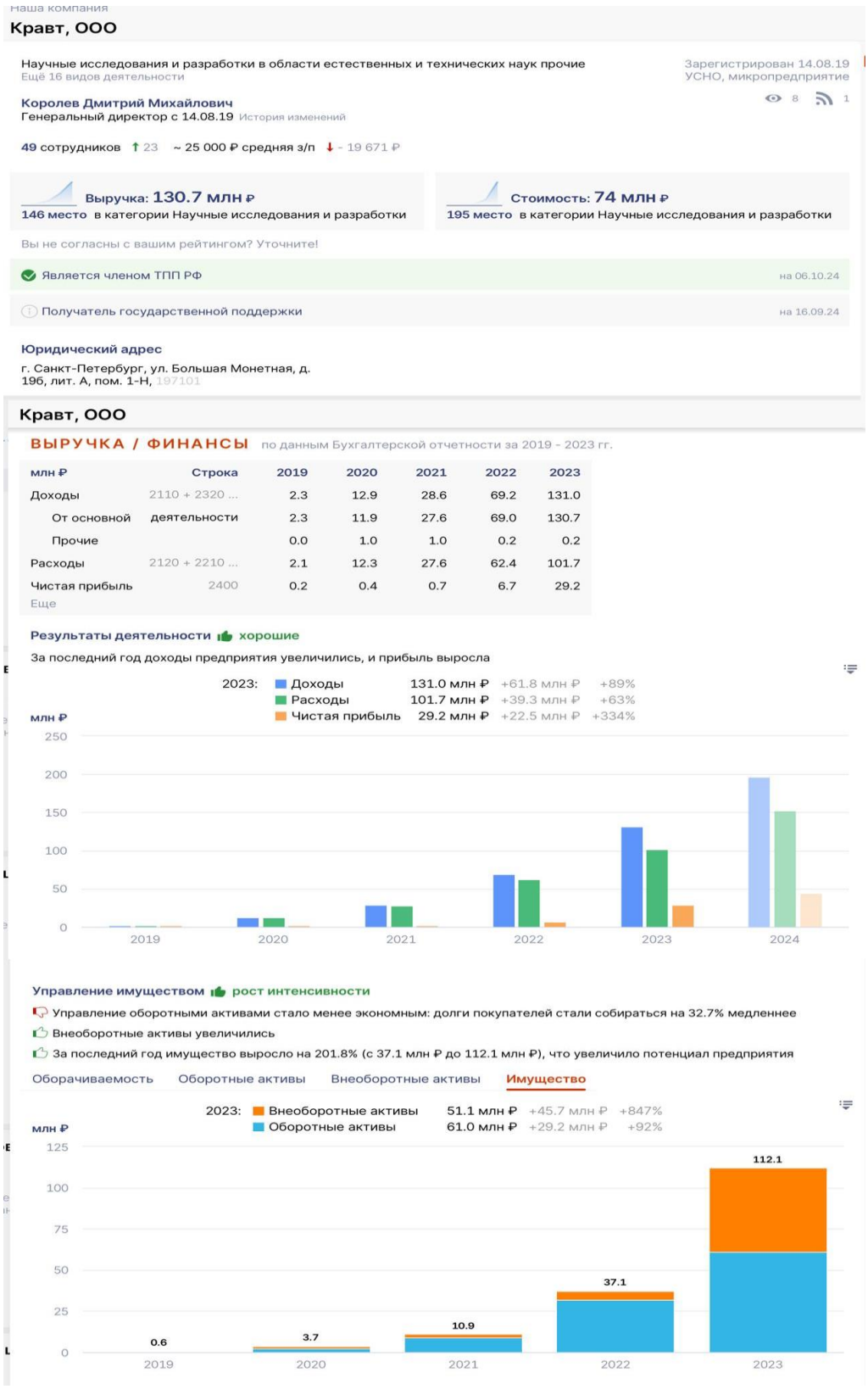

Рисунок 13 – Стоимость, выручка, финансы компании ООО «Кравт»

2.2.Нормативная база по защите информации

В компании по всем проектам имеется договор коммерческой тайны(NDA), который подписывается при подписании контракта на разработку проекта.

Положения NDA по всем проектам:
Получающая сторона обязуется не раскрывать, не передавать и не использовать конфиденциальную информацию в целях, отличных от цели настоящего Соглашения, независимо от того, будут ли между сторонами достигнуты договорённости и заключены соглашения в будущем.

Целью заключения настоящего Соглашения и получения конфиденциальной информации от другой стороны является оценка сторонами возможности и способов дальнейшего взаимодействия друг с другом.

Под конфиденциальной информацией стороны понимают любые сведения и/или данные, которые Получены получающей стороной от передающей стороны, имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании.

Получающая сторона обязуется принимать такие же меры предосторожности и защиты конфиденциальной информации, которые предпринимает в отношении своей собственной конфиденциальной информации.

Получающая сторона обязана определить круг работников, имеющих возможность и право ознакомления с конфиденциальной информацией передающей стороны.

Под передачей и соответствующим ей получением конфиденциальной информации стороны понимают ознакомление в любой возможной форме, в результате которого сторона получает обладание конфиденциальной информацией.

Под раскрытием конфиденциальной информации стороны понимают действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме становится известной третьим лицам.

Под использованием конфиденциальной информации стороны понимают извлечение пользы из конфиденциальной информации получающей стороной и/или третьими лицами, способной принести материальную выгоду получающей стороне.

Каждая сторона обязана сохранять в тайне и не вправе информировать третьих лиц о факте взаимодействия с другой стороной, о содержании и условиях такого взаимодействия.

В случае нарушения положений настоящего Соглашения нарушившая сторона возмещает потерпевшей стороне реальный ущерб. Срок на досудебное урегулирование – 60 календарных дней с момента направления претензии.

Приказ ФСТЭК №17: Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации. [2]

Приказ ФСТЭК №21: В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:идентификация и аутентификация субъектов доступа и объектов доступа; Управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защита машинных носителей информации, на которых хранятся и (или) обрабатываются

персональные данные (далее - машинные носители персональных данных); регистрация событий безопасности; антивирусная защита; обнаружение (предотвращение) вторжений; контроль (анализ) защищенности персональных данных; обеспечение целостности информационной системы и персональных данных; обеспечение доступности персональных данных; защита среды виртуализации; защита технических средств; защита информационной системы, ее средств, систем связи и передачи данных; выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них; управление конфигурацией информационной системы и системы защиты персональных данных. [3]

2.3.Расположение средств обработки информации

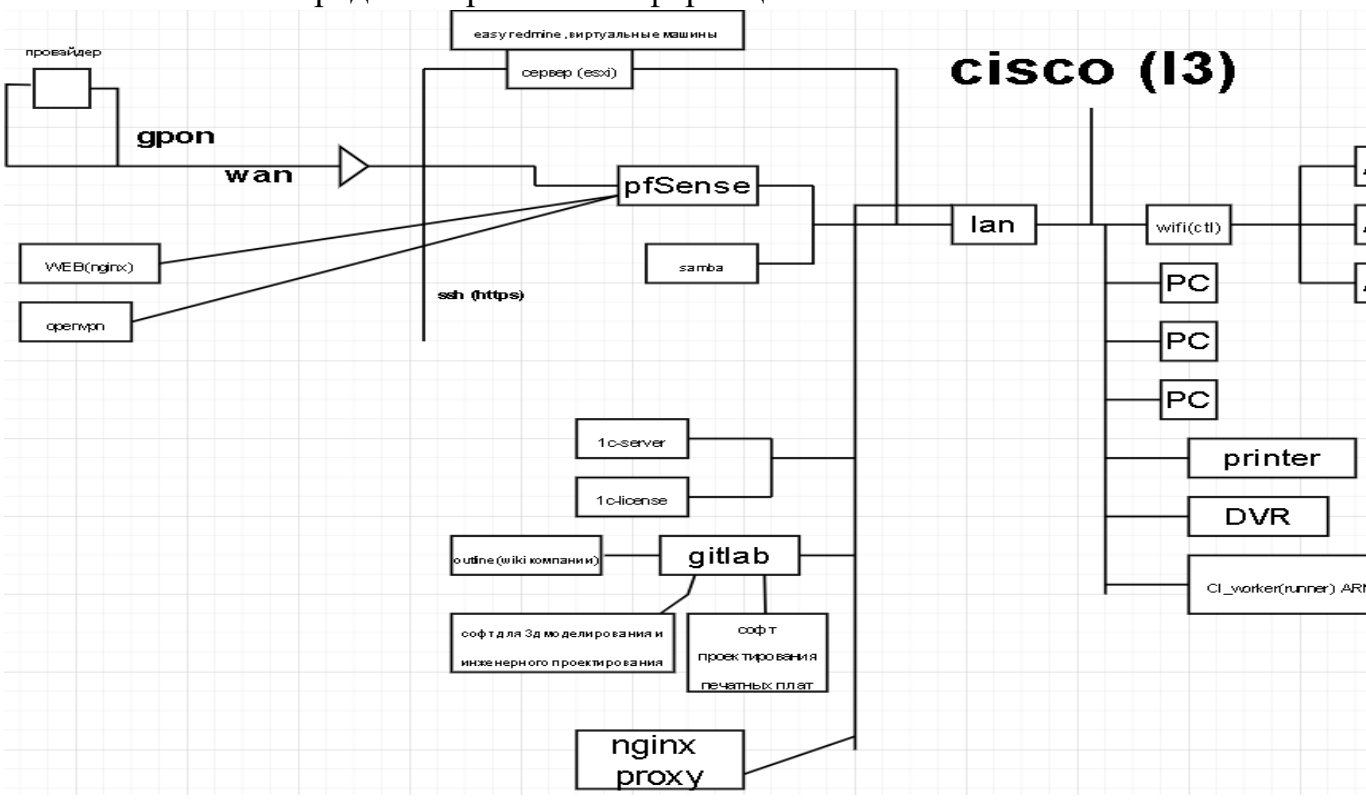

Рисунок 14 -Схема ИС, потоки данных

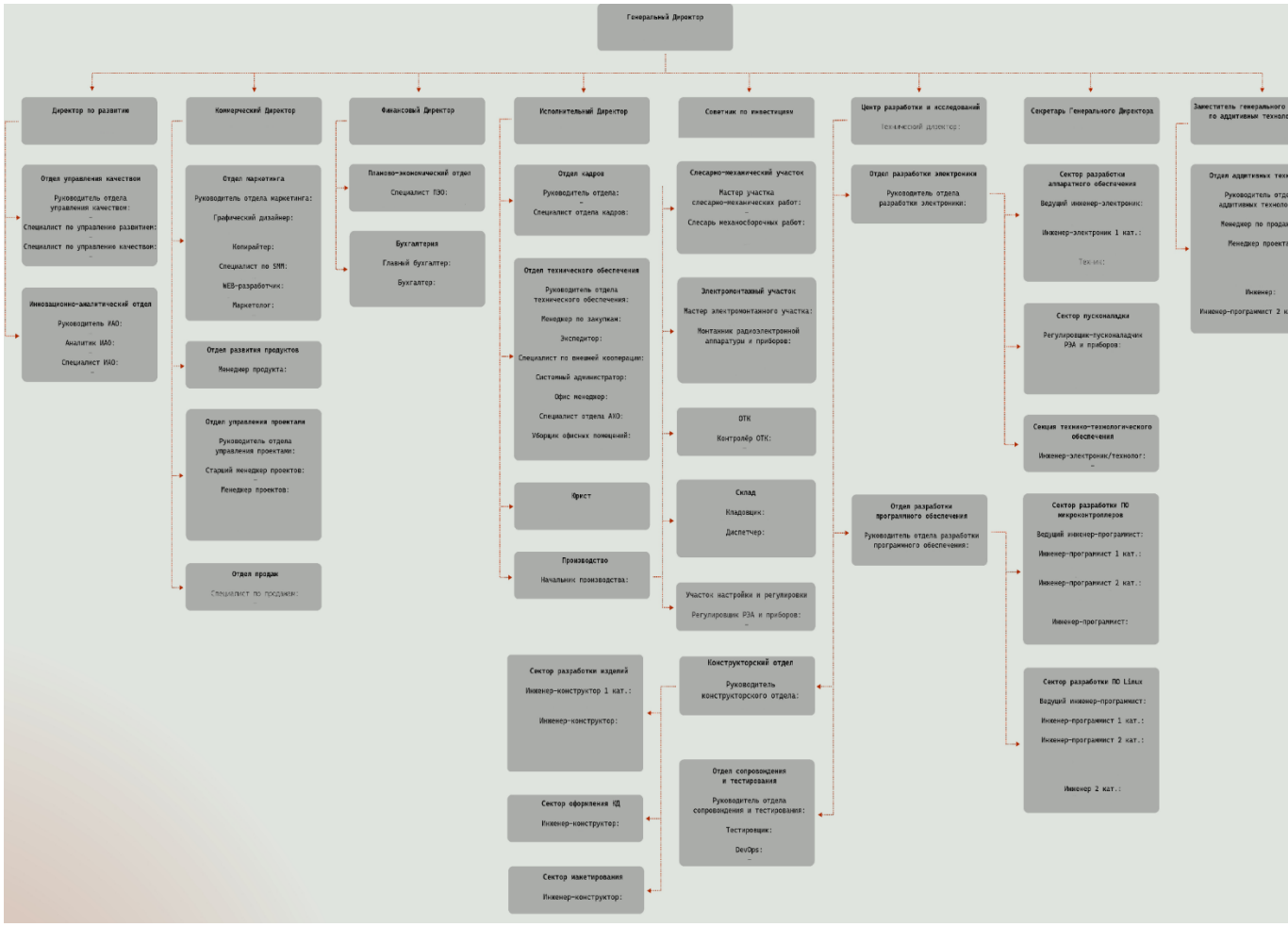

Рисунок 15 - Организационно-штатная структура компании

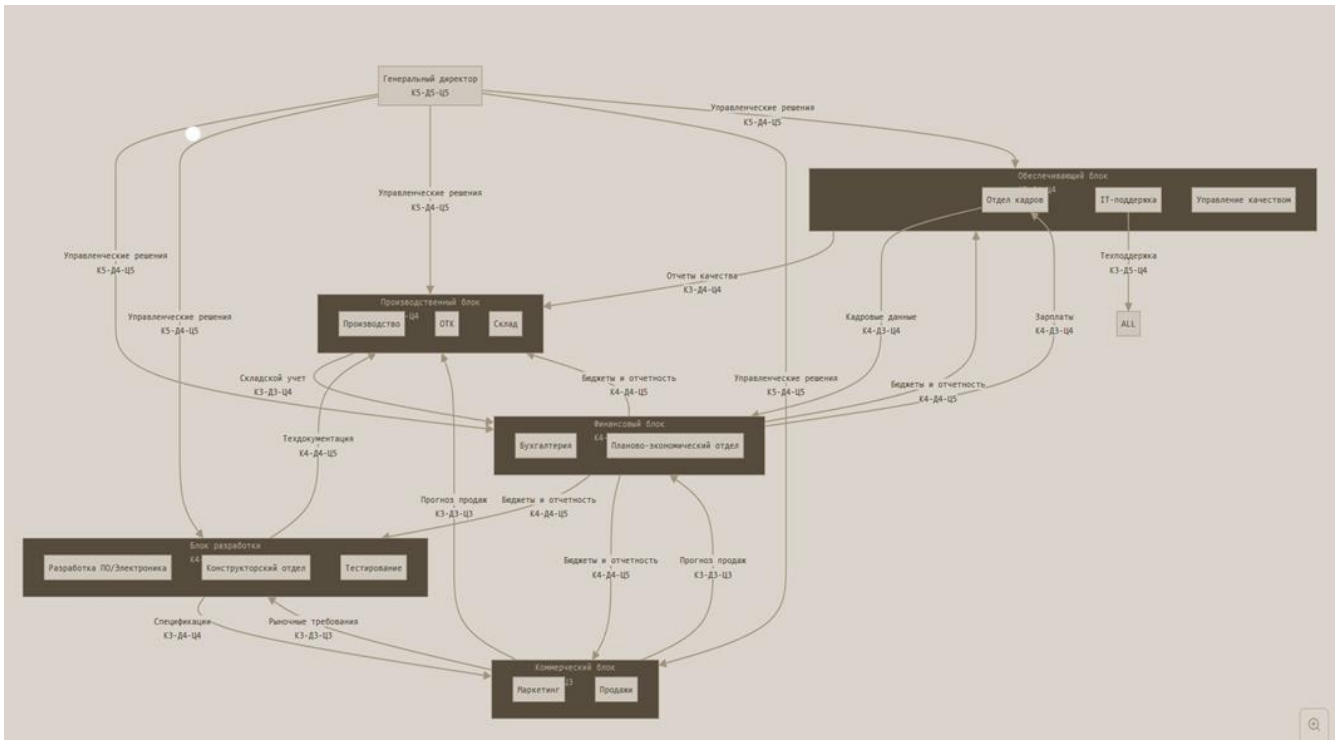

Рисунок 16 - Схема потоков данных между сотрудниками

Имеющиеся средства защиты информации:

В настоящее время наблюдается недостаток специализированных средств защиты информации от утечек по техническим канал. Исключением являются пароли для беспроводных сетей использующие алгоритм шифрования WPA2-PSK/WPA3-SAE с алгоритмом AES. Системы разграниченного доступа в применяемых информационных системах, программное обеспечение TinyWall на некоторых персональных компьютерах, прокси-сервер nginx и технологии NAT/Firewall. Удаленный доступ через персональные сертификаты OpenVPN.Имеется лишь одна камера видеонаблюдения, расположенная у парадного входа, выполняющая функции домофона.

Описанные бизнес-процессы компании

Рисунок.17 – Бизнес процесс 1 процесс разработки конструкции.

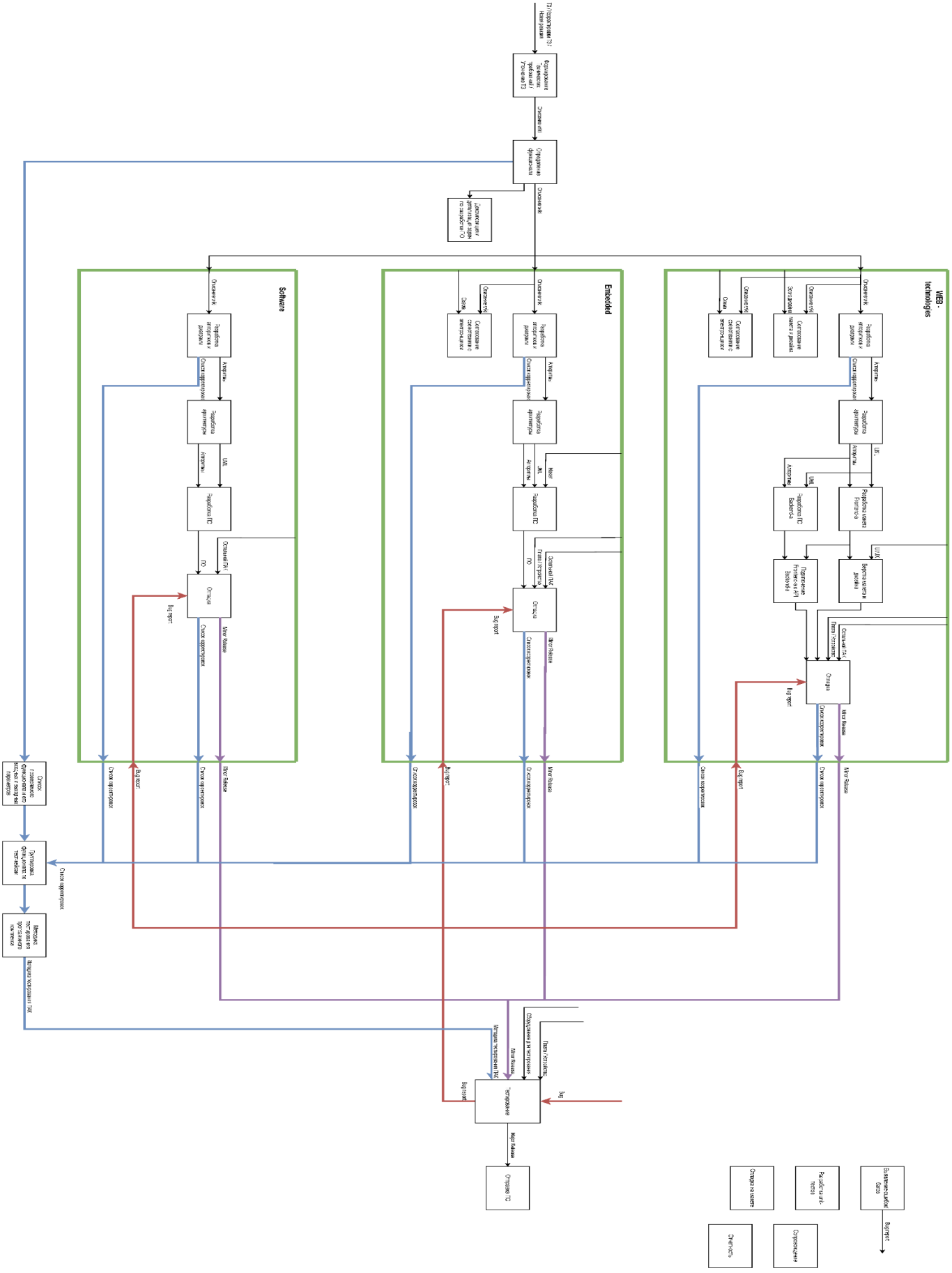

Рисунок.18 Бизнес-процесс №2, разработка программного обеспечения

Экспертный опрос по уязвимостям, ценностям активов

Ну я хоть и совершенно не эксперт. Но вот как мне кажется что тут выходит.

Ресурсы все лежат в локальной сети и доступа к ним извне нет. Однако, доступ извне у сотрудников есть. Как у некоторых сотрудников есть доступ через VPN, так и почти у каждого есть доступ через удалённый рабочий стол. Ссылками обмениваются все спокойно через telegram. Сложность паролей никак не проверяется, и если получить доступ в сеть, то можно получить доступ к любым ресурсам.

Максим Ногин, конструктор

2.4. Планы размещений ОТСС, ВТСС, границ контролируемых зон, силовых и сигнальных сетей, инженерной укрепленности объекта

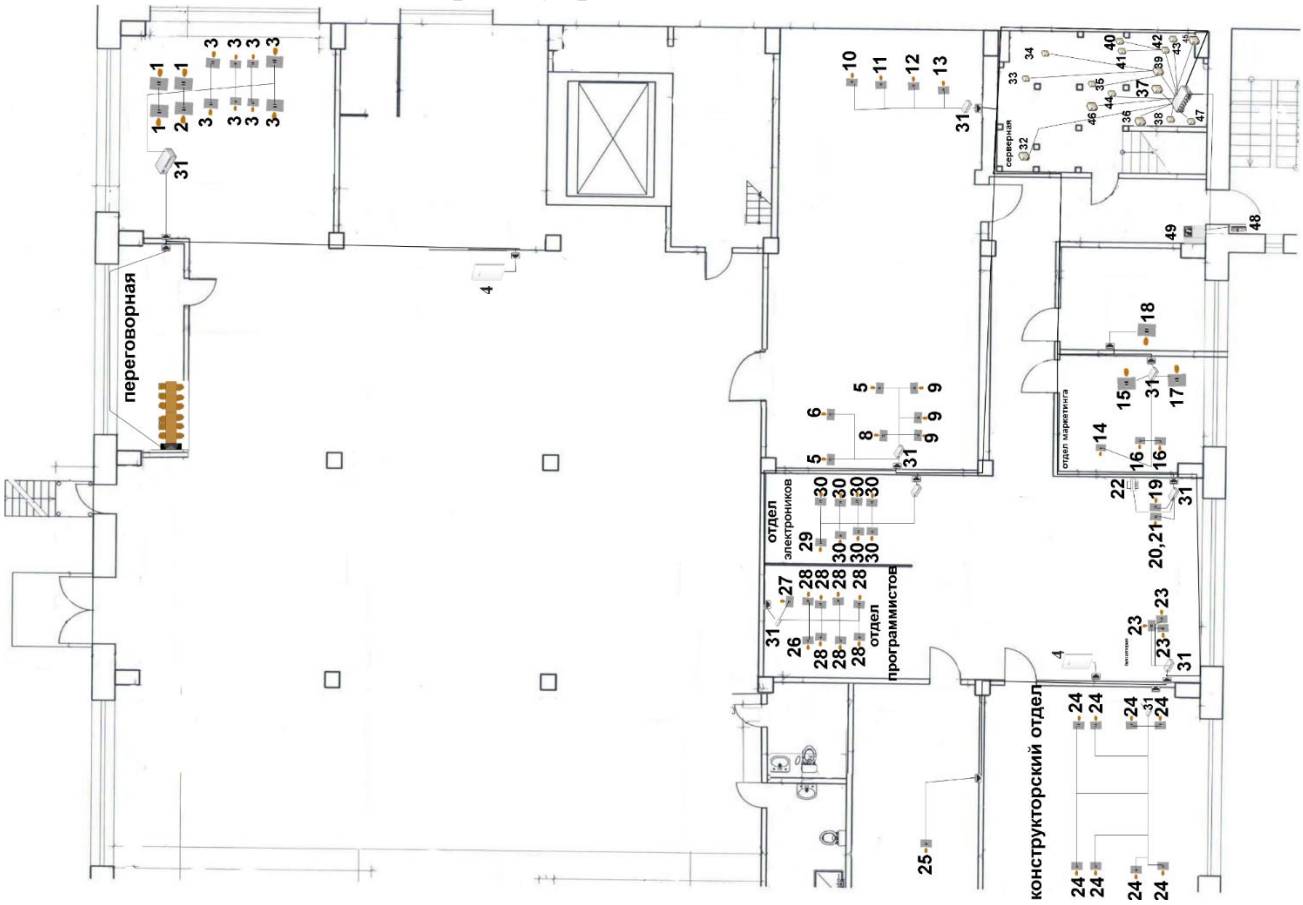

Рисунок. 19 - План размещения основных технических средств и систем (ОТСС)

Список обозначений: Регулировщик пусконаладчик – 1, кладовщик – 2, монтажник 3, EAP235-Wall -4, рук. отдела упр. Проектами -5, коммерческий директор -6, офис-менеджер (кадры) – 7, рук. отдела тех. Обеспечения -8, менеджер проектов – 9, тех.директор – 10, руководитель конструкторского отдела – 11, руководитель отдела разработки ПО – 12, ведущий инженер программист – 13, директор по развитию -14, советник по инвестициям -15, граф. Дизайнер- 16, руководитель отдела маркетинга – 17, исполнительный директор – 18, системный администратор – 19, закупщик – 20, экспедитор -21 принтер -22, специалист планово- экономического отдела -23, инженер конструктор – 24, ген.директор -25, ведущий инженер программист-26, тестировщик – 27, программист – 28, ведущий инженер электроник – 29, электроник – 30, интернет-свитч – 31, pfsense – 32, проектирование эл. Схем - 33, проектирование изделий – 34, docs(wiki) -35, openvpn -36, ssh(https) – 37, 1c, сервер, лицензии -38, gitlab – 39, персональные виртуальные машины(много) – 40, redmine -41, esxi гипервизор-42, samba(сетевой диск) -43, web(nginx) – 44, nginx proxy – 45, nat firewall -46, arm64 ci_runner (worker) -47, "домофон" с камерой -48, монитор - 49

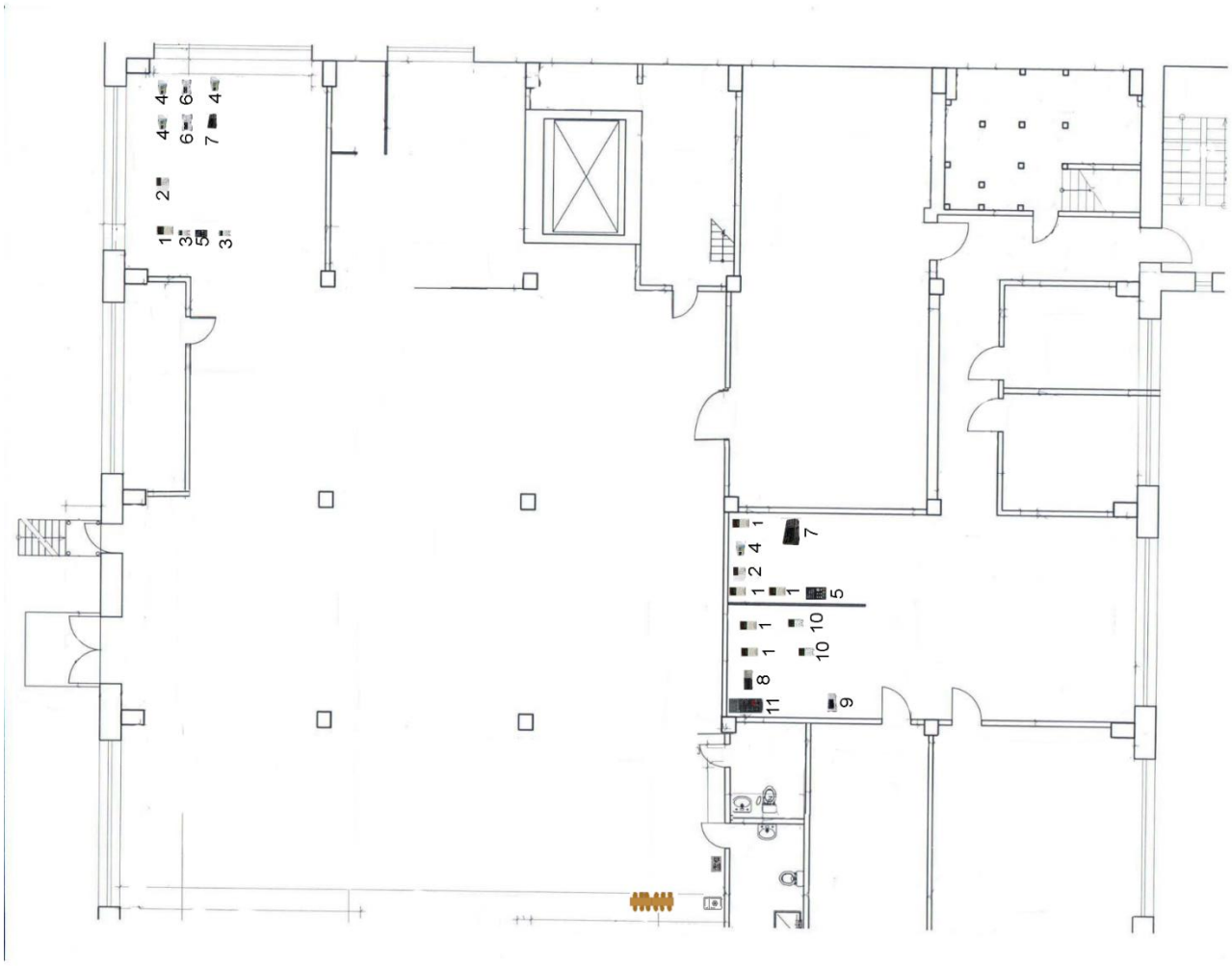

Рисунок 20 План размещения вспомогательных технических средств (ВТСС)

Список обозначений: Uni-t utp1310 – 1, Korad ka3005d – 2, Электронная нагрузка east tester et5410A+ - 3, Owon odp 3063 (источник питания) – 4, OWON SPE6102 – 5 Rigol dl3031a – 6, Rigol mso5102 – 7,Hantec dso4202 – 8,Rigol ds1104 – 9, Uni-t utp 1306 – 10,АКИП-1104 - 11

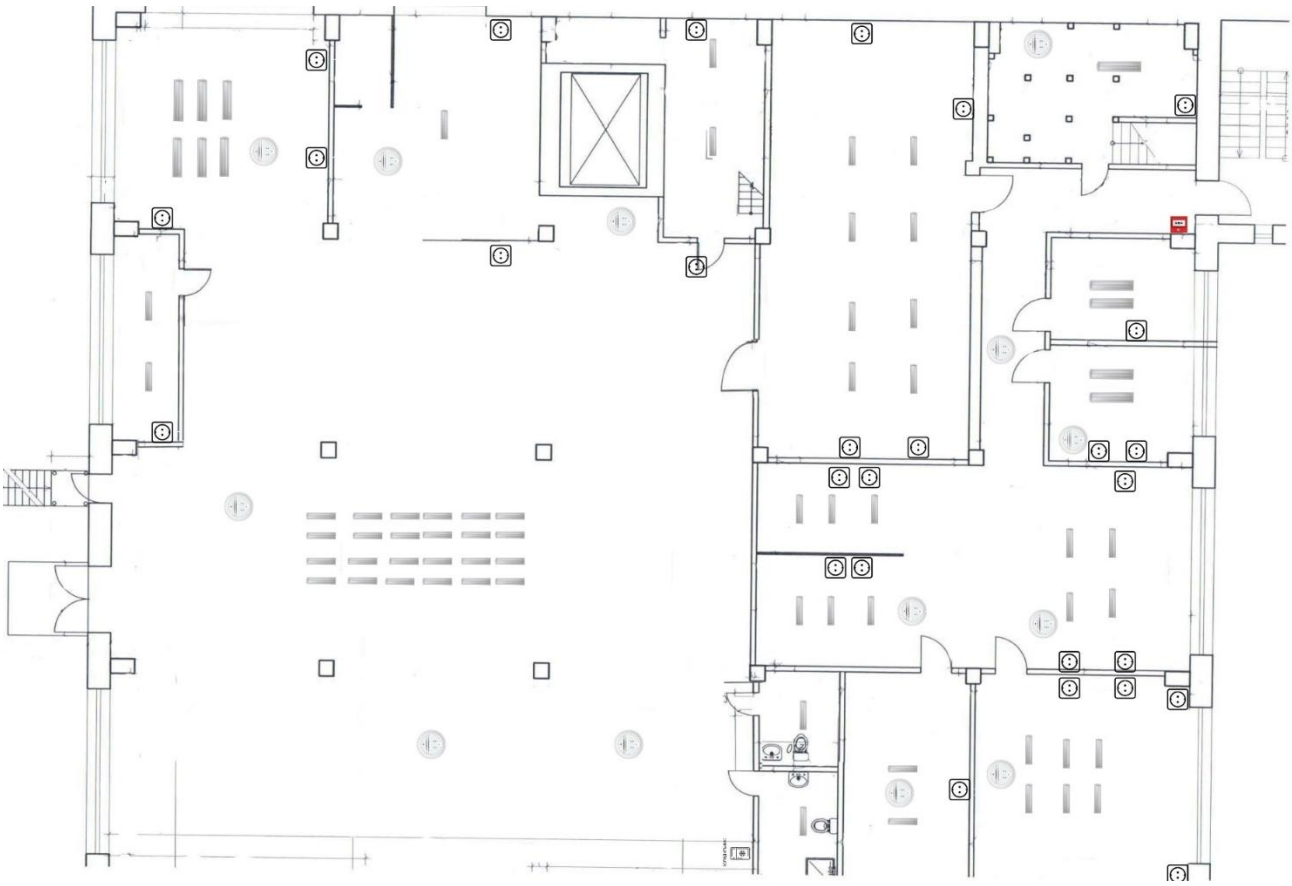

Рисунок 21 Планы силовых и сигнальных сетей

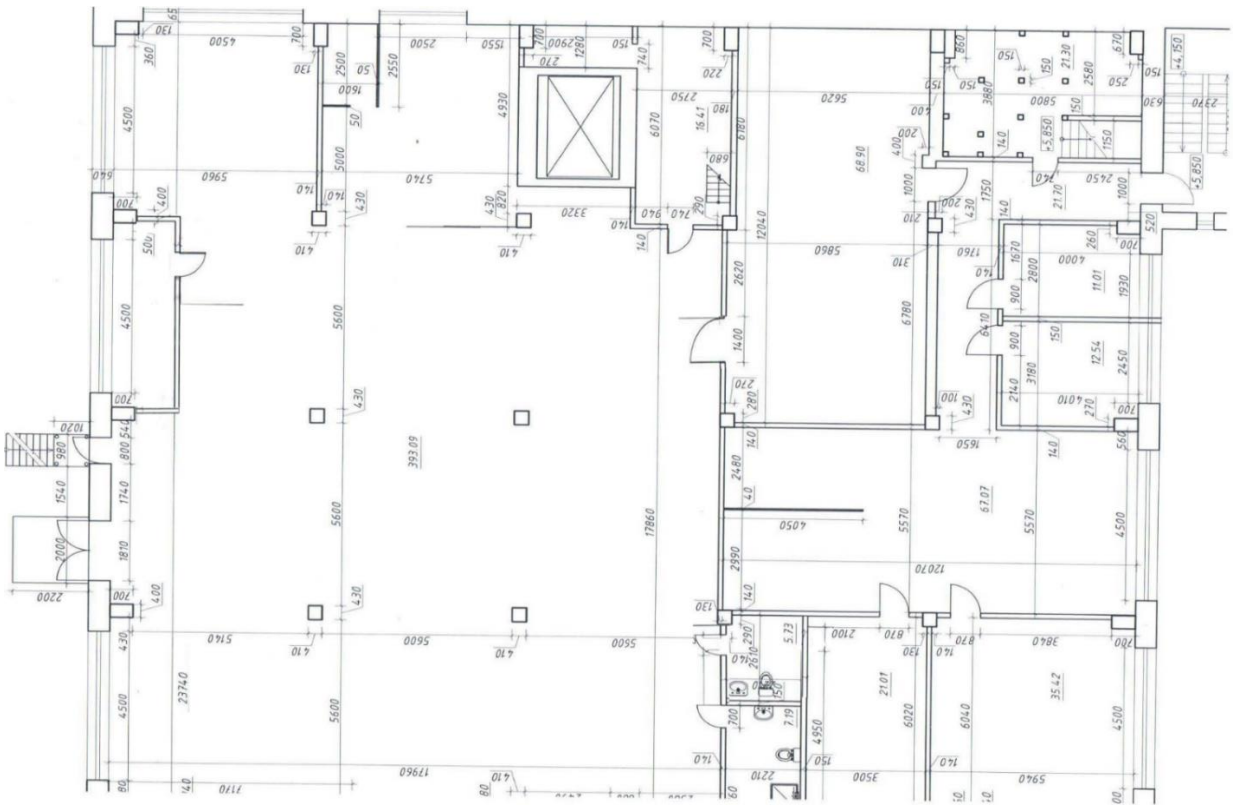

Рисунок.22 - План инженерной укрепленности объекта

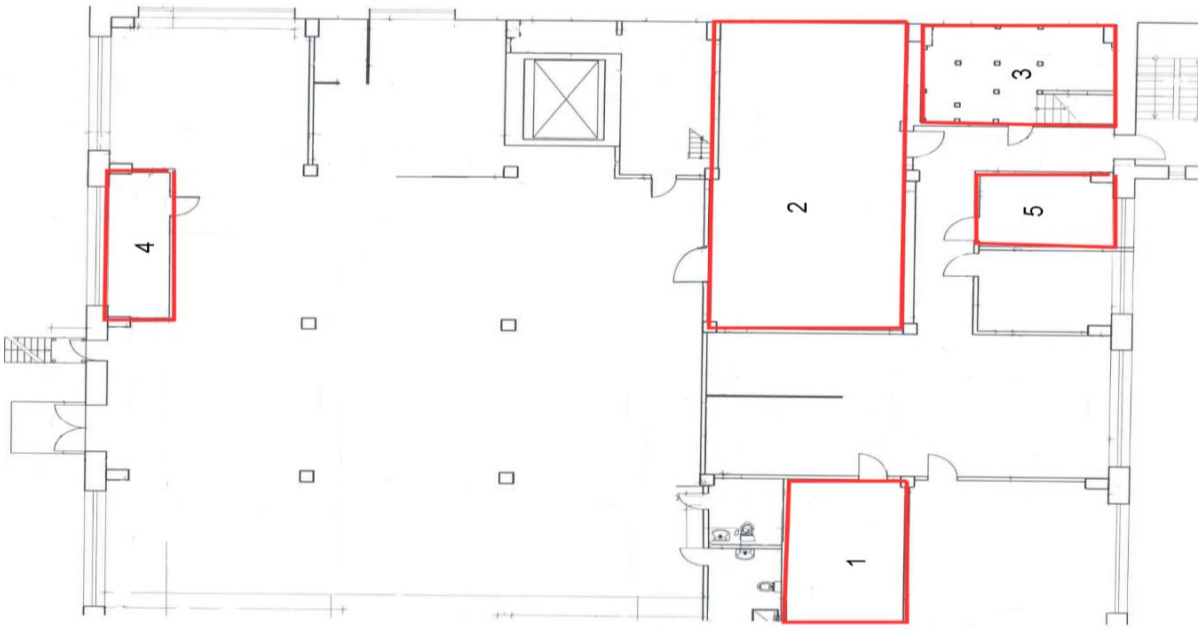

Рисунок 23 Границы контролируемых зон

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

Для компании граница контролируемой зоны проходит по периметру помещения.

2.5.Анализ уязвимостей в компании

Часть сотрудников использует как личные, так и выданные компанией ноутбуки, которые они могут выносить за пределы офиса. В связи с этим, контроль за установленными программами не осуществляется, что создает риски для безопасности.

Отсутствие надежной системы защиты паролей на рабочих станциях, включая легкость их подбора. В некоторых системах разрешен самостоятельный выбор пароля, что не предполагает обязательное использование сложных паролей, сгенерированных специализированными программами.

Кроме того, на рабочих станциях отсутствуют антивирусные программы, что делает их уязвимыми к потенциальным угрозам.

Серверная комната не оборудована замком на двери и располагается в непосредственной близости от парадного входа, что увеличивает риск несанкционированного доступа. Также следует отметить, что над серверной комнатой расположен гардероб, что может способствовать дополнительным угрозам безопасности

Отсутствует система регулярных (плановых) обновлений рабочих станций. Сотрудники имеют возможность самостоятельно обновлять свои персональные компьютеры, в случае использования Windows это осуществляется через функцию автоматического обновления.

В случае систем на базе Linux, используемых программистами, обновление также производится самостоятельно. В рамках разрабатываемых проектов обновления библиотек и пакетов, таких как Python, согласовываются между разработчиками.

Обновление программного обеспечения осуществляется по мере необходимости, при этом лишь в системе 1С поддерживается актуальная версия.

2.6. Оценка системы контроля управления доступом

В организации имеется система контроля доступа, однако, она не является именной. Для выдачи доступа используются одно устройство для прошивания пропусков, расположенное в офисе. Однако нет уверенности, что это устройство доступно исключительно одному лицу, и может передаваться друг другу между сотрудниками. Шлагбаум, располагающийся на задней части офиса, также не обеспечивает достаточный уровень контроля.

В связи с вышеизложенным, отмечаются следующие проблемы:

1.Отсутствие учета рабочего времени: Учет рабочего времени осуществляется исключительно через систему Easy Redmine, при этом его точность зависит от добросовестности сотрудников, которые самостоятельно вносят затраченное время.

2.Отсутствие контроля внутри помещения: После входа на территорию офиса каждый сотрудник имеет возможность свободно перемещаться по всем зонам без каких-либо ограничений.

3. В текущей системе отсутствует механизм, позволяющий отслеживать, кто именно вошел в помещениях компании, а также когда это произошло и когда они покинули офис.

4.Риск использования одного пропуска несколькими людьми: Существует вероятность, что один и тот же пропуск может быть использован несколькими сотрудниками для доступа на территорию.

5. Контроль доступа во двор: Пропускной пункт, обеспечивающий доступ во двор, действует только на машины, при пешем проходе КПП свободен для входа. Наличие лифта, который управляется из здания, и расположенной рядом лестницей добавляет дополнительные риски.

Дверь, находящаяся рядом с лифтом, ведущая к контролируемой зоне, остаётся открытой в рабочее время. Вход в само здание не контролируется, однако существует отдельная дверь, где доступ осуществляется по пропускам, которые не являются именными.

Таким образом, текущая система контроля доступа требует пересмотра и модернизации для повышения уровня безопасности и учета.

Оценка возможности проникновения на территорию

Существует два основных сценария возможного несанкционированного доступа к объекту:

1. Проникновение через парковку: В этом случае, индивиду может быть обеспечен доступ к территории через парковку, и поднявшись по лестнице, злоумышленник может беспрепятственно попасть в здание. Вероятнее всего, посторонний не будет вызывать подозрений и может быть принят за заказчика. Это создает легкую возможность для доступа к переговорной комнате или

серверной, а также для подключения к ближайшему компьютеру. Следует отметить, что в ночное время дверь на лестницу закрывается, что ограничивает доступ в поздние часы.

2.Проникновение через «парадный вход»: В случае получения доступа к ключам от «парадного входа» или проникновения в офис организации с помощью лица, связанного с ней, возможен непосредственный доступ в серверную комнату. Эта комната не имеет запирающего устройства (замка на двери), что позволяет злоумышленнику легко подключиться к локальной сети в комфортных условиях, или внести несанкционированные изменения в работу. Важно подчеркнуть, что серверная расположена непосредственно под гардеробом, что делает ее доступной для несанкционированного доступа. Окна: Визуально-оптический канал утечки, контакт достаточно обширен, так как отсутствуют роллеты, жалюзи и пр. Мониторы повернуты либо боком к окнам, либо параллельно окнам (мониторы направлены в сторону окон) в большинстве случаев.

2.7. Анализ возможных технических каналов утечки информации:
Вентиляция, находится только в большом помещении – вибро-акустический канал утечки

Акустический канал: в большом помещении, рядом с переговорной очень сильное эхо, ввиду размеров помещения. также там имеется вентиляция, Окна открываются часто. Все двери являются акустическим каналом учечки, так как кроме двух входов в офис установлены самые обычные двери.

По контролируемым зонам:

1 зона: (ген.дир)

Туалеты – акустический канал, так как находятся рядом с кабинетом генерального директора

Дверь, стены – акустический канал

2 зона (директора, руководители) – акустический канал, двери, визуальный, так как через них проходит много сотрудников для того чтобы попасть в другую часть офиса

3 зона (серверная) –

4 зона Переговорная:

Визуальный В переговорной окна выходят на парковку.

Акустический канал: ввиду самой обычной двери

5 зона: визуальный канал (окна), акустический – двери, стены

2.7.Разработка модели угроз

Наименование угрозы	Степень риска, объект	внутренний нарушитель	внешний нарушитель
УБИ.003: Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	Степень риска: Высокий Объект: Метаданные, системное программное обеспечение	мотивация: финансовая выгода недовольство.Нарушение конфиденциальности, целостности. Оснащение: доступ к служебным компьютерам и системам, инструменты для анализа уязвимостей. Подготовка: наличие тех. Образования в ИБ. Финансирование: возможность исп. ресурсы предоставляемые работодателем	мотивация: Нарушение конфиденциальности, целостности,. Оснащение: инструменты анализа уязвимостей. Подготовка: наличие образования ИБ, опыт работы с уязвимостями. Финансирование: от потенциальной фирмы конкурента

УБИ.004: Угроза аппаратного сброса пароля BIOS	Степень риска: Средняя обьект: пк сотрудников	мотивация: нарушение конфиденциальности, месть.Нарушение целостности Оснащение: доступ к джамперам на плате\отвертки подготовка: знание о bios\uefi финансирование: не требуется	мотивация: нарушение конфиденциальности, Нарушение целостности Оснащение: доступ к джамперам на плате\отвертки подготовка: знание о bios\uefi финансирование: личные средства
УБИ.017: Угроза доступа/перехвата/изменения HTTP cookies	Степень риска: Высокий объект: браузеры сотрудников		мотивация: нарушение конфединциальности, доступности получении доступа к системам с информацией. Оснащение: программы для анализа сетевых пакетов(Wireshark, Burp Suite). Подготовка: знание уязвимостей http, cookie-атак финансирование: не требуется
УБИ.018: Угроза загрузки нештатной операционной системы	Степень риска Средний Объект: персональные компьютеры сотрудников	мотивация:недовольство, нарушение конфиденциальности, целостности, доступности оснащение: доступ к	мотивация: нарушение конфиденциальности, целостности Информации. Оснащение: загрузочные диски.

		пк, usb-накопители, загрузочные диски подготовка: опыт работы в IT/сис.администрировании. Финансирование: минимальное	Подготовка: опыт в IT/сис.администрировании финансирование: минимальное
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Степень Риска: Высокий Объект: Сервер	мотивация: нарушение целостности, конфиденциальности, доступности оснащение:информация о производителе/модели объекта защиты подготовка: имеющаяся информация об исп. оборудовании финансирование: минимальное	мотивация: нарушение целостности, конфиденциальности, доступности оснащение:информация о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты подготовка: имеющаяся информация об исп. оборудовании финансирование: минимальное

УБИ.038: Угроза исчерпания вычислительных ресурсов хранилища больших данных	Степень риска: Высокий Объект: сервер	мотивация: недовольство, нарушение доступности. оснащение: знание о корпоративным системам, хранилищ данных, их характеристик. подготовка: возможность загрузки такого количества данных, чтобы превысить пропускную способность финансирование: не требуется	мотивация: нарушение доступности. оснащение: знание о корпоративным системам, хранилищ данных, их характеристик. подготовка: возможность загрузки такого количества данных, чтобы превысить пропускную способность финансирование: не требуется
УБИ.062: Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	Степень риска: Высокий Объект: браузеры сотрудников	мотивация: нарушение конфиденциальности, недовотльство, оснащение: доступ к компьютерам, возможность изменение настроек браузера(плагина) возможность обработки передачи данных, подготовка: опыт работы с прокси-серверами, опыт в эксплуатации уязвимостей	мотивания:нарушение конфиденциальности, финансовая выгода, конкуретное преимущество. Оснащение:доступ к инструментам настройки прокси серверов, подготовка: знание об установленных плагинах, навыки программирования

		браузера, знания о внутр. политике безопасности организации финансирование: компания конкурент	
УБИ.069: Угроза неправомерных действий в каналах связи	Степень риска:Средний объект: локальная сеть	мотивация: нарушение конфиденциальности, целостности оснащение: доступ к корп. сети, служебное оборудования, подготовка: инструменты и ПО для эксплуатации узвимостей системы: финансирование: отсутствие значительных затрат	мотивация: нарушение конфиденциальности, целостности. Информации для продажи конкурентам,нарушение работы,внесение модификаций. Оснащение: ПО для перехвата и анализа трафика, знания в сетевой безопасности,медотов атак финансирование: минимальное
УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Степень риска: Высокий, объект: маршрутизаторы, вирт. Машины	мотивация:нарушение конфиденциальности, целостности, доступности, недовольство Нарушение конфиденциальности, целостности, доступности оснащение: доступ к	мотивация: Нарушение конфиденциальности, целостности, доступности, оснащение: возможность получения удаленного доступа, наличие вредоносного ПО,подготовка:

		сетевому оборудованию, рабочим станциям, опыт в написании вредоносных программ подготовка: знание инфраструктуры компании,понимание уязвимостей оборудования,финансирование: компания конкурент, личные средства	исследование уязвимостей, навыки программирования, социальный инженеринг,финансирование: высокое(покупка ПО)
УБИ.074: Угроза несанкционированного доступа к аутентификационной информации	Степень риска: Средний, объект: персональные компьютеры сотрудников	мотивация: месть, Нарушение конфиденциальности оснащение: доступ к ПК сотрудников, инструменты для анализа оперативной памяти, ПО для мониторинга и записи действий пользователя, подготовка: опыт работы с ПО для анализа и извлечения данных финансирование: отсутствуют	мотивация:Нарушение конфиденциальности оснащение: опыт в эксплуатации узявимостей систем, возможность получения удаленного доступа, подготовка: исследование уязвимостей системы, медотов защиты, соц. Инженерия, фишинг, финансирование: компания конкурент

УБИ.076: Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	Степень риска: Высокий, Обьект: гипервизор	мотивация: конфликт с руководством, личное недовольство, Нарушение доступности, оснащение: доступ к внутренним системам, наличие админ. Прав, физический доступ, подготовка: знание архитектуры виртуальной инфрастуктуры, уязвимостей в работе гипервизора, финансирование: отсутствует	мотивация:Нарушение доступности, оснащение: инструменты для взлома, возможность получения прав для осуществления воздействия из виртуальных машин, подготовка: знание об уязвимостях гипервизора, финансирование:компания конкурент
УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам	Степень риска: Средний, объект: Wi-Fi точки доступа		мотивация:нарушение конфиденциальности, доступности, целостности оснащение: оборудование для анализа\перехвата беспроводных сигналов, ПО для эксплуатации уязвимостей, подготовка: знание о недостатках системы, инструменты для анализа беспроводных сигналов,

			реализующего функции эксплуатации уязвимостей протоколов финансирование: значительные затраты на оборудование
УБИ.088: Угроза несанкционированного копирования защищаемой информации	Степень риска: Высокий , объект: пк сотрудников\сетевой диск	мотивация:нарушение конфиденциальности, оснащение: доступ к системам, компьютерам сотрудников, съемный носитель, подготовка: знание где и какая информация хранится, привычки сотрудников(когда их нет за рабочим местом), финансирование: -	мотивация: нарушение конфиденциальности, оснащение: накопители информации, возможность проникновения в офис компании\удаленный доступ, фишинг, соц. Инженеринг,подготовка: изучение организации через открытые источники, финансирование: -
УБИ.139: Угроза преодоления физической защиты	Степень риска: Высокий, объект: сервер	мотивация: недовольство, нарушение конфиденциальности, целостности, доступности, оснащение: - подготовка: не требуется, ввиду	мотивация: нарушение конфиденциальности, целостности, доступности, оснащение: инструменты для взлома,знание о возможностях проникновение в здание, приборы

		наличия доступа финансирование: -	прослушивания и наблюдения, подготовка:исследование объекта, плана и графика работы сотрудников, финансирование: минимальное
УБИ.168: Угроза «кражи» учётной записи доступа к сетевым сервисам	Степень риска: высокий, объект: почта сотрудника,		мотивация: нарушение конфиденциальности, доступности,оснащение: фишинг, соц. Инженерия, кей-логгеры подготовка: предварительное исследование целевой компании, сотрудников, финансирование: -
УБИ.201: Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	Степень риска: Высокий , объект браузеры пользователей		мотивация: нарушение конфиденциальности оснащение: ПО для перехвата вводимых данных, подготовка: сбор информации из открытых источников, финансирование: приобретение спец. ПО

2.8. Выводы по второй главе

Анализ объекта информатизации служит основой для последующей разработки системы защиты информации.

В процессе работы мной были определены ключевые направления защиты информации в автоматизированной системе:

- Обеспечение защиты информации от утечки по техническим каналам во время ее обработки, хранения и передачи по каналам связи.
- Защита информации от кражи, потери, уничтожения, искажения, подделки и блокирования доступа в результате несанкционированного доступа(НСД)

ГЛАВА 3. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ПРИ ЕЕ ОБРАБОТКЕ, ХРАНЕНИИ И ПЕРЕДАЧЕ ДАННЫХ

3.1. Средства защиты информации от утечки по техническим каналам

Защита конфиденциальной информации от утечки по техническим каналам обязательна для обеспечения информационной безопасности организации. Для этого необходимо использовать комплекс организационных и технических мер, которые вместе формируют систему технической защиты информации на защищаемом объекте.

3.1.1. Организационные меры по защите информации

Организационная защита конфиденциальной информации является комплексом мер, процедурного и административного методов, регламентирующих работу с важными данными, их хранение, передачу, обработку.

Для данного объекта информатизации используются следующие организационные меры защиты информации:

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

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

3.1.2. Технические средства защиты информации

Технические средства защиты информации представляют собой специализированные устройства, обеспечивающие безопасность данных посредством аппаратных решений.

Надежная техническая защита информации играет ключевую роль в комплексной системе обеспечения информационной безопасности и способствует снижению финансовых затрат на защиту данных.

Для успешного выполнения задач по технической защите информации необходимо наличие квалифицированных специалистов в этой области и специальных устройств, способных выявлять и перекрывать потенциальные каналы утечки данных. Подбор таких устройств осуществляется на основе анализа текущих угроз и уровня защищенности объекта информатизации.

На основе текущей Модели угроз была определена актуальная угроза безопасности информации, реализация которой может привести к нарушению защищенности данных, обрабатываемых в автоматизированной системе и сетях:

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

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

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

Средства вычислительной техники – это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем [11].

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

Для перехвата побочных электромагнитных излучений от средств вычислительной техники применяются специальные стационарные, перевозимые и переносимые приёмные устройства, известные как технические средства разведки побочных электромагнитных излучений и наводок.

Побочные электромагнитные излучения от технических средств обработки информации могут создавать электромагнитные и параметрические каналы утечки данных, а также вызывать наводки информационных сигналов в посторонних токоведущих линиях и конструкциях. Поэтому значительное внимание уделяется снижению уровня этих побочных излучений.

Эффективность системы защиты основных и вспомогательных технических средств от утечки информации по техническим каналам оценивается через всесторонний анализ, учитывающий различные критерии.

Один из ключевых показателей — это отношение сигнал/шум, которое зависит от физических характеристик информационного сигнала.

Защита информации от утечки через побочные электромагнитные излучения и наводки (ПЭМИН) реализуется с применением пассивных и активных методов и средств. Классификация методов защиты информации от утечки по каналу ПЭМИН представлена на рисунке 22:

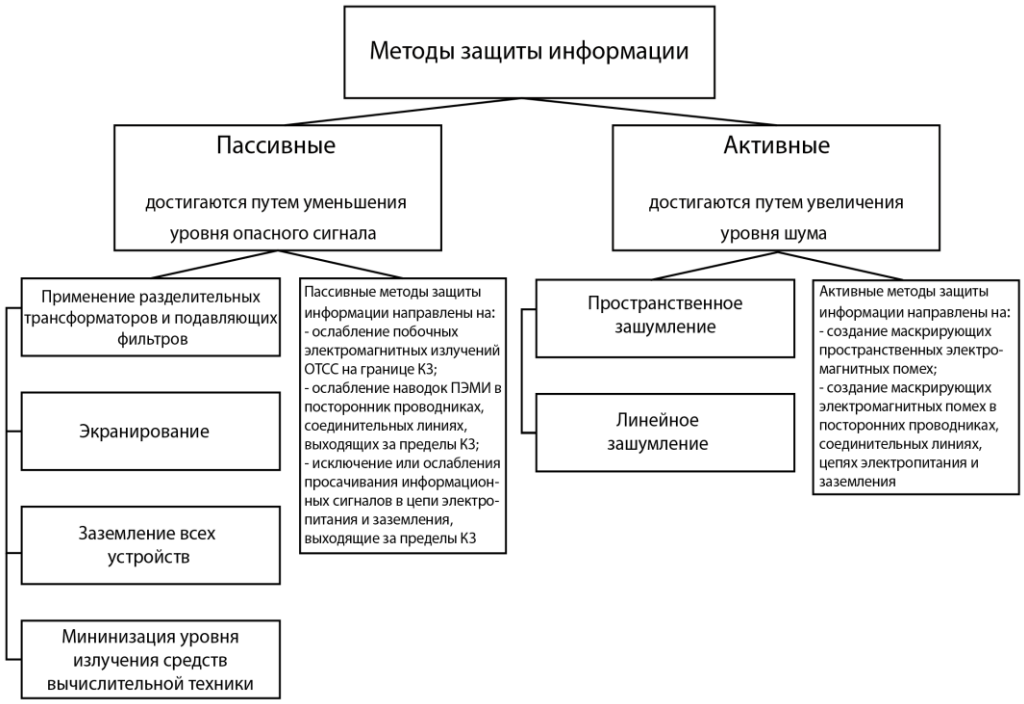

Рисунок 22 – Классификация методов защиты информации от утечки по каналу побочных электромагнитных излучений и наводок (ПЭМИН).

Активный метод защиты информации реализуется путем перекрытия полезного сигнала более мощным шумом. Генератор шума создает интенсивные электромагнитные излучения, которые не несут никакой информационной ценности и делают съем полезного сигнала практически невозможным. Однако следует учитывать, что генератор шума имеет свои недостатки:

- Мощное излучение может быть вредным для здоровья.
- Наличие маскирующих средств защиты может сигнализировать о присутствии конфиденциальной информации.

Пассивный же метод защиты информации заключается в уменьшении мощности излучаемого сигнала.

Таким образом, наиболее эффективным решением в соотношении цена/качество является комбинированный подход, сочетающий активные и пассивные методы защиты информации.

Рисунок 24 показывает схему работы активных и пассивных методов защиты от утечки информации по каналу ПЭМИН.

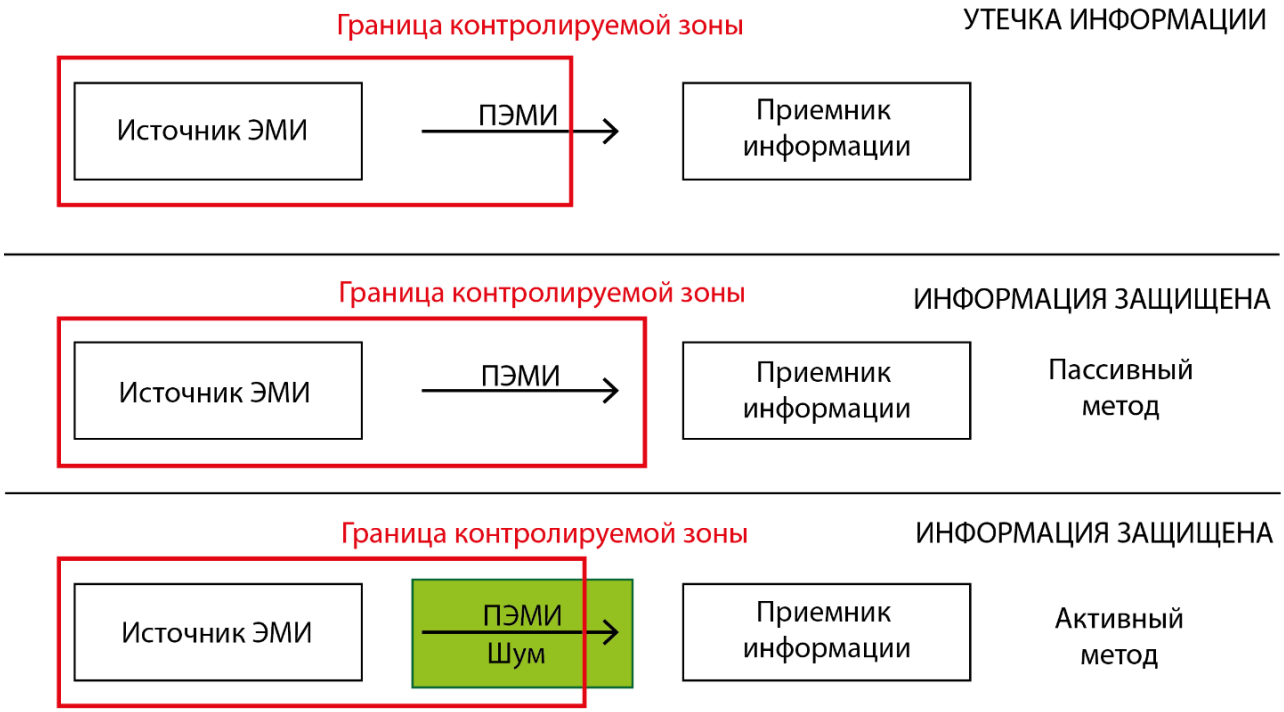

Рисунок 24 – Схема работы методов защиты от утечки информации по каналу ПЭМИН.

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

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

В своей работе для оценки защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы, я буду применять методику анализа защищенности конфиденциальных данных от утечки по техническим каналам.

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

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

При проведении оценки защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от ее утечки по каналу побочных электромагнитных излучений будет рассчитан радиус зон, и уровень допустимых сигналов, ввиду отсутствия оборудования для проведения измерений.

Допустимые уровни сигналов:

- Кабинет директора: P=10 μВт,
- Кабинет руководителей: P=10 μВт,
- Серверная комната: P=5 μВт,
- Переговорная комната: P=50 μВт,
- Кабинет исполнительного директора: P=10 μВт.

Условная мощность сигнала оборудования: Для вычислений принято P_0=100 мкВт

Расчеты для каждой зоны:

1. **Кабинет директора:** $r = \sqrt{\frac{1000}{10}} = 10\text{м}$
2. **Кабинет руководителей:** $r = \sqrt{\frac{1000}{10}} = 10\text{м}$
3. **Серверная комната:** $r = \sqrt{\frac{1000}{5}} = 14.14\text{м}$
4. **Переговорная комната:** $r = \sqrt{\frac{1000}{50}} = 4.47\text{м}$
5. **Кабинет исполнительного директора:** $r = \sqrt{\frac{1000}{10}} = 10\text{м}$

Зона	Инвентарь	Допустимый уровень сигнала	Радиус зоны
Кабинет директора	ПК, монитор, клавиатура, мышь	10	10
Кабинет руководителя	11 рабочих мест (ПК, монитор и др.)	10	10
Серверная комната	Сервер с данными	5	14.14
Переговорная комната	ПК, телевизор, клавиатура, мышь	50	4.47
Кабинет исп. директора	ПК, монитор, клавиатура, мышь	10	10

Таблица 2Уровень сигнала и рассчитанный радиус зоны R

Технические средства защиты информации (ТСЗИ) представляют собой аппаратные устройства, содержащие инженерные, механические или электронные компоненты. Эти устройства предназначены для решения задач по обеспечению безопасности информации, предотвращая ее утечку через различные каналы или защищая ее с помощью различных технических методов.

Исходя из рассчитанного радиуса R был выбран на генератор ПЭМИН КЕДР-П, который в свою очередь является средством активной защиты типа «А» и типа «Б» 2 класса защиты, информации от утечки за счет побочных электромагнитных излучений и наводок, так как значение показателя электромагнитной совместимости Изделия с радиоэлектронными средствами гражданского назначения Rэмс при установке регулятора выходной мощности в

положение, соответствующее максимальному уровню, составляет не более 14 м. И имеет сертификат соответствия №4837 ФСТЭК от 29.08.2024, действительный до 29.08.2029. Характеристики представлены в таблице 3.

Таблица 3 – характеристики устройства КЕДР-П

Параметр	Значение
Полоса излучения электромагнитного поля шумового сигнала, МГц, не менее	0,009 - 6000
Количество выходных розеток типа EURO с заземлением	6
Питание	220В+10%-15;%, 50Гц
Потребляемая мощность, не более, ВА	10
Ток нагрузки, подключаемой к розеткам, не более, А	10
Защита цепи электропитания и потребителей изделия от короткого замыкания	плавкий предохранитель, автомат
Защита цепи электропитания и потребителей изделия от перегрева	автоматический термопрерыватель
Рабочий диапазон температур	от + 5°С до + 40°С;
Относительная влажность воздуха	до 80% при + 25°С;
Атмосферное давление	от 630 до 795 мм. рт. ст.
Габаритные размеры, ДЛ*Ш*В, мм	310х170х50
Масса, не более, кг	1,2

3.3. Обеспечение защиты информации от кражи, потери, уничтожения, искажения, подделки и блокировке доступа в результате несанкционированного доступа.

Несанкционированный доступ (НСД) представляет собой незаконное умышленное получение конфиденциальной информации лицом, не имеющим права на доступ к защищенным данным.

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

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

Для защиты от угрозы несанкционированного доступа лиц к объекту информатизации был разработан ряд мер, целью которых является снижение вероятности реализации выявленных рисков.

- Внедрена система видеонаблюдения ;
- Произведена замена текущих дверей на металлические, с замком.
- Улучшена система видеонаблюдения
- Подключен видеодомофон, с магнитным замком на черный вход
- Установлено средство защиты информации от несанкционированного доступа

При выборе СЗИ выбор пал на Kaspersky Endpoint Security Cloud, исходя из его функционала и совместимости, и зарекомендовавшей себя с хорошей стороны компании Kaspersky:

- Совместим с устройствами Windows
- Защита от программ шифрования, вредоносного ПО
- Обеспечивает защиту от неизвестных угроз
- Защищает сетевую инфраструктуру от внешних угроз
- Позволяет контролировать доступ к облачным службам и сайтам

Стоимость на 14 рабочих мест составила 38010 руб. в год.

3.4. Анализ результативности используемых мер и средств защиты информации
Эффективность мер по обеспечению безопасности информации оценивается по следующим критериям:

1. Уровень надежности: ключевым условием для защиты данных является наличие грамотно организованных уровней защиты, которые последовательно предотвращают несанкционированный доступ, атаки и другие противоправные действия.
2. Эффективность системы: определяется несколькими важными факторами, такими как скорость и результативность предотвращения атак, способность оперативно реагировать на потенциальные угрозы и минимизировать воздействие на конфиденциальные данные.

3. Соответствие нормативно-правовым требованиям: юридическая защита данных.
4. Соотношение стоимости и эффективности: система должна быть признана целесообразной, учитывая затраты на реализацию, внедрение и поддержку. Безопасность должна обеспечивать баланс между расходами и достигнутыми результатами.

Чтобы эффективно использовать технические средства защиты информации от утечек по техническим каналам, необходимо проводить оценку и контроль защищенности данных, обрабатываемых на основных технических средствах и системах в составе автоматизированных систем, от утечек через каналы побочных электромагнитных излучений (ПЭМИ) и за счет наводок информативного сигнала на цепи электропитания и заземления, выходящие за пределы контролируемой зоны.

После применения ТСЗИ от утечки за счет ПЭМИН «Генератор ПЭМИН КЕДР-П», создается интенсивное шумовое поле в диапазоне от 0,009 до 6000 МГц. Информация считается защищенной от утечки через каналы побочных электромагнитных излучений и за счет наводок информативного сигнала на цепи электропитания и заземления, выходящие за пределы контролируемой зоны.

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

- СЗИ от НСД Kaspersky endpoint cloud
- Внедрена система видеонаблюдения и система контроля управления доступом

Таблица 4 - Спецификация выбранных средств защиты информации от утечки по техническим каналам

• Наименование товара	Тип	Цена, руб.	Количество, шт.	Сумма, руб.
Средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок	Генератор ПЭМИН КЕДР-П	35 000 руб.	9	315 000 руб.
СЗИ от НСД	«Kaspersky Endpoint Security Cloud»	2715 руб	14	38 010₽.
Видеокамера	HiWatch DS-I200(E)(2.8мм)	8 190,00 руб.	3	24570,00 руб.
Дверь	Однопольная техническая дверь с выдавленным рисунком	13500 руб.	6	81 000 руб
Итого				360 749 руб.

На рисунке 24 представлен рекомендуемый план расположения средств защиты информации

Рисунок 24. Размещение видеодомофонов, видеокамер, установленных дверей

3.5. Выводы по 3 главе

В главе приводятся результаты анализа защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы, от утечки по каналу побочных электромагнитных излучений. Также представлены итоги оценки эффективности используемых мер и средств защиты информации.

Согласно проведенным оценкам, установлено, что уровень защиты информации от утечки по каналу побочных электромагнитных излучений (ПЭМИН) повышен. Для повышения эффективности системы защиты информации было использовано устройство Средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «Кедр-П» и установлено СЗИ «Kaspersky Endpoint Security Cloud», система видеонаблюдения.

ЗАКЛЮЧЕНИЕ

Выпускная квалификационная работа посвящена повышению уровня системы защиты в ООО «Кравт» от утечки по техническим каналам, посредством использования специализированных технических средств защиты. На основе проведённых исследований в рамках поставленной задачи были достигнуты следующие результаты.

В ходе работы был проведен анализ объекта информатизации, в итоге которого были определены и описаны потенциальные технические каналы утечки информации.

Для повышения эффективности системы защиты информации в ООО «Кравт», были выбраны технические средства защиты информации - Средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «Кедр-П», предназначенный для обеспечения защиты информации, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) и СЗИ «Kaspersky Endpoint Security Cloud».

Также были установлены видеокамеры по периметру офиса, введен в эксплуатацию видеодомофон на заднем входе офиса. Была произведены замены дверей на металлические, имеющие замок.

После принятых мер и внедрения средств защиты общий уровень информационной безопасности в итоге повышен.

Подводя итог проделанной работы, можно сделать следующие выводы о том, что задачи, поставленные в начале работы, были решены, а цель исследования достигнута.

Результаты исследования могут применяться в практической деятельности компаний, для обеспечения безопасного обращения с конфиденциальной информацией.

Список литературы:

1. Соколов, А. И. Технические средства защиты информации: технические каналы утечки информации : учеб. пособие / А. И. Соколов, М. Ю. Монахов ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2006. – 71 с. (Комплексная защита объектов информатизации. Кн. 13 / под ред. М. Ю. Монахова).

2. Приказ ФСТЭК России от 11 февраля 2013 г. «N17» - https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (Дата обращения 09.12.2024).

3. Приказ ФСТЭК России от 18 февраля 2013 г. «N21» // https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (Дата обращения 09.12.2024).

4. Банк угроз ФСТЭК России - // https://bdu.fstec.ru/threat (Дата обращения - 19.11.2024)

5. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения 20.10.2024).

6. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 20.10.2024).

7. Банк данных угроз безопасности информации Список терминов // https://bdu.fstec.ru/ubi/terms/terms/index (дата обращения: 24.10.2023)

8. ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения (с Поправкой) : официальное издание М.: Стандартинформ, 2009.

9. Банк данных угроз безопасности информации Список терминов // https://bdu.fstec.ru/ubi/terms/terms/index (дата обращения: 24.10.2023).

10. Бузов Г.А. Защита от утечки информации по техническим каналам / Бузов Г.А., Калинин С.В., Кондратьев А.В. – М.: Горячая линия - Телеком, 2002. – 415 с.

11. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования : официальное издание М.: Издательство стандартов, 1995.

12. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники. [Электронный ресурс]. – Режим доступа: http://www.bnti.ru/showart.asp?aid=954&lvl=04.03 (дата обращения 04.12.2023).

13. Хорев А.А. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера // Доклады ТУСУР. 2014. №2 (32). [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/otsenka-vozmozhnosti-obnaruzheniya-pobochnyh-elektromagnitnyh-izlucheniyvideosistemy-kompyuter (дата обращения 04.12.2023).