МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование кафедры)

09.03.03 Прикладная информатика
(код и наименование направления подготовки, специальности)

Бизнес-информатика
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему: Разработка комплекса мероприятий по обеспечению информационной безопасности

Обучающийся А.А. Четвертной _____
(Инициалы Фамилия) (личная подпись)

Руководитель доцент, О.В. Оськина _____
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Тема: «Разработка комплекса мероприятий по обеспечению информационной безопасности».

Объектом исследования является система обеспечения информационной безопасности ООО «Мир Квартир», а предметом исследования - процесс её организации.

Цель выпускной квалификационной работы заключается в том, чтобы разработать комплекс мероприятий, направленных на повышение уровня информационной безопасности и защиты информации в ООО «Мир квартир».

Для достижения данной цели необходимо выполнить следующие задачи:

– изучить деятельность агентства недвижимости ООО «Мир квартир»;

– изучить организационную структуру агентства недвижимости ООО «Мир квартир»;

– провести анализ обеспечения информационной безопасности информации агентства недвижимости;

– провести анализ состояния информационной безопасности информации агентства недвижимости;

– провести проектирование системы обеспечения информационной безопасности агентства недвижимости;

– описать технологию управления процессами информационной безопасности агентства недвижимости.

Работа состоит из введения, четырех разделов, заключения и списка используемых источников.

В первом разделе проводится анализ обеспечения информационной безопасности, а именно:

– рассматривается существующая система обеспечения безопасности информации на предприятии;

– определяются информационные ресурсы и активы, которые подлежат защите, возможные угрозы, уязвимости;

– формулируются методы, применяя которые можно достичь повышение информационной безопасности информационной инфраструктуры компании.

Во втором разделе обосновывается выбор средств защиты информации, методов защиты информации, предлагаются конкретные организационные и программные меры защиты информации.

В третьем разделе происходит проектирование системы обеспечения информационной безопасности в ООО «Мир квартир».

В четвертом разделе описана технология управления процессами информационной безопасности.

Работа включает в себя: страниц – 69 с приложениями, рисунков – 37, таблиц – 10, источников – 20.

Содержание

Введение

Темой настоящей бакалаврской работы является разработка комплекса мероприятий по обеспечению информационной безопасности.

Актуальность темы выпускной квалификационной работы обусловлена необходимостью разработки комплекса мероприятий по обеспечению информационной безопасности агентства недвижимости, так как на данный момент у агентства низкий уровень информационной безопасности.

Информационная безопасность является одной из ключевых областей в современном мире, особенно в условиях развития цифровых технологий и распространения Интернета. Каждая организация, в том числе и ООО «Мир квартир», должна обеспечивать надежную защиту своих информационных ресурсов и персональных данных клиентов.

Целью выпускной квалификационной работы является разработка комплекса мероприятий по обеспечению информационной безопасности агентства недвижимости.

Объектом исследования является система обеспечения информационной безопасности данной организации, а предметом исследования - процесс ее организации.

Для достижения данной цели необходимо выполнить следующие задачи:

– изучить деятельность агентства недвижимости ООО «Мир квартир»;

– изучить организационную структуру агентства недвижимости ООО «Мир квартир»;

– провести анализ обеспечения информационной безопасности информации агентства недвижимости;

– провести анализ состояния информационной безопасности информации агентства недвижимости;

– провести проектирование системы обеспечения информационной безопасности агентства недвижимости;

– описать технологию управления процессами информационной безопасности агентства недвижимости.

Практическая значимость разработки заключается в последующем внедрении комплекса мероприятий по обеспечению информационной безопасности в ООО «Мир квартир».

Работа состоит из введения, четырех разделов, заключения и списка используемых источников.

В первом разделе представлен анализ обеспечения информационной безопасности информации в компании. В нем обсуждается текущее состояние обеспечения информационной безопасности, выделяются основные информационные активы, требующие защиты, и идентифицируются угрозы и уязвимости. Кроме того, описываются методы, которые могут быть использованы для обеспечения повышенной информационной безопасности информационной инфраструктуры компании.

Во втором разделе обосновывается выбор средств защиты информации, методов защиты информации, предлагаются конкретные организационные и программные меры защиты информации.

В третьем разделе происходит проектирование системы обеспечения информационной безопасности в ООО «Мир квартир».

В четвертом разделе описана технология управления процессами безопасности информации.

Результатом выполнения бакалаврской работы является разработанный комплекс мероприятий по обеспечению информационной безопасности агентства недвижимости.

1 Анализ обеспечения информационной безопасности

1.1 Актуальность и значимость обеспечения информационной безопасности

В современный век информационных технологий для многих компаний информационная безопасность крайне важна, особенно если по их роду деятельности происходит интенсивная работа с клиентами и их персональными данными. Одними из таких компаний и являются агентства недвижимости.

Информационная безопасность определяется уровнем защиты данных, благодаря которому исключаются утечки информации, важной как для клиента, так и для компании.

Каждый клиент оставляет в агентстве недвижимости персональные (паспортные, и прочие личные) данные при совершении сделок. Они должны тщательно скрываться и быть защищенными до момента окончания сделки и даже после, так как существует срок давности, который обычно равен трем годам.

В процессе совершения любых операций с недвижимостью, как правило, в обороте находятся огромные суммы финансовых средств. Любая утечка данных клиентов может быть чревата денежными потерями, как для компании, так и для клиента. Во избежание подобных ситуаций, агентствам недвижимости следует обеспечивать довольно высокий уровень безопасности.

Обеспечение информационной безопасности клиентов – одна из основных задач агентства недвижимости. Только таким образом может обеспечиваться доверие к компании, и, следовательно, ее популярность у клиентов.

Рассмотрим, как можно классифицировать существующие угрозы информации. Схематично это представлено на рисунке 1 [1].

Рисунок 1 – Типы информационных угроз

Рассмотрим классификацию угроз по факторам их возникновения (рисунок 2):

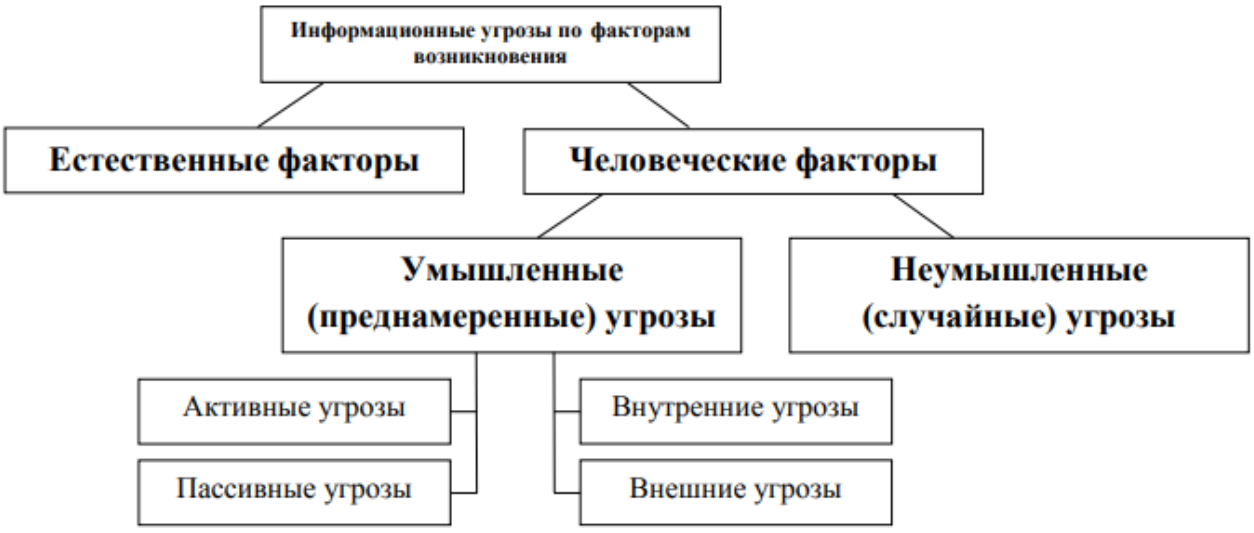


Рисунок 2 – Информационные угрозы по факторам возникновения

Естественные (природные) факторы – можно выделить стихийные бедствия, такие как пожары, наводнения, ураганы, молнии и другие причины.

Человеческие факторы, в свою очередь, подразделяются на

умышленные и неумышленные угрозы.

Неумышленные угрозы случайны по характеру.

Угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением информации. или связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы. Целью таких угроз является нанесение ущерба пользователям АИС. Умышленные угрозы можно разделить на активные и пассивные [1].

Для достижения своих целей, активные угрозы нарушают нормальный процесс функционирования системы. Это происходит через целенаправленное воздействие на аппаратные, программные и информационные ресурсы. К числу активных угроз относится, например, радиоэлектронное подавление линий связи, разрушение, вывод из строя ПЭВМ или ее операционной системы, искажение сведений в базах данных или системной информации и многое другое. Источниками активных угроз могут быть злоумышленники, программные вирусы и другие [2].

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Например, прослушивание каналов связи является формой пассивной угрозы.

Умышленные угрозы подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.

Внутренние угрозы, которые возникают внутри управляемой организации, чаще всего связаны с социальной напряженностью и неблагоприятным моральным климатом.

Внешние угрозы, с другой стороны, могут иметь различные причины, такие как злонамеренные действия конкурентов, экономические условия и даже стихийные бедствия.

Промышленный шпионаж широко распространен, по данным зарубежных источников. Он наносит ущерб владельцу коммерческой тайны

путем незаконного сбора, присвоения и передачи сведений, которые составляют коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

Основными угрозами безопасности информации, как правило, являются: раскрытие конфиденциальной информации, компрометация информации, несанкционированное использование информационных ресурсов, ошибочное использование ресурсов и несанкционированный обмен информацией [1].

1.2 Анализ применения современных методов и средств по защите информации

В качестве средства защиты информации от коммерческого шпионажа рассмотрим систему защиты информации (СЗИ). Она представляет из себя меры, которые необходимы для поддержания заданного уровня эффективности защиты информации в организации.

СЗИ решает задачи обеспечения условий для стабильного развития организации, а также эффективное обнаружение угроз утечки информации и их предотвращение.

С помощью СЗИ в организации обеспечивается: комплексная защита интересов организации, информационная безопасность сотрудников организации, защита ресурсов организации (материально-технических и финансовых), а также разграничиваются права доступа к ресурсам организации (информационным и техническим).

Рассмотрим этапы создания СЗИ:

– Методологический этап подразумевает создание методологической документации. В ней находится информация о правилах разработки СЗИ и ее поддержки.

– Организационный этап подразумевает обучение сотрудников, их инструктаж, а также создание локальной организационно-распорядительной документации.

– Технический этап – это подбор и установка в организации

программных и технических средств защиты информации.

Техническую безопасность организовывают таким образом, чтобы подавить наведенные информационные сигналы или снизить показатели сигнала или шума до приемлемых величин. Мероприятия (технические) классифицируют на активные и пассивные (рисунок 3).

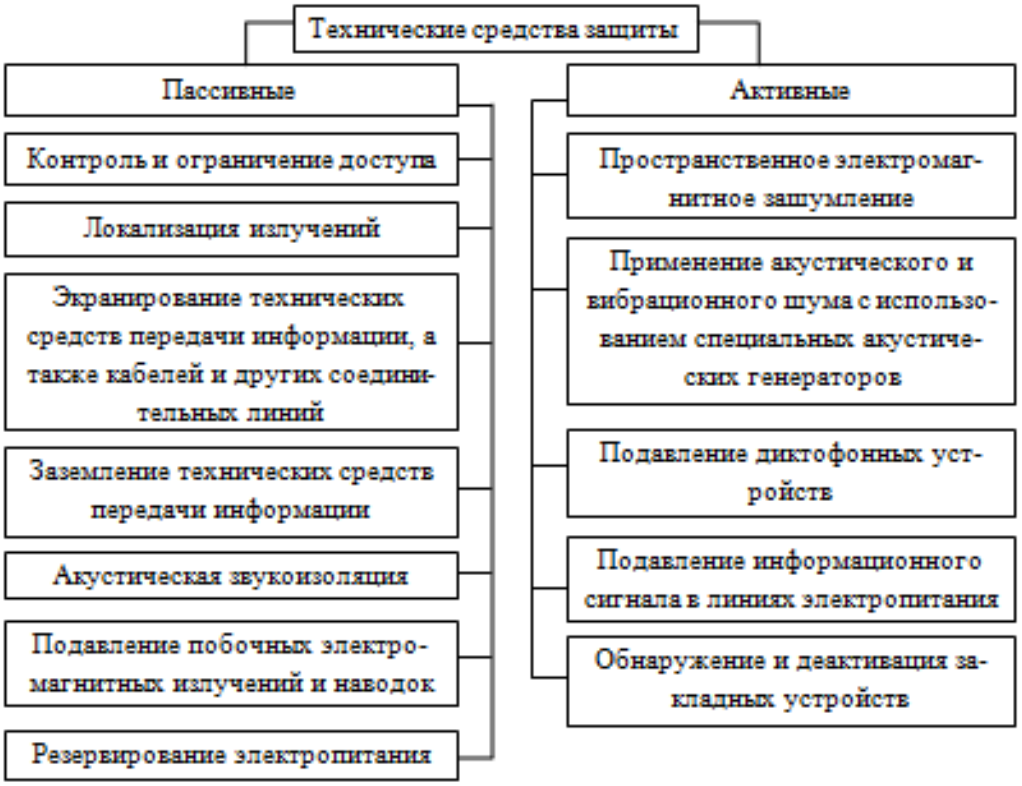


Рисунок 3 – Классификация технических средств защиты информации

Закладные устройства, которые предназначены для перехвата информации, можно найти и деактивировать с помощью оборудования. Поиск осуществляется:

– Закладки можно обнаружить с помощью использования пассивного оборудования;

– Для предотвращения утечки информации можно использовать в служебных помещениях обнаружители диктофонов;

– Закладки можно обнаружить с помощью использования активного оборудования;

– Найти аппаратные закладки можно с помощью индикаторов поля и программно – аппаратных комплексов контроля;

– Поиск закладок с помощью нелинейных локаторов.

1.3 Порядок создания системы обеспечения информационной безопасности в коммерческой организации

Необходимо разработать и зафиксировать в специальном организационном документе – «Руководство по обеспечению информационной безопасности» следующие положения.

– положение о защищаемой информации, ее описание и обоснование;

– положение о порядке создания и ввода в эксплуатацию, а также использования информационных ресурсов;

– положение о перечне конфиденциальной информации в организации, порядке доступа к ней.

2 Анализ состояния информационной безопасности в ООО «Мир Квартир»

2.1 Анализ деятельности агентства недвижимости ООО «Мир Квартир»

ООО «Мир Квартир» представляет собой коммерческую организацию, ее основной вид деятельности – Деятельность агентств недвижимости за вознаграждение или на договорной основе (ОКВЭД 68.31). Руководитель компании – Лищинский Сергей Александрович [9].

ООО «Мир Квартир» появилась на рынке недвижимости с 2017 года. В течение 8 лет занимается профессиональным оформлением и сопровождением всех законных операций с недвижимостью. Агентство напрямую сотрудничают с застройщиками. Это значит, что у компании самые выгодные предложения по новостройкам и строящемуся жилью.

В компанию обращаются люди, которые всерьез намерены решить свой жилищный вопрос. Ежедневно сотрудники компании совершают сделки по обмену старого жилья на новое, квартир на дома, а также помогают с нуля приобретать недвижимость.

Агентство недвижимости ООО «Мир Квартир» надежное, успешное и современное агентство недвижимости. Компания улучшает свой сервис, получая обратную связь от клиентов и партнеров.

Миссия компании - это выгодные сделки с недвижимостью для своих клиентов. Каждый день компания работает для того, чтобы клиенты переезжали в новое жилье и улучшали свою жизнь.

Под недвижимостью понимается вид имущества, признаваемого в законодательном порядке недвижимым. К нему относятся квартиры, комнаты, коттеджи, дачи, таунхаусы, земельные участки, коммерческая недвижимость.

Компания предоставляет следующие услуги своим клиентам:

– покупка недвижимости (за наличные, в ипотеку, с использованием мат. капитала;

– продажа недвижимости (оценка недвижимости, продажа с условиями и без них);

– аренда недвижимости на длительный срок, либо посуточно;

– обмен недвижимости (с доплатой, без доплаты, с ипотекой).

Выбирая компанию ООО «Мир Квартир», клиенты получают:

– бесплатные консультации;

– оперативность в принятии грамотных решений в интересах клиентов;

– проверенные партнеры в банковской и рекламной сферах;

– юридическая подкованность во всех вопросах недвижимости;

– проверенный временем коллектив, где каждый сотрудник – настоящий профессионал.

Основными направлениями совершенствования деятельности компании ООО «Мир Квартир» являются:

– дальнейшее развитие и совершенствование бизнес-процессов;

– увеличение продаж компании;

– расширение спектра оказываемых услуг;

– улучшение качества работы с клиентами.

Технико-экономические показатели ООО «Мир квартир»
2022г

За 2022 год ООО «Мир квартир» получила чистую прибыль на 23,83% меньше показателя за аналогичный период прошлого года. Продажи компании составили 18,45 млн. руб., то есть выросли в 3,89 раза. Прибыль от продаж составила 1,24 млн. руб. Она снизилась с 1,63 млн. руб. годом ранее.

2021г

ООО «Мир квартир» завершило 2021 год с чистой прибылью по РСБУ в 1,63 млн. руб. по сравнению с убытком 8,93 млн. руб. годом ранее. Объем продаж компании за отчетный период снизился на 3,44% до 4,74 млн. руб. с 4,91 млн. руб. за аналогичный период прошлого года. Прибыль от продаж

ООО «Мир квартир» за 2021 год достигла 1,63 млн. руб. по сравнению с убытком в 8,79 млн. руб. годом ранее.

Рассмотрим основные финансовые показатели ООО «Мир квартир» за 2021-2022 года.

Таблица 1– Основные финансовые показатели ООО «Мир квартир»

	2021	2022
Выручка (тыс. руб.)	4712	18447
Чистая прибыль (тыс. руб.)	1628	1240

Теперь рассмотрим выручку и прибыль фирмы за 2021-2022 года (рисунок 4).

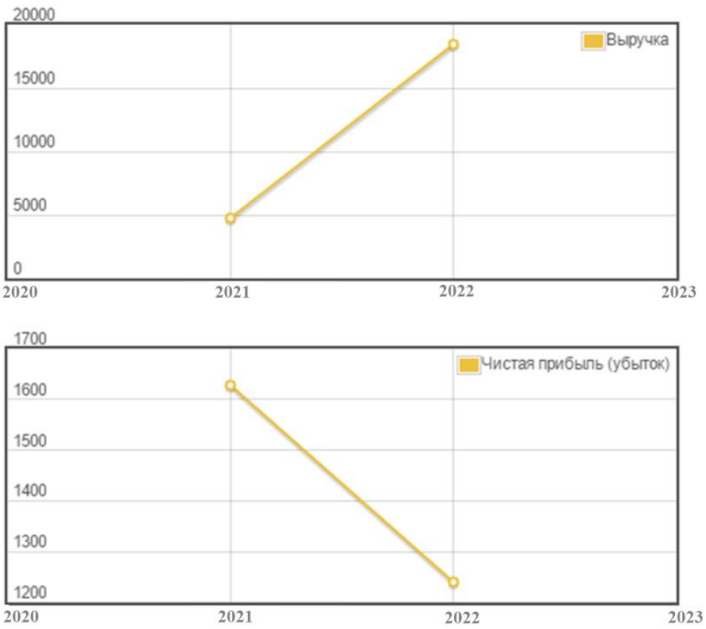


Рисунок 4 – Выручка и прибыль ООО «Мир квартир»

Характеристика используемых ресурсов:

Для успешного функционирования любая организация должна обладать всеми необходимыми для нее ресурсами. Рассмотрим ресурсы, которыми располагает ООО «Мир квартир».

В наличии имеется достаточное количество современного IT-оборудования, такого как настольные компьютеры, МФУ, принтеры, сканеры, факсы и др.

Рассмотрим организационную структуру ООО «Мир Квартир», представленную на рисунке 5.

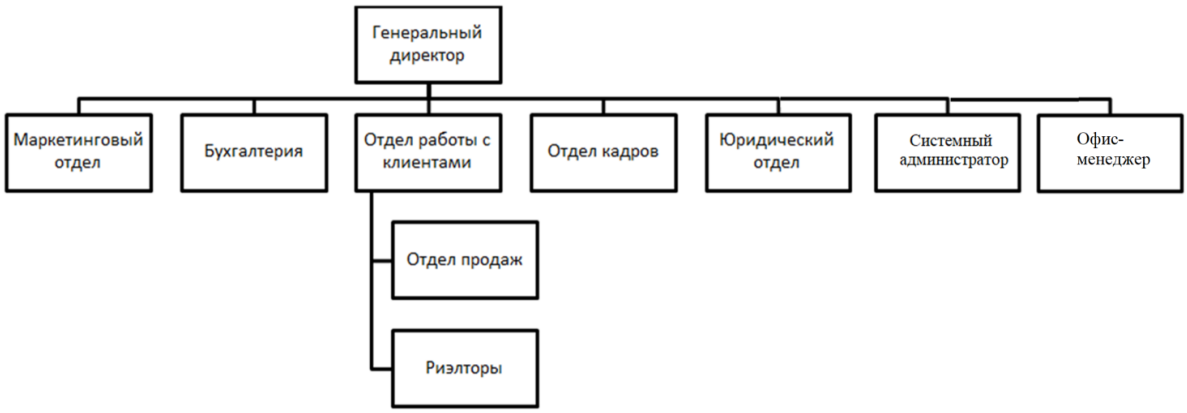


Рисунок 5 — Организационная структура ООО «Мир Квартир»

Руководство компанией осуществляется единолично генеральным директором, который находится во главе организационной структуры.

Он осуществляет руководство организацией и определяет направления его развития. Также он занимается оптимизацией бизнес-процессов организации.

В подчинении у генерального директора компании находятся следующие подразделения:

– маркетинговый отдел;

– бухгалтерия;

– отдел работы с клиентами;

– отдел кадров;

– юридический отдел

– системный администратор.

Менеджеры по продажам занимаются поиском новых клиентов и поддерживают обратную связь с постоянными клиентами. Крое того они

предлагают постоянным клиентам выгодные условия. Менеджеры по продажам ведут отчетность по работе с текущими клиентами, консультируют клиентов по объектам недвижимости и предоставлению услуг компании.

Менеджеры осуществляют приемом заявок от клиентов компании и передают в работу риелторам компании. Способы приема заявок на операции с недвижимостью: личное обращение в офис ООО «Альтера», по телефону, по электронной почте.

Риелтор компании проводит консультации, заключает договора, ведет базы, сопровождает сделки с недвижимостью.

Отдел бухгалтерии осуществляет платежи в наличной и безналичной форме в порядке, определяемом внутренними документами предприятия. Взаимодействие с контрагентами и финансовыми организациями в пределах своей компетенции;

Системный администратор обеспечивает поддержку правильной работы компьютерной техники и программного обеспечения, а также исполняет функции по обеспечению информационной безопасности организации;

Отдел кадров осуществляет следующие функции: кадровое делопроизводство, поиск подбора и адаптации персонала;

Юрист предоставляет полное юридическое сопровождение сделок, предоставляет интересы компании в суде.

Офис-менеджер контролирует рабочее состояние офисной техники, снабжает офис канцтоварами и другими расходными материалами, а также выполняет те или иные секретарские обязанности, такие как регистрация корреспонденции, распределение документации по отделам, ведение учета звонков и обращений, встреча посетителей и организация совещаний.

2.2 Определение информационных потоков в организации

Основным направлением деятельности агентства недвижимости является оказание услуг по операциям с недвижимостью.

Для качественного выполнения взятых на себя обязательств агентство

недвижимости обрабатывает, получает и хранит большой массив различных данных.

В связи с вышесказанным, организации требуется создать надежную систему обеспечения безопасности, включающую в себя:

– Средства программной и технической защиты;

– Организационные меры защиты информации.

В процессе анализа повседневной деятельности компании были определены информационные потоки, которые несут в себе конфиденциальную информацию (информацию ограниченного доступа). Полученные данные, по составу информации, приведены в таблице 2.

Под информационным потоком следует понимать непосредственно саму информацию, в процессе ее движения в пространстве и времени в определенном направлении [4].

Таблица 2 – Состав конфиденциальной информации

№ элемента информации	Перечень конфиденциальных данных
Сведения в области персональных данных	
1	Персональные данные сотрудников и клиентов агентства недвижимости (ст. 3, п. 1 Федерального Закона № 152-ФЗ «О персональных данных».
Сведения в области профессиональной тайны	
2	Информация о клиентах, квартирах, банковских операциях, номерах счетов.
3	Данные из сообщений, полученных/отправленных с использованием почтовых сервисов. Информация, доверенная телефонной аппаратуре, включая данные о пользователях, входящих и исходящих звонках и соединениях.
4	Информация об операциях с недвижимостью.
Сведения в области бухгалтерского учёта	
5	Содержание внутренней бухгалтерской отчетности.

Продолжение Таблицы 2

Сведения, составляющие коммерческую тайну	
6	Сведения, содержащие клиентскую базу о покупателях и продавцах квартир.
7	Условия по заключенным сделкам, условия договоров и соглашений
8	Сведения о расчетах тарифов, структуре и расчете цены, о продажной калькуляции, затратах.
9	Сведения, содержащие описание структуры локально-вычислительной сети и полномочий пользователей, обрабатывающих конфиденциальную информацию.
10	Сведения об организации и технических решениях по системе охраны помещений (система контроля и управления доступом).

Проведем анализ информационных связей между отделами ООО «Мир квартир», схематично отображенный на рисунке 6.

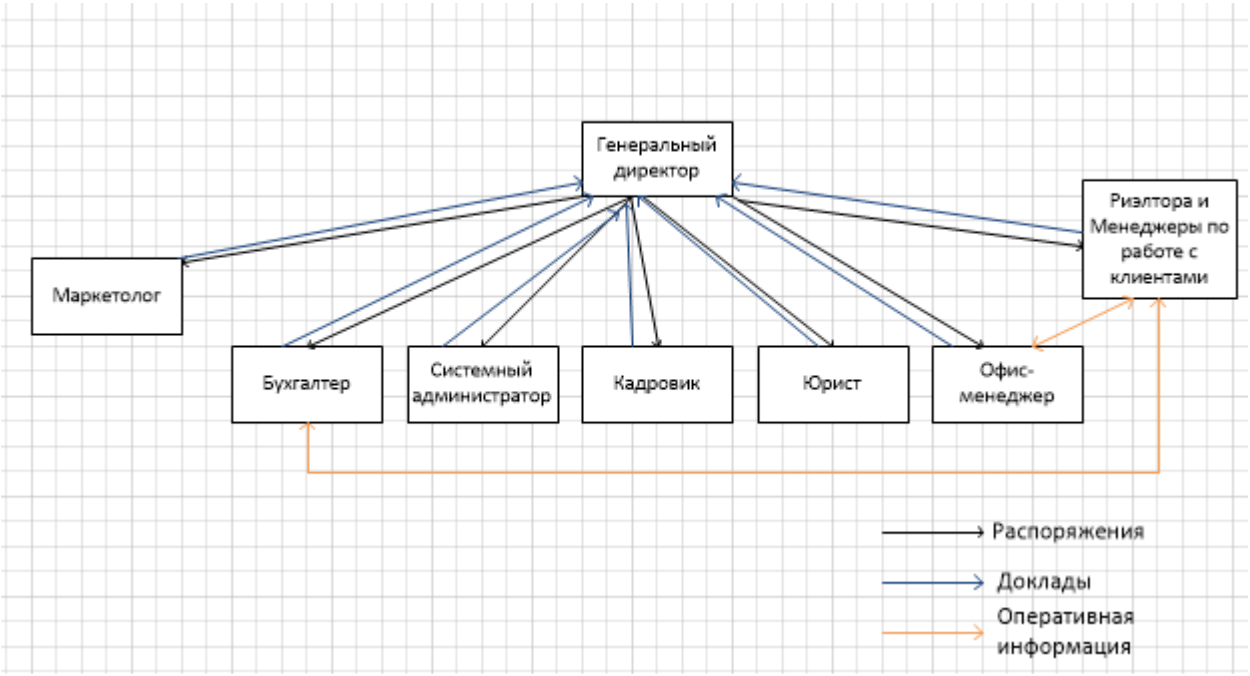


Рисунок 6 – Информационные связи между подразделениями ООО «Мир квартир»

По рисунку 6 видно, что в агентстве недвижимости активно перемещаются информационные потоки, такие как распоряжения, разного рода оперативная информация и доклады, предоставляемые сотрудниками

руководству, либо руководителям отделов и подразделений. Такая информация передается, в основном, посредством электронной почты, либо через папку общего доступа, находящуюся на сервере, либо в бумажном виде. Таким образом, в сети одновременно находится большое количество пользователей, передающих друг другу ценную информацию, а также те, кто использует сетевые принтеры, МФУ и т.д

В организации многие информационные потоки содержат конфиденциальную информацию. Также они содержат информацию, которую не рекомендуется разглашать по регламенту.

2.3 Анализ состояния защищенности ООО «Мир Квартир»

Рассмотрим схему ЛВС ООО «Мир квартир».

В ООО «Мир квартир» используются такие современные технические средства реализации информационных технологий, как персональные компьютеры, сервер, принтеры, сканеры, факсы, беспроводная сеть Wi-Fi, телефонная техника- телефон, факс, система видеонаблюдения и др. Таким образом, в агентстве недвижимости уровень использования информационных технологий является достаточно высоким. Отличительной особенностью является наличие беспроводной сети, в которой на одну точку доступа приходится 17 персональных компьютеров, 1 сервер и 2 многофункциональных устройства.

На рисунках 7 и 8 показана сеть агентства недвижимости, которая функционирует в данный момент. Как мы видим, все персональные компьютеры соединяются с сервером через беспроводную сеть Wi-Fi с помощью роутера. Они имеют возможность использовать многофункциональные устройства аналогичным образом, через Wi-fi. К большинству рабочих станций с помощью проводного соединения подключены различные периферийные устройства: принтеры, сканеры, факсы и др.

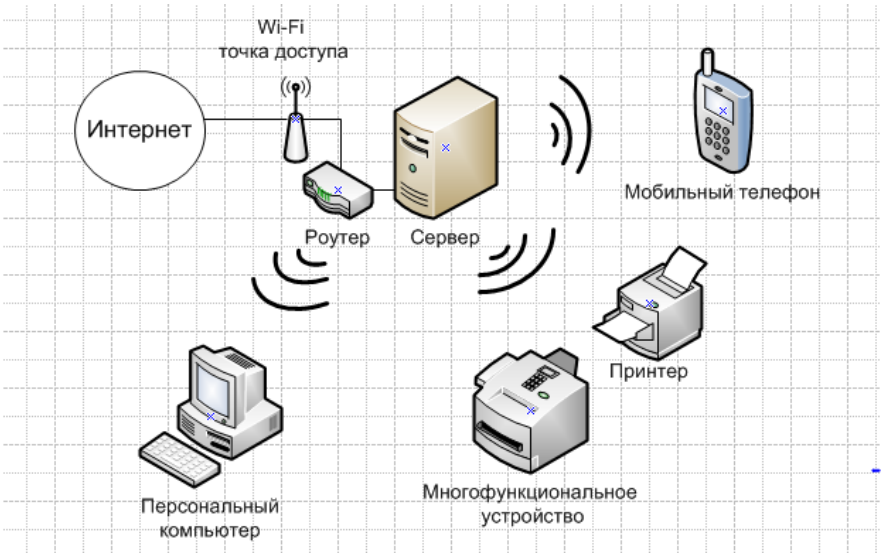


Рисунок 7 – Краткая схема локальной вычислительной сети ООО «Мир квартир»

На рисунке 8 показана схема помещения агентства недвижимости с расположением всех отделов. Так же на ней обозначено сетевое оборудование: сервер, рабочие станции, и периферийные устройства.

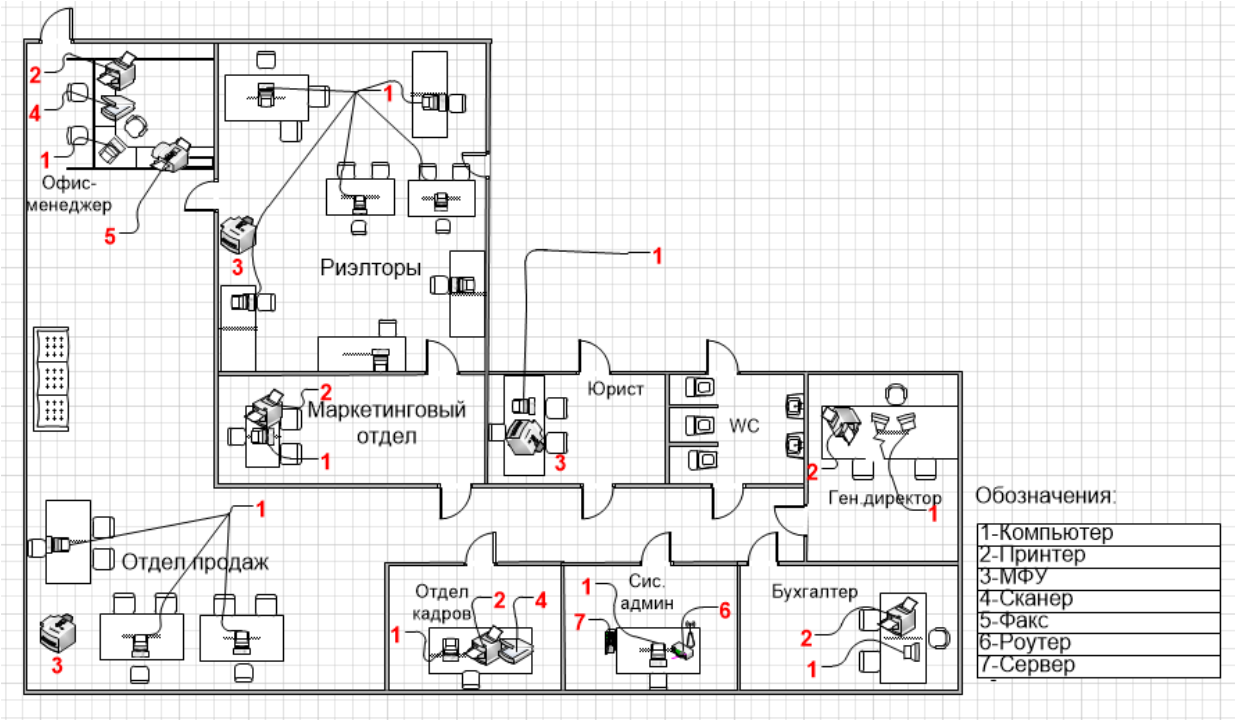


Рисунок 8 – Полная схема локальной вычислительной сети ООО «Мир квартир»

Объектом исследования является деятельность системного администратора, в должностные обязанности которого входит организация и поддержание информационной безопасности агентства недвижимости.

Рассмотрим организацию информационной безопасности агентства недвижимости ООО «Мир квартир». На данный момент в агентстве практически нет разработанной информационной безопасности. Информация плохо защищена от различных видов угроз, есть большой риск утечки информации через разные каналы (физический, технический, информационный). Также офис находится на 1 этаже 10-ти этажного здания, что не очень хорошо для информационной безопасности организации.

В организации для переговоров и совещаний есть выделенное помещение – это кабинет, где работают все риэлтора. Большое помещение около 80 м кв. В нем есть окна, двери, система вентиляции, система отопления, одна стена граничит с офисом другой компании, и другая стена граничит с

улицей. Все эти условия несут угрозу утечки информации через акустический канал утечки. Недостаточно эффективно и безопасно организована сеть ЛВС.

Компания «Мир квартир» столкнулась с такой проблемой, как отсутствие правильно организованной локально-вычислительной сети (ЛВС), а именно:

– Невозможность быстро обмениваться важными документами между отделами компании из-за низкой пропускной способности (скорости передачи данных) Wi-Fi соединения, т.к. одновременно в интернет выходят более 3 сотрудников агентства недвижимости;

– Беспроводное Wi-Fi соединение – это дополнительный риск несанкционированного доступа, так как в беспроводную сеть проникнуть проще, чем в проводную.

– Неудобное администрирование компьютеров. При низкой скорости передачи данных в сети, системный администратор обслуживает каждый из компьютеров отдельно, осуществляя установку/удаление программ, резервное копирование важных данных непосредственно на каждом рабочем месте в агентстве недвижимости;

– Неэкономное использование ресурсов в информационной системе. Имеется большое количество периферийных устройств, для того, чтобы сотрудники не занимали и без того нагруженную сеть;

– Невозможность использования программ, установленные на других компьютерах, опять же из-за низкой скорости передачи данный по Wi-Fi;

– Затруднение доведения задач по подразделениям, контроля их исполнения;

– Низкая оперативность получения данных о деятельности подразделений.

Также в компании ООО «Мир квартир» нет четко сформулированной политики информационной безопасности. И, соответственно, нет специализированных средств защиты информации (СЗИ), которые помогают

автоматизировать защиту информации и связанные с этим процессы. Это давно сформированный рынок решений, для самых разных клиентов и задач.

Проведем анализ существующего процесса организации информационной безопасности ООО «Мир квартир», в процессе которого целесообразно разработать функциональные диаграммы по методологии SADT (IDEF0) с использованием CASE средств.

На рисунке 9 представлена функциональная модель существующего процесса «Организовать информационную безопасность ООО «Мир квартир» нулевого уровня.

На входе расположены следующие информационные потоки:

– Входная информация;

– Физические угрозы безопасности;

– Технические угрозы безопасности;

– Программные и сетевые угрозы безопасности.

Выходными потоками являются:

– Слабозащищенная информация;

– Отчет о событиях.

Деятельность сотрудников ООО «Мир квартир» регламентируется должностными инструкциями сотрудников, регламентом компании.

Проведем декомпозицию модели А-0. Результат декомпозиции представлен на рисунке 10.

В результате выделены следующие функциональные блоки:

– Ликвидировать угрозу, поступившую через физический канал утечки информации;

– Ликвидировать угрозу, поступившую через технический канал утечки информации;

– Ликвидировать угрозу, поступившую через информационный канал утечки информации;

– Сформировать отчетность.

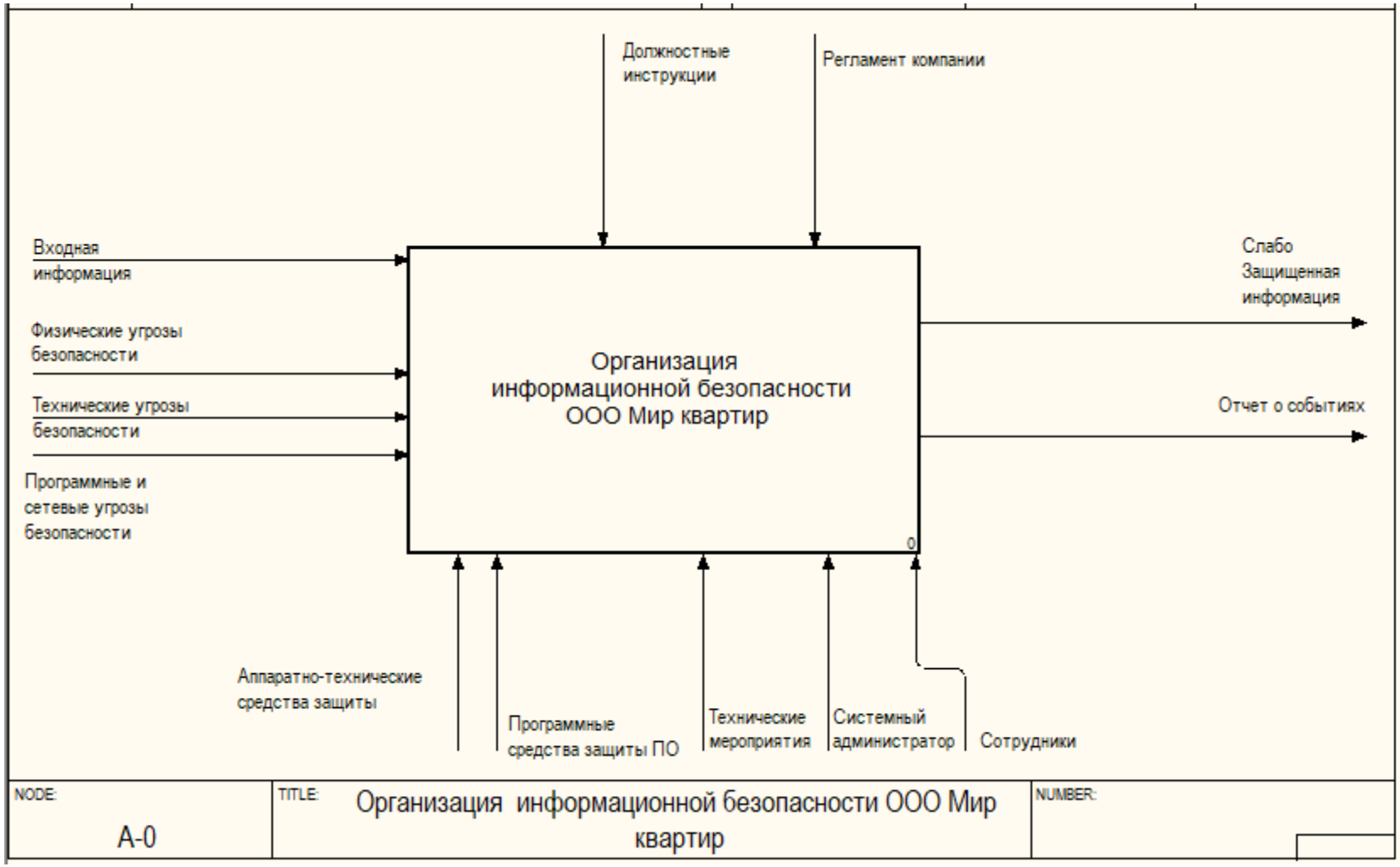


Рисунок 9 – Контекстная диаграмма AS-IS

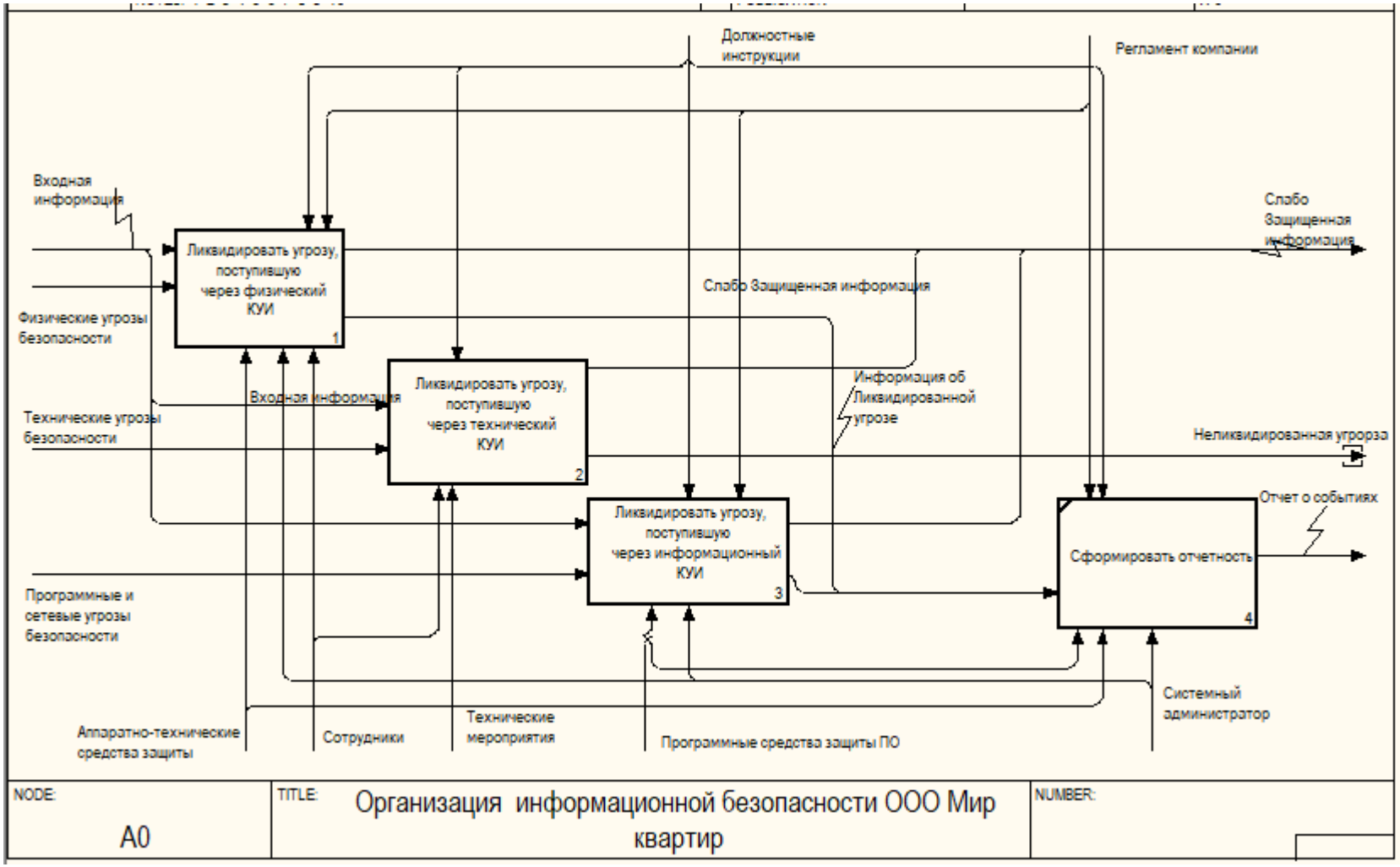


Рисунок 10 – Декомпозиция IDEF0-модели AS-IS

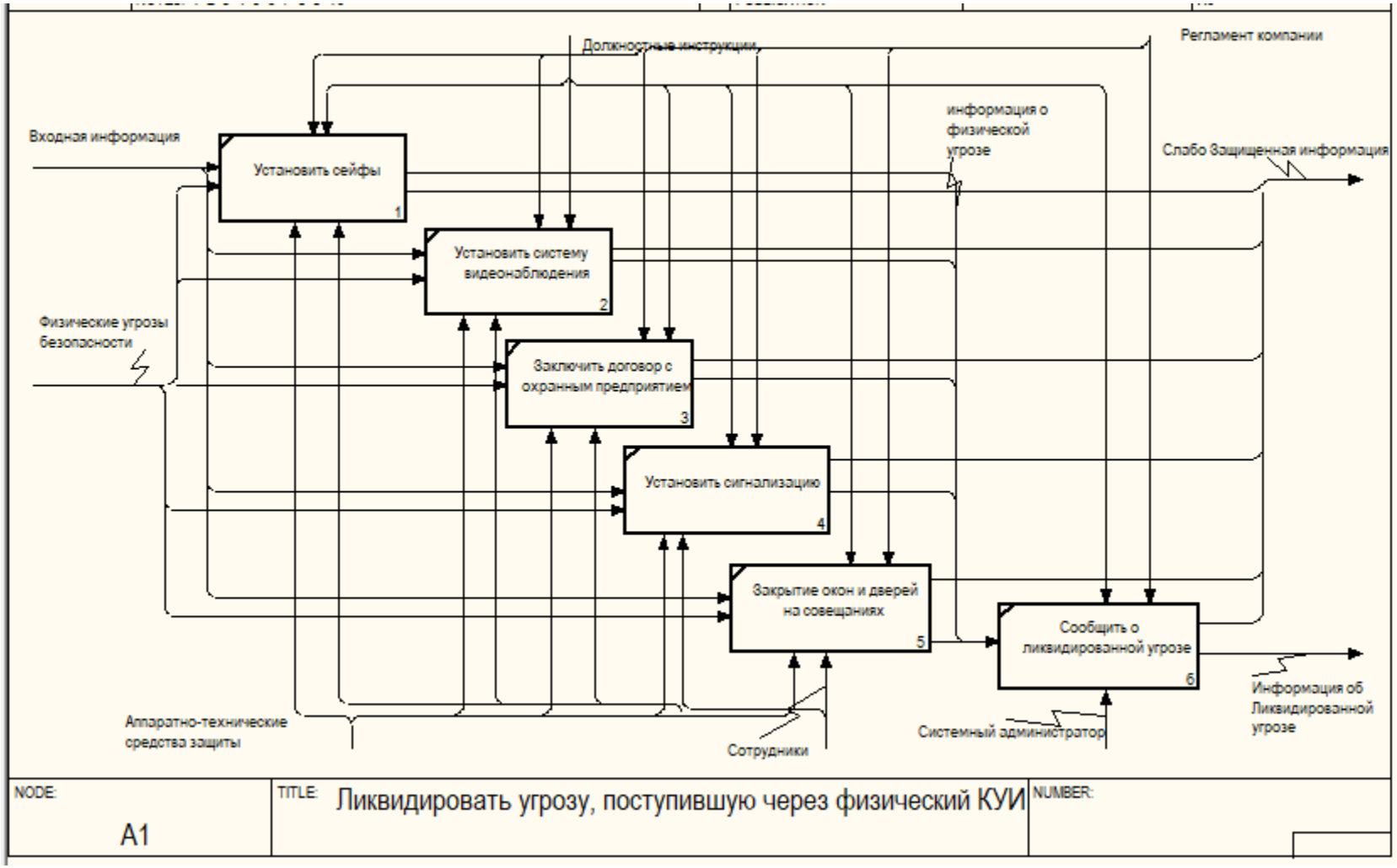


Рисунок 11 – Декомпозиция процесса «Ликвидировать угрозу, поступившую через физический КУИ»

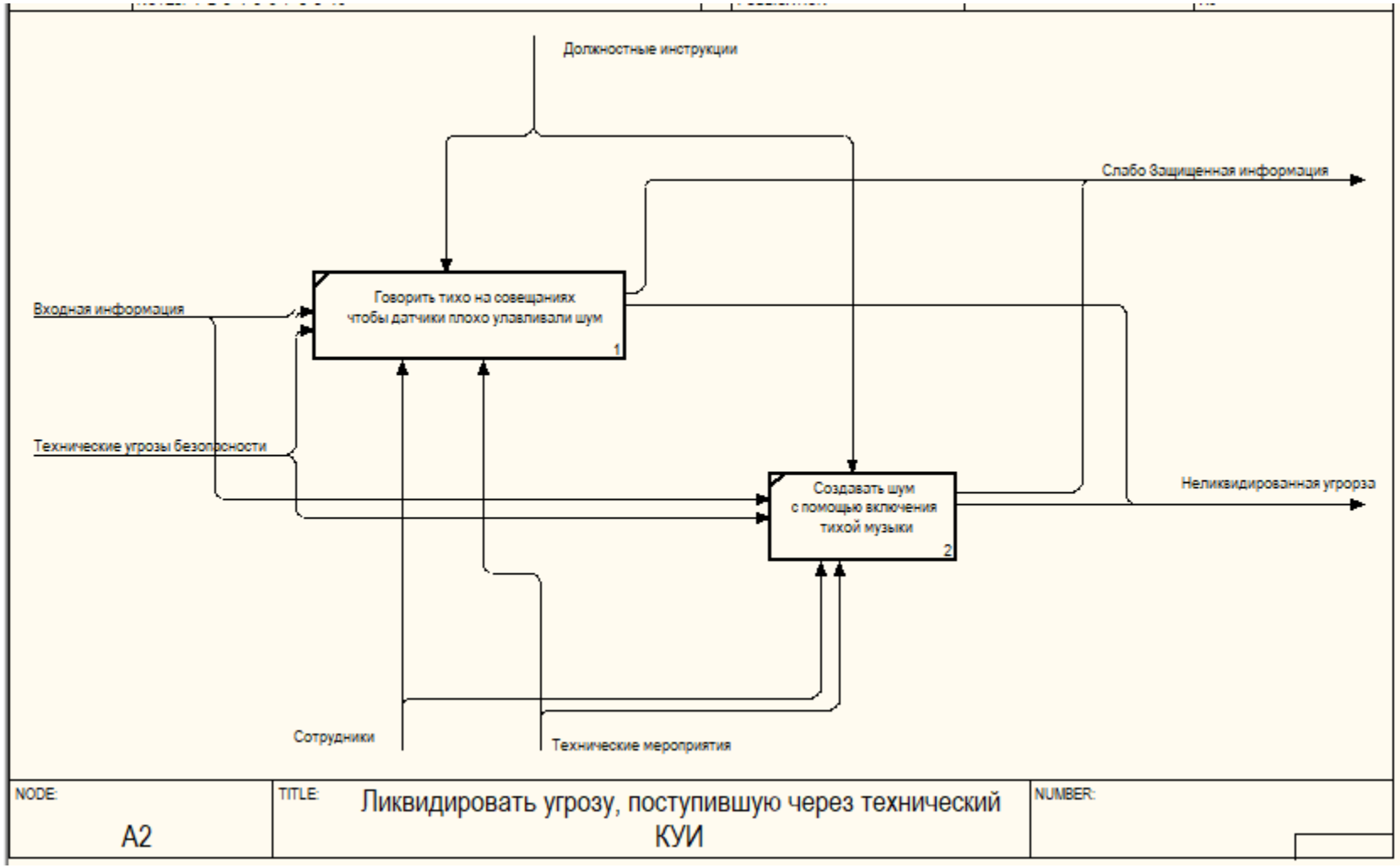


Рисунок 12 – Декомпозиция процесса «Ликвидировать угрозу, поступившую через технический КУИ»

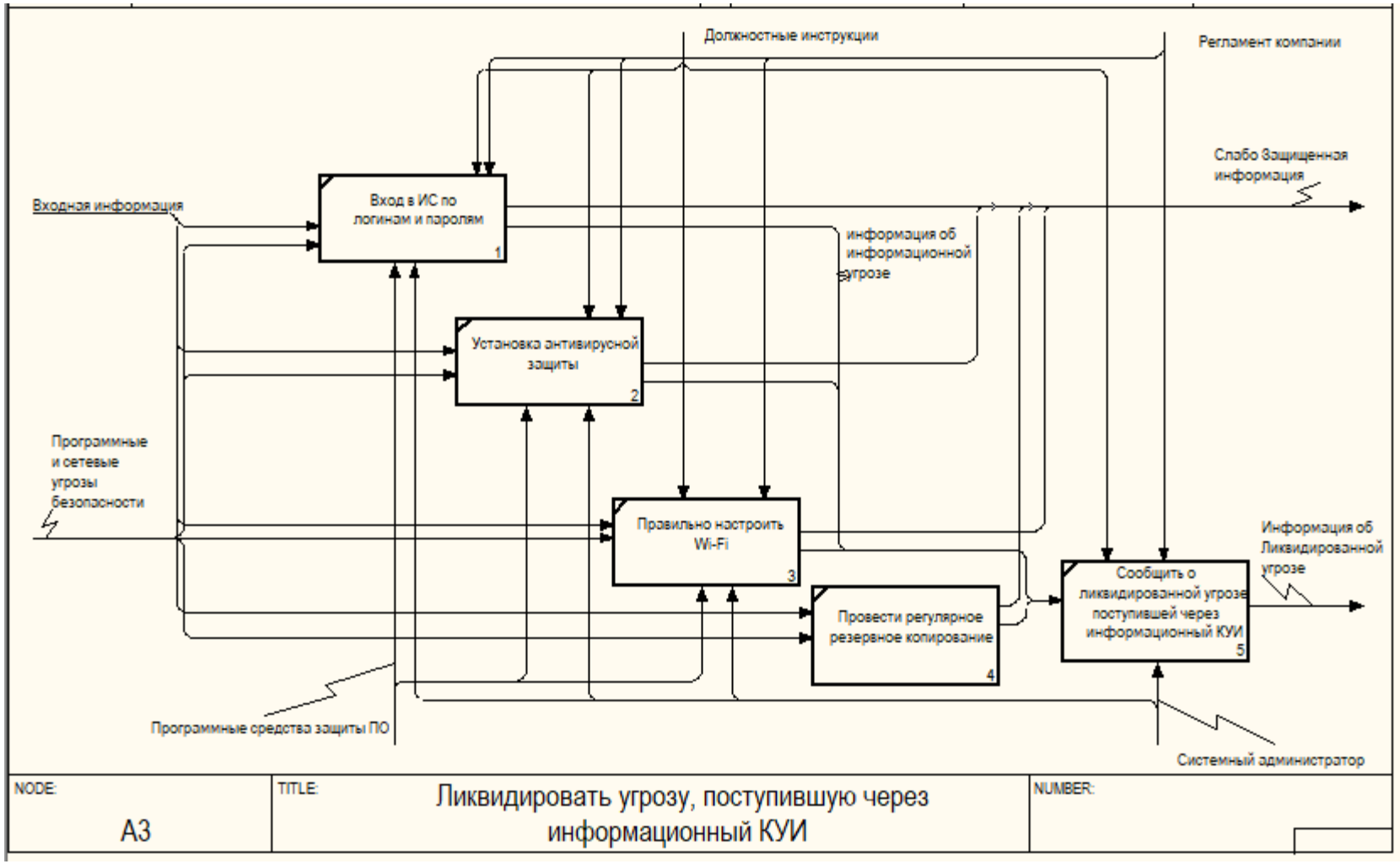


Рисунок 13 – Декомпозиция процесса «Ликвидировать угрозу, поступившую через информационный КУИ»

2.4 Оценка эффективности существующей системы безопасности информации в ООО «Мир Квартир»

Основные направления совершенствования процесса организации информационной безопасности агентства недвижимости представлены в таблице 3.

Таблица 3 – Основные направления совершенствования процесса организации информационной безопасности агентства недвижимости

Функциональные задачи	Существующее решение	Недостатки существующего решения
Ликвидировать угрозу, поступившую через физический КУИ	Установить сейфы Заключить договор с охранным предприятием Установить сигнализацию Закрытие окон и дверей на совещаниях Аппаратно-технические средства защиты	Нет системы видеонаблюдения, нет жалюзи на окнах, нет дверей специальных, с повышенной шумоизоляцией Есть высокий риск попадания информации в руки злоумышленников.
Ликвидировать угрозу, поступившую через технический КУИ	Говорить тихо на совещаниях чтобы датчики плохо улавливали шум Создавать шум с помощью включения тихой музыки и других средств	нет жалюзи на окнах, нет виброакустических датчиков; Нет звукоизоляции, Нет правильно организованной защиты выделенного помещения; Есть высокий риск попадания информации в руки злоумышленников.

Продолжение Таблицы 3

Ликвидировать угрозу, поступившую через информационный КУИ	Программные средства защиты информации Вход в ИС по логинам и паролям Установка антивирусной Защиты Правильно настроить Wi-Fi Провести регулярное резервное копирование	Нет СЗИ, Нет правильно организованной ЛВС, Есть высокий риск попадания информации в руки злоумышленников.
Сформировать отчетность	Аппаратно-технические средства защиты, Программные средства защиты информации	Для построения отчетов применяется файл MS Excel, нет автоматизированного формирования отчетности

В ходе анализа было принято решение разработать комплекс мероприятий по обеспечению информационной безопасности агентства недвижимости для устранения проблем, описанных в таблице 2.

3 Проектирование системы обеспечения информационной безопасности в ООО «Мир Квартир»

3.1 Обоснование методов и средств обеспечения информационной безопасности

С помощью методологии функционального моделирования IDEF0 проанализируем функции системы организации информационной безопасности агентства недвижимости, учитывая внедрение комплекса мероприятий по обеспечению ИБ.

Для этого построим контекстную диаграмму, представленную на рисунке 14. Диаграмма «как будет» построена на основе устраненных недостатков, с применением комплекса мероприятий по обеспечению ИБ.

На рисунке 15 представлена декомпозиция функционального блока «Организация информационной безопасности ООО Мир квартир», из которого видно, что разработанный комплекс мероприятий будет использоваться на всех этапах.

При разработке комплекса мероприятий по обеспечению ИБ необходимо учесть все выявленные проблемы и ликвидировать их.

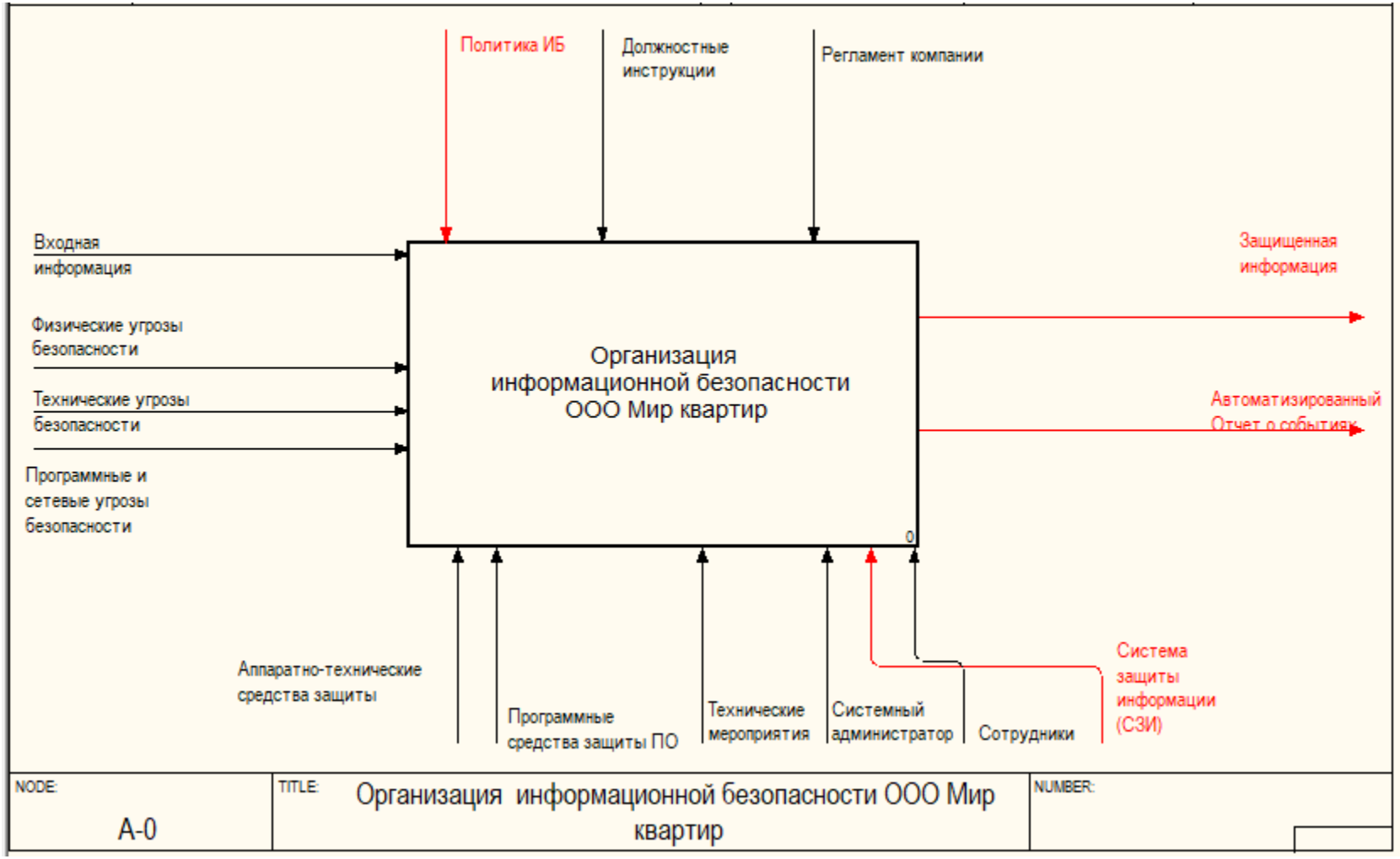


Рисунок 14 – Контекстная диаграмма TO-BE

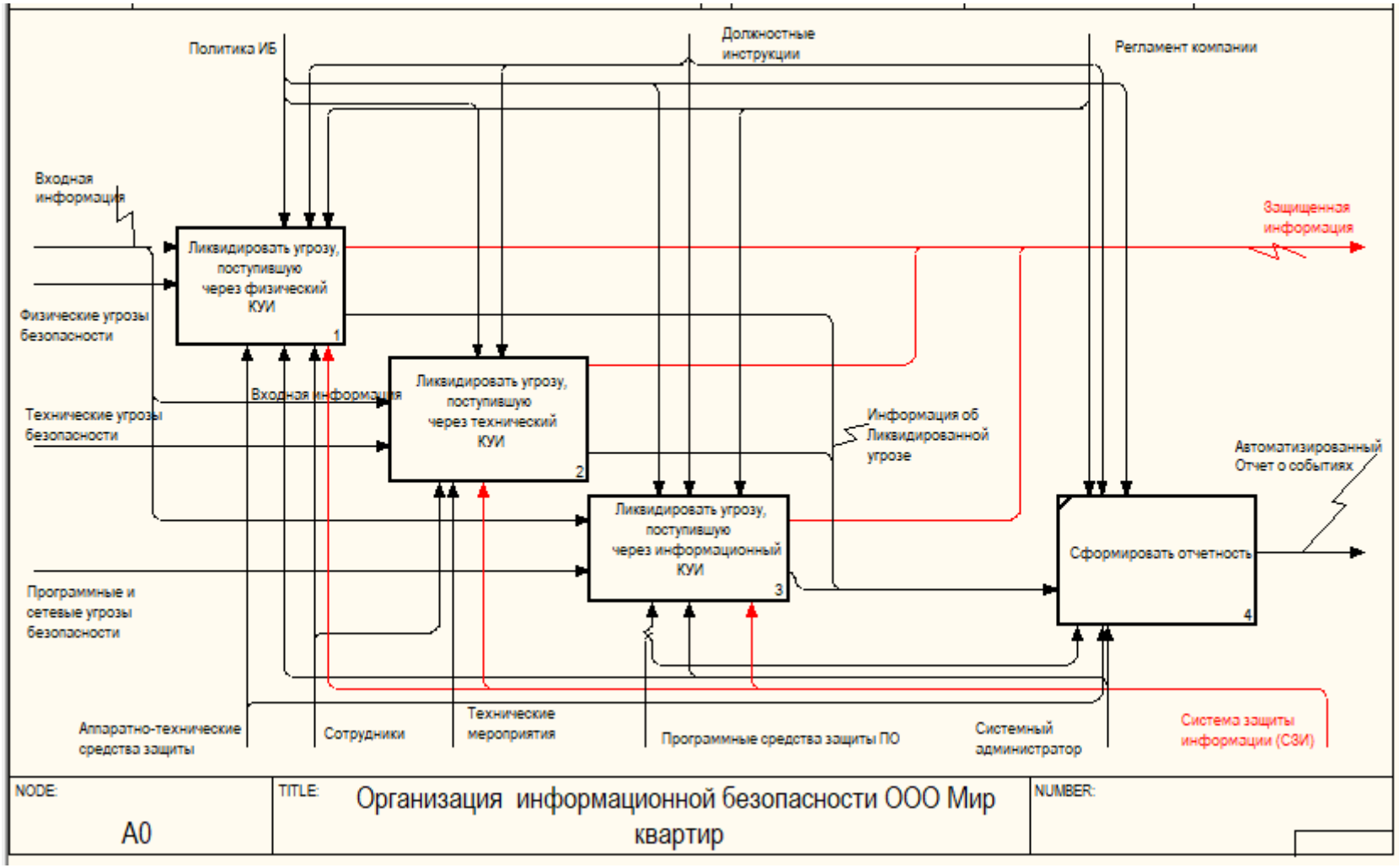


Рисунок 15 – Декомпозиция IDEF0-модели TO-BE

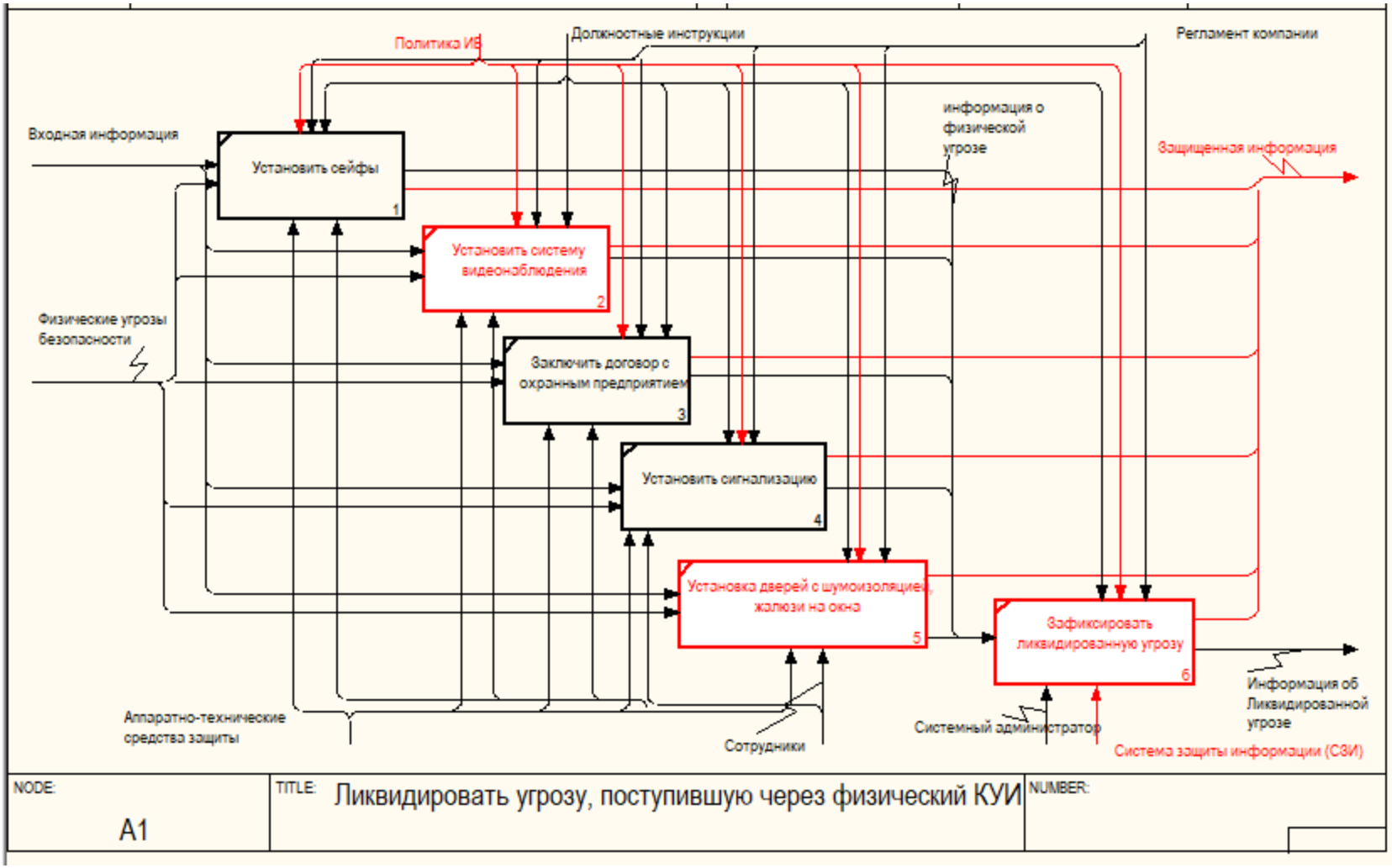


Рисунок 16 – Декомпозиция процесса «Ликвидировать угрозу, поступившую через физический КУИ»

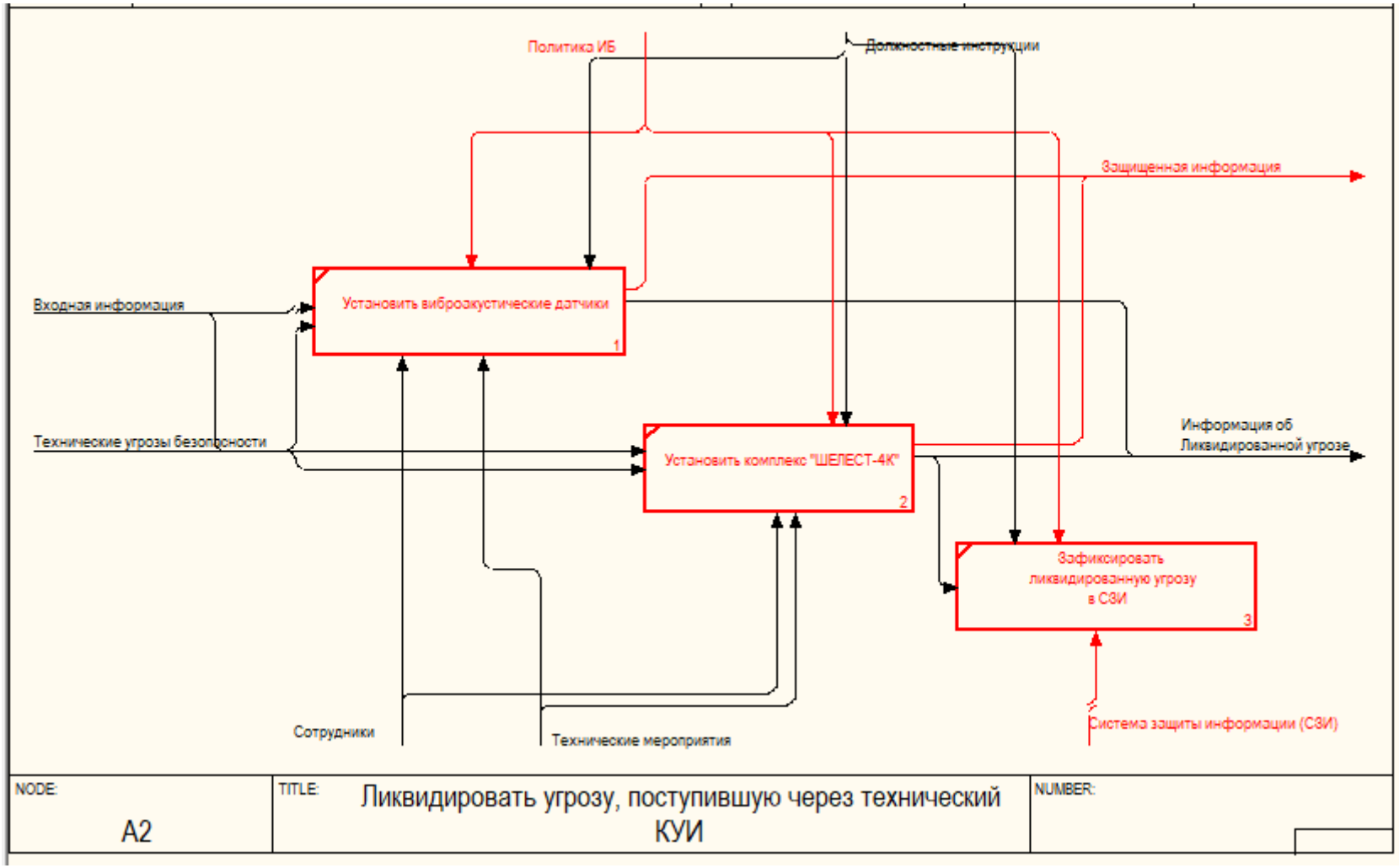


Рисунок 17 – Декомпозиция процесса «Ликвидировать угрозу, поступившую через технический КУИ»

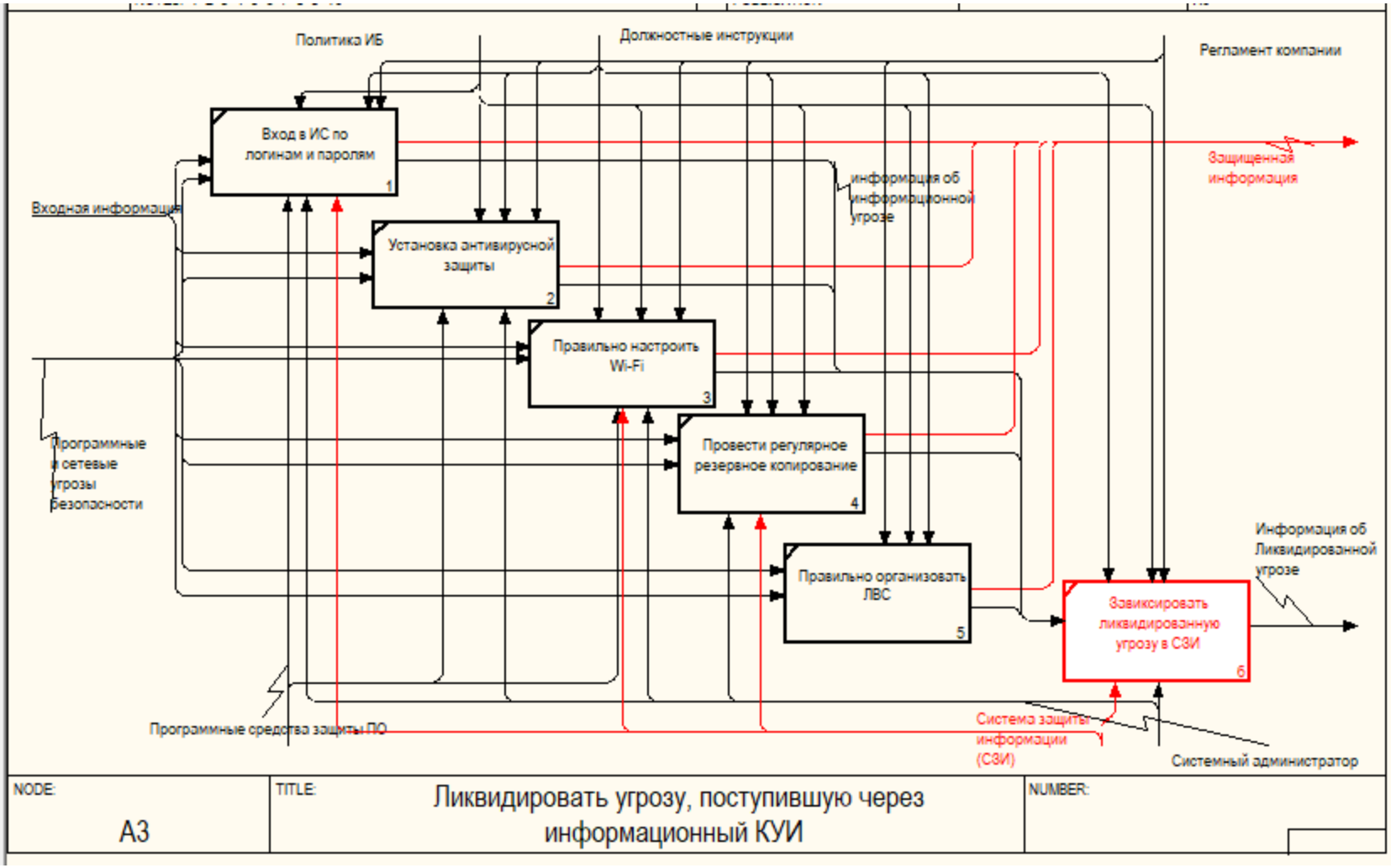


Рисунок 18 – Декомпозиция процесса «Ликвидировать угрозу, поступившую через информационный КУИ»

Теперь определен необходимый комплекс мер по защите информации (ЗИ):

- установлена система видеонаблюдения;
- установлены двери с повышенной шумоизоляцией;
- установлены жалюзи на окнах;
- установлены виброакустические датчики: в оконные проемы, в вентиляцию, стены, дверные проемы, в систему отопления.
- установлен комплекс «ШЕЛЕСТ-4К» – для предотвращения утечки информации по акустическому и виброакустическому каналу утечки информации;
- внедрение в организацию СЗИ;
- разработка политики информационной безопасности компании;
- правильная организация ЛВС для эффективной защиты информации.

Также будет разработана более эффективная схема ЛВС в организации с топологией «Звезда»:

Выбор архитектур сетевых конфигураций:

Для достижения высокой отказоустойчивости сети необходимо сначала определить топологию, то есть способ организации физических связей. Выбор топологии существенно влияет на характеристики сети в целом. В данной работе была выбрана топология «звезда», так как отказы на отдельных участках не влияют на работоспособность всей сети, и она наиболее надежна [6].

При выборе архитектуры для использования учитывались следующие особенности топологии «звезда»:

– к центральному узлу будет проложен отдельный сетевой кабель, что позволит расположить рабочие станции произвольным образом:

В нашем случае в агентстве недвижимости ООО «Мир квартир» будет находиться 1 коммутатор, который объединяет в сеть 17 компьютеров-клиентов (рабочих станции), подключаемых отдельным кабелем к общему устройству, находящемуся в центре сети. Разрыв одного из кабелей может

сказаться лишь на работоспособности одного компьютера и может быть быстро локализован.

– данная топология предполагает использование коммутатора одного из лидирующих производителей в качестве центрального узла, что обеспечивает высокую отказоустойчивость сети в целом.

Будет выбрано место для размещения активного сетевого оборудования, центра «звезды». От места расположения активного сетевого оборудования до каждой рабочей станции будет проложен монтажный короб для защиты сетевого кабеля от физических повреждений и для сохранения хорошего внешнего вида в агентстве недвижимости. Кабель канал будет проложен вдоль нижнего края стены, не обязательно доходя вплотную до рабочей станции – для последнего шага будет использоваться «патч-корды». К каждой рабочей станции будет протянут отдельный сетевой кабель. Каждый кабель будет обжат разъемом «RJ45» по категории «B» со стороны активного сетевого оборудования и розеткой со стороны рабочей станции (рисунок 19). Все сетевые кабели будут подключены к коммутатору.

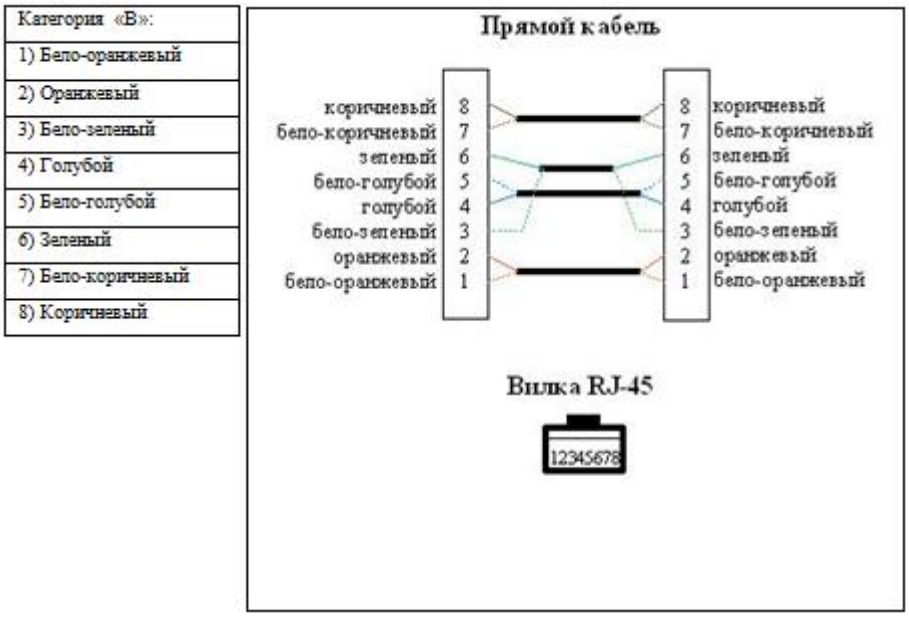


Рисунок 19 – Кабель с разъемом «RJ45» по категории «B»

В качестве линий связи или передающей среды будет использоваться кабель витая пара, волновое сопротивление которого 120 Ом. В следующей главе будет произведен расчет активной длины витой пары.

Сети с звездной топологией представляют собой пассивные сети, где компьютеры только принимают информацию, но не отвечают за ее передачу. Неисправность одной из подключенных машин не оказывает влияния на работу всей сети. Даже если происходит обрыв кабеля или нарушение контакта в разъеме, а также неисправность коммутатора, все остальные сегменты остаются работоспособными. Таким образом, преимуществом сети с топологией «звезда» является возможность продолжения работы сети при возникновении повреждения одного участка кабеля.

Также в агентстве недвижимости будет использоваться и беспроводное Wi-fi соединение, обеспечивающее связь рабочих станций с многофункциональными устройствами, сетевыми принтерами, а также для предоставления доступа в интернет клиентам агентства недвижимости - гостевого Wi-fi. Радиус передачи при использовании устройства составляет до 20 м., и к одному устройству можно подключить около 10 устройств. Для организации Wi-Fi сети потребуется Wi-Fi роутер. Все рабочие станции должны будут иметь доступ к Wi-Fi через собственный адаптер.

3.2 Определение мест размещения средств обеспечения информационной безопасности

Разработка схемы ЛВС:

Как говорилось ранее, в основе будущей сети будет лежать проводное соединение. Такая сеть более стабильная, надежная и безопасная. Так как чтобы злоумышленнику подключиться к сети, ему нужен физический доступ к розетке.

Итак, рассмотрим схему ЛВС, основанную на проводном соединении в ООО «Мир квартир». На рисунке 20 и 21 показана сеть агентства недвижимости, которая была разработана для более эффективной работы сети

ЛВС в данной компании.

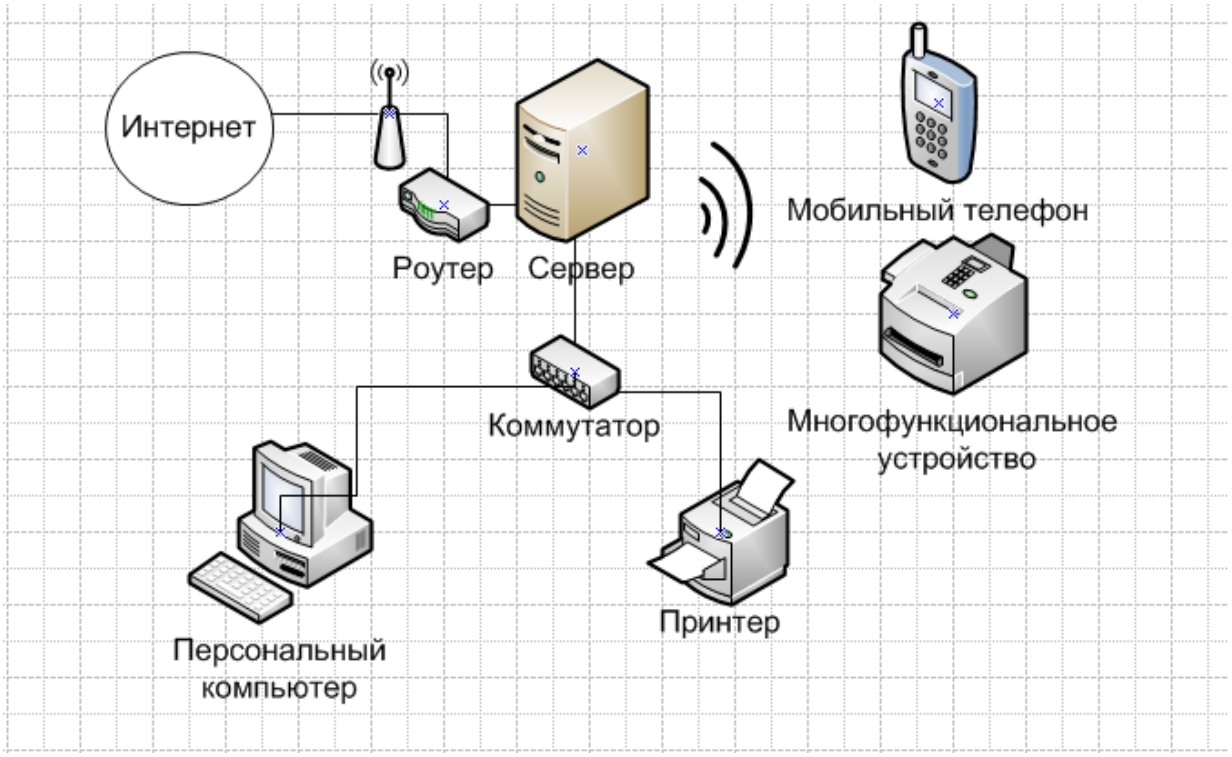


Рисунок 20 – Разработанная сеть ЛВС

В качестве линии связи использоваться кабель витая пара, а топология сети – «звезда». При ней, если один ПК выходит из строя, это не повлияет на работе сети в целом. Также кроме проводного соединения будет использоваться и беспроводное Wi-fi соединение, обеспечивающее связь рабочих станций с многофункциональными устройствами и для предоставления доступа в интернет клиентам агентства

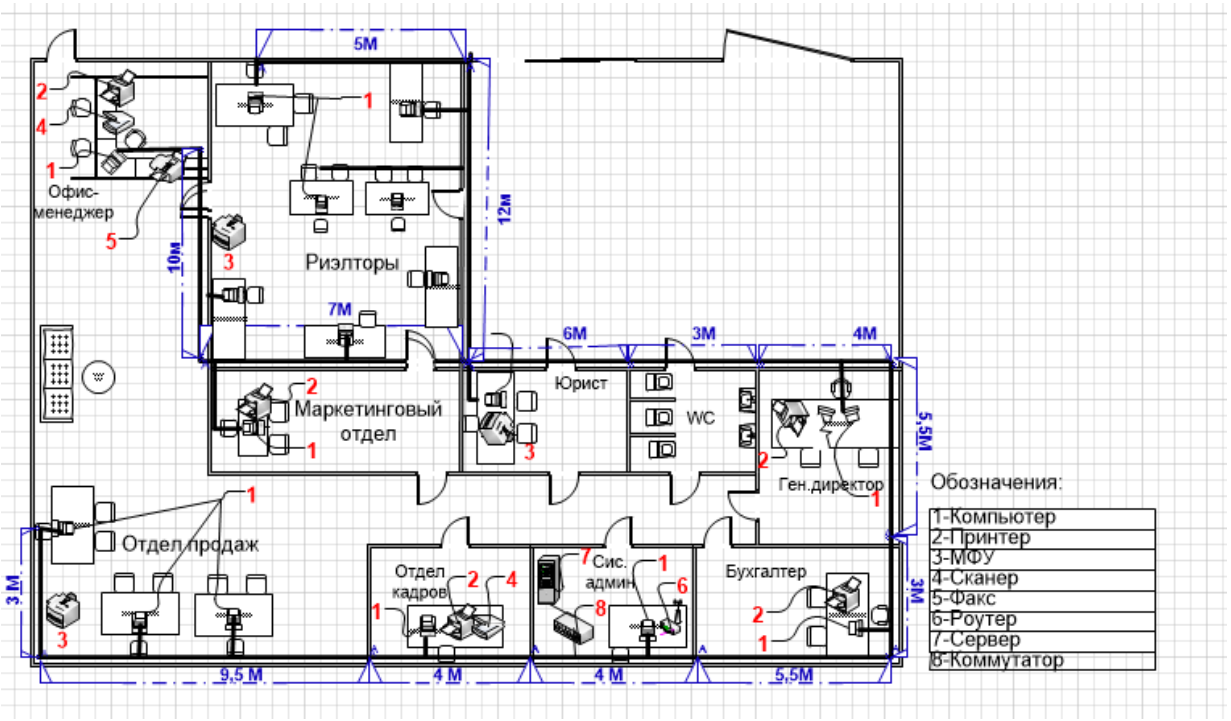


Рисунок 21 – Место расположение сетевого оборудования на плане

Было принято решение установить 1 коммутатор на 24 входа, к которым будут подключены все компьютеры относительно каждого рабочего места сотрудника. В агентстве недвижимости уже имеется необходимое количество рабочих станций, сервер и Wi-Fi роутер, поэтому нет необходимости в их приобретении.

Для информационной защиты конфиденциальных данных агентства недвижимости ООО «Мир квартир» было принято решение применить следующие меры защиты:

- установить систему видеонаблюдения;
- установить двери с повышенной шумоизоляцией;
- установить жалюзи на окнах;
- установить уничтожитель бумаги;
- заменить сейф директора на более надежный VALBERG ASM 46;
- организовать систему резервного копирования информации «Cobian Backup»;
- установить плату генератора шума «ГШ-К-1800».
- установить виброакустические датчики в защищаемое помещение;

- установить комплекс для защиты речевой информации в защищаемом помещении «ШЕЛЕСТ-4К»;
- внедрить СЗИ – программный комплекс ViPNet;
- разработать политику информационной безопасности компании;
- правильно организовать ЛВС для эффективной защиты информации.
- корректно расположить мониторы рабочих мест сотрудников в отделах для предотвращения возможности утечки конфиденциальной информации по визуальным и оптическим каналам.

План расположения всех ЭВМ и средств защиты представлен в Приложении А.

3.3 Разработка организационной и управленческой структуры информационной безопасности

Информационная безопасность в ЛВС:

Рассматривая проблемы, связанные с защитой данных в сети, может возникнуть вопрос, связанный с классификацией сбоев и несанкционированным доступом, который ведет к потере данных или их нежелательному изменению [8].

Это и сбои оборудования такого как: кабельная система, дисковая система, сервера, рабочие станции и т.д. Это и потеря информации из- за поражения ЭВМ вирусами, неправильного хранения данных, при нарушении прав доступа к данным. Также это некорректная работа пользователей ЭВМ.

Данные нарушения работы в сети вызвали необходимость создания различных видов защиты информации, которые условно можно разделить на три класса (рисунок 22).

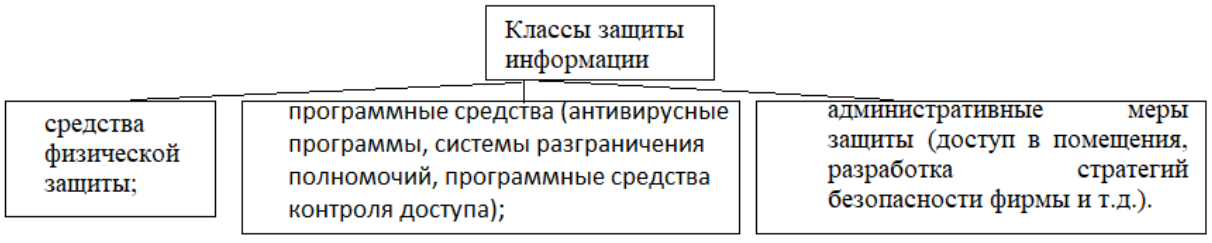


Рисунок 22 – Классы защиты информации

Для обеспечения высокого уровня информационной безопасности в риэлтерском агентстве необходимо определить зону ответственности каждого сотрудника и издать приказы, регламентирующие их действия при работе с ИС. Политика безопасности агентства будет включать ряд приказов и других руководящих документов (рисунок 23) [5].

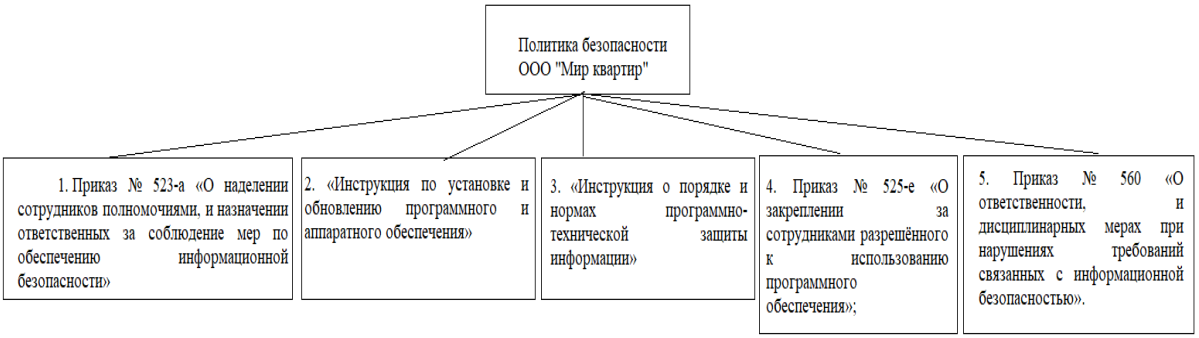


Рисунок 23 – Политика безопасности агентства недвижимости

Для успешного выполнения целей и задач, связанных с поддержанием информационной безопасности, необходимы конкретные меры.

В первую очередь, это должно быть четкое разделение принципов анализа данных, опирающееся на все документы, описывающие каждую важную нюанс ИБ. Помимо этого, не менее важным является обучение и мотивация сотрудников, непосредственно ответственных за контроль и поддержание ИБ.

Дополнительно, эффективным решением может стать передача некоторых полномочий персоналу для более полноценной реализации функциональных задач, связанных с доступом к информационным системам. Также необходимо строго следить за тем, чтобы все сотрудники полностью понимали и соблюдали предъявляемые требования в рамках поддержания безопасности данных при обслуживании и работе в рамках ПО.

Для того, чтобы обеспечить безопасность информационной системы (ИС), необходимо учитывать каждый защищаемый ресурс – данные, серверы, станции, каналы. Кроме того, необходимо выработать точные решения, которые обеспечат полноценность технических ресурсов и непрерывную

защищенность всей ИС.

Важным аспектом в обеспечении безопасности ИС является использование физических и технических СЗИ с постоянной поддержкой использования. Также необходимо обеспечить полноценную юридическую защиту фирмы и провести полноценный анализ, чтобы ответить на вопрос о достаточности реализуемых мер и используемых СЗИ [11].

Для повышения эффективности обеспечения безопасности ИС следует внедрять обновленные предложения по поддержанию лучшего уровня всей ИС. Реализация таких предложений позволит не только повысить уровень защищенности ИС, но и предотвратить возможные угрозы и проблемы в будущем.

В результате правильного и комплексного подхода к обеспечению безопасности ИС, организация может быть уверена в надежной защите своих ресурсов и сохранении конфиденциальности важной информации.

Для успешной работы компании в Интернете необходимо установить четкий порядок действий ее сотрудников в ИС, а также регламентировать доступ к основным ресурсам. Для этого компания должна разработать документ, который будет являться руководством для сотрудников при работе с ИС [3].

Важно понимать, что без регламентации действий в ИС возможны сбои в работе системы, а также утечка важной информации. Поэтому, в документе «Документ для корректировки перечня пользователей системы и их полномочий для доступа к системным ресурсам» нужно детально описать полномочия пользователей системы и ограничения на доступ к конфиденциальным данным.

Безусловно, регламентация является неотъемлемой частью управления ИТ-ресурсами компании и позволяет оптимизировать процессы работы, защитить от угроз и сократить риски нарушения безопасности. Регламентирование действий имеет большое значение для эффективности работы фирмы и помогает ей сохранить свою репутацию и имидж. Поэтому

каждая компания должна уделять должное внимание регламентации работы ИС и контролировать ее соблюдение.

Все сотрудники агентства должны иметь некий требуемый доступ с применением ресурсов автоматизированной системы для реализации своих функций.

Права на полное удаление данных и ресурсов системы не должен иметь никто.

Структура АРМ, которые анализируют все защищенные данные, обязана четко следить за правами пользователя, который работает сейчас за ПК.

Нужно отключить либо полностью, либо логически данные, которые не используются в работе и их источники (приводы, диски, дисководы).

Порядок установки новых компьютеров или изменения конфигураций программного обеспечения или аппаратной части уже имеющихся компьютеров регламентирован в «Инструкции по обновлению, установке и ТО программ и аппаратных средств РС АС» [5].

Одним из самых важных аспектов безопасности компьютерных систем является обеспечение физической целостности всех аппаратных составляющих. Это может быть достигнуто через использование организационных мер, таких как установка механических замков, пломбирование (наклеек, стикеров и т.д.) и защита всех комплектующих частей вычислительной техники.

Однако, необходимо отметить, что просто установка механических средств защиты не гарантирует полной безопасности. Для обеспечения максимальной защищенности компьютера также необходимо следить за тем, кто имеет доступ к нему и как он используется.

Кроме того, при выборе механических средств защиты необходимо учитывать факторы, такие как надежность и долговечность. Важно выбирать качественные замки и пломбы, которые надежно защитят систему от нежелательных вторжений.

В итоге, обеспечение физической целостности компьютера является важным аспектом безопасности. Использование организационных мер и механических средств защиты позволяет снизить риски взлома системы, однако, необходимо учитывать все факторы и следить за правильностью их применения.

Отслеживанием целостности и проверке пломб и т.д. занимаются все пользователи организации и администратор по информационной безопасности.

Для деятельности на защищенных компьютерах должны применяться помещения, в которых есть замки, сигнализация, видеонаблюдение и охрана. Это сводит к минимуму хищение информации третьими лицами.

Уборка в таких помещениях, где такие ПК, должна производиться в присутствии должностного лица, ответственного за эту технику.

В условиях строгой информационной безопасности, посетители офисных помещений не могут иметь доступ к данным, на которые у них нет права доступа. Это позволяет защитить конфиденциальную информацию компании и предотвратить несанкционированный доступ к ней.

После завершения работы на ПК, они передаются под охрану и ставятся отметки о сдаче/приеме помещений. Это еще одна мера безопасности, которая позволяет контролировать доступ к компьютерам и защищать информацию от утечек.

В настоящее время, при использовании сетевой инфраструктуры, очень важно разделять ЛВС на сегменты. Это позволяет улучшить безопасность сети и уменьшить риски компрометации информации. Особенно часто используются виртуальные ЛВС (VLAN), которые соответствуют организационной структуре соединения и методике работы отделов фирмы и хранят данные.

Важно отметить, что выделенные сегменты часто содержат серверы ЛВС, которые используются для хранения и обработки конфиденциальной информации компании. Безопасность этих серверов является критически

важной, и она должна быть обеспечена высокими стандартами защиты.

3.4 Оценка эффективности разработанной системы технической защиты средств обработки, хранения и передачи информации

Задачи организации информационной безопасности компаний в настоящее время являются особо актуальными. Многие компании, согласно законодательству РФ, несут ответственность за сохранность личных данных своих сотрудников и клиентов. И это действительно необходимо. Ведь утечка может нанести моральный ущерб или материальный урон. И в той, и в другой ситуации приятного мало.

Многие люди, обращаясь в агентства недвижимости, оставляют там свои персональные данные (ПДн), которые являются конфиденциальной информацией. Такую информацию необходимо защитить.

Для обеспечения безопасности персональных данных и гарантированного сохранения информации, агентства разрабатывают и внедряют новые информационные системы [4]. Это необходимо для того, чтобы предотвратить потенциальные угрозы от злоумышленников и хакеров.

Вместе с тем, безопасность агентства является ключевым приоритетом, поэтому наряду с созданием новых систем защиты, устанавливается специализированное оборудование, которое отвечает всем требованиям безопасности.

Процесс разработки и внедрения систем информационной безопасности предполагает проведение аудита существующих систем и выявление уязвимых мест.

При этом, не менее важным является соблюдение правил и процедур, связанных с доступом к конфиденциальной информации. Все сотрудники агентства должны проходить обучение и сертификацию по вопросам информационной безопасности, а также иметь понимание ответственности, связанной с доступом к конфиденциальным данным.

Итак, обеспечение безопасности информации является сложной и многогранным процессом, который требует постоянного и систематического подхода, используя новейшие технологии и комплексные решения.

Защита информации - одно из главных направлений в сфере компьютерных технологий. И одним из важнейших элементов защиты информации являются средства защиты. Средства защиты информации используются для обеспечения конфиденциальности, целостности и доступности информации.

Средства защиты информации могут быть программными или аппаратными. Программные средства защиты включают в себя программы для шифрования, антивирусы, программы для контроля доступа и т.д. Аппаратные средства защиты используются для защиты компьютерных систем, в том числе для защиты от взлома, хакерских атак и вирусов.

По сути, аппаратные СЗИ - это совокупность инженерно-технических, электронных, других устройств и технических систем, используемых для решения многих задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Введение данной системы СЗИ позволит агентству недвижимости автоматизировать защиту информации и связанные с этим процессы. Это давно сформированный рынок решений, для самых разных клиентов и задач.

Система защиты информации имеет множество задач, которые требуется решить для эффективного функционирования. Например, важно обеспечить учет, хранение и выдачу пользователям паролей, ключей и информационных носителей. Важную роль играет также задача ведения служебной информации, включающая сопровождение правил разграничения доступа, генерацию паролей и ключей. Еще одна существенная функция СЗИ - контроль за функционированием системы защиты информации и проверка соответствия программного обеспечения эталонам. Также в список задач СЗИ входит прием новых программных средств в информационную среду, а также сигнализация об опасных событиях и многое другое.

В целом, СЗИ должна быть универсальной и эффективной системой, которая сможет решать множество сложных задач и обеспечивать безопасность хранения, обработки и передачи информации.

Очень важно надлежащим образом организовывать поддержку программно-технических средств.

Обоснование решения по направлению и технологии оптимизации бизнес-процессов:

Программный комплекс ViPNet предназначен для обеспечения информационной безопасности. Он состоит из множества компонентов, тем самым обеспечивая защиту сети от атак из интернета, также дает возможность управления доступом к интернет-ресурсам. Позволяет создавать защищённые виртуальные частные сети. Комплекс предназначен для небольших и средних компаний [10, 11, 12].

Основные возможности программного комплекса отображены на рисунке 24.

Рисунок 24 – Основные возможности программного комплекса

В таблице 4 представлены ключевые показатели программного комплекса.

Таблица 4 - Ключевые показатели программного продукта ViPNet

Наименование программного обеспечения	Поддержка шифрования внешнего трафика	Поддержка шифрования внутреннего трафика	Масштабируемость (1-5 баллов)
VipNet 4	присутствует	присутствует	5

Программный комплекс ViPNet имеет ряд преимуществ перед другими аналогичными продуктами (рисунок 25).

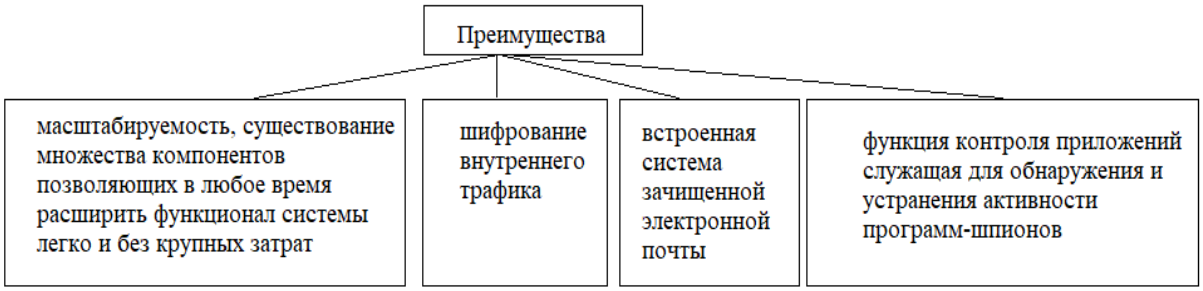


Рисунок 25 – Преимущества программного комплекса

При использовании программного продукта ViPNet в компании ООО «Мир квартир» ликвидируются основные уязвимости, что совместно с организационными мерами защиты информации позволит решить поставленную в данной выпускной квалификационной (бакалаврской) работе задачу.

Выбор и разработка мер по защите акустической информации:

Описание объекта защиты выделенного для переговоров помещения

Рассмотрение объекта исследования начнем с краткого описания помещения, в котором он находится.

Помещение находится в 10-ти этажном здании, состоит из холла, 7 кабинетов.

В качестве (объекта защиты) выделенного помещения мы будем рассматривать кабинет, используемый для переговоров (кабинет риелторов), который находится на 1-ом этаже данного здания. С двух сторон находятся задействованные помещения (холл и маркетинговый отдел), в которых

расположены кабинеты с сотрудниками, с одной стороны находится улица, с оставшейся – помещение с офисом другой компаний.

Предположим, что в данном помещении будут проходить совещания и встречи, на которых будет обсуждаться конфиденциальная информация, подлежащая защите.

Опишем выделенное помещение: помещение располагается на 1 этаже, в нем располагается система вентиляции и отопления, размеры помещения – 84 м^2, подвесной потолок, железобетонные перекрытия, стеновые перегородки выполнены из кирпича, толщина которого 0,5 м (рисунок 26).

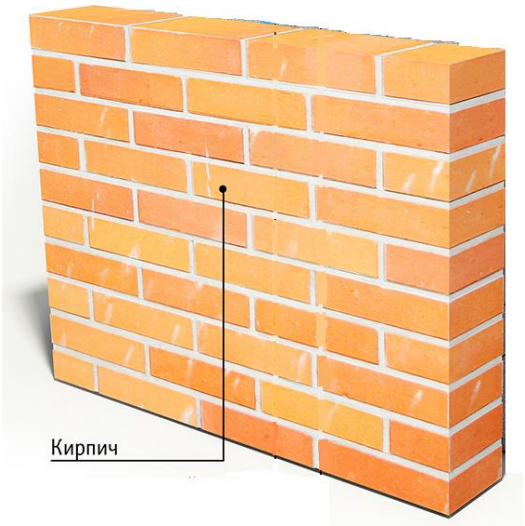


Рисунок 26 – Изображение стеновой перегородки

Наружные стены также кирпичные 0,75м толщиной, присутствует экранирование и штукатурка (рисунок 27).

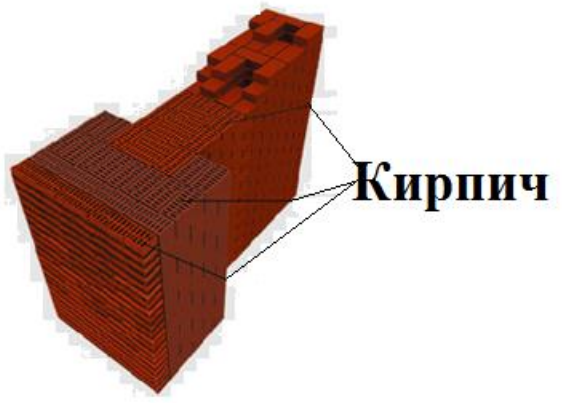


Рисунок 27- Изображение наружной стены

Оконные рамы - двухкамерные стеклопакеты размером 3 м на 1,5 м в количестве 5 штук (рисунок 28). Профиль оконной рамы представлен на рисунке 29.

Две двери размером 2,2 м на 1,3 м легкие без уплотнений с механическим замком.

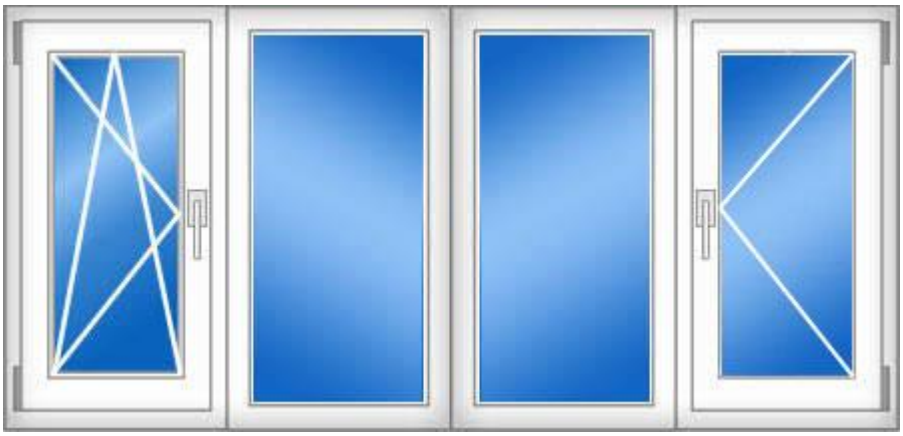


Рисунок 28 – Изображение оконных рам

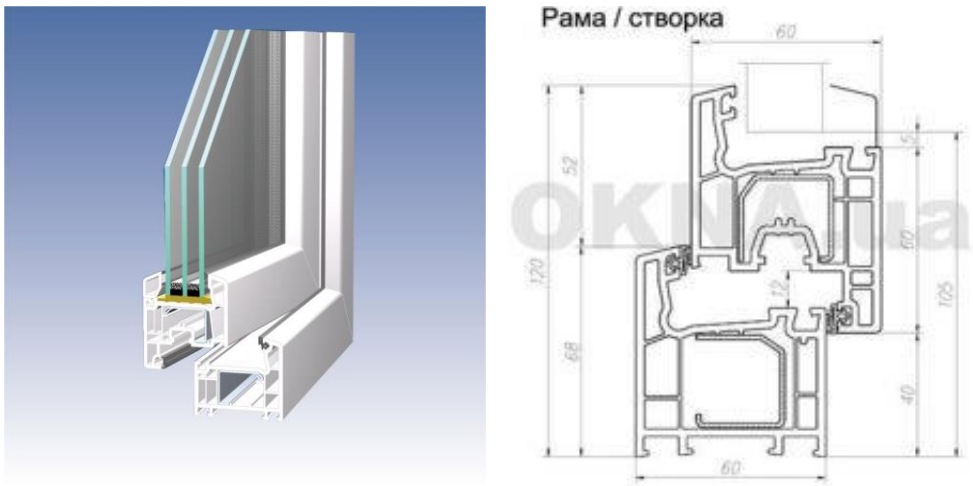


Рисунок 29 – Изображение профиля оконной рамы

Опишем смежные помещения: справа от защищаемого помещения располагается улица, а сверху – офисы других компаний. В защищаемом помещении имеется оргтехника 1 МФУ и 7 шт..ПК, сеть 220В, 6 потолочных светильников, пожарная сигнализация, система вентиляции, отопление центральное водяное (5 батарей, есть выход из труб), экраны на батареях,

имеется телефонная линия. В качестве офисной мебели располагаются 7 столов работников и стулья.

Опишем обстановку вокруг объекта: помещение располагается в центре города, оно окружено трассой с трех сторон, а с четвертой стороны находится офис другой компании. Представим план защищаемого помещения, изображенный на рисунке 30.

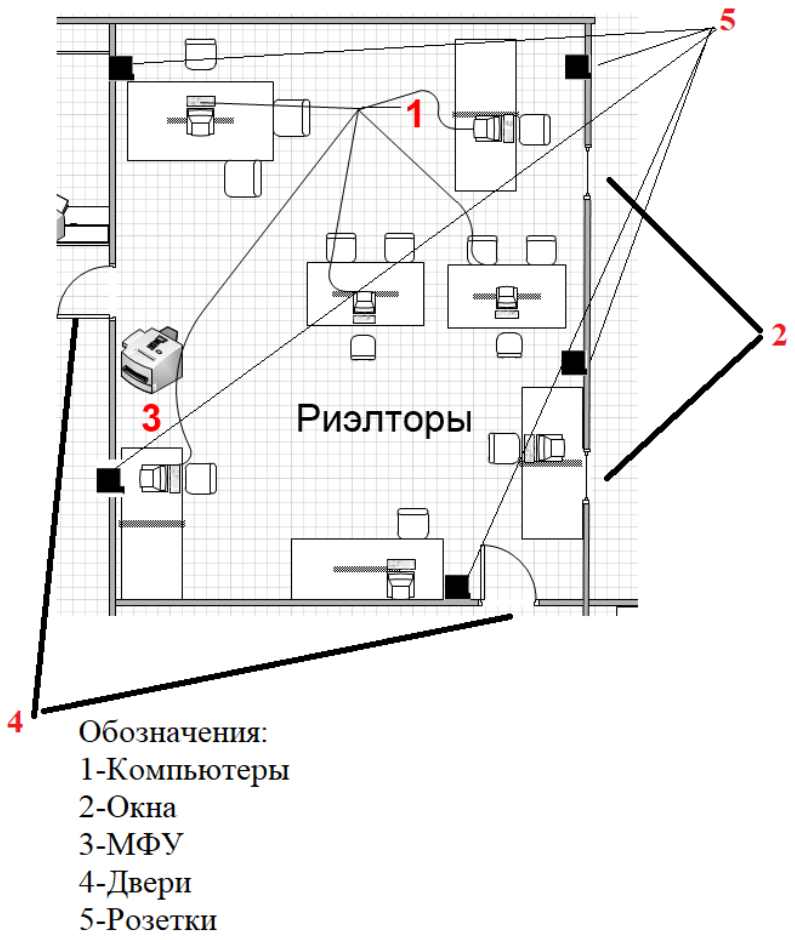
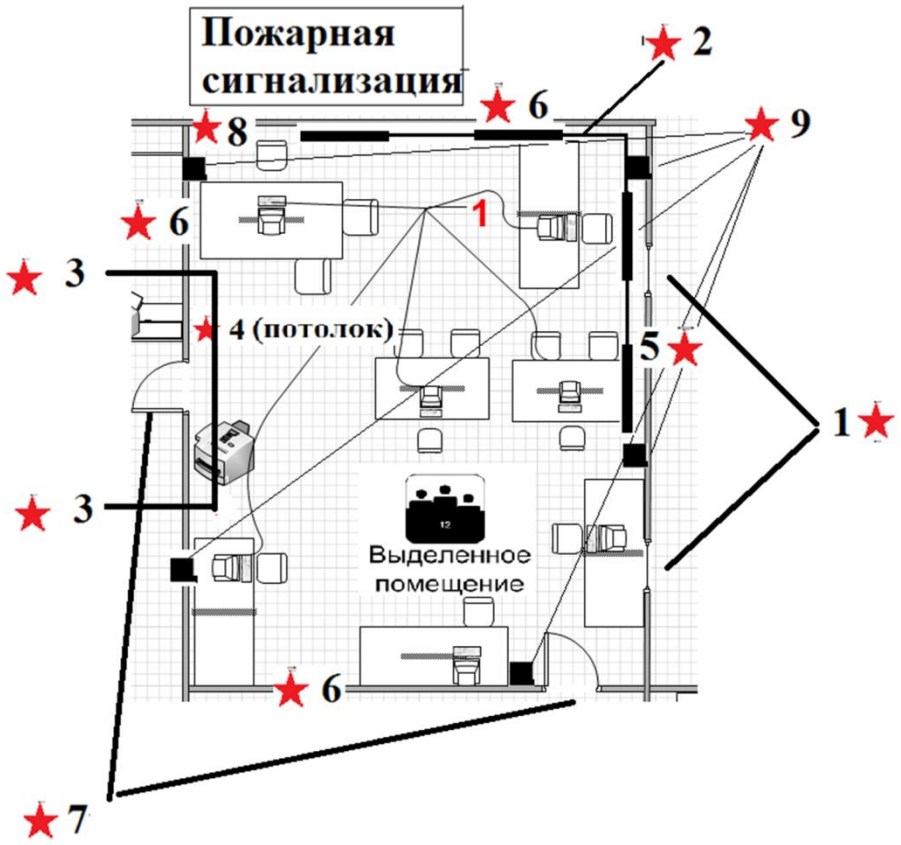


Рисунок 30 – Изображения схемы защищаемого помещения

В защищаемом помещении будет обрабатываться конфиденциальная информация. На рисунке 31 изображено защищаемое помещение (схема) с указанием технических каналов утечки речевой (акустической) информации.



Обозначения:

1 – виброакустический, оптико-электронный, утечка через фрагменты окон
2 – виброакустический, утечка через выходы системы отопления
3 – виброакустический, утечка через выходы системы вентиляции
4 – виброакустический, утечка через элементы конструкций потолка
5 – виброакустический, утечка через элементы конструкций наружных стен
6 – виброакустический, утечка через элементы конструкций межкомнатной стены
7 – виброакустический, утечка через элементы конструкций двери
8 – акустоэлектрический, утечка через слаботочную проводку ВТСС (в системах оповещения пожарной сигнализации)
9 – акустоэлектрический, утечка через сеть электропитания ОТСС и ВТСС, 220В

Рисунок 31 – Изображение схемы помещения с указанием технических КУИ

Методы и средства защиты акустической информации:

Для защиты акустической информации от утечки по техническим КУИ используются организационные и технические мероприятия, а также техника для выявления закладных устройств, предназначенных для перехвата информации [7, 14, 15].

На рисунке 32 представлены основные организационные мероприятия по защите речевой информации.

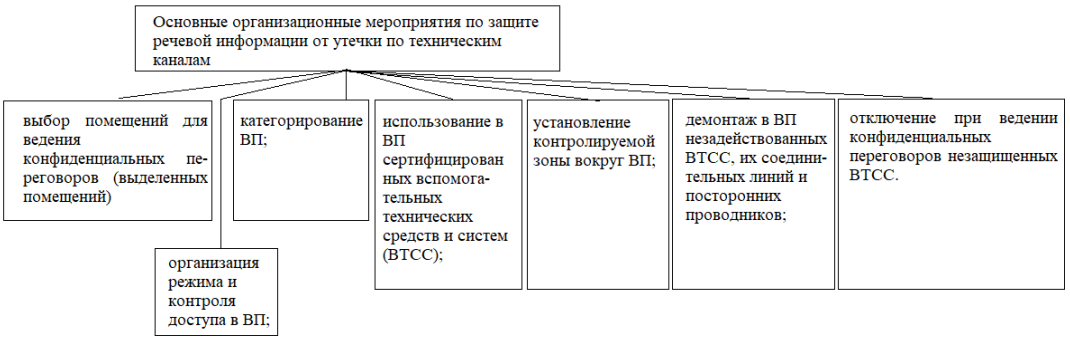


Рисунок 32 – Основные организационные мероприятия по защите речевой информации

В таблице 5 рассмотрены основные преимущества и недостатки выделенного помещения.

Таблица 5 – Преимущества и недостатки выделенного помещения

Преимущества	Недостатки
2) Возможность установления временной контролируемой зоны. 3) Возможность демонтажа средств ВТСС.	1) Имеет общие ограждающие конструкции с помещением, принадлежащим другой организации. 2) Имеет окна, выходящие на места стоянки автомашин, а также близлежащие здания. 3) Располагается на первом этаже

Техническое мероприятие - это мероприятие по защите информации, которое предусматривает применение специальных технических средств, а также реализацию технических решений [13, 16, 20].

Технические мероприятия обычно проводят, если не удалось обеспечить защиту информации с помощью организационных методов.

Технические способы защиты информации в зависимости от используемых средств подразделяются на пассивные и активные.

Классификация пассивных способов защиты речевой информации представлена на рисунке 33.

Рисунок 33 – Классификация пассивных способов защиты речевой информации в выделенных (защищаемых) помещениях

На рисунке 34 представлена классификация активных способов защиты речевой информации.

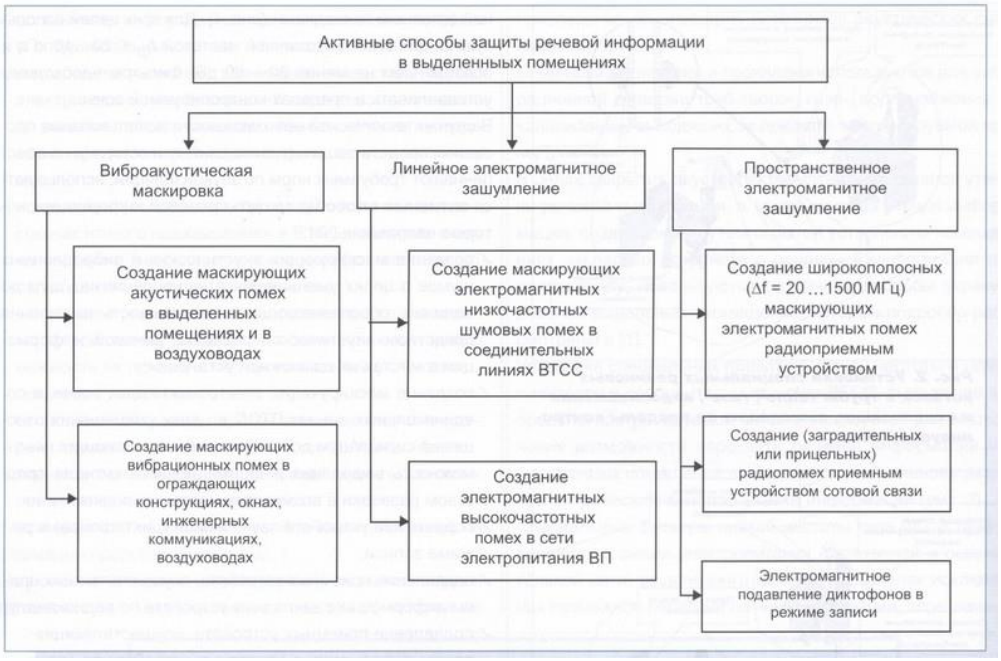


Рисунок 34 – Классификация активных способов защиты речевой информации

Защита информации от утечки по виброакустическим и оптико-электронным каналам [15]:

В рассматриваемом защищаемом помещении возможна установка таких устройств как Комплекс «ШЕЛЕСТ-4К» или комплекс «ВВ-301». Полная их характеристика дана в Приложении Б.

Установим виброакустические датчики, для этого составим схему:

Здание, в котором находится защищаемое помещение – десятиэтажное, на первом этаже расположено место охранника, который пускает сотрудников организации по пропускам. Поэтому для защиты акустической информации от утечки через конструкцию потолка будет достаточно использовать фальшпотолок в качестве пассивных средств защиты [19].

На окнах будут установлены виброакустические датчики, которые зашумляют до 2 м^2. стекла (по одному датчику на каждый фрагмент окна) [16].

На дверях будут установлены зашумляющие акустические колонки (2 шт.), которые зашумляют до 10 м^2. кирпичных стен. (понадобится 8 датчиков на каждую стену).

В систему вентиляции будут вмонтированы датчики по одному на каждый вывод системы вентиляции, понадобятся две штуки датчиков.

Количество датчиков представлено в таблице 6, их функциональное назначение представлено в таблице 7.

На рисунке 35 представлена схема расположения виброакустических излучателей в выделенном помещении.

Таблица 6 – Размещение и количественный состав виброакустических датчиков

Место установки	Общее количество датчиков
Оконный проем	8
Стены	8
Выводы системы отопления	4
Система вентиляции	2
Дверной проем	2

Таблица 7 – Обозначение и назначение виброакустических датчиков

Обозначение на схеме	Назначение виброакустического датчика
	Для зашумления виброакустического канала утечки информации через выводы системы вентиляции
	Для зашумления виброакустического канала утечки информации через выводы системы отопления
	Для зашумления виброакустического канала утечки информации через ограждающие конструкции (стены)
	Для зашумления виброакустического канала утечки информации через оконные проемы
	Для зашумления виброакустического канала утечки информации через дверной проем

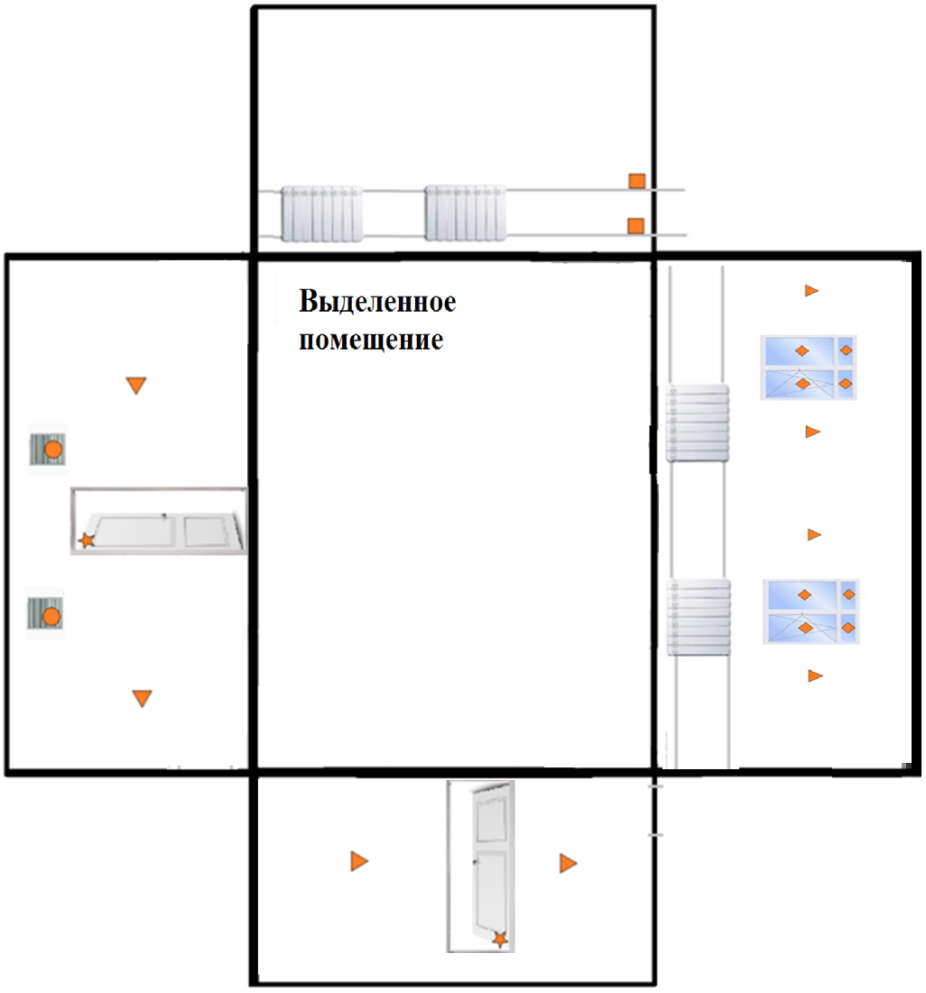


Рисунок 35 – Схема расположения виброакустических излучателей

Проведя исследование средств, методов и мероприятий по защите информации, можно сделать выводы:

– для достижения наибольшего эффекта по защите информации необходимо использовать все средства, методы и мероприятия, объединенные в единый механизм защиты информации;

– обязательно осуществлять постоянный контроль функционирования механизма защиты.

Построим UML диаграмму. На рисунке 36 представлена UML-диаграмма вариантов использования комплекса мероприятий по обеспечению информационной безопасности агентства недвижимости, выполненная с помощью программного средства MS Visio.

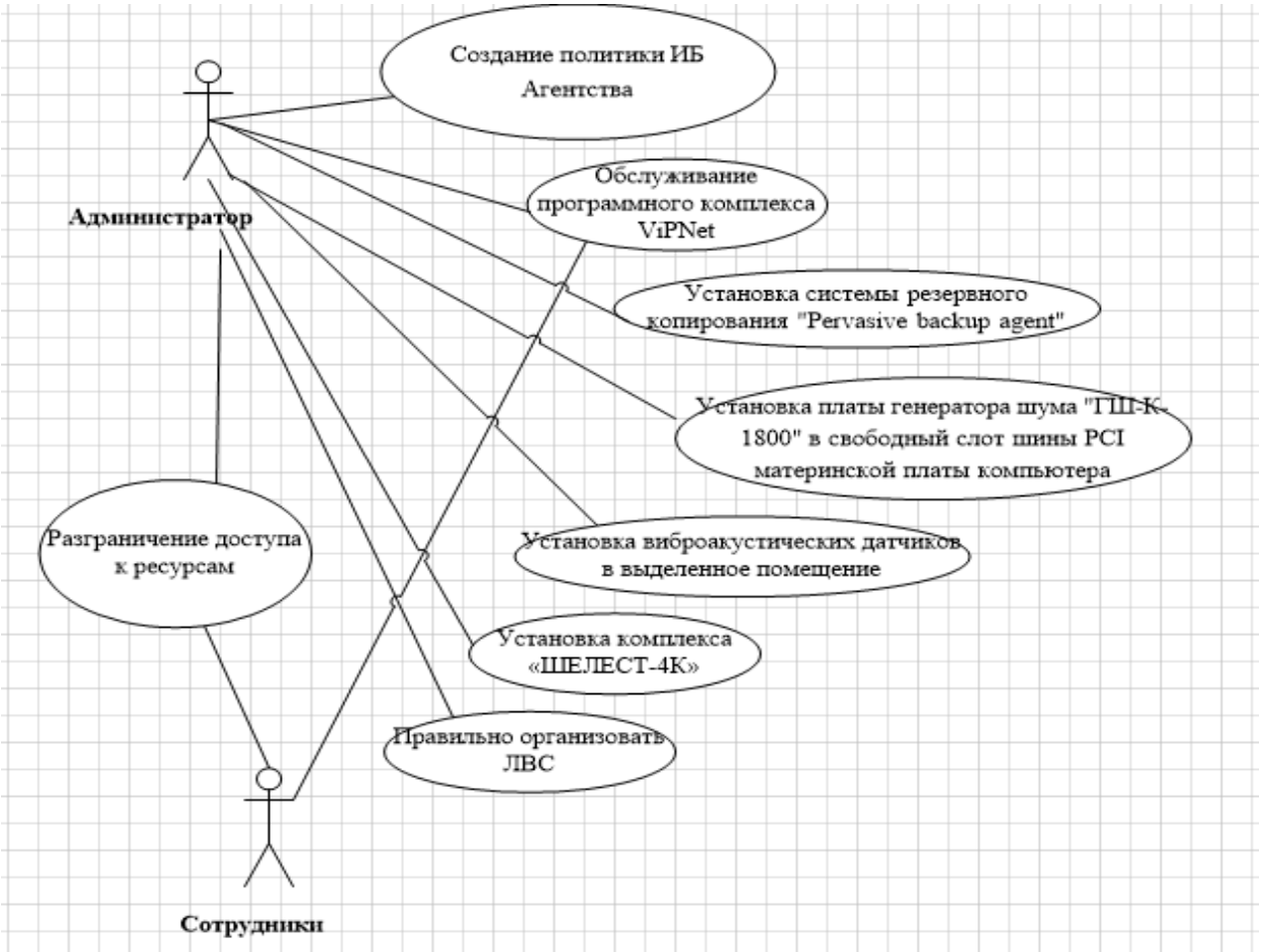


Рисунок 36 – UML-диаграмма

Данная диаграмма является графическим изображением возможных взаимодействий пользователя с системой.

4 Технология управления процессами обеспечения безопасности в ООО «Мир квартир»

4.1 Структурно-функциональная схема объекта обеспечения безопасности

Объектом обеспечения безопасности является рабочее место риелторов.

На рабочем месте риелторов агентства недвижимости необходимо провести оценку эргономических условий.

Эргономическая оценка рабочего места должна использовать комплексный подход, позволяющий проводить многофакторный анализ. В этом случае можно использовать несколько методов: методы изучения характера и организации труда, методы наблюдения и опроса, операционные и структурные описания трудовой деятельности, измерение времени, антропометрия, биомеханика, физиологические, психологические, гигиенические, экономические и другие методы. Набор методов выбирается в соответствии с характеристиками изучаемой системы. Необходимо обеспечить обоснованность методов, надежность и стабильность (достоверность) данных.

Составим схему расположения компьютеров в кабинете риелторов (рисунок 37).

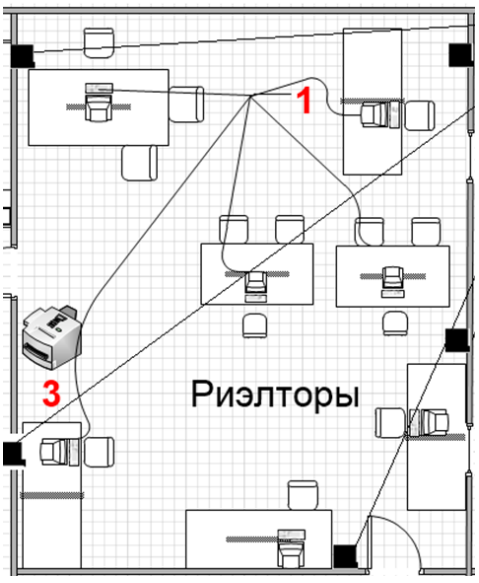


Рисунок 37 – Схема расположения персональных компьютеров

Опишем основные нарушения эргономических условий в кабинете риелторов в таблице 8.

Таблица 8 – Нарушения эргономических условий в кабинете риелторов

Нарушение
В отделе ярко выраженное нарушение микроклиматического режима, что ухудшает состояние и работоспособность. Влажность воздуха в помещении – 19-26%, что ниже минимально допустимого значения в 40%.
В пользовании риэлторов находится МФУ. МФУ располагается в рабочей зоне работника. Он находится на расстоянии вытянутой руки. Яркость поверхности принтера составляет 625 кд/м2, что в 3 раза превышает норму – 200 кд/м2.
Столы не соответствуют требованиям для работы с ПЭВМ. Глубина стола составляет 600 мм, при минимально установленном значении глубины – 800 мм. Из-за этого сокращается расстояние между монитором, установленным на столе и глазами пользователя. Так же за мониторами установлены светодиодные лампы, яркость которых отрицательно сказывается на работоспособности риэлторов.
Из-за недостаточной глубины рабочей поверхности и большого объема обрабатываемой информации, на столах скапливается много документации. Данное обстоятельство не позволяет полностью класть руку на стол, что может стать причиной переутомления или травмы.
Рабочее кресло имеет маленькую амплитуду регулировки, из-за чего работникам с ростом выше 170см приходится наклонять голову вниз для работы за компьютером. Из-за чего возможно развитие сколиоза и болезней шейного отдела позвоночника. Не смотря на это, кресло дает возможность быстро и легко перемещаться в рабочей зоне.
На рабочем месте отсутствует обязательная подставка для ног. Из-за ее отсутствия у работников наблюдается неправильное положение ног относительно корпуса, нагрузка на ступни распределяется неравномерно.

Данные показатели существенно влияют на эргономические условия риелторов.

4.2 Методика проведения оценки эргономических условий на рабочих местах сотрудников агентства недвижимости ООО «Мир квартир»

Опишем порядок проведения работ по оценке эргономических условий труда (таблица 9).

Таблица 9 – Порядок проведения работ по оценке эргономических условий труда

№ этапа	Наименование этапа
1	Заполнение индивидуальной карты рабочего места
2	Визуальный осмотр
3	Проведение измерений и внесение результатов
4	Заполнение отчетных материалов
5	Анализ полученных результатов

Эргономическая экспертиза включает две стадии: аналитическую и оценочную, состоящие из нескольких этапов. Для частных оценок используются справочные материалы и экспериментальные данные; общая оценка дается в качественной форме («хорошо», «удовлетворительно» и т. д.) и выбирается по согласованию экспертов. После проведения эргономической экспертизы производственного оборудования составляют заключение по эргономической оценке. Рабочие места, эргономическая оценка которых выявила наличие нарушений эргономических требований и установила степень тяжести и напряженности труда выше допустимой, должны стать в первую очередь объектами внимания с точки зрения разработки мер оптимизации функционирования системы.

4.3 Основные характеристики и результаты

В таблице 10 представлено чем оборудовано места сотрудников агентства недвижимости.

Таблица 10 – Состав оборудования мест сотрудников

Наименование
Регулируемые жалюзи
Система отопления
Система вентиляции
Система кондиционирования
Пожарная сигнализация
Кнопка вызова охраны
Система видео наблюдения

Характеристики визуального осмотра рабочей зоны представлены в Приложении В.

Анализ результатов:

Для того, чтобы оценить эргономические условия на рабочих местах сотрудников отдела риэлторов агентства недвижимости был разработан сетевой график мониторинга рабочего места. Также был разработан сетевой график устранения нарушений (параметров рабочей зоны, освещения, микроклиматических условий, конструкции стола и стула, расположения и комплектации элементов ПЭВМ).

Заключение

В рамках данной выпускной квалификационной (бакалаврской) работы был разработан комплекс мероприятий по обеспечению информационной безопасности в действующем агентстве недвижимости.

Первоначальный анализ существующего подхода к информационной безопасности показал, что в компании присутствовали серьезные уязвимости и была высокая вероятность несанкционированной утечки конфиденциальной информации.

Была доказана необходимость разработки и внедрения системы обеспечения безопасности.

При анализе средств защиты информации было выбрано соответствующее и наиболее приемлемое (в том числе по финансовым показателям) решение.

Главной целью коммерческой организации является получение прибыли. Именно поэтому агентства недвижимости занимаются продажей, покупкой, арендой и управлением недвижимостью. Однако, для достижения успеха и удовлетворения потребностей клиентов необходима не только прибыль, но и предоставление качественных услуг. Ведь только качественные услуги приводят к довольным клиентам, которые в свою очередь становятся лояльными к агентству и рекомендуют его своим знакомым. Поэтому важно не только зарабатывать, но и предоставлять качественный сервис.

В связи с этим, главным критерием при выборе средств защиты информации являлись стоимость и функционал. Исходя из вышесказанного, при существующем многообразии средств защиты на современном рынке, были использованы следующие:

– установлена система видеонаблюдения (Компании «ВИПАКС» - разработчик и производитель системы интеллектуального видеонаблюдения);

– установлены двери с повышенной шумоизоляцией (OptimaPlus 5);

– установлены жалюзи на окнах компании (производство «Эскар»);

– установлен уничтожитель бумаги ГЕЛЕОС АП40-4 черный);

– заменен сейф руководителя (VALBERG ASM 46);

– установлена система резервного копирования «Cobian Backup»

– установлена плата генератора шума «ГШ-К-1800».

– установлены виброакустические датчики в защищаемое помещение: в оконный проем, стены, выводы системы отопления, система вентиляции, дверной проем;

– установлен аппаратный комплекс «ШЕЛЕСТ-4К» для обеспечения защиты обрабатываемой в защищаемом помещении речевой информации от утечки по акустическому и виброакустическому каналам;

– внедрен в организацию ООО «Мир квартир» программный комплекс ViPNet;

– разработана политика информационной безопасности компании;

– правильно организована работа ЛВС для эффективной защиты информации.

Расположение и размещение автоматизированных рабочих мест было изменено таким образом, чтобы исключить возможность просмотра изображения на мониторах, кроме работающих за ним людей.

Были определены места размещения всех средств защиты и места размещения автоматизированных рабочих мест.

В результате был разработан комплекс мероприятий по обеспечению информационной безопасности агентства недвижимости ООО «Мир квартир».

Список используемой литературы

1. Батурин Ю.М., Жодзинский А.М. «Компьютерная преступность и компьютерная безопасность» - М.: Юрид. лит.,2017.
2. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1./ А. М. Блинов – Изд-во СПбГУЭФ, 2018. – 96 с.
3. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения. Критерии оценки безопасности информационных технологий. Ч.1. Введение и общая модель. – М.: Госстандарт России, 2002.
4. Домарев В.В. «Безопасность информационных технологий. Системный подход». - К.: ООО ТИД «Диасофт», 2004. – 992 с.
5. Как агентству недвижимости правильно хранить и обрабатывать персональные данные [Электронный ресурс]. – URL: https://news.ners.ru/kak-agentstvu-nedvizhimosti-pravilno-khranit-i-obrabatyvat-personalnye-dannye.html
6. Краковский Ю.М.: Защита информации. Учебное пособие, М., Феникс, 2017 г., 348 с.
7. Лекция 14: Защита акустической (речевой) информации – 2018. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/2291/591/lecture/12700.
8. Максимов Ю. Н. «Защита информации в системах и средствах информатизации и связи». - СПб. 2005.
9. ООО «Мир квартир» [Электронный ресурс]. – URL: https://zachestnyibiznes.ru/company/ul/1175190007662_5190072698_OOO-MIR-KVARTIR
10. Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в интернет. М.: ДМК Пресс, 2011. – 396 с.
11. Попов Л.И., Зубарев А.В. Основные принципы повышения эффективности реализации мероприятий по комплексной защите информации. «Альтпресс», 2009. – 512с.

12. Скрабцов Н.А.: Аудит безопасности информационных систем, М. Питер, 2017 г., 277 с.

13. Средства защиты информации (СЗИ) [Электронный ресурс]. – URL: https://itglobal.com/ru-ru/company/blog/sredstva-zashhity-informaczii/

14. Техническая защита информации. Основные термины и определения. Р 50.1.056 - 2005: Рекомендации по стандартизации. Утв. Приказом Ростехрегулирования от 29.12.2005 № 479-СТ. - Введ. 2006-06-01. - М.: Стандартинформ, 2019. - 20 с. + [Электронный ресурс]. - Режим доступа: http://lawrussia.ru/texts/legal_406/doc406a224x257.htm.

15. Хорев А.А. Способы и средства защиты информации, обрабатываемой ТСПИ, от утечки по техническим каналам / Специальная техника, 2018, № 2, с. 46-51.

16. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2017. – 436 с.

17. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2010. – 458 с.

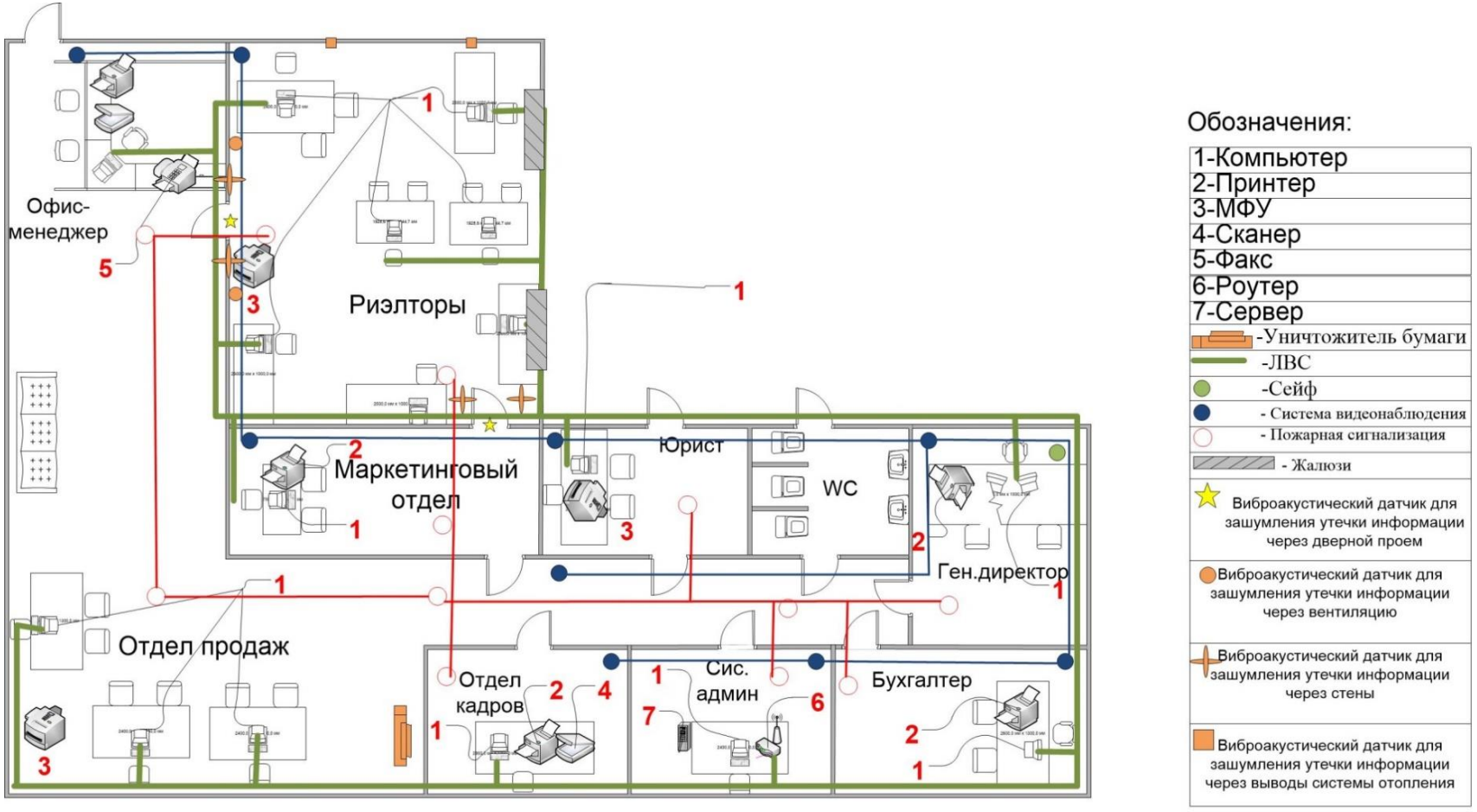
18. Шапаренко Ю. М., Бескид П. П., Суходольский В. Ю. «Проектирование защищенных информационных систем. Часть 1. Конструкторское проектирование. Защита от физических полей» Учебное пособие. – СПб: изд. РГГМУ, 2008. – 60 с.

19. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2017. – 544 с.

20. Ярочкин В. И. «Технические каналы утечки информации». - М., 2017

Приложение А

План размещения ПЭВМ



Приложение Б

Сравнительные характеристики СрЗИ

Таблица Б.1 – Сравнительные характеристики средств защиты информации от утечки по техническим каналам

Устройства для защиты информации от утечки по виброакустическим и оптико-электронным каналам	
1)Виброакустический комплект «ВВ 301»	2) Комплекс «ШЕЛЕСТ-4К» (ТУ РМАГ.438900.031)
Система виброакустической защиты (аппаратура виброакустической защиты помещений) «ВВ 301» (ТУ РМАГ.438900.012) – техническое средство защиты от утечки речевой информации по акустическому и виброакустическому каналам. Система «ВВ 301» может использоваться для защиты выделенных помещений до 1-й категории включительно. Назначение: Защита циркулирующей в помещении речевой информации, содержащей сведения, составляющие государственную тайну, служебную информацию ограниченного распространения, конфиденциальную информацию, персональные данные. Состав: 1. основной блок двухканальный; 2. блок электропитания (поддерживает работу трех основных блоков с полной нагрузкой); 3. блок дистанционного управления с пультом; 4. дополнительный акустомат; 5. вибропреобразователи для зашумления строительных конструкций и инженерных коммуникаций; 6. вибропреобразователи для зашумления для оконных конструкций; 7. акустические преобразователи для зашумления дверных проемов и технологических ниш; 8. установочные и крепежные элементы (по требованию).	Техническое средство защиты циркулирующей в помещении речевой информации от утечки по акустическому и виброакустическому каналам. Комплекс «ШЕЛЕСТ-4К» может использоваться для защиты выделенных помещений до 1 категории включительно. Назначение: 1. защита циркулирующей в помещении речевой информации, содержащей сведения, составляющие государственную тайну, служебную информацию ограниченного распространения, конфиденциальную информацию, персональные данные; 2. защита от прямого прослушивания, а также от прослушивания с использованием различных микрофонов, стетоскопов и лазерных систем съема информации; 3. для защиты больших площадей применяется совместно с системой виброакустической защиты (аппаратурой виброакустической защиты помещений) «ВВ 301». Состав: 1. блок управления; 2. вибрационный преобразователь (для оконных стекол); 3. вибрационный преобразователь (для ограждающих и инженерных конструкций); 4. датчик уровня сигнала; 5. акустический преобразователь; 6. блок дистанционного управления; 7. пульт управления; 8. модуль индикации.
Основные технические характеристики: - полоса частот маскирующего сигнала, в октавных полосах 250 Гц - 8000 Гц; - количество независимых каналов (один основной блок) 2к - дистанционное включение (выключение) в условиях здания не менее 30 м; - электропитание от сети переменного тока 220 В 50 Гц; - контроль шлейфа, защита и контроль короткого замыкания да; - регулировка выходного уровня в каждом канале от максимального уровня - 20 дБ; - нагрузочная способность канала не менее 10 Ом; - площадь железобетонной конструкции, зашумляемая одним датчиком не более 20 кв.м; - площадь кирпичной конструкции, зашумляемая одним датчиком не более 10 кв.м; - площадь оконных стекол, зашумляемая одним датчиком не более 2 кв.м; - протяженность инженерных коммуникаций, зашумляемая одним датчиком не более 15 м. (Сертификат № 782 действителен до 28.11.2015) Перекрывает следующие каналы утечки информации: -виброакустический канал утечки информации в оконных проемах -оптико-электронный канал утечки информации в оконных проемах -виброакустический канал утечки информации через ограждающие конструкции: стены, потолок -виброакустический канал утечки информации в инженерных сооружениях: система отопления -виброакустический канал утечки информации в системе вентиляции -виброакустический канал утечки информации в дверном проеме (тамбуре)	Основные технические характеристики: -количество независимых каналов (с повышенной мощностью) 4 (2); -полоса эффективной защиты на перекрытии толщиной 0,25 м, Гц 170-5700; -эффективный радиус действия на перекрытии толщиной 0,25 м, м 1,75 (2,5) -максимальное количество вибропреобразователей на канал, шт. 46 (23). -электропитание от сети переменного тока 220 В 50 Гц -потребляемая мощность, Вт 200. (Сертификат № 707 действителен до 28.02.2015) Перекрывает следующие каналы утечки информации: -виброакустический канал утечки информации в оконных проемах -оптико-электронный канал утечки информации в оконных проемах -виброакустический канал утечки информации через ограждающие конструкции: стены, потолок -виброакустический канал утечки информации в инженерных сооружениях: система отопления -виброакустический канал утечки информации в системе вентиляции -виброакустический канал утечки информации в дверном проеме (тамбуре)

Приложение В

Характеристики визуального осмотра

Таблица В.1 – Характеристики визуального осмотра рабочей зоны

Характеристики визуального осмотра рабочего места	
1	Свет от оконного проема падает сзади
2	Отсутствует подставка для ног
Характеристики помещения:	
1	S(LSD ВДТ/ЭТЛ ВДТ)=4,5-6,0м^2;
2	V($I_а$-$I_б$/$II_а$-$II_б$) =15/25м^3.
Характеристики освещения:	
1	Яркость потолка, стен, светильников, поверхностей
2	Яркость бликов стола и экранов компьютеров равна 40кд/м^2;
3	Освещенность в зоне расположения рабочего документа равна 300-500 лк;
4	Освещенность поверхности экрана равна до 300 лк;
5	Показатель ослепленности общего освещения равен 40;
6	Коэффициент пульсации общего освещения равен 5%.
Характеристики микроклиматических условий:	
1	Температура воздуха в теплый период равна 20-25°С;
2	Температура воздуха в холодный период равна 22-24°С;
3	Относительная влажность 40-60%;
4	Скорость движения воздуха 0,1 м/с.
Характеристики рабочей зоны:	
1	Высота стойки (разделительной перегородки) 1,5м.
Характеристики рабочего стола:	
1	Отсутствие острых краев;
2	Матовая (полуматовая) фактура поверхности стола;
3	Глубина стола не менее 800см
4	Длина одного рабочего места 1200см.

Продолжение таблицы В.1

Характеристики рабочего стула:	
1	Закругленный передний край;
2	Полумягкая поверхность сиденья, спинки и подлокотников;
3	Нескользящеене электризующееся, воздухонепроницаемое покрытие;
4	Возможность съема подлокотников;
5	Регулируемая высота;
6	Изменение угла наклона спинки на 30%.
Характеристики подставки для ног:	
1	Рифленая поверхность;
2	Регулировка высоты и угла.
Характеристики монитора:	
1	Дисплей ниже глаз пользователя и на расстоянии 600-700 см;
2	Возможность поворота по вертикали и горизонтали;
3	Матовый корпус однородного цвета;
4	Антибликовое покрытие;
5	Регулировка яркости и контраста.
Характеристики клавиатуры:	
1	Матовый корпус однородного цвета;
2	Наличие ножек и возможность изменения угла положения от 0° до15°[21].
Характеристики системного блока:	
1	Матовый корпус однородного цвета;
2	Удаленность от приборов отопления;
3	Расстояние между торцом стола и крышкой системного блока неменее 100 мм[21].