

Содержание

Введение	3
1 Назначение и цели создания системы	5
2 Описание предметной области	6
2.1 Описание объекта информатизации	6
2.2 Описание помещений объекта	8
2.3 Обследование объекта информатизации	10
3 Концепция и политика информационной безопасности организации	12
4 Постановка задачи	16
4.1 Система охранной сигнализации и оповещения	16
4.2 Система контроля и управления доступом	17
4.3 Система видеонаблюдения	18
4.4 Система технической защиты информации	19
5 Определение актуальных угроз безопасности	20
6 Модель нарушителя информационной безопасности организации	23
7 Методы и средства обеспечения информационной безопасности	
8 Реализация политики безопасности с использованием выбранных средств защиты	
9 Организационные мероприятия по обеспечению информационной безопасности	
10 Оценка стоимости реализации системы	
Заключение	
Список использованных источников	
Приложение А	

					<p>ККЭП 10.02.04 006 ПЗ</p> <p>Построение системы инженерно-технической защиты компании ООО «ИПК ОРИОН» Пояснительная записка</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33.33%;">Лит.</td><td style="width: 33.33%;">Лист</td><td style="width: 33.33%;">Листов</td></tr> <tr> <td>дп</td><td>2</td><td>-</td></tr> </table>	Лит.	Лист	Листов	дп	2	-
Лит.	Лист	Листов										
дп	2	-										
Изм.	Лист	№ докум.	Подпись	Дата								
Разраб.	Викторов											
Провер.	Копылов											
Рецензент												
Н.контр.												
Утв.												

Введение

ООО «Инженерно-проектная компания Орион» – организация, оказывающая услуги по проектированию инженерных систем безопасности. Организационная структура включает один офис в Краснодаре.

Актуальность защиты информации, протекающей в компании, обуславливается наличием большого числа потенциальных конкурентов, которые являются потенциальными угрозами для компании, или её клиентам. Защита конфиденциальности информации для большинства предприятий первостепенная задача, от качества решения которой зависит конкурентоспособность и рост места на рынке.

Деятельность и мероприятия, выполняющие задачу защиты, и обеспечивающие требуемый уровень защищённости информации в организации должны быть поддержаны соответствующей системой её защиты.

Инженерно-техническая защита – это совокупность технических средств и мероприятий, нацеленных на предотвращение утечек конфиденциальной информации, и несанкционированного доступа к ресурсам организации.

Цель работы – построение системы инженерно-технической защиты компании ООО «ИПК ОРИОН», обеспечивающей защиту критически важной информации.

Задачи:

- анализ информационных активов компании;
- создание модели нарушителя;
- проектирование системы инженерно-технической защиты информации;
- оценка стоимости реализации системы.

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

1 Назначение и цели создания системы

Инженерно-техническая защита информации (ИТЗИ) включает комплекс организационных и технических мер по обеспечению информационной безопасности (ИБ) техническими средствами. ИТЗИ подразделяется на следующие виды:

- физическая защита. К ней относятся системы охранно-пожарной сигнализации и оповещения, системы контроля и управления доступом, а также системы видеонаблюдения;
- аппаратная защита. К ней относятся электронные и механические устройства, предназначенные для защиты информации (ЗИ) и противодействия (генераторы помех, виброшторы и т.д.).

Особенностью инженерно-технической защиты является комплексность. Система ИТЗИ предназначена для решения следующих задач:

- охрана предприятия, наблюдение за территорией и помещениями, осуществление контролируемого доступа в здание;
- разграничение доступа по помещениям для сотрудников.
- предотвращение получения несанкционированного доступа (НСД) злоумышленником к носителям конфиденциальной информации (КНИ) с целью её уничтожения, хищения или изменения;
- нейтрализация технических каналов утечки информации (ТКУИ), к которым относятся:
 - 1) вибро-акустические,
 - 2) оптические,
 - 3) побочные электромагнитные излучения и наводки (ПЭМИН);
- контроль рабочего времени сотрудников;
- общая минимизация рисков утечки информации.

Изм.	Лист	№ докум.	Подпись	Дата

2 Описание предметной области

Объектом информатизации (ОИ) является информационная система ООО «Инженерно-проектная компания Орион», занимающейся разработкой проектной документации для инженерных систем безопасности, включающих в себя:

- системы контроля и управления доступом (СКУД);
- система охранной сигнализации и оповещения (СОС и СО);
- системы видеонаблюдения (СВн);
- системы технической защиты информации (СТЗИ).

Фактический место расположения здания офиса организации находится по адресу: г. Краснодар, ул. Рашилевская, д. 245.

Информационная система (ИС) данной организации располагается непосредственно в здании организации.

2.1 Описание объекта информатизации

В ИС организации циркулирует информация, составляющая персональные данные (ПДн) сотрудников и клиентов, а также сведения, составляющие коммерческую тайну. Эти сведения регулирует закон ФЗ №152 «О персональных данных», а также ФЗ №98 «О коммерческой тайне». Циркулирующие сведения более подробно представлены в таблице 1.

В данный момент офис компании находится в стадии проектирования, поэтому ещё не было разработано каких-либо инженерно-технических мер безопасности на объекте.

И отсутствие мер защиты, вроде СКУД, СВн, охранных извещателей и физических барьеров, является высоким риском уязвимости для различных видов угроз, включая НСД, вандализм и кражу оборудования. Более того, нехватка защиты приведёт не только к утечке КНИ, но и поломке самого оборудования,

Изм.	Лист	№ докум.	Подпись	Дата	Лист	5
					ККЭП 10.02.04 006 ПЗ	

предназначенного для обработки и хранения Кни, что в свою очередь будет стоить существенных финансовых потерь, вплоть до утраты данных.

Таблица 1 – Категорирование информации в организации

Информация	Тип информации	Субъекты, имеющие доступ к информации
Учётные записи (в т.ч. биометрические данные)	ДСП	отдел инженерного проектирования, отдел технической поддержки, финансовый отдел, отдел кадров, директор
ФИО, адреса, паспорта, СНИЛС, ИНН, фото сотрудников	Персональные данные	финансовый отдел, отдел кадров, директор
Финансовая и бухгалтерская документация	Коммерческая тайна	финансовый отдел, директор
Техническая и проектная документация объектов клиентов	Коммерческая тайна	отдел инженерного проектирования
Служебная переписка	ДСП	Директор

Также проблема отсутствия мер сказывается и на доверии клиентов, которые поставят под сомнение сохранность своих данных. Всё ранее перечисленное негативно влияет на репутацию компании и её дальнейшую конкурентоспособность.

Таким образом, наличие эффективных инженерно-технических мер безопасности необходимое условие для стабильной работы ОИ в целом.

2.2 Описание помещений объекта

Офис ООО «ИПК Орион» расположен на первом этаже, что также потребует дополнительной защиты окон. План этажа с помещениями представлен на рисунке 1, а также на листе 1 в графической части.

На таблице 2 представлена экспликация помещений.

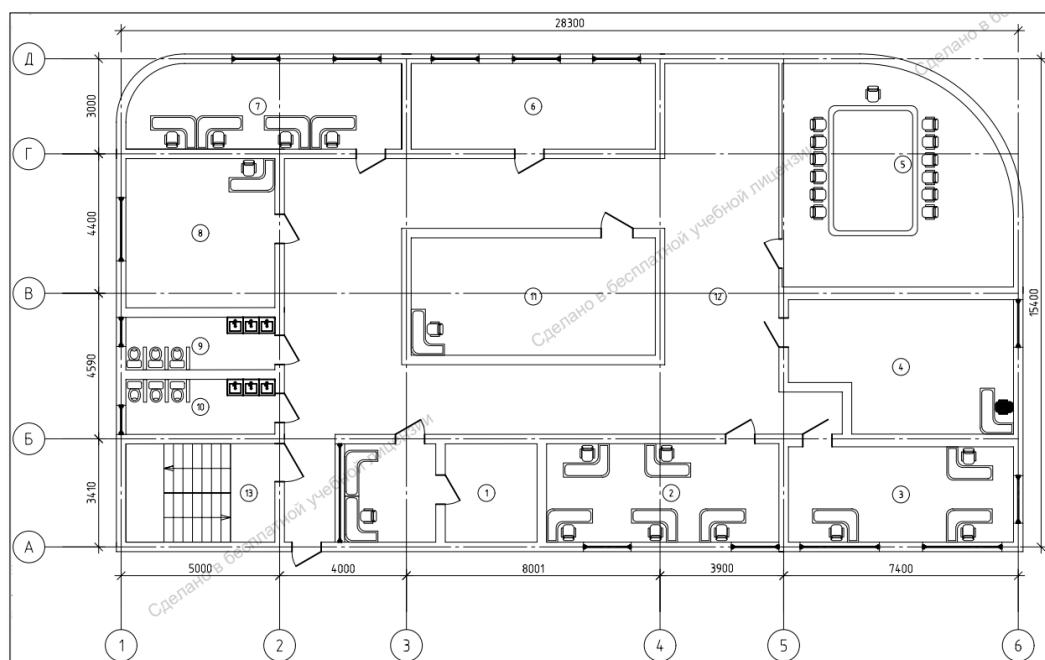


Рисунок 1 – Общий план первого этажа

Таблица 2 – Экспликация помещений

Номер	Наименование	Площадь, м ²
1	Помещение охраны	18,82
2	Финансовый отдел	22,72
3	Отдел связи с клиентами	21,36
4	Кабинет директора	26,87
5	Конференц-зал	46,42
6	Склад	20,79

Продолжение таблицы 2

Номер	Наименование	Площадь, м ²
7	Отдел кадров	22,76
8	Архив	22,09
9	Санузел женский	7,83
10	Санузел мужской	8,09
11	Серверная	28,52
12	Коридор	114,88
13	Лестничная клетка	14,57

Из всех представленных выше помещений АРМ будет отсутствовать в помещениях под номерами: 5, 6, 8, 9, 10, 12, 13.

Также Офис будет иметь подвальное помещение, предназначенное для ввода коммуникаций (водоснабжение и водоотведение, электроснабжение и газоснабжение). В качестве аварийного источника электроэнергии предусмотрена дизель-генераторная установка (ДГУ). Доступ в подвальное помещение необходимо контролировать с использованием СКУД и СВи. План данного помещения представлен на рисунке 2, а также на листе 2 в графической части.

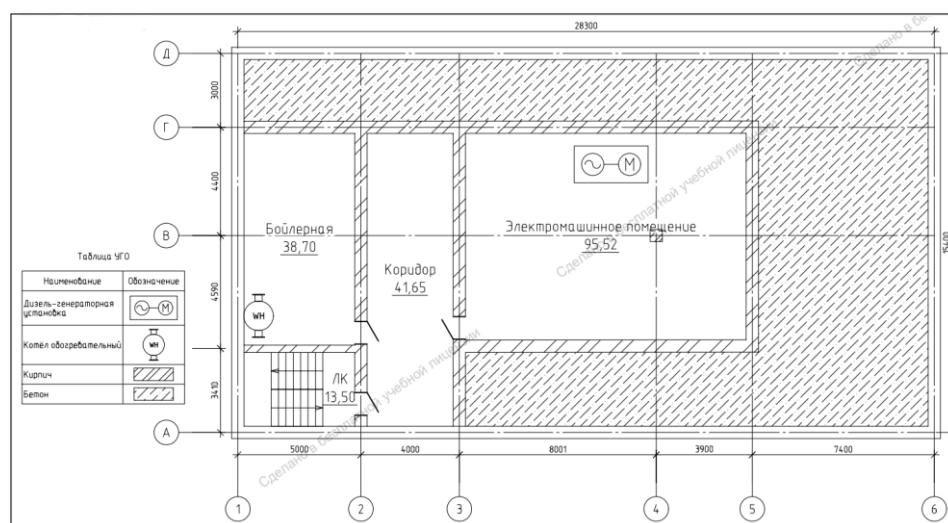


Рисунок 2 – План подвального помещения

2.3 Обследование объекта информатизации

Существует множество причин утечки информации из организации, и все они приводят к серьёзным последствиям. Также большие риски несет организация от потери имущества, которое хранится на ее территории.

Самая важная информация, которую обрабатывает организация – это ПДн клиентов и сотрудников, а также проектная документация систем безопасности. Проектная документация на бумажных носителях хранится в архиве. В зале совещаний проводятся переговоры с заказчиками, где обсуждаются конфиденциальные сведения о проектируемых объектах. На складе находится неиспользуемое или запасное оборудование. В серверной располагается оборудование, обрабатывающее и хранящее всю цифровую информацию компании.

Также потенциальную опасность представляет подвальное помещение, в котором расположены вводы основных коммуникаций здания, а также оборудование, поломка которого является материальным ущербом компании и потенциальной угрозой для жизни сотрудников.

Для построения этого комплекса необходимо определить назначение каждого помещения в офисе. В соответствии с планами этажей в таблице 3 указаны назначения всех помещений.

Изм.	Лист	№ докум.	Подпись	Дата

Таблица 3 – Назначение помещений офиса

Наименование	Назначение
Помещение охраны	Размещение приёмо-контрольных приборов СОС и СО, оборудования для хранения и управления видеоархивами, оборудования СКУД; Мониторинг систем обеспечения безопасности КЗ
Финансовый отдел	Управление финансами, бухгалтерский учёт, планирование бюджета, контроль расходов и обеспечение финансовой устойчивости организации
Отдел связи с клиентами	Установление доверительных отношений между компанией и её покупателями, получение обратной связи, предоставление технической поддержки клиентам
Кабинет директора	Рабочее пространство и место сосредоточения
Конференц-зал	Проведение рабочих заседаний, совещаний, деловых встреч, пресс-конференций, бизнес-презентаций, общих собраний
Склад	Хранение запасного оборудования
Отдел кадров	Подбор, найм и управление персоналом, оформление трудовых договоров
Архив	Хранение, учёт, использование и защита бумажных документов
Серверная	Размещение серверного и телекоммуникационного оборудования, хранение и обработка данных

Продолжение таблицы 3

Наименование	Назначение
Электромашинное помещение	Размещение оборудования для резервного источника энергии
Бойлерная	Размещение отопительного оборудования, а также ввод основных коммуникаций здания

Потенциальными местами проникновения злоумышленников на ОИ являются:

- входная дверь;
- окна
- помещения первого этажа.

Потенциальными объектами, позволяющими использовать ТКУИ являются:

- система отопления;
- система вентиляции;
- окна;
- стены.

Для сохранения безопасности организации необходимо определить контролируемую зону (КЗ), то есть территорию, на которой исключено неконтролируемое пребывание лиц, не имеющих допуска, а также право доступа определённых лиц компании к помещениям. Оптимальной границей КЗ будет периметр помещения организации.

Матрица доступа сотрудников к помещениям представлена в таблице 4.

Для комплексной защиты объекта необходимо предусмотреть установку системы охранной сигнализации и оповещения, системы контроля и управления доступом, системы видеонаблюдения и системы технической защиты информации.

Контрольные приборы для обнаружения сигналов с охранных извещателей, а также видеорегистраторы, фиксирующие данные с камер видеонаблюдения будут расположены в помещении охраны для удобства сотрудника охраны.

В соответствии с РД 78.36.006-2013 «Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1.» объекты разделяются на две группы: А и Б. Для дальнейшего построения систем ЗИ необходимо определить категорию объекта.

Опираясь на этот документ, ООО «ИПК ОРИОН» имеет категорию Б2. К этой категории относятся объекты организаций различных форм собственности, собственниками которых принято решение об установке системы тревожной сигнализации.

Проектирование СВн осуществляется в соответствии с ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний». В соответствии с этим стандартом СВн организации относится к группе II по функциональным характеристикам (с расширенными функциями). Это связано с необходимостью обеспечения записи видеоархива по расписанию и событиям, возможностью удаленного доступа к видеопотокам, регистрированием действий операторов и событий системы, а также наличием встроенного детектора движения в видеокамерах.

Изм.	Лист	№ докум.	Подпись	Дата	Лист	12
					ККЭП 10.02.04 006 ПЗ	

Таблица 4 – Матрица доступа

Объект / субъект доступа	Директор	Работники горячей линии	Бухгалтера	HR	Охрана	Системный администратор
Склад	+	-	-	-	+	+
Архив	+	-	+	-	+	-
Кабинет директора	+	-	-	-	+	+
Серверная	+	-	-	-	+	+
Помещение охраны	+	-	-	-	+	+
Финансовый отдел	+	-	+	+	+	+
Отдел связи с клиентами	+	+	-	-	+	+
Конференц-зал	+	+/-	+/-	+/-	+	+
Отдел кадров	+	-	+	+	+	+

В таблице определено разграничение доступа сотрудников по отношению к помещениям. Знаком «+» определён полный неограниченный доступ соответствующей должности, «-» – наоборот, сотрудник соответствующей должности не имеет права доступа в данное помещение. Знак «+/-» необходим для определения помещений, доступ в которые по-умолчанию не требуется соответствующим должностям сотрудников, однако, по распоряжению директора они получают временный доступ для проведения общих собраний.

С расширением штата или усложнения должностных инструкций сотрудников следует актуализировать и дополнять матрицу доступа.

3 Концепция и политика информационной безопасности организации

Политика безопасности любой организации является неотъемлемой частью обеспечения информационной безопасности внутри нее. Она определяет требования к информационной системе с точки зрения защиты ее материальных и информационных ресурсов. Основная ее задача заключается в предотвращении инцидентов информационной безопасности.

Политика безопасности ООО «ИПК Орион» разрабатывается на основании следующих нормативно-правовых актов:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методика оценки угроз безопасности информации, утвержденная Приказом ФСТЭК России от 5 февраля 2021 года.

Политика информационной безопасности также разграничивает доступ сотрудников к информационным ресурсам и физическим помещениям. Таким образом, сотрудники отдела связи с клиентами не имеют доступа к складу, архиву и серверной. Сотрудники финансового отдела имеют доступ только к своему рабочему месту и не попадут в подвальное помещение без разрешения.

Доступ в серверную имеет только системный администратор и директор организации. В зал совещаний неограниченный доступ имеют директор, охрана и системный администратор.

Изм.	Лист	№ докум.	Подпись

Остальные же сотрудники посещают данное помещение только по распоряжению директора.

В результате разработки и применения матрицы (таблица 4) доступа будут уменьшены риски, связанные с нарушением должностных инструкций сотрудников, а также усилится безопасность организации. Также ее применение упрощает управление правами сотрудников и помогает выявлять внутренних нарушителей.

Также политика безопасности должна предусматривать инженерно-технические методы защиты информации, такие как:

- СКУД;
- СОС и СО;
- СВн;
- СТЗИ.

Эти методы помогут создать многоуровневую систему защиты информации и повысят общий уровень безопасности в организации.

Изм.	Лист	№ докум.	Подпись	Дата	Лист
					15

4 Постановка задачи

Задача курсового проекта заключается в построении системы инженерно-технической защиты информации для организации ООО «ИПК ОРИОН», которая обеспечит комплексную защиту объекта информатизации от НСД и утечки КИ.

Для этого необходимо определить назначение и функционал каждой подсистемы по отдельности.

4.1 Система охранной сигнализации и оповещения

СОС и СО являются базовыми подсистемами комплекса ИТЗИ и обеспечивают своевременное обнаружение попыток проникновения на объект и в защищаемые помещения (ЗП), а также оперативное оповещение службы безопасности.

С учётом требований РД 78.36.006-2013, регламентирующего выбор и применение технических средств охранной и тревожной сигнализации и средств инженерно-технической укреплённости, для объектов категорий Б1–Б2 предусматривается многорубежная охрана периметра и внутренних помещений.

Основные задачи СОС и СО для офиса ООО «ИПК ОРИОН» формулируются следующим образом:

- обеспечение многорубежной защиты периметра и помещений объекта:
 - 1) рубеж дверей и окон (вибро-акустические и магнитоконтактные датчики);
 - 2) рубеж ЗП (оптико-электронные датчики);
- контроль целостности инженерно-технических преград (двери, замки, окна);
- непрерывный мониторинг состояния КЗ, включая:
 - 1) контроль взятия/снятия зон под охрану;

Изм.	Лист	№ докум.	Подпись	Дата	Лист	16
					ККЭП 10.02.04 006 ПЗ	

- 2) контроль состояния шлейфов сигнализации, линий связи и источников питания;
- 3) автоматическую диагностику отказов технических средств;
- формирование и передача извещений о тревоге на пульт приёмо-контрольный (ППК);
 - управление звуковыми оповещателями, обеспечивающими локальное предупреждение персонала и потенциального нарушителя о факте обнаружения проникновения;
 - интеграция с инженерно-технической укреплённостью объекта:
- 1) выбор мест установки извещателей с учётом конструкции стен, перекрытий, дверей и засвета с окон;
 - 2) соблюдение требований РД 78.36.006-2013 к прокладке линий сигнализации и электропитания (скрытая прокладка, защита от механических повреждений).
- обеспечение резервирования электропитания технических средств СОС и СО на время, достаточное для реагирования на инцидент, в соответствии с требованиями к надёжности и электробезопасности, установленными в нормативных документах на охранные системы.

4.2 Система контроля и управления доступом

СКУД предназначена для реализации пропускного и внутриобъектового режимов, разграничения доступа в ЗП и ведения учёта рабочего времени персонала. Она проектируется в соответствии с ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».

Для данного ОИ СКУД необходимо поддерживать следующие функции:

- разграничение доступа в соответствии с таблицей 4;

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

- идентификация и аутентификация пользователей на точках доступа с использованием специальных идентификаторов (например, карты Proximity, банковские карты, биометрия);
- управление исполнительными устройствами (например, замки, турникеты, электрозашёлки), включающее в себя:
 - 1) принятие решений о разрешении или запрете прохода;
 - 2) контроль состояния двери (фиксация попыток принудительного вскрытия);
 - 3) автоматическая блокировка точек доступа при срабатывании СОС;
- ведение журнала событий доступа, содержащих уникальные метки (дата и время, идентификатор пользователя), а также тревожных событий (вскрытие, недействительный идентификатор, неверный ввод PIN-кода);
- реализация временных или ограниченных допусков для клиентов или партнёров компании;
- интеграция с другими подсистемами (СВн, СОС)

4.3 Система видеонаблюдения

СВн предназначена для визуального контроля обстановки на объекте и вокруг него, фиксации событий, связанных с безопасностью и документирования инцидентов путём записи их в видеоархив. Сама это система является не надёжным препятствием для потенциального нарушителя, а только сдерживающим фактором. Также благодаря видеоархиву СВн помогает в расследовании инцидентов.

При её проектировании учитываются требования ГОСТ Р 51558-2014 «СРЕДСТВА И СИСТЕМЫ ОХРАННЫЕ ТЕЛЕВИЗИОННЫЕ. Классификация. Общие технические требования. Методы испытаний».

Изм.	Лист	№ докум.	Подпись	Дата	Лист	18
					ККЭП 10.02.04 006 ПЗ	

СВн для ОИ предоставляет следующие функции:

- непрерывный визуальный контроль КЗ объекта (входная группа, коридоры);
- получение доступа к камерам удалённо с использованием информационно-телекоммуникационной системы «Интернет» (далее Интернет);
- непрерывная запись видеопотоков в видеоархив;
- обнаружение тревожных событий средствами видеоаналитики и оповещение сотрудника охраны;
- взаимодействие с другими подсистемами ИТЗИ;

4.4 Система технической защиты информации

СТЗИ формируется для нейтрализации ТКУИ (вибро-акустический, оптический, ПЭМИН). Она проектируется в соответствии со «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утверждёнными приказом Гостехкомиссии России от 30.08.2002 № 282.

Согласно п. 2.2 СТР-К, требования документа распространяются в том числе на ПДн, а также на иную КНИ, обрабатываемую в автоматизированных системах, что делает его применимым к ИСПДн данного ОИ.

Исходя из этого, для офиса ООО «ИПК ОРИОН» подсистема СТЗИ должна решать задачу обеспечения защиты речевой (акустической) и визуальной (оптической) информации в защищаемых помещениях (зал совещаний). Для этого будут использованы следующие меры:

- обеспечение требуемого уровня звукоизоляции ограждающих конструкций и перегородок, систем вентиляции и кондиционирования;
- применение активных средств акустического и вибро-акустического зашумления (генераторы шума, виброшторы).

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

5 Определение актуальных угроз безопасности

Согласно Методическому документу «Методика оценки угроз безопасности», утверждённому ФСТЭК от 5 февраля 2021 г. (далее Методический документ ФСТЭК), для оценки потенциальных угроз ИБ исходными данными являются:

- нормативные правовые акты РФ;
- документация на системы и сети (ТЗ, конструкторская и эксплуатационная документация);
- структура компании.

Основными задачами, решаемыми в ходе оценки УБИ являются:

- определение объектов воздействия и негативных последствий, возникающих от реализации УБИ;
- определение источников УБИ и оценка их возможностей;
- оценка возможности реализации и определение актуальности УБИ.

К объектам организации, подверженным воздействию, относятся:

- база данных ИС, располагаемая в серверной;
- АРМ сотрудников, расположенных в офисных помещениях;
- материальные активы организации (например, оборудование);
- критическая инфраструктура (электромашинное и бойлерное помещения, серверная);
- физические барьеры (окна, двери).

Возможные виды воздействия:

- хищение КнИ из базы данных;
- нарушение целостности данных;
- хищение КнИ с АРМ сотрудников;
- нарушение работы организации из-за невозможности решения поставленных задач или снижения эффективности их решения.

Изм.	Лист	№ докум.	Подпись	Дата	Лист	20
					ККЭП 10.02.04 006 ПЗ	

Для организации ООО «ИПК Орион» характерные следующие пути реализации угроз в отношении инженерно-технической системы защиты информации:

- использование социальной инженерии для несанкционированного доступа на закрытые участки контролируемой зоны;
- хищение или повреждение оборудования;
- потеря материальных носителей информации;
- потеря электронных пропусков;
- выведение из строя систем безопасности;
- повреждение коммуникаций здания;
- перехват информации с использованием технических каналов утечки информации.

В целях структуризации и формализации сведений по возможным методам реализации угроз, а также определения мер противодействия была составлена таблица 5.

Таблица 5 – Вероятные угрозы

Угроза	Степень ущерба	Вероятность	Меры
Повреждение или выведение из строя оборудования в результате внешних воздействий	Средняя	Низкая	Организация охраны помещений с использованием СВн и СКУД
Социальная инженерия	Средняя	Высокая	Использование СКУД и СВн, инструктаж сотрудников, учёт рабочего времени

Продолжение таблицы 5

Нарушение условий эксплуатации	Средняя	Высокая	Инструктаж сотрудников
Разрушение ограждающих конструкций	Средняя	Низкая	Использование СВн и СОС
Нарушение электроснабжения	Высокая	Низкая	Использование СКУД и СВн
Съём КнИ с технических каналов утечки информации	Высокая	Низкая	Использование системы технической защиты информации

Исходя из таблицы определяется следующий вывод – вероятность возникновения угроз в среднем довольно низкая, однако, в случае возникновения одной из них компания понесёт значительный или крупный ущерб. Поэтому снабжение офиса компании ООО «ИПК Орион» системой инженерно-технической защиты информации имеет обязательный характер

6 Модель нарушителя информационной безопасности организации

Для актуальных нарушителей определены следующие категории в зависимости от имеющихся прав и условий по доступу к системам:

– внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;

– внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей. Они также имеют намеренные и непреднамеренный характеры.

В таблице 6 представлены основные виды нарушителей, присущих ООО «ИПК Орион» и их возможностей, подлежащих оценке, согласно Методическому документу ФСТЭК.

Таблица 6 – Основные виды нарушителей

Виды нарушителей	Категория	Уровень возможностей
Террористические, экстремистские группировки	Внешние	H3
Конкурирующие организации	Внешние	H2
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внешние	H2
Авторизованные пользователи систем и сетей	Внутренние	H1

Продолжение таблицы 6

Системные администраторы и администраторы ИБ	Внутренние	H2
Бывшие (уволенные) работники (пользователи).	Внешние	H1
Системные администраторы	Внутренние	

фвы

7 Методы и средства обеспечения информационной безопасности

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ККЭП 10.02.04 006 ПЗ

Лист
25

8 Реализация политики безопасности с использованием выбранных средств защиты

Защита от утечки КИ с АРМ и БД, находящихся в серверной, с использованием ПЭМИН.	Размещение слаботочных, силовых и заземляющих кабельных линий с учётом требований по минимизации ПЭМИН (раздел 5 СТР-К)
	Создание локальных экранированных зон (шкаф)
	Использование средств активной ЗИ от утечек за счёт ПЭМИН (например, Соната-Р3.1)
Исключение утечки через вспомогательные технические средства и системы (ВТСС), размещённых в защищаемых помещениях (извещатели СОС, периферийные устройства, телекоммуникационное оборудование).	Исключение использования беспроводных точек доступа (видеокамеры, смартфоны) без надлежащей защиты передаваемого трафика
Реализация организационно-режимных мер, предусмотренных СТР-К.	Использование сертифицированной продукции СОС
	Документальное закрепление перечня ЗП и ответственных лиц, ведение технических паспортов ЗП и ОИ
	Установление порядка регулярной проверки помещений с привлечением организаций по аттестации (ОпА)
	Регламентация доступа в ЗП, хранения и использования средств звукозаписи и носителей информации, содержащих КИ и пдн.

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

9 Организационные мероприятия по обеспечению информационной
безопасности

Изм.	Лист	№ докум.	Подпись	Дата

ККЭП 10.02.04 006 ПЗ

Лист

27

10 Оценка стоимости реализации системы

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ККЭП 10.02.04 006 ПЗ

Лист

28

Заключение

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ККЭП 10.02.04 006 ПЗ

Лист
29

Список использованных источников

Изм.	Лист	№ докум.	Подпись	Дата	Лист	30
					ККЭП 10.02.04 006 ПЗ	

Приложение А

(обязательное)

Техническое задание на разработку системы инженерно-технической защиты информации инженерно-проектной компании «ИПК Орион»

Техническое задание направлено на определение ключевых требований для создания комплекса систем инженерно-технической защиты информации офиса ООО «ИПК ОРИОН», специализирующегося на разработке проектной документации для инженерных систем безопасности.

Так как данный ОИ находится в стадии проектирования, то каких-либо инженерно-технических мер безопасности спроектировано ещё не было. Её отсутствие создаёт высокий риск уязвимости для различных видов угроз, включая несанкционированный доступ, утечку КнИ, вандализм и кражу оборудования.

Для обеспечения защиты ОИ необходимо реализовать совокупность связанных между собой подсистем инженерно-технической защиты:

- СОС и СО;
- СКУД;
- СВ;
- СТЗИ.

Система должна обеспечивать:

- защиту КнИ от утечки;
- разграничение доступа к помещениям;
- обнаружение и предупреждение о несанкционированном проникновении;
- видеофиксация событий безопасности;

Особое внимание следует уделить КЗ с залом для совещаний, где необходимо установить технические средства для защиты от вибро-акустического и оптического считывания с окон информации, оглашаемой во время переговоров.

Изм.	Лист	№ докум.	Подпись

ККЭП 10.02.04 006 ПЗ

Лист

31

Также необходимо защитить серверное помещение от считывания информации через побочные электромагнитные излучения и наводки (ПЭМИН).

Осуществление этих мер значительно повысит уровень безопасности на инженерно-проектной компании «ИПК Орион», обеспечивая соблюдение современных стандартов защиты.

Изм.	Лист	№ докум.	Подпись	Дата

ККЭП 10.02.04 006 ПЗ

Лист

32

Приложение Б

(справочное)

Описание микросхем

Изм.	Лист	№ докум.	Подпись	Дата

ККЭП 10.02.04 006 ПЗ

Лист

33