

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 КНИ.

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;

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 укрепленностью 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

ККЭП 10.02.04 006 ПЗ

Лист

17

– идентификация и аутентификация пользователей на точках доступа с использованием специальных идентификаторов (например, карты Proximity, банковские карты, биометрия);

– управление исполнительными устройствами (например, замки, турникеты, электрозащёлки), включающее в себя:

1) принятие решений о разрешении или запрете прохода;

2) контроль состояние 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 эта 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

ККЭП 10.02.04 006 ПЗ

Лист

18

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

ККЭП 10.02.04 006 ПЗ

Лист

19

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.

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

					ККЭП 10.02.04 006 ПЗ	Лист
Изм.	Лист	№ докум.	Подпись	Дата		32