Учебное пособие

В.А. Рыжова

ПРОЕКТИРОВАНИЕ И ИССЛЕДОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Санкт-Петербург ИТМО

В.А. Рыжова

ПРОЕКТИРОВАНИЕ И ИССЛЕДОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Учебное пособие

Санкт-Петербург
2013

Рыжова В.А. Проектирование и исследование комплексных систем безопасности. – СПб: НИУ ИТМО, 2013. – 156 с.

В пособии изложены основные вопросы по проектированию комплексных систем безопасности. Рассмотрены общие принципы организации защиты объектов, структурные и функциональные особенности технических средств обеспечения безопасности, а также способы объединения различных подсистем безопасности в интегрированный комплекс с учетом специфики конкретного объекта.

Учебное пособие предназначено для студентов по направлению подготовки бакалавров и магистров 200400 – «Оптотехника» и по специальности 200401 – "Электронные и оптико-электронные приборы и системы специального назначения".

Рекомендовано Учебно-методическим объединением вузов Российской Федерации по образованию в области приборостроения и оптотехники для студентов высших учебных заведений, обучающихся по направлению подготовки магистров 200400 «Оптотехника» и специальности 200401 – "Электронные и оптико-электронные приборы и системы специального назначения". Протокол №8 от 19.10.2012.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Содержание

ВВЕДЕНИЕ

Исследование вопросов эффективного обеспечения безопасности населения и промышленных объектов в современных условиях является особенно актуальным в связи с активизацией угроз международного терроризма и техногенных катастроф, а также ростом квалифицированных преступных посягательств, экономической нестабильностью, компьютерными преступлениями, промышленным шпионажем.

Решение задач охраны объектов основано на применении комплекса технических средств сигнализации, которые должны зафиксировать приближение или начало действий различных угроз — от пожара и аварий до попыток проникновения на объект или в компьютерную сеть.

При выборе и установке сигнализации на объектах уделяется особое внимание достижению высокой защищенности аппаратуры от ее преодоления. Существуют различные способы реализации этой задачи:

- контроль вскрытия аппаратных блоков;
- автоматическая проверка исправности технических средств;
- защита доступа к управлению аппаратурой с помощью кодов;
- архивирование событий;
- защита информационных потоков между составными частями сигнализации методами маскирования и шифрования и др.

Таким образом, проектирование эффективной системы сигнализации с учетом программно-аппаратных средств ее защиты от обхода злоумышленником является сложнейшей многоплановой задачей, решение которой невозможно без глубоких и исчерпывающих знаний о структуре, функциональных возможностях и принципах работы системы.

Охранные сигнализации можно разделить на две группы, в зависимости от того, на каких объектах они устанавливаются:

- аппаратура, применяемая на объектах народного хозяйства, как правило, охраняемых подразделениями ГУВО МВД России;
- аппаратура, применяемая на объектах, охрана которых, как правило, не находится в ведении ГУВО МВД России.

К первой группе относятся технические средства, номенклатура которых строго ограничена, регламентируется общегосударственными нормативными документами, а информация – открыта и общедоступна.

Ко второй группе относятся технические средства, номенклатура которых не ограничена, сведения о принципах и особенностях построения излагаются в закрытой печати, передача тревожной информации выполняется как на локальные звуковые и световые сигнализаторы, так и на удаленные стационарные или носимые пульты по телефонным линиям, специальным радиоканалам, посредством систем сотовой связи.

Повышение эффективности систем сигнализации на объектах в условиях резкого обострения криминогенной обстановки невозможно без

разработки и внедрения наукоемких интегрированных комплексных систем безопасности (ИКСБ). Проектирование ИКСБ основано на реализации идей системной концепции обеспечения комплексной безопасности объекта с параллельным решением задач автоматизации управления такими системами жизнеобеспечения объекта, как энергоснабжение, вентиляция, отопление, водоснабжение, лифтовое оборудование, кондиционирование и т.д.

Проектирование ИКСБ является одним из определяющих факторов, способных сократить убытки от наступления противоправных действий, чрезвычайных ситуаций, стихийных бедствий, а также расходы на устранение последствий указанных событий.

Системный подход к проектированию систем безопасности позволяет вскрыть и учесть следующие основные недоработки и несовершенства:

– в области издания нормативной документации с учётом изменившейся обстановки в государстве, создания устоявшегося рынка безопасных услуг и появления технических средств защиты нового поколения;

– в технических средствах защиты как отечественного, так и зарубежного производства, которые из-за некорректных конструкторских решений не могут быть максимально эффективно использованы в проектируемых системах безопасности без дополнительных доработок на местах;

– в проектных решениях, разработанных неспециализированными организациями, использующих технические средства защиты, которые морально устарели и не обеспечивают логики работы проектируемой системы в соответствии с требованиями нормативных документов, что приводит к бесполезному расходованию финансов;

– в отсутствии общего понимания значений терминов и понятий, используемых в технических описаниях на приборы, инструкциях, рекомендациях, особенно в журнальных статьях;

– в разобщённости действий, направленных на создание систем безопасности между заводами изготовителями, проектными, монтажными, эксплуатационными организациями и конечным потребителем, осуществляющим функцию управления, использования установленной системы безопасности;

– в уровне технической подготовки эксплуатационных структур установленной системы безопасности.

Таким образом, для решения прикладных проблем построения эффективных систем защиты, необходимо рассмотреть следующие вопросы структурных и функциональных особенностей комплексных систем безопасности:

– общие представления об охране и защите объектов;

– термины и определения, структурные схемы и состав объединенной, комплексной, интегрированной систем безопасности;

– основы системного подхода к решению проблем защиты и охраны;

– основы систематизации и классификации объектов охраны, угроз, моделей нарушителей, технических средств охраны, т.е. всего того, что нужно знать и понимать до того, как приступать к созданию систем безопасности объектов;

– принципы формирования зон обеспечения безопасности на объекте;

– принципы построения, состав и особенности проектирования систем охранно-пожарной и тревожной сигнализации, телевизионных систем безопасности, систем контроля и управления доступом;

– общие вопросы процедуры проектирования систем безопасности и оценки их эффективности.

Динамика мирового развития программно-аппаратных технических средств обеспечения комплексной безопасности объектов диктует необходимость не только изучения современных средств, но и отслеживания тенденций их развития в перспективе. Такой мониторинг позволяет проводить упреждающие разработки в области охранной техники, аналоги которых ожидаются к появлению в ближайшее время.

1 ОБЩИЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ОБЪЕКТОВ

Осуществление мероприятий по обеспечению превентивной и адекватной безопасности населения и промышленных объектов [50, 51] представляет собой сложный непрерывный процесс, а не одноразовые или случайные действия, которые выполняются от случая к случаю по мере возникновения необходимости и вносят несогласованность в работу различных служб.

Непрерывное и стабильное функционирование любого объекта невозможно без организации надежной защиты, включающей в себя комплекс мер, направленных на выявление основных угроз и опасных ситуаций, оценки ущерба при осуществлении этих угроз и создания системы комплексной безопасности объекта при определенных ограничениях (например, на стоимость системы).

Безопасность защищаемого объекта – это состояние защищенности объекта от угроз причинения ущерба (вреда) жизни или здоровью людей; имуществу физических или юридических лиц; государственному или муниципальному имуществу; техническому состоянию, инфраструктуре жизнеобеспечения; внешнему виду, интерьеру(ам), ландшафтной архитектуре; окружающей природной среде [15].

Противокриминальная безопасность объекта – это состояние защищенности объекта, которое характеризуется отсутствием недопустимого риска или угроз различного типа и обеспечивается комплексом защитных мер [11].

Для организации эффективной защиты необходимо разработать обобщенную системную концепцию безопасности [26, 27, 47, 48], которая в каждом конкретном случае должна быть адаптирована к конкретному объекту, исходя из условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и прочих факторов. Концепция безопасности представляет собой общий замысел организации технических и организационных мероприятий по защите объекта от прогнозируемых угроз. Исходя из ее положений, разрабатывается проект оснащения объекта инженерно-техническими, специальными и программно-аппаратными средствами безопасности.

Концепция обеспечения комплексной безопасности объекта предназначена для решения следующих задач:

– определение целей или предметов защиты, иначе, "кого или что защищать?" (объект – квартира, офис, предприятие);

– определение и оценка угроз, иначе, "от какого посягательства защищать?" (случайный хулиган, рецидивист или организованная группа);

– разработка и реализация адекватных мер защиты, иначе, "чем и как защищать?" (что должна сделать охранная система, чтобы предотвратить или уменьшить ущерб).

Для этого необходимо провести анализ уязвимости объекта и существующей системы защиты [18, 48].

Уязвимость (объекта) – это степень несоответствия принятых мер по защите объекта прогнозируемым угрозам или заданным требованиям безопасности.

Целями и задачами проведения анализа уязвимости являются:

а) определение важных для жизнедеятельности объекта предметов защиты (наиболее вероятных целей злоумышленных акций нарушителей);

б) определение возможных угроз и моделей вероятных исполнителей угроз (нарушителей);

в) оценка возможного ущерба от реализации прогнозируемых угроз безопасности;

г) оценка уязвимости объекта и существующей системы безопасности;

д) разработка общих рекомендаций по обеспечению безопасности объекта.

Работы по п.п. а-в проводятся методом экспертных оценок комиссией, в состав которой входят специалисты соответствующих служб заказчика: безопасности, главного технолога, главного инженера, пожарной охраны. Работы по п.п. г-д проводятся с применением метода математического моделирования.

Рассмотрим существующие классификации объектов охраны, на которых размещаются предметы защиты, возможные угрозы и модели вероятных нарушителей.

1.1 Классификация предметов защиты и объектов охраны

Охраняемый объект – это предприятие, организация, жилище, их часть или комбинация, оборудованные действующей системой охраны и безопасности [36].

Реализацию жизненно важных интересов любого предприятия обеспечивают его корпоративные ресурсы [47, 50]. Эти ресурсы должны быть надежно защищены от прогнозируемых угроз безопасности. Для промышленного предприятия такими важными для жизнедеятельности ресурсами, а, следовательно, предметами защиты являются:

- люди (персонал предприятия);
- имущество:
  - важное или дефицитное технологическое оборудование;
  - секретная и конфиденциальная документация;
  - материальные и финансовые ценности;
  - готовая продукция;

- интеллектуальная собственность (ноу-хау);
- средства вычислительной техники;
- контрольно-измерительные приборы и др.;

- информация конфиденциальная (на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях);
- финансово-экономические ресурсы, обеспечивающие эффективное и устойчивое развитие предприятия (капитал, коммерческие интересы, бизнес-планы, договорные документы и обязательства и т.д.).

Утрата перечисленных ресурсов ведет к следующим событиям:

- значительному материальному ущербу;
- созданию угрозы для жизни и здоровья людей;
- разглашению конфиденциальной информации или сведений, содержащих Государственную или коммерческую тайну;
- банкротству предприятия.

Перечисленные предметы защиты размещаются на соответствующих производственных объектах предприятия в зданиях и помещениях. Эти объекты и являются наиболее уязвимыми местами, выявление которых производится при обследовании объекта.

Таким образом, формулируется ответ на вопрос "что защищать?" [40]: жизнь и здоровье граждан; имущество, документы, денежные средства и иные ценности физических и юридических лиц, находящиеся на стационарных и подвижных объектах, а также собственно стационарные и подвижные объекты:

- здания, строения, сооружения, их отдельные части или помещения; территории, занимаемые ими, или прилегающие к ним, отдельные территории, отдельные предметы;
- транспортные средства (автомобильный, железнодорожный, водный, воздушный транспорт).

Надежность защиты перечисленных объектов определяется наличием инженерных средств защиты на путях возможного проникновения нарушителей. Совокупность этих средств определяет инженерно-техническую укрепленность защищаемого объекта.

К инженерным средствам защиты относятся различные заборы, ограждения, решетки, жалюзи, ставни, замки, засовы, специальным образом укрепленные двери, ворота, стены, полы, потолки, оконные проемы, воздуховоды и другие элементы строительных конструкций. Инженерные средства защиты увеличивают время, необходимое нарушителю для их преодоления, что делает более вероятной возможность его обнаружения и задержания, особенно если эти средства используются в сочетании с

техническими средствами охраны (охранной сигнализацией, системами охранного телевидения и т.п.).

Таким образом, **инженерно-техническая укрепленность объекта** – это совокупность мероприятий, направленных на усиление конструктивных элементов зданий, сооружений, помещений и защищаемых территорий, обеспечивающих необходимое и достаточное противодействие несанкционированному проникновению нарушителя в защищаемую зону, взлому и другим преступным посягательствам [36, 39].

Требования к инженерно-технической укрепленности объекта защиты формулируются с учетом его категории, его строительными и архитектурно-планировочными решениями, режимом работы и многими другими факторами, которые необходимо учитывать при проектировании комплексной системы безопасности.

Категория охраняемого объекта – это комплексная оценка объекта, учитывающая его экономическую или иную (например, культурную) значимость, в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой охраны [36].

Особо важный объект – объект, значимость которого определяется органами государственной власти Российской Федерации или местного самоуправления с целью определения мер по защите интересов государства, юридических и физических лиц от преступных посягательств и предотвращения ущерба, который может быть нанесен природе и обществу, а также от возникновения чрезвычайной ситуации.

Объект жизнеобеспечения – совокупность жизненно важных материальных, финансовых средств и услуг, сгруппированных по функциональному предназначению и используемых для удовлетворения жизненно необходимых потребностей населения (например, в виде продуктов питания, жилья, предметов первой необходимости, а также в медицинском, санитарно-эпидемиологическом, информационном, транспортном, коммунально-бытовом обеспечении).

Объект повышенной опасности – объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво-, пожароопасные, опасные химические и биологические вещества, создающие реальную угрозу возникновения источника чрезвычайной ситуации.

В зависимости от категории значимости все объекты, их помещения и территории подразделяются на четыре группы: АI и АII, БI и БII.

Объекты группы АI (особо важные объекты высокой ценности или высокой опасности):

– объекты особо важные, повышенной опасности и жизнеобеспечения, включенные в Перечень объектов подлежащих

государственной охране согласно постановлению Правительства Российской Федерации от 14 августа 1992 г. № 587;

– объекты, включенные органами власти субъектов Российской Федерации или местного самоуправления в перечни объектов особо важных, повышенной опасности и жизнеобеспечения;

– объекты по производству, хранению и реализации наркотических веществ, сильнодействующих ядов и химикатов, токсичных и психотропных веществ и препаратов (базы аптекоуправления, аптеки, склады медрезерва, научные, медицинские и другие учреждения, заведения, в практике которых используются эти вещества);

– ювелирные магазины, базы, склады и другие объекты, использующие в своей деятельности ювелирные изделия, драгоценные металлы и камни;

– объекты и помещения для хранения оружия и боеприпасов, радиоизотопных веществ и препаратов, предметов старины, искусства и культуры;

– объекты кредитно-финансовой системы (банки, операционные кассы вне кассового узла, дополнительные офисы, пункты обмена валюты, банкоматы);

– кассы предприятий, организаций, учреждений, головные кассы крупных торговых предприятий;

– сейфовые комнаты, предназначенные для хранения денежных средств, ювелирных изделий, драгоценных металлов и камней;

– другие аналогичные объекты и имущественные комплексы.

Объекты группы АII (наиболее опасные помещения на объектах группы АI):

– хранилища и кладовые денежных и валютных средств, ценных бумаг;

– хранилища ювелирных изделий, драгоценных металлов и камней;

– хранилища секретной документации, изделий;

– специальные хранилища взрывчатых, наркотических, ядовитых, бактериологических, токсичных и психотропных веществ и препаратов;

– специальные фондохранилища музеев и библиотек.

Объекты группы БI (объекты розничной торговли и пр.):

– объекты с хранением или размещением изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и другого имущества;

– объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски и другие аналогичные объекты).

Объекты группы БII (объекты категории Б, содержащие алкогольную продукцию или наиболее компактные легкосбываемые товары – электронику, товары повседневного спроса):

– объекты с хранением или размещением товаров, предметов повседневного спроса, продуктов питания, компьютерной техники, оргтехники, видео- и аудиотехники, кино- и фотоаппаратуры, натуральных и искусственных мехов, кожи, автомобилей и запасных частей к ним, алкогольной продукции с содержанием этилового спирта свыше 13% объема готовой продукции и другого аналогичного имущества.

Каждой группе объектов должен соответствовать определенный класс защиты конструктивных элементов (ограждающих конструкций и элементов инженерно-технической укрепленности), а также технических средств обеспечения комплексной безопасности. При этом регламентируется соответствие характеристик элементов первого класса минимально необходимой степени защиты, второго класса – средней, третьего класса – высокой и четвертого класса – специальной степени защиты объекта от проникновения. Чем ниже уровень требований к инженерно-технической укрепленности объекта, тем меньше средств потребуется для организации его эффективной охраны.

В области противокриминальной защиты также разработан технический регламент [40], описывающий классификацию объектов в зависимости от предполагаемых угроз и устанавливающий разные классы защиты в соответствии с выявленным уровнем угрозы.

В зависимости от степени потенциальной опасности, а также возможных последствий в случае реализации криминальных угроз объекты подразделяются на три основные группы:

– критически важные и потенциально опасные объекты;
– социально значимые объекты;
– объекты сосредоточения материальных ценностей.

Кроме того, в зависимости от вида и размеров ущерба, который может быть нанесен объекту, находящимся на нём людям и имуществу в случае реализации криминальных угроз принята следующая классификация:

– класс I (высокая значимость) – ущерб приобретет федеральный или межрегиональный масштаб;
– класс II (средняя значимость) – ущерб приобретет региональный или межмуниципальный масштаб;
– класс III (низкая значимость) – ущерб приобретет муниципальный или локальный масштаб.

В зависимости от класса объекта и вида находящегося (хранящегося) на нем имущества устанавливают классы защиты объектов.

Дальнейший анализ потенциальных угроз и уязвимых мест объекта позволяет проектировать адекватную систему охраны с использованием рекомендованных видов оборудования, которые соответствуют установленному классу значимости и группе опасности объекта.

Таким образом, учет классификаций объектов по степени их значимости, а также по размерам потенциального ущерба от реализации

угроз необходим для приближенной оценки возможных затрат на оснащение объектов инженерно-техническими, специальными и аппаратно-программными средствами защиты.

1.2 Классификация нарушителей и потенциальных угроз безопасности

Для ответа на вопрос "от какого посягательства защищать объект?" необходимо определить возможные угрозы предметам защиты (внутренние и внешние) и модели вероятных исполнителей угроз (нарушителей).

Угроза безопасности – это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. **Угроза криминальная** – это совокупность условий и факторов, создающих опасность преднамеренного противоправного нанесения ущерба объекту и имуществу, здоровью и жизни физического лица, хищение материальной и интеллектуальной собственности [11].

Источниками угрозы могут выступать человек, техногенная среда и природа. К основным угрозам можно отнести:

- угрозы жизни, здоровью, личным правам и свободам человека;
- угрозы материальным и культурным ценностям, физическим носителям информации;
- угрозы экономической деятельности;
- угрозы общественной безопасности;
- угрозы информационной безопасности;
- угрозы юридической деятельности;
- угрозы чрезвычайных ситуаций;
- угрозы отказа оборудования.

В связи с широким спектром угрожающих факторов безопасность защищаемого объекта должна быть комплексной для решения следующих важных задач:

- поддержание безопасного состояния объекта;
- предупреждение угроз;
- обнаружение угроз;
- противодействие угрозам;
- ликвидация последствий максимального количества из полного набора возможных угроз для данного объекта.

В частности, задача системы безопасности заключается в обнаружении и пресечении действий людей, пытающихся тайно или открыто (но несанкционированно) проникнуть на охраняемую территорию объекта. В современных условиях несанкционированные действия физических лиц (диверсантов, террористов, преступников, экстремистов) представляют особую опасность, так как могут привести к возникновению большинства прогнозируемых угроз.

Поэтому на этапе анализа угроз формируется модель вероятных исполнителей угроз (нарушителей), т.е. их количественные и качественные характеристики (оснащенность, тактика действий и т.п.).

Модель нарушителя – это совокупность параметров и характеристик, свойственных потенциальному нарушителю, определяющих его вероятные действия [14].

Существует следующая классификация нарушителей (исполнителей угроз) в зависимости от их подготовленности [26, 46].

1) Случайный нарушитель – не знающий, что объект охраняется и не имеющий специальной цели проникновения на объект.

2) Неподготовленный нарушитель – проникающий на объект со специальной целью и предполагающий возможность охраны объекта, но не имеющий представления о системе охраны и принципах ее функционирования. Направление вторжения такого нарушителя преимущественно определяется прилегающей к объекту топологией местности (дороги, тропы и т.д.), наличием городской застройки.

3) Подготовленный нарушитель – имеющий информацию о возможных методах обхода действующих средств охраны, прошедший соответствующую подготовку скрытно преодолевать зоны обнаружения средств из состава КСБ. Как правило, он имеет представление о физических принципах функционирования средств обнаружения, но не имеет сведений об организации системы охраны. Направление вторжения определяется нарушителем после предварительного изучения объекта с целью гарантированного преодоления зоны обнаружения. Топология местности и городская застройка прилегающей территории также играют роль.

4) Осведомленный нарушитель – обладающий специальной подготовкой, имеющий сведения об организации системы охраны на объекте. Как правило, он знает физические принципы функционирования средств обнаружения и имеет навыки преодоления зон обнаружения.

5) Сотрудник предприятия или охранник – обладающий специальной подготовкой, часто действующий в сговоре с осведомленным нарушителем (характерно для крупного предприятия).

В основе эффективного противодействия угрозам проникновения нарушителя в охраняемые помещения (сейфовые комнаты, переговорные помещения, архивы конструкторско-технологической документации, хранилища информационных баз данных и т.п.) лежит проведение следующих априорных оценок:

– приоритетов в системе защиты (т.е. следует определить, что может представлять наибольший интерес для нарушителя и должно защищаться в первую очередь);

– путей возможного проникновения нарушителей;

– информации, которой может располагать нарушитель об организации системы защиты предприятия;

– технических возможностей нарушителя (его технической вооруженности).

Рассмотренная совокупность оценок позволяет выявить количественные и качественные характеристики вероятного нарушителя и называется "моделью" нарушителя. Эта модель, наряду с категорией объекта, служит основой для выбора методов организации охраны объекта, определяет сложность и скрытность применяемых технических средств охранной сигнализации и телевизионного наблюдения, варианты инженерно-технической защиты, кадровый состав службы охраны и т.д.

1.3 Основы формирования комплекса технических средств обеспечения безопасности

Вопрос "чем и как защищать?" решается способностью существующей или разрабатываемой системы безопасности эффективно предупреждать, предотвращать угрозы и ликвидировать их последствия. Реализация концепции безопасности предусматривает несколько направлений обеспечения защищенности объекта – это экономическая, научно-техническая, технологическая, экологическая, информационная, инженерно-техническая безопасность и др. (рис.1.1). Все они являются элементами единой системы комплексной безопасности данного объекта.

Комплексное обеспечение безопасности защищаемого объекта определяется нормативными документами как деятельность по созданию условий и обеспечению ресурсов для предотвращения и/или уменьшения последствий для защищаемого объекта от угроз различной природы возникновения и различного характера проявления [15, 31].

Концепция безопасности является связующим элементом в рамках создания комплексной безопасности объекта и определяет основные направления ее модернизации и развития. Документ «Концепция безопасности» является основополагающим при оценке уровня организации защиты данного объекта и содержит следующие пункты:

1) Цели и задачи системы безопасности.
2) Описание объектов защиты.
3) Описание потенциальных угроз.
4) Описание основных принципов организации и функционирования системы безопасности.
5) Требования к основным подсистемам безопасности (ПСБ).

При этом состояние защищенности объекта формируется и поддерживается обоснованным в рамках концепции безопасности набором средств (организационных, информационных, финансовых, кадровых и др.). Одним из таких средств является комплекс Технических Средств Обеспечения Безопасности (ТСОБ). Цели, задачи, состав комплекса ТСОБ, а также характеристики и требования по эксплуатации оборудования ТСОБ

формулируются в процессе реализации комплекса инженерно-технической безопасности, который является главным при создании эффективной системы защиты.

Рисунок 1.1 – Инженерно-техническая безопасность в структуре концепции комплексной безопасности объекта

В общем случае комплексная безопасность любого объекта должна включать в себя следующие элементы (рис.1.2):

- организационные мероприятия обеспечения безопасности;
- физическую охрану;
- технические средства обеспечения безопасности.

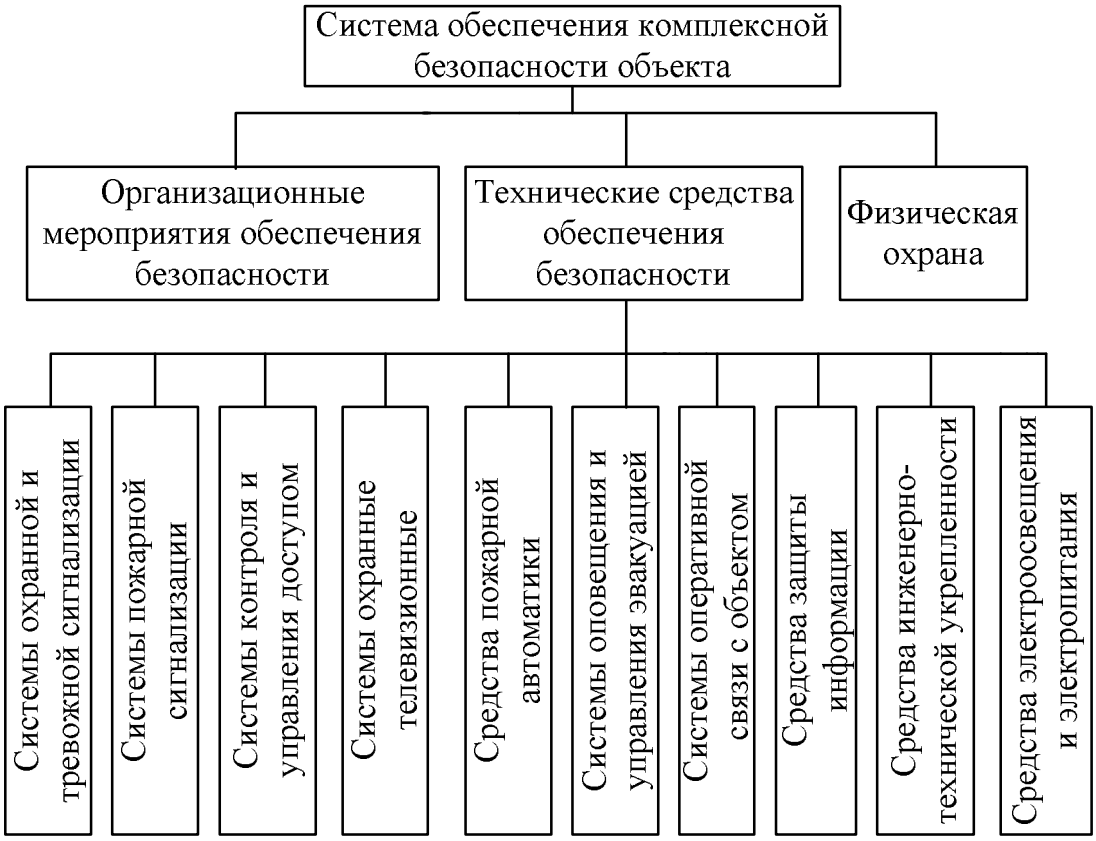

Рисунок 1.2 – Структура системы обеспечения комплексной безопасности объекта в рамках направления инженерно-технической безопасности

К мерам организационного характера при построении и функционировании системы безопасности объектов относятся:

– организация на объекте контрольно-пропускного режима;

– специально разработанные правила поведения сотрудников объектов, посетителей и сотрудников службы безопасности как в штатных, так и во внештатных ситуациях;

– порядок сдачи помещений под охрану и снятия их с охраны;

– порядок действия сотрудников, посетителей и службы охраны по сигналам тревоги и при возникновении чрезвычайных ситуаций;

– разработка системы документооборота службы охраны (журналы регистрации, порядок хранения и уничтожения оперативных и архивных документов и т.п.);

– освоение персоналом охраны основных принципов функционирования технических средств охраны на объекте, правил эксплуатации, в соответствии с тактикой охраны объекта, формирования навыков и умения решать охранные задачи в специфических условиях;

– обучение персонала объекта правилам пользования техническими средствами охраны;

– ознакомление посетителей объектов с правилами поведения;

– заключение и перезаключение договоров на охрану объекта, послегарантийное и сервисное обслуживание технических средств охраны;

– своевременное и в полном объеме финансовое и материально-техническое обеспечение деятельности охраны и функционирования технических средств охраны;

– своевременное административное реагирование руководства объекта на случаи нарушения требований безопасности, внутриобъектового и пропускного режима, возникновение нештатных ситуаций.

Физическая охрана объектов обеспечивается наличием:

– стационарных постов;
– обходных маршрутов (патрульных постов);
– сопровождающих постов;
– постов наблюдения;
– групп оперативного реагирования (групп задержания).

В состав комплекса ТСОБ объекта должны входить следующие технические подсистемы [15, 26, 31, 39, 40]:

– охранной и тревожной сигнализации;
– пожарной сигнализации;
– контроля и управления доступом;
– охранные телевизионные;
– досмотра и поиска;
– пожарной автоматики (пожаротушения, противодымной защиты);
– оповещения и управления эвакуацией;
– средства оперативной связи с объектом;
– защиты информации;
– инженерно-технической укрепленности;
– инженерного обеспечения объекта (электроосвещения и электропитания; газоснабжения; водоснабжения; канализации; поддержания микроклимата – теплоснабжения, вентиляции, кондиционирования).

Состав и количество объектовых ПСБ могут варьироваться в зависимости от назначения и значимости защищаемого объекта и конкретных условий по комплексному обеспечению его безопасности.

Защита объекта может осуществляться как в комплексе, так и по частям, например, созданием только системы охранной сигнализации. Это может быть обусловлено малой вероятностью реализации каких-либо угроз или относительно низкой ценностью части объекта защиты. Системы контроля и управления доступом (СКУД), системы охранные телевизионные (СОТ) и системы оповещения могут применяться для усиления защиты объекта и оперативного реагирования.

Для защиты отдельных конструктивных элементов объекта и его уязвимых мест возможно использование только СКУД или СОТ, при

наличии в них устройств, выполняющих аналогичные функции систем охранной и тревожной сигнализации (например, контроль открывания двери, автоматическое взятие/снятие с охраны по идентификатору, применение обнаружителей движения, передача изображения в пункт централизованной охраны (ПЦО)).

В подобных случаях целесообразно предусмотреть возможность дальнейшего развития системы защиты путем расширения и совершенствования отдельных элементов ее частей, а также добавлением новых подсистем.

1.4 Основные термины и определения

Общее определение системы безопасности (СБ) объекта может быть сформулировано исходя из ее функционального назначения [1].

Система безопасности – это совокупность средств и методов поддержания безопасного состояния объекта, предупреждения, обнаружения и ликвидации угроз жизни, здоровью и среде обитания, имуществу и информации.

При этом необходимость поддержания безопасного состояния объекта, предупреждения, обнаружения и ликвидации угроз определяется основными функциями СБ. Ликвидация этих угроз достигается применением специальных методов и средств (автоматизированного пожаротушения, блокировки замков при проникновении, противодействия утечке информации, управления жизнеобеспечением зданий, разработанных методов действия службы охраны и т.д.).

Усложнение реальной обстановки, требующей повышения уровня безопасности, предполагает развитие технически сложных систем охраны.

Система техническая сложная для защиты объекта – это организационно-техническая система, включающая в себя совокупность технических средств или их комплексов, программное обеспечение, а также документированные процедуры штатных действий персонала, эксплуатационную документацию, материалы, инструменты, приборы, необходимые для использования в комплексной защите объекта [15].

В большинстве случаев раздельное применение специализированных систем или подсистем не обеспечивает достаточный уровень безопасности. Поэтому организация эффективной защиты возможна на основе интеграции всех средств обеспечения безопасности в объединенную систему, включающую в себя следующие элементы:

- техническое обеспечение (аппаратные и программные средства);
- ресурсное обеспечение (финансы, материально-техническое обеспечение, кадровые ресурсы);
- правовое обеспечение (законодательная и нормативно-правовая база для реализации функций службы безопасности);

- организация деятельности службы безопасности (организационно-штатные мероприятия, обучение персонала, повышение квалификации).

Таким образом, объединенная (или общая) система безопасности (ОСБ) должна включать все аспекты защиты (технические, организационные, правовые и другие методы и средства) и охватывать все сферы жизнедеятельности живых организмов (в первую очередь, людей), а также материальную и интеллектуальную собственность, то есть все объекты защиты. При этом важной особенностью ОСБ является объединение всех методов и средств защиты под общим управлением для обеспечения максимальной эффективности.

ОСБ – это совокупность всех методов и средств, обеспечивающих поддержание безопасного состояния объекта, предотвращение, обнаружение и ликвидацию угроз жизни, здоровью, среде обитания, имуществу и информации, имеющая общие средства сбора и обработки информации и управления [1].

В данном определении ОСБ также рассматривается в точки зрения ее функционального назначения и является общим случаем комплексной СБ (КСБ). В отличие от ОСБ, комплексная СБ предполагает использование только технических и программных средств, за исключением таких групп ТСОБ, как, например, оперативная связь, средства инженерно-технической укрепленности, оружие.

КСБ – это совокупность технических и программных средств поддержания безопасного состояния, предотвращения, обнаружения, противодействия и ликвидации комплекса угроз объекту обеспечения безопасности [1].

То есть КСБ – это система, одновременно выполняющая несколько функций безопасности, снижающих риски, обусловленные несколькими видами и/или источниками опасностей. [14, 15]

Структурно КСБ рассматривается как неразделимая СБ, которая включает в себя алгоритмически упорядоченные совокупности технически сложных компонентов, раздельно выполняющих свои задачи. При этом функции централизованно управляемых компонентов КСБ должны дополнять друг друга, не оказывая взаимного мешающего влияния на работоспособность своих составных частей.

Существующими нормативными документами предусмотрена возможность создания комбинированных (комплексных) СБ объекта применительно к системам тревожной или охранной сигнализации [7, 30].

Комбинированная СБ – это совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемых объектах и пожара на них, передачи, сбора, обработки и представления в заданном виде информации [11].

При этом для создания необходимого уровня безопасности объекта и его персонала допускается применять системы тревожной или охранной

сигнализации совместно с другими системами (средствами) в рамках реализации концепции безопасности (например, технологической, пожарной или экологической), а также с инженерными средствами защиты (рис.1.1). В совместно действующих системах должны обеспечиваться алгоритмическая совместимость и раздельная регистрация поступающих от них служебных и тревожных сигналов.

В качестве примера может служить КСБ на основе контрольной панели, которая имеет шлейфы охранной, пожарной сигнализации, контроля окружающей среды (утечка воды и газа). Здесь выполняется обнаружение комплекса угроз, но это одна неразделимая система безопасности.

Существующие в настоящее время подходы к проектированию СБ основаны на методах, которые рассматривают систему как результат перехода от частного к общему, как совокупность компонентов, выполняющих свои задачи. При возрастании сложности систем классический подход оказывается малоэффективным, так как при создании СБ путем суммирования отдельных компонентов не учитывается возникновение новых системных эффектов. Этих недостатков лишена интегрированная система безопасности (ИСБ). Область ее применения – большие, средние и особо важные объекты, требующие повышения их технической оснащенности для обеспечения необходимого уровня безопасности [36, 40]. При этом построение интегрированной (то есть объединенной или суммированной) системы возможно на организационном и физическом (аппаратная и программная интеграция) уровнях.

Организационная интеграция предполагает построение ИСБ на основе отдельных ПСБ, физически не соединенных между собой. Интеграция при этом достигается использованием информации от отдельных подсистем для решения общей задачи обеспечения безопасности объекта. Возможность удаленной передачи информации имеется во многих системах на базе локальных компьютерных сетей.

Для территориально удаленных объектов объединение в общую систему контроля и управления безопасностью возможно с помощью организации удаленного доступа (с использованием стандартной аппаратуры передачи данных по телефонным линиям, радиоканалам и другим сетям передачи данных).

Физическая интеграция позволяет рассматривать СБ как совокупность технических средств, предназначенных для построения подсистем обеспечения безопасности объекта, которые обладают технической, информационной, программной и эксплуатационной совместимостью, объединены каналами связи и общей системой обработки информации и управления. Внедрение ИСБ требует значительных финансовых затрат, но они существенно меньше по сравнению с вариантом, когда каждая подсистема работает автономно, а эффективность применения ИСБ существенно выше.

Система безопасности интегрированная – это специализированная сложная техническая система, объединяющая на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных технические средства, предназначенные для защиты объекта от нормированной угрозы или нормированных угроз [15, 30].

Данное определение рассматривает ИСБ с точки зрения ее структуры, а не функционального назначения. Поэтому названия комплексная и объединенная СБ, определенные исходя из выполняемых ими функций, могут применяться в сочетании с термином «интегрированная». При этом задачи комплексной (комбинированной) ИСБ и объединенной ИСБ будут соответствовать задачам, сформулированным выше для КСБ и ОСБ, но с другой структурой ТСОБ.

Таким образом, как комплексная, так и интегрированная СБ предназначены для обеспечения безопасности объекта при наличии комплекса угроз. Отличие состоит в том, что ИСБ – это совокупность подсистем, которые могут быть как самостоятельными, так и управляться централизованно. При этом каждая из подсистем ИСБ предназначена для обнаружения определенной угрозы. Что касается КСБ, то она не является совокупностью подсистем. Здесь выполняется обнаружение комплекса угроз единой неразделимой системой безопасности.

Структурно интегрированная КСБ (ИКСБ) может включать в себя совместно функционирующие телевизионные системы наблюдения, системы контроля и управления доступом, охранную и пожарную сигнализацию, а также ряд дополнительных подсистем, обеспечивающих защиту от различных видов угроз, возникающих на объектах.

Таким образом, **ИКСБ** – это совокупность технических и программных средств подсистем обеспечения безопасности, объединенных каналами связи, решающая комплекс задач по обеспечению безопасности объекта, имеющая общие средства сбора и обработки информации и управления [1].

1.5 Структура комплексной системы безопасности

Будем рассматривать задачу обеспечения противокриминальной защиты объекта силами четырех основных неразделимых подсистем комплекса ТСОБ, раздельно выполняющих свои функции: системы охранной и тревожной сигнализаций, системы пожарной сигнализации, системы контроля и управления доступом, системы охранной телевизионной (рис.1.2). Комплекс дополняют различные вспомогательные устройства, к примеру, системы электропитания, охранного освещения, оповещения, предотвращения и ликвидации угроз и другие системы, которые обеспечивают жизнеспособность и надежное функционирование основных подсистем ТСОБ.

Каждая из основных подсистем ТСОБ может рассматриваться как КСБ, которая отрабатывает свой комплекс угроз и включает в себя совокупность технических средств охраны. Техническое средство охраны (ТСО) является базовым понятием, обозначающим аппаратуру, используемую в составе комплексов ТСОБ объектов от несанкционированного проникновения.

ТСО – это конструктивно законченное, выполняющее самостоятельные функции устройство, входящее в состав систем охранной, тревожной сигнализации, контроля и управления доступом, охранного телевидения, освещения, оповещения и других систем, предназначенных для охраны объекта [36].

При этом структура КСБ выполняется по классической схеме и состоит из следующих элементов [1, 26, 39]:

- ССОИУЦ – система сбора и обработки информации и управления центральная – сервер, где хранятся и обрабатываются все базы данных системы; контрольные панели, пульты, консоли управления; в общем случае входит в состав центрального пульта наблюдения наряду с автоматизированными рабочими местами (АРМ) операторов, администраторов систем, постов охраны и службы безопасности;
- рабочие станции отдельных систем (при необходимости), осуществляющие обмен данными и командами со своими периферийными устройствами и производящие предварительную обработку информации;
- ССОИУП – система сбора и обработки информации и управления периферийная – устройства (контроллеры, расширители, пульты управления), непосредственно на аппаратном уровне взаимодействующие со своими извещателями, датчиками или исполнительными устройствами, а на информационном уровне связывающие их по локальному интерфейсу (*RS*-485, *RS*-232) с рабочими станциями или с сервером;
- СОУ – средства обнаружения угроз – извещатели охранной, тревожной, пожарной сигнализации, считыватели, клавиатуры, видеокамеры в зависимости от назначения рассматриваемой КСБ;
- СПИ – система передачи извещений – каналы и средства передачи служебных и/или тревожных извещений и сообщений, визуальной и акустической информации об объекте и состоянии КСБ;
- локальная компьютерная сеть, информационно связывающая в единый комплекс отдельные компоненты системы;
- ПО – сетевое, системное и прикладное программное обеспечение сервера и рабочих станций, а также микропрограммное обеспечение системных контроллеров, контрольных панелей и модулей;
- СБЭП – система гарантированного бесперебойного электропитания, которая включает в себя:

– электрощитовую КСБ, подключенную к сети 220В и содержащую все необходимые входные и выходные силовые автоматы;

– источники бесперебойного питания (ИБП), обеспечивающие непрерывное и качественное электропитание всей аппаратуры КСБ в течение заданного времени;

– разведенную по всему объекту отдельную сеть питания с размещением при необходимости отдельных ИБП в специально выделенных помещениях, нишах или шкафах, находящихся под охраной.

- ВУ – вспомогательные устройства, которые обеспечивают выполнение системой охраны ряда функций и включают в себя:
  - СО – средства оповещения;
  - СОИ – средства отображения информации;
  - СРД – средства регистрации данных;
  - СПЛУ – средства противодействия и ликвидации угроз.

Обобщенная структурная схема КСБ, определяющая состав ее технических средств и систем, приведена на рис.1.3.

Учитывая важность для КСБ каждого элемента обобщенной структурной схемы, можно выделить три основные группы ТСО, без которых невозможна реализация системы безопасности: устройства обнаружения угроз, система сбора и обработки информации и управления, а также средства, связанные с тем или иным способом передачи информации о состоянии системы по каналам связи, доведения ее до потребителя (пользователей системы, специальных служб и т.д.). Перечисленные средства обеспечивают реакцию КСБ на обнаруженное событие.

Рассмотрим более детально состав и особенности некоторых элементов структурной схемы КСБ.

Средства обнаружения угроз (СОУ)

В общем случае представляют собой элементы аппаратуры ТСО, исполняющие функцию реагирования на внешнее воздействие. Например, сейсмическое СОУ реагирует на колебание почвы, вызванное движением одушевленного (человека, животного) или неодушевленного (автомобиля, трактора) предмета. Основу функционирования СОУ составляет физический принцип действия его чувствительного элемента (например, электромагнитный, вибрационный, радиотехнический, емкостный, оптический и т.д.).

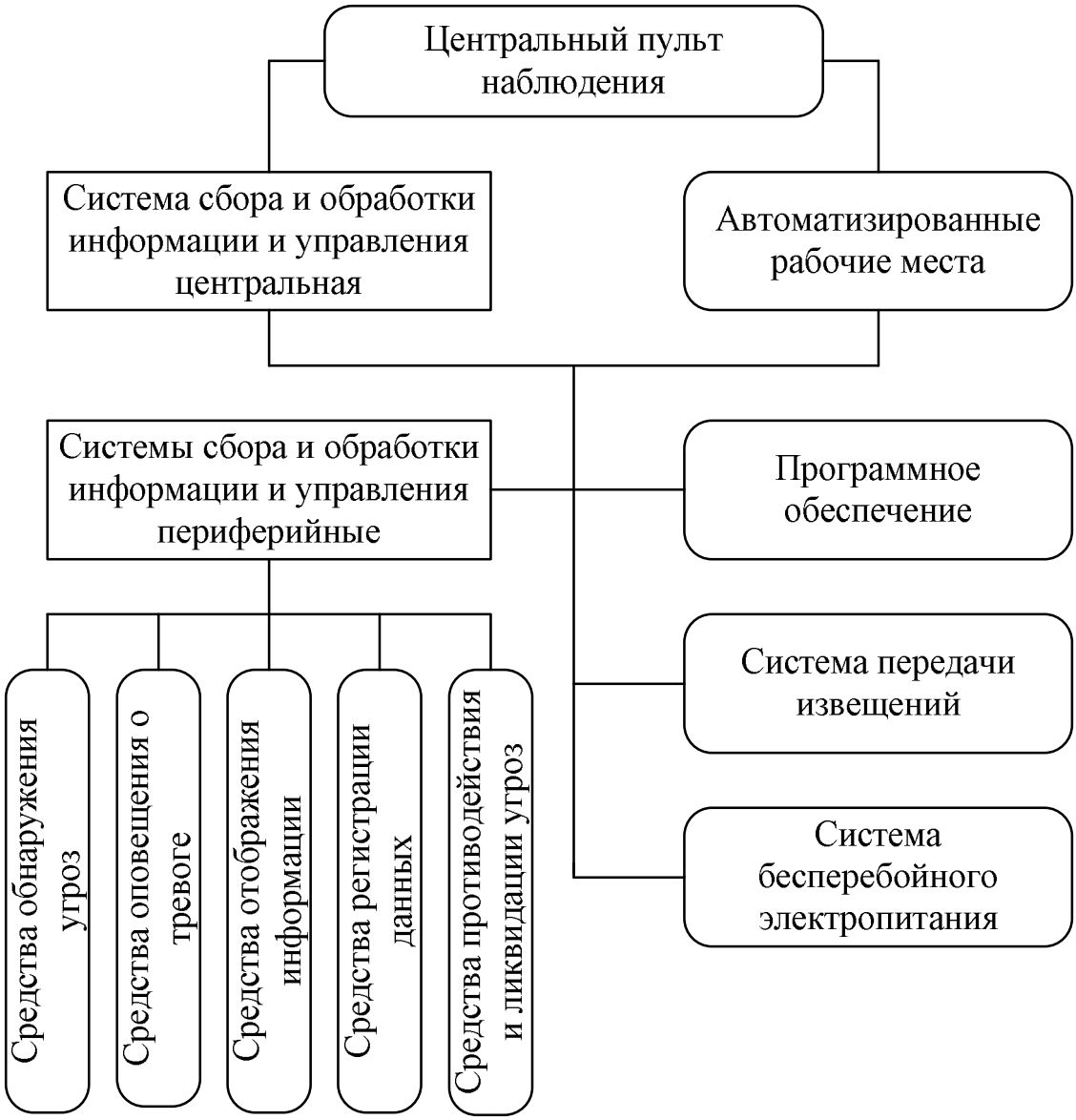

Рисунок 1.3 – Обобщенная структурная схема КСБ

Чувствительный элемент – это первичный преобразователь, реагирующий на воздействие на него (прямое или косвенное) объекта обнаружения и воспринимающий изменение состояния окружающей среды.

Средство обнаружения – это устройство, предназначенное для автоматического формирования сигнала с заданными параметрами (сигнала тревоги, иначе – сигнала срабатывания или оповещения) вследствие вторжения или преодоления объектом обнаружения чувствительной зоны (иначе – зоны обнаружения) данного устройства [26].

В области обеспечения противокриминальной защиты нормативные документы оперируют понятием **средство обнаружения проникновения** и определяют его для охранной и тревожной сигнализаций как автоматические и неавтоматические (тревожная сигнализация) охранные извещатели [40].

Извещатель (техническое средство обнаружения) – это устройство для формирования извещения о тревоге при проникновении (попытке проникновения) или инициирования сигнала тревоги потребителем [11].

Исходя из общей структуры КСБ, в каждой из подсистем ТСОБ можно выделить те устройства, которые являются средствами обнаружения различных угроз и действуют на основе анализа тех или иных физических параметров контролируемого объекта (в зависимости от назначения и выполняемых функций подсистемы). К средствам обнаружения угроз относятся следующие устройства:

1. Для систем охранной и тревожной сигнализаций (СОТС) – охранные и тревожные извещатели, формирующие сигналы при различных видах несанкционированного проникновения в защищаемые зоны. Формирование извещения о тревоге происходит при обнаружении извещателями следующих действий:

- движение или присутствие объекта в контролируемой зоне;
- разрушение каких-либо конструкций - стекол, стен и т. п.;
- смещение предметов, рам, дверей и т. п.;
- пересечение контролируемой зоны и др.

2. Для СОТ – устройства наблюдения (видеокамеры), позволяющие визуально следить за состоянием охраняемого объекта в различных условиях: днем во время нормальной работы объекта (например, магазина) фиксировать ситуацию при нападении на объект, ночью в период охраны регистрировать изменения в изображении и предупреждать об этом. Действующим стандартом видеокамера (ВК) определяется как с точки зрения физического принципа действия ее чувствительного элемента, так и с точки зрения ее положения в структуре сигнализации. **Видеокамера** – это устройство для преобразования оптического изображения в электрический видеосигнал. ВК является первичным источником видеосигнала в составе системы охранной сигнализации [12].

3. Для пожарной сигнализации – пожарные извещатели, которые представляют собой датчики обнаружения возгорания и вырабатывают сигналы при появлении признаков пожара (при повышении температуры выше допустимой, при увеличении концентрации дыма и т.п.). Определение пожарного извещателя основано на его функциональном назначении: **пожарный извещатель** – это техническое средство, предназначенное для формирования сигнала о пожаре [43].

4. Для СКУД – приемные устройства идентификации доступа, в качестве которых используются кодонаборные устройства *PIN*-кода (клавиатуры), для которых решение о доступе принимается при введении правильного кода, а также считыватели, которые расшифровывают информацию, записанную на идентификаторах разного типа и устанавливают права людей, имущества, транспорта на перемещение в охраняемой зоне (объекте). Для повышения уровня безопасности контроля

доступа может использоваться двойная технология, подразумевающая совместное использование клавиатуры для ввода *PIN*-кода и считывателя какого-либо типа (в зависимости от необходимого уровня обеспечения безопасности и финансовых или организационных ограничений). В этом случае код служит для подтверждения факта санкционированного использования идентификатора.

5. Для систем защиты информации – датчики обнаружения утечки информации, выдающие сигнал о попытках несанкционированного получения информации с объекта защиты. Это могут быть передатчики подслушивающих устройств, установленные в помещении или подключенные к телефонной линии; определители подключения к телефонной линии и др.

6. Для систем жизнеобеспечения – датчики контроля окружающей среды, выдающие информацию о состоянии среды проживания человека, позволяющие выявлять ситуации, опасные для жизни или здоровья человека, или предупреждать о возможности возникновения такой ситуации (например, утечка газа, повышение радиационного фона или протечки). Примером могут служить устройства для контроля чистоты воздуха в вентиляционных системах, дозиметры для обнаружения повышения радиационного фона.

7. Датчики контроля состояния СБ, контролирующие состояние и работоспособность системы и формирующие тревожные сигналы при нарушении режима работы или попытках вмешательства в элементы системы для вывода ее из строя. При этом система должна постоянно контролировать свою работоспособность (осуществлять самоконтроль), сообщать о неисправностях и охранять себя от попыток несанкционированного вмешательства (например, от попыток открыть корпус детектора или заблокировать его).

Система сбора и обработки информации и управления (ССОИУ)

Информация от СОУ поступает на систему сбора и обработки информации и управления. В зависимости от сложности задач, решаемых этой системой, ее реализация может быть различной. В простейшем случае ССОИУ может быть выполнена в виде реле, которое срабатывает от сигналов СОУ и управляет звуковыми или световыми средствами оповещения (например, сиреной или строб-вспышкой).

В общем случае ССОИУ представляет собой совокупность аппаратно-программных средств, которые предназначены для сбора, обработки, регистрации, передачи и представления оператору информации от СОУ, для управления дистанционно управляемыми устройствами (видеокамеры, освещение и т.п.), для контроля работоспособности СОУ,

других дистанционно управляемых устройств, а также работоспособности собственных составных элементов.

В области обеспечения противокриминальной защиты дается следующее определение, отображающее состав и функциональное назначение средств ССОИУ в составе охранной и тревожной сигнализации [40]:

средства сбора и обработки информации – это приборы приемно-контрольные, а также блоки, устройства и модули в составе комплексных (интегрированных) систем, обеспечивающие прием извещений от охранных извещателей, обработку и отображение информации, осуществление местного звукового и светового оповещения, управление взятием/снятием с охраны и передачу информации о состоянии охраняемого объекта (зоны) на пульт централизованного наблюдения.

В общем случае ССОИУ выполняет следующие основные задачи.

1. Непрерывный сбор и обработку информации о состоянии СБ и состоянии защищаемого объекта, поступающей от СОУ.
2. Выявление угроз на основе анализа поступающей информации и управления системой.
3. При угрозе – оповещение через каналы связи местных пунктов охраны, пультов централизованного наблюдения и специальных служб.
4. При угрозе – включение устройств оповещения: акустической (сирена, звонок), оптической и речевой сигнализации.
5. При угрозе – включение устройств управления средствами защиты и противодействия выявленной угрозе (автоматизированных средств пожаротушения, дымоудаления, блокировки доступа и др.).
6. Регистрация изменений состояния СБ и объекта, таких как постановка на охрану, снятие с охраны, тревоги, программные изменения в системе; в ряде случаев – электропитание СОУ.

Система передачи извещений (СПИ)

При возникновении нештатной ситуации на объекте необходимая визуальная и акустическая информация передается по каналам связи аварийным службам, в ПЦО, владельцам объекта и др. В качестве каналов и средств передачи служебных и/или тревожных извещений и сообщений в КСБ применяют специально проложенные проводные линии; выделенные и переключаемые телефонные линии ГТС и внутренних АТС объекта; радио- и видеоканалы; радиотрансляционные сети, сети электропитания, оптоволоконную и лазерную технику.

В общем случае **канал СПИ** – это совокупность совместно действующих устройств и технических средств связи, обеспечивающих передачу информации по последовательной цепи: оконечное устройство

системы передачи извещений - канал связи - ретранслятор - канал связи - пульт централизованного наблюдения [11].

СПИ в составе КСБ служит для решения следующих задач [15, 19, 40]:

– передача информации о состоянии охраняемых объектов,

– передача информации о проникновении на охраняемые объекты и/или пожаре на них,

– передача служебных и контрольно-диагностических извещений,

– передача и прием команд дистанционного контроля и управления (телеуправления) при наличии обратного канала связи.

Система бесперебойного электропитания (СБЭП)

Эффективность работы любой СБ объекта во многом зависит от электроснабжения ее элементов. Поэтому независимо от сложности построения СБ, ее функций и возможностей, она должна быть укомплектована надежным источником гарантированного резервного электропитания для работы при отключении или сбоях в сети в течение определенного промежутка времени. Последствиями некачественного электроснабжения могут быть как небольшие сбои и остановки в работе, так и серьезные повреждения оборудования, порча программного обеспечения и потеря данных.

Существующими стандартами и техническими документами в области обеспечения безопасности дается определение СБЭП, отражающее ее основные задачи в структуре КСБ, и формулируются требования к ее параметрам и режиму функционирования [10, 15, 19].

СБЭП – это совокупность совместно действующих устройств, предназначенных для автоматического переключения электропитания с основного на резервный или автономный источник электропитания и обратно при отклонениях параметров сетевого электропитания от предельно допустимых [10].

Электропитание технических средств подсистем КСБ/ИСБ может осуществляться от сети переменного тока или от вторичных источников электропитания постоянного тока для питания низковольтных (12В, 24В) слаботочных цепей. Основным параметром источников питания является длительность резервирования электропитания СБ. Для особоважных объектов эта длительность составляет не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги.

Средства оповещения (СО)

Средства оповещения о тревоге – это технические средства, предназначенные для светового и/или звукового оповещения людей о возникновении опасности [40]. Распространенными средствами

оповещения и связи являются средства свето-звуковой индикации (сирена, звонок, строб-вспышки), абонентская телефонная связь, радиосвязь, громкая связь, выдающая речевые сообщения на различных языках, телефаксы, мобильные телефоны, пейджеры, переговорные устройства, пневмопочта.

Комплекс средств оповещения формирует систему оповещения, которая совместно с системой связи решает задачи оперативного управления и координации действий персонала объекта в случае угрозы, а также одновременного доведения до большого числа пользователей речевых сообщений, звуковых и/или световых сигналов.

Системы оповещения и связи предназначены для выполнения следующих функций [15, 36, 40]:

– доведение достоверной, бесперебойной служебной информации об обстановке на объекте и в его контрольных зонах до служб охраны при возникновении нештатной ситуации или угрозе;

– оповещение лиц, санкционированно находящихся на охраняемом объекте, об аварийной ситуации;

– привлечение внимания окружающих или милиции к охраняемому объекту при попытке проникновения или кражи (например, включение звукового сигнала автомашины и мигание фар при проникновении в нее), пожаре или в других ситуациях;

– оперативная и одновременная передача распоряжений по действиям персонала в зависимости от обстановки на объекте.

Координация и управление перемещениями людей при возникновении нештатной ситуации на объекте достигается такими действиями системы оповещения, как:

– передача речевой информации о необходимости эвакуации и предусмотренных для этого направлениях движения;

– передача специальных текстов, предназначенных для управления поведенческой динамикой людей для обеспечения их безопасности;

– включение (переключением) световых указателей на рекомендуемых направлениях эвакуации, через эвакуационные и/или аварийные выходы;

– передача оперативных команд по действиям групп людей или отдельных людей на различных участках эвакуационных путей по результатам наблюдения в подсистеме охранного телевидения.

Средства отображения информации (СОИ)

Устройства отображения информации позволяют наблюдать состояние защищаемого объекта, изменения в работе ТСО, входящих в состав КСБ.

Простейшие СОИ представляют собой индикаторные лампы и светодиоды, цвет или режим работы которых соответствует определенному

объекту или его состоянию. Это может быть жидкокристаллический дисплей контрольной панели или клавиатуры, на котором индицируется соответствующий текст, например: набранный код доступа, номер видеокамеры, в поле зрения которой обнаружено движение, название или номер нарушенной зоны охраны, статус сигнализации (постановка на охрану, снятие с охраны, тревога и т.п.).

В более сложных системах это может быть монитор, на экране которого отображается план охраняемого объекта и его состояние. В качестве устройств вывода видеоизображения в СОТ используются аналоговые или жидкокристаллические видеомониторы, для которых установлены требования к размеру диагонали (не менее 17 дюймов) и рабочему разрешению экрана (не ниже 1280х1024 точек или 960х768 ТВЛ) [12, 19].

Таким образом, СОИ в составе КСБ позволяют наблюдать следующее:

– состав и состояние охраняемого объекта (например, план объекта, какие части объекта охраняются, какие нет, где и какое произошло нарушение);

– состав и состоянии всей СБ и ее элементов (например, количество и состояние шлейфов сигнализации, параметры системы, соответствующие ее нормальному функционированию или отклонениям от нормы, неисправности, сбои по электропитанию).

Средства регистрации данных (СРД)

Информация о состоянии СБ, о текущей обстановке и изменениях на объекте фиксируется устройствами регистрации данных. СРД обеспечивают регистрацию поступающих сообщений и команд управления, их хранение в течение установленного срока. При этом обычно документируются не только само событие, но также дата и время как передачи, так и получения подтверждения поступления информации о событии, например, кто из пользователей поставил систему на охрану, кто снял с охраны, какие нарушения защищаемого объекта произошли и др. Кроме того, при проникновении в зону защиты нарушителей фиксируются события и действия службы охраны по их обезвреживанию.

В качестве СРД могут использоваться запоминающие устройства персональных компьютеров (ПК), печатающие устройства.

Запись, воспроизведение и хранение видеоинформации в составе СОТ реализуется на базе предназначенных для этих целей устройств – цифровых видеорегистраторов, или программным методом на базе средств ПК с установленным ПО. При этом запись видеоинформации должна обеспечиваться либо непрерывно в реальном времени, либо отдельными фрагментами в зависимости от условий охраны объекта и требований заказчика [12, 19].

В составе СКУД также предусмотрена подсистема регистрации и учета входа/выхода пользователей в систему/из системы, изменений полномочий пользователей и статуса объектов доступа, создаваемых защищаемых объектов доступа. При документировании указываются время, дата, характеристики и результаты проведенной операции [13].

Средства противодействия и ликвидации угроз (СПЛУ)

При противодействии возможным угрозам и преступным посягательствам кадровые ресурсы СБ играют основную роль. Они несут охранную службу, проводят профилактические мероприятия, организовывают и поддерживают заданный режим работы КСБ и объекта, при поступлении сигнала тревоги обеспечивают немедленный выезд группы задержания для принятия адекватных мер противодействия угрозам.

При обеспечении безопасности объектов главной задачей для службы безопасности является сохранение материальных и иных ценностей на вверенном объекте. Для этого устанавливаются СБ, которые по составу ТСОБ можно разделить на две группы:

– пассивные, которые предупреждают о потенциальной или возникшей угрозе (например, о попытке проникновения или проникновении на охраняемый объект, о превышении температурного порога в помещении, о наличии подслушивающего устройства в телефонной линии);

– активные, которые непосредственно противодействуют возникшей угрозе, препятствуют ее дальнейшему развитию.

В активной СБ при обнаружении аварийной ситуации (вторжении или попытке вторжения на охраняемый объект, возникновении очага пожара, попытке несанкционированного съема информации, нарушении режима работы оборудования и т.п.) ССОИУ на основе анализа сигналов, поступающих от соответствующих СОУ, включает систему управления внешними устройствами (средствами противодействия и ликвидации угроз).

К СПЛУ в составе активной СБ можно отнести [1, 26, 39]:

– автоматизированные средства пожаротушения, дымоудаления и вентиляции, которые позволяют до прибытия пожарной охраны локализовать или потушить пожар;

– средства блокирования действий нарушителя (это могут быть простые устройства, включающие свет или радиоприемник в доме, чтобы отпугнуть преступников при попытке проникнуть в него; устройства, блокирующие замки дверей; устройства, блокирующие стартер и рулевое управление автомашины);

– средства воздействия на преступника (например, средство для распыления слезоточивого газа);

– средства противодействия утечке информации (временная приостановка систем передачи информации; включение генератора шума, когда работает передатчик закладного радиомикрофона, и др.);

– средства управления производственным оборудованием, возвращающие его в нормальный режим или приостанавливающие его работу.

Для эффективной защиты объекта необходимо, чтобы указанные действия предпринимались в предельно короткий срок, до прибытия специальных служб (пожарной охраны, милиции, скорой помощи, аварийных служб), чтобы свести к минимуму возможный ущерб.

Поэтому установленная на объекте СБ должна обеспечить максимальную вероятность обнаружения нарушителя с наиболее точным указанием места его проникновения для организации адекватного противодействия. В системах противокриминальной защиты эта задача решается использованием в комплексе ТСОБ правильно спроектированных средств освещения, связи и особенно СОТ.

СОТ должны обеспечивать передачу оператору видеонаблюдения (в случае получения извещения о тревоге) изображения из охраняемой зоны для определения характера, места нарушения, направления движения нарушителя с целью определения оптимальных мер противодействия [12, 39, 40].

1.6 Общие принципы построения систем безопасности

Рассмотрим принципы построения СБ объекта, на основе которых устанавливаются требования к созданию и организации функционирования СБ в целом и составляющих ее ТСОБ.

При построении СБ объекта необходимо руководствоваться следующими принципами [15, 40, 42]:

1) адекватности принятым моделям угроз (разработанные организационные и административные мероприятия, технические способы защиты объектов и их элементов должны соответствовать принятым угрозам и моделям нарушителей);

2) зонального построения или зональным принципом (СБ должна предусматривать организацию и создание зон ограниченного доступа и охраняемых зон, обеспечивающих "эшелонированную" защиту охраняемых объектов и их критических элементов);

3) равнопрочности (должен быть обеспечен требуемый уровень эффективности СБ для всех выявленных в процессе анализа уязвимости типов нарушителей и способов совершения преступных действий);

4) адаптивности (СБ не должна создавать препятствий

функционированию объекта и должна адаптироваться к технологическим особенностям его работы, в том числе в чрезвычайных ситуациях с учетом принятых на объекте мер технологической и пожарной безопасности).

Соблюдение принципов построения СБ позволяет обеспечить **эффективность защиты** объектов, которая определяется способностью технических подсистем КСБ и ИСБ противостоять нештатным ситуациям на объекте с учетом выявленных угроз и моделей нарушителей.

Свойство адекватности технической подсистемы позволяет не допустить ошибок в ее структурном построении и избежать неоправданной технической избыточности при реализации.

Рассмотрим более подробно зональный принцип построения СБ, который позволяет рационально сделать выбор и распределение технических средств подсистем для охраны объекта и его критических зон (элементов).

Под **критическими зонами** (элементами) объекта понимают помещения, их конструктивные элементы, участки, реализация угрозы в отношение которых (либо действие ее последствий) может привести к наиболее существенным потерям. Для своевременного обнаружения и нейтрализации потенциальных угроз необходимо определить последовательные зоны (или рубежи) обеспечения безопасности с одновременным выявлением угроз по каждой конкретной зоне.

В общем случае **зона защищаемая** определяется как находящееся непосредственно за защитной конструкцией пространство, механически огражденное от несанкционированного доступа и других нештатных действий [11].

Так как конкретные задачи и условия функционирования ТСОБ зависят от структуры объекта защиты, то охраняемая зона может быть определена как часть охраняемого объекта, контролируемая одним шлейфом охранной сигнализации (для комплексов охранной сигнализации), одним шлейфом пожарной сигнализации (для установок пожарной сигнализации), одним шлейфом охранно-пожарной сигнализации или совокупностью шлейфов охранной и пожарной сигнализации (для комплексов охранно-пожарной сигнализации) [19, 39].

Шлейф сигнализации – это цепь (электрическая, радиоканальная, оптоволоконная или другая), соединяющая выходные узлы извещателей, включающая в себя вспомогательные (выносные) элементы и соединительные линии и предназначенная для передачи на прибор приемно-контрольный или на устройство объектовое системы передачи извещений информации от извещателей о контролируемых ими параметрах, а в некоторых случаях – для подачи электропитания на извещатели [11, 19, 36].

Рубеж охранной сигнализации – это шлейф или совокупность шлейфов или лучей (для сигнализации, использующей передачу извещений

по радиоканалу), контролирующих охраняемые зоны территории, здания или помещения (периметр, объем или площадь, сами ценности или подходы к ним) на пути возможного движения нарушителя к материальным ценностям, при преодолении которых выдается соответствующее извещение о проникновении [11, 36].

Под рубежом охраны понимается совокупность охраняемых зон, контролируемых рубежом сигнализации [39].

При организации зонирования объекта должно обеспечиваться усиление защиты от периферии к центру, то есть к критическим элементам, определяющим категорию объекта. Если при оценке эффективности СБ выясняется, что существующих охраняемых зон недостаточно для нейтрализации потенциальных угроз, то могут организовываться дополнительные рубежи защиты внутри существующих зон.

Основу планировки и технического оснащения зон безопасности составляет принцип равнопрочности их границ. Например, если при оборудовании зоны периметра здания на одном из окон первого этажа не будет металлической решетки или ее конструкция ненадежна, то прочность и надежность других решеток окон этого этажа не имеют никакого значения, так как зона будет достаточно легко и быстро преодолена нарушителем через незащищенное (или слабо защищенное) окно. Следовательно, границы зон безопасности не должны иметь незащищенных участков.

Свойство адаптивности СБ позволяет своевременно и гибко учитывать динамику потенциальных и реальных угроз и опасностей объекту.

Таким образом, техническая подсистема КСБ и ИСБ должна обладать адекватностью по отношению к спектру угроз и опасностей объекту с учетом контрольных зон в своей подконтрольной области и адаптивностью к изменениям условий функционирования объекта.

1.7 Зоны обеспечения безопасности

Определение последовательных рубежей (или зон безопасности) с одновременным выявлением угроз по каждой конкретной зоне позволяет выбрать ТСОБ для наиболее эффективного решения задач охраны объекта.

Такие рубежи (или зоны безопасности) должны располагаться последовательно – в общем случае, от ограждения вокруг территории объекта до критических элементов объекта, таких как сейфы, хранилища ценностей и информации, взрывоопасных материалов, оружия и т.д. (рис. 1.4). Чем сложнее и надежнее защита каждой зоны безопасности, тем больше времени потребуется нарушителю на ее преодоление и тем больше вероятность того, что расположенные в зонах СОУ подадут сигнал тревоги. Следовательно, у службы охраны будет больше времени для определения причин тревоги и организации эффективного противодействия угрозам.

Начальной зоной обеспечения безопасности является прилегающая территория. Она не является частью объекта и может использоваться нарушителями для подготовительных работ по организации несанкционированных действий, например, для наблюдения и изучения режима охраны объекта и его охранных структур. Поэтому прилегающая территория также может рассматриваться как зона обеспечения безопасности и контролироваться, в первую очередь, средствами СОТ.

Первой зоной является внешний периметр территории объекта охраны.

Угрозы: преодоление периметральных средств инженерно-технической укрепленности (в том числе их разрушение) для проникновения на территорию с целью вторжения на объект.

В первой зоне могут использоваться средства инженерно-технической укрепленности (заграждения, заборы), СОТ, средства периметральной защиты в составе системы охранной сигнализации, а также физическая охрана, т.е. работники собственной службы безопасности или сотрудники вневедомственной охраны (рис.1.2).

Рисунок 1.4 – Расположение зон обеспечения безопасности

Запретная зона (или зона отторжения) при необходимости организуется вдоль основного ограждения периметра с внутренней стороны территории объекта и предназначена для размещения на ней ТСО и выполнения служебных задач личным составом подразделений охраны [11].

Запретная зона должна быть тщательно спланирована и расчищена. В ней не должно быть никаких строений, предметов и растительности, затрудняющих применение ТСО и действия сил охраны. Запретная зона может быть использована для организации охраны объекта при помощи сторожевых собак. Для обеспечения нормальной работы ТСО (извещателей) для открытых площадок и периметров объектов ширина запретной зоны должна превышать ширину их зоны обнаружения [36, 40].

Вторая зона охраны включает в себя территорию, на которой находится охраняемый объект.

Угрозы: несанкционированное проникновение на территорию с целью дальнейшего вторжения на объект.

При защите данной зоны используется комплекс мероприятий, состоящий из технических средств СОТ и охранно-пожарной сигнализации (ОПС).

Третью зону охраны составляет элементы периметра охраняемого здания или помещения [32]:

– строительные конструкции по периметру здания или помещений объекта, то есть все оконные и дверные проемы;
– места ввода коммуникаций, вентиляционные каналы;
– выходы к пожарным лестницам;
– некапитальные и капитальные стены;
– вентиляционные короба, дымоходы на "разрушение".

Угрозы: несанкционированное проникновение в здание через слабо укрепленные, незаблокированные средствами сигнализации участки, а также подготовительные работы для преодоления ("обхода") ТСОБ.

Эта зона контролируется средствами СОТ, ОПС и физической охраны.

Четвертая зона – внутренние объемы помещений объекта.

С помощью технических средств СКУД в четвертой зоне должны быть организованы пропускной и внутриобъектовый режимы. Для этого выполняется разделение объекта на три основные зоны доступа [1, 40]:

– первая зона (зона свободного доступа) – здания, территории, помещения, доступ в которые персоналу, посетителям и лицам, проживающим на объекте, не ограничен;

– вторая зона (зона ограниченного по времени или уровню приоритета доступа) – помещения, доступ в которые разрешен в ограниченное время (например, покупателям магазина в рабочие часы, персоналу – в соответствии с режимом работы) или ограниченному составу персонала, а также посетителям объекта по разовым пропускам или в сопровождении персонала объекта;

– третья зона – специальные помещения объекта, доступ в которые имеют строго определенные сотрудники и руководители (например, помещения руководства объекта и охраны), а также помещения непосредственного сосредоточения и хранения материальных и иных ценностей.

Пропуск пользователей на объект через пункты контроля доступа должен осуществляться:

– в первой зоне доступа по одному признаку идентификации;

– во второй зоне доступа – по двум признакам идентификации (например, электронная карточка и ключ от механического замка);

– в третьей зоне доступа – не менее, чем по двум признакам идентификации [40].

Угрозы: несанкционированное проникновение в помещения с материальными и финансовыми ресурсами; вывод из строя средств СОТ и ОПС; установка подслушивающих и других устройств съема информации; нейтрализация работников охраны или служб безопасности для последующего нападения на кассиров с целью завладения денежными средствами или иными материальными или финансовыми ресурсами; захват заложников; проникновение в компьютерную сеть предприятия с преступными целями; физическое уничтожение руководителей объекта с целью развала предприятия как конкурента; нападение на сотрудников охраны для совершения террористических или иных актов; хищение, кража из мест непосредственного хранения ценностей.

Эти зоны контролируются техническими средствами ОПС, СКУД, СОТ совместно со средствами защиты информации (СЗИ), физической охраной.

Пятая зона – отдельные предметы, например сейфы, картины, скульптуры и подходы к ним.

Угрозы: хищение, акты вандализма. Для защиты используется соответствующие технические средства охранной сигнализации и СОТ.

Шестая зона – собственно система безопасности. Включает в себя защиту технических и программных средств обеспечения безопасности.

Угрозы: несанкционированный доступ к элементам СБ с целью либо полного вывода ее из строя, либо блокировки отдельных элементов, делающей невозможным выполнение ими основных функций при внешнем сохранении работоспособности.

Для предотвращения угроз используются датчики вскрытия корпусов и снятия со стены, самодиагностика элементов системы, устройства обнаружения блокировки извещателей и др.

Каждая из охраняемых зон может включать в себя несколько рубежей охраны в зависимости от значимости объекта или его критических элементов, контролируемых данной зоной. При этом критическая зона (например, область непосредственного хранения материальных ценностей)

должна находиться в центре, и для подхода к ней необходимо преодоление всех зон и рубежей охраны [1, 26].

1.8 Условия функционирования систем безопасности

Объем и состав оборудования, используемого в каждой из систем, входящей в комплекс ТСОБ объекта, определяются необходимым уровнем обеспечения безопасности объекта и его персонала. Вариант совместного использования нескольких СБ на объекте может быть выбран на основе компромисса между стоимостью потерь от потенциальных угроз и затратами на реализацию этого варианта.

Приоритетными для каждой СБ являются требования, обеспечивающие безопасность для жизни людей, и пожарную безопасность объекта. Поэтому основным техническим требованием к СБ является обеспечение необходимой функциональной и аппаратной надежности, пожарной безопасности и помехоустойчивости. Под надежностью СБ понимается ее свойство обнаруживать с заданной вероятностью проникновение (попытку проникновения) на охраняемый объект (зону объекта) [18].

Основные условия функционирования СБ могут быть сформулированы следующим образом [1, 7, 39, 40].

1. Ни одна из подсистем в составе СБ не должна нарушать режим функционирования объекта, а именно:

   – функции совместно действующих систем должны дополнять друг друга, не оказывая взаимного мешающего влияния на работоспособность своих составных частей;

   – в совместно действующих системах должны обеспечиваться алгоритмическая совместимость и раздельная регистрация поступающих от них служебных и тревожных сигналов;

   – требования к эксплуатационной надежности, чувствительности и помехоустойчивости одной из подсистем не должны уступать аналогичным требованиям, предъявляемым к другим работающим совместно с ней подсистемам, чтобы не снижать общий уровень безопасности объекта в целом;

   – выход из строя одной или нескольких подсистем или каналов связи не должен приводить к выходу из строя всей СБ.

2. СБ должна управляться как централизованно, так и децентрализованно с контролем уровня доступа персонала к системе. Состав системы управления и контроля функционирования совместно действующих ПСБ должен определяться их назначением. Предпочтительны автоматические средства управления и контроля, в качестве дублирующих допускаются ручные. Целесообразность дублирования определяется требованиями по обеспечению

эксплуатационной надежности систем. Средства управления и контроля должны иметь защиту от возможных ошибочных действий персонала.

3. СБ должна сохранять исправное состояние при воздействии факторов окружающей среды и восстанавливать работоспособное состояние по окончании их воздействия.

4. СБ не должна выходить из строя при отключении электроэнергии на объекте и сохранять работоспособное состояние при отключении сетевого или другого основного источника электропитания в течение времени прерывания электропитания. Сигнализации не должны выдавать ложных тревог при переключениях источников электропитания с основного на резервный и обратно.

5. Все события, происходящие в системе, должны протоколироваться.

6. Система должна контролировать, тестировать и защищать себя от несанкционированного доступа к управлению.

7. Совместно действующие объектовые системы различного функционального назначения требуют различного реагирования на выдаваемые ими сигналы аварии, тревоги; при этом:

- сигналы от различных совместно действующих систем, передаваемые для регистрации автоматически, должны фиксироваться приборами управления раздельно (соблюдение данного условия позволяет предотвратить опасность "ложного вызова службы", то есть реагирования одной службы объекта на сигналы, предназначенные для другой службы и/или принятия персоналом объекта действий, неадекватных возникшей обстановке);
- виды и интенсивность сигналов систем различного назначения должны быть различными (при этом звуковые аварийные, тревожные сигналы не должны препятствовать использованию речевой, в том числе телефонной связи).

8. Система не должна создавать угроз объекту обеспечения безопасности.

В каждом конкретном случае охраны рассмотренный список может быть ограничен или дополнен дополнительными условиями.

2 ИНТЕГРИРОВАННЫЕ КОМПЛЕКСНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

При построении концепции безопасности необходимо не просто предусмотреть установку функционально независимых подсистем на объекте, но использовать интегрированные комплексные системы безопасности.

ИКСБ объединяет ТСОБ объекта на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных. Она обладает высокой эффективностью и надежностью за счет взаимодополнения и резервирования технических средств. В ней отсутствуют избыточные линии связи, управление осуществляется оперативно и централизованно с помощью АРМ.

Целями интегрирования являются:

- снижение рисков принятия ошибочных решений и уменьшение времени реакции при возникновении внештатной ситуации на объекте;
- получение новых функций, связанных с возможностью обеспечения оперативного взаимодействия подсистем и компонентов СБ при сохранении в полном объеме возможностей ее составных частей;
- экономия необходимых для реализации этих функций средств;
- максимальная автоматизация действий по всем направлениям защиты объекта.

Среди функций, обязательных для исполнения в рамках ИСБ, следует считать следующие [26, 37, 39]:

– контроль состояния объекта с созданием многорубежной защиты;

– иерархический доступ персонала и посетителей в помещения с четким разграничением полномочий по праву доступа в зависимости от времени суток и дней недели;

– идентификацию и аутентификацию личности человека, пересекающего рубеж контроля;

– предупреждение утечки информации;

– предупреждение попадания на объект запрещенных материалов и оборудования;

– документирование и архивирование информации для ее использования при расследовании происшествий и анализе действий служб охраны;

– оперативный инструктаж службы охраны о порядке действий в различных штатных и нештатных ситуациях путем автоматического вывода на экран монитора инструкций в нужный момент;

– обеспечение полной интеграции систем видеонаблюдения, сигнализации, мониторинга доступа, оповещения; связи между

персоналами службы охраны, службы пожарной безопасности, служб жизнеобеспечения объекта и т.д.;

– обеспечение взаимодействия постов охраны и органов правопорядка;

– контроль исполнения персоналом охраны своих служебных обязанностей.

2.1 Классификация ИКСБ

Классификация ИКСБ проводится на основе способов объединения различных ПСБ в интегрированный комплекс. Именно разные способы интеграции серьезно влияют на потребительские характеристики и свойства ИКСБ. Интеграция оборудования отдельных ПСБ, входящих в состав ИКСБ объекта, может быть выполнена на следующих уровнях: проектном, аппаратном, аппаратно-программном и программном [1, 23].

В рамках одной системы может быть реализовано несколько уровней (способов) интеграции оборудования отдельных ПСБ.

Определяющими признаками, по которым ту или иную интегрированную систему можно отнести к какому-либо типу, являются:

- тип информации (сообщения и команды или простейшие аналоговые сигналы), передаваемой между различными ПСБ;
- схема передачи информации между управляющими устройствами различных подсистем (контроллерами СКУД, приборами приемно-контрольными (ППК), системами ОПС, управляющим и записывающим оборудованием СОТ);
- схема принятия решений (централизованная, иерархическая или распределенная);
- тип управляющих устройств, принимающих решение (контроллеры или компьютеры с установленным программным обеспечением).

Интеграция на проектном уровне – предполагает объединение ПСБ на этапе проектирования системы для конкретного объекта. Такая работа проводится проектно-монтажными фирмами – "системными интеграторами". При этом применяются разнородные ПСБ различных производителей, объединение которых выполняется путем установки оборудования управления подсистемами в общем помещении – центральном пункте управления. Взаимодействие между ПСБ осуществляется на уровне операторов подсистем, то есть без автоматизации.

Рассмотренный способ взаимодействия систем соответствует самому низкому уровню интеграции. Недостатки его применения: "человеческий фактор", разнородность аппаратуры, сложность обслуживания, параллельность прокладываемых коммуникаций, отсутствие автоматизации и др. В настоящее время данный способ не является

перспективным, но его применение возможно, если фирмой разработано собственное проектное решение построения систем.

Интеграция на аппаратном уровне – предполагает объединение всех ПСБ исключительно с помощью аппаратного обеспечения каждой из систем без использования компьютеров управления и внешнего программного обеспечения. Классическим примером данного типа интеграции является объединение систем посредством релейных контактов.

Интегрированные таким образом системы строятся также на оборудовании разных производителей, а взаимодействие между ПСБ осуществляется путем включения реле одной подсистемы в шлейф другой. Это наименее эффективные из всех ИСБ, поскольку обладают низкой информативностью и лишены возможности реализации сложных алгоритмов взаимодействия между ПСБ.

Достоинством аппаратной (релейной) интеграции является простота и надежность используемого оборудования, невысокая стоимость и возможность объединения ПСБ различных производителей.

Недостатками данного решения являются:

- низкая устойчивость к несанкционированным действиям и подмене оборудования;
- ограниченность обратной связи и интерпретации событий;
- невозможность обеспечить передачу большого количества сигналов о различных событиях между системами;
- невозможность реализации отображения информации о состоянии систем на графических планах объекта и управления ресурсами систем по этим планам;
- высокая трудоемкость и затратность процесса внесения изменений в релейную интеграцию на этапе эксплуатации (так как каждая логическая связь представляет собой релейный контакт и линию связи между системами, то любое изменение приводит к необходимости проведения монтажных работ и перепрограммирования);
- при использовании релейной интеграции на крупных объектах с большим количеством связей между системами (начиная с 200–300) утверждение о дешевизне и надежности данного способа интеграции перестает быть верным (по мере роста количества реле и линий связи суммарная стоимость релейной интеграции может превысить стоимость интеграции другого типа);
- снижение надежности релейной интеграции с ростом количества связей из-за большого числа дополнительных соединений.

Таким образом, данное решение может использоваться в небольших системах с простой логикой функционирования или в тех сегментах сложных систем, где отсутствуют повышенные требования к устойчивости к враждебным действиям.

Интеграция на программном уровне (на программно-аппаратном уровне с приоритетом программной поддержки) – предполагает объединение за счет единого ПО подсистем разных производителей, оборудование каждой из которых работает по своему протоколу. Построение ИСБ данного типа может выполняться двумя способами. Первый способ состоит в применении специально разработанного ПО, которое объединяет все ПСБ. Второй способ предусматривает использование в качестве интегрирующего ПО программную оболочку одной из систем безопасности (чаще всего СКУД).

ИСБ со специализированным ПО

К данному виду ИСБ относятся комплексы, в которых взаимодействие между отдельными ПСБ реализуется с помощью специально разработанного для этих целей внешнего ПО, которое предназначено для функционирования в аппаратной среде на верхнем уровне ИСБ и устанавливается на компьютере управления системами. Сопряжение сервера ИСБ, на котором установлено интегрирующее ПО, и компьютера управления каждой из локальных ПСБ нижнего уровня реализуется аппаратно с помощью программ-драйверов, разрабатываемых для поддержки конкретных средств других производителей. В результате сервер с установленным на нем специализированным ПО является управляющим центром всей ИСБ, и все логические взаимосвязи между ПСБ программно реализованы на сервере.

Подобное построение ИСБ имеет следующие достоинства:

- возможность организации глубокого обмена информацией между отдельными ПСБ, входящими в комплекс (это позволяет строить современные высококачественные многофункциональные ИСБ с организацией автоматизированных алгоритмов реакции на события, с синхронизацией баз данных и автоматизацией поиска нужных событий в одной системе при известных входных событиях в другой);
- наличие удобного АРМ оператора, на дисплее которого отображается состояние ПСБ с привязкой к графическим планам объекта, могут выдаваться инструкции в соответствии с ситуацией на объекте, имеется возможность управлять системами по графическим планам объекта, что уменьшает время реакции и принятия решений;
- возможность интеграции с аппаратными средствами других производителей (при наличии соответствующих драйвера и интерфейсов обмена данными в самих применяемых средствах);
- по сравнению с ИСБ релейного типа, требует меньшего количества линий связи между системами, так как для интеграции каждой системы обычно нужен всего один кабель;

- по сравнению с ИСБ релейного типа, внесение изменений в логику работы ИСБ производится только перепрограммированием интеграционных настроек и не приводит к выполнению монтажных работ, что более удобно при эксплуатации.

Недостатки ИСБ со специализированным ПО:

- необходимость разработки драйверов для каждого применяемого аппаратного средства (при этом разработчик аппаратного средства не всегда предоставляет протоколы обмена данными);
- сложность обеспечения оптимального сопряжения из-за ограниченных возможностей протоколов обмена данных аппаратных средств каждой ПСБ;
- невозможность для разработчика интегрирующего ПО в полном объеме гарантировать работу системы в целом.

ИСБ с системным ПО

К данным системам относятся ИСБ с программной интеграцией, в которой роль интегрирующей программной оболочки выполняет ПО одной из входящих в комплекс ПСБ. Достоинством данного построения по сравнению в предыдущим является то, что уже существует работоспособное ПО для создания ИСБ. Недостатком – то, что ПО подсистемы при серьезной нагрузке дополнительными функциями и потоками данных может оказаться не в состоянии нормально функционировать, так как оно изначально не разрабатывалось для создания ИСБ.

Надежность ИСБ с программной интеграцией определяется в первую очередь надежностью компьютеров управления и ПО. При выходе из строя любого из этих компонентов практически все взаимосвязи между ПСБ нарушаются, что полностью парализует работу ИСБ в целом. Поэтому повышение их надежности для программной ИСБ представляет собой первоочередную задачу.

Интеграция на аппаратно-программном уровне предполагает максимальную степень взаимосвязи между ПСБ за счет работы всех модулей системы по одному протоколу вне зависимости от того, какую функцию они выполняют. Благодаря этому обеспечивается простота и снижение расходов при монтаже и наладке системы. Это наиболее совершенный тип ИСБ. Объединение входящих в ее состав подсистем происходит за счет общей для них базы данных, ПО и протокола передачи информации.

Аппаратное объединение элементов ПСБ реализуется не с помощью релейных контактов, а за счет интеграции систем, предусмотренной еще на этапе разработки оборудования каждой ПСБ и/или за счет использования высокоинтеллектуального оборудования, которое может обмениваться

информацией и принимать решения самостоятельно, без компьютера управления. Центральный компьютер с ПО обеспечивает дополнительный обмен информацией между ПСБ, управление ими и сервисные функции.

В этом случае аппаратные и программные средства разрабатываются в рамках единой системы, что позволяет достигнуть наилучших функциональных и экономических показателей (так как вся разработка сосредоточена, как правило, в одних руках и система, как законченный продукт, поставляется с полной гарантией производителя).

ИСБ с программно-аппаратной интеграцией имеют те же достоинства и функциональные характеристики, что и ИСБ с программной интеграцией. Но при этом надежность данной ИСБ выше, так как в случае выхода из строя компьютера управления или сбоя в работе ПО комплекс не распадется на отдельные системы, и интеграция сохранится между аппаратно интегрированными ПСБ.

Благодаря высокой надежности и наличию развитых функциональных характеристик ИСБ данного вида целесообразно применять на крупных объектах и на объектах с повышенными требованиями к безопасности.

Недостатком здесь является то, что каждая фирма предлагает свою оригинальную систему, не совместимую, как правило, с системами других производителей. Данный недостаток обусловлен отсутствием стандартов на сопряжение подсистем ИСБ. Определенный прогресс в этом направлении возможен по мере разработки нормативной базы.

В итоге проведенной классификации ИСБ можно отметить области применения различных типов ИСБ, обусловленные их архитектурой. Аппаратно-реализованные ИСБ целесообразно применять на небольших объектах с невысоким бюджетом. Благодаря более высокой надежности и быстродействию, программно-аппаратные ИСБ применяются на крупных объектах и на объектах с повышенными требованиями к безопасности.

2.2 Принципы организации ИСБ

ИСБ представляют собой сложные программируемые многофункциональные составные изделия, которые производятся предприятием-изготовителем по нормативной документации, утвержденной в установленном порядке [42].

В общем случае состав технических подсистем ИСБ на основе функциональных блоков аналогичен составу технических подсистем КСБ. Конкретный состав функциональных блоков ИСБ определяют при целевой разработке в соответствии с техническим заданием [15]. При этом структура подсистем, элементы которых взаимодействуют (интегрируются) между собой, определяется уровнем интеграции, на котором это взаимодействие происходит.

По функциональному назначению можно выделить следующие уровни взаимодействия элементов ПСБ [1, 37, 39].

Высший (глобальный) уровень (рис.2.1) предполагает взаимодействие интегрированных СБ с другими информационными системами, представляет собой компьютерную сеть типа «клиент/сервер» на основе сети *Ethernet*, с протоколом обмена *TCP/IP* и использованием сетевых операционных систем (ОС) профессионального класса типа *Windows* или *Linux*. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов, здесь обеспечивается управление ИСБ с использованием программного обеспечения АРМ. На данном уровне необходима высокая надежность и защита от несанкционированного доступа.

Первый (системный) уровень предполагает информационное взаимодействие ССОИУ отдельных ПСБ и подсистем противодействия и ликвидации угроз в пределах ИСБ (это могут быть приемно-контрольные приборы, обеспечивающие управление средствами ОПС, контроллеры СКУД, а также универсальные контроллеры для обеспечения управления автоматикой). На данном уровне ССОИУЦ или центральный процессор (сервер) объединяет все подсистемы ИКСБ и обеспечивает их взаимодействие. Каждая из подсистем автоматически выполняет какие-либо действия при поступлении определенного сигнала от любой другой.

Второй (системный) уровень – предполагает интеграцию локальных (или периферийных) систем сбора и обработки информации отдельных ПСБ. Интеграция может осуществляться по каналам связи ПСБ или через интерфейсы интеграции периферийных систем обработки (ИИПСО). Здесь возможно сочетание вертикальной интеграции (связь между контроллерами и компьютерами подсистем) и горизонтальной интеграции (связь между однородными контроллерами в каждой из подсистем). На вертикальном уровне наиболее часто используется интерфейс *RS*-232, на горизонтальном уровне – *RS*-485 или другие интерфейсы, предназначенные для построения сетей промышленного уровня с хорошей помехозащищенностью и достаточной скоростью обмена данными. В контроллерах некоторых ИКСБ возможен прямой выход на первый уровень в протоколе *TCP/IP*.

Третий (модульный) уровень предполагает взаимодействие между ССОИУП и СОУ своих подсистем. Контроллеры «местного» значения управляют небольшой группой извещателей, видеокамер, считывателей, исполнительных устройств и т.п. Здесь, как правило, применяются интерфейсы *RS*-485, *RS*-232 или стандартные интерфейсы считывателей *Wigand* 26. На этом уровне располагаются также средства управления оповещением, пожаротушением и противопожарной автоматикой, адресные блоки управления с релейными и потенциальными выходами.

Модульное построение ИКСБ имеет ряд преимуществ. Благодаря гибкой архитектуре система легко конструируется из определенного набора модулей и блоков практически для любых объектов. В процессе эксплуатации достаточно просто наращивать и совершенствовать функции системы путем подключения различных типов регистрирующих и исполнительных устройств [39].

Четвертый (нижний) уровень предполагает взаимодействие СОУ различных ПСБ через обобщенные шлейфы или соответствующие интерфейсы интеграции устройств обнаружения (ИИУО).

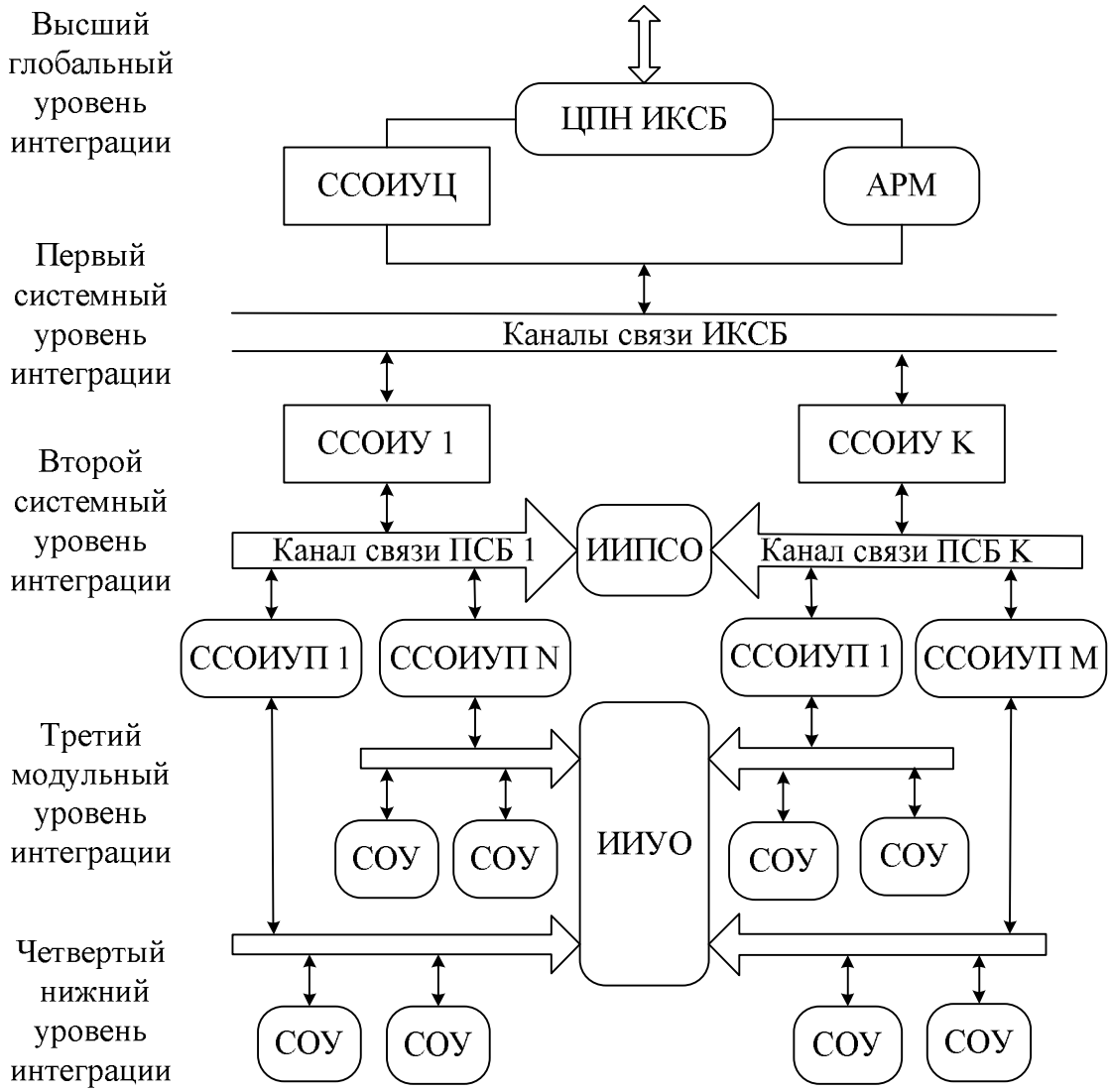

Рисунок 2.1 – Уровни интеграции различных элементов ИКСБ

Рассмотренное взаимодействие в общем случае может быть как аппаратным, так и программным. Верхние уровни взаимодействуют, как правило, на программном уровне, более низкие уровни могут использовать оба вида интеграции.

2.3 Структурные схемы ИСБ

Анализ существующих СБ позволяет выделить следующие основные структурные схемы ИСБ [1].

1. Обобщенная структурная схема ИСБ приведена на рис. 2.2

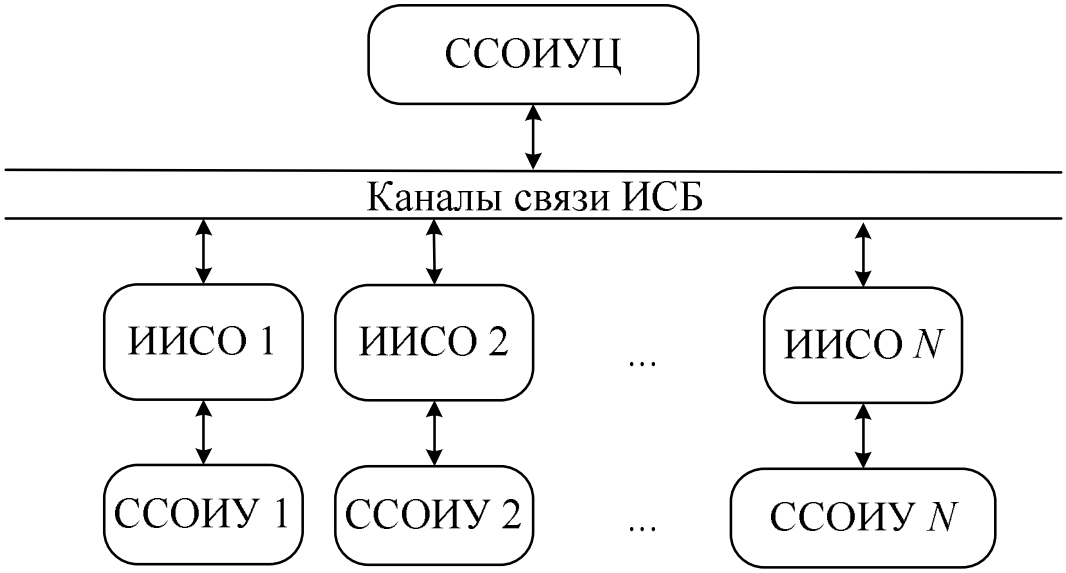

Рисунок 2.2 – Обобщенная структурная схема ИСБ

ИСБ включает в себя *N* подсистем безопасности (охранной и пожарной сигнализации, контроля и управления доступом и т.д.). ПСБ с помощью средств интеграции – специализированных интерфейсов интеграции систем обработки (ИИСО) через каналы связи взаимодействуют с центральной системой сбора и обработки информации и управления (ССОИУЦ). Специализированные ИИСО обеспечивают сигнальную (по физической природе сигналов, их параметрам) и нитратную совместимость (по типам разъемов, соединителей) с входными элементами канала связи, а также требуемую форму представления сигналов (форматы) и процедуру обмена данными (протоколы). В частном случае, средства интеграции могут отсутствовать при наличии аппаратной и сигнальной совместимости с каналом связи. На этой схеме указаны уровни системы и подсистем. Уровни локальных (периферийных) ССОИУ не рассматриваются.

2. Структурные схемы ИСБ системного уровня

Интеграция со специализированным ПО

Интеграция подсистем ИСБ может осуществляться по различным схемам в зависимости от конкретной задачи, угроз и т.п. В общем случае ССОИУЦ, АРМ администратора, рабочие АРМ ИСБ и специализированные АРМ (СОТ, СКУД и т. п.) формируют пульт централизованного наблюдения (ПЦН). Пример структурной схемы ИСБ со специализированным ПО представлен на рис. 2.3.

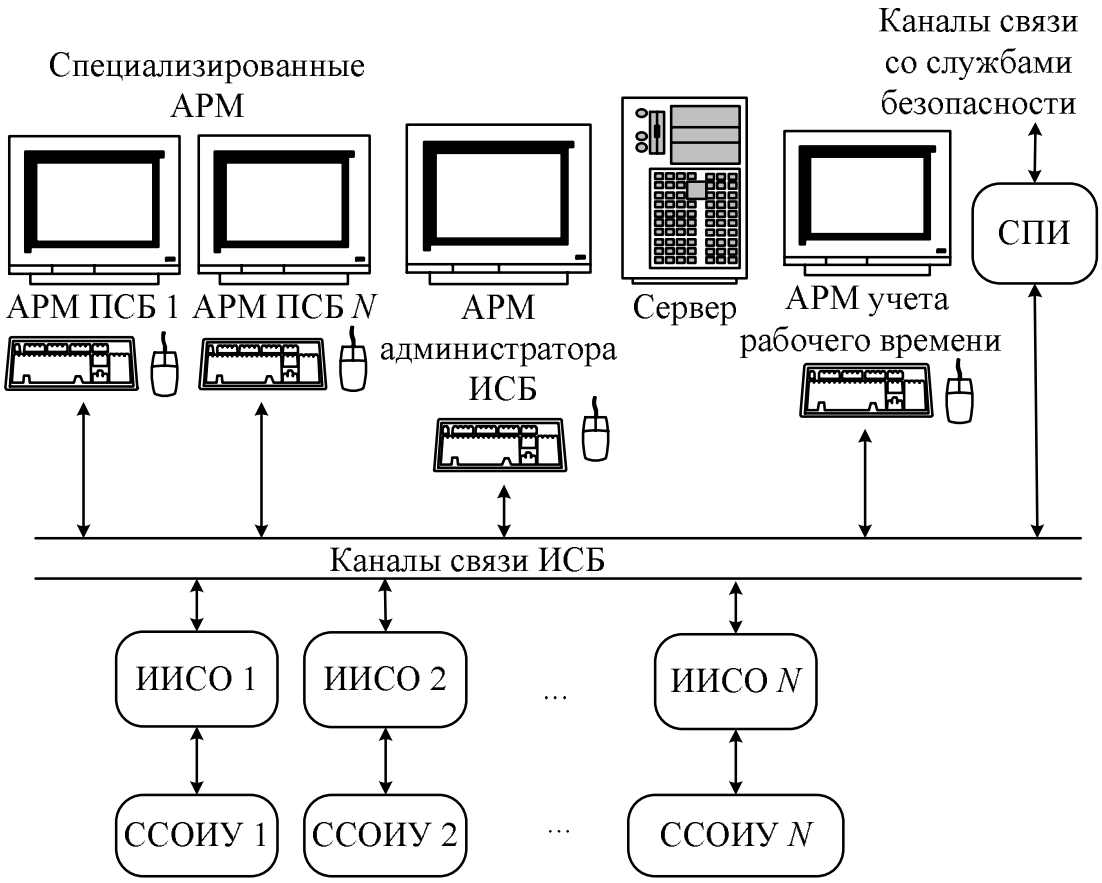

Рисунок 2.3 – Структурная схема ИСБ со специализированным ПО

Здесь используются специализированное программное обеспечение и универсальное аппаратное обеспечение, включая сетевые средства, например, локальные (*LAN*) или персональные (*PAN*) сети.

Интеграция с системным ПО

Данный вариант интеграции ПСБ является частным случаем рассмотренного выше взаимодействия на системном уровне и представлен схемой на рис. 2.4.

В такой структуре функции интерфейсов интеграции выполняет специализированный контроллер (СК). Системное ПО контроллера СКУД выполняет также часть функций ССОИУЦ по выделенным каналам связи (например, *RS*-232, *RS*-485) и общему каналу связи с подсистемами. Управление ведется с АРМ. Здесь мы имеем случай системного как аппаратного, так и программного обеспечения. Подобные структуры используют, как правило, ИСБ для небольших и средних объектов.

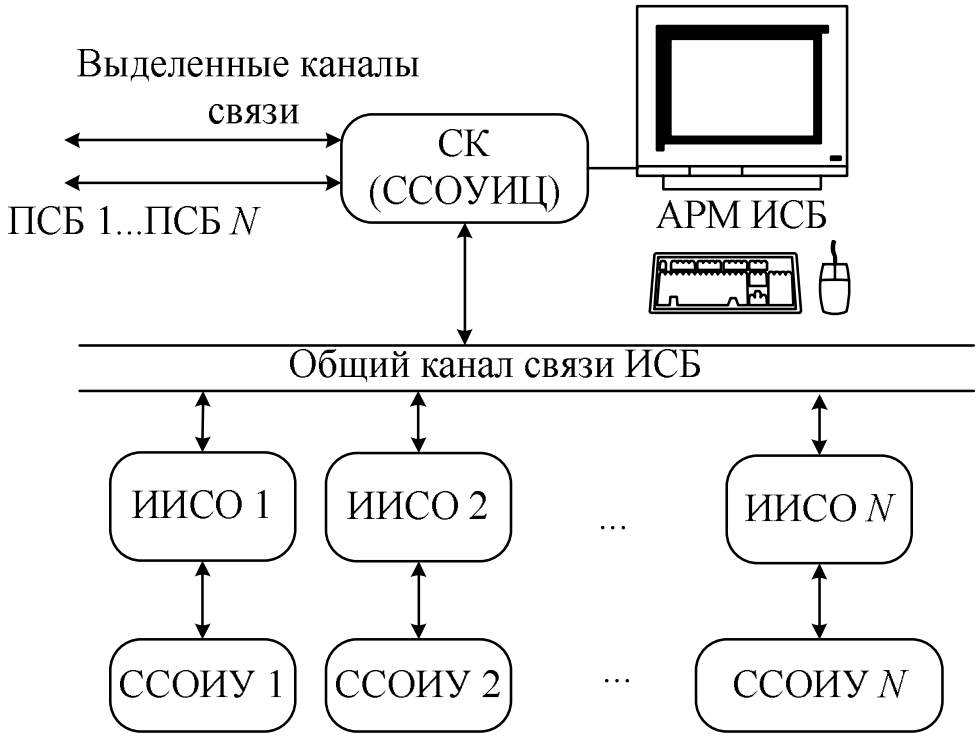

Рисунок 2.4 – Структурная схема ИСБ со специализированным контроллером

3. Структурная схема ИКСБ

Обобщенная структурная схема комплексной ИСБ должна быть дополнена подсистемами противодействия и ликвидации угроз (ПСПЛ) (рис. 2.5).

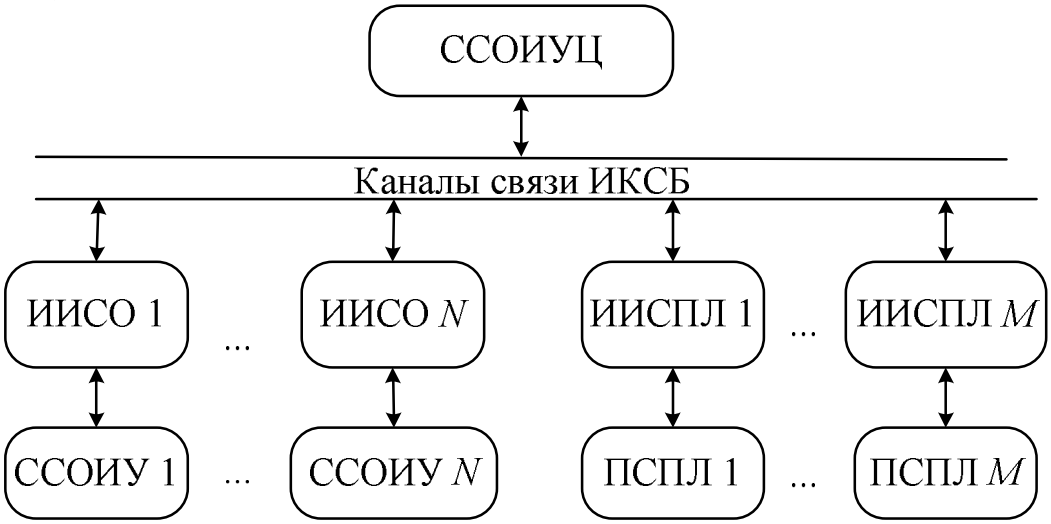

Рисунок 2.5 – Обобщенная структурная схема ИКСБ

ИКСБ включает в себя N подсистем безопасности и M подсистем противодействия и ликвидации угроз. В общем случае значения порядков указанных подсистем будут различными. Например, одна подсистема ОПС решает задачу обнаружения двух или трёх угроз (проникновения, нападения и возгорания).

3 СИСТЕМЫ ОХРАННОЙ, ТРЕВОЖНОЙ И ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Все элементы обобщенной структурной схемы КСБ (рис. 1.3) имеют важное значение при организации эффективной защиты объекта. При этом можно выделить три основные группы, без которых невозможна реализация СБ. Во-первых, это средства обнаружения угроз; во-вторых, система сбора и обработки информации; в-третьих, средства, связанные с тем или иным способом передачи информации о состоянии системы по каналам связи, доведения ее до потребителя (пользователей системы, специальных служб), а также обеспечивающие реакцию системы на обнаруженное событие.

Поэтому будем рассматривать именно эти три основные группы ТСО при описании следующих технических подсистем комплекса ТСОБ (рис.1.2):

1. системы охранной и тревожной сигнализации (СОТС);
2. системы пожарной сигнализации (СПС);
3. системы контроля и управления доступом (СКУД);
4. системы охранной телевизионной (СОТ).

3.1 Назначение и состав СОТС и СПС

Системы СОТС и СПС предназначены для определения факта несанкционированного проникновения на охраняемый объект или появления признаков пожара, выдачи сигнала тревоги и включения исполнительных устройств (световых и звуковых оповещателей, реле и др.).

СОТС содержит следующие основные элементы:

- СОУ – извещатели;
- средства тревожной сигнализации – кнопки, педали, извещатели;
- средства сбора, обработки, отображения информации и управления – прибор приемно-контрольный (ППК) охранный, контрольные панели, концентраторы, компьютеры, расширители, адресные и релейные модули, модемы, световые и звуковые оповещатели и т.п.

СПС содержит следующие основные элементы:

- СОУ – пожарные извещатели (тепловые, дымовые, световые (пламени), газовые, ручные и т.п.);
- средства сбора, обработки, отображения информации и управления – ППК пожарный, контрольные панели, пульты, компьютеры, панели и консоли управления, адресные модули, расширители, световые и звуковые оповещатели, согласующие устройства и т.п.

Оборудование помещений объекта техническими средствами пожарной сигнализации (ТС ПС) и противопожарной защиты жестко регламентируется существующими нормативными документами

[11, 16, 32, 43]. ТС ПС оборудуют все помещения объекта независимо от их назначения, за исключением помещений с мокрыми технологическими процессами (душевые комнаты, сауны и т.п.).

При этом допускается применять только ТС ПС и пожаротушения российского и зарубежного производства, имеющие сертификат соответствия ГОСТ Р в области пожарной безопасности.

Пожарные извещатели включаются в самостоятельные шлейфы СПС, которые должны быть подключены с функцией "Без права отключения" на пульт внутренней охраны или ППК. Установленная СПС должна быть рассчитана на круглосуточную непрерывную работу.

СОТС и СПС по идеологии построения очень близки друг другу и на небольших объектах, как правило, бывают совмещены на базе единого контрольного блока – ППК или контрольной панели. При этом реализуется охранно-пожарная сигнализация (ОПС), основной задачей которой является получение, обработка, передача и представление в заданном виде потребителям информации о проникновении на охраняемые объекты и пожаре на них с помощью технических средств. Пример структурной схемы ОПС предложен на рис. 3.1. Информация в ОПС доводится до персонала, на который возложены функции реагирования на тревожные и служебные извещения, поступающие с охраняемых объектов [37, 39].

Каждая ОПС использует извещатели, контролирующие различные физические параметры среды. В зависимости от способов выявления угроз и формирования сигналов, все извещатели и системы ОПС делятся на неадресные, адресные и адресно-аналоговые.

В неадресных системах извещатели имеют фиксированный порог чувствительности. При этом группа извещателей включается в общий шлейф ОПС, в котором в случае срабатывания одного из них формируется обобщенный сигнал тревоги.

Адресные системы отличаются наличием в извещении информации об адресе извещателя ОПС, что позволяет определить зону пожара с точностью до места расположения извещателя.

Адресно-аналоговая ОПС является наиболее информативной и развитой. В такой системе применяются "интеллектуальные" извещатели, которые передают текущие значения контролируемого параметра вместе со своим адресом по шлейфу ОПС. Такой способ мониторинга используется для раннего обнаружения тревожной ситуации, получения данных о необходимости технического обслуживания извещателей вследствие загрязнения или других факторов. Кроме этого, адресно-аналоговые системы позволяют, не прерывая работу ОПС, на программном уровне изменять фиксированный порог чувствительности извещателей при необходимости их адаптации к условиям эксплуатации на объекте.

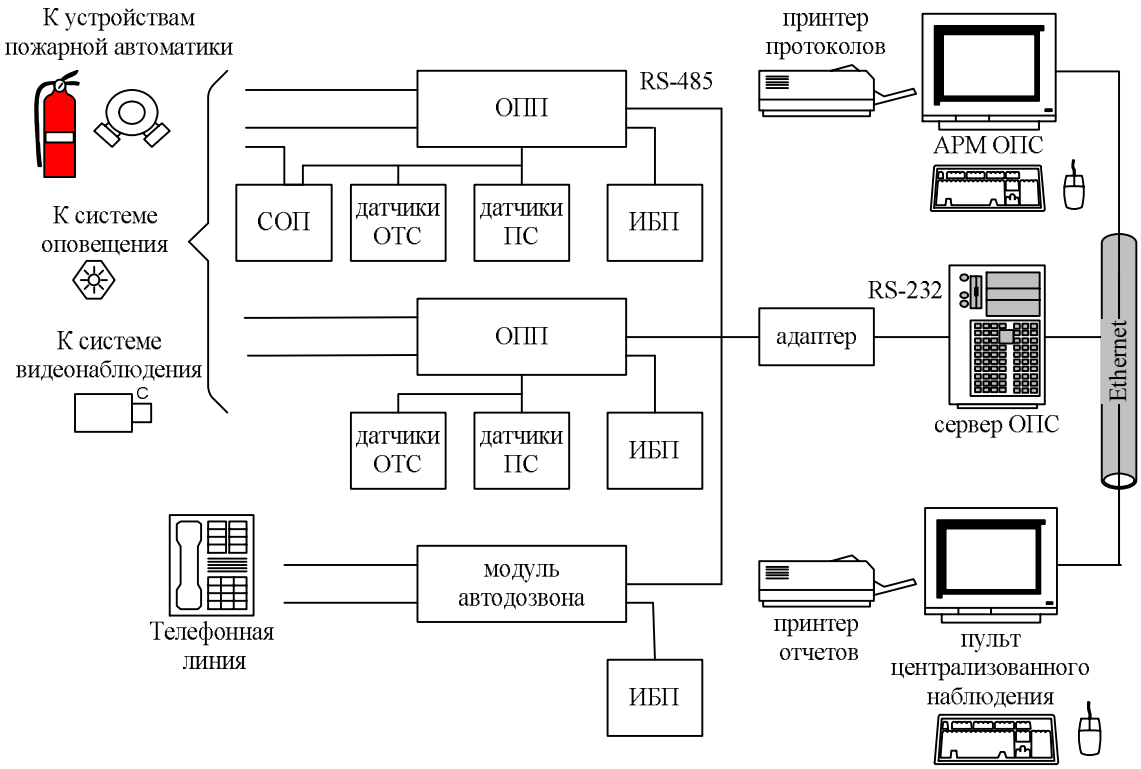

Рисунок 3.1 – Структурная схема охранно-пожарной сигнализации: ОПП – охранно-пожарная панель; АРМ – автоматизированное рабочее место; ОТС – охранно-тревожная сигнализация; ПС – пожарная сигнализация; СОП – система охраны периметра; ИБП – источник бесперебойного питания

Каждый тип извещателя имеет свой перечень основных технических характеристик, определяемых соответствующими стандартами. В то же время, даже однотипные извещатели имеют отличия в конструктивных особенностях составных частей, удобстве эксплуатации, надежности, уровне дизайна, что учитывается при выборе того или иного извещателя или фирмы-производителя.

3.2 Средства обнаружения угроз в составе ОПС

Наличие угрозы безопасности объекта определяется по большому числу физико-химических явлений с помощью технических средств, в основу построения которых положены различные принципы регистрации изменений состояния среды.

Технические средства обнаружения (ТСО) – это извещатели, которые формируют сигнал тревоги при изменении того или иного контролируемого параметра окружающей среды. Извещатели в составе ОПС отличаются друг от друга типом контролируемого физического параметра, принципом

действия чувствительного элемента, способом передачи информации на центральный пульт управления сигнализацией.

По принципу формирования информационного сигнала о проникновении на объект или пожаре извещатели ОПС делятся на:

– активные, которые генерируют в охраняемой зоне сигнал и реагируют на изменение его параметров;

– пассивные, которые реагируют на изменение параметров окружающей среды, вызванное вторжением нарушителя или возгоранием.

По области применения извещатели подразделяются на охранные, охранно-пожарные и пожарные.

Известны подходы к классификации извещателей охранных (ИО) по следующим признакам функционального назначения [10, 26, 39]:

1. По способу приведения в действие (постановка на охрану, снятие с охраны с центрального пульта) – автоматические и мануальные (ручные, ножные).

2. По условиям эксплуатации – устанавливаемые в отапливаемых помещениях, в неотапливаемых помещениях, для эксплуатации на открытом воздухе (для открытых площадок и периметров объектов).

3. По виду зоны, контролируемой автоматическим извещателем, рассматривают:

– точечный извещатель – контролирует проникновение на объект в точке своей установки;

– линейный извещатель – контролирует состояние вдоль линии, которая может быть образована между передатчиком и приёмником излучения (инфракрасного или микроволнового) или вдоль сенсорного кабеля;

– поверхностный извещатель – контролирует состояние охраняемой поверхности;

– объёмный извещатель – контролирует состояние зоны с тремя измерениями: длиной, шириной, глубиной.

4. По физическим принципам, положенным в основу обнаружения – механические (на практике выделяют электроконтактные, магнитоконтактные, ударно-контактные), электромагнитные бесконтактные, пьезоэлектрические, емкостные, акустические (инфразвуковые, ультразвуковые, звуковые), вибрационные, оптико-электронные (активные и пассивные), радиоволновые, электростатические, трибоэлектрические, радиолучевые (микроволновые), ольфактронные (строятся на принципе обнаружения запаха – одорологии), комбинированные, совмещенные.

5. По количеству зон обнаружения, создаваемых извещателями – однозонные и многозонные.

6. По дальности действия ультразвуковые, оптико-электронные и радиоволновые ИО для закрытых помещений рассматривают:

– малой дальности действия – до 12 м;
– средней дальности действия – свыше 12 до 30 м;
– большой дальности действия – свыше 30 м (кроме ультразвуковых).

7. По дальности действия оптико-электронные и радиоволновые ИО для открытых площадок и периметров объектов рассматривают:
– малой дальности действия – до 50 м;
– средней дальности действия – свыше 50 до 200 м;
– большой дальности действия – свыше 200 м.

8. По конструктивному исполнению ультразвуковые, оптико-электронные и радиоволновые ИО подразделяют на:
– однопозиционные – один или более передатчиков (излучателей) и приемник(и) совмещены в одном блоке;
– двухпозиционные – передатчик (излучатель) и приемник выполнены в виде отдельных блоков;
– многопозиционные – более двух блоков (один передатчик, два или более приемников; один приемник, два или более передатчиков).

9. По способу электропитания извещатели подразделяются на:
– токонепотребляющие (используется "сухой" контакт);
– питающиеся от шлейфа сигнализации;
– питающиеся от внутреннего автономного источника питания;
– питающиеся от внешнего источника постоянного тока напряжением 12-24 В;
– питающиеся от сети переменного тока напряжением 220 В.

Охранно-пожарные извещатели в настоящее время практически не выпускаются и не применяются.

Извещатели пожарные (ИП) классифицируют по следующим функциональным признакам [16, 39].

1. По способу приведения в действие – автоматические и ручные.

2. По характеру обмена информацией с ССОИУ автоматические ИП подразделяют на пороговые и аналоговые.

3. По виду контролируемого признака пожара автоматические ИП подразделяют на:
– тепловые, реагирующие на повышение температуры;
– дымовые, реагирующие на появление дыма;
– световые (пламени), реагирующие на оптическое излучение открытого пламени;
– газовые;
– комбинированные;
– по другому признаку пожара.

4. По характеру реакции на контролируемый признак пожара пороговые тепловые ИП подразделяют на максимальные, дифференциальные, максимально-дифференциальные.

5. По принципу действия дымовые ИП подразделяют на оптико-электронные и ионизационные.

6. По конфигурации измерительной зоны тепловые, газовые и дымовые оптико-электронные ИП подразделяют на:

- точечные, реагирующие на факторы пожара в компактной зоне;
- линейные, чувствительный элемент которых представляет собой термокабель или трубку (с помощью управляющего блока могут быть заданы разные пороги температуры срабатывания протяженной линии);
- многоточечные.

7. По рабочей области спектра излучения от пламени для чувствительного элемента, световые ИП подразделяют на:

- ультрафиолетового спектра;
- инфракрасного спектра;
- видимого спектра;
- многодиапазонного спектра.

8. По способу электропитания подразделяют на:

- питающиеся от шлейфа сигнализации;
- питающиеся от встроенного внутреннего источника питания (автономные ИП);
- питающиеся от внешнего источника постоянного тока.

Вероятность обнаружения комплекса угроз зависит от тактико-технических характеристик извещателей, которые закладываются, исходя из уровня необходимой защиты в зависимости от категории важности объекта охраны, и возможными (разумными) затратами на создание (приобретение) извещателей для конкретного объекта. Поэтому грамотный выбор извещателей является обязательным условием для построения эффективной СБ.

3.2.1 Извещатели охранные

Рассмотрим функциональные особенности некоторых активно применяемых на практике охранных извещателей в соответствии с определениями, которые даны в нормативных документах [11, 10, 37].

ИО точечный электроконтактный формирует извещение о тревоге при замыкании/размыкании электрических контактов (чувствительных элементов) от воздействия объекта обнаружения. Это самый простой тип охранных извещателей. Он представляют собой тонкий металлический проводник (фольгу, провод), специальным образом закрепленный на

защищаемом предмете или конструкции. Предназначен для защиты строительных конструкций (стёкол, дверей, люков, ворот, некапитальных перегородок, стен и т.п.) от несанкционированного проникновения через них путем разрушения.

ИО магнитоконтактный формирует извещение о тревоге при размыкании магнитных контактов извещателя. Предназначен для блокировки различных строительных конструкций на открывание (дверей, окон, люков, ворот и т.п.). Состоит из герметизированного магнитоуправляемого контакта (геркона) и магнита в пластмассовом или металлическом немагнитном корпусе. Магнит устанавливается на подвижной (открывающейся) части строительной конструкции (полотне двери, створке окна и т.п.), а магнитоуправляемый контакт – на неподвижной части (коробке двери, раме окна и т.п.).

ИО ударно-контактный формирует извещение о тревоге при ударном воздействии объекта обнаружения на контролируемую поверхность охраняемого объекта. Предназначен для блокировки различных остекленных конструкций (окон, витрин, витражей и т.п.) на разбитие. Состоит из блока обработки сигнала и от 5 до 15 датчиков разбития стекла (ДРС). Место расположения указанных составных частей извещателя определяется количеством, взаимным расположением и площадью блокируемых стеклянных полотен.

ИО пьезоэлектрический формирует извещение о тревоге при воздействии упругих волн, возникающих в твердом теле при физическом воздействии на него (ударе с целью разрушения или вскрытия), которое обнаруживается пьезоэлектрическим чувствительным элементом. Предназначен для блокировки строительных конструкций (стен, полов, потолков и т.п.) и отдельных предметов (сейфов, металлических шкафов, банкоматов и т.п.) на разрушение.

ИО (охранно-пожарный) оптико-электронный активный формирует извещение о проникновении (попытке проникновения) или пожаре при нормированном изменении (прекращении) отраженного потока (для однопозиционного извещателя) или прекращении (изменении) принимаемого потока (для двухпозиционного извещателя) энергии оптического излучения извещателя, вызванного движением нарушителя в зоне обнаружения. Зона обнаружения извещателей имеет вид “лучевого барьера”, образованного одним или несколькими расположенными в вертикальной плоскости параллельными узконаправленными лучами. Зоны обнаружения разных извещателей отличаются длиной и количеством лучей. Конструктивно такие ИО состоят из двух отдельных блоков – блока излучателя и блока приемника, разнесенных на рабочее расстояние (дальность действия). Предназначены для защиты внутренних и внешних периметров, окон, витрин и подступов к отдельным предметам (сейфам, музейным экспонатам и т.п.).

ИО (охранно-пожарный) оптико-электронный инфракрасный пассивный реагирует на изменение уровня инфракрасного излучения в результате перемещения человека в зоне обнаружения. Данные извещатели наиболее широко распространены в охранной практике. С помощью специально разработанных для них оптических систем (линз Френеля) можно просто и быстро получать зоны обнаружения различных форм и размеров и использовать их для защиты помещений любой конфигурации.

Извещатель регистрирует разницу между потоками инфракрасного излучения, исходящими от тела человека и фона (под фоном понимается поверхность стен, пола, потолка и других предметов в зоне обнаружения ИО) [49]. Чувствительным элементом является пироэлектрический преобразователь (пироприемник), на котором фокусируется инфракрасное излучение с помощью зеркальной или линзовой оптической системы (последние наиболее широко распространены).

Зона обнаружения извещателя представляет собой пространственную дискретную систему, состоящую из элементарных чувствительных зон в виде лучей, расположенных в один или несколько ярусов или в виде тонких и широких пластин, расположенных в вертикальной плоскости. Условно зоны обнаружения извещателей можно разделить на несколько видов: широкоугольная одноярусная типа “веер”; широкоугольная многоярусная; узконаправленная типа “занавес”, узконаправленная типа “лучевой барьер”; панорамная многоярусная и другие [26, 37, 39].

Возможность формирования зон обнаружения различной конфигурации объясняет универсальность применения пассивных инфракрасных оптико-электронных извещателей, которые могут использоваться для блокировки объемов помещений, мест сосредоточения ценностей, коридоров, внутренних периметров, проходов между стеллажами, оконных и дверных проемов, полов, потолков, помещений с наличием мелких животных, складских помещений и т.п.

ИО ёмкостный формирует извещение о тревоге при изменении емкости его чувствительного элемента (антенны), которое может быть обусловлено приближением человека к объекту охраны или его прикосновением к охраняемому предмету. При этом охраняемый предмет должен устанавливаться на полу с хорошим изоляционным покрытием или на изолирующей прокладке. Ёмкостные извещатели предназначены для блокировки металлических шкафов, сейфов, отдельных предметов, создания защитных заграждений. При этом к одному извещателю в помещении допускается подключать несколько металлических сейфов или шкафов. Количество подключаемых предметов зависит от их емкости, конструктивных особенностей помещения и уточняется при настройке извещателя.

ИО пассивный звуковой (акустический) предназначен для дистанционного обнаружения разрушения стеклянного листа путем

регистрации звуковых колебаний в помещении, генерируемых стеклом при его разрушении под воздействием механического удара, и для формирования извещения о тревоге [9]. Применяется для блокировки остекленных конструкций (окон, витрин, витражей и т.п.) на разбитие. При установке извещателя все участки охраняемой остекленной конструкции должны быть в пределах его прямого обозрения.

Извещатель охранно-пожарный ультразвуковой формирует извещение о проникновении (попытке проникновения) или пожаре (загорании) при воздействии на поле акустических волн ультразвукового диапазона, излучаемых извещателем, признаков появления человека или пожара в зоне обнаружения. Предназначен для блокировки объемов закрытых помещений. Зона обнаружения имеет форму эллипсоида вращения или каплевидную форму. Из-за низкой помехоустойчивости и сложности эксплуатации в настоящее время почти не используются.

ИО радиоволновый формирует извещение о проникновении (попытке проникновения) при нормированном возмущении поля электромагнитных волн сверхвысокочастотного (СВЧ) диапазона в его зоне обнаружения. Предназначен для защиты объемов закрытых помещений, внутренних и внешних периметров, отдельных предметов и строительных конструкций, открытых площадок. Зона обнаружения также имеет форму эллипсоида вращения или каплевидную форму и для разных извещателей различается только размерами. Различают одно- и двухпозиционные ИО. Однопозиционные применяют для защиты объемов закрытых помещений и открытых площадок. Двухпозиционные – для защиты периметров.

При выборе, установке и эксплуатации радиоволновых ИО следует помнить об их особенности – высокой проникающей способности излучения. Для электромагнитных волн СВЧ-диапазона некоторые строительные материалы и конструкции не являются препятствием (экраном), и они свободно, с некоторым ослаблением, проникают сквозь них. Поэтому зона обнаружения радиоволнового ИО может выходить за пределы охраняемого помещения, что может вызвать ложные срабатывания. К проницаемым материалам и конструкциям относятся, например, тонкие гипсокартонные перегородки, окна, деревянные и пластиковые двери и т.п. Поэтому радиоволновые ИО не следует ориентировать на оконные проемы, тонкие стены и перегородки, за которыми в период охраны возможно движение крупногабаритных предметов и людей. Не рекомендуется их применять на объектах, вблизи которых расположены мощные радиопередающие средства.

По сочетанию принципов обнаружения различают ИО, использующие один физический принцип (рассмотренные выше), а также два и более физических принципа: комбинированные, совмещенные (например, пассивный оптико-электронный с радиоволновым, ударно-контактный с магнитоконтактным и др.).

ИО комбинированный позволяет выявить объект обнаружения на основе использования двух и более различных физических принципов действия, при этом совмещаются зоны обнаружения по этим принципам.

При этом комбинированный ИО содержит каналы разного типа, которые защищают одну и ту же зону. Соответственно, ИО имеет только один выход тревоги, который активизируется в соответствии с заложенной логикой работы (два канала ИО объединены по схеме «и», т.е. только при срабатывании обоих каналов формируется тревожное извещение).

Каждый канал указанного ИО реализует свой физический принцип работы, а, следовательно, имеет свой набор факторов, вызывающих ложные срабатывания. Таким образом, сочетание каналов с разными наборами факторов, вызывающих ложные срабатывания, позволяет значительно снизить вероятность ложного срабатывания ИО в целом.

ИО совмещенный формирует извещение о тревоге при различных видах физического воздействия объекта обнаружения. Представляет собой два ИО, построенных на разных физических принципах обнаружения, объединенных конструктивно в одном корпусе. Каждый ИО работает независимо от другого и имеет свою зону обнаружения и свой собственный выход для подключения к шлейфу сигнализации. Наиболее широко распространена комбинация инфракрасных пассивных и звуковых извещателей [34, 39].

В соответствии с требованиями технического регламента ИО должны иметь следующие функциональные характеристики [40]:

- вид зоны обнаружения (точечная, линейная, поверхностная, объемная, комбинированная);
- размеры зоны обнаружения;
- чувствительность;
- помехоустойчивость;
- вероятность обнаружения.

ИО должны иметь защиту от несанкционированных действий, совершаемых в целях исключения их работоспособности.

3.2.2 Извещатели тревожной сигнализации

Извещатели тревожной сигнализации предназначены для ручной или автоматической подачи тревожного извещения на внутренний пульт охраны объекта в случаях возможного преступного нападения на сотрудников, клиентов или посетителей объекта.

В качестве извещателей тревожной сигнализации используются различные кнопки и педали ручного и ножного действия на основе магнито- и электроконтактных извещателей. Указанные извещатели имеют фиксацию в нажатом состоянии, и возврат в исходное положение возможен только с помощью ключа.

Особое место среди извещателей тревожной сигнализации занимают извещатели-ловушки. **Извещатель-ловушка** – это извещатель, скрытно устанавливаемый внутри охраняемого объекта на наиболее вероятном направлении перемещения нарушителя, блокирующий или имитирующий какой-либо предмет, наиболее подверженный криминальной угрозе [11]. Он предназначен для подачи тревожного извещения при попытке хищения денег или ограбления охраняемого объекта независимо от действий персонала. Он может представлять собой имитацию пачки денег в банковской упаковке объемом 100 купюр, в которую вмонтирован магнит. В специальную подставку, на которой располагается пачка, устанавливается магнитный датчик (геркон). При изъятии (перемещении) имитационной пачки денег с подставки происходит размыкание контактов магнитного датчика, и на пульт охраны объекта поступает тревожное извещение.

3.2.3 Извещатели пожарные

В настоящее время извещатель пожарный (ИП) является единственным устройством обнаружения пожара. Поэтому грамотный выбор типа ИП и места его установки определяет эффективность всей СПС, а, следовательно, безопасность жизни, здоровья людей и сохранность имущества. Рассмотрим определения основных ИП [5, 11, 16] в соответствии с приведенной ранее классификацией.

Извещатель пожарный – техническое средство, предназначенное для обнаружения факторов пожара и/или формирования сигнала о пожаре.

ИП тепловой максимальный срабатывает при превышении определенного значения температуры окружающей среды. Температура срабатывания находится в диапазоне от 54 до 160 градусов.

ИП тепловой дифференциальный срабатывает при превышении определенного значения скорости нарастания температуры окружающей среды. Применяется, если на начальных стадиях пожара выделяется значительное количество теплоты, например на складах горюче-смазочных материалов, либо в случаях, когда применение других ИП невозможно.

ИП дымовой оптико-электронный реагирует на продукты горения, способные воздействовать на поглощающую или рассеивающую способность излучения в инфракрасном, ультрафиолетовом или видимом диапазонах спектра.

ИП дымовой оптико-электронный точечный реагирует на продукты горения, способные поглощать, рассеивать или отражать излучение оптического сигнала, чувствительная зона для которого расположена в ограниченном объеме, много меньшем объема защищаемого помещения. Принцип действия основан на рассеивании серым дымом инфракрасного излучения. Хорошо реагирует на серый дым, выделяющийся при тлении на

ранних стадиях пожара. Плохо реагирует на черный дым, поглощающий инфракрасное излучение.

ИП дымовой оптико-электронный линейный – двухкомпонентный ИП, оптический луч которого проходит вне самого извещателя через контролируемую среду. Состоит из блока приемника и блока излучателя (либо одного блока приемника-излучателя и отражателя), реагирует на появление дыма между блоком приемника и излучателя.

ИП дымовой ионизационный – принцип действия основан на снижении значения электрического тока, протекающего через ионизированный воздух, при появлении частиц дыма (аэрозоля).

ИП аспирационный использует принудительный отбор воздуха из защищаемого объёма с мониторингом ультрачувствительными лазерными датчиками. Обеспечивает сверхраннее обнаружение критической ситуации, когда нужно обнаружить и ликвидировать очаг на самой ранней стадии развития, на этапе тления – задолго до появления открытого огня, либо при возникновении перегрева отдельных компонентов оборудования.

Аспирационные извещатели позволяют защитить объекты, в которых невозможно непосредственно разместить ИП. Применяются в больничных помещениях с высокотехнологичным диагностическим оборудованием, в помещениях архивов, музеев, складов, центров управления, серверных, компьютерных залов, радиовещательных станций, телевизионных центров, “чистых” производственных зон, в коммутаторных помещениях электронных узлов связи и в других помещениях с дорогостоящим оборудованием. Недостатком аспирационных извещателей является их высокая стоимость.

ИП световой (пламени) реагирует на электромагнитное излучение пламени или тлеющего очага. Применяется для защиты зон, где необходима высокая эффективность обнаружения, когда температура в помещении ещё далека от значений, при которых срабатывают тепловые ИП. Также применяется для защиты зон со значительным теплообменом и открытых площадок, где невозможно применение тепловых и дымовых ИП. Кроме того, применяется для контроля наличия перегретых поверхностей агрегатов при авариях, например, для обнаружения пожара в салоне автомобиля, под обшивкой агрегата, контроля наличия твердых фрагментов перегретого топлива на транспортере.

ИП ручной предназначен для ручного включения сигнала пожарной тревоги в системах пожарной сигнализации и пожаротушения. Ручные ИП должны устанавливаться на путях эвакуации в местах, доступных для их включения при возникновении пожара.

При защите техническими средствами СПС взрывоопасных объектов необходимо применять ИП со средствами взрывозащиты. Для точечных дымовых ИП используется тип взрывозащиты “искробезопасная электрическая цепь”. Для тепловых, ручных, газовых и световых

извещателей используется тип взрывозащиты “искробезопасная электрическая цепь” или “взрывонепроницаемая оболочка”. Также возможна в одном извещателе комбинация защит.

3.3 Средства сбора, обработки, отображения информации и управления

Как было указано ранее, аппаратно-технические средства сбора и обработки информации и управления формируют центральную и периферийные ССОИУ, входящие в состав комплексных (интегрированных) СБ. Они предназначены для выполнения ряда основных функций [19, 34, 39], а именно:

- непрерывного сбора информации от извещателей, включенных в шлейфы сигнализации;
- анализа тревожной ситуации на объекте и ее отображения;
- формирования и передачи извещений о состоянии объекта на центральный пост или пульт централизованного наблюдения (ПЦН);
- контроля исправности шлейфов сигнализации и каналов связи;
- управления местными световыми и звуковыми оповещателями, индикаторами и другими устройствами (реле, модемом, передатчиком);
- управления постановкой под охрану и снятием объекта (помещения) с охраны по принятой тактике;
- в ряде случаев обеспечения электропитанием извещателей по цепи шлейфа сигнализации и/или от отдельного выхода ППК при наличии встроенного блока электропитания от сети.

В связи с этим средства сбора и обработки информации должны иметь следующие функциональные характеристики, требования к которым регламентируются нормативными документами [10, 19, 20, 32, 40]:

- информационная ёмкость – количество контролируемых прибором зон безопасности;
- информативность – количество передаваемых (принимаемых) извещений на системы передачи извещений;
- время приема извещения от извещетелей (максимально допустимое время контроля всех извещателей, подключенных к прибору);
- параметры контроля состояния канала связи с извещателями (время обнаружения нарушений канала связи, предельные значения параметров линии связи, при которых должен выдаваться сигнал неисправности линии);
- уровень защиты от несанкционированного доступа к прибору при выполнении функций взятия под охрану и снятия с охраны объекта;
- параметры помехозащищенности линии (канала) связи прибора с извещателями;

- параметры и характеристики интерфейса канала связи прибора со средствами передачи тревожных извещений.

3.3.1 Приборы приемно-контрольные

ППК в системах ОПС являются промежуточным звеном между объектовыми первичными средствами обнаружения проникновения или пожара (извещателями) и СПИ.

ППК охранный (охранно-пожарный) – это техническое средство охранной или охранно-пожарной сигнализации для приема извещений от извещателей (шлейфов сигнализации) или других приемно-контрольных приборов, преобразования сигналов, выдачи извещений для непосредственного восприятия человеком, дальнейшей передачи извещений и включения оповещателей, а в некоторых случаях и для электропитания охранных извещателей [11].

Принята следующая классификация ППК охранных [10, 26, 39].

1. По виду организации тревожной сигнализации на объекте рассматривают ППК:
   - автономные – предназначенные для обеспечения автономной сигнализации, при которой извещения о состоянии контролируемого объекта выдаются только на звуковые и световые оповещатели, установленные на охраняемом объекте или в непосредственной близости к нему;
   - локальные – предназначенные для обеспечения локальной сигнализации на объекте, при которой извещения о состоянии, а также управление контролируемым шлейфом (зонами) осуществляется с помощью средств отображения информации и управления (индикаторные панели, пульты), входящих в состав ППК;
   - централизованные – предназначенные для централизованной сигнализации и работы совместно или в составе СПИ, при которой извещения с ППК передаются на ПЦН СПИ посредством использования различных каналов связи (телефонные линии, радиоканалы, выделенные линии и др.).
2. По способу контроля извещателей ППК подразделяются на:
   - безадресные (без регистрации адреса извещателя) – приборы, имеющие только безадресные шлейфы сигнализации;
   - адресные – приборы, имеющие адресные шлейфы сигнализации;
   - комбинированные – приборы, имеющие безадресные и адресные шлейфы сигнализации.
3. По структуре шлейфа сигнализации рассматривают ППК:
   - со шлейфами сигнализации радиальной структуры;

- со шлейфами сигнализации кольцевой структуры (магистральные);
- со шлейфами сигнализации древовидной структуры;
- со шлейфами сигнализации комбинированной структуры.

4. По виду канала связи с извещателями рассматривают ППК:
   - с проводными каналами связи;
   - с беспроводным (радиоканал или др.) каналом связи;
   - с другими каналами связи (силовая электросеть и т.д.).
5. По информационной емкости рассматривают ППК:
   - малой информационной емкости – до восьми шлейфов сигнализации (адресов);
   - средней информационной емкости – от девяти до 64 шлейфов сигнализации (адресов);
   - большой информационной емкости – свыше 64 шлейфов сигнализации (адресов).
6. По информативности рассматривают ППК:
   - малой информативности – до восьми видов извещений;
   - средней информативности – от девяти до 16 видов извещений;
   - большой информативности – свыше 16 видов извещений.

ППК для локальной сигнализации должны дополнительно к основным функциям обеспечивать:

а) отображение с помощью индикаторов, расположенных на приборе, выносном табло или пульте управления, состояния ППК или каждого шлейфа сигнализации или адреса;

б) звуковую сигнализацию о тревоге с помощью встроенного или внешнего звукового оповещателя;

в) возможность подключения принтера, компьютера, другого устройства для протоколирования событий или хранение данных о событиях для их последующего просмотра с помощью встроенной энергонезависимой памяти. Информация о событиях должна содержать данные о времени, виде события и адресе (номер шлейфа сигнализации или адрес).

Для ППК централизованной сигнализации рекомендуется иметь возможность подключения выносных элементов контроля состояния ППК.

Основными параметрами ППК охранного являются информационная емкость и информативность.

Емкость информационная – это число охраняемых объектов (для СПИ), контролируемых шлейфов сигнализации (для ППК), охраняемых зон, о состоянии которых может оповестить оповещатель (для оповещателей), или защищаемых зон (для приборов управления), информацию о (для) которых может передавать (принимать, отображать и т.п.) техническое средство охранной, пожарной или охранно-пожарной сигнализации [11].

Информативность – это число видов извещений, передаваемых (принимаемых, отображаемых и т.п.) техническим средством охранной,

пожарной или охранно-пожарной сигнализации [11]. Информативность ППК зависит от его класса и вида организации тревожной сигнализации на объекте. Например, для автономных ППК информативность должна составлять не менее четырех извещений: «Норма», «Тревога», «Взят под охрану», «Снят с охраны».

Различают следующие режимы работы ППК охранного:

а) «Снят с охраны» – режим, при котором контролируется только часть шлейфов, световой и звуковой оповещатели выключены;

б) «Норма» – режим, при котором все шлейфы (адреса, зоны), взятые под охрану, находятся в состоянии нормы; при этом световой оповещатель включен в постоянный режим, звуковой – выключен;

в) «Тревога» – режим, при котором хотя бы один ранее взятый под охрану шлейф (адрес, зона) нарушен; при этом световой оповещатель переходит в режим прерывистого включения, звуковой оповещатель включается на время от 3 до 10 мин, затем отключается (если по истечении указанного периода времени произойдет повторное нарушение шлейфов, то звуковой сигнал должен повториться); сигнал тревоги отправляется через СПИ на ПЦН;

г) «Тихая тревога» – режим, включающийся при нарушении специализированных шлейфов (тревожная кнопка); при этом световой и звуковой оповещатель включаться не должны, а сигнал тревоги отправляется через СПИ на ПЦН.

ППК пожарный – техническое средство, предназначенное для приема сигналов от пожарных извещателей, осуществления контроля целостности шлейфа пожарной сигнализации, световой индикации и звуковой сигнализации событий, формирования стартового импульса запуска прибора управления пожарного [43].

3.3.2. Технические средства оповещения

Система оповещения (СО) на охраняемом объекте и его территории создается для оперативного информирования людей о возникшей или приближающейся внештатной ситуации (аварии, пожаре, стихийном бедствии, нападении, террористическом акте) и координации их действий.

Оповещатель для СБ определяется как техническое средство охранной, пожарной или охранно-пожарной сигнализации, предназначенное для оповещения людей на удалении от охраняемого объекта о проникновении (попытке проникновения) и (или) пожаре [11].

Пожарный оповещатель – техническое средство, предназначенное для оповещения людей о пожаре посредством подачи светового, звукового или речевого сигнала [16, 43].

СО классифицируют по следующим признакам [10, 16]:

1. По виду выдаваемых сигналов оповещатели и СО подразделяют на:

- световые (сигнальные лампы, строб-вспышки, световые табло и указатели, в том числе светоуказатели направления движения);
- звуковые (сирены и ревуны, в том числе звукоуказатели эвакуационного выхода);
- речевые (системы громкоговорителей и ретрансляционные системы);
- комбинированные.

2. По информационной емкости (числу обслуживаемых охраняемых зон) – на однозонные и многозонные.

3. По исполнению для различных условий эксплуатации – для использования:
- в отапливаемых помещениях;
- в неотапливаемых помещениях (в том числе под навесами);
- на открытом воздухе.

4. По способу задания оповещателю и СО длительности оповещения, которое устанавливается:
- ППК охранным;
- оповещателем и системой оповещения.

Несмотря на большое разнообразие, системы оповещения имеют следующее строение:

– управление цифровой СО реализуется с помощью компьютера; управление аналоговой СО осуществляется через матричный блок управления, входящий в состав системы;

– блок коммутации сигналов;

– усилительное оборудование (предварительные усилители и усилители мощности) для усиления звуковых сигналов, поступающих от источника звука (микрофон, магнитофон и т.д.);

– выносные микрофонные консоли для организации удаленного рабочего места диспетчера;

– источники сигнала – микрофон, установленный на пульте диспетчера или на блоке тревожного оповещения, генератор тонального сигнала, радиоприемник, *CD*-проигрыватель;

– громкоговорители (рупорные, настенные и потолочные).

На объекте должен быть разработан план оповещения, который в общем случае включает в себя:
- схему вызова сотрудников, должностными обязанностями которых предусмотрено участие в мероприятиях по предотвращению или устранению последствий внештатных ситуаций;
- инструкции, регламентирующие действия сотрудников при внештатных ситуациях;
- планы эвакуации;
- систему сигналов оповещения.

СО должны обеспечивать выполнение следующих функциональных требований [36, 40]:

- подачу звуковых и (или) световых сигналов в здания, помещения, на участки территории объекта с постоянным или временным пребыванием людей;
- трансляцию речевой информации о характере опасности, необходимости и путях эвакуации, других действиях, направленных на обеспечение безопасности людей.

Количество оповещателей, их мощность должны обеспечивать необходимую слышимость во всех местах постоянного или временного пребывания людей. Оповещатели не должны иметь регуляторов громкости и разъемных соединений. Коммуникации СО допускается проектировать совмещенными с радиотрансляционной сетью объекта.

3.4 Средства передачи извещений

Системы передачи извещений (СПИ) о проникновении и пожаре представляет собой совокупность совместно действующих технических средств, предназначенных для контроля и управления территориально-распределенными (рассредоточенными) объектами на расстоянии с применением специальных преобразователей сигналов для эффективного использования каналов связи. При этом в качестве каналов передачи извещений используются линии городской телефонной сети или радиоканал.

СПИ классифицируются по следующим признакам [10, 39, 40]:

1. По информационной емкости (количеству охраняемых объектов) рассматривают СПИ:
   - малой информационной емкости – до 200 номеров (адресов) на охраняемых объектах;
   - средней информационной емкости – от 201 до 1000 номеров (адресов) на охраняемых объектах;
   - большой информационной емкости – свыше 1000 номеров (адресов) на охраняемых объектах.
2. По возможности наращивания информационной емкости – на системы с постоянной информационной емкостью и с возможностью нарашивания информационной емкости.
3. По информативности – на системы малой информативности (до 10 видов извещений), средней информативности (от 11 до 20 видов извещений), большой информативности (свыше 20 видов извещений).
4. По типу используемых линий (каналов) связи – на системы, использующие:
   - выделенные каналы (проводные, оптоволоконные или другие);

- линии (каналы) телефонной сети общего пользования, в том числе переключаемые, занятые телефонной связью, с использованием частотного выделения служебных сигналов, с использованием аппаратуры автоматического набора номера (информаторные);
- радиоканалы специальных радиосетей ведомственной принадлежности или общего пользования, в том числе сетей сотовой связи;
- комбинированные каналы связи.

5. По виду формата сообщения – на системы с постоянным форматом сообщения и с переменным форматом сообщения.

6. По алгоритму обслуживания объектов – на системы неавтоматизированные (с ручным взятием объектов под охрану и снятием с охраны путем ведения телефонных переговоров дежурного пульта управления с хозорганом) и автоматизированные (с автоматическим взятием объектов под охрану и снятием с охраны без ведения телефонных переговоров).

7. По способу отображения поступающей на ПЦН информации – на системы с индивидуальным или групповым отображением информации в виде световых и звуковых сигналов, с отображением информации на дисплеях с применением устройств обработки и накопления базы данных.

8. По числу направлений передачи информации – на системы:
- с однонаправленной передачей информации;
- с двунаправленной передачей информации (с наличием обратного канала) между ПЦН и объектом охраны.

Двунаправленная передача информации позволяет увеличить надежность охраны. Так при отсутствии подтверждения получения информации от ПЦН по одному каналу передачи информации её можно передать по резервному каналу СПИ.

Рассмотрим классификацию СПИ по признаку типа используемых каналов связи.

Различают проводные и радиоканальные СПИ. Организация проводных СПИ возможна на основе телефонных линий связи, по сети 220В или по компьютерной сети. Проводные СПИ на базе телефонных линий реализуются с использованием одного из трех состояний канала связи:

1. **Выделенные линии** телефонной связи с переключением на период охраны. Во время охраны линия переключается на обслуживание системы ОПС. Данные СПИ требуют установок дорогостоящего ретрансляторного оборудования на АТС и блокируют телефонную связь во время охраны. В настоящее время выводятся из эксплуатации.

2. **Занятые линии** телефонной связи. По одной телефонной линии на разных частотах передаются сигналы СПИ и телефонные переговоры. В настоящее время выводятся из эксплуатации.

3. **Коммутируемые телефонные линии**. Передача информации по телефонным линиям осуществляется с помощью специализированных модемов-коммуникаторов по специализированным протоколам: *Contact ID*, *SIA Level* 3, *Fast Format* и др. Модемы-коммуникаторы встроены в объектовые приборы. Достоинствами данного способа передачи извещений являются высокая информативность, доступность оборудования. К недостаткам можно отнести обязательное условие наличия телефонных линий на объекте охраны, сложности при использовании цифровых телефонных линий.

При формировании канала связи по силовой электрической сети 220В передача информации имеет ограниченную дальность. Система имеет небольшую емкость и применяется в основном для охраны малобюджетных объектов.

Системы с передачей информации по компьютерным линиям связи с использованием протокола *TCP/IP* представляют собой перспективное направление развития СПИ, но пока по ряду причин применяются редко.

Система передачи извещений радиоканальная (РСПИ) или СПИ по радиочастотным каналам связи [11] применяется для охраны нетелефонизированных объектов, от которых единственным способом передачи информации является радиосвязь, или как дополнение к телефонному каналу для повышения надежности системы ОПС.

В зависимости от типа используемого радиоканала все РСПИ можно разделить на три основные группы:

- РСПИ, использующие передачу сигнала в общедоступных частотных диапазонах (27, 433, 868 МГц);
- РСПИ, использующие передачу сигнала в выделенных частотных диапазонах (136 – 174МГц, 400 – 512МГц, 30 – 52МГц);
- системы мониторинга, использующие в качестве канала передачи сообщений сотовую связь стандарта GSM (GSM Voice, SMS, GPRS).

Основным преимуществом РСПИ на базе *GSM* является отсутствие необходимости приобретения частотного ресурса и построения сети ретрансляторов, использование существующих сетей ретрансляции, которые обеспечивают дальность действия в рамках зоны покрытия сотовой сети операторов мобильной связи.

Основными недостатками РСПИ на основе каналов сотовой связи являются неопределенное время доставки *SMS*-сообщений, отсутствие гарантированного оперативного соединения (особенно во время пиковых нагрузок сети в праздники), тарифицированная оплата оператору и свободная продажа недорогих устройств подавления каналов сотовой связи.

Основными достоинствами РСПИ с передачей на общедоступных или выделенных частотах являются:

- независимость от наличия телефонных линий или *GSM*-связи;

- оперативность и относительная простота развертывания и внедрения;
- высокая скорость передачи информации (менее секунды);
- высокая информативность сообщений, дающая полную картину о событиях на объектах;
- возможность создания системы охраны в рамках ведомства или отдельной организации.
- К недостаткам указанных РСПИ можно отнести:
- необходимость получения частот и регистрация передатчиков в органах Министерства связи РФ;
- более высокая стоимость базового оборудования, программного обеспечения и их обслуживания;
- необходимость установки ретрансляторов для обслуживания больших территорий;
- отсутствие единых стандартов передачи данных.

Комбинированные (гибридные) СПИ состоят из проводных и радиоканальных каналов СПИ в различных сочетаниях. Комбинированные системы применяются для повышения надежности передачи извещений от объекта охраны на ПЦН. Комбинированные системы имеют более высокую стоимость в сравнении с системами на базе одного канала. Это связано с компенсацией недостатков технического характера, а также с защитой от преднамеренного противодействия со стороны преступников и с расширением функциональных возможностей. Например, при использовании для охраны объекта коммутируемой телефонной линии и прямого радиоканала возможен мониторинг телефонной линии, т.е. в случае нарушения телефонной линии или при саботаже передатчик автоматически сообщит об этом на пульт. Поэтому тенденция выбора средств передачи извещений у средних и крупных охранных предприятий постепенно смещается в сторону гибридных систем обмена данными в силу их универсальности и высокой надежности.

Пульт централизованного наблюдения совместно с СПИ представляет собой систему, предназначенную для сбора информации с объектов, оборудованных средствами ОПС, и передачи информации о состоянии охраняемых объектов на АРМ операторов пульта.

Состав оборудования ПЦН зависит от количества и состава требуемых каналов связи, количества АРМ и других факторов. В общем случае ПЦН состоит из следующих элементов:

- приемник извещений от СПИ;
- сервер сбора, хранения и обработки информации;
- автоматизированное рабочее место оператора ПЦН;
- система связи ПЦН с патрульными экипажами.

ПЦН определяется существующими стандартами как самостоятельное техническое средство (совокупность технических средств) или составная часть СПИ, устанавливаемая в пункте централизованной охраны (пункте установки ПЦН) для приема тревожных извещений о проникновении на охраняемые объекты и/или пожаре на них, служебных и контрольно-диагностических извещений, обработки, отображения, регистрации полученной информации и представления ее в заданном виде для дальнейшей обработки, а также (при наличии обратного канала) для передачи команд телеуправления [11, 34, 40].

Основными техническими характеристиками ПЦН являются:

- информационная емкость (максимальное количество абонентов);
- количество и типы поддерживаемых каналов приема сообщений (радиоканал, телефонный канал, сеть *GSM*, протокол *TCP/IP* и др).

Основные функции ПЦН состоят в следующем [10, 19]:

- прием извещений о состоянии объекта охраны;
- отображение информации о состоянии объектов охраны для АРМ;
- автоматизация работы оператора ПЦН, визуализация плана объекта и подходов к нему, отображение сработавших датчиков и т.п.;
- ведение базы объектов и сигналов, создание и редактирование планов объектов;
- передача данных о тревожных извещениях патрульным экипажам в автоматическом или полуавтоматическом режиме;
- оповещение заказчика о состоянии объекта с передачей информации на телефон или через *Internet*;
- обеспечение многоуровневой системы доступа к информации с администрированием прав;
- документирование информации о состоянии объекта охраны и действиях персонала;
- автоматизация и контроль работы сервисной службы, статистический анализ информации;
- автоматизация учета платежей за услуги охраны (расчет платежей с учетом отключений, авансовых оплат, пени и скидок, выявление и формирование списка должников и т.д.).

Современные ПЦН использует автоматическую тактику постановки объектов под охрану и снятия их с охраны. В этом случае процедура не требует непосредственного участия оператора ПЦН в процессе постановки/снятия с охраны. Это обеспечивает высокую информационную ёмкость ПЦН и его надежную работу в часы пиковых нагрузок.

Для эффективной работы всей системы безопасности объекта СПИ должны иметь следующие функциональные характеристики [20, 40]:

- вид канала передачи данных от объекта до ПЦО;
- вид и количество передаваемых извещений (извещение о проникновении, извещение о пожаре, служебные и контрольно-диагностические сообщения, и другие, если они имеются в системе);
- вид и количество команд для передачи и приема телеуправления (для систем с обратным каналом передачи данных от ПЦО до охраняемого объекта);
- время доставки тревожного извещения (не более 60 секунд);
- приоритеты в передаче тревожных извещений;
- время доставки других видов извещений.

Время обнаружения неисправности канала для СПИ, в зависимости от используемого канала связи, должно быть не более 120 секунд.

4 СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Упорядоченный доступ сотрудников и посетителей, а также транспорта на территорию и в помещения охраняемого объекта организуется контрольно-пропускным режимом. Это комплекс организационно-правовых ограничений и правил, инженерно-технических решений и действий службы безопасности, который устанавливает порядок пропуска через контрольно-пропускные пункты в отдельные здания (помещения) людей, транспорта и материальных средств.

Управление доступом реализуется с помощью программно-технических средств и организационно-административных мероприятий, совокупность которых представляет собой систему контроля и управления доступом (СКУД) как на сам объект, так и в отдельные его помещения.

Целями включения подсистемы контроля и управления доступом в состав ИКСБ объекта являются [13, 15]:

- предотвращение несанкционированного доступа в контрольные зоны с ограниченным доступом, не создавая препятствий для прохода (проезда) в зоны со свободным доступом;
- обеспечение необходимых условий соблюдения внутриобъектового режима и выполнения соответствующих обязанностей персоналом объекта, в зависимости от конкретных условий и особенностей процессов деятельности на объекте, пребывания на нем людей и транспортных средств.

4.1 Назначение, состав и классификация СКУД

Для достижения целей, определенных существующими стандартами, СКУД в составе СБ должны решать следующие задачи [13, 19, 33]:

1. Защита от несанкционированного доступа на охраняемый объект (помещение, зону) в режиме снятия их с охраны:
   - ограничение доступа персонала в охраняемые помещения;
   - временной контроль перемещений персонала (посетителей) по объекту.
2. Контроль и учет доступа персонала (посетителей) на охраняемый объект (помещение, зону) в режиме снятия их с охраны:
   - контроль действий охраны во время дежурства;
   - табельный учет рабочего времени персонала;
   - фиксация времени прихода и ухода посетителей;
   - временной и персональный контроль открытия внутренних помещений (когда и кем открыты).
3. Автоматизация процессов взятия под охрану и снятия с охраны объекта (помещения, зоны) с помощью средств идентификации СКУД в

составе ППК и объектовых устройств СПИ.

4. Регистрация и выдача информации о попытках несанкционированного проникновения в охраняемое помещение.

5. Совместная работа с системами ОПС и СОТ (при срабатывании извещателей блокируются или разблокируются, например, при пожаре, двери охраняемого помещения).

6. Защита и контроль доступа к компьютерам автоматизированных рабочих мест ПЦН и АРМ ИСБ.

7. Защита от несанкционированного доступа к информации.

Решение перечисленных задач аппаратно-программными и техническими средствами КУД основано на организации процессов идентификации и аутентификации личности.

Идентификация предполагает опознавание пользователя по присущему или присвоенному ему идентификационному признаку. При этом выполняется сравнение предъявляемого идентификатора с полным перечнем присвоенных идентификаторов.

Аутентификация подразумевает установление подлинности личности на основе идентификационных признаков пользователя. При этом выполняется сравнение введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного пользователя.

Функционирование СКУД реализуют следующие программно-технические средства:

- приемные устройства доступа (устройства идентификации доступа) – идентификаторы личности, считыватели, кодонаборные устройства;
- ССОИУ – ПК (центральное устройство управления), контроллеры, панели и консоли управлении, согласующие устройства и т.д.;
- преграждающие управляемые устройства доступа (преграждающие конструкции и исполнительные устройства) – электромеханические, электромагнитные и механические кодовые замки, доводчики, автоматические турникеты и шлагбаумы, автоматические и полуавтоматические шлюзы (кабины) и т.д.;
- средства обнаружения различных материалов – металлодетекторы, обнаружители взрывчатых веществ и радиационных материалов и т.д.

Пример структурной схемы СКУД представлен на рис.4.1.

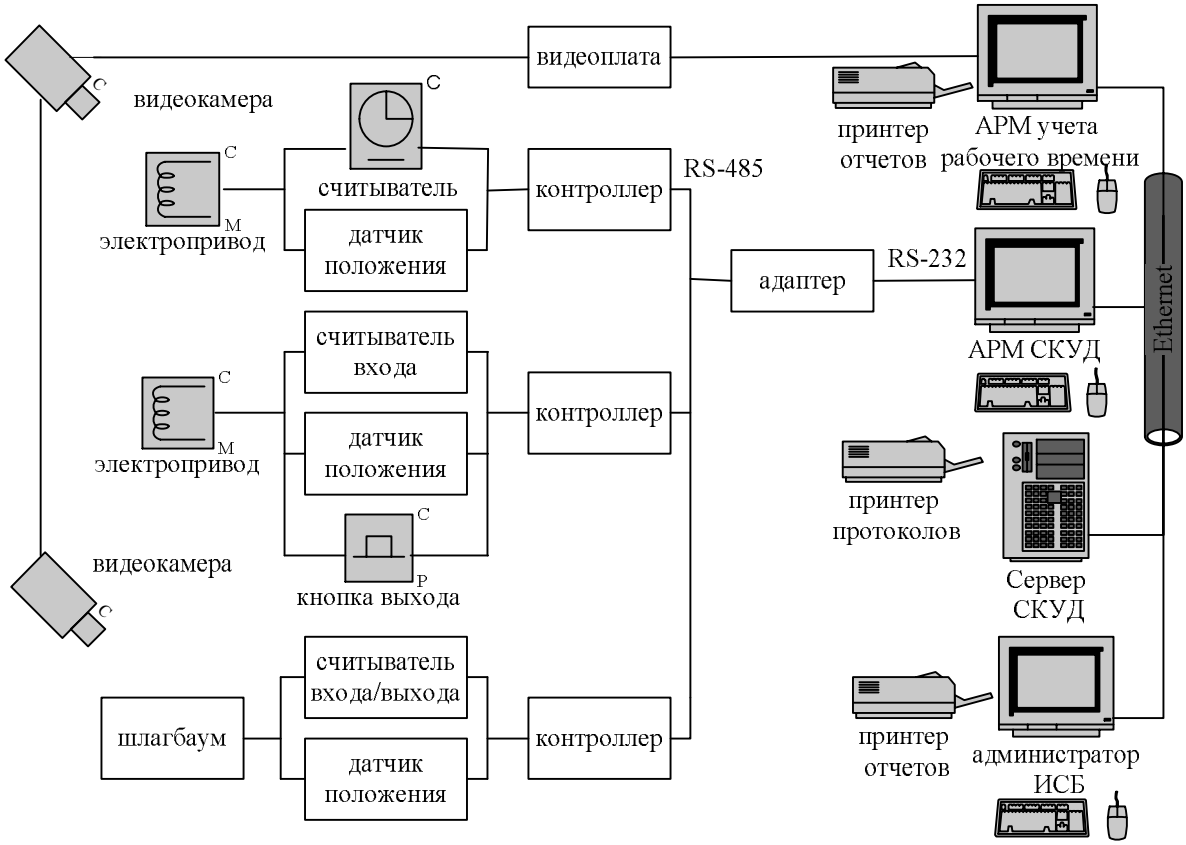

Рисунок 4.1 – Структурная схема системы контроля и управления доступом

Классификацию современных СКУД принято проводить по следующим техническим и функциональным признакам [3, 13, 26, 33, 37]:

1. По способу управления:

- автономные – для управления одним или несколькими исполнительными устройствами без передачи информации на центральное устройство управления и контроля со стороны оператора;
- централизованные (сетевые) – для управления исполнительным устройством с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;
- универсальные или распределенные (комбинированные), включающие в себя функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи.

2. По уровню идентификации:

- одноуровневые (идентификация осуществляется по одному признаку, например, по считыванию кода карты);

- многоуровневые (идентификация осуществляется по нескольким признакам, например, по считыванию кода и биометрическим данным).

3. По числу контролируемых точек доступа (контролируемых мест):
   - малой емкости (не более 84 точек);
   - средней емкости (от 84 до 256 точек);
   - большой емкости (более 256 точек).
4. По функциональным возможностям СКУД делят на четыре класса:
   - 1-й – системы с ограниченными функциями;
   - 2-й – системы с расширенными функциями;
   - 3-й и 4-й – многофункциональные системы.
5. По уровню защищенности системы от несанкционированного доступа к информации.

Деление СКУД на классы выполняется на основе сравнительного анализа ряда их функциональных возможностей: оперативного перепрограммирования, уровня секретности, автоматической идентификации, автоматического сбора и анализа данных, разграничения полномочий пользователей по доступу, выборочной распечатки данных, надежного механического запирания точек доступа с возможностью аварийного ручного открытия.

СКУД 1-го класса – малофункциональные системы малой емкости для работы в автономном режиме и допуска всех лиц, имеющих соответствующий идентификатор. В таких системах используется ручное или автоматическое управление исполнительными устройствами, а также световая или/и звуковая сигнализация. Степень защиты от несанкционированного доступа недостаточная. Применяются на объектах, где требуется только ограничение доступа посторонних лиц.

СКУД 2-го класса – малофункциональные системы малой или средней емкости с возможностью расширения и включения их или их составных частей в общую линию связи. Они могут быть одноуровневыми и многоуровневыми, работают как в автономном, так и в сетевом режимах. Допуск лиц (групп лиц) осуществляется по дате, временным интервалам. Обеспечивается автоматический режим регистрации событий и управления исполнительными устройствами. Степень защиты от несанкционированного доступа средняя. Применяются в качестве дополнения к имеющимся на объектах системам защиты, где требуются учет и контроль присутствия сотрудников в разрешенной зоне.

СКУД 3-го и 4-го классов, как правило, являются сетевыми. В них используются сложные идентификаторы и различные уровни сетевого взаимодействия (клиент-сервер, интерфейсы считывателей карт *Wiegand* или магнитных карт, специализированные интерфейсы и др.).

СКУД 3-го класса – одноуровневые и многоуровневые системы средней емкости, интегрируются с системами ОПС и СОТ на уровне

переключений реле. Количество взаимодействий между ПСБ невелико. Данный уровень является простым, универсальным и надежным, предполагает наличие дополнительных модулей в системе, к которым подключаются охранные или пожарные извещатели, релейные выходы для управления видеокамерами и другими устройствами. Подобная интеграция применяется на малых объектах, где требуется табельный учет и контроль перемещений сотрудников по объекту. Степень защиты от несанкционированного доступа высокая.

СКУД 4-го класса – многоуровневые системы средней и большой емкости. Их отличительной особенностью является наличие развитого программного обеспечения, которое позволяет реализовать большое число функциональных возможностей и высокую степень интеграции на программном (системном) уровне с другими ПСБ. Применяются в интегрированных системах безопасности и управления системами жизнеобеспечения. Степень защиты от несанкционированного доступа очень высокая.

4.2 Устройства идентификации доступа

Устройство идентификации доступа (идентификаторы и считыватели) считывает и расшифровывает информацию, записанную на идентификаторах разного типа и устанавливает права людей, имущества, транспорта на перемещение в охраняемой зоне (объекте).

Контролируемые места, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода) определяются как **точки доступа** и оборудуются считывателем, исполнительным устройством и другими необходимыми средствами.

По виду используемых идентификационных признаков устройства идентификации доступа подразделяются на [13]:

- механические – используют элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
- магнитные – используют намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т.д.);
- оптические – используют нанесенные на поверхность или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, топографические метки);
- электронные контактные – используют электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т.д.);

- электронные радиочастотные – считывание кода происходит путем передачи данных по радиоканалу;
- акустические – используют кодированный акустический сигнал;
- биометрические (для считывателей) – используют индивидуальные физические признаки человека (отпечатки пальцев, геометрию ладони, рисунок сетчатки глаза, голос, динамику подписи и т.д.);
- комбинированные – используют одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков считыватели могут быть:

- с ручным вводом – с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;
- контактными – при непосредственном, в том числе и при электрическом, контакте между считывателей и идентификатором;
- бесконтактными – при поднесении идентификатора на определенное расстояние к считывателю;
- комбинированными.

Для эффективного и надежного управления доступом на охраняемый объект считыватели СКУД должны выполнять следующие функции [19, 37]:

- считывание идентификационного признака с идентификаторов;
- сравнение введенного идентификационного признака с информацией, хранящейся в памяти или базе данных ССОИУ;
- формирование сигнала на открывание исполнительного устройства при положительной идентификации пользователя;
- обмен информацией с ССОИУ.

4.2.1 Идентификатор доступа

Идентификатором доступа является носитель уникального идентификационного признака, по которому определяются полномочия пользователя СКУД и осуществляется управление доступом в охраняемую зону. В качестве такого носителя может использоваться как техническое устройство, так и сам человек (его индивидуальные биологические признаки или память).

В зависимости от вида идентификационного признака, идентификаторы доступа могут быть атрибутными (использующими вещественный код, который передается носителю с помощью специальной технологии) или биометрическими (использующими запоминаемый код или индивидуальные физические признаки человека).

В качестве атрибутных идентификаторов используют автономные носители признаков допуска: магнитные карты, бесконтактные *proxmity*-карты, контактные брелки «*touch-memory*», различные

радиобрелки. К биометрическим идентификаторам относятся изображение радужной оболочки глаза, отпечаток пальца, отпечаток ладони, черты лица и многие другие физические признаки. Каждый идентификатор характеризуется определенным уникальным двоичным кодом.

В соответствии с приведенной выше классификацией рассмотрим наиболее распространенные при организации доступа идентификаторы.

Магнитные карты представляют собой карты с магнитной полосой с записанной на неё информацией. Для записи двоичного кода используется полоска магнитного материала, нанесенного вдоль края карты. Снятие информации происходит при проведении карты через щель считывателя. Информация легко поддается стиранию и перезаписыванию, что актуально для кредитных карт, но недопустимо в СКУД.

Достоинства технологии магнитных карт: низкая стоимость, возможность перекодирования.

Недостатки: низкий уровень защищенности от подделки, недолговечность (карты через некоторое время надо заменять), контактная технология считывания, низкая помехозащищенность, низкая устойчивость к механическим повреждениям и электромагнитным полям, низкая пропускная способность системы.

Карты Виганда – магнитные карты, выполненные по *Wiegand*-технологии, названные по имени ученого, открывшего магнитный сплав, обладающий прямоугольной петлей гистерезиса. Внутри карты Виганда запрессованы металлические проволочки, выполненные из специального ферромагнитного сплава. Считывание карты происходит с помощью электромагнитного поля, индуцируемого считывателем. При проведении карты через щель считывателя два ряда проволочек, запаянных в карту, вызывают разнополярные всплески индукционного тока, которые преобразуются в двоичный код.

Достоинства *Wiegand*-технологии: небольшая стоимость, высокая помехозащищенность, устойчивость к механическим повреждениям, долговечность, надежность и неплохой уровень безопасности.

Недостатки: условно-контактная технология считывания, отсутствие возможности перезаписи, невысокая пропускная способность. Данная технология является переходной к бесконтактным технологиям типа *Proximity*.

Оптические штрих-кодовые карты. На карту наносится штриховой код. Существует более сложный вариант – штрих-код закрывается материалом, прозрачным только для инфракрасного излучения, считывание происходит в ИК-области спектра. Является наиболее известной и широко используемой технологией автоматической идентификации.

Существуют различные типы штрихового кода, которые различаются как по способу отображения, так и по типам данных, которые могут быть внесены в код. Некоторые отображают только цифровые характеристики,

другие несут в себе цифровые, буквенные и некоторые специальные символы, третьи позволяют закодировать до 256 символов полного набора кодировочной таблицы *ASCII* (таблица для кодированного представления десятичных цифр, латинского и национального алфавитов, знаков препинания и управляющих символов). Современные составные (композитные) штрих-коды включают возможность кодирования с использованием сразу нескольких символик.

Штриховые коды (штрих-кодирование) недороги в производстве и поэтому доступны, точно отображают информацию, устойчивы к механическим повреждениям. Они могут оптически считываться как в видимом, так и в инфракрасном диапазонах.

Достоинства штрихового кода (штрих-кодирования): точность в идентификации объектов, малое количество ошибок в сравнении с ручной идентификацией, высокая скорость считывания, простота изготовления пропуска, низкая стоимость пропуска, невосприимчивость к электромагнитным помехам, хорошая устойчивость к механическим повреждениям (если печатать не на бумаге).

Недостатки штрих-кодирования: простота подделки и фальсификации кода, невозможность перезаписи информации, низкая пропускная способность, невысокая информационная емкость.

Электронные контактные ключи-брелки *«touch-memory»* – являются частью электронной системы, основанной на однопроводном протоколе обмена информацией 1-*Wire*. Метка помещена в стандартный металлический корпус (обычно имеющий вид «таблетки»), который служит для защиты находящихся внутри микросхем. При прикосновении к считывателю метка активизируется, операции чтения и записи осуществляются практически мгновенно. В простейшем случае – это энергонезависимая память, размещаемая в металлическом корпусе. Также внутри может использоваться разнообразная электроника от однократно записываемой и флэш-памяти, до электронных схем контроллеров, таймеров, датчиков температуры и т. п.

Электронные радиочастотные бесконтактные *proxmity*-карты – наиболее перспективный в настоящее время тип карт. Бесконтактные карты срабатывают на расстоянии и не требуют четкого позиционирования, что обеспечивает их устойчивую работу, удобство использования, высокую пропускную способность системы.

Радиочастотная идентификация *RFID* (*Radio Frequency Identification*) представляет собой метод автоматической идентификации объектов, при котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или *RFID*-метках. Любая *RFID*-система состоит из считывающего устройства (считыватель, ридер) и транспондера (он же *RFID*-метка, иногда также применяется термин *RFID*-тег). Большинство *RFID*-меток состоит из двух частей.

Первая – интегральная схема для хранения и обработки информации. Вторая – антенна для приема и передачи сигнала. *Proxmity*-считыватель постоянно посылает радиосигнал. При попадании в зону действия считывателя *RFID*-метка активизируется и посылает в ответ сигнал, содержащий уникальный код доступа, записанный в памяти его электронной схемы. Считывание кода с *proxmity*-идентификатора происходит на определенном расстоянии от считывателя, т.е. без непосредственного контакта. *RFID*-системы отличаются по следующим признакам:

- по дальности считывания – ближней идентификации (до 20 см), средней идентификации (от 20 см до 5 м), дальней идентификации (от 5 м до 100 м);
- по рабочей частоте – *LF* (125 – 150 КГц), *HF* (13,56 МГц), *UHF* (860 – 960 МГц и 2,4 – 5 ГГц);
- по источнику питания – пассивные, активные, полуактивные.

Пассивные *RFID*-метки не имеют встроенного источника энергии, их питание осуществляется индуцированным в антенне электромагнитным сигналом от считывателя, достаточным для функционирования кремниевого КМОП-чипа, размещенного в метке, и передачи ответного сигнала.

Активные *RFID*-метки обладают собственным источником питания, поэтому они читаются на дальнем расстоянии, имеют б*о*льшие размеры и могут быть оснащены дополнительной электроникой. Активные метки более надежны и обеспечивают самую высокую точность считывания на максимальном расстоянии. Однако, такие метки наиболее дороги, а у батарей ограничено время работы.

Полуактивные *RFID*-метки аналогичны пассивным меткам, но оснащены батареей, которая обеспечивает чип энергопитанием. Такие метки могут функционировать на большем расстоянии и с лучшими характеристиками, чем пассивные.

Достоинства радиочастотной идентификации: высокая скорость чтения меток, возможность перезаписи данных, отсутствие необходимости прямой видимости метки, большое расстояние чтения, долговечность работы *RFID*-метки, большой объем хранения данных, поддержка одновременного чтения нескольких меток, низкая зависимость считывания от позиционирования метки относительно считывателя, устойчивость к воздействию окружающей среды, интеллектуальное поведение *RFID*-метки, высокая степень безопасности данных за счет разделения доступа и шифрования.

Недостатки радиочастотной идентификации: сложность самостоятельного изготовления, подверженность помехам в виде электромагнитных полей, возможность скрытого от пользователя

считывания данных в простых *RFID*-метках, не применяющих шифрование, недостаточная открытость выработанных стандартов.

Бесконтактные *Smart*-карты – данная технология появилась сравнительно недавно, но в некоторых приложениях уже успела завоевать огромную популярность. Бесконтактные *Smart*-карты как один из классов *RFID*-систем относятся к среднечастотному диапазону. Главные признаки, отличающие данные считыватели и карты от обычных *proximity*-устройств:

1. Наличие в карте области перезаписываемой памяти. С информацией, содержащейся в памяти, можно оперировать (добавлять, изменять, удалять) бесконтактным способом. При этом доступ к информации можно получить по специальному ключу. Длина кода в ключе зависит от технологии изготовления.
2. Уникальный серийный номер (УСН) у каждой карты является гарантией того, что двух одинаковых карт не может быть выпущено. В качестве идентификатора карты в СКУД используется именно УСН.
3. Использование способов взаимной аутентификации между считывателем и картой, за счёт которых осуществляется привязка карт к нужным считывателям.
4. В СКУД *Smart*-карты могут использоваться совместно с биометрическими считывателями. В этом случае шаблон с отпечатком пальца пользователя записывается в память карты.
5. Память внутри одной карты может быть разделена на несколько независимых секторов. Доступ к каждому из секторов осуществляется по разным ключам. Таким образом, реализуется возможность использования одной и той же карты для различных приложений (например, в разные сектора заносится информация о доступе в разные помещения объекта).

Достоинства *Smart*-карт: возможность перезаписи информации на карте с защитой от несанкционированного использования, высочайший уровень безопасности, самостоятельная обработка хранящихся в памяти карты данных, взаимная аутентификация карты и считывателя, **мультиаппликационность** – возможность использования в разных приложениях помимо СКУД. Недостатки *Smart*-карт: более высокая стоимость, чем у *Proximity*-карт.

Биометрические технологии предполагают идентификацию личности по отдельным специфическим биометрическим признакам (идентификаторам), присущим конкретному человеку. Данные признаки можно условно разделить на две основные группы:

1. Генетические и физиологические параметры (геометрия ладони, отпечаток пальца, рисунок радужной оболочки или сетчатки глаза, форма и геометрия лица).
2. Индивидуальные поведенческие особенности, присущие каждому человеку (динамика и форма почерка, речь, "индивидуальный стиль работы на клавиатуре" и пр.).

Основным достоинством биометрии является то, что указанные признаки являются уникальной универсальной и неотделимой характеристикой конкретного человека и, в отличие от носителя вещественного кода, не могут быть потеряны, украдены, подделаны, переданы другому человеку. В связи с этим возможно исключить ряд актуальных проблем, возникающих при организации доступа:

- доступ в охраняемые зоны за счет подделки идентификаторов, кражи документов, паролей;
- доступ к информации и обеспечение персональной ответственности за ее сохранность;
- допуск к ответственным объектам только сертифицированных специалистов;
- расходы, связанные с эксплуатацией СКУД (карты, ключи);
- утеря, порча или забывание ключей, карт, паролей;
- организация достоверного учета доступа и посещаемости сотрудников.

Работа биометрических систем производится в четыре этапа.

1. Посетитель предоставляет образец (*sample*) – опознаваемое, необработанное изображение или запись физиологической или поведенческой характеристики – с помощью регистрирующего устройства (например, сканера или видеокамеры).
2. Полученный биометрический образец обрабатывается для получения информации об отличительных признаках, в результате чего получается контрольный биометрический идентификатор. Идентификатор представляет собой набор больших числовых последовательностей. При этом сам образец невозможно восстановить из идентификатора.
3. Контрольный идентификатор сравнивается с базой шаблонов зарегистрированных пользователей.
4. Система принимает решение о том, совпадают или не совпадают вновь предъявленный и ранее зарегистрированный идентификатор.

Сравнение биометрических идентификаторов может осуществляться в двух режимах.

При идентификации сравнение идет в режиме "один-ко-многим" (1: *N*). То есть вновь предъявленный идентификатор сравнивается со всеми ранее зарегистрированными. Система ищет ответ на вопрос "Кто Вы?", анализируя весь перечень идентификаторов, сведения о которых были зарегистрированы ранее. При этом формируется перечень возможных "кандидатов" на совпадение с предъявленным идентификатором, расположенных по мере убывания вероятности совпадения, и окончательное решение принимает оператор системы.

При верификации сравниваются сведения о двух конкретных идентификаторах (режим "один-к-одному", или 1:1). Примером может служить сравнение сведений о вновь предъявленном идентификаторе со

сведениями, записанными в память специальной карты – при этом необходимо предъявлять и биометрический идентификатор, и карту.

Пропускная способность биометрической системы контроля доступа невысокая. Поскольку объем данных, анализируемых считывателем, весьма велик, то даже простой перебор базы данных происходит достаточно долго. Для ускорения распознавания пользователю может быть предложено применение дополнительного идентификатора (например, *PIN*-кода, обозначающего номер отдела, секции и т.п.). В этом случае в режиме идентификации производится сравнение не со всем списком, а только с его частью, выделяемой в соответствии с введенным дополнительным идентификатором.

Так как все биометрические технологии связаны с вопросом распознавания образов, то параметры, описывающие их работу, носят вероятностный характер. Основные показатели эффективности биометрических систем:

- Коэффициент ложного приема (*FAR*) – вероятность ложной идентификации, то есть вероятность того, что система по ошибке признает подлинным пользователя, не зарегистрированного в системе.
- Коэффициент ложного совпадения (*FMR*) – вероятность того, что система неверно сравнивает входной образец с несоответствующим шаблоном в базе данных.
- Коэффициент ложного отклонения (*FRR*) – вероятность того, что система не признает подлинность отпечатка пальца зарегистрированного в ней пользователя.
- Коэффициент ложного несовпадения (*FNMR*) – вероятность того, что система ошибется в определении совпадений между входным образцом и соответствующим шаблоном из базы данных. Система измеряет процент верных входных данных, которые были приняты неправильно.
- Ёмкость шаблона – максимальное количество наборов данных, которые могут храниться в системе.

4.2.2 Считыватели и кодонаборные устройства

Важным элементом в составе СКУД является считыватель, который подключается к контроллеру и является частью оборудования **точки прохода** – некоторой преграды (дверь, ворота), доступ через которую должен быть регламентирован. Точка прохода может быть контролируемой только на вход или полностью контролируемой. В первом случае проход оснащается только считывателем на вход, выход осуществляется свободно или по кнопке. Во втором случае организуется двунаправленный контроль прохода через одну дверь с установкой двух считывателей: один – на вход, другой – на выход.

Считыватель – это электронное устройство, предназначенное для считывания (ввода) кодовой информации с идентификатора и преобразования ее в стандартный формат, передаваемый для анализа и принятия решения в контроллер [13, 33].

В зависимости от способа ввода информации (от вида носителя идентификационного признака) считывание кода может быть дистанционным, контактным, электроконтактным, с помощью ручного набора кода и биометрическим.

Кодонаборные устройства (клавиатуры, цифровые кодонаборные терминалы) в отличие от считывающих систем не требуют идентификационных карточек или пластиковых ключей, которые могут быть потеряны или подделаны. Это позволяет избежать расходов, связанных с заменой пропусков. Клавиатуры являются разновидностью биометрических устройств, так как носителем *PIN*-кода является память человека. В этом случае ответственность за сохранность кода и использование его неполномочным лицом возлагается на пользователя СКУД. Поэтому кодонаборные терминалы предоставляют возможность пользователю, если он действует по принуждению, незаметно подать обусловленный сигнал охране путем набора специального кода, при использовании которого доступ предоставляется, но при этом на пост охраны подается сигнал тревоги.

К недостаткам клавиатур относится то, что код доступа может быть узнан посторонним лицом в результате неосторожных или умышленных действий законного пользователя или путем визуального изучения клавиатуры на неравномерность истирания кнопок. Также использование клавиатур позволяет лишь идентифицировать предъявляемый код, но не аутентифицировать личность пользователя. При этом по сравнению со считывателями, обеспечивающими проверку идентификатора в темпе ходьбы, клавиатуры занимают больше времени на ввод данных.

Компенсация указанных недостатков достигается за счет совместного использования клавиатуры со считывателем какого-либо типа (в зависимости от необходимого уровня обеспечения безопасности и финансовых или организационных ограничений).

Считыватели и кодонаборные устройства должны обеспечивать выполнение следующих функциональных требований [13, 19, 40]:

- считывание идентификационного признака с идентификаторов;
- ввод запоминаемого кода (для кодонаборного устройства);
- ввод биометрической информации (для считывателей биометрической информации);
- преобразование введенной информации в электрический сигнал;
- сравнение введенного идентификационного признака с хранящимся в памяти или базе данных устройства управления;
- обмен информацией с устройством управления;

- формирование сигнала на открывание преграждающего устройства при идентификации пользователя;
- защищенность от манипулирования путем перебора или подбора идентификационных признаков;
- защищенность от открывания исполнительных устройств при взломе или вскрытии, а также при обрыве или коротком замыкании электрических цепей (при этом автономные системы должны выдавать звуковой сигнал тревоги, а системы с централизованным управлением – дополнительно передавать сигнал тревоги на пункт управления).

Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов.

Считыватели и кодонаборные устройства должны иметь световую индикацию работоспособности и состояния доступа. При необходимости они могут быть оборудованы звуковым сигнализатором.

4.3 Контроллеры в составе СКУД

Главными задачами, которые решает ССОИУ в составе СКУД, являются обеспечение установки режимов доступа, приема и обработки информации от считывателей, проведение идентификации и аутентификации, выработка сигналов управления исполнительными и преграждающими устройствами, отображения и регистрации информации. Кроме этого, система должна выполнять следующие функции [19, 40]:

- введение информации в базы данных персонала и посетителей объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и др.);
- ведение электронного журнала регистрации прохода персонала и посетителей через точки доступа;
- приоритетный вывод информации о тревожных ситуациях в точках доступа;
- контроль исправности состояния считывающих, исполнительных устройств и линий связи.

Выполнение перечисленных функций реализуется следующими средствами ССОИУ:

- аппаратные средства (устройства) – контроллеры доступа, приборы приемно-контрольные доступа (ППКД);
- программные средства – ПО СКУД.

Контроллер доступа представляет собой устройство, применяемое для обработки информации от считывателей идентификаторов, принятия решения и управления исполнительными устройствами. По способу управления контроллеры делятся на три класса: автономные, централизованные (сетевые) и комбинированные.

Автономный контроллер – полностью законченное устройство, предназначенное для обслуживания, как правило, одной точки прохода. Автономные контроллеры могут быть конструктивно совмещенными со считывателем или встроенными в электромагнитный замок. Рассчитаны на применение разных типов считывателей. Предназначены для обслуживания небольшого количества пользователей СКУД**,** обычно до пятисот.

Сетевой контроллер – контроллер, работающий под управлением компьютера. В этом случае функции принятия решения ложатся на персональный компьютер с установленным специализированным ПО. Сетевые контроллеры применяются для создания СКУД любой степени сложности. При этом кроме основной функции разрешения или запрещения прохода, могут быть реализованы следующие новые возможности:

- получение отчета о наличии или отсутствии персонала на работе;
- оперативное определение местонахождения конкретного сотрудника;
- ведение автоматического табеля учета рабочего времени;
- получение отчета о перемещениях персонала и посетителей объекта за любой период времени;
- формирование временного графика прохода сотрудников, то есть кто, куда и в какое время может перемещаться;
- ведение базы данных персонала (электронной картотеки), в которую заносится необходимая информацию о сотрудниках, включая их фотографии.

Комбинированные контроллеры – совмещают в себе функции сетевых и автономных контроллеров. При наличии связи с управляющим компьютером контроллеры работают как сетевое устройство, при отсутствии связи – как автономные.

Возможности контроллеров наиболее полно раскрываются при организации распределенной сети СКУД, схема которой представлена на рис.4.2. Периферийные пункты оснащены локальными сетями на базе микрокомпьютеров (контроллеров), которые выполняют процедуру проверки самостоятельно, а сервер включается в работу лишь для актуализации локальных баз данных и статистической и логической обработки информации.

Отличительная особенность СКУД с распределенной архитектурой состоит в том, что база данных идентификаторов (и событий в системе) содержится не в одном, а в нескольких контроллерах, которые, как правило, сами выполняют функции управления внешними устройствами и охранными шлейфами через реле и входы охранной сигнализации, расположенные непосредственно на плате самого контроллера [3].

Распределенная архитектура СКУД позволяет организовать надежную защиту процесса обработки информации от негативного воздействия сбоев в работе центрального ПК, нарушений целостности проводной линии,

связывающей его с периферией и т.п. Кроме того, ПО больших систем позволяет использовать для управления сразу несколько компьютеров и осуществлять распределение исполнительных функций между ними. При этом возможна интеграция распределенных СКУД с другими подсистемами объекта: ОПС, СОТ, с системами жизнеобеспечения, оперативной связи и др.

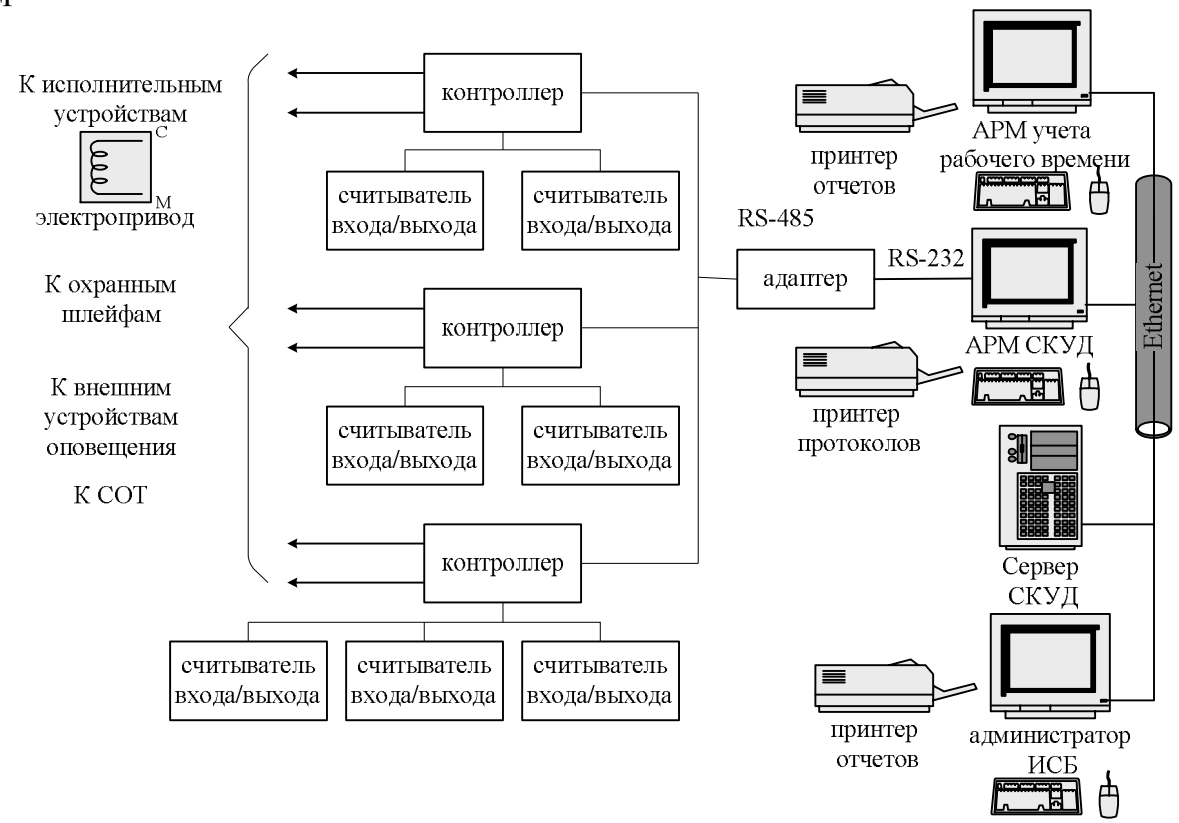

Рисунок 4.2 – Схема распределенной сети СКУД

Для повышения уровня безопасности при организации доступа на охраняемую территорию может применяться оснащение точек прохода дополнительным оборудованием. Например, можно организовать функцию запрета двойного прохода (*anti passback*), то есть запрета на пропуск через одну и ту же точку прохода пользователя, не вышедшего из помещения. Реализация запрета двойного прохода возможна только для полностью контролируемой точки прохода, так как понять, что человек вошел, но не вышел, можно только на проходе, оборудованном двумя считывателями – одним на вход и другим на выход. Данная функция вводится для того, чтобы затруднить передачу идентификатора другому лицу.

В качестве дополнительной меры защиты от несанкционированного прохода посторонних применяется функция видеоидентификации. То есть организуется возможность вывода на экран монитора компьютера фотографии владельца идентификатора-карточки (из базы данных). При этом решение о проходе может приниматься как автоматически, так и с подтверждением от контроллера или службы охраны на проходной.

5 ТЕЛЕВИЗИОННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Одним из наиболее распространенных технических средств защиты является охранное телевидение, которое активно используется в СБ самого широкого круга государственных и коммерческих объектов. Его главным привлекательным качеством является возможность не только фиксировать нарушение режима охраны объекта, но и визуально контролировать обстановку. Целью правильно спроектированной телевизионной системы является предоставление возможности оценить обстановку в контролируемых зонах в реальном масштабе времени, снизить время реакции на нештатную ситуацию и обеспечить принятие наиболее целесообразных мер защиты и противодействия возникшим угрозам.

В отечественной и зарубежной практике систему охранного телевидения иногда называют по-другому – замкнутая (закрытая) видеоаппаратура (*Closed Circuit Video equipment*, сокращенно *CCVE*). Термин «замкнутое-закрытое» показывает отличие от обычного вещательного телевидения, с помощью которого можно принимать разнообразные телепрограммы, настраиваясь на различные передающие каналы. В системе же охранного телевидения на экране монитора принимается только определенное изображение от одной или нескольких видеокамер, установленных в известном месте. Кроме оператора, никто не может наблюдать эти изображения, поэтому такую систему и называют закрытой или замкнутой.

Система охранная телевизионная (СОТ) – это телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной защиты [12].

Использование СОТ в составе ИСБ позволяет существенно повысить эффективность охраны в целом, снизить численность обслуживающего СБ персонала и затраты на обеспечение безопасности объекта, организовать круглосуточный автоматический видеоконтроль за ситуацией, создать видеоархивы; в случае получения сигнала о нарушении достоверно классифицировать факт проникновения или ложные срабатывания средств ОПС, определить характер нарушения, место нарушения, направление движения нарушителя и принять необходимые меры; повысить комфортность работы как администрации, так и служб безопасности объекта.

Поэтому применение СОТ в составе ИСБ или в дополнение к системе охранной сигнализации является обязательным [19, 37]. СОТ, интегрированные в состав ИСБ, должны строиться на основе цифровых и компьютерных технологий (цифровые СОТ), а также специализированных цифровых устройств обработки видеоинформации.

5.1 Назначение и состав СОТ

С учетом конкретных условий и особенностей процессов деятельности на объекте СОТ в составе ИСБ должна обеспечивать выполнение следующих функций [12, 15, 19]:

- прямое видеонаблюдение оператором контролируемой зоны, обнаружение и идентификацию субъектов наблюдения – людей, транспортных средств, имущества, элементов объектовой инфраструктуры;
- передачу визуальной информации о состоянии охраняемых зон, помещений, периметра и территории объекта в пункт охраны для **видеоверификации тревог –** подтверждения с помощью видеонаблюдения факта нарушения зон охраны и выявления ложных срабатываний охранной сигнализации;
- запись видеоинформации в архив для последующего анализа состояния охраняемого объекта (зоны), тревожных ситуаций, идентификации нарушителей и других задач.

Прямое видеонаблюдение должно осуществляться в непрерывном режиме с выводом видеоизображения на видеомонитор (видеомониторы) операторов отдельного поста видеонаблюдения (не более четырех изображений от видеокамер на один монитор – для непрерывного наблюдения одним оператором). На практике прямое видеонаблюдение осуществляется периодически в качестве отклика на вызвавшую его угрозу или для проверки состояния удаленного объекта. Различают четыре основные возможности просмотра видеоинформации:

1. **Локальное наблюдение** непосредственно с выхода устройств видеозаписи или сервера – применяется для мониторинга территории небольших объектов (в розничной торговле, банках и на предприятиях малого бизнеса).
2. **Удаленное наблюдение с помощью ПК –** для просмотра прямого или записанного видеоизображения используется ПК с установленным специальным приложением к клиентскому ПО или веб-браузером.
3. **Мобильное наблюдение** позволяет охраннику, находящемуся на территории объекта, мгновенно проверить, что отображает видеонаблюдение. Мобильное наблюдение имеет большой потенциал в плане обеспечения оперативной и слаженной работы групп быстрого реагирования и мобильной охраны.
4. **Видеостена –** это идеальное решение для больших ситуационных центров, имеющих для просмотра сотни и тысячи видеокамер. Видеостена образует очень большой экран, что позволяет осуществлять наблюдение сразу группе людей. Это особенно важно при чрезвычайных ситуациях. Видеостена имеет возможность переключения между видеокамерами, а также автоматической демонстрации изображения от тех видеокамер, где произошла тревога.

Для видеоверификации тревог видеоизображение должно выводиться на видеомонитор по сигналу тревоги от извещателя охранной сигнализации, который логически связан с конкретной видеокамерой. Видеокамеры могут также включаться по сигналу видеодетектора движения (аппаратного устройства или программно реализованного в составе АРМ СОТ).

Автоматическая запись видеоинформации в архив может производиться непрерывно, периодически по расписанию, по срабатыванию извещателей, по срабатыванию видеодетектора СОТ. Технические средства архивации должны обеспечивать хранение необходимых объемов видеоинформации в течение времени, которое задается условиями и режимом охраны объекта. Рекомендуемое время хранения архива не менее 15 суток.

Типовой состав СОТ (рис.5.1) содержит видеокамеры, количество которых определяется задачами, возложенными на видеосистему, каналов передачи видеосигнала от каждой видеокамеры до устройств обработки и хранения и видеомониторов как устройств отображения видеоинформации.

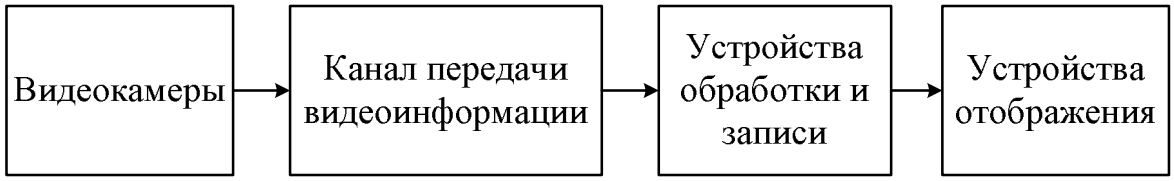

Рисунок 5.1 – Обобщенная структурная схема СОТ

Основные аппаратно-технические и программные средства СОТ по функциональному назначению подразделяют на [12, 19]:

- источники видеосигнала (видеокамеры с объективами);
- устройства аналого-цифрового преобразования видеосигнала;
- устройства коммутации и передачи видеосигнала (УКВС);
- устройства видеозаписи, цифровые видеорегистраторы;
- устройства вывода видеоизображения (видеомониторы);
- устройства приема и обработки видеоданных для цифровых СОТ (платы видеоввода, видеосерверы, ПО АРМ в цифровых СОТ).

Дополнительно в состав СОТ должны входить: блоки питания, коммутационное оборудование, аппаратура передачи видеосигнала по различным каналам, устройства крепления и поворота видеокамер, кожухи для видеокамер, средства освещения и инфракрасной подсветки и другое оборудование, необходимое для обеспечения работоспособности СОТ.

Конструктивно системы охранного телевидения должны строиться по модульному принципу и обеспечивать выполнение следующих функций в процессе эксплуатации и технического обслуживания [40]:

- взаимозаменяемость сменных однотипных технических средств;
- удобство технического обслуживания, ремонта и эксплуатации;
- исключение несанкционированного доступа к элементам управления;
- санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

Один из возможных вариантов построения СОТ представлен на рисунке 5.2.

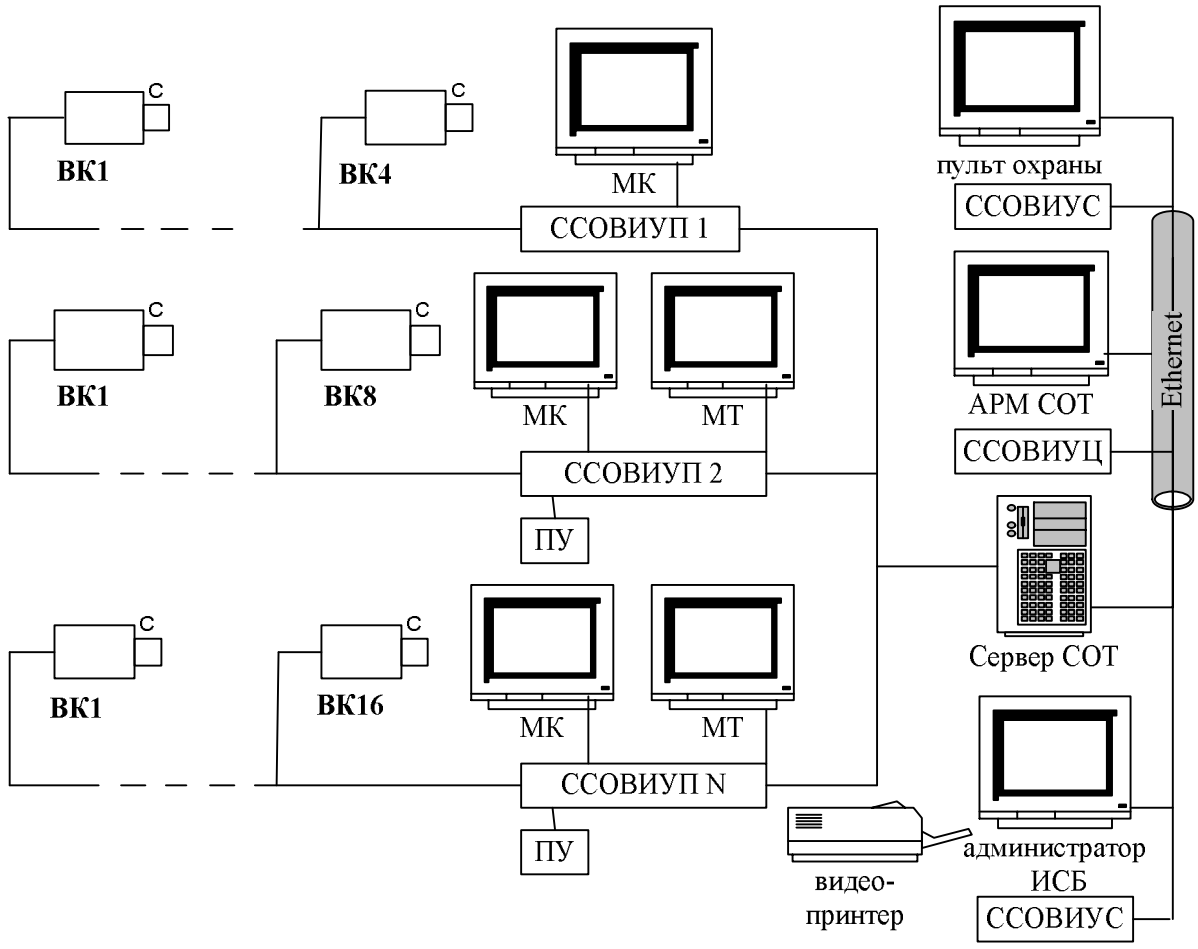

Рисунок 5.2 – Структурная схема системы охранной телевизионной: ССОВИУЦ – система сбора, обработки видеоинформации и управления центральная; ССОВИУС – система сбора, обработки видеоинформации и управления станционная; ССОВИУП 1…N – система сбора, обработки видеоинформации и управления периферийная; АРМ – автоматизированное рабочее место; ПУ – пульт управления; МК – монитор контроля; МТ – монитор тревоги; ВК – видеокамера

5.2 Источники видеосигнала (видеокамеры)

Видеокамера представляет собой оптико-электронное устройство, которое преобразует оптическое изображение наблюдаемого объекта в электрический видеосигнал определенного стандарта (набора требований к структуре и характеру составляющих видеосигнала, позволяющего стандартизировать процесс приема/передачи видеоизображений) [12, 26].

Видеокамера является важнейшим элементом СОТ, так как именно с нее в систему поступает первичная информация об объекте и именно ее характеристиками определяется качество изображения в целом.

Видеокамера представляет собой электронную плату, на которой размещен чувствительный элемент (сенсор), и объектив. В зависимости от конструктивного исполнения, технических характеристик и условий эксплуатации видеокамеры подразделяют на: корпусные и бескорпусные; черно-белого и цветного изображения; обычной и повышенной чувствительности; обычного и высокого разрешения; для внутреннего и наружного наблюдения; для скрытого наблюдения.

Эффективность СОТ достигается размещением видеокамер в критических зонах с использованием двух основных принципов:

- наблюдение точек прохода (двери, коридоры, проезды);
- наблюдение за наиболее ценным.

Точками прохода являются зоны, через которые люди и транспорт должны пройти для попадания в определенные области. Размещение камер в точках прохода является экономически оправданным способом фиксации всех, кто попадает на охраняемый объект.

Ценными являются специфические объекты, которые требуют повышенного уровня безопасности, и значимость которых определяется потребностями и приоритетами конкретного заказчика.

Примерами ценного являются такие физические объекты, как материальные ценности, области, где они размещаются; кроме того, это места, в которых осуществляются важные действия – например, зоны с кассовыми аппаратами, места парковок машин или приемные.

Качество изображения от видеокамеры определяется целым рядом показателей, однако в большинстве случаев при выборе камеры для конкретной системы достаточно ориентироваться на следующие ее параметры [4, 12, 17, 24].

Оптический формат – размер фоточувствительной области сенсора в дюймах по диагонали (1 дюйм соответствует 25,4 мм). Основные форматы: 1/4", 1/3", 1/2", 2/3" и 1". Чем больше оптический формат, тем меньше (при прочих равных условиях) геометрическое искажение изображения.

Разрешающая способность видеокамеры (разрешение) **–** параметр, определяющий возможность видеокамеры передавать в выходном видеосигнале мелкие детали изображения. Определяется как число градаций (переходов) в видимой части растра от черного к белому или

обратно, которое может быть получено от камеры в центральной части экрана (области наблюдения). На краях экрана допускается некоторое ухудшение качества изображения. Измеряется в телевизионных линиях (ТВЛ) по горизонтали и вертикали.

Рабочий диапазон освещенностей – диапазон освещенностей в поле зрения видеокамеры от минимальной до максимальной, в пределах которого разрешающая способность и отношение сигнал/шум видеокамеры не менее заданных значений.

Пороговая чувствительность (чувствительность) – минимальная освещенность на фоточувствительной площадке, при которой видеокамера сохраняет работоспособность.

5.2.1 Чувствительные элементы видеокамер

В основе современных видеокамер лежит применение сенсоров, выполненных по одной из двух технологий построения электронных схем:

– КМОП (комплементарная логика на транзисторах металл-оксид-полупроводник) или *CMOS*-ма́трица (*Complementary-symmetry / metal-oxide semiconductor*);

– ПЗС (прибор с зарядовой связью) или *CCD*-ма́трица (*Charge-Coupled Device*).

Принцип действия ПЗС и КМОП сенсоров одинаков: под действием оптического излучения в полупроводниковых элементах появляются носители заряда, которые преобразуются в электрический сигнал.

Данные типы матриц имеют одну светоприемную плоскость, на которой расположены миниатюрные светочувствительные элементы, реагирующие на световой поток разных цветов. После обработки сигналов от этих элементов появляется изображение, которое, в свою очередь, складывается из элементарных цветовых точек (пикселов).

Первоначально были разработаны ПЗС-матрицы. Почти одновременно с ними были разработаны КМОП-матрицы. Различие между ПЗС и КМОП сенсорами заключается в способе накопления и передачи заряда, а также в технологии преобразования его в аналоговый сигнал.

ПЗС-ма́трица – специализированная аналоговая интегральная микросхема, состоящая из светочувствительных фотодиодов, выполненная на основе кремния. Основная задача ПЗС-матрицы – накапливание энергии светового потока в потенциальных ямах – пикселах. При дальнейшей обработке информации, сосредоточенной в пикселах, используются сдвиговые регистры, после которых сигнал поступает на АЦП и дальше на устройства формирования стандартного видеосигнала. ПЗС-матрицы обладают следующими достоинствами:

- низкий уровень шумов;
- высокий коэффициент заполнения пикселов (около 100%);

– высокая эффективность (отношение числа зарегистрированных фотонов к их общему числу, попавшему на светочувствительную область матрицы, для ПЗС – 95%);

– высокая чувствительность (возможность получения изображения достаточно хорошего качества даже в условиях низкой освещенности);

– улучшенная цветопередача.

Недостатками ПЗС-матриц являются:

– сложный принцип считывания сигнала, а, следовательно, технология;

– высокий уровень энергопотребления (до 2 – 5Вт);

– высокая стоимость производства;

– вертикальные размытые полосы ниже и выше очень яркого объекта в кадре.

КМОП-матрица представляет собой не просто светочувствительную матрицу, использующую полевые транзисторы; это полноценная интегральная схема, на которой реализованы схемы обработки сигнала. В результате видеокамеры на КМОП-матрицах более компактны, по сравнению с видеокамерами на ПЗС, и позволяют получать доступ к каждому пикселу или к выбранным группам пикселов, что облегчает решение задач при формировании и обработке сигналов с матрицы.

Логическим продолжением КМОП-матриц стали *PIXIM*-матрицы. Ключевым моментом *PIXIM*-матриц является «присутствие» аналого-цифрового преобразователя непосредственно в каждом пикселе матрицы и независимая микропроцессорная обработка сигнала в режиме реального времени. В *PIXIM*-матрицах для каждого пиксела производится «замер» интенсивности освещения. После этого подбирается наилучшее время экспозиции из пяти возможных значений. Такой подход называется «мультисемплингом» и позволяет работать с динамическим диапазоном освещенности сцены до 120 дБ.

Достоинства КМОП-матриц:

– высокое быстродействие (до 500 кадров/с);

– низкое энергопотребление (почти в 100 раз по сравнению с ПЗС);

– простота и низкая стоимость в производстве;

– перспективность технологии (на одном кристалле реализуются все необходимые дополнительные схемы: аналого-цифровые преобразователи, процессор, память, получая, таким образом, законченную цифровую камеру на одном кристалле).

Недостатки КМОП-матриц:

– низкая чувствительность;

– высокий уровень шума (он обусловлен так называемыми темповыми токами – даже в отсутствие освещения через фотодиод течет довольно значительный ток);

– невысокий динамический диапазон.

КМОП-матрицы активно применяются за рамками охранного телевидения, например, в бытовых видеокамерах, электронных фотоаппаратах и в камерах, встроенных в средства коммуникации.

5.2.2 Объективы видеокамер

Как и видеокамера, объектив – один из главных элементов системы видеонаблюдения. От выбора объектива будет зависеть угол зрения видеокамеры, чувствительность и разрешение всей системы. Рассмотрим основные виды объективов для видеокамер.

В зависимости от способа регулировки диафрагмы, объективы делятся на три группы: имеющие фиксированную, ручную и автоматическую диафрагму. Наиболее простыми являются объективы с фиксированной диафрагмой, которые устанавливаются на видеокамеры, имеющие электронный затвор, для видеонаблюдения внутри зданий в условиях с практически не меняющейся освещенностью. Фокусировку выполняют вручную.

Объективы с автодиафрагмой (*AI – autoiris*) применяют для наружного наблюдения. Лепестки диафрагмы такого объектива могут перемещаться при помощи микропривода, который управляется электросхемой, находящейся либо в объективе (*VD – Video Drive* – управление по уровню сигнала), либо внутри камеры (*DD – Direct Drive* – управление по постоянному току). Механизм автоматической диафрагмы является отрицательной электронно-механической обратной связью для сдерживания сигнала от видеокамеры на ранее обозначенном уровне.

Варифокальный объектив (вариообъектив) – это единая оптическая система, компоненты которой могут взаимно перемещаться относительно друг друга. При этом изменяется эквивалентное фокусное расстояние системы, и сохраняется резкость изображения. Данный объектив имеет переменное фокусное расстояние. Он дает возможность масштабировать, то есть увеличить размер изображения, не меняя положение камеры. Оптическое увеличение дает возможность сохранить высокое качество изображения. Фокусное расстояние вариообъектива изменяется вручную в относительно небольших пределах.

Трансфокатор – это объектив, имеющий изменяемое в больших пределах фокусное расстояние. Главным параметром трансфокатора является масштабирование или наибольшая степень увеличения. Этот показатель можно определить как отношение максимального фокусного расстояния к минимальному. Регулировка угла обзора выполняется автоматически и дистанционно с помощью сигналов телеметрии. Данный объектив используется, если необходимо подробно разглядеть определенные части изображения. В редких случаях применяются

трансфокаторы, которые управляются вручную. Их используют, если заранее не известно, какой угол обзора должна обеспечивать видеокамера.

5.2.3 Способы повышения качества изображения

Чтобы оценить качество изображения, которое позволяет получить проектируемая СОТ, необходимо обратиться к целям, в которых она должна использоваться, и соответствующим требованиям к качеству. Рекомендуется распределить эти цели на четыре группы:

- Мониторинг – наблюдение за обстановкой, либо перемещением людей на объекте, где отсутствует необходимость останавливать внимание на отдельных лицах (человек должен занимать не менее 5% высоты изображения; если используется оцифрованное изображение, то высота человека должна составлять не менее 30 пикселов, прежде чем будет применен алгоритм сжатия изображения).
- Обнаружение – определение факта наличия человека в кадре без необходимости рассмотреть его лицо (человек должен занимать не менее 10% высоты изображения; если используется оцифрованное изображение, то высота человека должна составлять не менее 60 пикселов, прежде чем будет применен алгоритм сжатия изображения).
- Опознание – определение того, известен ли вам попавший в кадр человек, либо неизвестен (человек должен занимать не менее 50% высоты экрана; если используется оцифрованное изображение, то высота человека должна составлять не менее 288 пикселов, прежде чем будет применен алгоритм сжатия изображения).
- Идентификация – формирование и запись высококачественных изображений лица, по которым можно однозначно и бесспорно идентифицировать личность при предъявлении доказательных материалов в суде (человек (незнакомый) должен занимать не менее 100% высоты экрана; при этом предполагается, что лицо человека (голова) составляет примерно 15% высоты человека; если используется оцифрованное изображение, то голова должна занимать не менее 90 пикселов по высоте, прежде чем будет применен алгоритм сжатия изображения).

Необходимо, чтобы СОТ производила изображения именно того уровня качества, которое требуется для выполнения поставленных перед ней задач. Если необходимо выполнить идентификацию, некачественные изображения могут поставить под сомнение целесообразность установки всей системы. Поэтому при проектировании СОТ проводятся следующие относительно объективные измерения:

– проверка области покрытия системы видеонаблюдения на заданном участке;

– проверка масштаба и специальных требований по различимости деталей;

– комплексная проверка качества и скорости выполнения своей задачи оператором;

– комплексная проверка записи.

В современных видеокамерах используются различные технические решения, направленные как на улучшение их характеристик, так и на повышение эффективности СОТ в целом.

Видеокамеры, работающие при недостаточной освещенности или при полном отсутствии света

Освещенность объекта сильно влияет на разрешение, поэтому для объектов с очень низкой освещенностью следует выбирать видеокамеры с повышенными значениями чувствительности и разрешающей способности. Кроме того, видеокамеры, которые устанавливают на подобных объектах, должны иметь автоматическую регулировку усиления сигнала, которая обеспечивает работоспособность камеры при малой освещенности.

При необходимости вести скрытое видеонаблюдение в условиях недостаточной освещенности сцены могут применяться специализированные камеры на базе ПЗС-матриц с *докоммутирующим усилением*. По показателям чувствительности такие камеры превосходят лучшие модели обычных полупроводниковых камер в сотни и даже в тысячи раз. Такое повышение светочувствительности достигается с помощью усилителя излучения, помещаемого между объективом и ПЗС-матрицей. По стоимости подобные камеры для ночного видения в 10-20 раз превосходят обычные.

Тепловизионные камеры работают в диапазоне длин волн от 3,5 мкм до 8-14 мкм. ИК-сенсоры реагируют на изменение тепловой энергии, излучаемой непосредственно объектами, которые находятся в пределах наблюдаемой сцены [39]. Тепловизоры способны работать в полной темноте. Им не требуется источников освещения – видимого либо инфракрасного. По сути, тепловизор является пассивной монохромной камерой. Тепловизионные камеры способны обнаруживать людей и иные теплоизлучающие объекты (животных, транспортные средства, нагретые части зданий и сооружений), а также любые предметы, температура которых отличается от температуры окружающего фона.

Видеокамеры "День/Ночь"

Монохромные и цветные видеокамеры имеют свои преимущества и недостатки. Цветные камеры более информативны, но обладают меньшей чувствительностью, что ограничивает их применение в условиях недостаточной освещенности.

Матрицы цветных видеокамер чувствительны к ИК излучению, что дает существенную прибавку к их рабочему диапазону освещенностей. Однако для цветных камер, используемых в СОТ, используется ИК фильтр,

который ограничивает их спектральные характеристики видимой частью спектра. Конструктивно ИК фильтр представляет собой пластинку из стекла или любого светопрозрачного полимера с нанесенным на него слоем, поглощающим ИК излучение. Также фильтр может представлять собой тонкую пленку отражающего ИК излучение материала, нанесенного на линзы оптики камеры или на матрицу. Указанные меры принимаются в связи с тем, что при отсутствии фильтра, задерживающего ИК спектр, происходит ухудшение качества изображения, которое проявляется в виде снижения контраста, появления шумов и искажения цветопередачи.

В камерах типа день/ночь также применяется решение в виде механического ИК фильтра: днем при достаточной освещенности он установлен и камера снимает в видимом спектре, а ночью, когда освещение падает, камера переходит в черно-белый режим, фильтр удаляется и включается ИК подсветка. Таким образом, сочетается информативность цветной и высокая чувствительность черно-белой видеокамеры.

Режим день/дочь, реализованный на базе механически сдвигаемых ИК-фильтров, обозначают в документации как *TDN* (*True Day/Night*) или *ICR* (*Infrared Cut Filter Removable*) – убираемый вырезающий ИК фильтр.

Существует недорогая реализация режима день/ночь за счёт электронной обработки видеосигнала.

Режим компенсации яркой засветки (HLC – High Light Compensation)

Видеокамера отрабатывает уровень освещенности, меняя время накопления заряда (электронный затвор) или управляя диафрагмой объектива. Если в поле зрения камеры находятся очень яркие участки, они влияют на эту отработку, и настройка затвора или диафрагмы по средней яркости приводит к неразличимости деталей в темных участках. Если яркие участки исключить из расчета средней яркости, детали в темных тонах будут лучше различимы. Исключает из обработки (маскирует) чрезмерно яркие участки функция «компенсации яркой засветки».

Режим повышенной чувствительности (Sense-Up)

При работе видеокамеры в полной темноте полезный сигнал становится слабо различимым на фоне шумов матрицы и каскадов обработки видеосигнала. Для повышения чувствительности известны методы накопления сигналов, в которых сигналы суммируются по амплитуде (до 500 кадров). Значение чувствительности камер возрастает пропорционально. Недостаток метода – движущиеся объекты будут размыты. Быстро идущий человек будет выглядеть как призрак на изображении ночного города. Режим повышенной чувствительности не пригоден для наблюдения за быстро движущимися объектами. При

большом количестве суммируемых полей можно вообще не увидеть на стоп-кадре быстро движущиеся объекты.

Режим компенсации затенения объектива (LSC – Lens Shadow Compensation)

Часто объективы видеокамер создают затенения по углам изображения. Особенно это характерно для варифокальных объективов при установке максимального угла обзора. Функция компенсации затенения объектива выравнивает среднюю яркость в углах изображения. В случае, когда яркость в углах изображения должна быть меньше по естественным условиям освещенности функцию можно отключить.

Рассмотрим другие функции и способы повышения качества изображения, которые стали доступны в последние годы, благодаря использованию процессоров цифровой обработки сигнала (*DSP – Digital signal processor*).

Расширенный динамический диапазон (WDR – Wide Dynamic Range)

Матрице видеокамеры часто не хватает динамического диапазона, например, если установленная в помещении камера наблюдает за проходом на ярко освещенную улицу. При этом затвор или автодиафрагма настраиваются на средние значения яркости по полю кадра, но объекты наблюдения (люди) теряют различимость как в самых ярких участках, так и в тени. Задачу наблюдения в таких условиях частично решает функция компенсации встречной или фоновой засветки – *BLC* (*Back Light Compensation)*, которая настраивает камеру на среднюю освещенность в центре кадра. Человек в центре кадра будет виден лучше, но детали фона при этом теряются.

Для того чтобы лучше видеть детали в светлых и темных участках изображения, используется функция *WDR*. В течение одного полукадра делают два снимка: один с длительной выдержкой, второй – с короткой. Полученные изображения сводят в единое в выходном сигнале. Для реализации этой функции либо применяют специальные матрицы с двойным сканированием или двойной плотностью (на 30% дороже обычной камеры), либо снимки с разными выдержками делают на обычных матрицах. При этом скорость вывода информации падает в 2 раза, до 25 полей в секунду, что создает некомфортные условия для наблюдения в режиме реального времени.

Цифровое подавление шумов (DNR – Digital Noise Reduction)

В условиях недостаточной освещенности изображение бывает зашумленным. Такое изображение плохо сжимается алгоритмами в

регистраторах, и растет объем архива. Для устранения этого явления проводится цифровое подавление шумов двумя способами.

2*D* подавление шумов (2*DNR*). Процессор производит коррекцию яркости соседних пикселов одного кадра: определяет, насколько это изменение соответствует параметрам шума и, если вероятность влияния шума высока, уменьшает разницу в яркости на рассчитанную величину.

3*D* подавление шумов (3*DNR*). Расчеты производятся для нескольких последовательных кадров, что позволяет более точно выделить шум как меняющийся во времени процесс. Эта технология считается более современной и более эффективной.

5.2.4 Поворотные видеокамеры

Поворотные камеры часто называют *PTZ*-камерами от английского сокращения *Pan, Tilt, Zoom*. Поворотная видеокамера может быть реализована двумя способами:

- как статическая видеокамера, установленная на поворотном устройстве;
- как скоростная поворотная видеокамера, выполненная в прозрачном кожухе куполообразной формы или в виде шара.

Поворотная видеокамера – конструктивно законченный узел, состоящий из видеокамеры, объектива с трансфокатором, поворотного устройства, блока питания, приемника сигналов телеуправления и кожуха.

Дистанционное управление объективом и поворотным устройством позволяет ориентировать видеокамеру как по азимуту, так и по углу обзора.

Управление аналоговой *PTZ*-камерой производится с использованием интерфейса *RS*-485 и специального протокола. Наиболее распространенными являются протоколы *Pelco-P*, *Pelco-D*. Камера подключается к специализированному пульту управления. Он позволяет управлять поворотным устройством по двум координатам, фокусным расстоянием объектива, а также скоростью поворота. Один пульт поддерживает управление до 256 камер. Выбор камеры для управления осуществляет оператор видеосистемы. Если оператору необходимо постоянно управлять камерами, пульт должен иметь джойстик. Обычно пульты поддерживают несколько протоколов. *PTZ*-камера и пульт должны работать на одинаковом протоколе управления.

Управление поворотной камерой также может быть интегрировано в систему видеозаписи. Основные функции и возможности *PTZ*-камеры:

- поворот в горизонтальной плоскости на 360° и на 180° в вертикальной плоскости;
- x12…x36-кратное оптическое и x10…x25-кратное цифровое увеличение;

- 4…256 точек предустановки – точек наблюдения видеокамеры с заранее установленными при настройке параметрами углов в вертикальной и горизонтальной плоскостях и фокусом объектива;
- 1…32 маршрута автопатрулирования – последовательного просмотра видеокамерой нескольких точек предустановки;
- автоматическое сканирование заданного сектора наблюдения;
- тревожные входы, служащие для подключения внешнего оборудования (при подаче сигнала на тревожный вход видеокамера поворачивается в заранее заданную точку предустановки);
- "автослежение" – режим, при котором видеокамера автоматически "захватывает" самый большой объект в кадре, следует за ним на 360° по горизонтали и 90° по вертикали. Видеокамера автоматически приближает движущийся объект, сохраняя его в центре кадра.

Слежение за объектом заканчивается, когда он выходит за границы обзора видеокамеры или когда время, установленное на "автослежение", заканчивается. Когда отслеживаемый объект уходит из поля зрения камеры, она ищет другой объект. При попадании в поле зрения нескольких объектов отслеживание заданного объекта *PTZ*-системой может сбиваться. Поэтому применение *PTZ*-видеокамер для отслеживания объектов без вмешательства оператора интересно при малой загруженности – на парковках, в коридорах.

Достоинство *PTZ*-видеокамеры состоит в том, что она позволяет контролировать большие территории, поочередно охватывая наблюдением различные части сканируемого охраняемого пространства. При более высокой стоимости, по своей информативности одна поворотная видеокамера превосходит несколько расположенных на территории статических видеокамер. К недостаткам применения *PTZ*-видеокамер можно отнести следующие:

– информативность видеокамеры во многом определяться тем, насколько удачно в нужный момент оператор выбрал ее направление и задал угол обзора;

– возможность пропуска нарушителя при неудачном характере управления поворотной видеокамерой;

– более высокая нервно-психологическая нагрузка на оператора видеонаблюдения.

PTZ-видеокамеры используются для просмотра больших открытых территорий, для наблюдения за периметром объекта охраны, где служат для верификации тревог охранной сигнализации в составе ИСБ. Например, если охранная сигнализация локализовала нарушение периметра в достаточно узкой области, то на входы тревоги *PTZ*-видеокамеры могут быть поданы сигналы от извещателей для управления поворотом видеокамеры в предварительно заданном направлении для отображения нарушенного участка зоны отторжения, забора и пр. Подобное решение позволяет

упростить работу оператора, поскольку его внимание будет привлекаться к экрану монитора только в режиме тревоги.

5.2.5 ИК подсветка

Одним из способов обеспечить работоспособность видеокамеры в условиях недостаточной освещенности на объекте является организация дежурного освещения. Самым простым и доступным является обычное освещение, которое при оснащении специальными устройствами (реле времени, фотоэлементами, охранными извещателями, реагирующими на перемещение) может включаться и выключаться по расписанию, по уровню освещенности или при приближении человека. Использование обычного искусственного освещения видимого диапазона является наиболее предпочтительным, так как позволяет видеокамере работать в максимуме ее чувствительности (555 нм).

Для решения задач скрытого видеонаблюдения, а также чтобы не привлекать внимание к видеокамере, используется освещение, не видимое для глаз – подсветка в инфракрасном диапазоне. Можно выделить два случая применения ИК подсветки.

1. Требуется обеспечить невидимость рассеянного или диффузно отраженного светового потока, но допустимо свечение самих источников излучения. При этом возможно применения излучателей с длиной волны 920, 880 и даже 850 нм.

2. Требуется обеспечить невидимость излучателя при прямом визуальном наблюдении его с близкого расстояния. Для этого применяются излучатели с длиной волны 940–950 нм.

Все инфракрасные источники света для видеонаблюдения можно разделить на две группы, различающиеся назначением, а, следовательно, характеристиками и конструктивным исполнением:

– ИК прожекторы, фары и фонари с лампами накаливания в качестве излучателя;

– полупроводниковые ИК осветители (на основе полупроводниковых дискретных элементов и малогабаритные излучатели на основе шестиэлементных светодиодных матриц).

ИК осветители на основе ламп накаливания предназначены для освещения объектов наблюдения как на улице, так и внутри помещения. В основном в них используются лампы с галогенным циклом (например, вольфрамовая лампа накаливания), имеющие отдельный или встроенный отражатель. Прожекторы имеют влагозащищенный корпус с ребрами охлаждения и простыми кронштейнами для крепления и наведения по углу. Они выпускаются с напряжением питания 220, 110, 24 или 12 В. Для выделения ИК области и подавления видимой части спектра излучения используются ИК фильтры.

Скрытность подсветки в этом случае обеспечивается только в условиях темноты на достаточно большой дальности, вследствие существенного свечения в красной области спектра. Кроме того, по внешнему виду они ассоциируются с осветительным прибором. Для полностью скрытой подсветки с использованием осветителей данного типа создается рассеянный световой поток от потолка или специальных экранов с диффузным отражением. Для этих случаев максимально эффективны широкоугольные осветители с углами излучения до 80–90°. Осветители располагаются за карнизами, балками и другими элементами, скрывающими их от глаз наблюдателя.

Основными преимуществами полупроводниковых излучателей по сравнению с лампами накаливания являются большая спектральная яркость на рабочей длине волны, существенно больший ресурс, достигающий 100 тыс. часов и меньшая стоимость (с учетом эксплуатационных расходов). Основной технической проблемой для полупроводниковых ИК осветителей является обеспечение эффективного отвода тепла от площадки светодиода. От этого зависит допустимый ток и световой поток единичного излучателя, а, следовательно, необходимое суммарное количество светодиодов, размеры и себестоимость всего прожектора.

Кроме прожекторов, собранных на дискретных элементах, получили распространение малогабаритные излучатели на основе шестиэлементных светодиодных матриц с питающим напряжением 12В. Выпускаются излучатели в различном конструктивном исполнении и с углами излучения 160, 120, 40 и 20°. Излучатели снабжены радиатором, используются в качестве миниатюрных прожекторов, либо встраиваются в конструктивные элементы зданий или оборудования для скрытой ИК подсветки.

Функция адаптивной ИК подсветки – реализуется с помощью *DSP* в видеокамерах высокого и сверхвысокого разрешения. Кроме возможности обработки изображения с разрешением 600ТВЛ, в процессоре может быть реализована возможность адаптивной регулировки яркости встроенной ИК подсветки. Суть алгоритма заключается в управлении интенсивностью встроенного ИК прожектора в зависимости от уровня сигнала матрицы. Если в какой-то части изображения появляется объект, который интенсивно отражает свет от ИК прожектора, то процессор на основании анализа изображения посылает сигнал блоку управления подсветкой для уменьшения питающего напряжения. Таким образом, интенсивность ИК подсветки будет уменьшаться до тех пор, пока изображение перед камерой не достигнет приемлемой яркости.

Преимущества видеокамеры с адаптивной подсветкой: четкая идентификация объекта наблюдения (лицо человека, номер автомобиля и т.д.); увеличение срока службы светодиодов за счет уменьшения интенсивности их свечения и нагрева. При этом цена камеры с адаптивной

подсветкой практически не отличается от цены камеры, оборудованной блоком нерегулируемой ИК подсветки.

5.3 Устройства видеозаписи (видеорегистраторы)

Видеозапись в составе СОТ может быть реализована на базе устройств видеозаписи – цифровых видеорегистраторов (ЦВР) или программным методом на базе средств ПК с установленным программным обеспечением АРМ СОТ. Режим записи устанавливается в зависимости от условий охраны объекта и требований заказчика.

В соответствии с определенными в нормативных документах требованиями, устройства видеозаписи в составе ИСБ должны обеспечивать запись и хранение видеоинформации в следующих режимах [12,19]:

1. непрерывная видеозапись в реальном времени;
2. видеозапись отдельных фрагментов или видеокадров по срабатыванию охранных извещателей, по видеодетектору движения, по командам управления оператора или по заданному времени.

Видеорегистратор – это устройство, предназначенное для записи, воспроизведения и хранения видеоинформации в составе СОТ [12].

При динамическом распределении ресурсов видеорегистратора для каждой из видеокамер существует возможность индивидуально настроить параметры записи (разрешение, степень компрессии и скорость).

В ЦВР предусмотрена запись отдельных фрагментов или видеокадров по принципу «кольцевого буфера», при котором обеспечивается запись видеоинформации до момента наступления «предтревожной ситуации».

При воспроизведении записи видеорегистратор позволяет:

- регулировать скорость просмотра (просмотр в ускоренном и замедленном режимах работы), в том числе при покадровом прямом и обратном воспроизведении;
- отображать информацию как одной, так и нескольких видеокамер;
- отображать одну видеокамеру с максимальным разрешением;
- выполнять поиск записей с возможностью печати и перезаписи изображения по времени и дате по каждой видеокамере;
- выполнять запись и воспроизведение аудиоданных, времени, даты, номера видеокамеры и другой информации, сопутствующей изображению и выводимой на экран в разборчивом виде и не мешающей просмотру изображения.

Видеорегистраторы в составе СОТ выполняют функции ССОИУ – принимают сигналы от видеокамер, сохраняют их и управляют распределением видеоинформации между наблюдателями.

Существует четыре варианта системы управления видеонаблюдением. При организации СОТ на большинстве объектов используется один из них,

но может применяться несколько вариантов, когда необходимо иметь возможность перехода от одного варианта к другому.

- Системы на базе ПК (*PC-based*) – компьютер с установленной платой видеозахвата и специализированным ПО.
- *Stand-Alone DVR* (*Digital Video Recorder* – цифровой видеорегистратор) – специализированное автономное устройство цифровой записи аналогового видеопотока; сочетает в себе три составляющие: аппаратуру, ПО и жесткий диск для хранения видеоархива. Данные видеорегистраторы имеют входы для подключения только аналоговых видеокамер, поддерживают удаленное наблюдение через интернет. Они просты в установке, но имеют существенные ограничения в части расширения или изменения состава оборудования.
- *HDVR* (*hybrid DVR* – гибридный видеорегистратор) – видеорегистратор, поддерживающий как аналоговые, так и сетевые (*IP*) видеокамеры. Гибридные видеорегистраторы имеют функциональность *DVR* видеорегистраторов.
- *NVR* (*Network Video Recorder* – сетевой видеорегистратор) аналогичен *DVR* видеорегистратору, но поддерживает только *IP*-камеры. Для поддержки аналоговых камер необходимо использовать специальное кодирующее устройство (*encoder*).

Для небольших и средних объектов *DVR* является самым востребованным вариантом системы видеозаписи благодаря наличию всех самых необходимых функций при умеренной цене, простой настройке, не требующей глубоких специальных знаний в области *IT*-технологий и широкому ассортименту существующих моделей ЦВР. К недостаткам *DVR* видеорегистраторов можно отнести:

1. Плохую масштабируемость и гибкость (так как количество входов является фиксированным, то добавление даже одной дополнительной камеры требует покупки дополнительного оборудования).
2. Ограниченность выбора функций (функциональные возможности регистратора заданы производителем и не меняются пользователем в зависимости от стоящих перед ним задач).
3. Невозможность модернизации.

5.3.1 Основные параметры видеорегистраторов

Выполнение требований к устройствам видеозаписи в составе ИСБ реализуется соответствием параметров и функциональных характеристик ЦВР, установленным в технических условиях на конкретные устройства. Рассмотрим основные параметры и функции *DVR* видеорегистраторов.

Видеоканал – совокупность технических средств СОТ, обеспечивающих передачу телевизионного изображения от одной видеокамеры до экрана видеомонитора в составе СОТ [12]. Количество

видеоканалов *DVR* указывает максимальное количество видеокамер, которое допускается подключить к *DVR*. В основном применяются видеорегистраторы на 4, 8, 16 видеоканалов, и редко на 24 и 32 видеоканала.

Выдеовыходы служат для подключения устройств отображения видеоинформации – видеомониторов. Существует несколько вариантов конструктивного оформления выдеовыходов в зависимости от того, на какое устройство выводится видеосигнал: *BNC* видеовыход для композитного видеосигнала; *S-VIDEO, VGA, DVI, HDMI* видеовыходы. Наиболее востребованными являются видеовыходы – *BNC* и *VGA*. Они позволяют выводить изображение на обычный и компьютерный мониторы. Часто кроме основного видеовыхода у ЦВР имеются дополнительные *SPOT*-выходы для вывода, например, в полный экран «тревожной» видеокамеры, в поле зрения которой в данный момент произошло движение. Дополнительный видеовыход с более широкими возможностями называется *MATRIX*. С него можно выводить независимое мультиэкранное изображение или архив видеозаписей.

Аудиовходы служат для подключения микрофонов и позволяют осуществлять синхронную аудиозапись. Количество аудиоканалов колеблется от одного до количества видеовходов ЦВР в зависимости от конструкции.

Тревожные входы и выходы используются для подключения охранных датчиков и исполнительных устройств (сирен, строб-вспышек и т.д.). Количество тревожных входов, как правило, совпадает с количеством видеовходов. При подаче сигнала на тревожный вход регистратор может включить запись по определенному каналу и вывести изображение от него на монитор для привлечения внимания оператора видеонаблюдения.

Разрешающая способность видеорегистратора указывается в пикселах по горизонтали и вертикали. Для *DVR* чаще всего используются следующие разрешения: 352×288, 704x288, 704x576 пикселов.

Скорость записи указывает то количество кадров, которое может обработать регистратор за 1 секунду. Скорость указывают либо в расчете на 1 видеоканал регистратора (скорость на канал), либо на все видеоканалы в сумме (скорость на систему). При указании скорости на систему нужно учитывать количество видеоканалов конкретного видеорегистратора. Так для 4-х канального *DVR* скорость записи может составлять 25, 50, 100 кадров в секунду, для 16 канального регистратора – 100, 200, 400 кадров в секунду на систему.

В системах видеонаблюдения кадровая скорость на канал не может превышать 25 кадров в секунду. Скорость и разрешение записи выбираются из набора дискретных значений и, как правило, указываются совместно. Примеры: 100 к/с (352x288), 12 к/с (704x288), 25 к/с (704x576).

5.3.2 Основные функции видеорегистраторов

Сжатие (компрессия) видеосигнала

ЦВР должны обеспечивать ведение видеоархива и его хранение не менее 15 суток. При этом качество изображения (цветопередача, разрешение) не должно ухудшаться более чем на 10% от максимального качества изображения, получаемого непосредственно от видеокамеры.

Цифровая видеозапись одного видеоканала длительностью 1 секунда с разрешением 704x576 пикселов со скоростью 25 к/с может иметь размер около 30Мбт. Нетрудно посчитать размер архива видеозаписей за 1 час, сутки или месяц. Для того чтобы уменьшить большие объемы видеозаписей, используют алгоритмы сжатия (компрессии) [24,25], которые уменьшают размер файла цифровой видеозаписи посредством удаления графических элементов, не воспринимаемых человеческим глазом. Алгоритмы кодирования видеосигнала применяются для цифрового представления, сжатия, хранения, передачи и обработки видеоинформации.

Алгоритмы делят на статические (работающие с каждым кадром в отдельности) и потоковые (работающие с последовательностями кадров). Компрессия видеосигнала в статических алгоритмах достигается за счет метода обработки изображения каждого кадра. Причем обрабатывается как целое изображение, так и его отдельные блоки. Наиболее распространены в настоящее время алгоритмы *M(Motion)JPEG* и *JPEG*-2000.

Компрессия видеосигнала в потоковых алгоритмах осуществляется с учетом того, что рядом стоящие кадры почти не отличаются друг от друга. Выбирается и кодируется с хорошим качеством один опорный кадр, далее кодируется разница между опорным и текущим кадрами. При появлении значительных отличий выбирается новый опорный кадр и процесс повторяется. Алгоритмы учитывают наличие в изображении объектов, их положение и динамику в последовательности кадров. При этом не только усложняется алгоритм сжатия, но и значительно увеличивается степень компрессии, а, соответственно, и сильно сжимается потоковое видео.

MPEG-2 – потоковый алгоритм, дающий высокое качество видеоизображения (используется в *DVD*).

MPEG-4 – потоковый алгоритм, в три раза более эффективный по сравнению с *MJPEG*.

H.264 – самый прогрессивный на сегодняшний день потоковый алгоритм, сочетает высокое качество видеоизображения (используется для телевизионного вещания *HD-TV*) и высокую степень компрессии. Он способен уменьшить размер файла, содержащего цифровой видеосигнал, более чем на 80% по сравнению с сигналом, сжатым по алгоритму формата *Motion JPEG*, и на 30% эффективней, чем *MPEG*-4 при аналогичных показателях визуального качества.

Потоковые алгоритмы сжимают в несколько раз эффективнее, чем покадровые. Покадровые дают чуть более четкое изображение при

воспроизведении. Наиболее распространены алгоритмы *JPEG*-2000 и *H*.264.

Многозадачность

Видеорегистратор обладает многозадачностью, то есть способностью выполнять несколько задач одновременно: видеозапись, отображение мультикартины, воспроизведение видеоархива, копирование созданного видеоархива на внешние носители информации, трансляции и управления по компьютерной сети. Предусмотрено несколько режимов многозадачности в зависимости от конструкции ЦВР:

- *Simplex* – единовременное выполнение одной операции (когда начинается просмотр архива, запись останавливается);
- *Duplex* – возможность просмотра архива без остановки записи;
- *Triplex* – выполнение трех операций одновременно (например, трансляция, просмотр архива и работа по сети одновременно);
- *Pentaplex* – выполнение пяти и более операций одновременно (например, запись, локальное наблюдение на одном мониторе, просмотр архива на другом мониторе, архивация и сетевая работа).

Видеодетекторы движения

В ЦВР применяется алгоритм, реализующий функцию видеодетектора движения, который анализирует видеоизображение и обеспечивает автоматическое обнаружение движущихся объектов. При срабатывании видеодетектора регистратор может включить запись и вывести изображение с видеокамеры на монитор оператора видеонаблюдения. В сложных системах для увеличения эффективности видеосистемы производится выделение маршрута движения объекта ярким цветом.

У видеодетектора движения настраивается зона детектирования и уровень чувствительности. Чувствительность определяет минимальный размер объекта, на который будет срабатывать видеодетектор. Видеодетектор экономит дисковое пространство, записывая только те кадры, в которых есть движение, экономит время пользователя на поиск событий в видеоархиве.

Видеоаналитика

Для снижения влияния человеческого фактора и повышения эффективности СОТ создаются интеллектуальные системы видеонаблюдения, в которых видеорегистратором или сервером реализуется функция видеоаналитики (видеоанализа) [24,45]. Значительный поток данных передается от видеокамеры к ЦВР, где происходит декомпрессия и видеоанализ. При этом масштабируемость системы ограничивается конечными вычислительными ресурсами ЦВР или сервера. Функциональность интеллектуальных систем видеонаблюдения делится на две группы:

- распознавание и классификация объектов видеонаблюдения;
- отслеживание пути объекта видеонаблюдения.

Возможности видеоанализа находят применение при решении различных задач охраны и контроля объектов видеонаблюдения:

- для видеонаблюдения за поведением объектов, например, за интенсивностью потока в определённой зоне;
- для подсчёта объектов видеонаблюдения, например, транспортных средств или людей в охраняемой зоне;
- для отслеживания путей объектов видеонаблюдения – маршрута движения нарушителя или оставленного без присмотра чемодана в оживленном месте.

Подсчёт объектов видеонаблюдения – одно из важнейших применений видеоанализа. Алгоритм определения количества приходящих и уходящих на объект людей и машин позволяет получить исчерпывающую информацию для оптимизации работы объекта охраны.

Определение несанкционированного прохода средствами видеоанализа позволяет определять ситуации, когда один человек с помощью карточки открывает дверь, а проходит через неё несколько человек.

Контроль толпы реализуется благодаря возможности вести подсчет людей в определенных областях. При этом система может посылать предупреждения при наличии скоплений людей, близких по количеству к критическим, или в ситуациях, когда что-то мешает свободному проходу.

Обнаружение пересечения границы позволяет определить границу или область, доступ в которую будет контролироваться. Если объект видеонаблюдения пересекает эту границу, входит или покидает определенную область, система видеонаблюдения может послать сигнал тревоги охранному персоналу.

Обнаружение оставленных объектов для публичных объектов, правительственных зданий является критически важным компонентом СБ из-за опасностей террористических актов. Ведется наблюдение за областью, при этом сохраняется информация о перемещении объектов внутри неё. Если объект видеонаблюдения сначала двигался, а потом становится неподвижным и долгое время остается без движения, система видеонаблюдения инициирует тревогу и передает информацию о подозрительном объекте оператору СБ.

Сетевые функции

Сетевые функции ЦВР подразумевают реализацию следующих возможностей:

- трансляция видео в реальном времени;
- трансляция аудио;
- просмотр архива;

- архивация (копирование записей с ЦВР на удалённый ПК);
- удаленная настройка ЦВР.

Сетевые функции не только предполагают дистанционное использование возможностей видеорегистратора, но и объединение видеорегистраторов в единую систему видеонаблюдения на базе компьютера.

CMS – Станция централизованного мониторинга (*Central Monitoring Station*) осуществляет управление единой системой видеонаблюдения с использованием ПО для централизованного мониторинга видеорегистраторов и сетевого видеооборудования. Является идеальным решением для контроля ЦВР в распределенных системах видеонаблюдения.

Интерфейсы ЦВР

В видеорегистраторах используются различные интерфейсы для реализации необходимых функций.

USB – последовательный интерфейс передачи данных – используется для архивации видеозаписей на внешние носители информации, а также для подключения компьютерной «мышки» для управления ЦВР через графический интерфейс. Часто *USB*-интерфейс применяется для обновления ПО видеорегистратора.

RS-485 – интерфейс предназначен для управления. Его можно использовать для подключения клавиатур управления ЦВР, либо для передачи сигналов управления от регистратора поворотным камерам.

RS-232 – интерфейс для подключения устройств диагностики и программирования ЦВР.

5.4. Устройства вывода видеоизображения (мониторы)

В качестве устройств вывода видеоизображения в СОТ до недавнего времени применялись аналоговые видеомониторы на основе электронно-лучевых трубок. В последнее время стали активно применяться жидкокристаллические (ЖКИ или *LCD*) мониторы, которые имеют ряд преимуществ: мониторы компактны, долговечны (служат не менее 6–7 лет), просты в настройке и эксплуатации, не чувствительны к электромагнитным полям, эргономичны, быстро монтируются в стойку или на стены и имеют низкое энергопотребление. При выборе монитора для СОТ руководствуются техническими, эксплуатационными и эргономическими требованиями, в соответствии с которыми подбираются параметры видеомонитора, указанные в технической документации [12]:

- размер экрана;
- параметры экрана;
- разрешающая способность экрана;
- параметры видеовхода (тип видеоинтерфейса для компьютерного монитора);

- параметры, связанные с особенностями применения и эксплуатации, показатели безопасности, надежности, электромагнитной совместимости.

Разрешение является одним из основных параметров монитора. Разрешение измеряется числом точек (пикселов) по горизонтали и вертикали. В соответствии с существующими требованиями к ТСОБ, аналоговые или ЖКИ видеомониторы в составе СОТ должны иметь диагональ экрана не менее 17 дюймов и разрешение экрана не ниже 1280x1024 точек (960x768 ТВЛ) [19].

Яркость монитора определяется яркостью заднего освещения экрана. Уровень яркости 250 кд/кв.м является для ЖКИ мониторов достаточно высоким и позволяет видеть контрастное изображение даже в сильно освещенном помещении. С контрастностью монитора связан коэффициент контрастности, соответствующий разнице между яркостью белых и черных тестовых прямоугольников. Чем выше контрастность, тем более естественным и насыщенным будет выглядеть цветное изображение. Современные мониторы для СОТ имеют коэффициент контрастности от 800:1 до 1200:1.

Угол обзора ЖКИ монитора равен крайнему значению, при котором коэффициент контрастности снижается до 10:1 от стандартного значения, соответствующего перпендикулярному положению наблюдателя к плоскости экрана. Современные мониторы, предназначенные для систем видеонаблюдения, имеют значение угла обзора 160 – 170^{o}, что позволяет персоналу службы безопасности видеть изображение на мониторе без потери качества даже тогда, когда ЖКИ монитор находится под углом к оператору.

ЖКИ мониторы могут устанавливаться как на столе с помощью специальной подставки, так и монтироваться на стену или в стандартную 19-дюймовую стойку.

ЖКИ мониторы являются цифровыми устройствами, но могут работать как в аналоговых, так и в цифровых СОТ. Для приема аналогового видеосигнала мониторы, как правило, оснащаются двумя *BNC*-видеовходами. Монитор имеет стандартный 15-контактный *VGA*-вход, который позволяет подключать монитор к компьютеру цифровой СОТ. Некоторые мониторы имеют встроенные динамики для воспроизведения аудиосигнала.

5.5 Кожухи для видеокамер

Для установки видеокамеры в неблагоприятных условиях применяется кожух – устройство, предохраняющее видеокамеру от внешних воздействий (перепадов температуры, влажности, осадков, несанкционированных действий и др.). Кожухи для видеокамер можно разделить на две основные группы:

- гермокожухи – защищают видеокамеру от пыли, случайного механического повреждения, попадания влаги и предназначены для установки внутри помещений;
- термокожухи – способны поддерживать необходимый для функционирования видеокамеры температурный режим. Они предназначены для установки вне помещений и обеспечивают полную защиту от пыли и водяных струй с любых направлений.

В отличие от гермокожухов термокожухи оснащены системами обогрева для работы в условиях низких температур.

Основные параметры и особенности функционирования кожухов определяются как технической документацией, так и существующими нормативными документами [8, 12, 40].

Класс защиты от воздействий пыли и воды (*IP – International Protection*) указывается в виде двух цифр *IP*xx. Первая цифра от 0 до 6 обозначает степень защиты от проникновения твердых механических предметов (в том числе пыли), вторая цифра от 0 до 8 показывает степень защиты от воздействия воды. Например, для уличной установки используют кожухи с классом защиты *IP*66 и *IP*67.

Рабочий диапазон температур термокожуха должен соответствовать климатическим условиям территории, на которой устанавливается система видеонаблюдения.

Поддержание работоспособности видеокамеры в условиях низких температур достигается подогревом, который включается при помощи встроенного в кожух термореле при понижении температуры до –10^{o}C. При этом ведется подогрев как установленного в кожух оборудования, так и смотрового стекла для предохранения его от замерзания. Для предотвращения перегрева видеокамеры в летнее время в некоторые модели кожухов устанавливаются вентиляторы. Вентилятор обеспечивает движение воздуха в замкнутом пространстве термокожуха и равномерное распределение тепла по всему его объёму, предотвращая локальный перегрев.

Размер термокожуха обусловлен внутренним полезным объемом, который должен быть достаточным для размещения видеокамеры с объективом с автодиафрагмой, а также дополнительных устройств, входящих в состав той или иной модели. Во внутреннем пространстве кожуха по усмотрению производителя и установщика дополнительно могут быть расположены встроенный источник питания, устройство передачи видеосигнала по кабелю типа «витая пара», устройство защиты линии видеосигнала от повреждения высоким напряжением («грозозащиты»).

Напряжение питания термокожуха выбирается с учетом действующих на объекте правил электробезопасности и установленной системы бесперебойного питания. Напряжение питания ~220В проще довести без потерь на большие расстояния, но оно опасно для жизни

обслуживающего персонала. Выпускается достаточно много термокожухов с безопасными напряжениями питания 12, 24, ~24В и даже ~42В. Мощность, потребляемая комплектом для наружного видеонаблюдения, определяется суммой мощностей, потребляемых видеокамерой, системой подогрева и дополнительным оборудованием, установленным в кожух.

Большинство моделей кожухов имеют кронштейн с поворотной системой, которые обеспечивают возможность установки кожуха на стене или потолке и ориентации видеокамеры в нужном направлении.

В зависимости от специфики применения отдельных видеокамер применяются модели кожухов с внешними ИК прожекторами, с автоматическим очистителем и омывателем стекла, с дополнительным жидкостным охлаждением и другие.

5.6 Передача видеоинформации в СОТ

В СОТ необходимо передавать видеоинформацию от видеокамер к оборудованию, установленному на постах охраны – видеомониторам, видеорегистраторам и другим устройствам системы видеонаблюдения. Кроме видеосигнала в системе может осуществляться передача аудиосигнала и данных управления функциями объектива и поворотного устройства *PTZ*-видеокамеры – фокусом, диафрагмой, поворотом, наклоном, масштабированием и др. При этом расстояние, на которое осуществляется передача видеосигнала, может составлять от десятков метров до десятков километров. В настоящее время в СОТ используются несколько основных способов передачи видеосигнала: по коаксиальному кабелю, по кабелю «витая пара» и по волоконнооптическому кабелю. В зависимости от расстояния применяют различные технологии и средства передачи видеосигнала.

Коаксиальный кабель в СОТ наиболее распространен. Это надежный и недорогой способ передачи, однако, он имеет свои недостатки. При передаче видеосигнала на расстояние свыше 300 м качество видеосигнала ухудшается – происходит падение уровня сигнала, могут возникать частотные искажения, которые приводят к снижению четкости изображения. Чтобы избежать этого, необходимо через каждые 250–300 м устанавливать усилители видеосигнала. В свою очередь усилители требуют подводки электропитания к месту установки и снижают соотношение сигнал/шум, что также сказывается на качестве видеосигнала.

При расстоянии до 1,5 км используют технологии и устройства передачи видеосигнала по кабелю типа «витая пара». При этом не требуется устанавливать усилители. Данная технология обеспечивает устойчивость к помехам, создаваемым внешними источниками. В состав системы входит специальный передатчик, кабель витая пара и приемник. Использование витой пары позволяет производить передачу различной информации – видеосигнала, аудиосигнала, данных управления, телефонии и пр. При этом

количество передаваемых по одному кабелю сигналов ограничивается только числом витых пар в кабеле. Возможность использования уже имеющихся линий связи снижает стоимость СОТ. В целом, прокладка кабеля «витая пара» обходится существенно дешевле, чем монтажные работы по прокладке коаксиальных или волоконнооптических линий. Кроме того, в случае обрыва линии, ее можно легко восстановить – достаточно соединить проводники соответствующих пар обычной скруткой.

Волоконнооптические системы передачи видеосигнала устойчивы к электромагнитным и радиочастотным помехам, обеспечивают передачу видеосигнала на расстояние до десятков километров без использования усилителей и эффективны для СОТ территориально-распределенных объектов. При этом передача видеосигнала осуществляется с высоким разрешением и без потери качества. Кроме того, волоконнооптические системы отличаются высокой пропускной способностью и исключают возможность несанкционированного доступа к передаваемым видеосигналам и к другой информации.

Несмотря на то, что волоконнооптические системы достаточно дороги, при увеличении дальности передачи видеосигнала стоимость волоконнооптической системы становится меньше стоимости системы с использованием коаксиального кабеля, укомплектованной усилителями видеосигнала, корректорами частотных искажений и другим оборудованием.

В традиционных аналоговых СОТ может использоваться беспроводной способ передачи сигнала от камеры к монитору, использующий радиочастотную либо инфракрасную передачу данных. В цифровых системах использование беспроводных сетей *WiFi* позволяет перенаправить данные к любому удаленному пользователю. Как в аналоговых, так и в цифровых системах при беспроводной передаче используется определенный вид кодирования либо шифрования данных, чтобы исключить попадание информации и возможностей управления в руки посторонних лиц. Такие устройства работают в диапазонах более высоких частот, чем используются в вещательном телевидении – 920 МГц, 2,4 ГГц, 5,8 ГГц. Если требуется высокая степень защищенности передачи данных, то прибегают к помощи передачи в ИК диапазоне. В этом случае видеосигналы передаются по узкому лучу волн видимого спектра либо ближнего ИК диапазона. Перехватить такой луч крайне сложно.

5.7 Сетевые технологии. *IP* камеры

Цифровая СОТ – это система, в которой видеосигнал от видеокамер преобразуется в цифровую форму с помощью аналого-цифрового преобразователя и далее обрабатывается в СОТ в цифровом виде [12].

Цифровая видеокамера, которая передает видеопоток в цифровом формате по сети *Ethernet* с использованием протокола *IP* (*Internet Protocol*), называется ***IP*-камерой**. Системы видеонаблюдения на базе *IP*-камер часто называют системами сетевого видеонаблюдения или *IP*-видеонаблюдением. Они используют проводную или беспроводную *IP*-сеть в качестве среды передачи видео-, аудиопотоков и других данных. Система сетевого видеонаблюдения позволяет просматривать и записывать видеоинформацию из любой точки сети, независимо от того, локальная это сеть или глобальная, такая как Интернет.

Активное внедрение *IP*-систем в охранном телевидении обусловлено рядом причин:

- возможность использования достижений *IT* индустрии;
- отсутствие искажений изображения при передаче и хранении информации в цифровом виде;
- реализация новых функций благодаря возможностям видеоанализа;
- экономическая эффективность для больших видеосистем.

Базовыми компонентами системы сетевого видеонаблюдения являются сетевые видеокамеры, видеокодеры (переводят видеосигналы от аналоговых камер в цифровые *IP*-видеопотоки) и ПО для управления видео. Остальные компоненты, включая сеть, системы хранения и серверы представляет собой стандартное *IT*-оборудование.

Подключение к сетевой системе аналоговых видеокамер с помощью сетевого видеокодера дает пользователям возможность получить преимущества сетевого видео без необходимости полной замены уже существующего на объекте аналогового оборудования (видеокамер и коаксиального кабеля).

Являясь сетевым устройством, каждая *IP*-камера в сети имеет свой *IP*-адрес. *IP*-камеры могут передавать видеоинформацию как в несжатом, так и в сжатом виде с помощью покадровых (*MJPG*) и потоковых (*MPEG*-4, *H*.264) методов. В качестве протоколов транспортного уровня в *IP*-камерах могут использоваться протоколы: *TCP (Transmission Control Protocol* – протокол управления передачей*)*, *UDP (User Datagram Protocol* – протокол пользовательских датаграмм*)*, *RTP(Real-time Transport Protocol* – используется при передаче трафика реального времени) и другие транспортные протоколы сетевого протокола *IP*.

Благодаря тому, что *IP*-камерам не требуется передавать аналоговый сигнал, в *IP*-камерах могут использоваться большие разрешения, включая мегапиксельные. Стандартное разрешение для сетевых камер: 640x480 точек. Существуют видеокамеры с мегапиксельными разрешениями: 1280x1024, 1600x1200 и более высокими значениями.

Система сетевого видеонаблюдения обладает преимуществами и функциональностью, недоступными аналоговым системам наблюдения:

- Достижение высокого качества изображения, необходимого для четкой фиксации происходящего и идентификации участников события. Использование прогрессивной развертки и мегапиксельной технологии в сетевых камерах позволяет достичь лучшего качества и большего разрешения изображения, чем в аналоговых камерах.
- В системе сетевого видеонаблюдения добиться высокого качества изображения проще, чем в аналоговой системе. В настоящее время в аналоговых системах, использующих ЦВР, происходит несколько преобразований: сначала аналоговые сигналы преобразуются в камере в цифровые, затем обратно в аналоговые для передачи, а после вновь оцифровываются при записи. Качество сохраняемого изображения ухудшается с каждым преобразованием, а также при передаче на большие расстояния. Чем больше дальность передачи аналогового видеосигнала, тем слабее он становится. В полностью цифровой СОТ изображение оцифровывается один раз в сетевой камере и затем остается в цифровом виде без дополнительных преобразований и потерь качества вне зависимости от дальности передачи по сети. Также цифровое изображение легче хранить и получать доступ к носителям видеоинформации, по сравнению с аналоговыми видеокассетами.
- Управление событиями и применение интеллектуальных видеотехнологий. Часто при больших объемах записанной видеоинформации не хватает времени для качественного анализа записей. Сетевые камеры и видеокодеры со встроенными интеллектуальными или аналитическими функциями помогают решать эту проблему, уменьшая количество ненужных записей и используя заранее определенные события. Такие возможности недоступны в аналоговых системах.

Преимущества сетевых видеокамер по сравнению с аналоговыми:

- возможность построения масштабируемых распределённых систем видеонаблюдения;
- широкий диапазон параметров настроек работы видеокамеры;
- отсутствие «привязки» к аналоговым видеостандартам, в результате чего возможно внедрение *IP*-камер со значительно более высоким разрешением;
- удаленный доступ – *IP*-камеры можно настраивать удаленно, обеспечив возможность нескольким авторизованным пользователям просматривать изображение в режиме реального времени и записывать видео практически из любой, имеющей доступ в сеть, точки мира;
- возможность передачи аудиопотока по сети параллельно с видеопотоком;
- возможность передачи потока с высоким сжатием, которое позволяет экономить место на цифровых носителях, не требуя при этом высокопроизводительного видеорегистратора.

Недостатки сетевых видеокамер по сравнению с аналоговыми:

- цена на *IP*-камеры выше, чем у аналоговых камер, но если рассматривать оборудование объекта системой видеонаблюдения в целом, то цены на "проект + оборудование + монтаж" являются сопоставимыми;
- чувствительность матрицы мегапиксельных *IP*-камер как правило существенно ниже, чем у аналоговых камер;
- необходимость наличия значительной вычислительной мощности устройства обработки информации для декомпрессии видеопотока на компьютерной платформе (клиенте), что увеличивает затраты;
- подверженность к внешнему сетевому воздействию (взлому);
- аппаратное зависание (при отсутствии функции *Watchdog timer*).

Функции *Watchdog Timer*

Любая, даже самая качественная *IP*-камера может дать сбой, и в такие моменты не обойтись без ручной перезагрузки, а, значит, необходимо участие оператора. Даже элементарные неполадки системы занимают достаточно много времени от момента их возникновения до устранения вручную, что неприемлемо для СБ. Данная проблема решается с помощью аппаратно реализованной схемы контроля за «зависанием» системы «Сторожевой таймер» (*Watchdog timer*).

Схема представляет собой таймер, который периодически сбрасывается контролируемой системой. Если сброса не произошло в течение некоторого интервала времени, происходит принудительная перезагрузка системы. В некоторых случаях сторожевой таймер может посылать системе сигнал на перезагрузку («мягкая» перезагрузка), в других случаях перезагрузка происходит аппаратно. Сорожевой таймер используется как в *IP*-камерах, так и в системах передачи, обработки и записи видеопотока.

***NVR* и *PC-based* видеосерверы**

Выбор станционного оборудования для системы *IP*-видеонаблюдения – один из самых ответственных этапов в построении современной СОТ. В настоящее время используется два варианта решений:

- сетевые видеорегистраторы (*NVR*) по назначению аналогичны *DVR* в случае с аналоговыми видеокамерами;

- устройства на основе ПК, так называемые *PC-based,* представляют собой сервер с операционной системой и установленным ПО обработки видеоизображения.

Преимущества *DVR* и *NVR* сходны: простота в установке и настройке, сохранен основной принцип «включил и работает»; высокая надежность в работе *NVR* по сравнению с *PC-based* реализацией.

Недостатки *NVR* по сравнению с *PC-based* платформой:

1. Функциональная ограниченность и ограниченность возможности модернизации.

2. Часто невозможность использования *IP*-устройств различных производителей. Производители *NVR* как правило поддерживают совместную работу только с собственными *IP*-камерами.

3. Ограничение по количеству поддерживаемых *IP*-камер. Количество *IP* камер, поддерживаемых одним *NVR*, обычно ограничено до шестнадцати.

4. Сложность ремонта. В случае выхода из строя *NVR* его необходимо ремонтировать в сервисном центре производителя. При использовании *PC-based* платформы программное обеспечение можно при необходимости переустановить на другой ПК, а отремонтировать ПК гораздо проще.

Преимущества *PC-based* видеосерверов:

1. Функциональность, возможность модернизации. Видеосерверы *PC-based* строятся либо на открытой платформе, либо на базе коммерческого ПО. Оба варианта позволяют расширять систему, масштабировать и наращивать функционал. Производители открытых платформ свободно предоставляют все изменения в ПО, пользователи получают доступ ко всем последним достижениям и наработкам в сфере *IP*-видеонаблюдения. Коммерческое ПО позволяет расширять систему и наращивать её возможности на платной основе. Модернизация на уровне платформы ПК позволяет увеличивать глубину архива, производительность и функциональные возможности.

2. Использование разнотипного оборудования. Гибридные схемы. *PC-based* видеосерверы позволяет интегрировать оборудование разных производителей, что позволяет инсталлятору подобрать наиболее подходящее клиенту решение. В ситуациях, когда к существующей системе на основе аналоговых камер и *PC-based* видеосервера добавляются *IP*-видеокамеры, не понадобится менять станционное оборудование.

3. Возможность интеграции подсистем безопасности. Благодаря открытой платформе, возможно интегрировать в единую СБ системы видеонаблюдения, контроля доступа, охранной и пожарной сигнализации, систему инженерно-технической укрепленности здания. Это позволяет реализовать множество алгоритмов взаимодействия ПСБ, которые существенно повышают эффективность системы в целом. Единый интерфейс, распределенная архитектура, удаленный доступ делают работу службы безопасности более продуктивной.

6 ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ

При разработке эффективной СБ следует учитывать перспективы развития объекта охраны, прогноз возникновения новых угроз и современные достижения в области охранных технологий. В противном случае СБ может быстро устареть, а её модернизация будет неэффективной.

Комплексный научный подход к созданию СБ важных объектов подразумевает реализацию трех основных этапов [21]:

1. Концептуальное (системное) проектирование.
2. Рабочее проектирование.
3. Внедрение.

Структура мероприятий по созданию и внедрению комплекса СБ в эксплуатацию на охраняемом объекте приведена на рис.6.1. Рассмотрим более подробно содержание основных элементов жизненного цикла системы комплексной безопасности объекта.

6.1 Жизненный цикл систем безопасности

Каждый из этапов жизненного цикла СБ имеет свои цели и задачи по их достижению. Для решения этих задач должны быть выделены определенные ресурсы.

Основными разделами концептуального проекта являются:

1. Анализ уязвимости объекта и существующей СБ.
2. Разработка принципов комплексной защиты объекта.
3. Разработка технико-экономического обоснования (ТЭО) создания СБ и комплекса ТСОБ.

Основной задачей первых двух разделов этапа концептуального проектирования является разработка "Концепции безопасности объекта", которая определяет направления и методы решения задач по обеспечению безопасности объекта. Концепция безопасности формируется на основе обработки результатов предпроектного обследования объекта, которое выполняется экспертами проектной организации.

Предпроектное обследование проводится с целью анализа уязвимости существующей на объекте СБ. При этом решаются следующие задачи:

- определение объекта охраны и его категории значимости;
- составление списка и параметров угроз для объекта охраны;
- создание модели нарушителя;
- оценка вероятности реализации угроз;
- оценка потенциального ущерба при реализации угроз;
- оценка эффективности существующей СБ.

При определении объекта охраны производится уточнение и детализация списка жизненных приоритетов и ценностей. Например, при

ограничении списка только имуществом выполняется конкретизация защищаемого имущества применительно к данному объекту.

При определении угроз и модели их исполнителя составляется максимально полный перечень не только реальных, но и потенциальных угроз, которые могут возникнуть по различным причинам. Это позволит в дальнейшем точнее определить основной состав СБ, перечень ПСБ, входящих в нее, и обнаружить выявленные угрозы.

Оценка вероятности угроз, а также возможных потерь, ущерба при их реализации позволяет оптимизировать структуру создаваемой СБ с точки зрения целесообразности создания соответствующих подсистем обнаружения и ликвидации угроз и, следовательно, избежать в будущем лишних затрат.

Таким образом, данная оценка позволяет конкретизировать и сократить составленный прежде полный перечень угроз. Например, небольшой возможный ущерб от угрозы, низкая вероятность ее реализации и, в то же время, высокая стоимость создания соответствующей подсистемы делают нецелесообразным ее включение в состав СБ.

Результаты предпроектного обследования используются для составления ТЭО создания СБ и комплекса ТСОБ данного объекта [28, 32].

ТЭО представляет собой документ, который может использоваться службой безопасности заказчика в качестве руководства по организации СБ и планированию работ по оборудованию объекта комплексом ТСОБ или его подсистемами. При разработке ТЭО решаются следующие задачи:

- разработка структуры СБ и различных вариантов построения комплекса ТСОБ с оценкой стоимости их реализации;
- количественная оценка уязвимости СБ с различными вариантами структуры ТСОБ и выбор наиболее эффективного варианта охраны.

Формирование структуры СБ и выбор ТСОБ выполняются, исходя из перечней жизненных приоритетов и угроз их существованию.

Количественная оценка уязвимости объекта и эффективности предлагаемых вариантов СБ, производится с учетом выявленных ранее угроз и модели нарушителей, вероятности обнаружения нарушителя с помощью ТСОБ, вариантов тактики ответных действий сил охраны, а также временных параметров (времени задержки преодоления нарушителем физических барьеров, времени ответных действий сил охраны и др.) [18, 27]. Путем моделирования действий нарушителей и сил охраны производится оценка основного показателя эффективности СБ – ***вероятности перехвата нарушителя*** силами охраны, действующими по сигналу срабатывания комплекса ТСОБ.

По результатам анализа уязвимости разрабатываются общие рекомендации по обеспечению безопасности объекта с ориентировочной оценкой стоимости создания предлагаемой СБ. При этом сравнивается ориентировочная стоимость предотвращаемого ущерба ($С_{ПУ}$) и затраты на

создание предлагаемой СБ ($С_{СБ}$). Обязательным условием целесообразности внедрения СБ в систему охраны объекта является выполнение неравенства:

$$С_{ПУ} > С_{СБ}$$

Сравнительная количественная оценка эффективности вариантов комплекса ТСОБ позволяет на начальной (допроектной) стадии выбрать вариант, обладающий достаточно высокой эффективностью при минимальных затратах на его создание и внедрение в СБ. Такой подход позволяет избежать серьезных ошибок в рабочем проекте и излишних затрат на возможную доработку системы при ее эксплуатации.

Результатом оценки эффективности СБ могут быть следующие решения:

- утверждение ее структуры и состава, если результаты оценки вписываются в действующие ограничения (финансовые, технические, юридические, ведомственные, организационные);
- пересмотр структуры и состава при несоответствии ограничениям.

В последнем случае, в зависимости от характера и степени несоответствия, следует вернуться либо на начало процедуры, либо на один из промежуточных этапов или шагов (рис.6.1).

Таким образом, результаты работы оформляются в виде ТЭО, которое содержит необходимые сведения по следующим вопросам:

- концепция безопасности объекта;
- структура и состав СБ и комплекса ТСОБ;
- количественная оценка уязвимости объекта и эффективности существующей и предлагаемой СБ;
- ожидаемые тактико-технико-экономические показатели ТСОБ;
- рекомендации по организации оперативных действий сил охраны с применением комплекса ТСОБ;
- ориентировочный расчет необходимой численности технического персонала для обслуживания комплекса;
- ориентировочный расчет необходимой численности сил охраны;
- ориентировочный расчет стоимости всех этапов работ по оборудованию объекта предлагаемым комплексом ТСОБ.

Результаты, полученные на стадии ТЭО, используются в качестве исходных данных для разработки технического задания (ТЗ) на рабочее проектирование оборудования объектов комплексами ТСОБ.

Рисунок 6.1– Структура жизненного цикла системы безопасности

Составление ТЗ на разработку проекта по созданию (модернизации) СБ выполняется проектной организацией и представляет собой документ, который определяет параметры проектируемой системы, методы их измерения, а также устанавливает основные сроки выполнения проектных работ и порядок их финансирования [29, 35].

При проектировании СБ создается, согласуется и утверждается рабочая документация, включающая следующие обязательные элементы:

- структурные и функциональные схемы СБ;

- планы объектов с указанием мест размещения оборудования СБ;
- схемы соединений;
- кабельный журнал;
- сметы расходов;
- расчетно-пояснительная записка с описанием схем и расчетами для обоснования предлагаемых технических, организационных и тактических аспектов защиты объекта охраны;
- описание последовательности оснащения объекта элементами СБ.

Оснащение (модернизация, демонтаж) СБ объекта охраны предполагает решение следующих задач:

- организацию тендера на выполнение работ по оснащению (модернизации, монтажу) СБ;
- определение и реализацию схемы финансирования проведения работ;
- заключение договоров подряда и субподряда на выполнение работ, согласно проектной документации;
- приобретение материальной базы системы;
- организацию режима работы СБ;
- заключение договоров на выполнение функций службы безопасности и технического обслуживания комплекса ТСОБ;
- проведение монтажных и пусконаладочных работ;
- выполнение авторского надзора проектной организацией;
- ввод СБ в эксплуатацию с оформлением соответствующих актов.

Эксплуатация СБ объекта охраны должна обеспечивать:

- требуемый уровень защиты от проектных угроз;
- поддержание работоспособного состояния оборудования СБ в течение всего жизненного цикла системы, ведение эксплуатационной документации;
- проведение тактических учений с моделированием угрожающих воздействий;
- исключение саботажа работы СБ.

Рассмотрим основные вопросы, связанные с рабочим проектированием и подбором оборудования для оснащения СБ охраняемого объекта.

6.2 Процедура проектирования систем безопасности

Проектирование комплекса средств инженерно-технической безопасности является одной из наиболее важных задач при построении комплексной СБ. От качества ее проработки будет зависеть эффективность создаваемой системы. Проектируемый комплекс ТСБ должен быть ориентирован на решение **конкретных задач** и **минимизацию возможных рисков и угроз** с учетом специфики конкретного объекта. То есть каждая видеокамера, каждый извещатель или считыватель должны решать четко

определенную задачу и вносить свой вклад в единую систему обеспечения безопасности объекта [36, 38].

При проектировании СБ необходимо учитывать то, что ограничения списков жизненных приоритетов, возможных угроз и состава технических средств приводят к увеличению риска того, что СБ не выполнит свои функции. Например, снижение затрат на оборудование всегда означает отказ от некоторых защитных функций. Необоснованная экономия на первичных затратах приводит к увеличению эксплуатационных расходов и к снижению эффективности системы. Рассмотрим основные риски, которые могут повлиять на эффективность проектируемой СБ [1, 26].

Осознанный риск означает, что могут быть реализованы угрозы, которые не вошли в перечень, сформированный на этапе предпроектного обследования обекта, и СБ не предусматривает защиту от них. Например, при создании только системы охранной сигнализации, отсутствует защита от пожара.

Непредсказуемый риск означает, что угрозы, которые вошли в отобранный перечень, могут быть реализованы в отношении других жизненных приоритетов. Например, если проникновение злоумышленников в квартиру с целью кражи имущества происходит в момент присутствия жильцов дома, создается не предусмотренная ранее угроза жизни владельцев имущества.

Заданный риск определяет заданный уровень последствий реализации угроз (определение допустимого уровня ущерба).

Технический риск означает, что СБ, как любая техническая система, может не выполнить свои задачи, например, из-за отказа, неисправности оборудования.

Если заказчик ознакомлен и согласен с рисками, возможными в связи с ограничениями на СБ, он берет на себя ответственность за нежелательные последствия, которые могут иметь место из-за снижения защитных функций проектируемой системы.

6.2.1 Выбор оборудования для системы безопасности

Выбор систем защиты и состава оборудования для комплекса ТСОБ по каждому конкретному объекту должен отвечать принципу необходимости и достаточности [22, 23, 50, 51]. Для подбора и объективного сравнения систем, предлагаемых для использования в комплексе ТСОБ, при проведении тендера целесообразно исходить из анализа тактико-технических данных оборудования и следующих исходных данных по объекту охраны:

- размер защищаемой площади, $м^2$;
- количество этажей в здании;
- общее количество помещений;
- наличие чердаков, подвалов;

- количество входов (выходов);
- количество помещений складов;
- количество особо важных помещений, вход в которые ограничен;
- общее количество сотрудников;
- общее количество людей, одновременно находящихся в здании;
- объекты контроля системы охранного телевидения;
- необходимость децентрализованной «постановки/снятия» с охраны помещений с помощью индивидуальных считывателей или групповых пультов;
- возможность перспективного развития объекта, %;
- необходимость видеонаблюдения по периметру и площади;
- уровень освещенности охраняемой территории;
- режимы цифровой записи изображений от видеокамер;
- время архивирования и хранения видеоизображений;
- скорость записи видеоизображений – не менее 6 кадров/с;
- одновременная запись «тревог» от видеокамер.

При выборе ТСОБ необходимо предварительно убедиться в наличии на каждую систему следующей документации:

- сертификатов соответствия: ГОСТ Р и пожарной безопасности на систему и все блоки, входящие в ее состав;
- сертификата *ISO* 9001 (для импортных систем);
- полного комплекта эксплуатационно-технической и ремонтной документации на русском языке;
- русифицированного ПО и описания отображения информации на блоках контроля и управления;
- лицензий на проектирование и монтаж соответствующих систем;
- наличие предлагаемого оборудования в перечне МВД РФ;
- расчета эффективности использования базового комплекта аппаратуры для защиты заданного количества объектов.

Далее необходимо сравнить элементы предлагаемых ПСБ по следующим параметрам.

Система охранной сигнализации:

- фирма, страна производитель;
- наличие промышленного серийного производства;
- минимальная и максимальная ёмкости системы;
- возможность расширения ёмкости;
- количество регистрируемых параметров;
- возможность интегрирования с другими ПСБ;
- общее количество контролируемых шлейфов сигнализации;
- наличие выносных пультов программирования, контроля и управления;

- возможность организации нескольких АРМ;
- максимальная длина линии интерфейса *RS*-485;
- количество команд, реализуемое по интерфейсу *RS*-485;
- количество сообщений, передаваемых по интерфейсу на центральный пульт;
- среднее время наработки на отказ в «дежурном» режиме;
- вероятность ложных срабатываний за 1000 часов работы в «дежурном» режиме;
- наличие в комплекте считывателей с режимом «постановки/снятия» и контроля доступа;
- устойчивость к воздействию электромагнитных помех;
- обеспечение пожарной безопасности в аварийном режиме;
- диапазон рабочих температур;
- наличие в документации схем: структурной, принципиальной, входного контроля;
- состав и стоимость комплекта оборудования и ПО для защиты объекта.

Системы пожарной сигнализации и оповещения о пожаре:

- фирма, страна производитель;
- тип системы (аналоговая, адресная, адресно-аналоговая);
- количество радиальных/кольцевых шлейфов;
- общее количество датчиков/блоков, подключаемых в шлейф;
- объем сохраняемой информации;
- наличие режима повышенной чувствительности (день/ночь);
- возможность управления системами оповещения и пожаротушения;
- возможность организации нескольких АРМ;
- наличие адресных модулей (контроля, управления), шлейфов с традиционными датчиками;
- наличие выхода на ПК;
- наличие порта *RS*-232 или *RS*-485 для передачи информации на другие ПСБ;
- количество независимо программируемых групп;
- возможность и диапазон увеличения ёмкости системы;
- возможность интегрирования с другими ПСБ;
- максимальная длина (сопротивление) шлейфа сигнализации;
- максимальная длина линии интерфейса *RS*-485;
- наличие выносных пультов управления;
- состав и стоимость комплекта оборудования и ПО для конкретного объекта;

- ПО для приема и отображения информации;
- ПО для передачи конфигурации системы на ПК;
- возможность управления и контроля инженерными системами здания.

Система охранного телевидения:

- тип используемых видеокамер черно-белого/цветного изображения: аналоговые; цифровые;
- формат чувствительного элемента видеокамеры;
- разрешающая способность;
- чувствительность (по освещенности объекта);
- соотношение сигнал/шум;
- наличие автодиафрагмы;
- максимальное количество видеокамер, подключаемое к системе;
- минимальная суммарная скорость записи;
- алгоритм сжатия видеоизображения;
- объем памяти (в базовом варианте);
- формат мультиэкрана;
- наличие «стоп-кадра»;
- возможность и длительность (в секундах) записи видеоизображения «до» (предтревожная запись) и «после» тревожного события;
- наличие встроенного генератора данных (дата, время, номер видеокамеры);
- наличие встроенного видеодетектора движения;
- наличие «тревожных» входов, управляемых сигналами от других ПСБ;
- наличие и количество выносных пультов управления;
- состав и стоимость комплекта системы и ПО для оборудования объекта.

Система контроля и управления доступом:

- фирма, страна производитель;
- тип идентификатора для контроля доступа;
- учет количества сотрудников (посетителей), прошедших через проходную;
- наличие режима учета рабочего времени;
- возможность создания единой сети считывателей;
- общее количество распределенных по объекту точек прохода, которые контролируются системой;

- возможность использования считывателей для «входа/выхода» в помещение для его «сдачи/снятия» с охраны;
- максимальный объем информации, который обрабатывается системой за сутки (количество человек);
- количество проходов и регистраций событий в течение часа;
- возможность использования турникетов в качестве шлюзов;
- наличие индикаторов (зеленый/красный) для обозначения разрешения/запрещения прохода;
- наличие системного ПО и указание количества модулей для решения конкретных задач;
- возможность изменения алгоритма пропуска заказчиком системы;
- ресурс работы механической части системы;
- состав и стоимость комплекта оборудования и ПО.

Система бесперебойного электроснабжения:

- вид системы;
- мощность нагрузки;
- напряжение нагрузки;
- оптимальный ток нагрузки;
- время непрерывной работы системы при использовании аккумуляторов или бензо/дизель-агрегатов;
- автоматическое переключение на резервное питание при пропадании основного электроснабжения;
- время выхода на рабочий режим бензо/дизель-агрегатов;
- фирма, страна производитель;
- стоимость.

6.2.2 Выбор вариантов охраны объекта

Методика выбора рационального варианта охраны объекта с использованием комплекса ТСОБ содержит два основных этапа.

1. Обследование объекта охраны, в результате которого определяется:

- тип объекта, его важность или значимость (характер и структура размещения материальных, информационных и других ценностей, места их расположения, концентрация);
- структура объекта (территории, зоны, здания, сооружения и помещения, подлежащие защите, их количество, типы, размеры, расположение);
- наиболее уязвимые и вероятные места проникновения на объект, их количество, конструктивные особенности и размеры;
- зоны и помещения объекта, требующие ограничения доступа и дистанционного контроля с помощью телевидения;

- другие характеристики объекта (архитектурно-строительные особенности, местоположение, телефонизация, количество въездов/выездов, входов/выходов, этажность);
- телефонизация и характеристика сети питания (энергоснабжение).

2. Формирование структуры построения системы, которое предполагает:

- выбор тактики охраны объекта (автономная, централизованная или комбинированная);
- определение структуры охраны (количество зон или рубежей охраны, какие ПСБ будут использоваться, их состав, организация их взаимодействия, уровни интеграции ПСБ в единый комплекс, наличие и количество АРМ);
- определение точек доступа, зон просмотра видеокамерами, зон оповещения и т.п.;
- определение количества шлейфов сигнализации и их структуры (разделение шлейфов на самостоятельные блокируемые участки и определение мест их расположения на объекте);
- определение размеров и характеристик уязвимости блокируемых участков (открывание, пролом, перелаз, подкоп, разбитие, комбинация способов);
- выбор СОУ (по назначению, виду зоны контроля, принципу действия, и конкретным тактико-техническим характеристикам, таким как дальность обнаружения, угол обзора, чувствительность, диапазон рабочих температур, помехоустойчивость, надежность, сложность установки и монтажа, удобство технического обслуживания и ремонта, антисаботажные свойства);
- выбор технических средств ССОИУ (ППК, КП, устройства их сопряжения с СПИ и другими ПСБ, типы световых и звуковых оповещателей, тип идентификатора, считыватели, преграждающие устройства, контроллеры, мониторы, устройства записи, хранения и воспроизведения информации);
- определение схемы электроснабжения ТСОБ и охранного освещения (выбор источников бесперебойного и резервного электропитания);
- определение мест размещения оборудования, трасс и способов прокладки соединительных проводов и кабелей.

Выбор тактики охраны объекта выполняется заказчиком.

При **автономной тактике** охрана объекта может осуществляться постами охраны либо собственными силами (охранники, служба безопасности объекта), либо с привлечением сторонних охранных структур. При этом на объекте может отсутствовать комплекс ТСОБ. Данный вид охраны применяется для офисов небольших компаний или организаций.

Более распространен другой вариант охраны, который предполагает оснащение объекта полным комплексом ТСОБ, наличие центрального пункта управления системами (пультовой), собственной службы безопасности и собственных или привлеченных сил реагирования на нештатные ситуации. Такой вид охраны характерен для средних и крупных объектов.

Централизованная тактика охраны применяется подразделениями вневедомственной охраны МВД РФ, которая является естественным монополистом этого вида охраны и обладает самой разветвленной и технически оснащенной сетью ПЦО и подразделений в стране. При этом обязательным является оснащение объектов техническими средствами охранной и (или) тревожной сигнализации. Допускается оснащение и другими ПСБ [34, 41].

В настоящее время в крупных городах появились альтернативные ПЦО частных охранных структур, использующие централизованную тактику охраны объектов с помощью СПИ, работающих по радиоканалу.

Для передачи извещений о срабатывании сигнализации в ПЦО используются ППК, КП, внутренний пульт охраны или устройство оконечной СПИ. Передача извещений выполняется по специально проложенным линиям связи, свободным или переключаемым на период охраны телефонным линиям, радиоканалу, занятым телефонным линиям с помощью аппаратуры уплотнения или информаторных СПИ методом коммутируемого телефонного соединения («автодозвона»). При поступлении на ПЦО сигнала тревоги на охраняемый объект немедленно высылается группа задержания для принятия адекватных мер противодействия.

При данной тактике объекты находятся под охраной только в нерабочее время, то есть объекты закрыты, на них отсутствуют люди, они полностью находятся под защитой комплекса ТСОБ. В рабочее время объекты снимаются с охраны и функционируют в обычном режиме. Если объекты оснащены тревожной сигнализацией, то ее контроль на ПЦО осуществляется в круглосуточном режиме, то есть и в рабочее время.

При **комбинированной тактике** сочетаются элементы автономной и централизованной охраны. Например, в рабочее время объект охраняется собственными силами или силами сторонних охранных структур, а в нерабочее время сдается под охрану на ПЦО. Возможен вариант круглосуточной охраны собственной службой безопасности, при котором часть наиболее важных помещений объекта (хранилище ценностей, комнаты хранения оружия, наркотических веществ) одновременно охраняется с помощью ПЦО, либо на ПЦО выведена только тревожная сигнализация объекта. Такая тактика охраны характерна для объектов кредитно-финансовой сферы, крупных организаций, а также органов власти.

Рассмотрим рекомендации по выбору оборудования сигнализации для блокировки наиболее уязвимых мест рубежей охраны объекта [21, 42].

Первым рубежом (или зоной) обеспечения безопасности объекта является его периметр, основные уязвимые места которого следующие:

- строительные конструкции по периметру здания или помещений объекта (все оконные и дверные проемы);
- места ввода коммуникаций, вентиляционные каналы;
- выходы к пожарным лестницам;
- некапитальные и капитальные стены (если необходима защита).

При этом строительные конструкции здания (помещений) объекта блокируют:

- дверные проемы, погрузоразгрузочные люки блокируются на «открывание» и «пролом» (только для деревянных конструкций);
- остекленные конструкции – на «открывание» и «разрушение стекла»;
- места ввода коммуникаций, некапитальные и капитальные стены (если необходима защита) – на «пролом»;
- вентиляционные короба, дымоходы – на «разрушение».

Допускается проводить блокировку указанных конструкций только на «проникновение» с помощью активных и пассивных оптико-электронных извещателей. Блокировку дверей, остекленных конструкций на «открывание» рекомендуется проводить магнитоконтактными извещателями, а блокировку ворот, погрузоразгрузочных люков, дверей хранилищ, лифтовых шахт – конечными выключателями. Блокировку остекленных конструкций на «разрушение» стекла рекомендуется проводить омическими извещателями (типа «фольга»), поверхностными ударно-контактными или звуковыми извещателями. Блокировку стен на «пролом» следует проводить поверхностными вибрационными, пьезоэлектрическими или омическими (типа «провод») извещателями.

При создании первого рубежа охраны периметр делят на участки длиной не более 200м в зависимости от технических характеристик применяемого оборудования. Это позволяет оперативно определить участок периметра, на котором произошло нарушение, и принять соответствующие меры.

Должна быть предусмотрена блокировка путей проникновения на защищаемые объекты из примыкающих к ним бесхозных, заброшенных строений, а в частные дома и квартиры граждан – через потолки, подвалы, балконы и лоджии соседних квартир.

Для визуального контроля, а также для повышения надежности выявления места и характера нарушения применяют средства СОТ, а для ограничения доступа в защищаемые помещения и на территорию объекта – средства СКУД. Для обеспечения функционирования видеокамер на периметре объекта, он должен быть оснащен охранным освещением

(видимого или инфракрасного диапазона) с дистанционным управлением включения: ручного (по команде оператора) и автоматического (по сигналу тревоги).

Вторым рубежом охраны защищают внутренние объемы помещений пассивными оптико-электронными, ультразвуковыми, комбинированными или радиоволновыми извещателями. Выбор извещателя определяется площадью помещения, характером сосредоточения (рассредоточения) и местом размещения материальных и иных ценностей в помещениях объекта, помеховой обстановкой, условиями окружающей среды.

Третий рубеж охраны защищают непосредственные места хранения ценностей (сейфы, металлические шкафы, ящики, сами ценности, например, экспонаты музеев, выставок) и подходы к ним. Для этого используются емкостные, пьезоэлектрические, пассивные и активные оптико-электронные или радиоволновые извещатели. На крупных и важных объектах устанавливают дополнительные извещатели-«ловушки», которыми оснащают локальные участки и пути, ведущие к местам хранения ценностей.

На объектах может быть установлена тревожная сигнализация, предназначенная для передачи сигналов тревоги на пульты местной или централизованной охраны. Тревожной сигнализацией оснащаются рабочие места сотрудников, производящих денежные операции с клиентами, в банках, кассах крупных торговых компаний и фирм, почтовых отделениях и узлах связи, ювелирных магазинах, ломбардах, хранилищах ценностей, комнатах инкассаторов и хранения оружия, кабинетах руководителей организаций, компаний и фирм, на постах охраны. В качестве средств тревожной сигнализации используют кнопки (в том числе носимые, работающие по радиоканалу), педали, магнитоконтактные или оптико-электронные извещатели.

Таким образом, несмотря на сложность и многогранность выбора и построения системы безопасности объекта, все необходимые требования к ней должны быть четко сформулированы и оформлены заказчиком в виде технического задания на ее проектирование.

6.3 Методы оценки эффективности систем безопасности

Для оценки эффективности ИСБ существуют методы, на основе которых можно сравнивать конкурирующие варианты ИСБ, оценивать и обосновывать обеспечение заданных заказчиком характеристик. Без этих методов заказчик часто находится под «гипнозом» цены (чем дешевле, тем лучше), а вопросы обеспечения эффективности отходят на второй план.

Эффективность СБ характеризует вероятность выполнения системой своей основной целевой функции по обеспечению защиты объекта от угроз,

источниками которых являются умышленные противоправные (несанкционированные) действия физических лиц (нарушителей).

Учитывая сложность решаемых задач, исходя из принципов рационального и эффективного использования денежных средств, создание системы защиты должно базироваться на следующих принципах:

- разумной достаточности мер;
- четкой правовой основе;
- организованной службе физической охраны;
- оптимальном составе технических средств защиты.

Система считается эффективной, если выполняются следующие требования:

1. в заданных условиях эксплуатации полностью и в установленные сроки выполняет стоящие перед ней задачи (техническая эффективность);

2. затраты на создание и эксплуатацию системы не превышают положительного эффекта от ее использования (экономическая эффективность).

Оптимизацию структуры СБ можно рассматривать как выбор наилучшего варианта из множества альтернатив. При этом основным критерием выбора является удовлетворение СБ требованиям эффективности при минимальном уровне затрат. Поэтому вопрос количественной оценки эффективности функционирования СБ является актуальным, но применительно к СБ он разработан слабо.

Применение общих критериев к СБ затруднено по нескольким причинам. К ним следует отнести многообразие угроз объекту, способов их реализации; разнообразие объектов с точки зрения конфигурации и пространственного расположения, режима функционирования, режима обеспечения безопасности; структурную и организационную сложность СБ.

Тем не менее общие методы оценки эффективности систем различного назначения можно с соответствующими изменениями применять к СБ. Принято использовать экономические, вероятностные, комбинированные и надежностные методы для оценки эффективности СБ [1,20,31].

При определении **экономической** эффективности СБ рассматривается соотношение положительного экономического эффекта (Э) от использования системы и общих затрат (З), включающих стоимости её создания и обслуживания в течение срока эксплуатации. При этом оценивается относительная эффективность системы, которая может быть представлена в следующем виде [1]:

$$Э_О = \frac{П - З}{П_О} = У_П - \frac{З}{П_О}, \qquad (6.1)$$

где $П = П_О \times У_П$ – предотвращенные потери в результате использования системы; $П_О$ – общие возможные потери; $У_П$ – относительный

предотвращенный ущерб в результате использования системы безопасности ($0 < У_{П} < 1$).

Величина ущерба складывается из следующих составляющих:

- стоимости, направленной на возмещение последствий события (компенсация);
- стоимости похищенного или уничтоженного пожаром имущества, (ремонт объекта и т.п.);
- стоимости дополнительных временных расходов (восстановление работоспособности участка, которому нанесен ущерб);
- относительной стоимости, определенной убытками из-за случившегося хищения или пожара (простоя оборудования, штрафами за срыв сроков поставки и т.п.);
- размера материальных затрат и рабочего времени, потраченных на расследование происшествий.

Перечисленные виды стоимости образуют так называемую «группу риска». Разница между возможными ущербом и прямыми затратами составляет условную прибыль по данной системе. Величина условной прибыли определяет величину капиталовложений в оборудование объекта комплексом ТСОБ.

Анализ формулы (6.1) показывает, что система тем эффективнее ($Э_{О} > 0$), чем выше условный предотвращенный ею ущерб и чем ниже относительные затраты на ее создание и эксплуатацию, то есть если выполняется соотношение $У_{П} > З/П_{О}$.

Приведем пример использования этого метода. Пусть стоимость СБ составляет 20% от суммы возможных потерь, то есть $С_{О} = 0{,}2П_{О}$, срок службы СБ составляет Т=10 лет, затраты на эксплуатацию СБ в течение периода Т составляют 5% от стоимости системы $С_{Э} = 0{,}05 \times 10С_{О}$. Тогда общие затраты на создание системы будут равны

$$З = С_{О} + С_{Э} = 0{,}2П_{О} + 0{,}05 \times 10С_{О} = (0{,}2 + 0{,}05 \times 10 \times 0{,}2)П_{О} = 0{,}3П_{О}.$$

Таким образом, система будет эффективна, если относительный предотвращенный ущерб $У_{П}$ составит не менее 30% общих возможных потерь от реализации угроз.

Вероятностные методы включают такие параметры как вероятности реализации угроз; обнаружения угроз; ложных тревог; пресечения несанкционированных действий и др. Указанные параметры могут быть получены на основе статистических данных и экспертных оценок.

Дополнительную сложность указанных методов создает то, что практически отсутствует статистический материал по вероятностям реализации угроз, вероятностным характеристикам оборудования

обеспечения безопасности, а экспертные оценки представляются достаточно субъективными.

Комбинированные методы, учитывающие как экономические, так и вероятностные характеристики, позволяют определить максимальный относительный предотвращенный ущерб от реализации всех угроз с учетом случайного характера их появления.

Надежность системы можно рассчитать по формулам, которые позволяют определить эффективность тех или иных методов задержки нарушителя [18, 48].

Указанные критерии могут быть применены как к СБ в целом, так и к отдельным подсистемам, поскольку систему безопасности, как сложную иерархическую систему, можно декомпозировать. Однако, естественно, окончательный и более полный вывод можно сделать только на основе анализа эффективности функционирования всех подсистем не по отдельности, а во взаимодействии.

В последнее время растет интерес к комплексным показателям эффективности работы СОТ, которые позволяют оптимизировать выбор компонентов системы для решения конкретной задачи обеспечения безопасности объекта.

Принято рассматривать два подхода к оценке эффективности, которые используют принципиально разные методы [1, 26, 38]:

1. Метод непосредственного подсчета значения эффективности, если известна аналитическая зависимость (как правило, аналитическая зависимость не известна, поскольку каждый объект уникален).

2. Метод с использованием экспертных оценок (метод может быть эффективен в условиях ограниченности времени на принятие решения по оборудованию комплекса СОТ, кроме того, часть информации о СОТ не поддается количественной оценке).

При этом необходимо определять влияние каждого элемента СБ на реализацию конкретной угрозы (содействие, независимость, конфликт) для получения значений коэффициентов эффективности каждой ПСБ.

Комплексный показатель эффективности технических решений СБ можно оценить функциональной зависимостью:

$$K_{ЭФ} = f(k_1, k_2 \ldots k_n), \qquad (6.2)$$

где k_1, k_2 … k_n – значения частных показателей эффективности, которые характеризуют основные и вспомогательные подсистемы СБ. Перечислим эти подсистемы:

1. Надежность оборудования периметра объекта средствами сигнализации.

2. Инженерная подготовка местности (подступов к объекту, внешней полосы отчуждения, внутренней запретной зоны) и периметра.

3. Характеристики и параметры ССОИУ.
4. Характеристики и параметры СКУД.
5. Характеристики и параметры СОТ.
6. Характеристики системы тревожного освещения (СТО).
7. Характеристики системы оперативной связи (СОС).
8. Системы резервного бесперебойного электроснабжения, климатической и вандалозащищенности (СЭС).
9. Мероприятия по противодействию технической разведке организованных преступных групп, незаконных вооруженных формирований и иностранных спецслужб (ПДТР).

Каждый частный показатель эффективности подсистемы является комплексным, так как включает в себя такие параметры, как вероятности обнаружения и ложной тревоги или наработку на отказ.

Группа экспертов формируется с целью выбора тех или иных технических предложений по оборудованию объекта комплексом ТСОБ или для выработки экспертных оценок эффективности различных систем или оценки их параметров. Методом оценки может быть метод групповой экспертизы, так как групповые оценки позволяют компенсировать смещения оценок отдельных членов экспертной группы.

При отборе экспертов используют специальные анкеты для определения уровня компетентности методом самооценок потенциальных экспертов по пятибалльной системе. После получения индивидуальных самооценок экспертов формируется групповая средняя самооценка экспертной группы в каждой области знаний, необходимой для проведения экспертизы. Численность экспертной группы влияет на точность оценок и может зависеть от сложности и масштабности оцениваемой СБ. Группа экспертов может насчитывать от 3 до 7 специалистов разного профиля.

В анкетах экспертам предлагается выставить оценку в баллах по каждому из частных показателей эффективности. После обработки результатов экспертных оценок получают усредненные частные показатели эффективности комплекса СБ (таблица 6.1).

Таблица 6.1. Значения частных показателей эффективности ПСБ

Периметр	ССОИУ	Инж.оборуд.	СОТ	СКУД	СЭС	СОС	ПДТР	СТО
k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9

Обоснование оптимального выбора СБ выполняется методом обобщенных параметров оптимизации [18, 46]. В методе переходят от абсолютных значений частных показателей, имеющих свой физический смысл и размерность, к безразмерной обобщенной функции желательности Харрингтона (*Desirability Profile*), которая определяется следующим образом:

$$d = 1/(\sqrt[x]{e}), \qquad (6.3)$$

где e – основание натурального логарифма; x – приведенное значение исследуемого показателя. Функция определена в интервале 0…1 и используется в качестве безразмерной шкалы, названной шкалой желательности или предпочтительности, для оценки уровней сравниваемых показателей подсистем (рис.6.2).

Шкала желательности устанавливает соотношение между натуральным значением частного показателя (k_n) и значением функции желательности (d). При этом значение $d = 0$ соответствует абсолютно неприемлемому значению частного показателя, а $d = 1$ – самому лучшему его значению. Степень важности частного показателя можно учесть крутизной функции желательности. Имея оценки уровней частных показателей подсистем СОТ, можно рассчитать обобщенную функцию желательности того или иного технического решения как среднее геометрическое значений обобщенного частного показателя эффективности подсистемы. При этом искомую обобщенную функцию желательности можно рассматривать как комплексный показатель эффективности $K_{ЭФ}$ согласно формуле [46, 47]:

$$K_{ЭФ} = \sqrt[n]{S_1 S_2 ... S_n}, \qquad (6.4)$$

где $S_n = d_n \cdot g_n$ – значение обобщенного частного показателя эффективности подсистемы с учетом его значимости; g_n – коэффициент значимости подсистемы (рис.6.3).

Данная методика позволяет производить сравнительный анализ технических рекомендаций и предложений по оборудованию СОТ объекта методом экспертных оценок. Ее можно рекомендовать для использования на этапе проведения конкурса по оборудованию объекта комплексом ТСО при наличии нескольких участников.

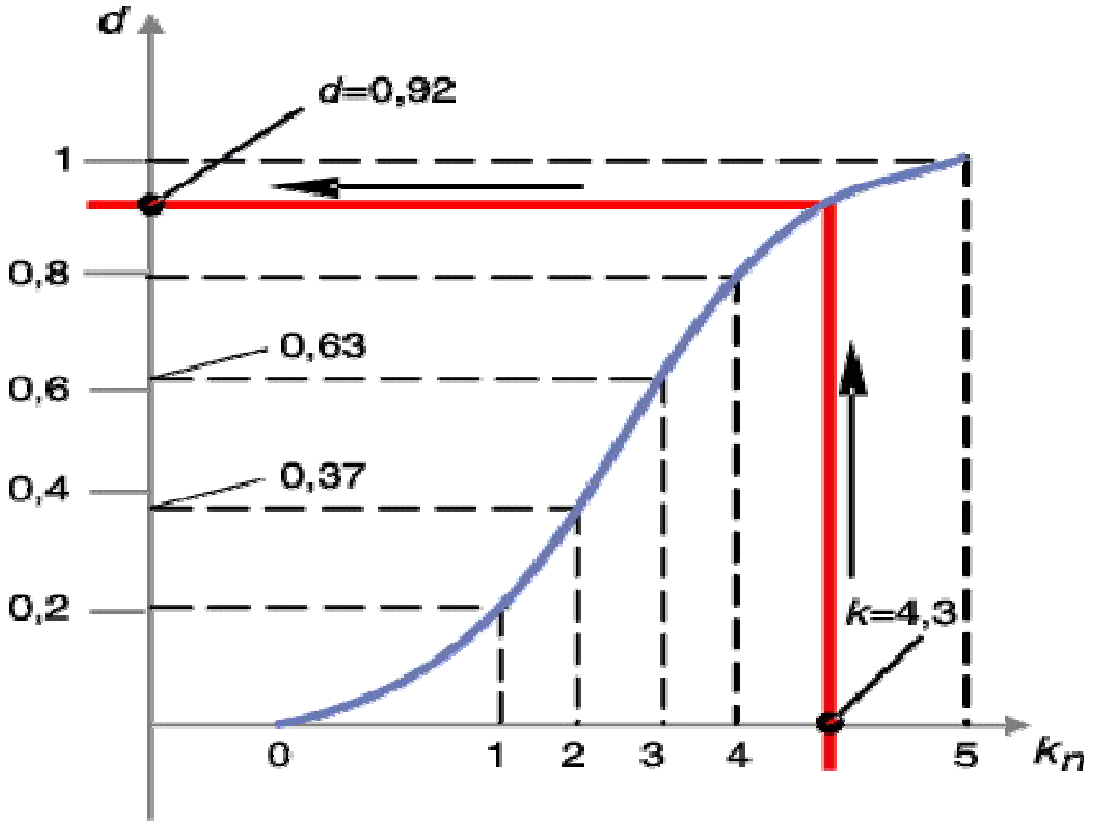

Рисунок 6.2 – Значения обобщенной функции желательности

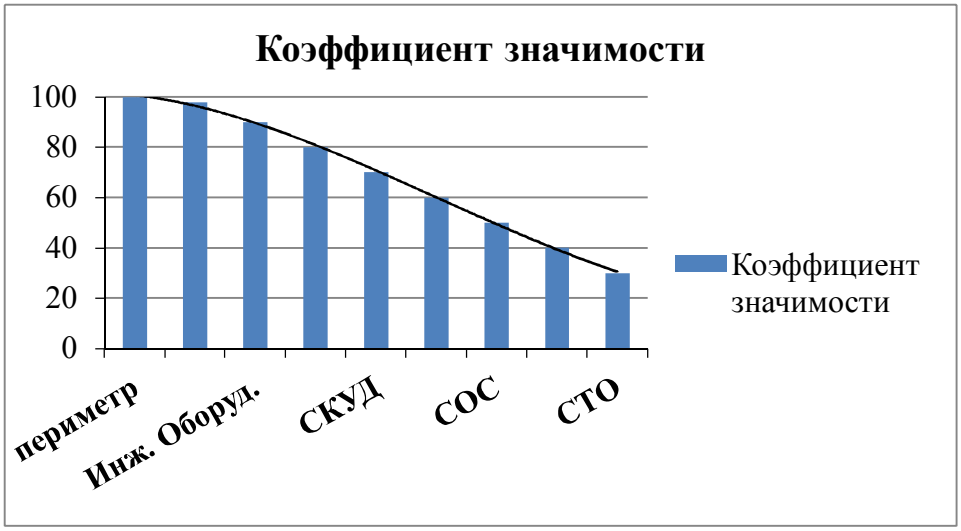

Рисунок 6.3 Значения коэффициентов значимости подсистемы

Рассмотренные выше методы и выражения хоть и являются достаточно общими, могут служить основой для дальнейшей детализации и применения для оценок эффективности СБ. Таким образом, оценка эффективности СБ является сложной задачей, требующей тщательного отбора и учета различных факторов, влияющих на работу СБ.

ЗАКЛЮЧЕНИЕ

Вопросы обеспечения эффективной защиты объектов, рассмотренные в данном пособии, способствуют формированию базовой (основополагающей) теоретической и практической подготовки в области комплексных систем безопасности. Изучение основных терминов, определений и принципов организации интегрированных комплексных систем безопасности позволяет решать следующие задачи проектирования и анализа функционирования комплексных систем безопасности:

- выбор варианта охраны объекта с использованием комплекса технических средств обеспечения безопасности в соответствии с требованиями к технической укрепленности объекта;
- выполнение основных этапов проектирования комплексных систем безопасности с использованием основных принципов разработанной концепции безопасности;
- разработка структурной схемы интегрированной комплексной системы безопасности на основе данных о входящих в нее подсистемах контроля доступа, охранно-пожарной сигнализации и телевизионной системы безопасности;
- синтез отдельных компонентов комплексных систем безопасности на базе готовых унифицированных функциональных узлов, расчет их основных параметров и характеристик;
- выполнение оптимизации структуры комплексной системы безопасности с использованием методов оценки эффективности ее функционирования.

Выполнение указанных задач развивает способности собирать, обрабатывать, анализировать и систематизировать научно-техническую информацию по теме исследования КСБ, выбирать перспективные методы решения профессиональных задач на основе современного развития оптико-электронных и телевизионных систем безопасности.

Коллективное решение задач проектирования оптико-электронных приборов и систем безопасности предполагает активное приобретение навыков грамотно формулировать основные требования к параметрам элементов оптико-электронных систем безопасности, к их сборке, юстировке, контролю и испытанию, а также к системе безопасности в целом на основе анализа требований заказчика и обследования объекта.

СПИСОК ЛИТЕРАТУРЫ

1. Волхонский В.В. Системы охранной сигнализации: 2-е изд., доп. И перераб.: СПб.: Экополис и культура, 2005. – 204 с.: ил.
2. Волковицкий В.Д., Волхонский В.В. Цифровые системы ТВ-наблюдения // БДИ. Безопасность, достоверность, информация. СПб., 2009. № 5. С. 38-47.
3. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия - Телеком, 2010. – 272 с.: ил.
4. Гедзберг Ю.М. Охранное телевидение. – М.: Горячая линия – Телеком, 2005. – 312 с.: ил.
5. ГОСТ 26342-84 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры. – Москва: Стандартинформ, 1986.
6. ГОСТ Р 50725-94 Соединительные линии в каналах изображения. - Москва: Стандартинформ, 1995.
7. ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию (с Изменением N 1). - Москва: Стандартинформ, 1996.
8. ГОСТ 14254-96 (МЭК 529-89) Степени защиты, обеспечиваемые оболочками (код IP). – Москва: Стандартинформ, 1997.
9. ГОСТ Р 51186-98 Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний. - М.: МВД РФ, НИЦ «Охрана» ГУВО, 1998.
10. ГОСТ Р 52435-2005 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний.- М.: МВД РФ, НИЦ «Охрана» ГУВО, 2006.
11. ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения. – М.: Стандартинформ, 2006.
12. ГОСТ Р 51558-2008 Системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. – М.: Стандартинформ, 2009.
13. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – М.: Стандартинформ, 2008.
14. ГОСТ Р 53195.1-2008 статья 3.11 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1.Основные положения. - Москва: Стандартинформ, 2009.

15. ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования. – Москва: Стандартинформ, 2010.

16. ГОСТ Р 53325 — 2009 Техника пожарная. Технические средства пожарной автоматики. Общие технические требования. Методы испытаний. – Москва: Стандартинформ, 2009.

17. Дамьяновски Владо, CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии/Пер. с англ. - М.: ООО «Ай-Эс-Эс Пресс», 2006, — 480 с: ил.

18. Двинских В.И. Анализ уязвимости системы охраны. Оценки показателей уязвимости. Официальный сайт охранно-информационного агентства Каскад-Сервис, г. Харьков. URL: http://www.tehbezpeka.com.ua/papers/papers103.php

19. Единые технические требования к объектовым подсистемам технических средств охраны (ТСО), предназначенным для применения в подразделениях вневедомственной охраны, Москва 2008 г. Официальный сайт ФКУ НИЦ «Охрана» МВД России. URL: http://nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html

20. Единые технические требования к системам централизованного наблюдения, предназначенным для применения в подразделениях вневедомственной охраны. Москва 2010 г. Официальный сайт ФКУ НИЦ «Охрана» МВД России. URL: http://nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html

21. Измайлов А.В. Методы системного проектирования комплексов технических средств физической защиты российских ядерных объектов // Российско-американский семинар по физической защите ядерных материалов и установок, ГП СНПО "Элерон", М., Россия. 1995.

22. Крахмалев А.К. Новый стандарт на УПУ СКУД // SS. Системы безопасности. СПб., 2011, апрель-май. С. 120-122.

23. Крахмалев А.К. Перспективы развития ИСБ. Платформы интеграции. // SS. Системы безопасности. СПб., 2010, апрель-май. С.146-148.

24. Кругль Герман, Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового CCTV, 2-е изд.: Пер. с англ. - М.: Секьюрити Фокус (Security Focus), 2010. – 640 с.: ил.

25. Лукьяница А.А., Шишкин А.Г. Цифровая обработка видеоизображений – М.: «Ай-Эс-Эс Пресс», 2009.

26. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие для вузов/ Р.Г. Магауенов. – 2-е изд., перераб. и доп. – Горячая линия – Телеком, 2008. – 496 с.

27. Омельянчук А.М. Анализ угроз при проектировании систем технических средств охраны. http://www.sigma-is.ru/articles/analiz-ugroz-pri-proektirovanii-sistem-t.html

28. Омельянчук А.М. Формирование системы комплексной безопасности. Часть 1. Предпроектное обследование объектов и разработка технического задания. // SS. Системы безопасности. СПб., 2009, февраль-март. С. 100-101.

29. Омельянчук А.М. Формирование системы комплексной безопасности. Часть 2. Подготовка техзадания и проектирование. // SS. Системы безопасности. СПб., 2009, апрель-май. С. 114-117.

30. П 78.36.001 – 2004 Перечень технических средств, разрешенных к применению во вневедомственной охране в 2004 году. – Москва: 2004.

31. ПР-1649 от 28 сентября 2006 г. Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов. - М.: Администрация Президента РФ - С. 9.

32. Р 78.36.007-99 Рекомендации. Выбор и применение средств охранно-пожарной сигнализации и средств технической укрепленности для оборудования объектов. - М.: МВД РФ, НИЦ «Охрана» ГУВО, 1999.

33. Р 78.36.005-99 Рекомендации. Выбор и применение систем контроля и управления доступом. - М.: МВД РФ, НИЦ «Охрана» ГУВО. 31 марта 1998.

34. Р 78.36.011-2000 Рекомендации. Организация работы пунктов централизованной охраны. – М.: МВД РФ, НИЦ "Охрана" ГУВО МВД России, 2000.

35. РД 78.145-93. Руководящий документ. Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ. – М.: МВД РФ, НИЦ «Охрана» ГУВО. 12 января 1993.

36. РД 78.36.003-2002. Руководящий документ. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств. – М.: МВД РФ, НИЦ «Охрана» ГУВО. 06 ноября 2002.

37. РМ 78.36.001-99 Справочник инженерно- технических работников и электромонтеров технических средств охранно-пожарной сигнализации. - М.: МВД РФ, НИЦ "Охрана" ВНИИПО МВД России, 1999.

38. Румянцев М.Н. Эффективная СКУД на крупном НПЗ. Опыт завода «Славнефть-ЯНОС» (Ярославль). // SS. Системы безопасности. СПб., 2011, апрель-май. С. 128-130.

39. Синилов В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации : учебник для нач. проф. образования / В. Г. Синилов. — 5-е изд., перераб. и доп. — М. : Издательский центр «Академия», 2010. — 512 с.

40. Федеральный закон «Технический регламент «О технических средствах обеспечения противокриминальной защиты объектов и

имущества». Информационно-справочная система «Техэксперт». URL: http://docs.cntd.ru/document/1200057776

41. ТТ 78.36.001-99. Типовые требования по технической укрепленности и оборудованию сигнализацией предприятий торговли. - М.: МВД РФ, НИЦ «Охрана» ГУВО. 1999.

42. Федеральный закон Российской Федерации от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Официальный сайт ФКУ НИЦ «Охрана» МВД России. URL: http://nicohrana.ru/pravovaya-informaciya.html

43. Федеральный закон Российской Федерации от 22.07.2008 г. №123-ФЗ «Технический регламент о требованиях пожарной безопасности». Официальный сайт ФКУ НИЦ «Охрана» МВД России. URL: http://nicohrana.ru/pravovaya-informaciya.html

44. Федеральный закон Российской Федерации от 30 декабря 2009 г. №384-ФЗ «Технический регламент о безопасности зданий и сооружений». Официальный сайт ФКУ НИЦ «Охрана» МВД России. URL: http://nicohrana.ru/pravovaya-informaciya.html

45. Хофман Кристоф. Интеллектуальный видеоанализ – идеальный помощник оператора. // SS. Системы безопасности. CCTV. СПб., 2011. С.10.

46. Информационный портал журнала «БДИ». URL: http://bdi.spb.ru/. Архив журнала «БДИ» http://mx1.algoritm.org/61/61_Perimetr.htm

47. Информационный портал центра информационных технологий «Орбита-Союз». URL: http://os-info.ru/oxrannaya-deyatelnost/texnologiya-obespecheniya-bezopasnosti-obekta.html

48. Информационный портал объединения охранных предприятий и агентств безопасности Оскордъ. URL: http://www.oskord.ru/ru/News/Message/45730KI.html

49. Электронно-библиотечная система. Издательство «Лань» [Электронный ресурс] Мирошников М.М. Теоретические основы оптико-электронных приборов. — Лань, 2010. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=171&pl1_id=644

50. Электронно-библиотечная система. Издательство «ЭНАС» [Электронный ресурс] Петров С.В. Обеспечение безопасности организаций и производственных объектов: Практическое пособие для руководителей и работников предприятий и организаций. – ЭНАС, 2007. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1919

51. Электронно-библиотечная система. Издательство «ЭНАС» [Электронный ресурс] Петров С.В. Обеспечение безопасности образовательного учреждения: Практическое пособие для руководителей и работников образовательных учреждений. – ЭНАС, 2006. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1924

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА ОПТИКО-ЭЛЕКТРОННЫХ ПРИБОРОВ И СИСТЕМ И ЕЕ НАУЧНО-ПЕДАГОГИЧЕСКАЯ ШКОЛА

Кафедра создавалась в 1937-38 годах и существовала под следующими названиями:

– с 1938 по 1958 год - кафедра военных оптических приборов;

– с 1958 по 1967 год - кафедра специальных оптических приборов;

– с 1967 по 1992 год - кафедра оптико-электронных приборов;

– с 1992 года - кафедра оптико-электронных приборов и систем.

Кафедру возглавляли:

– с 1938 по 1942 год - профессор К.Е. Солодилов;

– с 1942 по 1945 год - профессор А.Н. Захарьевский (по совместительству);

– с 1945 по 1946 год - профессор М.А. Резунов (по совместительству);

– с 1947 по 1972 год - профессор С.Т. Цуккерман;

– с 1972 по 1992 год - заслуженный деятель науки и техники РСФСР, профессор Л.Ф. Порфирьев;

– с 1992 по 2007 год - заслуженный деятель науки РФ, профессор Э.Д. Панков.

– с 2007 года по настоящее время - почетный работник высшего профессионального образования, профессор В.В. Коротаев.

История кафедры началась в 1937-38 годах с организации в Ленинградском институте точной механики и оптики (ЛИТМО) кафедры военных оптических приборов. Первым заведующим кафедрой был К.Е. Солодилов, до этого возглавлявший Центральное конструкторское бюро (ЦКБ) Всесоюзного объединения оптико-механической

промышленности (ВООМП). Преподавателями кафедры стали сотрудники этого ЦКБ - М.А. Резунов, М.Я. Кругер, С.Т. Цуккерман, В.А. Егоров, Б.М. Кулежнов.

В годы Великой Отечественной войны кафедра была эвакуирована в Черепаново, где обязанности заведующего кафедрой выполнял профессор А.И. Захарьевский. Преподавателями кафедры по состоянию на 01.04.1945 г были профессор Чулановский, доцент Кругер, ст. преподаватель Гриневич, ассистенты Дедюлин и Погарев. После возвращения в Ленинград кафедрой в 1945-46 годах по совместительству заведовал начальник конструкторского бюро (КБ) Государственного оптического института им. С.И. Вавилова (ГОИ) М.А. Резунов.

В начале 1947 года кафедру возглавил профессор С.Т. Цуккерман, который руководил ею до 1972 года. В 1958 году кафедра была реорганизована в кафедру специальных оптических приборов, а в 1967 году в кафедру оптико-электронных приборов (ОЭП).

Создание С.Т. Цуккерманом в предвоенные годы книги «Точные механизмы» (М.: Оборонгиз, 1941) является значительным вкладом в развитие отечественного точного приборостроения. С.Т. Цуккерман является автором более 120 научных работ и более 50 изобретений. В предвоенные, военные и послевоенные годы С.Т. Цуккерман работал над созданием прицельных устройств для зенитной и авиационной артиллерии. Он был одним из создателей серийного авиационного гироскопического прицела АСП с автоматической выработкой поправки на упреждение, который устанавливался на истребителях МиГ, а также механического ракурсного прицела для мелкокалиберной зенитной артиллерии, широко применяемого во время войны во Вьетнаме.

В 1958 г. при кафедре была организована отраслевая лаборатория «Специальные оптические приборы» с достаточно сильной группой конструкторов-разработчиков. ……

С.Т. Цуккерман и старший научный сотрудник А.С. Гридин руководили разработкой приборов управления по лучу (ПУЛ), предназначенных для управления движением различных подвижных объектов по прямой линии или по программе.

В начале 60-х годов старший научный сотрудник Г.Г. Ишанин занимался разработкой фотометрической аппаратуры, предназначенной для паспортизации оптико-электронных приборов и систем различного назначения.

Значительное влияние на содержание подготовки специалистов и научных исследований оказало привлечение к работе на кафедре выдающегося специалиста в области оптико-электронного приборостроения, члена-корреспондента Российской академии наук (РАН), Героя Социалистического Труда, лауреата Ленинской премии профессора М.М. Мирошникова, который, работая на кафедре ОЭП с 1969 года по 1976

год в должности профессора по совместительству, поставил и читал курс «Теория оптико-электронных приборов».

С 1972 года по 1992 год кафедрой ОЭП заведовал заслуженный деятель науки и техники РСФСР, профессор Л.Ф. Порфирьев, известный специалист в области автоматических ОЭПиС в комплексах навигации и управления авиационной и космической техникой. Соответственно тематика выполнения научно-исследовательских работ на кафедре приобрела новые направления, существенно увеличилось число тем, носящих поисковый фундаментальный характер. Были разработаны новый учебный план и программы учебных дисциплин.

Л.Ф. Порфирьев является автором 19 учебников, учебных пособий и монографий, среди которых можно выделить такие как «Теория оптико-электронных приборов и систем» (Л.: Машиностроение, 1980), «Основы теории преобразования сигналов в оптико-электронных системах» (Л.: Машиностроение, 1989). Результаты его работ можно оценить как значительный вклад в разработку общей теории оптико-электронных систем.

Л.Ф. Порфирьев как руководитель проводил достаточно жесткую кадровую политику, при которой на кафедре оставались работать только те сотрудники, которые отличались преданностью делу. При этом он оказывал всемерную поддержку сотрудникам кафедры по разработке ими различных направлений теории и практики оптико-электронного приборостроения. По результатам научно-исследовательских работ в этот период защитили диссертации на соискание ученой степени доктора технических наук Г.Н. Грязин (1983 г.), Е.Г. Лебедько (1985 г.), Э.Д. Панков (1986 г.), Г.Г. Ишанин (1988 г.), защищено много диссертаций на соискание ученой степени кандидата технических наук.

В этот период под руководством Э.Д. Панкова начали проводиться исследования по разработке новых оптико-электронных систем измерения взаимного положения разнесенных в пространстве объектов.

Г.Н. Грязин, перешедший на кафедру с радиотехнического факультета в конце 60-х годов, продолжил свои работы в области прикладного телевидения, в частности, по разработке систем наблюдения за быстродвижущимися объектами и быстропротекающими процессами.

С 1975 года заведующим отраслевой лабораторией стал старший научный сотрудник А.Н. Тимофеев, который продолжил исследования по разработке методов и средств контроля пространственного положения объектов с помощью ОЭП с оптической равносигнальной зоной для машиностроения, энергетики, строительства, судостроения и железнодорожного транспорта.

С 1975 года, после увольнения в запас, из Ленинградской военной инженерной краснознаменной академии (ЛВИКА) им. А.Ф. Можайского на кафедру пришел работать в должности профессора С.П. Авдеев, известный

специалист в области ОЭПиС космических аппаратов. Он поставил курсы и читал лекции по учебным дисциплинам «Оптико-электронные приборы», «Оптико-электронные приборы систем управления», «Оптико-электронные приборы для научных исследований».

Существенное влияние на содержание подготовки специалистов и научных исследований оказало привлечение к работе на кафедре лауреата Ленинской и Государственной премий профессора Б.А. Ермакова, известного специалиста в области физической оптики и оптико-электронного приборостроения. Б.А. Ермаков работал на кафедре ОЭП с 1979 года по 1992 год в должности профессора по совместительству и поставил курс «Оптико-электронные приборы с лазерами».

В 70-80 годах под руководством доцента Е.Г. Лебедько проводились исследования законов отражения лазерного излучения от нестационарных поверхностей и протяженных объектов, исследования в области теории идентификации объектов по их излучению в сложной фоновой ситуации. Создан комплекс для лазерной локации крупногабаритных морских объектов сложной конфигурации и водной поверхности. В этих работах принимали участие доценты О.П. Тимофеев и С.Б. Лукин.

В 70-90 годах под руководством Л.Ф. Порфирьева был разработан ряд астродатчиков, систем астроориентации и космической навигации (В.И. Калинчук, А.Л. Андреев, С.Н. Ярышев).

С 1992 г. заведующим кафедрой является заслуженный деятель науки Российской Федерации, профессор Э.Д. Панков. В 1992 году кафедра была переименована в кафедру оптико-электронных приборов и систем (ОЭПиС).

Под руководством Э.Д. Панкова в 70-90-х годах были проведены разработки ряда оптико-электронных приборов и систем специального и гражданского применения, нашедших практическое внедрение и способствующих научно-техническому прогрессу и укреплению обороноспособности нашей страны.

В частности, исследования и разработки в области линейных и угловых измерений позволили приступить к решению общей проблемы согласования отсчетных баз на нестационарно деформируемых объектах с помощью оптико-электронных систем.

В рамках указанной проблемы доцентом И.А. Коняхиным проводились исследования, результаты которых можно классифицировать как разработку теории построения автоколлимационных систем с компонентами нарушенной типовой конфигурации.

В то же время доцентом В.В. Коротаевым разработан ряд поляризационных приборов и измерительных установок. Теоретическим результатом работ явилась разработка методологии анализа поляризационных свойств оптических систем с изменяющейся ориентацией элементов. По результатам указанных работ В.В. Коротаев (в 1997 г.) и

И.А. Коняхин (в 1998г.) защитили диссертации на соискание ученой степени доктора технических наук.

Применение многоэлементных приемников в системах пеленгации дало толчок развитию телевизионных систем технического зрения, измерительных телевизионных систем и систем обработки изображений. Результаты этих исследований были использованы доцентом А.Л. Андреевым при постановке учебных курсов «Оптико-электронные системы с ЭВМ», «Специализированные аппаратные и программные средства ОЭП», «Автоматизированные телевизионные вычислительные комплексы», а также доцентом С.Н. Ярышевым при постановке им в 1993 году учебной дисциплины «Видеотехника».

Указанные курсы обеспечиваются лабораторным практикумом на базе рабочих мест, оснащенных персональными компьютерами, объединенными в локальную сеть. Рабочие места оснащены аппаратными и программными средствами цифровой видеозаписи и обработки изображений. В этот период Г.Н. Грязиным были подготовлены дисциплинам: «Телевизионные системы», «Прикладное телевидение и телевизионно-вычислительные комплексы» (совместно с А.Л. Андреевым).

На основе обобщения методик расчета оптико-электронных систем различного назначения и принципа действия в 1981 году были развернуты работы по созданию элементов систем автоматизированного проектирования ОЭП. За период с 1981 по 1987 год под руководством И.А. Коняхина были разработаны оригинальные пакеты прикладных программ расчета параметров систем измерения пространственного положения объектов.

Развитие компьютерной техники и программного обеспечения общего назначения позволило создать проблемно-ориентированное программное обеспечение поддержки проектирования ОЭП на системотехническом уровне.

По результатам научных работ сотрудниками кафедры ОЭПиС выпущено в свет 15 монографий, 11 учебников и учебных пособий. На кафедре подготовлено 14 докторов наук, а также более 110 кандидатов наук.

На разработки кафедры получены авторские свидетельства СССР и патенты Российской Федерации на более чем 200 изобретений. Наибольший вклад в изобретательскую деятельность внес Э.Д. Панков - автор 123 изобретений, из которых 33 внедрены в промышленности.

При заявлении научно-педагогической школы «Оптико-электронное приборостроение» в 2009 году были сформулированы следующие основные научно-технические результаты, достигнутые в период с 1938 по 2009 годы:

– разработаны принципы построения военных оптико-механических приборов;

– разработаны принципы построения точных механизмов;

– разработаны принципы построения оптико-электронных приборов с оптической равносигнальной зоной;

– систематизированы теоретические основы и принципы построения оптико-электронных приборов;

– разработаны методы описания импульсных сигналов, идентификации и классификации объектов в системах нестационарной лазерной локации;

– разработаны теория, принципы построения и методы расчета импульсных телевизионных систем наблюдения быстродвижущихся объектов;

– обнаружен термоупругий эффект в кристаллическом кварце и создан новый тип приемников оптического излучения;

– разработана теория построения автоколлимационных систем с компонентами нарушенной типовой конфигурации;

– разработана методология анализа поляризационных свойств оптических систем с изменяющейся ориентацией элементов;

– систематизированы теоретические основы и принципы построения измерительных систем на основе матричных фотопреобразователей;

– разработаны основы построения ОЭС согласования отсчетных баз на нестационарно деформируемых объектах.

Основоположники научной школы:

- Солодилов Константин Евгеньевич, заведующий кафедрой с 1938 г. по 1942 г., профессор;
- Цуккерман Семен Тобиасович, заведующий кафедрой с 1947 г. по 1972 г., профессор;
- Мирошников Михаил Михайлович, директор ГОИ, д.т.н., профессор,

профессор кафедры ОЭП с 1967 г. по 1978 г.; член-корреспондент Российской Академии наук, Герой Социалистического Труда, лауреат Ленинской премии.

- Порфирьев Леонид Федорович, заведующий кафедрой с 1972 г. по 1992 г., д.т.н., профессор, Заслуженный деятель науки и техники РСФСР.
- С 2007 г. заведующим кафедрой является почетный работник высшего профессионального образования Российской Федерации, профессор В.В. Коротаев.

На кафедре была открыта подготовка по новой специализации инженеров «Оптико-электронные приборы и системы обработки видеоинформации» и новая магистерская программа «Оптико-электронные методы и средства обработки видеоинформации».

В 2007 году был создан научно-образовательный центр оптико-электронного приборостроения (НОЦ ОЭП).

Научно-образовательный центр оптико-электронного приборостроения выполняет научно-исследовательские и опытно-конструкторские работы по созданию видеоинформационных и информационно-измерительных приборов различного назначения, высокоточных приборов для измерения линейных, угловых и других физических величин в промышленности, энергетике, на транспорте, а также систем технического зрения и обработки видеоинформации. К выполнению научно-исследовательских и опытно-конструкторских работ широко привлекаются студенты, аспиранты, молодые специалисты, молодые кандидаты наук. Научно-образовательный центр является активным участником Федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009-2013 годы.

Направления научных исследований кафедры ОЭПиС в 2007-2012 годах.

Развитие теоретических основ и принципов построения оптико-электронных приборов и систем, в том числе:

- видеоинформационных измерительных систем;
- видеоинформационных систем наблюдения;
- видеоинформационных импульсных систем наблюдения быстродвижущихся объектов;
- комплексированных телевизионно-тепловизионных систем наблюдения,
- ОЭПиС обеспечения техносферной безопасности;
- ОЭПиС согласования отсчетных баз на нестационарно деформируемых объектах;
- автоколлимационных систем с компонентами нарушенной типовой конфигурации;
- ОЭПиС цветового и спектрального анализа объектов;
- фотометрических систем аттестации ОЭПиС, источников и приемников оптического излучения;
- систем лазерной локации с нестационарным облучением;
- ОЭС сепарации полезных ископаемых.

По результатам исследований в этот период на кафедре были защищены 14 диссертаций на соискание ученой степени кандидата технических наук.

Идет активное пополнение преподавательского состава молодыми кандидатами наук. В настоящее время на кафедре работает 7 кандидатов наук в возрасте до 35 лет.

Мы занимаемся разработкой оптико-электронных приборов и систем в целом:

– системотехническое проектирование,

– разработка (выбор) оптической системы,

– разработка конструкции,

– разработка (выбор) электроники и средств обработки информации,

– разработка программного обеспечения,

– сборка, юстировка, настройка и испытания.

Мы учим тому, что сами умеем делать!

По итогам конкурсов ведущих научно-педагогических коллективов СПб НИУ ИТМО 2007-2011 годов кафедра занимала призовые места.

С 2011 года подготовка бакалавров, магистров и специалистов на кафедре ОЭПиС осуществляется по Федеральным государственным образовательным стандартам третьего поколения (ФГОС).

Подготовка бакалавров по направлению:

200400 «Оптотехника» (профиль - Оптико-электронные приборы и системы). Срок обучения - 4 года

Подготовка магистров по направлению:

200400 Оптотехника.

Магистерские программы:

– Оптико-электронные методы и средства обработки видеоинформации

– Оптико-электронные приборы и системы безопасности

Срок обучения – 2 года.

Подготовка инженеров по специальности:

200401 -Электронные и оптико-электронные приборы и системы специального назначения.

Специализация:

– Оптико-электронные информационно-измерительные приборы и системы. Срок обучения – 5,5 лет.

Подробная информация о кафедре ОЭПиС имеется на сайте кафедры: http://oeps.ifmo.ru/

Виктория Александровна Рыжова

ПРОЕКТИРОВАНИЕ И ИССЛЕДОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Учебное пособие

В авторской редакции В.А. Рыжова
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж 100 экз
Отпечатано на ризографе

Редакционно-издательский отдел
Санкт-Петербургского национального
исследовательского университета
информационных технологий, механики
и оптики
197101, Санкт-Петербург, Кронверкский пр., 49