Содержание

1. Средства и системы контроля доступа на объекты охраны

1.1 Технические средства охраны

1.2 Общая информация по системам контроля доступа

1.3 Контроль и учет материальных ценностей в системе охраны и физической защиты предприятия

Список литературы

1. Средства и системы контроля доступа на объекты охраны

1.1 Технические средства охраны

Автоматическая система охранной сигнализация широко используется при оснащении различных типов помещений (жилые, производственные, складские, учреждения и т.п.) Цель охранной сигнализации – абсолютное пресечение любой возможности незаконного проникновения в охраняемое помещение или на охраняемую территорию. Основой охранной системы служат контрольные датчики, которые передают информацию на центральный контрольный пункт. При этом охранная сигнализация может быть не только автономной, но и функционировать в комплексе с другими системами безопасности охраняемого объекта. Система охранной сигнализации позволяет контролировать охраняемое помещение или территорию 24 часа в сутки.

Система пожарной сигнализации - это сложный комплекс технических средств, который реагирует на задымление, изменение температуры воздуха при помощи специальных датчиков. Датчики посылают сигнал тревоги на приёмно-контрольный прибор, после чего сигнал моментально передаётся на пульт пожарной охраны. Система автоматической пожарной сигнализации бывает разной комплектации. Это зависит от типа помещения.

Системы видеонаблюдения позволяют осуществлять видеоконтроль за ситуацией на объекте. Системы видеонаблюдения дают уникальную возможность видеозаписи происходящих событий, контроля за ними и записи их на цифровые или магнитные носители информации[[1]](#footnote-1).

Существуют стандартные системы видеонаблюдения и компьютерные системы видеонаблюдения. Последние считаются наиболее актуальными и отличаются большой функциональностью в совокупности с простотой использования. В зависимости от типа объекта комплектация системы видеонаблюдения варьируется. Например, при установке системы видеонаблюдения могут использоваться различные виды видеокамер.

Система контроля доступа предназначена для отслеживания прохода людей в определенное помещение и для осуществления сбора и записи информации о действиях сотрудников объекта и его посетителей. Система контроля доступа постоянно обеспечивает контроль за порядком на объекте. Система контроля доступа - это совокупность программно-технических средств и чётко сформированной системы управления движением персонала и временем его нахождения на объекте. Основными местами для установки системы контроля доступа на предприятиях являются проходные, офисы, помещения особого назначения и пункты въезда и выезда автотранспорта. Система контроля доступа может быть автономной или же одной из составляющих интегрированной системы безопасности здания.

1.2 Общая информация по системам контроля доступа

Системы контроля доступа (СКД) используют специальное оборудование, обеспечивающее определение полномочий доступа людей и автотранспорта на охраняемую территорию. Они также обеспечивают функции контроля перемещения людей и автотранспорта по территориям организации. Информация о прохождении объекта через пункты контроля доступа записывается в базу данных и в дальнейшем может анализироваться.

Системы контроля доступа применяются в офисных зданиях, бизнес-центрах, предприятиях оптовой торговли, супермаркетах и т.п.

В простейшем случае для идентификации личности могут использоваться два считывателя – на вход и на выход. При предъявлении посетителем карточки на мониторе дежурного появляются фотография и краткие сведения о владельце карточки. Идентификацию личности и определение прав прохода осуществляет дежурный. В более сложных системах используются турникеты. Проход через турникеты в обоих направлениях возможен при предъявлении карточки. Над турникетами могут быть установлены камеры системы видеонаблюдения[[2]](#footnote-2).

В системах контроля доступа может также применяться специальное оборудование для предотвращения проноса или провоза запрещенных предметов, в том числе оружия, взрывчатых веществ, делящихся материалов и т.п.

Системы контроля доступа могут быть тесно интегрированы с системой охранно-пожарной сигнализации, видеонаблюдением, платежной системой, с инженерными системами здания, с информационными системами организации.

Для идентификации могут использоваться биометрические технологии, в том числе устройства идентификации по форме кисти руки, по отпечатку пальца, по радужной оболочке глаза.

Оборудование контроля доступа может устанавливаться на двери всех помещений служебной зоны. Для повышения уровня безопасности на двери, отделяющие клиентскую зону от служебной, могут устанавливаться считыватели двойной технологии – Ргох или Smart-карта плюс отпечаток пальца.

Системы контроля доступа обычно тесно интегрируются с системой охранной сигнализации. Нередко системы контроля доступа и охранной сигнализации разных производителей интегрируются на уровне программного обеспечения, что дает возможность подключения уже установленного на объекте оборудования к единому управляющему центру.

Системы контроля доступа широко используются для управления движением транспортных средств по территориям подземных автостоянок. Идентификация производится постановкой автомобиля на индукционную петлю и предъявлением водителем Ргох-карты на считывателе. С учетом приоритета данного пользователя с помощью светофоров, шлагбаумов и ворот организуется трасса для проезда автомобиля. Для предотвращения прорывов в здание могут использоваться гидравлические блокираторы подъемного типа.

На базе систем контроля доступа могут быть построены интегрированные охранные системы, объединяющие в единый комплекс подсистемы безопасности различного назначения. При этом осуществляется управление всеми подсистемами как единой многофункциональной охранной системой, в том числе обеспечивается ведение единого протокола событий всех подсистем, обработка событий всех подсистем, программирование реакций на события, определение сложных алгоритмов взаимодействия подсистем. Такая система должна функционировать в чрезвычайных ситуациях, в том числе в условиях выхода из строя и поражения ее отдельных компонентов.

1.3 Контроль и учет материальных ценностей в системе охраны и физической защиты предприятия

Система физической защиты представляет собой совокупность технических средств и сил охраны, реализующих выполнение мероприятий (рис.1), направленных на:

субъект угрозы с целью его физической нейтрализации;

объект охраны с целью повышения его резистивных свойств противостоять угрожающим воздействиям;

физическую среду, разделяющую субъект угрозы и объект охраны с целью замедления (задержки) и ослабления угрожающих воздействий.

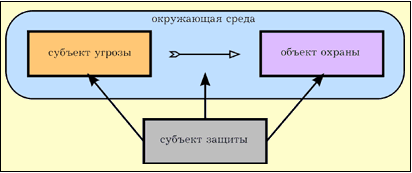


Рис. 1. Структура взаимодействий в системе физической защиты объекта

Главной целью физической защиты является решение задачи нейтрализации человека (нарушителя), инициирующего физические угрозы. Система физической защиты предстает как автоматизированная человеко-машинная система управления (рис.2) качеством «физическая безопасность объекта охраны». Создание нормативной модели системы управления предполагает разработку нормативных моделей составляющих ее элементов, в том числе: модели объекта охраны, модели субъекта угрозы (нарушителя), модели физической среды и средств физической защиты, модели охранного мониторинга, модели системы принятия управляющих решений, оперативных моделей взаимодействия технических средств защиты и персонала охраны.

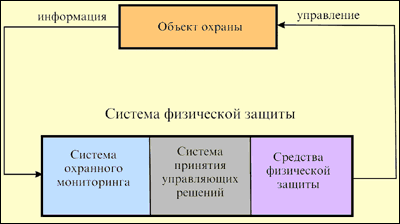


Рис. 2. Система управления качеством «физическая безопасность объекта охраны»

Системы управления физической защитой можно разделить на две основные группы по способам реализации функций охранного мониторинга по обнаружению «внешнего» и «внутреннего» нарушителей[[3]](#footnote-3):

Непосредственное обнаружение внешнего нарушителя по характеру возмущений физической среды, вызываемых его несанкционированным вторжением в контролируемое (охраняемое) пространство, в котором он ранее отсутствовал.

Опосредованное обнаружение внутреннего нарушителя путем оценки результатов его несанкционированного вмешательства в производственные, технологические, снабженческие и информационные технологические процессы предприятия при санкционированном присутствии нарушителя в контролируемом пространстве.

В первом случае процесс физической защиты выступает как процесс обеспечения охранно-территориальной безопасности объекта или как обнаружения и нейтрализации нарушителя в процессе контроля и управления персональным доступом на различные участки территории ОО, осуществляемый известными «системами контроля и управления доступом» (СКУД). Во втором случае — как нейтрализация нарушителя, обнаруженного в процессе контроля и учета движения «материальных ценностей» (МЦ) предприятия (документация, денежная масса, продукция, комплектующие изделия, носители информации, материалы, сырье, полуфабрикаты и т.д.), реализуемого «системами контроля и учета материальных ценностей» (СКУМЦ). В реальных условиях системы СКУД и СКУМЦ дополняют друг друга, решая общую задачу физической нейтрализации противоправных действий внутренних и внешних нарушителей. Интеграция СКУМЦ в системы физической защиты, построенные на базе СКУД, представляет важнейшую проблему дальнейшего развития систем безопасности объектов промышленно-коммерческого назначения (ПКО).

Выбор структуры СКУМЦ предполагает необходимость уточнения категорийности предприятий на основе уровней значимости движущихся через предприятие МЦ. С этих позиций очевидно наличие, по крайней мере, двух основных категорий ОО:

Особо важные объекты — предприятия, через которые проходят МЦ стратегического значения (ядерные и оружейные материалы; токсичные, наркотические и отравляющие вещества; энергоносители; оружие и боеприпасы и т.д.) особо высокой денежной (дензнаки, драгметаллы и т.д.), информационной, культурно-исторической или духовно-нравственной ценности, когда возможный ущерб максимален, а по значению и масштабам нарушение режима движения МЦ может иметь катастрофические последствия трансграничного, федерального или регионального уровней.

Промышленно-коммерческие объекты (ПКО) — предприятия, компании, банки, корпорации и т.д., характеризующиеся тем, что возможный ущерб от нарушения движения МЦ носит имущественный, в основном, коммерческий характер, приводящий к финансово-экономическим потерям и снижению эффективности жизнедеятельности хозяйствующих субъектов (владельцев) предприятия[[4]](#footnote-4).

Необходимо отметить, что признаки категорирования особо важных объектов, выделяемые в системах обеспечения охранно-территориальной безопасности СКУД и в системах контроля и учета СКУМЦ, совпадают по большинству пунктов.

Основной целью внедрения СКУМЦ в систему физической защиты особо важных объектов является нейтрализация физических угроз, вызванных изменениями режимов движения стратегических МЦ и, как следствие, возможностью возникновения чрезвычайных ситуаций катастрофического характера, при этом, в целом, решаются следующие задачи:

предупреждение несанкционированного доступа персонала к МЦ с использованием систем СКУД, как основная задача охраны;

контроль и учет движения МЦ с помощью системы СКУМЦ, содержащей специальные аппаратные средства мониторинга для идентификации, контроля физической сохранности МЦ и документирования; режима их движения;

выявление и нейтрализация лиц из числа персонала, нарушающих режим доступа и причастных к нарушению режима сохраняемости и движения МЦ (по результатам аппаратного контроля и учета движения МЦ). В силу специфики нейтрализация внешних и внутренних нарушителей решается различными подразделениями охраны, поэтому интеграция систем менее актуальна.

В физической защите ПКО основную роль играет система СКУМЦ, при этом на первый план выдвигаются процедуры обнаружения «внутренних» нарушителей и предотвращения хищений МЦ, в том числе:

метрологический контроль в целях измерения параметров, идентификации состояния и местонахождения МЦ;

учетно-отчетное балансовое документирование и выявление фальсификации данных;

своевременное информационное оповещение руководства о состоявшихся фактах хищения, порчи или несанкционированного использования МЦ, нарушении режима движения МЦ;

установление, идентификация и физическая нейтрализация лиц, чья деятельность привела к хищениям, порче или несанкционированному использованию МЦ, а также местоположения участка нарушения.

Системные функции элементов СКУД и СКУМЦ во многом сходны, отличаясь, главным образом, специализацией аппаратных средств охранного мониторинга, специализированной информационной системы документирования результатов контроля и балансовой системы учета движения МЦ с использованием компьютерных сетей, причем основной целью СКУМЦ является выявление и нейтрализация внутреннего нарушителя. Включение в состав СКУМЦ средств мониторинга окружающей среды позволяет также интегрировать в единую систему физической защиты подсистему управления экономической и экологической безопасностью объекта. Учитывая ограниченные средства ПКО, интеграция систем СКУД и СКУМЦ в единую систему чрезвычайно актуальна[[5]](#footnote-5).

К настоящему времени технические средства СКУМЦ нашли широкое применение на объектах ядерно-оружейного комплекса, ядерной энергетики, авиационного транспорта и военной промышленности, но сравнительно редко применяются на ПКО. Свыше 90 % действующих ПКО России не имеют необходимого оборудования и экономически ограничены в возможностях установки СКУМЦ и модернизации действующих систем охраны предприятий. Вместе с тем, уровень ущерба от деятельности внутренних нарушителей продолжает нарастать. Усредненный размер имущественного ущерба предприятиям ПКО, причиненного внутренними нарушителями, возрос до 15-20 % стоимости МЦ, проходящих через предприятия. В документах ГАЗПРОМА доля имущественных преступлений в общем объеме преступлений оценена уровнем в 60 %. Следует указать и на рост дерзости и изощренности внутренних нарушителей. Учитывая перечисленное, можно констатировать, что внедрение СКУМЦ на ПКО назревшая проблема, требующая решения, и что внедрение СКУМЦ требует модернизации существующих систем охраны.

Технические средства охранного мониторинга СКУМЦ, как и средства СКУД, основаны на различных физических принципах действия, размещаются в определенных контрольных точках зон пространства («зоны учетно-отчетного баланса») на траекториях движения МЦ на территории объекта. При этом размещение зон баланса СКУМЦ и зон обнаружения СКУД должно соответствующим образом координироваться в пространстве, создавая единую интегрированную пространственную структуру физической защиты. Линии информационной связи и энергоснабжение СКУМЦ и СКУД объединяются в локальные сети с подключением к системообразующей аппаратуре на базе современных ПЭВМ и систем технического зрения с разделением на высшие и низшие уровни информационной иерархии. С учетом перечисленного при разработке современных интегрированных систем охраны должна быть предусмотрена возможность технической аппаратной стыковки СКУД и СКУМЦ.

Интеграция СКУМЦ в системы охраны и физической защиты ПКО требует реализации мероприятий, аналогичных мероприятиям инженерного проектирования и оборудования объектов средствами СКУД. Упрощенная схема организационно-технических мероприятий, касающихся внедрения СКУМЦ, представленная на рис.3, должна предусматривать:

координацию деятельности операционных структур СКУД и СКУМЦ в пространстве и времени;

координацию деятельности по управлению МЦ предприятия, схемам и графикам их движения;

внедрение системы стратегического планирования деятельности модернизированной физической защиты;

внедрение системы независимого контроля результатов оперативной деятельности интегрированных структур.

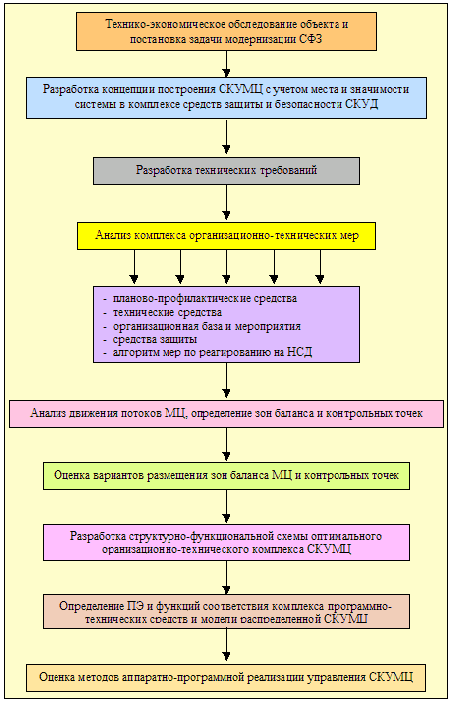


Рис. 3. Алгоритм разработки концепции модернизации систем физической защиты объектов

Итак, результаты проведенного анализа показывают, что интеграция систем физической защиты СКУД и СКУМЦ на особо важных объектах охраны имеет важное значение, но значительно менее актуальна по сравнению с актуальностью задачи модернизации существующих систем охраны и физической защиты на промышленно-коммерческих объектах. Это вызвано необходимостью снижения финансово-экономических потерь, обусловленных ростом масштабов имущественных преступлений, совершаемых внутренними нарушителями производственных режимов на коммерческих предприятиях.

Список литературы

1. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2009. - 496 с.
2. Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. - М.: Нолидж, 2009. - 496 с., ил.
3. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия -Телеком, 2008. - 452 с., ил
4. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред.А.П. Леонова. - Минск: АРИЛ, 2010. - 552 с.
5. Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. - М.: Академический проект: Трикста, 2007. - 544 с.

1. См.: Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2009. – С. 75. [↑](#footnote-ref-1)
2. См.: Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. - М.: Нолидж, 2009. – С. 76. [↑](#footnote-ref-2)
3. См.: Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. - М.: Академический проект: Трикста, 2007. – С. 121. [↑](#footnote-ref-3)
4. См.: Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред.А.П. Леонова. - Минск: АРИЛ, 2010. - . 87. [↑](#footnote-ref-4)
5. См.: Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. - М.: Нолидж, 2009. – С. 109. [↑](#footnote-ref-5)