Федеральное государственное казенное образовательное
учреждение высшего образования
«Сибирский юридический институт
Министерства внутренних дел Российской Федерации»

А.А. Черных,
Ф.В. Безгачев

ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ И БЕЗОПАСНОСТИ, ИСПОЛЬЗУЕМЫЕ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Красноярск
СибЮИ МВД России
2024

УДК 654.9:654.17
ББК 38.48+32.94-5

Рецензенты: А.В. Еськов – начальник кафедры информационной безопасности Краснодарского университета МВД России доктор технических наук, профессор;
А.В. Черепанов – заместитель начальника отдела организации аналитической работы ФГКУ «УВО ВНГ России по Красноярскому краю».

Учебное пособие подготовлено кандидатом юридических наук, доцентом А.А. Черных, Ф.В. Безгачевым.

Черных, А.А.
Технические средства охраны и безопасности, используемые в органах внутренних дел : учебное пособие / А.А. Черных, Ф.В. Безгачев. – Красноярск : СибЮИ МВД России, 2024. – 70 с.

В учебном пособии разобран комплекс проблем в области инженерно-технической укрепленности объектов органов внутренних дел. Детально рассмотрены системы сигнализаций, их состав, классификация и функциональное назначение. Кроме того, в работе раскрываются вопросы функционирования системы централизованного наблюдения (понятие, функции, состав), алгоритм действий персонала пункта централизованной охраны при поступлении тревожных сообщений и организация несения службы сотрудниками групп задержания вневедомственной охраны Росгвардии. Подвергнуты глубокому анализу системы охранного телевидения, системы контроля и управления доступом, а также комплексные и интегрированные системы безопасности.

Данное учебное пособие предназначено для курсантов и слушателей образовательных организаций МВД России. Кроме того, оно может представлять интерес для преподавателей и сотрудников органов внутренних дел, желающих повысить уровень своей компетентности в сфере технических средств охраны и безопасности.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Деятельность правоохранительных органов в борьбе с преступностью связана с активным применением современных достижений науки и техники. Обладая высокой эффективностью, они способствуют раскрытию и предотвращению преступлений, розыску и изобличению преступников. Значимое место в практике предупреждения, раскрытия и расследования преступлений отводится техническим средствам охраны и безопасности.

ГОСТ Р 52551-2016 устанавливает термины и их определения в целях формирования единого технического языка в области обеспечения охраны и безопасности объектов различной ведомственной принадлежности и формы собственности, а также имущества граждан и организаций.

Охраняемый объект – отдельное помещение или несколько помещений в одном здании, объединенные единым периметром, здания, строения, сооружения, прилегающие к ним территории и акватории, помещения, транспортные средства, а также грузы, денежные средства и иное имущество, подлежащее защите от противоправных посягательств.

Ведомственная охрана – совокупность сил и средств, создаваемых федеральными государственными органами и организациями органов управления, предназначенных для защиты охраняемых объектов от противоправных посягательств[1].

Вневедомственная охрана – структурное подразделение Федеральной службы войск национальной гвардии Российской Федерации, предоставляющее услуги по охране объектов всех форм собственности, а также квартир и других мест хранения имущества граждан[2].

Антитеррористическая защита объектов – деятельность, осуществляемая с целью повышения устойчивости объектов к террористическим угрозам[3].

Антитеррористическая защищённость объектов обеспечивается выполнением следующих общих требований.

1. Наличием организационно-распорядительных документов по организации защиты объектов от возможных террористических актов и назначение должностных лиц, ответственных за проведение мероприятий по антитеррористической защищённости объектов.

---

[1] О ведомственной охране : Федеральный закон от 14 апреля 1999 г. № 77-ФЗ.

[2] О войсках национальной гвардии Российской Федерации : Федеральный закон от 3 июля 2016 г. № 226-ФЗ.

[3] Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ МВД России от 31 декабря 2014 г. № 1152.

2. Разработкой порядка взаимодействия должностных лиц объектов и подразделений с органами исполнительной власти субъектов Российской Федерации, территориальными органами ФСБ России, МЧС России, Минобороны России, а также медицинскими учреждениями и аварийно-спасательными службами по вопросам обмена информацией, проведения совместных учений (тренировок) и реагирования на сообщения об угрозе террористического акта.

3. Организацией охраны объектов.

4. Обеспечением пропускного режима на объектах и оборудованием контрольно-пропускных пунктов[1] досмотровой техникой, а также специальными инженерно-техническими сооружениями, препятствующими несанкционированному проходу и проезду.

5. Выполнением требований нормативных документов, регламентирующих порядок обеспечения охраны, пропускного и внутриобъектового режимов.

6. Выделением особо охраняемых зон объектов и их периметра по степени наибольшей террористической уязвимости и масштабов последствий террористических актов.

7. Оборудованием объектов и прилегающей территории средствами инженерно-технической укреплённости и техническими средствами охраны в соответствии с требованиями **Инструкции по обеспечению инженерно-технической укреплённости и повышению уровня антитеррористической защищенности объектов органов внутренних дел Российской Федерации от преступных посягательств**, утверждённой приказом МВД России от 31.12.2014 № 1152.

8. Обеспечением личного состава дежурных смен, охраняющих объекты, переносными и стационарными средствами связи и табельным оружием в соответствии с требованиями нормативных правовых актов МВД России.

9. Оборудованием и оснащением специализированных площадок для досмотра автомобильного и иного транспорта, въезжающего на территорию объектов и выезжающего с их территории.

10. Исключением доступа посторонних лиц к эксплуатационной документации и во внутренние компьютерные сети объектов.

11. Обеспечением должного обслуживания и контроля за наличием и работоспособностью всех систем обеспечения безопасности объектов.

Инженерно-техническая укреплённость и оснащенность техническими средствами охраны специальных помещений органа, организации, подразделения системы МВД России (помещения дежурных частей,

[1] Контрольно-пропускной пункт – стационарный пост, выставляемый для обеспечения пропускного режима на территорию объекта.

комнаты хранения оружия, боеприпасов, взрывчатых веществ и специальных средств, помещения для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, изоляторы временного содержания подозреваемых и обвиняемых, архивы, хранилища, кассы) должны соответствовать требованиям действующих ведомственных нормативных документов, регламентирующих их защищённость.

Объекты и помещения, в которых осуществляется деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список 1 перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации[1], прекурсоров, и (или) культивирование наркосодержащих растений для использования в научных, учебных целях и в экспертной деятельности оборудуются в соответствии с требованиями:

– постановления Правительства РФ от 17 декабря 2010 г. № 1035 «О порядке установления требований к оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и их прекурсоров, и (или) культивирование наркосодержащих растений»;

– постановления Правительства РФ от 31 декабря 2009 г. № 1148 «О порядке хранения наркотических средств, психотропных веществ и их прекурсоров»;

– приказа Федеральной службы войск национальной гвардии Российской Федерации и Министерства внутренних дел Российской Федерации от 9 января 2018 г. № 1/5 «Об утверждении Требований к оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список I перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, прекурсоров, и (или) культивирование наркосодержащих растений для использования в научных, учебных целях и в экспертной деятельности».

Техническое средство охраны (далее – ТСО) – конструктивно законченное устройство, выполняющее самостоятельные функции в составе системы, предназначенной для обеспечения охраны или безопасности объекта.

Перечень ТСО для охраны объектов и имущества:

1. Средства аудио- и видеонаблюдения.

[1] Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации : постановление Правительства РФ от 30 июня 1998 г. № 681.

2. Технические средства охранной и охранно-пожарной сигнализации.

3. Средства инженерно-технической защиты и контроля доступа.

4. Технические средства обнаружения предметов и веществ, ограниченных в обороте.

5. Технические средства мониторинга и навигации подвижных и стационарных объектов.

Технические средства охраны применяются в целях повышения надёжности охраны и сокращения численности личного состава, задействованного для обеспечения безопасности объектов органов внутренних дел Российской Федерации. Они включают: периметровые и объектовые средства обнаружения, технические средства предупреждения и воздействия, аппаратуру сбора и обработки информации, средства управления доступом на объект, технические средства наблюдения, системы электропитания, кабельные и проводные линии, средства связи системы охраны объектов, а также средства обеспечения эксплуатации технических средств охраны.

Надежность охраны объектов с применением технических средств охраны достигается: правильным выбором типа технических средств охраны и использованием их в комплексе с инженерными заграждениями и сооружениями на постах; скрытностью проводимых мероприятий по установке средств охраны и их маскировкой; ограничением круга лиц, допущенных к их установке и эксплуатации; закреплением технических средств охраны за конкретными должностными лицами; высоким качеством монтажа, постоянным обслуживанием и контролем за их состоянием; бдительностью и своевременностью действий личного состава караула при срабатывании технических средств охраны.

Для усиления охраны специальных объектов может применяться система средств физической защиты, являющаяся составной частью охраны. Порядок ее использования и применения определяется соответствующими руководствами и инструкциями.

Тип и количество применяемых на объекте технических средств охраны определяются в зависимости от его важности, физико-географических, эксплуатационных и других особенностей.

Технические средства охраны и безопасности играют важную роль в противодействии преступности. Применение средств централизованного наблюдения, средств охранного телевидения, средств контроля и управления доступом на особо важных промышленных объектах, а также на объектах повышенной опасности позволяет снизить к минимуму возможность осуществления террористических актов, а на объектах проведения крупных международных массовых мероприятий позволяет предотвратить гибель большого количества людей от возможных террористических актов. Особую роль в охране объектов МВД России играют

сигнализации, средства централизованного наблюдения и охранного телевидения. В связи с чем особую актуальность приобретают вопросы антитеррористической защищенности объектов МВД России, а также вопросы организации деятельности органов внутренних дел по обеспечению безопасности имущества граждан.

Для того чтобы уметь правильно выбирать и организовать защиту объектов органов внутренних дел от противоправных посягательств, обучающиеся должны овладеть базовыми знаниями в области обеспечения охраны зданий, сооружений, а также прилегающей территории. Эта задача может быть успешно решена в ходе подготовки специалистов в образовательных организациях МВД России при реализации рабочих программ дисциплины «Специальная техника ОВД», рабочей учебной программы междисциплинарного курса «Специальная техника» и других программ. В процессе получения базовых знаний у обучающихся должны сформироваться способности, позволяющие им в будущем периодически повышать уровень собственной компетенции в рассматриваемой сфере.

Данное учебное пособие может быть использовано для подготовки обучающихся и преподавателей к занятиям лекционного и семинарского типа, касающихся вопросов применения систем охраны и безопасности в деятельности органов внутренних дел, а также для самостоятельного изучения учебного материала действующими сотрудниками ОВД, заинтересованными в повышении своей квалификации.

1. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ УКРЕПЛЁННОСТЬ ОБЪЕКТОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

К объектам ОВД, которые должны быть защищены от противоправных посягательств, относят:

– комплексы зданий или сооружений, имеющие общую прилегающую территорию и внешние границы;

– отдельно стоящие здания или сооружения, имеющие прилегающую территорию (или без таковой);

– обособленные помещения или группы помещений, находящиеся в ведении органа, организации, подразделения системы МВД России.

Перед установкой на объектах ОВД каких-либо систем безопасности необходимо принять меры по их инженерно-технической укреплённости.

Инженерно-техническая укреплённость охраняемого объекта – это совокупность мероприятий, направленных на усиление конструктивных элементов зданий, помещений и охраняемых территорий, обеспечивающих необходимое противодействие несанкционированному проникновению в охраняемую зону, взлому и другим преступным посягательствам.

Для того чтобы упростить задачу обеспечения защиты объектов ОВД от криминальных угроз каждому охраняемому объекту присваивается определённая категория (т.е. проводится процедура категорирования охраняемых объектов).

Категория охраняемого объекта – комплексная оценка объекта, учитывающая его государственную, общественную или иную значимость в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надёжности охраны.

В зависимости от степени потенциальной угрозы объекты ОВД подразделяются на четыре категории – I, II, III, IV[1].

Объект I категории – комплекс зданий или сооружений, имеющих общую прилегающую территорию (или без таковой) и внешние границы; отдельно стоящее здание или сооружение, имеющие прилегающую территорию (или без таковой), на которых обязательно осуществление круглосуточного **пропускного режима**[2] и круглосуточного дежурства.

---

[1] I категория – высшая, IV категория – низшая.

[2] Пропускной режим – порядок, обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц, въезда (выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества на объекты.

Объект II категории – обособленное помещение или группа помещений, расположенных в зданиях или сооружениях, не относящихся к системе органов внутренних дел Российской Федерации, в которых **внутриобъектовый режим**[1] требует осуществления пропускного режима и круглосуточного дежурства.

Объект III категории – отдельно стоящие здания или сооружения, имеющие прилегающую территорию (или без таковой), на которых осуществление круглосуточного пропускного режима и круглосуточного дежурства не обязательно.

Объект IV категории – обособленное помещение или группа помещений, расположенных в зданиях или сооружениях, не относящихся к системе органов внутренних дел Российской Федерации, в которых внутриобъектовый режим не требует осуществления пропускного режима и круглосуточного дежурства.

Объекты, не отнесённые к указанным категориям, классифицируются по ближайшему аналогу с учётом возможного риска и ущерба вследствие противоправного посягательства на них. Допускается оборудование объектов территориальных органов МВД России, расположенных в регионах с введенным режимом чрезвычайного положения, на территориях проведения контртеррористических операций, зонах вооруженных конфликтов, а также при наличии дополнительных угроз безопасности объекту (при существенном обострении криминогенной обстановки на территории дислокации объекта) дополнительными средствами инженерно-технической укреплённости и техническими средствами охраны.

Решение о принадлежности объекта к определённой категории формируется с учётом предложений руководителей подразделений, в ведении которых находятся категорируемые объекты, оформляется приказом (распоряжением) и принимается:

1. Министром внутренних дел Российской Федерации – в отношении объектов, занимаемых подразделениями центрального аппарата МВД России, органами, организациями, подразделениями системы МВД России.

---

[1] Внутриобъектовый режим – порядок, обеспечиваемый совокупностью мероприятий и правил, выполняемых лицами, находящимися на объектах, в соответствии с требованиями внутреннего распорядка, и определяемый руководителем (начальником) территориального органа МВД России, образовательной, научной, медицинской (в том числе санаторно-курортной) организаций системы МВД России, окружного управления материально-технического снабжения системы МВД России, а также иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел.

2. Начальником территориального органа МВД России на окружном или межрегиональном уровне – в отношении объектов, занимаемых подчиненными подразделениями.

3. Начальником территориального органа МВД России на региональном уровне – в отношении объектов, занимаемых территориальными органами МВД России на региональном уровне, а также объектов, занимаемых подчинёнными территориальными органами МВД России на районном уровне.

4. Руководителем (начальником) образовательной, научной, медицинской (в том числе санаторно-курортной) организаций, окружного управления материально-технического снабжения системы МВД России, а также иной организации, подразделения, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел, – в отношении объектов, занимаемых подчинёнными подразделениями (организациями) и филиалами.

Каждой категории объектов должен соответствовать определённый **класс (степень) защиты**[1] конструктивных элементов (ограждающих конструкций и элементов инженерно-технической укреплённости).

Инженерно-техническая укреплённость охраняемого объекта достигается при помощи средств инженерно-технической укреплённости.

Под средствами инженерно-технической укреплённости охраняемых объектов понимаются строительные, механические и/или электромеханические изделия и конструкции, преграждающие пути проникновения злоумышленников на объект или доступа к имуществу.

Средства инженерно-технической укреплённости должны обеспечивать защиту от несанкционированного проникновения и иметь свой класс защиты, при этом особое внимание следует уделять направлениям, ведущим к критическим элементам объекта (территории), на трудно просматриваемых участках периметра и уязвимых местах объекта (территории).

Средства инженерно-технической укреплённости предназначены:

– для защиты объекта и находящихся на нём людей путём создания физической преграды несанкционированным действиям нарушителя;

– для создания препятствий на пути движения нарушителя с целью затруднения (задержки) его продвижения к объектам защиты на время, достаточное для прибытия группы задержания[2].

---

[1] Класс защиты – комплексная оценка, учитывающая размещение, прочностные характеристики, особенности конструктивных элементов и показывающая степень достаточности обеспечения надлежащей защиты объекта.

[2] Группа задержания – подвижной наряд строевого подразделения вневедомственной охраны Росгвардии численностью не менее двух сотрудников, осуществляющий патрулирование по заданному маршруту и оперативное реагирование на

К средствам инженерно-технической укреплённости относят:

1) защитные конструкции:

– ограждения (временные и постоянные, внешние и внутренние, основные и дополнительные);

– ворота, калитки, двери в воротах;

2) строительные конструкции:

– стеновые и потолочные строительные конструкции кладовой, хранилища;

– наружные стены здания, первого этажа, а также стены и перекрытия охраняемых помещений, расположенных внутри здания, примыкающие к помещениям других собственников[1];

– наружные стены охраняемых помещений, расположенных на втором и выше этажах здания, а также стены, перекрытия этих помещений, расположенных внутри здания, не примыкающие к помещениям других собственников;

– внутренние стены, перегородки в пределах каждой подгруппы, вентиляционные короба;

3) дверные конструкции:

– входные двери в здание, выходящие на улицы и магистрали;

– двери запасных выходов, двери, выходящие на крышу (чердак), во дворы;

– входные двери охраняемых помещений;

– внутренние двери в помещениях в пределах каждой подгруппы;

4) оконные конструкции:

– оконные проёмы первого и подвального этажей, выходящие на оживленные улицы и магистрали;

– оконные проёмы второго и выше этажей, не примыкающие к пожарным лестницам, балконам, карнизам и т.п.;

– оконные проёмы первого и подвального этажей, выходящие во дворы, малолюдные переулки;

– оконные проёмы, примыкающие к пожарным лестницам, балконам, карнизам и т.п.;

– оконные проёмы помещений охраны;

5) замки и запирающие устройства:

– запирающие устройства входных и запасных дверей в здание, входных дверей охраняемых помещений, дверей, выходящих на крышу (чердак);

тревожные сигналы, поступающие с охраняемых объектов, подключённых к пульту централизованного наблюдения.

[1] Собственниками могут являться как физические, так и юридические лица, владеющие, пользующиеся или распоряжающиеся зданиями и помещениями на законных основаниях.

– запирающие устройства внутренних дверей.

Уязвимые места охраняемых объектов дополнительно оснащаются системами охранной сигнализации и/или охранными телевизионными системами, предназначенными для обнаружения попыток несанкционированного вторжения. При невозможности оборудования уязвимых мест ограждения техническими средствами охраны необходимо размещать в этих местах посты охраны (наблюдательные будки и вышки) или проводить другие инженерно-технические и организационные мероприятия, направленные на обеспечение требуемого уровня защиты.

Средства инженерно-технической укреплённости должны:

– препятствовать несанкционированному проникновению на охраняемый объект и/или охраняемую зону;

– ограничивать использование нарушителем подручных средств;

– обеспечивать достаточную пропускную способность при санкционированном доступе и/или экстренной эвакуации в чрезвычайной ситуации;

– не оказывать влияния на работу технических средств охраны, применяемых на охраняемом объекте;

– создавать необходимые условия для выполнения задач по защите объекта лицами, отвечающими за обеспечение его безопасности;

– обладать прочностью и долговечностью.

Таким образом, всем объектам ОВД присваивается определённая категория, в соответствии с которой проводятся мероприятия по защите указанных объектов от криминальных угроз. На первом этапе решается задача усиления конструктивных элементов зданий, помещений и охраняемых территорий. Для обеспечения необходимого уровня противодействия несанкционированному проникновению в охраняемую зону, взлому и другим преступным посягательствам разработаны требования к инженерно-технической укреплённости объектов ОВД, которые включают в себя:

1) требования к защите периметра, отдельных участков территории (к инженерному заграждению, к ограждению);

2) требования к защите акватории;

3) требования к постам;

4) требования к воротам и калиткам;

5) требования к контрольно-пропускным пунктам[1];

6) требования к стенам, перекрытиям и перегородкам;

7) требования к дверным конструкциям;

8) требования к оконным конструкциям;

9) требования к запирающим устройствам;

---

[1] Контрольно-пропускной пункт (КПП) – стационарный пост, выставляемый для обеспечения пропускного режима на территорию объекта.

10) требования к вентиляционным коробам;

11) требования к водопропускам, воздушным трубопроводам, подземным коллекторам.

Инженерно-техническая укреплённость и оснащённость техническими средствами охраны специальных помещений органа, организации, подразделения системы МВД России (помещения дежурных частей, комнаты хранения оружия, боеприпасов, взрывчатых веществ и специальных средств, помещения для хранения средств защиты, связи, специальной, оперативной и криминалистической техники, изоляторы временного содержания подозреваемых и обвиняемых, архивы, хранилища, кассы) должна соответствовать требованиям ведомственных нормативных документов, регламентирующих их защищённость.

Контрольные вопросы

1. Что понимается под инженерно-технической укреплённостью охраняемого объекта?
2. Что понимается под категорией охраняемого объекта?
3. На какие категории подразделяются объекты ОВД в зависимости от степени потенциальной угрозы?
4. Что понимается под средствами инженерно-технической укреплённости охраняемых объектов?
5. Для чего предназначены средства инженерно-технической укреплённости?
6. Чем дополнительно оснащаются уязвимые места охраняемых объектов?
7. Какие защитные конструкции относят к средствам инженерно-технической укреплённости?
8. Какие строительные конструкции относят к средствам инженерно-технической укреплённости?
9. Какие дверные конструкции относят к средствам инженерно-технической укреплённости?
10. Какие оконные конструкции относят к средствам инженерно-технической укреплённости?
11. Какие функции должны выполнять средства инженерно-технической укреплённости?
12. Какие существуют требования к инженерно-технической укреплённости объектов ОВД?

2. СИСТЕМЫ СИГНАЛИЗАЦИИ, УСТАНАВЛИВАЕМЫЕ НА ОХРАНЯЕМЫХ ОБЪЕКТАХ

Системы сигнализации представляют собой функционально законченные комплексы технических средств, установленные на охраняемом объекте и предназначенные для обнаружения тревожных событий и формирования (трансляции) соответствующих извещений. В зависимости от назначения систем под тревожным событием понимается либо пожар (возгорание), либо обнаружение несанкционированного проникновения (попытки такого проникновения) на охраняемый объект.

Системы сигнализации подразделяются на автоматические и ручные.

Автоматическая система сигнализации – это система сигнализации, обеспечивающая автоматический переход из нормального состояния в отключенное и обратно под управлением ответственного лица, пользователя, владельца или жильца без обращения к другим системам, например, к системе электросвязи.

Ручная система сигнализации – это система сигнализации, обеспечивающая переход из нормального состояния в отключенное и обратно неавтоматически.

В настоящее время существуют следующие виды систем сигнализации:

– системы охранной сигнализации,

– системы пожарной сигнализации,

– системы охранно-пожарной сигнализации.

Система охранной сигнализации – это совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемых объектах, передачи, сбора, обработки и представления информации в заданном виде.

Система пожарной сигнализации – это совокупность взаимодействующих технических средств, предназначенных для обнаружения пожара, формирования, сбора, обработки, регистрации и передачи в заданном виде сигналов о пожаре, режимах работы системы, другой информации и выдачи (при необходимости) сигналов на управление техническими средствами противопожарной защиты, технологическим, электротехническим и другим оборудованием.

Система охранно-пожарной сигнализации – это совокупность совместно действующих технических средств для обнаружения появления признаков нарушителя на охраняемых объектах и/или пожара на них, передачи, сбора, обработки и представления информации в заданном виде.

Рассмотрим системы охранно-пожарной сигнализации более подробно.

Системы охранно-пожарной сигнализации должны:

– выдавать извещение о несанкционированном доступе и обнаруживать саботажные действия нарушителя[1];

– выдавать извещение о неисправности при отказе технических средств охранно-пожарной сигнализации;

– сохранять исправное состояние при воздействии влияющих факторов окружающей среды;

– восстанавливать работоспособное состояние после воздействия опасных факторов окружающей среды;

– быть устойчивыми к любым установленным в стандартах государств на системы конкретного вида повреждениям какой-либо своей части и не вызывать других повреждений в системе или не приводить к косвенной опасности вне её;

– сохранять работоспособное состояние при отключении сетевого источника электропитания или другого основного источника электропитания в течение времени прерывания электропитания.

Системы охранно-пожарной сигнализации не должны выдавать ложных тревог при переключениях источников электропитания сети и резерва или других видов с одного на другой.

Автоматические системы охранно-пожарной сигнализации должны обеспечивать идентификацию лиц, осуществляющих доступ на охраняемые объекты, и/или паролей этих лиц.

Системы охранно-пожарной сигнализации должны быть защищены от несанкционированного доступа к управлению программными средствами кодом.

В состав систем охранно-пожарной сигнализации входят:

1) извещатели;
2) шлейфы сигнализации;
3) приёмно-контрольные приборы;
4) оповещатели;
5) источники электропитания;
6) дополнительное оборудование.

Извещатели – это устройства, предназначенные для формирования состояния тревоги при обнаружении опасности и/или устройства для формирования извещения о тревоге при проникновении или попытке проникновения, или для инициирования сигнала тревоги потребителем.

[1] Саботаж – это преднамеренное воздействие на техническое средство (систему) охраны (безопасности) с целью нарушения его нормального функционирования.

В зависимости от способа приведения в действие извещатели классифицируют на автоматические и мануальные (ручные и ножные).

Также извещатели подразделяются на охранные и пожарные.

Охранный извещатель – это техническое средство охранной сигнализации, предназначенное для формирования тревожного извещения автоматическим или ручным способом при обнаружении проникновения (попытки проникновения) или других противоправных воздействий на охраняемый объект.

В зависимости от вида охраняемой зоны автоматические охранные извещатели классифицируют на:

– точечные,

– линейные,

– поверхностные,

– объёмные.

В зависимости от используемых физических принципов обнаружения автоматические охранные извещатели классифицируют на:

1) контактные (электроконтактные, магнитоконтактные, ударно-контактные),

2) пьезоэлектрические,

3) ёмкостные,

4) трибоэлектрические,

5) радиоволновые,

6) звуковые, ультразвуковые, инфразвуковые,

7) вибрационные,

8) активные и пассивные оптико-электронные (инфракрасные),

9) инерционные,

10) электростатические,

11) сейсмические,

12) манометрические,

13) волоконно-оптические,

14) проводноволновые,

15) другие (определяются по мере их разработки).

По сочетанию принципов обнаружения автоматические охранные извещатели подразделяют на:

– извещатели, основанные на одном физическом принципе обнаружения;

– извещатели, основанные на двух или более физических принципах обнаружения.

Охранные извещатели, основанные на двух и более физических принципах обнаружения, классифицируют на:

– комбинированные,

– совмещённые,

– комбинированно-совмещённые.

Комбинированный извещатель – это извещатель, основанный на двух или более физических принципах обнаружения.

Совмещённый извещатель – это извещатель, выполняющий одновременно функции нескольких охранных извещателей с различными физическими принципами и зонами обнаружения или выполняющий одновременно функции охранного извещателя и другого средства контроля охраняемого объекта.

Комбинированно-совмещённый извещатель – это извещатель, обеспечивающий на аппаратном и/или программном уровне логическое комбинирование и/или совмещение функции нескольких охранных извещателей, использующих различные физические принципы обнаружения, и/или других средств контроля охраняемого объекта.

Основные типы извещателей, обеспечивающие защиту от предполагаемых (возможных) способов криминального воздействия, приведены в таблице № 1.

Таблица 1

Способ воздействия	**Тип извещателя (принцип действия)**
Проникновение через ограждение 2-4 класса зашиты способами разрушения полотна, подкопом, перелазом, отгибом	Комбинированно-совмещённый с четырьмя каналами обнаружения (ёмкостный, вибрационный, сейсмический, радиоволновый)
Проникновение перемещением через неогороженный, слабозащищенный периметр или периметр 1-го класса	Линейный радиоволновый, линейный оптико-электронный (активный инфракрасный)
Проникновение перемещением на открытую площадку с материальными ценностями, подход к охраняемому объекту (здание, складское помещение)	Объёмный радиоволновый
Проникновение перемещением в технологические колодцы, выходы воздуховодов подземных сооружений, туннелей, площадок, огороженных сеткой типа «рабица» или металлическим прутком	Объёмный радиоволновый двухпозиционный
Разрушение остеклённых конструкций (разбитие, вырезание, выдавливание, выворачивание, терморазрушение)	Поверхностный ударно-контактный, поверхностный звуковой (акустический)
Разрушение остеклённых конструкций (разбитие, вырезание, выдавливание, выворачивание, терморазрушение) и проникновение перемещением в охраняемое помещение	Поверхностный совмещённый (акустический и пассивный инфракрасный), объёмный совмещённый (акустический и пассивный инфракрасный)

Способ воздействия	Тип извещателя (принцип действия)
Разрушение деревянных конструкций (пролом, выпиливание, сверление, разборка)	Поверхностный вибрационный (пьезоэлектрический)
Разрушение металлических конструкций (разрубание, раздвигание, выкусывание, выпиливание, высверливание, выдавливание, прожигание)	Поверхностный вибрационный (пьезоэлектрический)
Открывание конструкций (дверей, оконных рам)	Точечный магнитоконтактный
Проникновение перемещением в помещение через двери, оконные рамы	Поверхностный оптико-электронный (пассивный инфракрасный) – «защитная штора»
Перемещение во внутреннем объёме помещения	Объёмный ультразвуковой, объёмный оптико-электронный (пассивный инфракрасный), объёмный радиоволновый, объёмный комбинированный: - пассивный инфракрасный плюс радиоволновый; - пассивный инфракрасный плюс ультразвуковой; - пассивный инфракрасный плюс видео
Пересечение во внутреннем объёме помещения ловушек, барьеров	Линейный оптико-электронный (активный инфракрасный)
Касание, приближение к картинам (с металлической фольгой на подрамнике), к электропроводящим предметам (металлическим шкафам)	Поверхностный ёмкостный
Проникновение в небольшие замкнутые объёмы (витрины, шкафы, киоты и т.п.)	Объёмный ультразвуковой
Перемещение персонала и посетителей в зону охраны отдельных и групп предметов	Объёмный комбинированный (пассивный инфракрасный плюс радиоволновый) – для установки на потолке
Разрушение стенок сейфа взломом, сверлением, выворачиванием	Поверхностный вибрационный (пьезоэлектрический)

Конкретные типы охранных извещателей выбираются после проведения обследования объекта, в зависимости от его категории (класса), на основании анализа особенностей объекта, наиболее вероятных криминальных угроз, наличия помех, внешних воздействующих факторов и стоимости.

Пожарный извещатель – это техническое средство, предназначенное для обнаружения пожара посредством контроля изменений физических параметров окружающей среды, вызванных пожаром, и/или

формирования сигнала о пожаре. По виду контролируемого признака пожара эти извещатели подразделяют на:

– тепловые,

– дымовые,

– пламени,

– газовые,

– комбинированные.

Выбор типов пожарных извещателей осуществляется в зависимости от функционального назначения здания, помещения или сооружения, а также условий эксплуатации и вида пожарной нагрузки[1].

Часть пространства, контролируемая извещателем, при перемещении в которой нарушителя и/или при воздействии на которую извещатель формирует извещение о тревоге, называется зоной обнаружения извещателя. Совокупность зон обнаружения извещателей и средств инженерно-технической укреплённости, условно образующих границу, преодоление которой должно приводить к формированию тревожного извещения, образуют рубеж охранной сигнализации.

Для того чтобы повысить надёжность охраны и своевременно обнаружить проникновение злоумышленника на объект используют многорубежный комплекс охранной сигнализации. Такой комплекс представляет собой совокупность двух или более рубежей охранной сигнализации, на которых применяются технические средства охранной сигнализации, основанные на различных физических принципах действия. Например, если вокруг здания имеется территория, то первым рубежом будет являться периметр территории, сформированный забором и воротами. Вторым рубежом будет периметр здания, третьим – периметр помещения, четвёртым – зона или предмет внутри помещения.

Для каждого рубежа охранной сигнализации рекомендуется выделять отдельный шлейф сигнализации, контролирующий отдельную зону или элемент объекта. Не рекомендуется блокировать одним шлейфом сигнализации более пяти соседних помещений. Под шлейфом сигнализации понимается линия связи, предназначенная для передачи извещений, формируемых техническими средствами сигнализации, на приёмно-контрольный прибор. Они могут быть использованы для электропитания технических средств сигнализации и/или передачи на них сигналов управления.

Для обеспечения возможности взятия под охрану на объектах отдельных помещений, сейфов и металлических шкафов для хранения ценностей и документов, рекомендуется блокировать их посредством отдельных шлейфов сигнализации.

---

[1] Пожарная нагрузка – количество теплоты, которое может выделиться в помещении при пожаре.

Приёмно-контрольный прибор – это составная часть системы охранно-пожарной сигнализации, предназначенная для приёма извещений от извещателей и других технических средств, преобразования и передачи извещений, формирования извещений о состоянии системы для оповещения ответственного лица и/или для дальнейшей передачи извещений, и/или передачи сформированных команд на другие устройства, оповещатели или системы оповещения.

Приёмно-контрольные приборы должны обеспечивать выполнение следующих основных функций:

1) приём извещений от извещателей и других устройств, включённых в шлейфы сигнализации;

2) формирование извещений для передачи на пульт централизованного наблюдения (при организации централизованной охраны);

3) контроль исправности шлейфов сигнализации и каналов связи;

4) управление оповещателями, средствами отображения информации и другими объектовыми устройствами;

5) управление постановкой на охрану и снятием с охраны.

По виду организации тревожной сигнализации на объекте приёмно-контрольные приборы подразделяют на:

1) автономные (извещения о состоянии контролируемых объектов выдаются только на звуковые и световые оповещатели, установленные на охраняемых объектах или в непосредственной близости к ним);

2) локальной сигнализации (извещения о состоянии контролируемых объектов, а также управление контролируемым шлейфом и контролируемыми зонами осуществляют с помощью средств отображения информации и управления (индикаторных панелей, пультов), входящих в состав приёмно-контрольных приборов);

3) централизованной сигнализации (используются для централизованной охраны и работы совместно с системой передачи извещений или в составе такой системы, передающей извещения с приёмно-контрольных приборов на пульт централизованного наблюдения посредством использования различных каналов связи (телефонных линий, радиоканалов, выделенных линий и др.).

По информативности приёмно-контрольные приборы подразделяют на:

– малой информативности (до 8 извещений),

– средней информативности (от 9 до 16 извещений),

– большой информативности (свыше 16 извещений).

По информационной ёмкости приёмно-контрольные приборы подразделяют на:

– малой информационной ёмкости (до 8 шлейфов сигнализации),

– средней информационной ёмкости (от 9 до 64 шлейфов сигнализации),

– большой информационной ёмкости (свыше 64 шлейфов сигнализации).

Оповещатели предназначены для оповещения людей о нападении, проникновении или пожаре на охраняемом объекте.

Оповещатели бывают световые, звуковые и речевые. Световые оповещатели выдают световые сигналы, звуковые оповещатели – звуковые неречевые сигналы, а речевые оповещатели – речевые сигналы.

Системы охранно-пожарной сигнализации питаются от электрической сети с фазным номинальным напряжением 230 В и частотой 50 Гц либо от аккумуляторных батарей.

В качестве дополнительного оборудования в системах сигнализации могут использоваться устройства ввода (клавиатуры и считыватели), устройства защиты от несанкционированного доступа, средства активной защиты[1], оконечные объектовые и прочие устройства.

Хотя системы охранной, пожарной и охранно-пожарной сигнализации являются разновидностями систем тревожной сигнализации, однако на практике системами тревожной сигнализации называют комплексы технических средств охраны, в которых вместо автоматических охранных извещателей используются средства тревожной сигнализации (тревожные кнопки, педали и т.п.). Средства тревожной сигнализации бывают стационарные и носимые. Их размещают так, чтобы они были незаметны для посторонних лиц. В случае нападения на объект такая кнопка должна быть незаметно нажата уполномоченным сотрудником ОВД с целью передачи сигнала «Тревога» на пункт централизованной охраны, принадлежащий вневедомственной охране Росгвардии. Кнопки тревожной сигнализации подключаются к пультам централизованного наблюдения отдельным шлейфом без права снятия с охраны.

Дополнительно отметим, что вневедомственная охрана рекомендует оборудовать места хранения особо ценных предметов, денежных средств, драгоценных металлов, камней и изделий из них специальными техническими средствами (ловушками), формирующими сигналы тревоги при попытках нарушителя завладеть ими. Указанные технические средства включаются в шлейфы тревожной сигнализации охраняемых объектов. Например, для этого может применяться ручной точечный электроконтактный охранный извещатель «Кукла-Л». Он устанавливается там, где хранятся наличные денежные средства, и при изменении положения закладного элемента, закамуфлированного в упаковке банкнот, формирует тревожное извещение, которое передаётся на пульт цен-

[1] Средство активной защиты – это техническое средство, предназначенное для психологического и/или физического воздействия на нарушителя, а также создания в окружающем пространстве условий, препятствующих осуществлению противоправных действий, и привлечения внимания к охраняемому объекту или предмету охраны.

трализованного наблюдения. Этот извещатель используется для предотвращения краж из сейфов, касс, шкафов и т.п., а также для облегчения розыска и своевременного задержания преступника в случае совершения кражи.

Средства тревожной сигнализации должны устанавливаться:

– в помещениях, в которых хранятся оружие и боеприпасы;

– на охраняемой территории в помещении КПП у центрального входа (въезда) и запасных выходах (выездах);

– на постах и в помещениях охраны, расположенных в здании, строении, сооружении и на охраняемой территории;

– в хранилищах, кладовых, кассах и сейфовых комнатах;

– в кабинетах руководства организации;

– на рабочих местах персонала, осуществляющего операции с наркотическими средствами и психотропными веществами;

– в других местах (по требованию руководителя ОВД или по рекомендации сотрудника вневедомственной охраны).

Таким образом, системы сигнализации позволяют своевременно обнаружить опасность на охраняемом объекте и подать сигнал тревоги для принятия мер по устранению опасности. Такие системы должны:

– передавать извещение о тревоге в любое время;

– иметь минимальную вероятность ложных извещений;

– обеспечивать информирование о неисправностях системы;

– выполнять текущую проверку работоспособности системы при условии минимального периода прерывания её нормальной работы;

– иметь защиту от несанкционированного доступа к органам управления и программному обеспечению системы.

Контрольные вопросы

1. Что понимается под автоматической системой сигнализации?
2. Что понимается под ручной системой сигнализации?
3. Что понимается под системой охранной сигнализации?
4. Что понимается под системой пожарной сигнализации?
5. Что понимается под системой охранно-пожарной сигнализации?
6. Что входит в состав систем охранно-пожарной сигнализации?
7. Что понимается под извещателем?
8. Какие существуют виды автоматических охранных извещателей в зависимости от используемых физических принципов обнаружения?
9. Какие существуют виды пожарных извещателей?
10. Что понимается под приёмно-контрольным прибором?
11. Как подразделяют приёмно-контрольные приборы в зависимости от информативности?

12. Как подразделяют приёмно-контрольные приборы в зависимости от информативной ёмкости?

13. Какие существуют виды оповещателей?

14. На каких объектах устанавливаются средства тревожной сигнализации?

3. ЦЕНТРАЛИЗОВАННАЯ ОХРАНА ОБЪЕКТОВ

Автономная охрана – охрана объекта, имеющая функцию оповещения без формирования тревожного извещения.

Локальная охрана – охрана зон с передачей информации о состоянии технических средств охраны в пределах объекта.

Техническое средство охраны (далее – ТСО) – конструктивно законченное устройство, выполняющее самостоятельные функции в составе системы, предназначенной для обеспечения охраны или безопасности объекта.

Централизованная охрана – охрана территориально рассредоточенных объектов с помощью пунктов централизованной охраны.

Пункт централизованной охраны (далее – ПЦО) – структурное подразделение организации, обеспечивающей круглосуточную централизованную охрану объектов с применением систем централизованного наблюдения в целях организации оперативного реагирования при поступлении информации о проникновении (попытке проникновения), а также о возникновении криминальных и технологических угроз.

Централизованная охрана объектов обеспечивается при помощи систем централизованного наблюдения.

3.1 Понятие, функции и состав системы централизованного наблюдения

Система централизованного наблюдения (далее – СЦН) – совокупность программно-аппаратных средств и модулей, взаимодействующих в едином информационном поле, предназначенная для обнаружения криминальных и иных угроз на охраняемых объектах, передачи данной информации на пункт централизованной охраны, приёма информации и представления её в заданном виде на пульт централизованного наблюдения.

СЦН должна работать в круглосуточном режиме и обеспечивать:

– обнаружение криминальных угроз на охраняемых объектах и отображать данную информацию на пульте централизованного наблюдения (на АРМ дежурного оператора);

– осуществление звукового и/или визуального информирования пользователей о состоянии технических средств охраны и модулей объектовых подсистем, а также выполнения соответствующих команд управления;

– местный и дистанционный контроль состояния технических средств охраны и модулей, входящих в состав СЦН (реализуется на автоматизированных рабочих местах);

– хранение совокупности данных о работе СЦН;

– доступ к базе данных СЦН;

– подключение новых объектовых подсистем и подсистем передачи информации с помощью автоматизированных рабочих мест.

СЦН могут иметь дополнительные функции, позволяющие:

– по запросу сотрудника пункта централизованной охраны получать аудио-, видео- и фотоинформации с охраняемых объектов и отображать её на автоматизированных рабочих местах;

– дистанционно управлять техническими средствами охраны и модулями, входящими в состав СЦН;

– использовать средства активной защиты в целях обеспечения оперативного реагирования для устранения криминальной угрозы;

– выполнять иные задачи по обеспечению функционирования пункта централизованной охраны;

– осуществлять комплекс мероприятий, направленных на недопущение несанкционированного доступа на охраняемые объекты;

– обнаруживать технологические угрозы и отображать такого рода информацию на пульте централизованного наблюдения (на АРМ дежурного оператора);

– оповещать людей на объектах о криминальной или технологической угрозе посредством световых и/или звуковых сигналов.

В состав СЦН входят:

– объектовые подсистемы,

– подсистемы передачи информации,

– пультовая подсистема,

– интерфейс подсистем передачи информации[1],

– интерфейс пультовой подсистемы[2].

В отдельных случаях функции средств сбора и обработки информации, подсистемы передачи информации и пультовой подсистемы выполняет система передачи извещений, что должно быть указано в сопроводительной технической документации на СЦН. При этом система передачи извещений должна отвечать требованиям, установленным для средств сбора и обработки информации, для подсистемы передачи информации и пультовой подсистемы, а также соответствующих интерфейсов в составе СЦН.

Система передачи извещений (далее – СПИ) – совокупность совместно действующих технических средств охраны, предназначенных

[1] Интерфейс – совокупность средств и правил, обеспечивающая взаимодействие и сопряжение технических средств и модулей в составе системы централизованного наблюдения. Интерфейс подсистемы передачи информации – интерфейс между подсистемой объектовой и подсистемой передачи информации.

[2] Интерфейс пультовой подсистемы – интерфейс между подсистемой передачи информации и пультовой подсистемой.

для передачи по каналам связи и приёма в пункте централизованной охраны извещений о состоянии охраняемых объектов, служебных и контрольно-диагностических извещений, а также (при наличии обратного канала) для передачи и приёма команд телеуправления.

СПИ должны обеспечивать надёжную передачу извещений о тревоге от охраняемого объекта до ПЦН.

Если при передаче извещений возникает какая-либо неисправность, которая может воспрепятствовать передаче состояния тревоги, то должно быть обеспечено формирование состояния тревоги или неисправности в удалённом центре либо следует регламентировать программу текущей проверки.

У СПИ должны быть указаны следующие параметры:

а) вид канала передачи данных от объекта до ПЦН;

б) вид, тип и число передаваемых извещений (извещение о проникновении, извещение о пожаре, служебные и контрольно-диагностические сообщения и другие, если они предусмотрены в системе);

в) вид, тип и число команд для передачи и приёма телеуправления (для систем с обратным каналом передачи данных от ПЦО до охраняемого объекта);

г) время доставки извещения о тревоге (от момента возникновения до момента индикации на ПЦН);

д) приоритеты в передаче извещений о тревоге;

е) время доставки других видов сообщений.

При нарушении связи между СПИ и другими элементами системы сигнализации на ПЦН должно выдаваться извещение о неисправности. Время задержки извещения о неисправности и максимальное время выявления неисправности для СПИ с автоматической диагностикой должны соответствовать времени, установленному национальным стандартом Российской Федерации.

СПИ должны обеспечивать:

– защиту информации в канале связи от несанкционированного доступа;

– контроль канала передачи извещений от охраняемого объекта до ПЦО;

– работоспособность при подключении/отключении пользователей и изменении их числа.

СПИ с автоматической сдачей под охрану и снятием с охраны, имеющие обратный канал связи, должны обеспечивать передачу сигналов индикации сдачи под охрану и снятия с охраны, а также передачу сигнала подтверждения сдачи под охрану и снятия с охраны на оборудование, расположенное на охраняемом объекте.

СПИ должны выдавать извещение о тревоге или неисправности в случае короткого замыкания, обрыва всех проводов или любого провода соединительной линии, который может прервать передачу извещения о тревоге в течение времени, установленного национальным стандартом Российской Федерации.

Объектовая подсистема – составная часть СЦН, предназначенная для обнаружения криминальных угроз посредством контроля состояния технических средств безопасности и модулей охраняемого объекта и передачи тревожной, контрольно-диагностической, служебной, видео и другой информации в подсистему передачи информации.

В состав объектовой подсистемы входят базовые и дополнительные технические средства охраны и модули, сопряжение и взаимодействие между которыми обеспечивает объектовый интерфейс[1].

К базовым техническим средствам охраны и модулям объектовой подсистемы относят:

– средства сбора и обработки информации,

– охранные извещатели,

– модули управления и индикации состояния,

– средства обеспечения электропитанием.

В состав дополнительных технических средств охраны и модулей объектовой подсистемы могут входить:

– охранные оповещатели,

– средства активной защиты[2],

– средства охранного телевидения,

– средства контроля и управления доступом,

– средства охранного освещения,

– технологические извещатели.

Подсистема передачи информации – составная часть СЦН, предназначенная для передачи информации между объектовыми подсистемами и подсистемой пультовой и представляющая собой совокупность совместно действующих технических средств и модулей, объединённых каналами передачи информации.

В состав подсистемы передачи информации входят базовые и дополнительные технические средства охраны и модули.

---

[1] Объектовый интерфейс – интерфейс между устройствами объектовой подсистемы.

[2] Средство активной защиты – техническое средство, предназначенное для психологического и/или физического воздействия на нарушителя, а также создания в окружающем пространстве условий, препятствующих осуществлению противоправных действий, и привлечения внимания к охраняемому объекту или предмету охраны.

Базовый состав технических средств охраны и модулей подсистемы передачи информации должен состоять из канала передачи информации, в который входят:

– объектовый модем,

– среда передачи,

– пультовой модем.

В состав дополнительных технических средств охраны и модулей подсистемы передачи информации могут входить ретранслятор и средства электропитания.

Пультовая подсистема – составная часть СЦН, предназначенная для приёма, обработки, регистрации, представления в заданном виде и хранения тревожной, контрольно-диагностической, служебной, видео- и другой информации, сформированной на охраняемых объектах и принятой от объектовых подсистем, подсистем передачи информации.

Пультовая подсистема представляет собой совокупность средств электропитания и комплекса средств автоматизации пункта централизованной охраны (далее – КСА ПЦО) на базе локальной вычислительной сети.

В состав КСА ПЦО входят:

– модуль управления;

– автоматизированные рабочие места (АРМ дежурного оператора пульта централизованного наблюдения, АРМ дежурного офицера/начальника дежурной смены, АРМ администратора, АРМ инженера, АРМ для отображения видео-, аудио-, фотоинформации и другие АРМ);

– система управления базой данных;

– система хранения данных и база данных;

– средства электропитания.

Таким образом, СЦН является технической основой, позволяющей организовать централизованную охрану различных объектов, расположенных на определённой территории.

3.2 Алгоритм действий персонала пункта централизованной охраны при поступлении тревожных сообщений

При организации централизованной охраны её базовым структурным элементом является пункт централизованной охраны (мониторинговый центр).

На ПЦО располагается **пульт централизованного наблюдения** (далее – ПЦН). ПЦН является частью СЦН и входит в состав пультовой подсистемы на базе автоматизированного рабочего места дежурного оператора.

Рассмотрим алгоритм действий сотрудников и работников вневедомственной охраны Росгвардии, реализуемый ими при поступлении на ПЦО сигнала «Тревога».

ПЦО вневедомственной охраны является диспетчерским пунктом и обеспечивает:

1. Реализацию мероприятий по техническому перевооружению и оптимизацию затрат на эксплуатацию технических средств ПЦО.

2. Ввод (вывод) в эксплуатацию систем передачи извещений, специализированных программно-аппаратных комплексов, локально-вычислительных сетей, аппаратуры звукозаписи, источников бесперебойного электропитания, систем контроля доступа и видеонаблюдения, их эксплуатацию и техническое обслуживание.

3. Запас пультовой (ретрансляционной) ёмкости, необходимый для подключения принимаемых под охрану объектов.

4. Подключение (отключение) систем сигнализаций, смонтированных на охраняемых объектах.

5. Ведение базы данных об охраняемых объектах.

6. Охрану объектов с применением соответствующих технических средств.

7. Приём, обобщение и доведение сообщений о срабатывании систем сигнализаций на подключенных к ПЦН объектах должностным лицам дежурной смены центров оперативного управления (групп обеспечения служебной деятельности нарядов) управлений (отделов) вневедомственной охраны или их филиалов, нарядам строевых подразделений вневедомственной охраны Росгвардии, а также физическим и юридическим лицам, являющимся собственниками объектов либо владеющим ими на ином законном основании, и (или) их уполномоченным представителям.

8. Приём, хранение и выдачу дубликатов ключей от замков дверей на объектах в соответствии с условиями, указанными в договоре (контракте) на оказание охранных услуг.

9. Ведение служебной документации.

Задачи, возложенные на ПЦО, осуществляют инженерно-технический персонал[1] и дежурная смена. Дежурная смена несёт службу круглосуточно. Она включает в себя дежурных пульта управления и электромонтёров.

При поступлении сигнала «Тревога» дежурный пульта управления обязан:

[1] Инженерно-технический персонал – работники и лица, несущие службу на ПЦО и осуществляющие реализацию мероприятий по обеспечению охраны объектов и имущества с помощью технических средств.

1. Немедленно передать информацию о поступлении сигнала «Тревога» на АРМ дежурного центра оперативного управления (группы обеспечения служебной деятельности нарядов) и по радиосвязи группе задержания. При этом дежурному центра оперативного управления (группы обеспечения служебной деятельности нарядов) сообщается пультовой номер, вид извещения, наименование объекта (фамилия собственника), свою фамилию (кодированный идентификатор) и фактическое время поступления сообщения. Особое внимание обращается на сигналы «Тревога», поступившие с особо важных объектов и объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации, в ночное время, во время, не характерное для прибытия людей на объект, и в нерабочие дни.

2. Зафиксировать время получения информации о срабатывании технического средства охраны.

3. Зафиксировать информацию от группы задержания о месте её нахождения и подтверждении времени получения сигнала.

4. В пути следования довести до старшего группы задержания особенности охраняемого объекта и его краткую характеристику (при этом пультовой номер не называется)[1].

5. При изменении состояния охраны «тревожного» объекта незамедлительно проинформировать дежурного центра оперативного управления (группы обеспечения служебной деятельности нарядов) и по радиосвязи группу задержания.

6. Убедиться в принятии тревожного извещения дежурным центра оперативного управления (группы обеспечения служебной деятельности нарядов) и группой задержания.

7. Произвести обработку извещения, поступившего на ПЦО, в соответствии с порядком выполнения операций на АРМ дежурного пульта управления.

8. Принять информацию от дежурного центра оперативного управления (группы обеспечения служебной деятельности нарядов) и по радиосвязи от группы задержания о результатах отработки переданного сигнала «Тревога».

9. Если сведения о результате выезда группы задержания не поступили, принять меры по выяснению причин отсутствия данной информации.

10. Повторное взятие объекта под охрану проводится только по указанию дежурного центра оперативного управления (группы обеспечения служебной деятельности нарядов) после получения сообщения от группы задержания о результатах выезда по сигналу «Тревога».

[1] Эти сведения отражаются в оперативной карточке охраняемого объекта.

Запрещается перепроверять у заказчика охранных услуг информацию о возможных причинах срабатывания сигнализации по телефону или иным способом до получения сообщения от группы задержания о результатах выезда по сигналу «Тревога».

11. Внести результаты отработки сигнала «Тревога» в графы рабочего журнала АРМ.

12. При поступлении на ПЦН информации о нарушении линии связи или подмене оконечного устройства («авария», «короткое замыкание», «подмена устройства» и т.д.) дежурный пульта управления обязан немедленно передать и проконтролировать получение данной информации дежурному центра оперативного управления (группы обеспечения служебной деятельности нарядов) в автоматическом режиме (на АРМ) или по телефону для принятия решения о направлении группы задержания.

Повторное взятие объекта под охрану производится только по указанию дежурного центра оперативного управления (группы обеспечения служебной деятельности нарядов) по результатам выезда группы задержания по сигналу «Тревога». После получения от группы задержания сообщения о возможности повторного взятия объекта под охрану дежурный пульта управления производит повторное взятие объекта под охрану.

В случае не взятия объекта под охрану после поступления сигнала «Тревога», повторного поступления с объекта сигнала «Тревога» после повторного взятия под охрану и не выявления причин срабатывания технических средств охраны, порядок организации охраны такого объекта осуществляется в соответствии с условиями договора. При этом дежурный центра оперативного управления (группы обеспечения служебной деятельности нарядов) обязан организовать перезакрытие таких объектов. Дежурный пульта управления должен проинформировать заказчика охранных услуг (доверенное лицо) о необходимости прибытия на объект с целью выявления причин срабатывания.

Перезакрытие охраняемого объекта должно быть произведено в присутствии заказчика (доверенного лица). В случае необходимости (отсутствие заказчика или доверенного лица) для перезакрытия в качестве понятого можно привлекать дежурного электромонтера обслуживающей организации или ПЦО.

Перезакрытие с помощью дубликатов ключей производится при невозможности прибытия заказчика (доверенного лица) в соответствии с установленными правилами. Факт выдачи пенала с ключами из хранилища для осмотра охраняемого объекта фиксируется в журнале регистрации выдачи и приёма дубликатов ключей для осмотра и перезакрытия объекта.

По окончании осмотра охраняемого объекта и выяснения причин поступления сигнала «Тревога» сотрудник подразделения вневедомственной охраны, производивший вскрытие объекта, составляет акт вскрытия и осмотра объекта в двух экземплярах. Один экземпляр акта оставляется в ранее согласованном с заказчиком месте, второй – сдаётся вместе с дубликатами ключей на ПЦО (центр оперативного управления, группу обеспечения служебной деятельности нарядов).

Если перезакрытие охраняемого объекта производится в присутствии заказчика или его доверенного лица, акт перезакрытия не составляется.

При обращении заказчика на ПЦО по вопросам неисправности технических средств охраны, установленных на объекте, должностное лицо ПЦО разъясняет ему положения договора на оказание охранных услуг в части организации технического обслуживания средств охраны, а также рекомендует обратиться в обслуживающую организацию. Название и контактные телефоны обслуживающей организации рекомендуется вносить в оперативную карточку охраняемого объекта на этапе заключения договора на оказание охранных услуг и обновлять её по мере необходимости.

Также разработаны алгоритмы действий персонала ПЦО в нештатных, экстремальных и чрезвычайных ситуациях. К нештатным ситуациям относятся: выход из строя ТСО, отключение электропитания, неисправности коммуникационного оборудования и линий связи. В случае предполагаемого длительного периода восстановления электроснабжения или устранения неисправности телекоммуникационного оборудования и линий связи, сотрудники вневедомственной охраны обязаны принять меры по информированию заказчиков о временной невозможности предоставления охранных услуг. При стихийном бедствии природного и техногенного характера (пожаре, наводнении, землетрясении, урагане и т.п.) сотрудники, несущие службу на ПЦО, и работники ПЦО обязаны обеспечить максимально возможную охрану объектов в соответствии с условиями договора на оказание охранных услуг.

3.3 Организация несения службы сотрудниками групп задержания вневедомственной охраны Росгвардии

Группы задержания строевых подразделений вневедомственной охраны (далее – ГЗ) несут службу путём патрулирования обслуживаемых территорий по определённым маршрутам[1] и реагирования на сигналы «Тревога», поступающие с охраняемых объектов, подключённых к ПЦН. Сотрудники ГЗ передвигаются на служебных автомобилях, соот-

[1] Маршруты патрулирования ГЗ определяются сводной дислокацией, в которой отражается информация, необходимая для несения службы в течение смены.

ветствующих требованиям национального стандарта Российской Федерации[1]. Как правило, в состав одной ГЗ входят 2 сотрудника вневедомственной охраны. В регионах со сложной криминогенной обстановкой к несению службы могут привлекаться 3 сотрудника вневедомственной охраны.

Количество ГЗ определяется начальником подразделения вневедомственной охраны Росгвардии в пределах установленной штатной численности с учётом количества охраняемых объектов, надёжности работы систем сигнализации на объектах, подключённых к ПЦН, и обеспечения своевременного прибытия к этим объектам по сигналам «Тревога».

При несении службы ГЗ выполняют следующие задачи:

1. Отработка поступающей из центра оперативного управления (группы обеспечения служебной деятельности нарядов, ПЦО) информации о состоянии охраняемых объектов, расположенных в зоне реагирования группы задержания.

2. Предупреждение и предотвращение краж и иных правонарушений на охраняемых объектах, а в случаях их совершения – задержание правонарушителей «по горячим следам».

3. Повторное закрытие охраняемых объектов, не взятых под централизованное наблюдение, с которых поступил сигнал «Тревога», либо их охрана до выяснения причин срабатывания ТСО.

4. Охрана места происшествия до прибытия представителей органов следствия или дознания.

5. Оказание помощи другим нарядам строевых подразделений вневедомственной охраны при пресечении правонарушений.

6. Изучение специфики и расположения вновь принятых под охрану объектов.

Как правило, протяжённость маршрута патрулирования одной ГЗ составляет:

– до 8 км в населённых пунктах с населением свыше 500 тысяч человек или нагрузкой по количеству охраняемых объектов до 900 единиц;

– до 12 км в населённых пунктах с населением от 100 до 500 тысяч человек или нагрузкой по количеству охраняемых объектов до 600 единиц;

– до 15 км в населённых пунктах с населением до 100 тысяч человек или нагрузкой по количеству охраняемых объектов до 450 единиц.

[1] Автомобили, автобусы и мотоциклы оперативных служб. Цветографические схемы, опознавательные знаки, надписи, специальные световые и звуковые сигналы. Общие требования : ГОСТ Р 50574-2019 : национальный стандарт : дата введения 2019-07-01.

Протяжённость маршрутов патрулирования ГЗ может увеличиваться в зависимости от количества ГЗ и особенностей территории муниципального образования (района, поселения), в том числе нескольких муниципальных образований.

Зона реагирования ГЗ определяется с учётом количества охраняемых объектов, географических особенностей местности, состояния криминогенной обстановки, дорожного покрытия и должна предусматривать оперативное прибытие наряда к охраняемому объекту по сигналу «Тревога».

С разрешения дежурного центра оперативного управления (группы обеспечения служебной деятельности нарядов, ПЦО) либо лица, уполномоченного начальником подразделения вневедомственной охраны Росгвардии, допускается временное оставление маршрута патрулирования сотрудниками ГЗ в целях:

1) оперативного реагирования на сигналы «Тревога» с охраняемых объектов в границах территории, обслуживаемой строевым подразделением вневедомственной охраны;

2) оказания содействия другим нарядам строевых подразделений вневедомственной охраны при пресечении правонарушений;

3) задержания правонарушителей;

4) принятия мер к ликвидации пожара или иного чрезвычайного происшествия;

5) охраны места происшествия;

6) приёма пищи (в специально отведённом для этого месте).

В случае получения сигнала «Тревога» в момент охраны ГЗ места происшествия, задержания и доставления правонарушителей дежурный центра оперативного управления (группы обеспечения служебной деятельности нарядов, ПЦО) задействует для реагирования на поступивший сигнал другие наряды вневедомственной охраны.

ГЗ при несении службы находится в постоянной готовности к выезду по сигналам тревоги, поступившим с охраняемых объектов. При получении информации о срабатывании ТСО на охраняемом объекте старший ГЗ докладывает дежурному центра оперативного управления (группы обеспечения служебной деятельности нарядов), а при его отсутствии информирует дежурного пульта управления о своём местонахождении, подтверждает время получения сигнала и незамедлительно, кратчайшим путём, следует по указанному адресу. В пути следования старший ГЗ уточняет особенности охраняемого объекта и обеспечивает скрытое прибытие ГЗ к нему. О времени прибытия и начале осмотра с подтверждением адреса охраняемого объекта или при невозможности своевременно прибыть к охраняемому объекту старший ГЗ сообщает дежурному центра оперативного управления (группы обеспечения служебной деятельности нарядов) и действует по его указанию.

По прибытии ГЗ к охраняемому объекту:

– при помощи служебного транспортного средства блокируются пути отхода (выезда) правонарушителей с учётом особенностей охраняемых объектов;

– осуществляется скрытый подход к охраняемому объекту рассредоточено, предварительно заперев двери служебного транспортного средства, с соблюдением мер личной безопасности, взаимной страховки с обнажённым оружием, готовым к применению;

– производится осмотр периметра, уязвимых мест (дверей, окон, люков, крыш, чердачных, подвальных и смежных с охраняемым объектом помещений) и прилегающей территории;

– при следовании к охраняемому объекту производится осмотр окон, балконов, тыльной и фасадной сторон зданий (для обнаружения лестниц, канатов и иных предметов, используемых для проникновения), а также лестничных пролётов, подвальных и чердачных помещений, в ходе которого определяются места и способы проникновения на объект;

– при поступлении от дежурного центра оперативного управления (группы обеспечения служебной деятельности нарядов) информации о неисправности (аварии) электроснабжения или канала связи на охраняемом объекте дополнительно осматриваются соответствующие проводные линии и коммуникационные шкафы на предмет несанкционированного вмешательства и наличия имитирующих устройств.

В случае обнаружения правонарушителя или нарушения целостности охраняемого объекта старший ГЗ немедленно докладывает об этом и принимает меры по пресечению правонарушения, задержанию злоумышленника, установлению очевидцев и сохранению следов правонарушения.

Без разрешения уполномоченных лиц ГЗ запрещается покидать охраняемый объект до выяснения причин срабатывания ТСО, повторно закрывать охраняемый объект и сдавать его под охрану.

При невозможности восстановления работоспособности ТСО на охраняемом объекте ГЗ обеспечивает его охрану в соответствии с условиями заключенного договора на оказание охранных услуг.

Следует подчеркнуть, что помимо охраны объектов, подключённых к ПЦН вневедомственной охраны, ГЗ обеспечивают реагирование на информацию, поступающую из дежурных частей территориальных органов МВД России и частных охранных организаций, использующих СЦН и экономящих денежные средства на содержание мобильных групп охраны (групп быстрого реагирования).

Завершая рассмотрение данного раздела, необходимо отметить, что централизованная охрана является наиболее эффективным способом обеспечения безопасности объектов. Она основывается на использовании системы централизованного наблюдения и может сочетаться с ло-

кальной охраной органов внутренних дел. Безусловно, такая охрана также не лишена недостатков и зависит от своевременности, грамотности и слаженности действий сотрудников вневедомственной охраны Росгвардии.

Контрольные вопросы

1. Что понимается под техническим средством охраны?
2. Что понимается под пунктом централизованной охраны?
3. Что понимается под системой централизованного наблюдения?
4. Что должна обеспечивать система централизованного наблюдения?
5. Какие дополнительные функции могут иметь системы централизованного наблюдения?
6. Что входит в состав системы централизованного наблюдения?
7. Что понимается под системой передачи извещений?
8. Что должны обеспечивать системы передачи извещений?
9. Что понимается под подсистемой передачи информации?
10. Какой алгоритм действий сотрудников и работников вневедомственной охраны Росгвардии, реализуемый ими при поступлении на ПЦО сигнала «Тревога».
11. Какие действия обязан предпринять дежурный пульта управления при поступлении сигнала «Тревога»?
12. Какие задачи выполняет группа задержания при несении службы?
13. Какая протяжённость маршрута патрулирования одной ГЗ?
14. Какие действия выполняет ГЗ по прибытию к охраняемому объекту при поступлении сигнала «Тревога»?

4. СИСТЕМЫ ОХРАННОГО ТЕЛЕВИДЕНИЯ

Системы охранного телевидения (далее – СОТ) являются разновидностью систем видеонаблюдения. Они представляют собой телевизионные системы замкнутого типа, предназначенные для противокриминальной и антитеррористической защиты объекта.

Под системой видеонаблюдения понимается совокупность функционирующих видеоканалов, программных и технических средств записи и хранения видеоданных, а также программных и/или технических средств управления, осуществляющих информационный обмен между собой.

Видеоканал – совокупность технических средств СОТ, обеспечивающих передачу телевизионного изображения от видеокамеры до экрана видеомонитора в составе СОТ.

Видеоданные (видеоинформация, видеопоток) – аналоговый сигнал, несущий информацию о пространственно-временных параметрах изображений.

Если система видеонаблюдения использует программное обеспечение, реализующее алгоритмы автоматизированного получения различных данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей, то такую систему называют интеллектуальной. Видеоаналитика, основанная на искусственном интеллекте, позволяет существенно повысить эффективность работы персонала, осуществляющего текущий мониторинг. Кроме того, она способствует оперативному реагированию в случае нарушений установленных правил и границ, идентификации объектов, возникновения опасных ситуаций (попытки проникновения, нападения, пожара и т.д.), позволяет прогнозировать развитие событий, отслеживать ход проведения служебных проверок и другие действия пользователей, обусловленные возможностями конкретной телевизионной системы.

СОТ бывают аналоговые и цифровые.

В аналоговых СОТ видеосигнал от видеокамер до видеомониторов и/или видеорегистраторов передаётся в аналоговом виде, не подвергаясь аналого-цифровому преобразованию.

В цифровых СОТ используются кодеры и декодеры, конструктивно и функционально выделенные или объединенные с другими техническими средствами, а архив хранится в виде сжатых видеоданных.

Система, содержащая элементы аналоговой СОТ и цифровой СОТ, называется комбинированной СОТ.

СОТ систематизируют в зависимости:

– от функциональных возможностей,

– от устойчивости к несанкционированным действиям,

– от степени надёжности.

В зависимости от функциональных возможностей СОТ делят на три группы:

I – с ограниченными функциями,

II – с расширенными функциями,

III – многофункциональные.

По устойчивости к несанкционированным действиям (далее – НСД) СОТ классифицируют на три категории:

I – базовая устойчивость,

II – повышенная устойчивость,

III – высокая устойчивость.

По степени надёжности СОТ подразделяют на три группы:

I – базовая надёжность,

II – повышенная надёжность,

III – высокая надёжность.

СОТ должна обеспечивать:

– получение локального отображения и сохранения видеопотоков от одной или нескольких видеокамер;

– получение локального воспроизведения и сохранения аудиопотоков от одного или нескольких микрофонов, встроенных в видеокамеры или внешних;

– формирование архива в режимах непрерывной записи, записи по событиям (тревогам), записи по расписанию[1];

– автоматическую связь событий, регистрируемых видеосервером, с его автоматическими действиями, такими как включение/выключение формирования архива, выведение уведомления оператора на экран;

– хранение установленных параметров в энергонезависимой памяти при отключении напряжения питания;

– размер объектов на изображении не менее 5% высоты изображения (или не более 80 мм на пиксель изображения);

– возможность настройки автоматических реакций со стороны видеокамеры на фиксацию заданных событий;

– наличие встроенного настраиваемого детектора активности в зоне обзора видеокамеры[1];

---

[1] При заполнении архивом всего имеющегося объёма накопителя запись должна производиться циклически, автоматически замещая самые старые по времени данные. В определённых случаях может быть предусмотрена функция защиты фрагментов данных от перезаписи. Понятие «запись по расписанию» предполагает, что в заданные оператором промежутки времени запись может не производиться совсем, производиться непрерывно или производиться по событиям.

– наличие тревожных входов для подключения внешних извещателей, работающих по принципу «сухого контакта»[2];

– наличие тревожных выходов для подключения внешних исполнительных устройств.

В состав СОТ входят:

1) видеокамеры,

2) оборудование для обработки и записи информации,

3) устройства отображения видеоинформации,

4) каналы передачи информации,

5) вспомогательное оборудование.

Видеокамера – это устройство, предназначенное для телевизионного анализа передаваемой сцены при помощи оптоэлектронного преобразования и передачи телевизионного сигнала. Под сценой видеокамеры понимается часть пространства, телевизионный анализ которой осуществляется одной видеокамерой в определённый момент времени.

Видеокамеры бывают:

– аналоговые и цифровые,

– чёрно-белого и цветного изображения,

– для внутренней и наружной установки,

– стационарные и подвижные,

– корпусные и бескорпусные,

– для открытого и скрытого наблюдения,

– пониженной и повышенной чувствительности,

– стандартного и высокого разрешения[3],

– для применения в обычных и особых условиях.

Видеокамеры должны иметь следующие основные характеристики:

– разрешающая способность[4],

– рабочий диапазон освещённостей[5],

---

[1] Активность в зоне обзора видеокамеры может определяться как на аппаратном, так и на программном уровнях.

[2] Термин «сухой контакт» используется в области промышленной автоматики и сигнализации. Он обозначает дискретный выходной сигнал прибора. Слово «сухой» говорит о том, что на клеммах такого контакта нет никакого напряжения, если клеммы не подключены к другому оборудованию.

[3] Разрешение – свойство оцифрованных видеоданных, выражающее возможность различать на отдельных кадрах детали исходного изображения, которое определяется как количество пикселей (элементов изображения) по горизонтали и по вертикали, содержащихся в кадре.

[4] Разрешающая способность – максимальное число телевизионных линий, различаемых в выходном сигнале видеокамеры при глубине модуляции 10±3%.

[5] Рабочий диапазон освещенностей – диапазон освещённостей в поле зрения видеокамеры от минимальной до максимальной, в котором разрешающая способ-

– чувствительность[1],

– соотношение сигнал/шум,

– угол зрения по горизонтали и вертикали,

– параметры выходного видеосигнала,

– габаритные размеры и масса,

– вид климатического исполнения,

– характеристики, связанные с особенностями эксплуатации, показатели безопасности, надёжности, электромагнитной совместимости и другие необходимые параметры.

Видеокамеры должны иметь функционал, обеспечивающий повышение качества изображения в условиях слабых искажающих факторов и отслеживание движущихся объектов.

Важным элементом любой видеокамеры является объектив. **Объектив** – это устройство, формирующее изображение объекта в плоскости матрицы. К основным характеристикам объектива относят:

– фокусное расстояние[2],

– тип диафрагмы[3],

– максимальную апертуру[4],

– диапазон изменения диафрагмы,

– диапазон резкости,

– угол обзора.

Объективы могут быть:

– с фиксированной диафрагмой,

– с диафрагмой, управляемой вручную,

– с автоматически регулируемой диафрагмой,

ность и отношение сигнал/шум видеокамеры должны быть не менее заданных. Освещённость – это значение светового потока, приходящегося на единицу площади (измеряется в люксах).

[1] Чувствительность видеокамеры – это минимальная освещённость объекта наблюдения, позволяющая получать результирующее изображение с допустимым уровнем шумов (указывается в люксах). Чем меньше данный параметр, тем лучше камера «видит» в ночное время при прочих равных условиях.

[2] Фокусное расстояние – расстояние между оптическим центром линзы объектива и фокальной плоскостью матрицы видеокамеры при фокусировке объектива (измеряется в миллиметрах). Увеличение фокусного расстояния приводит к уменьшению угла обзора.

[3] Диафрагмой называется отверстие внутри объектива, через которое свет попадает на матрицу. Она может быть фиксированной и регулируемой. Основные свойства регулируемой диафрагмы заключаются в изменении количества света, попадающего на матрицу, и глубины резкости наблюдаемой сцены.

[4] Максимальная апертура объектива – это размер светового отверстия объектива, когда лепестки диафрагмы (лопасти, которые открываются и закрываются, чтобы дать больше или меньше света) широко открыты.

– с фиксированным фокусным расстоянием,

– с переменным фокусным расстоянием, регулируемым вручную,

– с фокусным расстоянием, управляемым посредством видеосервера (рекомендуется использовать его совместно с поворотным устройством).

Существуют видеокамеры с PTZ-функцией. PTZ-камеры оборудуются приводом для поворота, наклона и зумирования. Фактически функционал таких видеокамер заложен в их названии – Pan (панорама), Tilt (наклон), Zoom (зум).

Уличные видеокамеры помещаются в термокожухи, которые предохраняют их от внешних воздействующих факторов (перепадов температуры, влажности, осадков, несанкционированных действий и др.).

IP-камеры[1] отвечают за сканирование лица нового посетителя, обработку полученной модели и отклика системы. Специфические характеристики камер делят их на несколько видов в зависимости от функции, которую они выполняют в системе:

1. Обнаружение объекта – устройства выступают своего рода «сторожами» подконтрольной территории. Они не распознают лица, а лишь наводят на объект умные видеокамеры с более совершенными техническими характеристиками, которые и сканируют биометрические параметры гостя. Их устанавливают при входе на территорию для фиксации посетителей, используют для общей видеосъёмки. Их технические характеристики далеки от совершенства – фокусное расстояние до 1 мм, разрешение от 1 Мрх, – но для обнаружения проникновения на объект этого вполне достаточно.

2. Опознание – устройства берут за основу 3-4 основных биометрических параметра, по которому и осуществляется сканирование. Фокусное расстояние доходит до 6 мм, разрешение начинается от 2 Мрх.

3. Идентификация – такие камеры делают детальное сканирование лица по нескольким параметрам, чтобы полученное изображение высокого качества могло использоваться в более совершенной системе распознавания лиц. Фокусное расстояние колеблется от 8 до 12 мм, а разрешение – от 5 Мрх. Кроме фокусного расстояния и разрешения, на качество распознавания влияют количество источников света, адаптация камеры к плохому освещению, место её установки, угол обзора и средства защиты от негативных проявлений окружающей среды. Обычно камеры размещаются на проходной или в дверях производственного или коммерческого помещения. Оптимальное место – на уровне лица посе-

[1] IP-камера – цифровая видеокамера, особенностью которой является передача видеопотока в цифровом формате по сети Ethernet и TokenRing, использующей протокол IP. Каждая IP-камера в сети имеет свой IP-адрес.

тителя или под небольшим углом. Так можно обеспечить лучший угол обзора и качество распознавания.

В качестве оборудования для обработки и записи информации могут быть использованы видеосерверы либо видеорегистраторы.

Видеосервер – устройство в составе цифровой СОТ, предназначенное для преобразования аналогового видеосигнала с выхода видеокамер в цифровой формат с целью его обработки, передачи по компьютерной сети и/или записи на цифровой носитель информации.

В технической документации на видеосервер должны быть указаны:

– число подключаемых к видеосерверу видеокамер;

– алгоритм сжатия видеосигнала;

– скорость передачи видеоизображения (таблица соответствия разрешения кадра, числа каналов и скорости передачи видеоизображения);

– поддерживаемые сетевые протоколы;

– управление телеметрией (управление поворотным устройством видеокамеры, изменение фокусного расстояния объектива и др.);

– наличие и характеристики встроенных функций детектора движения;

– возможность подключения к видеосерверу внешних охранных датчиков (электрические характеристики входных цепей);

– сохранение текущей видеоинформации (видеобуфер «предтревожной записи» и его параметры);

– возможность передачи аудиоинформации;

– характеристики, связанные с особенностями применения и эксплуатации видеосерверов, показатели их безопасности, надёжности и электромагнитной совместимости.

В комплект поставки видеосервера может входить программное обеспечение, предоставляющее возможность просмотра видеоизображения и управления видеокамерами с сетевого компьютера, на котором установлен стандартный веб-браузер.

Видеосервер должен обеспечивать поддержку двухпоточности[1], если это предусмотрено применяемыми техническими средствами. Для передачи по сети должен выбираться видеопоток максимально низкого

[1] Двухпоточность – свойство IP-видеокамер и устройств кодирования видео предоставлять два видеопотока различного качества для каждого канала видео. Поток высокого разрешения используется для сохранения в архив и для отображения в полноэкранном режиме. Поток низкого разрешения используется для отображения в режиме мультиэкрана. В общем случае возможно предоставление более двух потоков.

разрешения, но достаточного для реализации требуемой функциональности.

Передача аудио- и видеоинформации по сети должна осуществляться только в случае наличия пользователей, у которых периодически возникает потребность в данной информации. Потоки, которые в определённый момент времени не требуются для отображения, записи или работы других алгоритмов, не должны передаваться по сети.

Для снижения нагрузки на сеть передачи данных необходимо применять широковещательную передачу аудио- и видеоинформации.

Видеосервер должен использовать алгоритмы сжатия без потерь с целью сохранения исходного качества для локальной обработки и применения видеоаналитики.

При использовании собственного аналого-цифрового преобразователя видеосервер должен реализовывать алгоритмы компрессии видео с покадровым сжатием. Например, MJPEG для удалённой передачи видео со скоростью не более 5 Мбит/с и с сохранением возможности применения видеоаналитики. Кроме того, он также должен реализовывать алгоритмы компрессии видео с межкадровым сжатием – например, H.264 или MPEG-4 для эффективной удалённой передачи видео со скоростью не более 10 Мбит/с. В противном случае видеосервер должен использовать алгоритм сжатия, применяемый в устройстве предоставления видеосигнала, например, видеокамере.

Видеосервер должен обеспечивать:

1. Распределённую обработку изображения:

– с ограниченными возможностями администрирования;

– с полнофункциональными возможностями администрирования с центральным хранением конфигурации;

– с полнофункциональными возможностями администрирования с распределённым хранением конфигурации.

2. Оперативное отображение видеоинформации.

3. Оптимизацию использования машинных носителей для хранения архива аудио- и видеоинформации.

4. Отказоустойчивое хранение данных.

5. Доступ к архиву аудио- и видеоинформации.

6. Протоколирование[1]:

– всех действий операторов по изменению настроек (конфигурации) СОТ и её компонентов;

– попыток подбора пароля для доступа к видеосерверу;

– всех регистрируемых событий (неисправность оборудования, срабатывание встроенной или внешней видеоаналитики и др.).

[1] Протоколирование – это процесс записи в энергонезависимую память регистрируемых СОТ событий, осуществляемый в хронологическом порядке.

7. Отображение планов охраняемых зданий, помещений и участков местности как в ручном режиме (по команде оператора), так и в автоматическом при регистрации заданного события или тревоги.

8. Мониторинг работоспособности машинных носителей информации, а также доступности и работоспособности технических средств СОТ.

Видеорегистратор – устройство, предназначенное для записи, хранения и воспроизведения видеоинформации. Техника такого рода работает по следующему принципу: видеокамеры подключаются к видеорегистратору и передают на него видео по кабелям. Регистратор получает видеосигналы, преобразует их в изображение, сжимает и записывает на машинный носитель. Просмотреть видео можно, подключив к видеорегистратору телевизор или монитор, а также используя удалённое подключение.

Существует несколько видов видеорегистраторов для систем видеонаблюдения:

– аналоговые регистраторы (работают исключительно с аналоговыми видеокамерами);

– сетевые регистраторы (работают только с IP-видеокамерами);

– гибридные регистраторы (работают с аналоговыми и цифровыми видеокамерами).

Различные виды видеорегистраторов выполняют следующие функции:

– сжатие видеосигнала по специальному алгоритму и его запись;

– запись аудиосигналов от микрофонов;

– передача данных через LAN порт;

– обработка сигналов от датчиков движения и подача тревожного сигнала;

– вывод картинки на один или несколько мониторов.

Основные характеристики видеорегистраторов:

– количество видеоканалов;

– количество аудиоканалов;

– максимальная частота кадров;

– максимальное разрешение записи;

– поддерживаемые кодеки;

– количество и максимальный объём носителей информации;

– скорость сети Ethernet (для сетевых и гибридных регистраторов).

Устройства отображения видеоинформации (видеомониторы) бывают для индивидуального и коллективного пользования.

Время отклика видеомониторов, предназначенных для наблюдения за движущимися объектами, должно быть не более 16 мс.

Выбор размера видеомонитора зависит от числа камер, изображения с которых будут одновременно транслироваться на экран. Для отображения изображений с нескольких видеокамер рекомендуется использовать видеомониторы, у которых размер не менее 21 дюйма[1] и разрешение не менее 1920×1080 пикселей (формат Full HD). Если в СОТ 16 и более видеокамер, то лучше использовать видеомонитор с диагональю не менее 27 дюймов и разрешением не менее 2560×1440 пикселей.

При осуществлении круглосуточного мониторинга устройство отображения должно:

– иметь срок службы не менее 6 лет;

– обеспечивать работу с композитным видеосигналом;

– иметь возможность коррекции диапазона яркости для того, чтобы сделать его шире (коррекция нужна для полного отображения сигнала, поступающего с видеокамеры);

– иметь схему синхронизации сигнала яркости и цветности.

У любого видеомонитора должны быть указаны следующие основные характеристики:

– размер экрана;

– параметры экрана;

– разрешающая способность экрана;

– цветность (цветной/чёрно-белый);

– параметры видеовхода (тип видеоинтерфейса для компьютерного монитора);

– параметры, связанные с особенностями эксплуатации, показатели безопасности, надёжности, электромагнитной совместимости.

Отображение видеоинформации должно осуществляться как в полноэкранном режиме (одна камера на один монитор), так и в режиме мультиэкрана[2] в произвольном шаблоне, выбранном оператором. При этом должна предоставляться возможность коммутации видеопотоков[3] и окон отображения мультиэкрана.

На видеомонитор выводится следующая информация:

– текущая дата;

– текущее время;

– номер и/или имя отображаемой видеокамеры или воспроизводимого аудиопотока, настроенных на режим формирования архива.

---

[1] Под дюймом обычно подразумевают используемый в США английский дюйм (англ. inch), в точности равный 2,54 см.

[2] Мультиэкран – режим для отображения на экране изображений от нескольких видеокамер.

[3] Коммутация видеопотоков – соотнесение видеопотоков с конкретными окнами отображения.

Каналы передачи информации необходимы для трансляции видео- и аудиопотоков, управления видеокамерами и контроля функционирования СОТ. Информация может передаваться как по проводным, так и по беспроводным каналам связи.

Для проводных каналов применяют кабели с носителями электрических зарядов, сделанными из меди, либо оптические волокна. В основном в СОТ используются именно такие каналы. Если на охраняемых объектах невозможно или нецелесообразно прокладывать кабели, то применяются беспроводные каналы, в которых информация передаётся при помощи технологий Wi-Fi и 3G/4G. В редких случаях используются параболические антенны, рассчитанные на работу с частотами от 18 до 24 ГГц.

К вспомогательному оборудованию СОТ можно отнести детекторы движения, прожекторы, тепловизоры, поворотные устройства, резервные источники электропитания и прочие технические средства.

Детекторы движения предназначены для формирования сигнала извещения о тревоге при обнаружении движения в поле зрения видеокамеры. Детекторы встраиваются в видеокамеры или производятся как отдельные устройства (наиболее часто в качестве детекторов движения применяются активные инфракрасные датчики). Также движение каких-то объектов, попадающих в объектив видеокамеры, может быть обнаружено при помощи программного обеспечения.

Для достижения необходимого уровня освещённости сцены видеокамеры широко используются прожекторы (осветители). Кроме обычных осветителей существуют инфракрасные прожекторы (ИК-прожекторы). ИК-прожекторы могут быть встроены в корпус видеокамеры и изготовлены как отдельное устройство. Они позволяют осуществлять скрытую или полускрытую подсветку объектов. При скрытой подсветке длина излучаемой волны должна быть в диапазоне от 940 до 950 нм, при полускрытой подсветке – в диапазоне от 850 до 880 нм. ИК-прожекторы должны работать при освещённости менее 15 лк.

В состав СОТ могут входить тепловизоры[1], которые способны:

– работать в сложных условиях (в полной темноте; во время тумана, снегопада, дождя, песчаной бури; в условиях задымления и буйной растительности);

– обнаружить опасные объекты и события на больших расстояниях;

– снизить количество ложных тревог;

– решить проблему встречной засветки (лучами солнца, фарами и т.д.);

[1] Тепловизор – устройство, регистрирующее тепловое излучение объекта наблюдения и преобразующее его в изображение.

– обеспечить скрытое наблюдение (в данном случае подсветка не требуется).

Поворотные устройства обеспечивают перемещение (сканирование) видеокамеры или другого устройства по осям пространственных координат по командам оператора или в соответствии с заранее заданным алгоритмом. К основным характеристикам поворотных устройств относят:

– число плоскостей сканирования,

– максимальный угол поворота,

– скорость поворота,

– точность установки,

– максимальную нагрузку.

При пропадании напряжения в сети переменного тока СОТ должна подключиться к резервному источнику электропитания. Резервный источник электропитания должен обеспечивать выполнение основных функций СОТ при пропадании напряжения в сети на время не менее 0,5 часа при условии устранения неисправности основного электропитания в течение этого времени. СОТ должны сохранять работоспособность при допустимых отклонениях напряжения резервного источника электропитания от минус 15% до плюс 10% номинального значения. В качестве резервного источника электропитания может применяться генераторная установка либо источники электропитания постоянного тока. При использовании в качестве источника резервного электропитания аккумуляторных батарей их зарядка должна осуществляться автоматически.

Таким образом, СОТ является обязательным и неотъемлемым компонентом современной системы безопасности. Она осуществляет наблюдение за охраняемыми объектами, позволяет предотвратить потенциальные противоправные действия (несанкционированное проникновение на подконтрольную территорию, возникновение возгорания, аварии и др.) и, как следствие, служит значимым инструментом при установлении обстоятельств происшествия либо преступления. Записи, полученные с видеокамер, позволяют без труда восстановить хронологию событий произошедшего.

Главное преимущество СОТ – оперативное реагирование на возможные угрозы в режиме реального времени и мгновенное принятие мер по обеспечению безопасности.

Чтобы СОТ полноценно выполняла задачу видеоохраны, важно грамотно определить места установки и тип видеокамер. Кроме того, необходимо в полной мере использовать возможности видеоаналитики и обеспечить интеграцию СОТ с другими системами, осуществляющими безопасность охраняемого объекта. Крайне важно, чтобы пользователи СОТ являлись квалифицированными специалистами, способными изучить полученную информацию и принять соответствующие решения.

Контрольные вопросы

1. Что понимается под системой охранного телевидения?
2. Какие преимущества имеет система СОТ в охране?
3. Что понимается под видеоканалом?
4. Какие существуют виды СОТ в зависимости от функциональных возможностей?
5. Что обеспечивает СОТ?
6. Что входит в состав СОТ?
7. Какие существуют виды видеокамер, которые могут входить в состав СОТ?
8. Что понимается под видеосервером в составе СОТ?
9. Что должен обеспечивать видеосервер СОТ?
10. Что понимается под видеорегистратором в составе СОТ?
11. Какие функции выполняют видеорегистраторы СОТ?
12. Какие существуют характеристики видеорегистраторов СОТ?
13. Какие функции выполняют тепловизоры в составе СОТ?

5. СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Системы контроля и управления доступом предназначены для предотвращения несанкционированного доступа людей, транспорта и других объектов в зону (из зоны) доступа (здания, помещения, территории, транспортные средства) в целях обеспечения противокриминальной защиты.

Аутентификация – процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта.

Идентификация – процесс опознавания субъекта или объекта по присущему или присвоенному ему идентификационному признаку. Под идентификацией понимают также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Контроллер доступа (КД), **прибор приемно-контрольный доступа** (ППКД) – аппаратное устройство в составе средств управления СКУД.

Контроль и управление доступом (КУД) – комплекс мероприятий, направленных на предотвращение несанкционированного доступа.

Криминальная безопасность – состояние объекта защиты, при котором отсутствует недопустимый риск, связанный с причинением ему вреда от реализации криминальной угрозы.

Система контроля и управления доступом (СКУД) – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Средства управления (СУ) – аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации.

Средства контроля и управления доступом (средства КУД) – механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом.

В зависимости от разных признаков средства КУД подразделяют:

1. По функциональному назначению устройств:

– устройства преграждающие управляемые;

– устройства исполнительные;

– устройства считывающие;

– идентификаторы (ИД);

– средства управления в составе аппаратных устройств и программных средств.

2. По функциональным характеристикам:

– **устройства преграждающие управляемые** (УПУ) – устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием. В зависимости от вида перекрытия проема прохода выделяют УПУ с частичным перекрытием (турникеты, шлагбаумы); с полным перекрытием (полноростовые турникеты, специализированные ворота); со сплошным перекрытием проема (сплошные двери, ворота); с блокированием объекта в проеме (шлюзы, кабины проходные);

– **устройства исполнительные** (УИ) – устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ. В зависимости от способа запирания УИ делятся на электромеханические замки, электромагнитные замки, электромагнитные защелки, механизмы привода дверей, ворот.

– **идентификаторы и считыватели** – по следующим признакам:

– механическими – представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);

– магнитными – представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т.д.);

– оптическими – представляют собой нанесенные на поверхность или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т.д.);

– электронными контактными – представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т.д.);

– электронными радиочастотными – считывание кода с электронных идентификаторов происходит путем передачи данных по радиоканалу;

– акустическими – представляют собой кодированный акустический сигнал;

– биометрическими (только для считывателей) – представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрию ладони, рисунок сетчатки глаза, голос, динамику подписи и т.д.);

– комбинированными – для идентификации используют одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков считыва-

тели могут быть:

– с ручным вводом – ввод осуществляется с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;

– контактными – ввод происходит при непосредственном, в том числе и при электрическом, контакте между считывателем и идентификатором;

– бесконтактными – считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю;

– комбинированными.

3. По устойчивости к несанкционированному доступу.

Данная классификация основана на устойчивости к разрушающим и неразрушающим воздействиям по уровням устойчивости:

– нормальной;

– повышенной;

– высокой.

В состав СКУД могут входить другие дополнительные средства: источники электропитания, датчики (извещатели) состояния УПУ, дверные доводчики, световые и звуковые оповещатели, кнопки ручного управления УПУ, устройства преобразования интерфейсов сетей связи, аппаратура передачи данных по различным каналам связи и другие устройства, предназначенные для обеспечения работы СКУД.

В состав СКУД могут входить также аппаратно-программные средства – средства вычислительной техники (СВТ) общего назначения (компьютерное оборудование, оборудование для компьютерных сетей, общее программное обеспечение).

Классификация средств управления СКУД включает в себя:

– аппаратные средства (устройства) – контроллеры доступа, приборы приемно-контрольные доступа (ППКД);

– программные средства – программное обеспечение СКУД.

СКУД классифицируют по:

1. Способу управления:

– автономные – для управления одним или несколькими УПУ без передачи информации на центральное устройство управления и контроля со стороны оператора;

– централизованные (сетевые) – для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;

– универсальные (сетевые) – 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. Числу контролируемых точек доступа:

– малой емкости (не более 64 точек),

– средней емкости (от 64 до 256 точек),

– большой емкости (более 256 точек).

3. Функциональным характеристикам:

1-й – системы с ограниченными функциями,

2-й – системы с расширенными функциями,

3-й – многофункциональные системы.

Средства и системы КУД должны обеспечивать возможность непрерывной работы с учетом проведения регламентного технического обслуживания.

Системы КУД в рабочем режиме должны обеспечивать автоматическую работу. Режим ручного или автоматизированного управления (с участием оператора) должен обеспечиваться только при возникновении чрезвычайных, аварийных или тревожных ситуаций, а также по требованию заказчика.

Средства и системы КУД в составе систем противокриминальной защиты объектов должны обеспечивать:

– защиту от несанкционированного доступа на охраняемый объект (помещение, зону) в режиме снятия их с охраны;

– контроль и учет доступа персонала (посетителей) на охраняемый объект (помещение, зону) в режиме снятия их с охраны;

– автоматизацию процессов взятия/снятия охраняемого объекта (помещения, зоны) с помощью средств идентификации СКУД в составе устройств и приборов охранной сигнализации;

– защиту и контроль доступа к компьютерам автоматизированных рабочих мест (АРМ) пультового оборудования систем охранной сигнализации;

– защиту от НСД к информации.

К функциональным характеристикам СКУД предъявляются требования.

Автономные СКУД должны обеспечивать:

– выдачу сигнала на открывание УПУ при считывании зарегистрированного в памяти системы идентификационного признака;

– запрет открывания УПУ при считывании незарегистрированного в памяти системы идентификационного признака;

– запись идентификационных признаков в память системы;

– защиту от несанкционированного доступа при записи кодов идентификационных признаков в памяти системы;

– сохранение идентификационных признаков в памяти системы при отказе и отключении электропитания;

– ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и пра-

вилами противопожарной безопасности;

– автоматическое формирование сигнала закрытия на УПУ при отсутствии факта прохода;

– выдачу сигнала тревоги при аварийном открывании УПУ для несанкционированного проникновения.

СКУД с централизованным управлением и универсальные должны соответствовать общим функциональным требованиям для автономных систем и дополнительно обеспечивать:

– работу в локальной сети контроллеров СКУД;

– регистрацию и протоколирование тревожных и текущих событий;

– приоритетное отображение на экране управляющего компьютера тревожных событий;

– управление работой УПУ в точках доступа по командам оператора;

– задание временных режимов действия идентификаторов в точках доступа и уровней доступа;

– защиту технических и программных средств от несанкционированного доступа к элементам управления, к установке режимов и к информации;

– автоматический контроль исправности средств, входящих в систему, и линий передачи информации;

– возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;

– установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т.п.);

– блокировку прохода по точкам доступа командой с пункта управления в случае нападения;

– возможность подключения дополнительных средств специального контроля, средств досмотра.

Универсальные системы должны обеспечивать автономную работу при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи, а также восстановление режимов работы после устранения отказов и восстановление связи.

Таким образом, СКУД осуществляет контроль доступа к ее объектам и отслеживает перемещение посетителей, персонала и транспорта на охраняемой территории. Использование СКУД является одним из наиболее действенных методов, обеспечивающих безопасность защищаемых объектов и предотвращающих несанкционированный доступ в подконтрольную зону.

СКУД существенно упрощает процедуру идентификации и аутентификации, значительно экономит время и повышает эффективность работы сотрудников оперативных служб. Тем не менее, при всех своих преимуществах система, так или иначе, требует пристального контроля со стороны ее пользователей.

Контрольные вопросы

1. Что такое система контроля и управления доступом?
2. Что понимается под средствами контроля и управления доступом?
3. Какие существуют виды средств КУД в зависимости от функционального назначения устройства?
4. Какие существуют виды средств КУД в зависимости от функциональных характеристик устройства?
5. Какой принцип работы системы контроля и управления доступом?
6. Какие задачи решает система контроля и управления доступом?
7. Какие существуют средства контроля и управления доступом?
8. Какие дополнительные средства могут входить в состав СКУД?
9. Что понимается под термином «идентификация»?
10. Что понимается под термином «аутентификация»?
11. Какие существуют задачи средств и систем КУД в составе систем противокриминальной защиты объектов?
12. Что понимается под устройствами преграждающими управляемыми?
13. Что понимается под устройствами исполнительными?
14. Какие существуют виды идентификаторов и считывателей?
15. Какая существует классификация СКУД?

6. КОМПЛЕКСНЫЕ И ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

6.1 Понятие, назначение, состав комплексных систем безопасности

Комплексная система безопасности (КСБ) –специализированная сложная организационно-техническая открытая система, проектируемая для конкретного объекта, состоящая из алгоритмически объединенных (интегрированных) целевых функционально самостоятельных технических подсистем и средств, предназначенных для комплексной защиты объекта от различных угроз (от техногенных аварий, пожаров, криминальных проявлений, нештатных (сверхнормативных) природно-климатических воздействий, последствий стихийных бедствий, ошибочных (случайных или преднамеренных) действий людей, в т.ч. персонала объекта.

КСБ объектов представляют собой алгоритмически упорядоченные и взаимосвязанные совокупности централизованно управляемых функционально самостоятельных технических подсистем конкретного целевого назначения, а также средств инженерного обеспечения объектов и занимаемой ими территории.

В состав КСБ должны входить такие технические подсистемы, как:

– дежурно-диспетчерская,

– производственно-технологического контроля,

– охранной и тревожной сигнализации,

– пожарной сигнализации,

– контроля и управления доступом,

– теле/видеонаблюдения и контроля,

– досмотра и поиска,

– пожарной автоматики (пожаротушения, противодымной защиты, оповещения, эвакуации),

– связи с объектом,

– защиты информации,

– инженерно-технических средств физической защиты,

– инженерного обеспечения объекта (электроосвещения и электропитания, газоснабжения, водоснабжения, канализации, теплоснабжения, вентиляции, кондиционирования).

В случае возникновения на объекте чрезвычайной ситуации технические средства подсистем КСБ должны обеспечивать формирование служебного или тревожного извещения для оповещения персонала и других людей, находящихся на объекте, а при необходимости – передачу извещения в ЕДДС.

Для передачи тревожных и служебных извещений и сообщений в КСБ применяют специально проложенные проводные линии; выделенные и переключаемые телефонные линии городской телефонной сети и внутренних автоматических телефонных станций объекта; радио- и телевизионные каналы; радиотрансляционные сети, сети электропитания, оптоволоконную и лазерную технику.

Для передачи визуальной и акустической информации применяют звуковую и световую технику, факсимильную связь.

6.2 Понятие, назначение, состав интегрированных систем безопасности

Интегрированная система безопасности (ИСБ) – разрабатываемая специализированная сложная техническая система, объединяющая (интегрирующая) целевые функциональные технические подсистемы и средства, предназначенные для комплексной защиты объекта от различных угроз, с общей информационной средой и единой базой данных на основе единого программно-аппаратного комплекса.

ИСБ должны быть рассчитаны на непрерывную круглосуточную работу и иметь возможность восстановления работоспособного состояния после отказа в процессе эксплуатации.

ИСБ разрабатывают на основе функциональных модулей, позволяющих формировать функционально ориентированные блоки, образующие ИСБ с заданной конфигурацией, обеспечивающей возможность адаптации функциональных возможностей под конкретные условия практического применения на объекте.

Возможно использование ИСБ в составе КСБ объектов в качестве базовой технической подсистемы.

Состав технических подсистем ИСБ на основе функциональных блоков аналогичен составу технических подсистем КСБ:

– дежурно-диспетчерская,
– производственно-технологического контроля,
– охранной и тревожной сигнализации,
– пожарной сигнализации,
– контроля и управления доступом,
– теле/видеонаблюдения и контроля,
– досмотра и поиска,
– пожарной автоматики (пожаротушения, противодымной защиты, оповещения, эвакуации),
– связи с объектом,
– защиты информации,
– инженерно-технических средств физической защиты,
– инженерного обеспечения объекта.

6.3 Требования к техническим подсистемам и средствам КСБ и ИСБ

Дежурно-диспетчерские подсистемы (ДДП) могут быть централизованными либо строиться по зонально-кустовому принципу, образуя сеть локальных пунктов, передающих информацию в центральный пункт.

ДДП для обеспечения безопасности объекта в контрольных зонах должна осуществлять:

– технический контроль обстановки с постоянной периодичностью;

– регистрацию и анализ информации о состоянии и текущей обстановке;

– непрерывную техническую связь по контролю общей обстановки на объекте;

– доведение полученной информации о возникшей нештатной, угрожающей или чрезвычайной ситуации на объекте или вблизи объекта до функциональных профильных служб объекта по принадлежности, а также при необходимости до пункта административно-территориальной ЕДДС в нормированный срок с документированной регистрацией даты и времени передачи и получения подтверждения поступления информации;

– получение из ЕДДС управляющих команд по обстановке и последующим действиям на объекте.

Подсистемы производственно-технологического контроля

Основное назначение подсистем производственно-технологического контроля – предельно возможное снижение угроз нанесения ущерба (вреда) объекту из-за технологических/технических и возможных природно-климатических причин при обязательном соблюдении принципа «равнопрочности» относительно обеспечения защищенности на всех этапах контроля.

Идентификация результатов производственно-технологического контроля является обязательным этапом контроля с целью определения и устранения причин выявленных нарушений (несоответствий) в состоянии объекта, в деятельности и поведении людей, т.е. для отслеживания результатов контроля и предотвращения повторных нарушений (несоответствий).

Подсистемы сигнализации

Подсистемы сигнализации могут использоваться как централизованные, так и автономные в зависимости от конкретных условий и особенностей процессов деятельности на объекте.

Функциональное назначение, целевые свойства, режимы работы, состав и техническое построение подсистем сигнализации на объекте определяются видами угроз, информация о которых должна регистриро-

ваться и передаваться (аварийно-технологическая, охранная, пожарная, тревожная, комбинированная).

Более подробно мы рассматривали системы сигнализации в разделе 2 «Системы сигнализации, устанавливаемые на охраняемых объектах».

Подсистемы контроля и управления доступом

Подсистемы контроля и управления доступом должны предотвращать несанкционированный доступ в контрольные зоны объекта с ограниченным доступом, не создавая препятствий для прохода в зоны со свободным доступом.

Подсистемы контроля и управления доступом должны обеспечивать необходимые условия соблюдения внутриобъектового режима и выполнения соответствующих обязанностей персоналом объекта в зависимости от конкретных условий и особенностей процессов деятельности на объекте, пребывания на нем людей, транспортных средств.

Более подробно мы рассматривали системы сигнализации в разделе 5 «Системы контроля и управления доступом».

Подсистемы теле/видеонаблюдения и видеоконтроля

Подсистемы теле/видеонаблюдения и видеоконтроля должны обеспечивать визуальное наблюдение ситуационной обстановки в заданном формате изображения, обнаружение и идентификацию субъектов наблюдения в зависимости от назначения – людей, транспортных средств, имущества, элементов объектовой инфраструктуры, а также визуальное документирование и архивирование получаемой видеоинформации.

Видеоинформация из контрольных зон объекта должна поступать в локальные и (или) централизованные пункты ДДП для верификации и регистрации.

Более подробно мы рассматривали системы сигнализации в разделе 4 «Системы охранного телевидения».

Подсистемы досмотра и поиска

Подсистемы досмотра и поиска могут включать в себя досмотровые шлюзовые кабины, стационарные и (или) передвижные (переносные) обнаружители несанкционированного перемещения подконтрольных предметов, веществ и материалов (например, металлообнаружители, интроскопы, спектрометры, радиометры, дефектоскопы, тепловизоры) в зависимости от конкретных условий и особенностей процессов деятельности на объекте.

Подсистемы автоматического пожаротушения должны обеспечивать:

– срабатывание в течение времени, меньшего начальной стадии развития пожара;

– локализацию пожара в течение времени, необходимого для вве-

дения в действие оперативных сил и средств пожаротушения объекта;

– тушение пожара с целью его ликвидации;

– необходимую интенсивность подачи и/или концентрацию тушащего вещества;

– надёжность функционирования в реальных условиях эксплуатации на объекте.

Подсистемы противодымной защиты должны обеспечивать:

– защиту людей и помещений объекта от повышенной концентрации дыма, токсичных летучих продуктов горения, нагретого до опасной для здоровья человека температуры воздуха (не более 60° С в тёплое время года);

– возможность своевременной эвакуации людей из помещений в начальной стадии возникшего пожара.

Подсистемы противодымной защиты должны включаться автоматически (дистанционно) от подсистемы пожарной сигнализации или вручную персоналом объекта.

Подсистема связи и подсистема оповещения предназначены для оперативного управления и координации действий персонала, а также при необходимости для оповещения и руководства действиями других людей, санкционированно находящихся на объекте.

Подсистемы связи и оповещения КСБ объекта должны включать: абонентскую телефонную связь, радиосвязь, громкую связь, телефаксы, мобильные телефоны, пейджеры, переговорные устройства, средства свето- и звуковой индикации, пневмопочту.

Подсистема управления эвакуацией людей осуществляет:

– передачу речевой информации о необходимости эвакуации в предусмотренном для этого направлении движения, например, через эвакуационные или аварийные выходы, а также передачу специальных текстов, предназначенных для управления поведенческой динамикой людей в целях обеспечения их безопасности;

– включение световых указателей на рекомендуемом пути и направлении эвакуации через эвакуационные или аварийные выходы;

– дистанционное управление электромагнитных запирающих устройств и замков, дверей и ворот, управляемых преграждающих устройств подсистем КУД на путях эвакуации;

– передачу оперативных команд по действиям групп людей или отдельных людей на различных участках эвакуационных путей по результатам наблюдения в подсистеме теле/видеонаблюдения и видеоконтроля.

Подсистема защиты информации предназначена для обеспечения информационной и компьютерной безопасности на объекте. Она должна включать в себя средства физической и электронной защиты в зависимости от места расположения объекта, конкретных условий и

особенностей процессов деятельности на объекте, действующего внутриобъектового режима, наличия инженерно-технических средств физической защиты.

Инженерно-технические средства физической защиты объекта должны препятствовать несанкционированному проникновению (проходу, проезду) в контрольные зоны объекта с ограниченным доступом. К ним относят:

– средства инженерной защиты территории или участков территории объекта (барьеры, ограждения, заграждения, противотаранные устройства защиты от удара колёсным автотранспортом, строительно-земляные сооружения, естественные природные препятствия);

– средства технической укреплённости (защитные конструкции) оконных и дверных проёмов, а также строительных панелей и перекрытий зданий, строений, сооружений на территории объекта, обладающие повышенными прочностными свойствами.

Защитные конструкции могут быть металлическими, неметаллическими и комбинированными: ворота, двери, ставни, жалюзи, роллеты, экраны, шторы, решетки, сетки.

Подсистемы инженерного обеспечения объекта

Средства электроосвещения. На объекте должны быть установлены рабочее, дежурное, аварийное, тревожное, эвакуационное виды электроосвещения.

Рабочее электроосвещение должно стабильно обеспечивать работу подсистем теле/видеонаблюдения и видеоконтроля, освещение контрольных, в том числе рекреационных зон в соответствии с санитарными нормами в сумеречное, вечернее и ночное время суток в любых климатических и метеорологических условиях.

Дежурное освещение должно обеспечивать достаточный визуальный контроль ситуационной обстановки в контрольных зонах, на маршрутах передвижения дежурного персонала объекта.

Тревожное электроосвещение предназначено для обеспечения дополнительных условий верификации нештатных, угрожающих или чрезвычайных событий в контрольных зонах и не должно иметь постоянного режима работы. Тревожное освещение выполняет сигнальную функцию.

Сеть тревожного освещения должна выполняться отдельно от сетей рабочего и дежурного освещения и давать возможность выборочного включения в контрольных зонах объекта.

Аварийное электроосвещение объекта предназначено для работы при возникновении нештатной или чрезвычайной ситуации и отключении основного (рабочего) электроосвещения. Оно не должно иметь постоянного режима работы.

Аварийное освещение выполняет сигнальную функцию и должно размещаться в контрольных зонах с повышенной опасностью возникно-

вения технологических аварий, чрезвычайной ситуации, в местах работы подсистем производственно-технологического контроля.

Осветительные приборы аварийного освещения должны конструктивно отличаться от иных осветительных приборов.

Переключение с рабочего освещения на аварийное и обратно должно быть автоматическим.

Эвакуационное электроосвещение предназначено для использования только в условиях чрезвычайной ситуации в контрольных зонах и при необходимости в условиях своевременной и безопасной эвакуации людей с объекта.

Эвакуационное электроосвещение должно работать автономно от всех других видов электроосвещения на объекте и иметь отличительные от рабочего освещения конструктивные решения.

Устройства электропитания технических подсистем и средств устанавливают в специально оборудованных помещениях с ограниченным доступом людей. Помещения с устройствами электропитания должны иметь пояснительные и предупреждающие надписи, мнемосхемы, пиктограммы, знаки по электробезопасности.

При мониторинге **сетей и сооружений водо-, газоснабжения, канализации и поддержания микроклимата в помещениях** (отопление, вентиляция, кондиционирование), а также официально разрешенных к применению на объекте электробытовых приборов постоянного использования проверяется их исполнение, техническое состояние и наличие документов, подтверждающих их электрическую, санитарно-гигиеническую и пожарную безопасность, а также обеспечение условий для контроля рабочих и потребительских характеристик и параметров в пределах действующих норм безопасности.

Таким образом, можно прийти к выводу, что безопасность не должна существовать как отдельный компонент системы, а должна быть внедрена фактически в каждый из этапов ее функционирования. Для оптимизации работы по всестороннему обеспечению безопасности того или иного объекта требуется интеграция всевозможных технических средств, повышение квалификации персонала для работы с ними и разработка системы мониторинга.

Комплексные и интегрированные системы безопасности – основные инструменты для обеспечения защиты информационных систем и данных. При их использовании возможность возникновения нештатных ситуаций и инцидентов, угроз и рисков значительно меньше, а уровень безопасности информации существенно выше. Важно отметить, что в ходе работы с КСБ и ИСБ предполагается не только предотвращение угроз различного характера – от угроз физической безопасности до информационной, но и выстраивание алгоритма действий при их возникновении.

Контрольные вопросы

1. Что понимается под комплексной системой безопасности?
2. Какие технические подсистемы входят в состав КСБ?
3. Что должны обеспечивать технические средства подсистем КСБ в случае возникновения на объекте чрезвычайной ситуации?
4. Какие каналы связи используются в КСБ для передачи тревожных и служебных извещений и сообщений?
5. Что понимается под интегрированной системой безопасности?
6. На основе каких модулей разрабатывают ИСБ?
7. Что входит в состав ИСБ?
8. Что понимается под дежурно-диспетчерской подсистемой КСБ и ИСБ?
9. Какие функции возложены на дежурно-диспетчерскую подсистему КСБ и ИСБ?
10. Какое назначение у подсистемы производственно-технологического контроля КСБ и ИСБ?
11. Какие подсистемы сигнализации могут использоваться в КСБ и ИСБ?
12. Что должны обеспечивать подсистемы контроля и управления доступом КСБ и ИСБ?
13. Что должны обеспечивать подсистемы теле/видеонаблюдения и видеоконтроля КСБ и ИСБ?
14. Что входит в состав подсистемы досмотра и поиска КСБ и ИСБ?
15. Какие функции возложены на подсистемы автоматического пожаротушения КСБ и ИСБ?
16. Что должны обеспечивать подсистемы противодымной защиты КСБ и ИСБ?
17. Для чего предназначены подсистема связи и подсистема оповещения КСБ и ИСБ?
18. Какие операции выполняет подсистема управления эвакуацией людей КСБ и ИСБ?
19. Что относят к инженерно-техническим средствам физической защиты КСБ и ИСБ?
20. Что входит в состав подсистемы инженерного обеспечения объекта КСБ и ИСБ?

ЗАКЛЮЧЕНИЕ

В процессе оптимизации функционирования любого объекта вне зависимости от его принадлежности к тому или иному роду деятельности во главу угла неизменно ставится обеспечение его безопасности и грамотное осуществление пропускного режима. Центральная роль в данных мероприятиях отводится техническим средствам охраны и безопасности, которые позволят своевременно и оперативно выявлять нештатные ситуации, а также контролировать доступ к расположенным на подконтрольной территории объектам в режиме реального времени. При этом крайне важно, чтобы обслуживание и контроль за работоспособностью всех систем обеспечения безопасности был возложен на квалифицированных работников, компетентных анализировать поступающую информацию и принимать решения в зависимости от ситуации.

Чтобы повысить надёжность охраны объектов, необходимо правильно определиться с выбором технических средств. В нынешних реалиях с появлением и развитием всевозможных технических процессов и устройств к организациям предъявляются все новые и новые требования по обеспечению безопасности, которые с каждым годом становятся все выше. С применением технических средств защиты появились так называемые интегрированные системы технических средств охраны и безопасности. Их применение позволяет существенно повысить эффективность работы, а также оказать значительную помощь персоналу, поскольку человеческие ресурсы так или иначе ограничены.

На сегодняшний день существует множество преимуществ современных технических средств охраны и безопасности. Среди них – эффективность (возможность контроля ситуационной обстановки в режиме реального времени), экономия ресурсов (сокращение числа персонала и возможность долгосрочного использования ресурсов), универсальность (использование на различных объектах), надёжность (постоянное обеспечение безопасности и своевременное обнаружение и предотвращение нештатных ситуаций). Однако важно помнить о том, что технические средства охраны и безопасности – это лишь часть комплекса мероприятий по обеспечению защиты и безопасности объектов. Их функциональность напрямую зависит от грамотного выбора технических средств, настройки и своевременного обслуживания.

Системы сигнализации позволяют своевременно обнаружить опасность на охраняемом объекте и подать сигнал тревоги для оперативного принятия мер по устранению опасности. Качественные системы сигнализации должны обладать такими свойствами как:

- передача извещения о тревоге в любое время,
- минимизация вероятности ложных извещений,
- обеспечение информирования о неисправностях системы,

- осуществление текущей проверки работоспособности системы при условии минимального периода прерывания её нормальной работы,

- осуществление защиты от несанкционированного доступа к органам управления и программному обеспечению системы.

Комплексный подход использования различных технических средств охраны и безопасности повышает уровень антитеррористической защищённости объектов, в том числе и объектов органов внутренних дел. К примеру, в качестве комплексного подхода можно рассмотреть установку системы охранно-пожарной сигнализации совместно с системой охранного телевидения с интегрированными алгоритмами видеоаналитики, а также подключить объект к централизованной охране. А для контрольно-пропускных пунктов объекта использовать систему контроля и управления доступом. Таким образом, вероятность обнаружения опасности значительно повышается.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Баумтрог, В.Э. Специальная техника органов внутренних дел : технические средства сигнализации и охранного телевидения [Электронный ресурс] : учебное пособие / В.Э. Баумтрог. – Барнаул : Барнаульский юридический институт МВД России, 2022. – 44 с.

2. Ватагин, В.С. Системное видеонаблюдение и охранно-пожарная сигнализация в комплексной системе безопасности объектов для предотвращения ЧС и террористических актов / В.С. Ватагин // Пожаровзрывобезопасность. – 2010. – Т. 19. – № 6.

3. Винокуров, С.А. Организация деятельности подразделений органов внутренних дел по антитеррористической защищенности объектов [Электронный ресурс] : методические рекомендации / С.А. Винокуров [и др.]. – Воронеж : Воронежский институт МВД России, 2020. – 47 с.

4. Винокуров, С.А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С.А. Винокуров, С.А. Гречаный, Д.Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – 175 с.

5. Выбор и применение систем контроля и управления доступом : методические рекомендации Р 064-2017. – М. : ФКУ «НИЦ «Охрана» Росгвардии; Саратов : Амирит, 2017. – 92 с.

6. Галанкин, А.В. Структура системы контроля и управления доступом организации / А.В. Галанкин, С.В. Чащин // Известия Тульского государственного университета. Технические науки. – 2021. – № 4.

7. Гобеджишвили, В.П. Современные системы видеонаблюдения и их составляющие / В.П. Гобеджишвили, В.И. Капалин // Евразийский научный журнал. – 2017. – № 4.

8. Губанов, Н.Н. Применение систем видеонаблюдения в правоохранительной деятельности : учебное пособие / Н.Н. Губанов. – Ставрополь : Ставропольский филиал Краснодарского университета МВД России (СФ КрУ МВД России), 2016 . – 84 с.

9. Еськов, А.В. Технические средства охраны : учебное пособие / А.В. Еськов. – Барнаул : Барнаульский юридический институт МВД России (БЮИ МВД России), 2015. – 52 с.

10. Зарубин, В.С. Технические системы антитеррористической и противокриминальной защиты : курс лекций / В.С. Зарубин, О.В. Багринцева. – Воронеж : Воронежский институт МВД России, 2018. – 85 с.

11. Зенов, А.Ю. Комплексный подход к обнаружению, классификации и распознаванию нарушителя на охраняемой территории / А.Ю. Зенов // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2012. – № 2(22).

12. Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения

имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации : методические рекомендации Р 078-2019. — М. : ФКУ «НИЦ «Охрана» Росгвардии, 2019. – 58 с.

13. Инструкция по действиям персонала пунктов централизованной охраны в штатных и нештатных ситуациях, возникающих в ходе обеспечения централизованной охраны объектов и мест проживания и хранения имущества граждан : методические рекомендации Р 079-2019. – М. : НИЦ «Охрана», 2019. – 16 с.

14. Могилин, К.А. Интеллектуальные системы видеонаблюдения в комплексах безопасности / К.А. Могилин, В.А. Селищев // Известия Тульского государственного университета. Технические науки. – 2020. – № 3.

15. Наумова, И.Ю. Качественный выбор системы охраны как надежность защиты охраны объектов и помещений / И.Ю. Наумова, В.В. Князева // Труды международного симпозиума "Надежность и качество". – 2016. – Т. 2.

16. Никулин, В.В. Датчики в системах охранной сигнализации / В.В. Никулин, С.С. Попкова // Огарёв-Online. – 2021. – № 14(167).

17. Организация использования систем охраны периметра объектов : учебно-методическое пособие / С.А. Винокуров [и др.]. – Воронеж : Воронежский институт МВД России, 2018. – 93 с.

18. Основы применения систем охранного телевидения правоохранительными органами : учебное пособие / Б.В. Рудаков, Ю.В. Кочкин. – Челябинск : Челябинский юридический институт МВД РФ(ЧелЮИ МВД России), 2009 . – 135 с.

19. Особенности использования и перспективы применения систем централизованного наблюдения для повышения эффективности взаимодействия сил и средств правоохранительных органов : отчет о НИР (заключ.) / науч. рук. С.А. Винокуров. – Воронеж : Воронежский институт МВД России, 2019. – № ГР 07194285.

20. Применение оборудования охранных телевизионных систем в условиях ограниченной видимости или других дестабилизирующих факторов : методические рекомендации Р 78.36.049-2015. – М. : НИЦ «Охрана», 2015. – 111 с.

21. Рекомендации по выбору антитеррористических средств для защиты объектов : методические рекомендации / С.А. Гречаный [и др.]. – Воронеж : Воронежский институт МВД России, 2020. – 48 с.

22. Рудаков, Б.В. Основы средств наблюдения органов внутренних дел [спецтехника] : учебное пособие / Б.В. Рудаков . – Челябинск : Челябинский юридический институт МВД РФ (ЧелЮИ МВД России), 2006. – 95 с.

23. Рудич, Д.Н. Разработка системы охранного телевидения на производстве / Д.Н. Рудич, В.Н. Дущак // Актуальные проблемы авиации и космонавтики. – 2017. – Т. 2. – №13.

24. Сагидова, М.Л. Современные системы контроля и управления доступом / М.Л. Сагидова // Международный журнал гуманитарных и естественных наук. – 2022. – № 9-1(72).

25. Селищев, В.А. Выбор системы охраны периметра / В.А. Селищев, О.В. Чечуга // Известия Тульского государственного университета. Технические науки. – 2010. – № 2-2.

26. Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесённых к первой категории : методические рекомендации Р 78.36.052-2015. – М. : НИЦ «Охрана», 2015. – 192 с.

27. Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесенных к 2, 3 и 4 категориям : методические рекомендации Р 78.36.059-2016. – М. : ФКУ «НИЦ «Охрана» Росгвардии, 2016. – 386 с.

Список использованных нормативных правовых актов:

1. О ведомственной охране : Федеральный закон от 14.04.1999 №77-ФЗ.

2. О войсках национальной гвардии Российской Федерации : Федеральный закон от 03.07.2016 № 226-ФЗ.

3. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ МВД России от 31.12.2014 № 1152.

4. Об утверждении Наставления по организации службы строевых подразделений вневедомственной охраны войск национальной гвардии Российской Федерации : приказ Росгвардии от 21.09.2018 № 420.

5. Об утверждении Руководства по организации службы пунктов централизованной охраны подразделений вневедомственной охраны войск национальной гвардии Российской Федерации : приказ Росгвардии от 06.02.2019 № 59.

6. Об утверждении Руководства по организации службы центров оперативного управления (групп обеспечения служебной деятельности нарядов) подразделений вневедомственной охраны войск национальной гвардии Российской Федерации : приказ Росгвардии от 06.02.2019 № 35.

7. Об утверждении Требований к оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список I перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, прекурсоров, и (или) культиви-

рование наркосодержащих растений для использования в научных, учебных целях и в экспертной деятельности, для производства используемых в медицинских целях и (или) в ветеринарии наркотических средств и психотропных веществ : приказ Росгвардии № 335, МВД России № 677 от 15.09.2021.

8. ГОСТ 26342-84 Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры

9. 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

10. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний : утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 17.12.2008 № 430-ст.

11. ГОСТ Р 51558-2014 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний.

12. ГОСТ Р 52551-2016 Системы охраны и безопасности. Термины и определения.

13. ГОСТ Р 53195.1-2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Общие положения.

14. ГОСТ Р 53325-2012 Техника пожарная. Технические средства пожарной автоматики. Общие технические требования и методы испытаний.

15. ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования

16. ГОСТ Р 56102.1-2014 Национальный стандарт РФ Системы централизованного наблюдения. Часть 1. Общие положения

17. ГОСТ Р 56677-2015 Национальный стандарт РФ Средства физической защиты инженерно-технические. Кодирование, идентификация и маркировка. Общие требования

18. ГОСТ Р 57674-2017. Национальный стандарт Российской Федерации. Интегрированные системы безопасности. Общие положения

19. ГОСТ Р 59638-2021. Национальный стандарт Российской Федерации. Системы пожарной сигнализации. Руководство по проектированию, монтажу, техническому обслуживанию и ремонту. Методы испытаний на работоспособность.

План-график выпуска учебных
и научных изданий № 33

,
Андрей Анатольевич Черных,
Фёдор Владимирович Безгачев

Технические средства охраны и безопасности, используемые в органах внутренних дел

Учебное пособие

Подготовлено к изданию Е.Н. Полежаевой, В.Е. Рыбиным.

Подписано в печать *16.09.2024*
Формат Р 60х84. Бумага типографская.
Гарнитура Times New Roman.
Печать офсетная 3,4 уч.-изд. л. (4,3 усл. печ. л.).
Тираж 100 экз. Заказ _____.

Научно-исследовательский и редакционно-издательский отдел.
Сибирский юридический институт МВД России.
660131, г. Красноярск, ул. Рокоссовского, 20.

Отпечатано в типографии НИРИО СибЮИ МВД России.
660050, г. Красноярск, ул. Кутузова, 6.