



**МИНИСТЕРСТВО ОБРАЗОВАНИЯ
РЕСПУБЛИКИ БЕЛАРУСЬ**

**Белорусский национальный
технический университет**

**Кафедра «Информационно-измерительная техника
и технологии»**

ТЕОРИЯ СИСТЕМ БЕЗОПАСНОСТИ

Пособие

**Минск
БНТУ
2025**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
Белорусский национальный технический университет

Кафедра «Информационно-измерительная техника и технологии»

ТЕОРИЯ СИСТЕМ БЕЗОПАСНОСТИ

Пособие

для обучающихся по специальности 6-05-0716-05
«Технические системы обеспечения безопасности»

*Рекомендовано учебно-методическим объединением по образованию
в области приборостроения*

Минск
БНТУ
2025

УДК 681.2 (075.8)

ББК 34.9я7

Т33

С о с т а в и т е л ь

А. А. Антошин

Р е ц е н з е н т ы:

главный инженер проекта ООО «ТехноИнтелСервис»

В. Н. Кнотько;

зав. кафедрой проектирования информационно-компьютерных систем Белорусского государственного университета информатики и радиоэлектроники, канд. техн. наук, доцент *В. В. Хорошко*

Т33 Теория систем безопасности : пособие для обучающихся по специальности 6-05-0716-05 «Технические системы обеспечения безопасности» / А. А. Антошин. – Минск : БНТУ, 2025. – 59 с.
ISBN 978-985-31-0124-9.

В пособии приведены сведения, раскрывающие содержание программы дисциплины «Теория систем безопасности», включая положения, определяющие суть мер, обеспечивающих безопасность личности, общества, государства и предприятия. Охрана объекта в пособии рассматривается как реализация режимных мер, состоящих из пропускного и внутриобъектового режимов. Рассматриваются задачи, решаемые техническими системами охраны и их подсистемами, системами охранной сигнализации, контроля и управления доступом и охранного телевидения.

Пособие предназначено для обучающихся по специальности 6-05-0716-05 «Технические системы обеспечения безопасности», а также для работников организаций, занимающихся проектированием систем охраны.

УДК 681.2 (075.8)

ББК 34.9я7

ISBN 978-985-31-0124-9

© Белорусский национальный
технический университет, 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1. БЕЗОПАСНОСТЬ ОБЪЕКТА.....	6
1.1. Безопасность личности, общества и государства	6
1.2. Безопасность промышленных объектов.....	8
1.3. Классификация событий, приводящих к ущербу	10
1.4. Концепция обеспечения безопасности объекта.....	12
2. КОНЦЕПЦИЯ ОХРАНЫ ОБЪЕКТА	17
2.1. Система охраны зданий	17
2.2. Проектирование системы охраны предприятия	22
2.3. Цели и задачи системы охраны.....	23
2.4. Описание объекта охраны. Категорирование	24
2.5. Уязвимости объекта охраны.....	30
2.6. Модель нарушителя	32
2.7. Зоны доступа и рубежи охраны объекта	36
2.8. Принцип рубежей или зональный принцип функционирования системы охраны	38
3. ОСНОВНЫЕ ПОДСИСТЕМЫ ТЕХНИЧЕСКОЙ СИСТЕМЫ ОХРАНЫ.....	43
3.1. Система охранной сигнализации	46
3.2. Системы контроля и управления доступом	48
3.3. Система охранного телевидения.....	50
ЛИТЕРАТУРА	57

ВВЕДЕНИЕ

Дисциплина «Теория систем безопасности» является частью подготовки инженера по специальности 6-05-0716-05 «Технические системы обеспечения безопасности». Она направлена на изучение научных принципов и положений, обобщающих практический опыт и закономерности, лежащие в основе применения технических средств при построении систем охраны объектов, а также прогнозирования эффективности технических средств охраны.

Целью учебно-методического пособия является помощь студентам в освоении основных положений, определяющих суть мер, обеспечивающих безопасность личности, общества, государства и предприятия. В пособии показана связь между безопасностью и особенностями разнообразных ресурсов, которыми обладают объекты безопасности. Охрана объекта рассматривается только как часть его безопасности, которая направлена на реализацию режимных мер, которые состоят из пропускного режима и внутриобъектового режима. При этом охрана нацелена на уменьшение или недопущение ущерба объекту от несанкционированного проникновения и преступных посягательств нарушителя. Основой для создания эффективной системы охраны является грамотное деление объекта на зоны доступа и зоны контроля с последующим использованием для достижения этой цели охранных мер. Особое внимание в отношении охранных мер требует применение технических средств охраны, среди которых наиболее важными являются системы: охранной сигнализации, охранного телевидения, контроля и управления доступом.

В первом разделе пособия рассматриваются наиболее общие аспекты безопасности личности, общества, государства, а также системы безопасности предприятия. В разделе рассматривается классификация событий, приводящих к ущербу объекта охраны. Особое внимание уделяется разработке концепции обеспечения безопасности объекта и ее методологической основы. Рассматриваются основные принципы создания системы безопасности.

Второй раздел пособия посвящен систематизированному изложению методики разработки концепции охраны объекта. Система охраны объекта рассматривается как комплекс мер, важнейшими из которых являются режимные меры. Проектирование системы охраны предприятия рассматривается с точки зрения обязательной раз-

работки концептуального проекта, предшествующего рабочему проектированию системы охраны предприятия. Концептуальный проект предполагает определение целей и задач системы охраны, категорирование объекта охраны, анализ его уязвимостей, описание модели потенциального нарушителя, основных принципов организации и функционирования системы охраны, определение требований к основным подсистемам безопасности. Особое внимание уделяется определению зон доступа и рубежей охраны объекта. Дается обоснование делению рубежей охраны на зоны контроля объекта.

В третьем разделе рассматриваются основные подсистемы технической системы охраны с анализом задач, решаемых этими подсистемами. Примером таких подсистем являются системы охранной сигнализации, передачи извещений, контроля, управления доступом, телевизионные системы видеонаблюдения (системы охранного телевидения). Основными задачами охранной сигнализации является информирование персонала о состоянии контролируемой зоны и управление контролируемыми шлейфами сигнализации, т. е. постановка и снятие их с охраны. Одной из основных задач системы контроля и управления доступом является задача организации санкционированного доступа сотрудников и посетителей на объект охраны. Система охранного телевидения решает задачи реализации пропускного и внутриобъектового режимов на объекте охраны применением технических средств для организации наблюдения в местах, которые определены соответствующими документами предприятия.

1. БЕЗОПАСНОСТЬ ОБЪЕКТА

1.1. Безопасность личности, общества и государства

Актуальность усилий, прилагаемых государством в отношении обеспечения безопасности населения и промышленных объектов, не вызывает сомнений. При этом необходимо понимать, что само понятие безопасности является достаточно широким и разносторонним понятием [1–6]. В случае, когда имеется в виду защищенность населения и государства от внутренних и внешних угроз, понятие безопасности определяют следующим образом. Безопасность – это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз [2]. Объектами безопасности в этом случае являются права и свободы личности, материальные и духовные ценности общества, конституционный строй, суверенитет и территориальная целостность государства. Характеристиками названных объектов безопасности являются жизненно важные интересы, к которым относят совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства [3]. Например, к таким характеристикам можно отнести состояние здоровья человека, количество и вид материальных ресурсов, которыми располагает человек или государство и т. п.

В Республике Беларусь наиболее общее понятие безопасности рассматривается в Концепции национальной безопасности Республики Беларусь [4]. В этом документе вводится понятие «национальная безопасность» как состояние защищенности национальных интересов Республики Беларусь от внутренних и внешних угроз. Национальные интересы определяются как совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства, позволяющих обеспечивать конституционные права, свободы, высокое качество жизни граждан, независимость, территориальную целостность, суверенитет и устойчивое развитие Республики Беларусь.

Концепция национальной безопасности Республики Беларусь призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов

законодательства в различных сферах национальной безопасности, разработки документов стратегического планирования. В качестве угрозы национальной безопасности рассматривают потенциальную или реально существующую возможность нанесения ущерба национальным интересам Республики Беларусь. Источниками угрозы национальной безопасности выступают фактор (или их совокупность), способный при определенных условиях привести к возникновению угрозы национальной безопасности.

Принято считать, что национальная безопасность состоит из следующих частей:

- 1) политическая безопасность;
- 2) экономическая безопасность;
- 3) научно-технологическая безопасность,
- 4) социальная безопасность;
- 5) демографическая безопасность;
- 6) биологическая безопасность;
- 7) информационная безопасность;
- 8) военная безопасность;
- 9) экологическая безопасность.

Политическая безопасность – состояние защищенности политической системы от внешних и внутренних угроз, обеспечивающее реализацию национальных интересов во всех сферах национальной безопасности.

Экономическая безопасность – состояние экономики, при котором гарантированно обеспечивается защищенность национальных интересов Республики Беларусь от внутренних и внешних угроз.

Научно-технологическая безопасность – состояние отечественного научно-технологического и образовательного потенциала, обеспечивающее возможность реализации национальных интересов Республики Беларусь в научно-технологической сфере.

Социальная безопасность – состояние защищенности жизни, здоровья и благосостояния граждан, духовно-нравственных ценностей общества от внутренних и внешних угроз.

Демографическая безопасность – состояние защищенности общества и государства от демографических явлений и тенденций, социально-экономические последствия которых оказывают негативное воздействие на устойчивое развитие Республики Беларусь.

Биологическая безопасность – состояние защищенности населения, животных и растений, окружающей среды от воздействия опасных биологических факторов, при котором обеспечивается допустимый уровень биологического риска.

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Военная безопасность – состояние защищенности национальных интересов Республики Беларусь от военных угроз.

Экологическая безопасность – состояние защищенности окружающей среды, жизни и здоровья граждан от угроз, возникающих в результате антропогенных воздействий, а также факторов, процессов и явлений природного и техногенного характера.

Реализация социальной безопасности включает в себя обеспечение безопасности промышленных объектов и граждан, включая защиту объектов и физических лиц от пожара, несанкционированного доступа и противоправных посягательств.

1.2. Безопасность промышленных объектов

Реализация безопасности государства невозможна без обеспечения безопасности, в том числе и отдельных промышленных объектов. В качестве промышленного объекта обычно берут предприятие. Предприятие – это самостоятельный хозяйствующий субъект с правом юридического лица, который на основе имеющихся у него (или закрепленных за ним) ресурсов производит и реализует продукцию, выполняет работы и оказывает услуги. Ресурсами предприятия являются источники и предпосылки получения необходимых людям материальных и духовных благ.

К основным видам ресурсов, используемых предприятием, относят:

- 1) материальные;
- 2) средства труда;
- 3) трудовые, в том числе интеллектуальные ресурсы;
- 4) финансовые;
- 5) информационные.

Ресурсы предприятия обеспечивают получение как материальных, так и духовных благ людьми не только работающими на предприятии, но и потребляющими производимую предприятием про-

дукцию. Для гарантированного получения людьми необходимых материальных и духовных благ требуется обеспечение сохранности и развития всех перечисленных ресурсов предприятия. Выполнение этой задачи достигается в результате реализации комплекса разнообразных мер, в том числе обеспечением безопасности предприятия. Обеспечение безопасности предприятия обеспечивается мерами, к которым относят:

- 1) организационные;
- 2) правовые;
- 3) режимные;
- 4) охранные.

Перечисленные выше меры образуют систему безопасности предприятия, которая направлена на недопущение или уменьшение **ущерба** предприятию. Таким образом, недопущение или уменьшение ущерба предприятию является целью создания системы безопасности предприятия.

Итак. **Система безопасности предприятия** включает в себя комплекс разнообразных мер, таких, как: организационные, правовые, режимные, охранные, которые нацелены на недопущение или уменьшение ущерба предприятию от противоправных действий нарушителя или совершения нежелательного события.

Мерой эффективности имеющейся на предприятии системы безопасности или мерой потенциального ущерба предприятию в результате совершения нежелательного события является **риск** [5, 6].

Риск – это мера потенциального ущерба или возможной потери имущества, выражаемая вероятностью нежелательного события. Риск определяется как произведение вероятности ущерба (или убытков) на величину этого ущерба.

Обобщенный риск включает несколько **видов рисков**:

- 1) финансовый;
- 2) материальный;
- 3) юридический.

Нейтрализация или управление рисками направлено на достижение одного из следующих результатов:

- 1) избежание риска;
- 2) уменьшение риска;
- 3) передача риска;
- 4) принятие риска.

Поясним перечисленные результаты управления рисками.

Избежание риска. Избежание риска выполняется путем оценки источника риска и устранения его. Например, компания может не самостоятельно изготавливать, а покупать важный компонент оборудования у другой компании. Это снимает вопрос о защите собственной производственной линии от нежелательных событий.

Уменьшение риска. Уменьшение риска достигается проведением ряда мероприятий (в том числе созданием системы безопасности), которые способны лишь уменьшить ущерб от нежелательного события для предприятия. Кроме того, риск может быть распределен по нескольким объектам. В результате, если разместить сходное производство на разных объектах, то ущерб, полученный в результате прекращения производства на одном объекте, может быть возмещен путем увеличения объема выпуска продукции на другом. Таким образом, при рассредоточении запасов меньшая часть имущества будет подвергаться риску, например, в результате действий злоумышленника.

Передача риска. Передачей риска является использование страхования для возмещения убытков, связанных с ущербом, нанесенным объекту в результате нежелательных событий.

Принятие риска. Принятие риска есть признание того факта, что некий остаточный риск присутствует при любых условиях. Важным является при проектировании системы безопасности сознательно определить уровень риска, который допустим для предприятия, а не принимать его произвольно. Руководство предприятия должно осознано идти на принятие определенного уровня риска и осознавать его значение для предприятия. Например, разрушение остекления окон при попытке проникновения нарушителя на объект в большинстве случаев является неизбежным ущербом даже для эффективно действующей системы безопасности, и он должен быть принят руководством предприятия [7].

1.3. Классификация событий, приводящих к ущербу

В общем случае ущерб объекту охраны можно причинить в результате совершения следующих **трех групп** событий (угроз):

а) **во-первых**, ущерб может быть результатом несанкционированного доступа на объект охраны и последовавшими за ним про-

тивоправными посягательствами нарушителя на средства труда, материальные, финансовые, информационные, и другие виды ресурсов предприятия;

б) **во-вторых**, ущерб может быть результатом возникновения пожара;

в) **в-третьих**, к ущербу могут привести действия (угрозы) экономического, политического или, например, социального характера.

В рамках изучаемой дисциплины будем рассматривать только первые два типа событий, приводящих к ущербу на промышленном объекте, а именно ущерб, наносимый в результате несанкционированного доступа на объект и последовавших после этого противоправных посягательств нарушителя на различные виды ресурсов предприятия и/или ущерб, наносимый предприятию пожаром.

Таким образом система безопасности объекта нацелена на недопущение или уменьшение ущерба объекту охраны в результате совершения двух принципиально разных типов событий, а именно:

1) несанкционированного доступа и противоправных посягательств нарушителя;

2) пожара.

Защита объекта от несанкционированного доступа и противоправных посягательств обеспечивается с помощью охраны объекта, а защита жизни и здоровья людей, национального достояния и экономики Республики Беларусь от пожаров достигается с помощью системы обеспечения пожарной безопасности Республики Беларусь.

Закон Республики Беларусь «О пожарной безопасности» определяет систему обеспечения пожарной безопасности Республики Беларусь следующим образом. Система пожарной безопасности в Республике Беларусь состоит из комплекса экономических, социальных, организационных, научно-технических и правовых мер, а также сил и средств, направленных на предупреждение и тушение пожаров [8].

Особое место в системе безопасности объекта занимает информационная безопасность. Содержание этого понятия раскрыто в Концепции национальной безопасности Республики Беларусь [4]. В концепции говорится, что информационная безопасность – это состояние защищенности информационного пространства, информационной инфраструктуры и информационных ресурсов от внешних и внутренних угроз в информационной сфере. **Защита информации** (в том числе в автоматизированных системах обработки информации),

обеспечивается специальными методами защиты [5]. Система защиты информации – это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия.

Названные составные части системы безопасности не охватывают системы противодействия всем возможным угрозам в отношении предприятий, например угрозы политического или социального характера. В настоящем пособии будет рассматриваться только система охраны объектов как одна из составных частей системы безопасности предприятия.

1.4. Концепция обеспечения безопасности объекта

Концепция безопасности объекта представляет собой общий замысел разработчиков, включающий в себя перечень технических и организационных мероприятий по защите объекта от прогнозируемых угроз.

Разработка концепции осуществляется в ходе создания концептуального проекта, который должен содержать два раздела, а именно, «Концепцию безопасности объекта» и «Технико-экономическое обоснование» создания системы безопасности и комплекса технических средств обеспечения безопасности [7]. Раздел «Концепция безопасности объекта» включает подразделы:

1. Описание потенциальных угроз.
2. Цели и задачи системы безопасности.
3. Описание объектов защиты. Категорирование.
4. Анализ уязвимости объекта.
5. Описание основных принципов организации и функционирования системы безопасности.
6. Требования к основным подсистемам безопасности.

При описании потенциальных угроз необходимо ответить на вопрос «от каких или какого посягательства требуется защитить объект?». Определяется тактика совершения вероятного преступления.

Подраздел «Цели и задачи системы безопасности» описывает те ресурсы предприятия, которые необходимо сохранить или уменьшить их ущерб от противоправных действий нарушителя или совершения нежелательного события в результате реализации мер системы безопасности. То есть необходимо дать ответ на вопрос «что

необходимо защищать?». Цели системы безопасности предприятия будут состоять из перечня ресурсов, для которых требуется исключить или уменьшить ущерб до уровня, который может быть принят. Например, может идти речь об информационных, материальных, финансовых и других ресурсах.

Цели системы безопасности достигаются в результате решения задач, которые отражают способы достижения цели, в первую очередь зависящие от вида сохраняемого ресурса. В этом отношении особо важное значение имеет тип события, приводящего к ущербу. Недопущение или уменьшение ущерба ресурсам предприятия в результате несанкционированного доступа и противоправных посягательств нарушителя это одно. Совсем по-другому формулируется задача в случае обеспечения сохранности ресурсов от пожара в результате применения противопожарной защиты ресурсов предприятия или организации. Таким образом, задача по защите объекта от несанкционированного доступа и противоправных посягательств обеспечивается с помощью охраны объекта, а задача по защите жизни и здоровья людей, ресурсов предприятия от пожаров достигается применением средств обеспечения пожарной безопасности.

В пятом и шестом подразделах разрабатываются адекватные меры защиты ресурсов. Указывается, что необходимо сделать, чтобы предотвратить или уменьшить возможный ущерб, т. е. разрабатывается методологическая основа системы безопасности предприятия. Методология – это учение, в котором излагаются базовые принципы, положенные в основу той или иной деятельности. При создании систем безопасности на предприятии необходимо руководствоваться следующими основными принципами:

- комплексности, или системности;
- приоритета мер предупреждения;
- непрерывности;
- законности;
- плановости;
- экономности;
- принцип взаимодействия;
- сочетания гласности и конфиденциальности;
- компетентности.

Дадим комментарии некоторым из перечисленных принципов:

1. *Принцип комплексности (или системности)*. Реализация этого принципа предполагает создание такой системы безопасности, которая бы обеспечила защищенность предприятия от всевозможных опасностей и угроз, включая:

- его имущество;
- персонал;
- информацию.

Опасности и угрозы могут быть такими:

- экономическими;
- экологическими;
- научно-техническими;
- кадровыми;
- пожарными и др.

2. *Принцип приоритета мер предупреждения*. Следует обратить внимание в связи с этим принципом на то, что его реализация экономически значительно выгоднее, чем устранение нанесенного ущерба.

3. *Непрерывность*. В соответствии с этим принципом система безопасности должна действовать постоянно, защищая интересы предприятия в условиях риска.

4. *Законность*. Все действия по обеспечению безопасности предприятия должны осуществляться на основе действующего законодательства и не противоречить ему.

5. *Плановость*. Данный принцип предполагает, что каждый участник процесса обеспечения безопасности действует логически последовательно, строго выполняя возложенные на него обязанности. Деятельность по обеспечению безопасности в целом организуется на основе единого замысла, изложенного в комплексной программе и конкретных планах по отдельным направлениям и подвидам безопасности.

6. *Экономность*. Система безопасности согласно этому принципу должна быть выстроена таким образом, чтобы затраты на ее обеспечение были экономически целесообразными, а стоимость затрат была оптимальной и не превышала тот уровень, при котором теряется экономический смысл их применения.

7. *Принцип взаимодействия*. Для обеспечения безопасности предприятия необходимо, чтобы усилия всех обеспечивающих ее лиц, подразделений, служб были скоординированы. Принцип взаимодей-

ствия предполагает также согласование действий с внешними организациями, к которым можно отнести правоохранительные органы, местные или районные службы безопасности, органы власти различного уровня и т. д., способные оказать необходимое содействие в обеспечении безопасности предприятия.

8. *Принцип сочетания гласности и конфиденциальности.* Система основных мер безопасности должна быть известна всем сотрудникам предприятия, ее требования должны выполняться. В то же время целый ряд способов, сил, средств, методов обеспечения безопасности должен быть законспирирован и известен очень узкому кругу специалистов, что позволит более эффективно бороться как с внутренними, так и внешними угрозами, своевременно предотвращать нанесение ущерба предприятию.

9. *Принцип компетентности.* Этот принцип означает, что вопросами обеспечения безопасности предприятия должны заниматься не дилетанты, а профессионалы, глубоко знающие сущность проблемы, умеющие своевременно оценить обстановку и принять правильное решение.

Концепция безопасности предприятия должна не противоречить политике и стратегии безопасности предприятия. Политика безопасности предприятия представляет собой систему взглядов, мер, решений, действий в области безопасности, не противоречащих принципам безопасности и создающих благоприятные условия для достижения целей бизнеса, т. е. политика безопасности позволяет предприятию выполнять производственную программу, выпускать конкурентоспособную продукцию (товары, услуги, работы), повышать эффективность производства, преумножать собственность, получать прибыль и т. д.

Под стратегией безопасности предприятия понимается совокупность наиболее значимых решений, направленных на обеспечение принятого предприятием уровня безопасности его функционирования. Различают три типа стратегий безопасности.

Первый тип – это стратегия, ориентированная на необходимость внезапно реагировать на реально возникшие угрозы производственной деятельности, имуществу, персоналу и т. д. В этом случае действует принцип «угроза – отражение». Созданные на предприятии (часто поспешно) для решения этой задачи подразделения, службы, а также выделенные силы и средства могут ослабить или даже пре-

дотвратить воздействие угроз и, тем не менее, предприятию в этих условиях может быть нанесен ущерб.

Второй тип – это стратегия, ориентированная на прогнозирование, заблаговременное выявление опасностей и угроз, целенаправленное исследование экономической и криминогенной ситуаций как внутри предприятия, так и в окружающей среде. Выделенные для решения этой задачи специалисты, созданные подразделения и службы безопасности дают возможность осознанно и целенаправленно проводить работу по созданию благоприятных условий для предпринимательской деятельности.

Третий тип – это стратегия безопасности, направленная на возмещение (восстановление, компенсацию) нанесенного ущерба. Данная стратегия может считаться приемлемой лишь тогда, когда ущерб восполним, или тогда, когда нет возможности осуществить стратегии первого или второго типа.

Разработка концепции безопасности объекта требует последующей разработки концепции отдельных составляющих безопасности объекта. К таким составляющим относят концепцию систем охраны, противопожарной защиты, информационной безопасности и т. д.

2. КОНЦЕПЦИЯ ОХРАНЫ ОБЪЕКТА

2.1. Система охраны зданий

При рассмотрении концепции безопасности предприятия или организации показано, что охрана объекта представляет собой одну из важнейших задач, решение которой существенно повышает их безопасность. Как следует из СТБ 1250-2000 [9], охрана объектов от несанкционированного доступа и от противоправных посягательств на имущество состоит в реализации на охраняемом объекте правовых, организационных, режимных и технических мер, которые осуществляются уполномоченными на то органами и лицами в соответствии с законодательством. Таким образом, об охране объекта можно говорить только в том случае, если охрана осуществляется законным образом уполномоченными на то органами и лицами. Осуществление охраны объектов происходит в результате охранной деятельности. Термин охранный деятельность определен в этом же документе. Охранный деятельность – деятельность уполномоченных в соответствии с законодательством органов и лиц по охране объектов (имущества) юридических и физических лиц, в том числе личного имущества или индивидуальных предпринимателей, в том числе физических лиц и перемещаемых (перевозимых) грузов, по охране физических лиц, а также по проектированию, монтажу, наладке, техническому обслуживанию технических средств и систем охраны и иная деятельность в соответствии с законодательством.

Круг лиц и организаций, имеющих право заниматься охранной деятельностью, определяется Законом Республики Беларусь «Об охранный деятельности в Республике Беларусь» [10]. Согласно этому Закону, организациями, осуществляющими охранный деятельность, являются: Служба безопасности Президента Республики Беларусь, Министерство обороны Республики Беларусь, Министерство внутренних дел Республики Беларусь, Комитет государственной безопасности Республики Беларусь, Государственный пограничный комитет Республики Беларусь, подчиненные им юридические лица, а также органы и подразделения по чрезвычайным ситуациям, таможенные органы. Особо следует отметить, что на основании специальных разрешений (лицензий) организации, работающие в сфере охранный деятельности, вправе осуществлять деятельность по обеспечению

безопасности юридических и физических лиц, охрану своих работников и принадлежащих этим организациям объектов, а также осуществлять проектирование, монтаж, наладку и техническое обслуживание средств и систем охраны, за исключением средств охраны индивидуального пользования. Полный перечень организаций, имеющих право осуществлять охранную деятельность, приводится в Законе [10]. Там же приведены требования к лицам, которые могут заниматься этой деятельностью.

Теперь дадим ответ на вопрос. Что означает утверждение «объект охраняется»? Из определения, приведенного в СТБ [9], следует, что охрана объекта от несанкционированного доступа и противоправных посягательств на имущество состоит в реализации правовых, организационных, режимных и технических мер.

Правовые меры охраны представляют собой систему мероприятий по созданию и совершенствованию нормативных правовых актов и совершению юридически значимых действий, обеспечивающих правовое регулирование охранной деятельности.

Организационные меры охраны – система мероприятий по организации охранной деятельности и координации действий органов и осуществляющих ее лиц.

Охранные меры – система мероприятий по обеспечению охранной деятельности путем применения различных способов.

Важнейшее значение для охраны объекта имеют режимные меры. **Режимные меры охраны** – это система мероприятий по установлению и соблюдению на охраняемом объекте пропускного и внутриобъектового режимов [9]. Перечень режимных мероприятий для каждого объекта охраны содержится в документах, которые разрабатываются руководством объекта охраны. Объект охраны – объекты, подлежащие защите от противоправных посягательств. К ним относятся: здания, сооружения, помещения, квартиры, участки местности, транспортные средства, перемещаемые (перевозимые) грузы, денежные средства, материальные ценности, физические лица, личное имущество физических лиц и т. п. Составными частями режимных мер являются пропускной и внутриобъектовый режимы.

Пропускной режим согласно Закону об охранной деятельности [10] определяется следующим образом. Пропускной режим – порядок, обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц, въезда

(выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества на охраняемые объекты или с охраняемых объектов. Таким образом, пропускной режим устанавливается в целях защиты охраняемых объектов от противоправных посягательств, которые заключаются в бесконтрольном перемещении лиц или материальных ценностей через границу охраняемого объекта или внутри этого объекта. Важной особенностью принципа осуществления пропускного режима является то, что с одной стороны пропускной режим обеспечивает **санкционированный** проход (проезд) следующих лиц и автотранспорта: персонала, осуществляющего свою деятельность на территории учреждения, посетителей данного учреждения, автотранспорта, в том числе служебного, а также обеспечивается ввоз (вывоз) материальных ценностей. С другой стороны, пропускной **режим исключает несанкционированный доступ** на территорию учреждения, в его здания, сооружения и помещения посторонних лиц; въезд на территорию учреждения автотранспортных средств, не имеющих оформленных разрешений; вывоз (вынос) материальных средств без оформленных надлежащим образом на то соответствующих документов; внос (ввоз) на территорию учреждения запрещенных предметов (материалов).

Для реализации пропускного режима предусматриваются следующие организационные и охранные меры:

- оборудование на территории учреждения контрольно-пропускных пунктов для осуществления контроля санкционированного прохода людей и проезда автотранспорта;

- установление при необходимости системы визуального и иного контроля основных мест прохода (проезда) и маршрутов движения.

Осуществляться такие организационные и охранные меры могут силами сотрудников охраны, которые уполномочены осуществлять указанные функции на территории учреждения. Однако для этих целей можно использовать технические средства и системы, как в рабочее время, так и в нерабочее время. К таким системам относятся: системы телевизионного наблюдения, системы контроля и управления доступом; системы охранной сигнализации с применением извещателей охранной сигнализации для обнаружения несанкционированного проникновения или попытки проникновения нарушителей на охраняемый объект через уязвимые места (особенно в нерабочее время).

Другая составляющая режимных мер – это совокупность мер, обеспечивающих внутриобъектовый режим объекта охраны. **Внутриобъектовый режим** – порядок, обеспечиваемый совокупностью мероприятий и правил, выполняемых лицами, находящимися на охраняемых объектах, в соответствии с требованиями соответствующих документов, а именно: правилами внутреннего трудового распорядка и правилами пожарной безопасности. Внутриобъектовый режим направлен на поддержание установленного порядка на территории учреждения, в его зданиях и сооружениях, местах общего пользования и обеспечение комфортных и безопасных условий нахождения в учреждении сотрудников и посетителей.

Внутриобъектовый режим определяет:

- порядок нахождения на территории учреждения или в отдельных его помещениях лиц и организаций, осуществляющих свою деятельность (кто в каком помещении и на протяжении какого времени может находиться?);
- режим работы основных инженерных систем и коммуникаций, дополнительного оборудования;
- общие правила поведения в учреждении лиц, их права и обязанности;
- порядок проведения ремонтно-строительных, погрузочно-разгрузочных и иных работ на территории, в зданиях и помещениях учреждения;
- поддержание общественного порядка и режимов безопасности.

Реализуется внутриобъектовый режим с помощью организационных и охранных мер, которые используют различные способы охраны в том числе:

- 1) установление пропускного режима;
- 2) обнаружение несанкционированного проникновения, попытки проникновения на охраняемый объект или противоправных посягательств на охраняемые ресурсы предприятия, в том числе с использованием систем охранной сигнализации;
- 3) оборудование охраняемых объектов техническими средствами и системами охраны;
- 4) патрулирование;
- 5) выставление постов;
- 6) осмотр охраняемых объектов;

7) задержание, в том числе с применением инженерно-технических средств охраны, и досмотр лиц, совершающих противоправные посяательства на охраняемые объекты и физические лица;

8) применение оружия, специальных средств и т. д.

Под техническими средствами охраны понимают конструктивно законченные, выполняющие самостоятельные функции устройства, в том числе аппаратно-программные, входящие в состав системы охраны объектов и физических лиц. При этом технические системы охраны представляют собой совокупность совместно действующих технических средств охраны, установленных на охраняемом объекте и объединенных системой инженерных сетей и коммуникаций. К техническим системам охраны относятся: системы тревожной сигнализации; системы передачи извещений; системы контроля и управления доступом; телевизионные системы видеонаблюдения и т. п.

Одним из способов охраны, который используется для реализации внутриобъектового режима, является задержание лиц, в том числе с применением инженерно-технических средств охраны, совершающих противоправные посяательства на охраняемые объекты. При этом под задержанием можно понимать кратковременное лишение свободы лица, подозреваемого в несанкционированном проникновении на объект охраны, а можно понимать увеличение времени, необходимого нарушителю для перемещения по охраняемому объекту к намеченной цели, или времени, необходимого для взлома устройств, защищающих материальные ценности. Инженерно-технические средства охраны применяются для обеспечения необходимого противодействия несанкционированному проникновению на охраняемые объекты, взлому и другим противоправным действиям. К инженерно-техническим средствам охраны могут быть отнесены: защитные кабины, двери, стекла, решетки, ставни, жалюзи, замки, запирающие устройства, сейфы, механические ограждения и преграды и т. п. Общепринято считать, что кратковременное лишение свободы лица, подозреваемого в несанкционированном проникновении на объект охраны (задержание нарушителя), в результате осуществления охраны объекта является конечным результатом ее успешного функционирования.

2.2. Проектирование системы охраны предприятия

Проектирование системы охраны, которая является составной частью системы безопасности предприятия, начинается с разработки концепции. Концепция системы охраны представляет собой общий замысел разработчиков, включающий перечень технических и организационных мероприятий по защите объекта от прогнозируемых угроз, которыми в данном случае являются несанкционированный доступ и противоправные посягательства на имущество. Концепция системы охраны является одним из двух разделов концептуального проекта [7]. Вторым разделом концептуального проекта является технико-экономическое обоснование (ТЭО) создания системы охраны и комплекса технических средств охраны. Концептуальное проектирование предшествует рабочему проектированию по оснащению объекта охраны техническими средствами и системами охраны и инженерно-техническими средствами защиты, которые и составляют технические меры охраны.

Структура документа «Концепция охраны объекта» содержит следующие пункты:

1. Цели и задачи системы охраны (Что охранять? Каким образом минимизировать вероятный ущерб).
2. Описание объектов охраны. Категорирование.
3. Анализ уязвимости объекта.
4. Описание потенциальных угроз. Модель нарушителя (от какого посягательства требуется защитить объект? Определяется тактика совершения вероятного преступления).
5. Описание основных принципов организации и функционирования системы охраны. Описание рубежей и деление объекта на зоны контроля (что должна сделать охранная система, чтобы предотвратить или уменьшить ущерб).
6. Требования к основным подсистемам безопасности (ПСБ).

При разработке концепции системы охраны организации или предприятия важно понимать, что разрабатываемая система охраны не может быть универсальной и обеспечить достижение цели в любом случае. Система охраны строится в предположении только определенной тактики совершения вероятного преступления, например, совершается проникновение с разрушением периметра или без разрушения, будет применяться тактика насилия или нет и т. п. По-

этому при описании принципов организации и функционирования системы охраны учитываются вероятные оснащённость преступника и применяемая им тактика, например, указывается в каком месте необходимо обнаружить нарушителя и как после его обнаружения задержать или ограничить его перемещение внутри объекта, как отследить маршрут его перемещений. Обязательно рассматриваются меры по укреплению периметра и ограничению перемещения нарушителя внутри объекта. Выполняется эта работа с привлечением информации об инженерных средствах защиты на путях возможного проникновения и перемещения нарушителей.

2.3. Цели и задачи системы охраны

При определении целей системы охраны организации или предприятия необходимо исходить из целей системы их безопасности, в частности необходимо знать в отношении каких ресурсов ущерб может быть нанесен в результате несанкционированного доступа и противоправных посягательств нарушителя. Именно в этом случае обеспечение сохранности или уменьшение ущерба ресурсам предприятия возможно в результате организации его охраны. Целями системы охраны предприятия будет обеспечение сохранности именно таких ресурсов предприятия. Важнейшим шагом при определении целей системы охраны является определение критериев достижения целей создаваемой системы и способы их проверки. Следует отметить, что каждое предприятие имеет свой набор ресурсов, ущерб которым может быть нанесен в результате несанкционированного доступа и тех последствий, которые могут наступить в случае возможных преступных посягательств на названные выше ресурсы.

Анализ ресурсов предприятия обычно выполняют по следующим характерным признакам не только ресурсов, но и предприятия, на котором эти ресурсы находятся:

- 1) по значимости объекта охраны;
- 2) по концентрации размещенных на объекте ресурсов;
- 3) по последствиям, которые могут иметь место в случае возможных преступных посягательств на перечисленные выше ресурсы;
 - а) по опасности хранящихся на объекте материалов или по опасности производств, расположенных на этом объекте;

б) по величине материального ущерба, к которому могут привести противоправные действия нарушителя;

4) по сложности обеспечения требуемого уровня защиты объекта.

Цели системы охраны предприятия или организации, учитывающие перечисленные характерные признаки ресурсов, позволяют отнести предприятие или организацию к соответствующей категории. Установленная категория объекта охраны указывает на необходимую для такого объекта техническую укрепленность, а также позволяет принять обоснованное решение по необходимым мерам способным обеспечить минимально необходимый уровень безопасности объекта охраны после оборудования его техническими средствами и системами охраны.

Достичь сформулированные цели можно, решив ряд задач. Так, обеспечить необходимую охрану объекта, в связи с его значимостью можно, реализовав режимные меры, которые должны решать задачи пропускного и внутриобъектового режимов. В свою очередь задача реализации пропускного режима может распадаться на задачу реализации пропускного режима в рабочее время с помощью применения системы контроля и управления доступом и в нерабочее время, применяя систему охранной сигнализации для того, чтобы исключить несанкционированное проникновение в охраняемые помещения. Для достижения сформулированных целей на каждом предприятии и в организации решаются свои задачи, которые обусловлены особенностями объекта охраны и его ресурсами.

2.4. Описание объекта охраны. Категорирование

Для обоснованного принятия решения о целях системы охраны предприятия или организации следует, как уже отмечалось, определить, что именно надо защищать, т. е. необходимо выяснить, что представляет собой объект охраны и какими ресурсами он располагает. При недостаточно полном описании характеристик объекта система безопасности может оказаться либо избыточной с чрезмерной защитой незначительного имущества, либо не будет обеспечивать защиту важных частей объекта. Важным является также то, кто будет осуществлять охрану объекта. Здесь особое значение имеет случай, когда предполагается, что объект будет передаваться под

охрану подразделениям Департамента охраны Министерства внутренних дел Республики Беларусь.

Описание таких объектов начинается с анализа того, что подлежит охране и что представляет собой сам объект. В результате такого анализа устанавливается соответствие объекта категории согласно классификации объектов по требуемому обеспечению их технической укреплённости [11]. Согласно этой классификации, объекты подразделяются на пять категорий. Деление объектов на категории выполняется в зависимости от следующих факторов:

- 1) в зависимости от значимости объекта;
- 2) в зависимости от концентрации размещённых на объекте ресурсов:
 - а) материальных ценностей;
 - б) художественных ценностей;
 - в) исторических ценностей;
 - г) секретной документации и изделий;
 - д) жизненно важных материальных, финансовых средств и услуг, сгруппированных по функциональному назначению и используемых для удовлетворения жизненно необходимых потребностей населения (продукты питания, жильё, предметы первой необходимости, предметы медицинского, санитарно-эпидемиологического, информационного, транспортного, коммунально-бытового обеспечения);
- 3) в зависимости от последствий, которые могут иметь место в случае возможных преступных посягательств на названные выше ценности и вещества;
- 4) в зависимости от сложности обеспечения требуемого уровня защиты объекта.

Анализ перечисленных факторов в отношении объекта охраны позволяет определить его категорию. Определение категории объекта охраны начинается с оценки их значимости. **По значимости** объекты охраны подразделяются на:

- **особо важные**, объекты или специальные помещения особо важных объектов (определяется органами государственной власти Республики Беларусь);
- объекты дипломатических представительств, приравненных к ним международных организаций и консульских учреждений иностранных государств в Республике Беларусь;
- складские здания, кассы предприятий, учреждений, организаций;

– помещения (комнаты) для хранения наркотических, психотропных, ядовитых, бактериологических и токсичных веществ и препаратов;

– объекты, предназначенные для осуществления деятельности по изготовлению печатей и штампов;

– объекты, на (в) которых осуществляется полиграфическая деятельность;

– сервисные зоны банкоматов:

а) с сейфами I класса устойчивости ко взлому, расположенные вне зоны реагирования нарядов милиции Департамента охраны МВД Республики Беларусь;

б) с сейфами II–III класса устойчивости ко взлому, расположенные в зоне реагирования нарядов милиции Департамента охраны МВД Республики Беларусь;

– здания (помещения) следующего назначения:

а) органов прокуратуры;

б) Следственного комитета;

в) Государственного комитета судебных экспертиз;

г) судов;

д) телерадиокомпаний;

е) телевизионных и радиовещательных центров;

ж) республиканских органов государственного управления и иных государственных организаций, подчиненных Совету Министров;

з) местных Советов депутатов;

и) местных исполнительных и распорядительных органов;

к) офисные помещения предприятий, учреждений, организаций;

л) объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски и т. п.).

Для определения значимости объекта составляется перечень его характеристик из перечисленных выше, которые указывают на его значимость. Например, указывается, что здание относится к Следственному комитету или объект охраны является офисным помещением организации (указывается наименование организации) и т. п. Целью системы охраны такого объекта будет обеспечение режимных мер, соответствующих установленной значимости.

Следующим шагом по анализу объекта является **установление факта хранения, переработки или реализации драгоценных металлов и камней, изделий из них**. Составляется перечень мест на

объекте, где расположены материальные ценности, драгоценные металлы и камни, изделия из них, т. е. перечисляются следующие помещения:

- хранилища;
- кладовые;
- сейфовые комнаты.

Назначение помещений определяется для объектов, к которым относятся:

- ювелирные магазины;
- пункты скупки драгоценных металлов и драгоценных камней;
- ломбарды;
- помещения для хранения драгоценных металлов для зубопротезирования;
- предприятия по производству ювелирных изделий, обработке драгоценных камней;
- мастерские по ремонту и изготовлению ювелирных изделий и т. п.

Кроме того, устанавливается факт наличия переработки, хранения либо реализации драгоценных металлов и камней, изделий из них на данном объекте охраны.

Анализ перечисленной информации на соответствие требованиям [11] позволяет отнести объект к той или иной категории по признаку хранения, переработки или реализации драгоценных металлов и камней, изделий из них, а сами материальные ценности определяют цели создания системы охраны.

Важным для определения категории охраняемого объекта и целей создания системы охраны является также установление возможности отнести объект к **объектам повышенной опасности** или **жизнеобеспечения**.

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

Объект жизнеобеспечения – объект, на котором сконцентрированы жизненно важные материалы, финансовые средства и услуги, сгруппированные по функциональному назначению и используемые для удовлетворения жизненно необходимых потребностей

населения (например, в виде продуктов питания, жилья, и предметов первой необходимости, а также медицинского, санитарно-эпидемиологического, информационного транспортного, коммунально-бытового обеспечения).

Анализ составленного списка на предмет соответствия той или иной категории по ТКП 652-2020 [11] позволяет отнести объект к категориям от 1-й до 4-й по значимости.

К объектам 5-й категории относят: жилые дома (помещения) физических лиц под которыми понимаются квартиры или помещения в блокированных или многоквартирных жилых домах, жилые дома, садовые домики на дачах (включая примыкающие к ним строения), а также расположенные отдельно от них хозяйственные (подсобные и дворовые) постройки, гаражи, иные строения общей площадью (каждого строения) до 100 квадратных метров включительно, принадлежащие физическим лицам на праве собственности, либо предоставление в нем каких-либо услуг третьим лицам, указанное помещение классифицируется как объект 1–4 категории в зависимости от вида осуществляемой деятельности и наличия в нем материальных ценностей.

В случае, когда материальные, художественные, историко-культурные и иные подобные ценности, размещены не на всей площади объекта, а в его отдельных помещениях, требования к объекту 2-й категории устанавливаются только для этих помещений (комнат), а не для всего объекта в целом.

Отметим, что каждой установленной категории должны соответствовать определенные классы защиты конструктивных элементов объектов охраны. Требования к ним перечислены в [11].

Использование подходов ТКП 652-2020 [11] для определения ресурсов подлежащих охране не позволяет в полном объеме определить цели системы охраны. Для завершения определения целей создаваемой системы охраны необходимо учесть ресурсы, рассмотренные в ТКП 627-2018 [12], определяющем требования по применению технических средств и систем охраны. Согласно этому документу, категорирование по значимости объекта охраны необходимо дополнить критически важными объектами.

Критически важные объекты – объекты социальной, производственной, инженерно-транспортной, энергетической, информационно-коммуникационной и иной инфраструктуры, нарушение функ-

ционирования которых в результате акта терроризма может способствовать дестабилизации общественного порядка и достижению иных целей терроризма и (или) повлечь за собой человеческие жертвы, причинение вреда здоровью людей или окружающей среде, значительный материальный ущерб и нарушение условий жизнедеятельности людей [13].

В рамках рассматриваемой классификации к объектам повышенной опасности дополнительно отнесены объекты, на которых нарушение их функционирования может привести к негативным последствиям для обороны, национальной безопасности, международных отношений, экономики, другой сферы хозяйствования или инфраструктуры страны либо для жизнедеятельности населения. Кроме того, противоправные действия на таких объектах могут привести к материальному ущербу государству, обществу, организации, экологии или иному владельцу свыше 1000 базовых величин.

По величине материального ущерба, к которому могут привести противоправные действия нарушителя, дополнительно относят объекты подгруппы БI – объекты, противоправные действия на которых могут привести к материальному ущербу государству, обществу, организации, экологии или иному владельцу до 250 базовых величин включительно. Объекты подгруппы БII – объекты, противоправные действия на которых могут привести к материальному ущербу государству, обществу, организации, экологии или иному владельцу от 250 до 1000 базовых величин включительно.

Итак, использование ТКП 627-2018 [12] позволяет для определения целей системы охраны использовать подходы, применяемые для классификации объектов охраны на категории А и Б с последующим дополнительным делением этих категорий на подгруппы АI и АII, БI и БII. Деление объектов охраны на категории А и Б называют категорированием объектов охраны.

Категория охраняемого объекта – классификация охраняемого объекта в процессе комплексной оценки объекта, учитывающая его социальную, экономическую, культурную, и иную значимость, в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных противоправных посягательств на них, сложности обеспечения требуемого уровня защиты объекта.

Объекты подгруппы А1 – это особо важные, повышенной опасности, критически важные объекты, а также объекты, включенные

в Перечень объектов подлежащих обязательной охране Департаментом охраны МВД Республики Беларусь. Объекты подгруппы АП это специальные помещения объектов подгруппы АІ.

Тактика охраны объекта в значительной степени определяется категорией и требуемым для данного объекта уровнем безопасности.

Уровни безопасности бывают низкий, средний, повышенный и высокий. Требования к применяемым техническим средствам и системам охраны, которые обеспечивают необходимый уровень безопасности, оговорены в ТКП 627-2018 (33030) [12].

2.5. Уязвимости объекта охраны

Основной принцип, который должен соблюдаться при проектировании систем охранной сигнализации, состоит в обязательном оснащении техническими средствами охранной сигнализации всех уязвимых мест объекта (помещения), защищаемого с помощью системы охранной сигнализации. Давая характеристику помещениям объекта, необходимо составить список всех уязвимых мест с их характеристиками, в необходимых случаях указать являются ли они капитальными или нет.

Уязвимыми местами считаются строительные конструкции объекта (помещения), являющиеся вероятными местами проникновения нарушителя.

Строительная конструкция сооружения – это часть сооружения, выполняющая следующие функции:

- 1) несущие;
- 2) ограждающие;
- 3) в открытом виде – эстетические функции.

Несущие конструкции – это элементы, которые воспринимают все силовые нагрузки и не силовые воздействия и передают их на грунт.

Ограждающие конструкции – это элементы, которые ограничивают внешний контур здания или сооружения и разделяют его внутреннее пространство на изолированные объемы (помещения).

Ограждающие конструкции, в свою очередь, подразделяют на наружные и внутренние. Основная функция наружных ограждающих конструкций – защищать строение от различных внешних воздействий: температурных, атмосферных (осадки, излучения), химических, акустических и др.

Внутренние ограждающие конструкции предназначены для организации пространства внутри здания или сооружения и обеспечения звукоизоляции отдельных помещений.

К ограждающим конструкциям относят:

1) перегородки;

2) стены:

а) не несущие;

б) самонесущие (самонесущие стены – это стены, на которые ничего не опирается и нагрузки в них возникают лишь от собственного веса);

3) элементы заполнения проемов:

а) окна;

б) ворота;

в) двери;

4) витражное остекление;

5) зенитные фонари и другие.

Определение понятия «Уязвимое место» содержит понятие «объект». В соответствии с ТКП 627-218 [12]: объект – это здания, сооружения, строения их части (включая изолированные помещения), иные объекты недвижимого имущества, участки местности, транспортные средства и другое имущество, подлежащее охране.

К уязвимым местам относят:

1) остекленные конструкции периметра, (окна независимо от их противовзломной стойкости и оснащения инженерно-техническими средствами защиты);

2) строительные конструкций (например, двери), имеющих непосредственный выход наружу или в неохраемое помещение;

3) погрузочно-разгрузочные люки, вентиляционные шахты, короба, дымоходы независимо от их оснащения инженерно-техническими средствами защиты;

4) смежные строительные конструкции, которые представляя собой строительные конструкции (например, стены), разделяющие помещение на охраняемый и неохраемый объект или на охраняемые объекты, принадлежащие различным потребителям охранной услуги или одному, но имеющему различное время охраны (например, граничащие с помещениями, принадлежащими другим организациям и учреждениям, а также котельными, бойлерными, электро-

щитовыми, техническими подвалами, подъездами жилых зданий, бесхозными строениями и т. п.;

5) некапитальные (по охране) строительные конструкции (стены, полы, потолки).

Капитальными (по охране) считаются следующие строительные конструкции (стены, перегородки, полы, потолки):

- кирпичные стены толщиной 250 мм и более для объектов подгруппы БП и 380 мм и более для объектов подгруппы АІ;

- наружные стеновые панели, внутренние стеновые панели и блоки стеновые из легких бетонов толщиной от 100 до 300 мм для объектов подгруппы БП и 300 мм и более для объектов подгруппы АІ;

- стены из монолитного железобетона, изготовляемого из тяжелых бетонов толщиной до 100 мм и более для объектов подгруппы БП и от 100 до 300 мм для объектов подгруппы АІ;

- пустотные железобетонные плиты толщиной 220 мм и более из легких бетонов для объектов подгруппы БП;

- пустотные железобетонные плиты толщиной 160 мм и более из тяжелых бетонов для объектов подгруппы БП и 220 мм и более для объектов подгруппы АІ;

- сплошные железобетонные перекрытия толщиной 120 мм и более из легких бетонов для объектов подгруппы БП;

- сплошные железобетонные перекрытия толщиной 120 мм и более из тяжелых бетонов для объектов подгруппы АІ.

Некапитальными (по охране) считаются строительные конструкции из стеклопрофилита, стеклоблоков, бревен, бруса, гипсолита, гипсобетона, а также из кирпича или бетона толщиной меньшей, чем указано в приложении А ТКП 627-2018 [12].

Из приведенного перечня видно, что для правильной оценки капитальности строительной конструкции необходимо знать категорию объекта и требуемый для этой категории класс (степень) защиты конструктивных элементов.

2.6. Модель нарушителя

Ранее было показано, что в качестве угроз, создающих опасность преднамеренного противоправного нанесения ущерба объекту, могут выступать лица, мотивация и возможности которых ориентированы на кражу имущества, диверсию или на другие злонамеренные

действия, ведущие к пропаже имущества на объекте. Таким образом ущерб предприятию или организации может быть нанесен в результате несанкционированного доступа на объект охраны и последовавшими за ним противоправными посягательствами нарушителя на средства труда, материальные, финансовые, информационные и другие виды ресурсов предприятия. Ущербом от преступного посягательства будем называть экономические, экологические или социальные последствия (убытки, потери) от такого преступного посягательства нарушителя на охраняемый объект [11].

Модель нарушителя содержит следующие сведения:

1. Описание типов возможных нарушителей.
2. Мотивы нарушителя.
3. Потенциальные цели нарушителя в отношении объекта.
4. Тактику возможных действий.
5. Численность возможных нарушителей.
6. Возможности, которыми могут обладать нарушители.

Общепринятым является деление всех нарушителей на три большие группы:

- 1) посторонние лица;
- 2) сотрудники;
- 3) посторонние лица, действующие в сговоре с сотрудниками.

Группу сотрудников составляют лица, обладающие информацией о действиях службы безопасности на объекте, о характеристиках системы безопасности, а также те, кто имеет доступ без сопровождения на объект и те, кто имеет интересы, связанные с безопасностью.

Кроме того, сотрудники делятся на следующие три разновидности:

- 1) пассивные лица;
- 2) активные лица, не вовлеченные в насильственные действия;
- 3) активные лица, участвующие в насильственных действиях.

Пассивные лица – это, например, те, кто передает информацию.

Активные лица, не вовлеченные непосредственно в насильственные действия, подготавливают входы и выходы, отключают сигнализацию и связь. Численность таких нарушителей может быть самой разной, но наиболее вероятно, что нарушитель такого типа один.

Особенно тяжелую проблему представляет собой силы охраны. Охранники ответственны за 41 % преступлений, совершенных против охраняемых объектов.

Отметим, что система охранной сигнализации наиболее эффективна для посторонних лиц, действующих в одиночку или в сговоре с сотрудниками. Для защиты от сотрудников применяют контроль и учет имущества, которые осуществляются с использованием соответствующих процедур проверок и инвентаризации, а также программ проверок персонала. По имеющейся информации сотрудники являются наиболее вероятными нарушителями системы безопасности.

К посторонним лицам можно отнести тех, кто не обладает информацией о действиях службы безопасности на объекте, о характеристиках системы безопасности, а также те, кто не имеет доступа без сопровождения на объект, и те, кто не имеет интересов, которые связаны с безопасностью.

Посторонними лицами могут быть прохожие, но прохожие вблизи, например, здания суда и университета очевидно будут сильно отличаться друг от друга. К посторонним лицам можно отнести покупателей в магазине и посетителей детского сада, которые тоже имеют целый ряд отличительных особенностей. Таким образом посторонние лица для каждого конкретного объекта имеют свои отличительные признаки.

Мотивы, побуждающие потенциальных нарушителей предпринять преступные действия против объекта охраны, можно свести к трем категориям:

1. Идеологические.
2. Экономические.
3. Личные.

Идеологические мотивы связаны с политической или философской системой взглядов и характерны для политических террористов, а также некоторых групп философских и религиозных фанатиков.

Экономические мотивы обусловлены желанием получить финансовую выгоду. Преступники могут рассматривать информацию или материальное имущество как потенциально привлекательные цели для кражи с последующим выкупом или продажей похищенных ценностей, а также для вымогательства.

Личные мотивы. Круг лиц, совершающих преступления по личным причинам, варьируется от враждебно настроенного служащего, обиженного на работодателя, до психопата. Возможны нападения ради развлечения. Причиной нападений могут быть наркотическая или алкогольная зависимость, желание сбыть наркотики.

Возможности потенциального нарушителя имеют чрезвычайную важность для разработчика системы безопасности.

Вопросы, которые рассматриваются при описании возможностей потенциального нарушителя:

1. Будет ли нарушитель обладать оружием и взрывчатыми веществами, если да, то какими?

2. Имеющиеся у нарушителя инструменты и оборудование (болторезы, клещи, ножовочное полотно, электрические инструменты, газовые резаки и т. д.).

3. Средства транспортировки (грузовой автомобиль, вертолет и т. д.).

4. Технические навыки и опыт нарушителя.

5. Возможность использования инструментов и оборудования, имеющегося на объекте охраны.

Тактика нарушителя. Говоря о тактике нарушителя, имеют в виду три основных тактических приема:

- 1) насилие;
- 2) скрытность;
- 3) обман.

При использовании тактики насилия нарушитель преодолевает систему охраны, не скрывая своих намерений, не опасаясь быть замеченным. Скорее всего, в этом случае нарушитель имеет оружие, чтобы принудить других не препятствовать достижению его цели.

При использовании тактики скрытности преступник старается тайком проникнуть на объект. Его задача состоит в том, чтобы оставаться незамеченным как можно дольше.

Обман подразумевает использование реальных или поддельных документов для получения доступа к информации или имуществу и их изъятия под видом, изъятия, санкционированного руководством.

Источниками необходимой для создания системы безопасности информации, в том числе информации о вероятных нарушителях являются:

- 1) разведывательные данные;
- 2) исследования вопросов преступности;
- 3) профессиональные организации и службы в области безопасности;
- 4) печатные издания и Интернет;

5) правительственные директивы и документы законодательных органов.

Разведывательные и другие данные можно получить в результате взаимодействия с правоохранительными и разведывательными органами.

2.7. Зоны доступа и рубежи охраны объекта

Обеспечение защиты объекта от несанкционированного доступа и противоправных посягательств означает реализацию ряда мер, включая режимные и технические. Режимные меры предполагают установление на объекте внутриобъектового и пропускного режимов. **Установление внутриобъектового режима** требует ответа на вопрос: **кто, в каких помещениях объекта и на протяжении какого времени может находиться?** Чтобы ответить на этот вопрос весь объект охраны делится на **зоны доступа**. Несанкционированное нахождение нарушителя в зоне доступа или его переход из одной зоны в другую должно обнаруживаться системой охраны.

Переход из одной зоны доступа в другую происходит в некоторой части пространства объекта, которую обычно занимают ограждающие конструкции образующие **рубеж охраны**. Рубежом охраны является и сама зона доступа, нахождение и перемещение людей в которой, как санкционированное, так и несанкционированное, должно контролироваться согласно пропускному и внутриобъектовому режимам. Именно в этой части пространства объекта охраны должно произойти обнаружение несанкционированного проникновения, попытки проникновения или перемещение в зоне доступа. **Обнаружение несанкционированного проникновения**, попытки проникновения в зону доступа или противоправных посягательств на охраняемые ресурсы, хранящиеся в этой зоне доступа, является **способом охраны**.

Для организации эффективной охраны объекта, состоящего из двух и более изолированных объемов (помещений), необходимо обязательно обеспечить условия для выполнения в этих помещениях основных производственных функций, которые определяются реализацией внутриобъектового режима, а для этого все помещения необходимо распределить по зонам доступа, каждая из которых характеризуется рабочим временем и временем охраны (режим работы) или уровнем приоритета (правом) доступа в эти помещения как со-

трудников, так и случайных лиц. После деления объекта охраны на зоны доступа в каждой из зон доступа определяются рубежи охраны.

В разные зоны доступа должны входить помещения:

- охраняемые и неохраняемые;
- принадлежащие различным потребителям охранной услуги;
- принадлежащие одному потребителю, но имеющие различное время охраны;
- принадлежащие разным организациям и учреждениям;
- котельные, бойлерные, электрощитовые, технические подвалы и т. п.

Названные характеристики помещений являются критериями для распределения помещений по зонам доступа, образуя принципы деления объекта охраны на зоны доступа.

Зона доступа на объекте охраны – это помещение(я), для которого определено время нахождения в нем людей или время его охраны (режим работы), а также уровень приоритета, т. е. право доступа в эти помещения как сотрудников, так и случайных лиц в соответствии с режимом работы.

Объект охраны обычно может иметь **четыре основных вида зоны доступа**:

- **зона доступа первого вида** или **зона свободного доступа** – здания, территории, помещения, доступ в которые персоналу, посетителям и другим лицам не ограничен;

- **зона доступа второго вида** или **зона ограниченного по времени**;

- **зона доступа третьего вида** или **зона ограниченного по уровню приоритета доступа**;

- **зона доступа четвертого вида** – **специальные** помещения объекта, доступ в которые имеют **строго определенные сотрудники**, к этому виду зоны доступа могут относиться также **помещения непосредственного сосредоточения** и хранения материальных и иных ценностей.

Зона ограниченного по времени доступа предполагает, например, доступ покупателей в торговые залы магазина в соответствии со временем работы торговых залов, при этом персоналу доступ на рабочие места может быть разрешен в соответствии с их рабочим временем.

Зона доступа ограниченного уровнем приоритета предполагает наличие ограничений по доступу в отдельные помещения объекта

отдельным группам персонала, например только имеющим пропуск, а посетителям доступ может быть разрешен по разовым пропускам или в сопровождении персонала.

2.8. Принцип рубежей или зональный принцип функционирования системы охраны

Принцип рубежей означает создание последовательных рубежей, в которых угроза, т. е. проникновение нарушителя на территорию охраняемого объекта (в зону доступа) должно быть обнаружено, а его продвижению внутрь зоны доступа или по территории этой зоны будут препятствовать надежные преграды. Таким образом, **рубежом** в этом случае является часть пространства объекта, в котором решаются следующие задачи: во-первых, происходит **обнаружение** нарушителя и, во-вторых, с помощью инженерных средств охраны создаются препятствия для продвижения нарушителя вглубь зоны доступа объекта, т. е. **происходит задержка его продвижения по объекту**. При этом задержка продвижения нарушителя должна происходить после его обнаружения. Пространство рубежа охраны образуют ограждающие конструкции. Ограждающими конструкциями могут быть забор, стены, окна, двери, ворота, калитки и т. п. Эти конструкции ограничивают пространство каждой отдельной зоны доступа объекта охраны, включая пространство, ограниченное внешним контуром объекта. Границы зон доступа и объекта в целом называют периметром зоны доступа или объекта.

Местами проникновения нарушителя внутрь объекта охраны являются уязвимые места, которыми могут быть строительные конструкции, перечисленные выше, а также, например, следующие строительные конструкции [12]:

1) остекленные конструкции периметра, строительные конструкции, имеющие непосредственный выход наружу или в неохраняемое помещение, погрузочно-разгрузочные люки, вентиляционные шахты, короба, дымоходы;

2) смежные строительные конструкции, которые представляют собой строительные конструкции, разделяющие помещение на охраняемый и неохраняемый объект или на охраняемые объекты, принадлежащие различным потребителям охранной услуги или одному, но имеющее различное время охраны;

3) некапитальные строительные конструкции (стены, полы, потолки). Какие конструкции относят к капитальным, а какие к некапитальным определяется в ТНПА [12].

Рубежи охраны **могут** делиться на зоны контроля, которые иногда называют рубежами охранной сигнализации. **Рубеж охранной сигнализации или зона контроля** – это шлейф охранной сигнализации, контролирующий периметр или часть периметра, объем или часть объема объекта, сами ценности или подходы к ним, на пути возможного движения нарушителя к материальным ценностям. Индикация последовательности срабатывания рубежей охранной сигнализации или зон контроля позволяет отслеживать маршрут перемещения нарушителя по соответствующим зонам доступа объекта охраны.

Шлейф сигнализации – это цепь (электрическая, радиоканальная, оптоволоконная или другая), соединяющая выходные узлы технических средств обнаружения нарушителя (охранных извещателей) и предназначенная для передачи информации о контролируемых параметрах зоны контроля.

Обязательным условием обеспечения повышенного и высокого уровней защиты объектов (помещений) подгрупп А1, АП и БП должно являться наличие многорубежной системы охранной сигнализации, когда применяется не менее двух видов рубежей охранной сигнализации.

Рубежи охранной сигнализации или зоны контроля могут быть трех разновидностей:

- первый рубеж охранной сигнализации – шлейф охранной сигнализации содержит извещатели для блокировки строительных конструкций периметра зоны доступа или объекта охраны в целом;
- второй рубеж охранной сигнализации – шлейф охранной сигнализации содержит извещатели для блокировки объема и площадей зон доступа или объекта охраны в целом, в том числе «ловушки»;
- третий рубеж охранной сигнализации – шлейф охранной сигнализации содержит извещатели для блокировки мест непосредственного хранения ценностей.

Блокировка – оборудование техническими средствами и системами охраны объекта или его части, обеспечивающее формирование извещений о проникновении (попытке проникновения), нарушении целостности.

Рубежами охранной сигнализации объекта считаются независимые друг от друга шлейфы охранной сигнализации, которые поз-

воляют осуществлять **раздельное управление** системами охранной сигнализации частей объекта, которые также называют зонами контроля. Управление системами охранной сигнализации предполагает возможность осуществлять взятие объекта под охрану и снятие с охраны ручным или автоматическим способом каждой зоны контроля независимо друг от друга.

Задачи, которые решают рубежи охранной сигнализации, отличаются друг от друга. Задача, которую должен решать первый рубеж охранной сигнализации, состоит в том, чтобы не допустить проникновение нарушителя на территорию объекта. На этом рубеже нарушитель в первую очередь должен быть обнаружен, а затем с помощью инженерных средств задержан на время, которое необходимо для прибытия группы задержания. Ущерб, который может быть нанесен объекту при попытке несанкционированного проникновения нарушителя с использованием тактики насилия, будет состоять из разрушенных или поврежденных строительных конструкций периметра (окна, двери и т. д.).

Задача, которую решает второй рубеж охранной сигнализации, – обеспечить обнаружение нарушителя, который проник внутрь объекта, не нарушая первый рубеж или сумев его обойти, например, спрятавшись на объекте в то время, когда объект не находился на охране. После обнаружения такой нарушитель должен быть ограничен в своем передвижении по объекту, а его маршрут движения должен отслеживаться.

Периметр и конфигурация зоны контроля могут иметь большие размеры и площадь. В этом случае рубеж охранной сигнализации может делиться на части, например, фасад и тыл периметра зоны доступа. Управляться зоны контроля одного и того же рубежа могут независимо друг от друга по разному алгоритму. Например, тыл 1-го рубежа охраны в рабочее время может сниматься с охраны, а фасад нет. Второй рубеж охраны может содержать «ловушки», т. е. скрытно установленные охранные извещатели на путях возможного перемещения нарушителя. Такие ловушки могут помочь отследить маршрут перемещения нарушителя по зоне доступа объекта охраны.

Третий рубеж решает задачу обнаружения и задержки нарушителя, который сумел обойти первые два рубежа. После обнаружения на третьем рубеже нарушитель должен быть ограничен в своих возможностях овладеть охраняемыми материальными ценностями или

другими объектами охраны до момента прибытия группы задержания, например, достигнуть этого можно в результате применения сейфа или других инженерных средств защиты.

Структура системы рубежей охранной сигнализации или зон контроля объекта строится так, чтобы обеспечить возможность с максимальной точностью определять место проникновения или нахождения нарушителя на объекте. В результате такая структура зон контроля позволяет лицам, осуществляющим охрану объекта, принимать правильные меры реагирования. Для этого, например, периметр зоны доступа объекта может разбиваться на участки, контролируемые отдельными рубежами (шлейфами) охранной сигнализации с индикацией каждого из них на приборе приемно-контрольном (шлейф сигнализации тыла, фасада, левой стороны тыла 1-го этажа, правой стороны 2-го этажа и т. п.).

Процедура разработки структуры зон доступа и рубежей охраны, а также зон контроля или рубежей охранной сигнализации объекта охраны состоит из следующих четырех шагов:

1. Определяется перечень помещений для каждого вида зон доступа.

1.1. Помещения свободного доступа.

1.2. Помещения ограниченного доступа **по уровню приоритета**, а именно для каждого собственника (хозяина или ответственного);

1.3. Помещения, ограниченного **по времени доступа** (помещения каждого собственника (ответственного) делят на группы с одинаковым временем работы);

1.4. Помещения **четвертого вида** зон доступа – специальные помещения объекта, доступ в которые имеют строго определенные сотрудники и руководители (например, помещения руководства объекта и охраны, а также помещения непосредственного сосредоточения и хранения материальных и иных ценностей).

2. Определяются области пространства (в том числе помещения), которые образуют **первый и второй рубежи охраны** в пределах зон доступа первого и второго видов.

2.1. Определяют области пространства (помещения) образующие второй рубеж охраны в каждой зоне доступа, при этом зона доступа может иметь несколько областей образующих второй рубеж и управлять этими областями зачастую необходимо независимо друг от друга;

2.2. Определяют области пространства, образующие первый рубеж охраны, включая строительные конструкции, ограждающие зоны доступа.

3. Определяются **зоны контроля** первого и второго рубежей охраны, т. е. области пространства или помещения, образующие рубежи охраны и контролируемые одним шлейфом охранной сигнализации. Зоны контроля называют также первым или соответственно вторым рубежом охранной сигнализации. Один рубеж охраны может состоять из нескольких рубежей охранной сигнализации или зон контроля. На несколько зон контроля при необходимости можно делить **зоны ограниченного по времени или уровню приоритета доступа**. Разбиение рубежа охраны на зоны контроля выполняется в следующей последовательности:

3.1. Помещения, образующие второй рубеж охраны и при этом имеющие одного собственника (ответственного) с одинаковым временем работы, расположенные так, что все помещения могут контролироваться любым сотрудником из любой точки помещения, образуют одну зону контроля или один второй рубеж охранной сигнализации. Второй рубеж охраны при необходимости может состоять из нескольких зон контроля. Это может произойти в случае, если второй рубеж представляет собой большой объем со сложной конфигурацией, состояние которого сложно контролировать. В этом случае второй рубеж делится на несколько зон контроля, которые управляются независимо друг от друга.

3.2. Составляется перечень уязвимых мест, входящих в первый рубеж охранной сигнализации каждой зоны контроля (если их несколько) второго рубежа охраны. При этом зоны контроля 1-го рубежа охранной сигнализации у разных зон контроля второго рубежа не должны иметь общих уязвимых мест.

4. Составляется перечень помещений, которые можно отнести к зоне доступа третьего вида. Каждое из этих помещений будет отдельной зоной контроля.

Правильно разработанная структура зон контроля объекта охраны позволяет определить оптимальное количество шлейфов охранной сигнализации для своевременного обнаружения места проникновения нарушителя на объект охраны и наблюдения маршрута его перемещения. Все это дает возможность группе задержания с меньшими затратами времени настигнуть и задержать нарушителя.

3. ОСНОВНЫЕ ПОДСИСТЕМЫ ТЕХНИЧЕСКОЙ СИСТЕМЫ ОХРАНЫ

Технические системы охраны как совокупность совместно действующих технических средств охраны являются составной частью системы охраны объекта. Именно технические системы охраны призваны помочь в реализации применяемых на объекте способов охраны, к которым относят установление не только пропускного, но и внутриобъектового режимов. Важным для достижения целей по недопущению или уменьшению ущерба ресурсам, которые сконцентрированы в отдельных помещениях и на территории объекта, является реализация режимных мер одновременно с применением технических средств охраны (в том числе охранной сигнализации). Наряду с охранной сигнализацией к техническим системам охраны относят системы контроля и управления доступом, телевизионные системы видеонаблюдения, а также системы передачи извещений, которые совместно образуют систему централизованного наблюдения (СЦН). Каждая из названных подсистем в ходе обеспечения охраны объекта призвана решать свои задачи.

Например, пропускной режим предполагает решение следующих задач:

- исключить бесконтрольное перемещение лиц или материальных ценностей через границу охраняемого объекта или внутри этого объекта;
- обеспечить санкционированный проход (проезд) лиц и автотранспорта персонала, осуществляющего свою деятельность на территории учреждения, посетителей данного учреждения, автотранспорта, в том числе служебного, а также ввоз (вывоз) материальных ценностей.

Реализация внутриобъектового режима предполагает в том числе решение задач:

- контроль нахождения на территории учреждения или в отдельных его помещениях лиц и организаций, осуществляющих свою деятельность;
- порядок проведения ремонтно-строительных, погрузочно-разгрузочных и иных работ на территории, в зданиях и помещениях учреждения;
- поддержание общественного порядка и режимов безопасности.

Решение перечисленных задач происходит с помощью различных способов, в том числе:

- 1) обнаружения несанкционированного проникновения, попытки проникновения на охраняемый объект или противоправных посягательств на охраняемые ресурсы предприятия, в том числе с помощью систем охранной сигнализации;

- 2) оборудования охраняемых объектов техническими системами охраны, включая системы контроля и управления доступом и телевизионные системы видеонаблюдения;

- 3) применения инженерно-технических средств защиты и т. п.

Таким образом, система централизованного наблюдения представляет собой совокупность программно-аппаратных средств, предназначенных для обнаружения криминальных угроз на охраняемых объектах, посредством использования объектовой подсистемы СЦН, а также для передачи этой информации посредством системы передачи извещений (СПИ) на пульт централизованного наблюдения (ПЦН), расположенный в пункте централизованной охраны (ПЦО) [14].

Система централизованного наблюдения в общем случае включает в себя следующие устройства:

- 1) пульт централизованного наблюдения;
- 2) систему передачи извещений;
- 3) объектовую подсистему СЦН.

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

В пункте централизованной охраны располагается **пульт централизованного наблюдения**. ПЦН – это самостоятельное техническое средство или составная часть системы передачи извещений, устанавливаемая в пункте централизованной охраны для приема от пультовых оконечных устройств или ретранслятора(ов) извещений о проникновении на охраняемые объекты и (или) пожаре на них, служебных и контрольно-диагностических извещений, обработки, отображения, регистрации полученной информации и представления ее в заданном виде для дальнейшей обработки, а также (при

наличии обратного канала) для передачи через пультовое оконечное устройство на ретранслятор(ы) и объектовые оконечные устройства команд телеуправления [15]. Формируя команды телеуправления, например, можно управлять режимами объектовых подсистем. Вид ПЦН показан на рис. 1.



Рис. 1. Пульты централизованного наблюдения для использования в системах охраны

Подсистема объектовая. Составная часть системы централизованного наблюдения, предназначенная для обнаружения криминальных угроз посредством контроля состояния технических средств охраны охраняемого объекта и передачи тревожной, контрольно-диагностической, служебной, видео и другой информации в подсистему передачи информации.

Технические системы охраны в составе подсистем объектовых представляют собой совокупность совместно действующих технических средств охраны, установленных на охраняемом объекте и объединенных системой инженерных сетей и коммуникаций. Примером таких систем являются системы тревожной сигнализации, передачи извещений, контроля и управления доступом, телевизионные системы видеонаблюдения и т. п. Каждая из названных систем призвана решать свои задачи.

3.1. Система охранной сигнализации

В соответствии с СТБ [9] **Система тревожной сигнализации** – это совокупность совместно действующих технических средств охраны, предназначенных для обнаружения и (или) сигнализации о наличии опасности. К системам тревожной сигнализации относятся системы охранной сигнализации, ручные системы тревожной сигнализации и т. п. **Системой охранной сигнализации** называют совокупность совместно действующих технических средств для обнаружения проникновения (попытки проникновения) на охраняемые объекты, сбора, обработки, передачи и представления в заданном виде потребителям информации о проникновении (попытке проникновения), другой информации. Информация о проникновении (попытке проникновения) формируется охранными извещателями, которые включаются в шлейфы охранной сигнализации. Шлейф охранной сигнализации представляет собой электрическую цепь, соединяющую выходные цепи охранных извещателей. Он включает в себя соединительные провода и предназначен для выдачи на приемно-контрольный прибор извещений о проникновении (попытке проникновения) [15]. В свою очередь прибор приемно-контрольный является составной частью охранной системы сигнализации, которая предназначена для приема извещений от извещателей и других технических средств, преобразования и передачи извещений, формирования извещений о состоянии системы сигнализации, а также для передачи сформированных им команд на другие устройства. Из сказанного можно сделать вывод о том, что систему охранной сигнализации можно представить состоящей из следующих основных структурных элементов:

- 1) охранные извещатели;
- 2) шлейфы охранной сигнализации, в которые включены охранные извещатели;
- 3) прибор приемно-контрольный, к которому подключены шлейфы охранной сигнализации.

Структура охранной сигнализации показана на рис. 2.

В рассмотренном составе система охранной сигнализации образует локальную систему сигнализации. В этом случае извещения о состоянии, а также управление контролируемым шлейфом, **контролируемыми зонами** осуществляют с помощью средств отобра-

жения информации и управления, входящих в состав прибора приемно-контрольного.

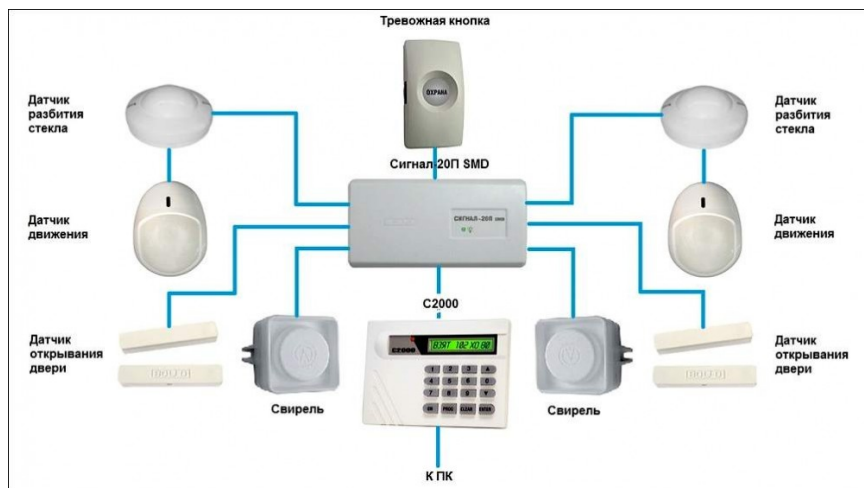


Рис. 2. Структура охранной сигнализации

К прибору приемно-контрольному могут подключаться несколько шлейфов охранной сигнализации, которые образуют контролируемую зону прибора приемно-контрольного. Контролируемая зона [16] представляет собой контролируемый объект, часть объекта и/или территории, рубеж охраны или его часть, состояние которого может быть однозначно отображено с помощью средств индикации (оповещения) или передана информация о его состоянии на пульт централизованного наблюдения. Кроме того, должно быть обеспечено раздельное управление контролируемой зоной. Раздельное управление контролируемой зоной предполагает возможность взятия под охрану шлейфа охранной сигнализации (зоны контроля) и снятие его с охраны независимо друг от друга для любого шлейфа охранной сигнализации. Средствами управления могут быть индикаторные панели, пульта или считыватели устройств ввода идентификационных признаков.

Нахождение шлейфа охранной сигнализации в состоянии «Взят под охрану» означает, что его нарушение (хотя бы один охранный извещатель, включенный в шлейф, сработал) приводит к переходу

ППК в режим «Тревога». В режиме «Тревога» включаются световой и звуковой оповещатели и на ПЦН передается извещение «Тревога».

Нахождение шлейфа охранной сигнализации в состоянии «Снят с охраны» означает, что срабатывание охранного извещателя, включенного в шлейф сигнализации не ведет к передаче на ПЦН извещения «Тревога». Световой и звуковой оповещатели не включаются.

3.2. Система контроля и управления доступом

Для обеспечения охраны объекта большое значение имеет реализация на этом объекте режимных мер, составными элементами которых являются пропускной и внутриобъектовый режимы. Пропускной режим, как известно, представляет собой порядок, обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц, въезда (выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества в зоны доступа объекта охраны. Объект охраны как известно разбивается на зоны доступа, в каждую из которых имеют право проходить строго определенные лица, которые называют субъектами. Проход в зоны доступа осуществляется через точки доступа, которые располагаются на первом рубеже охраны соответствующей зоны доступа. В каждой точке доступа устанавливаются считыватели и исполнительные устройства. Считыватель – это элемент в составе устройства ввода идентификационных признаков, предназначенное для ввода идентификационных признаков. Считыватель передает информацию «свой/чужой» на управляющее устройство (контроллер). Именно эта информация позволяет управляющему устройству принять решение имеет ли право субъект на проход через данную точку доступа. Таким образом, контроллер системы контроля и управления доступом является управляющим устройством, которое предназначено для обработки информации со считывателя, принятия решения и управления исполнительными устройствами. К исполнительным устройствам относятся шлагбаумы, турникеты, двери с замками и тому подобное.

Из сказанного следует, что технические средства, с помощью которых можно обеспечить выполнение пропускного режима, относятся к системам контроля и управления доступа. Под **системой контроля и управления доступом (СКУД)** понимают совокупность совместно

действующих средств (механических, электромеханических, электрических, электронных), обеспечивающих контроль и управление доступом, т. е. перемещением людей, предметов, транспорта в помещениях, зданиях, сооружениях и по территории охраняемых объектов. Управление доступом заключается в его ограничении и санкционировании [9, 17]. Под санкционированным доступом понимают доступ людей или объектов, имеющих право доступа.

Рассмотренная базовая структура системы контроля и управления доступом показана на рис. 3. Из рисунка видно, что идентификаторы, считыватели, контроллеры и исполнительные устройства являются основными компонентами системы контроля и управления доступом.

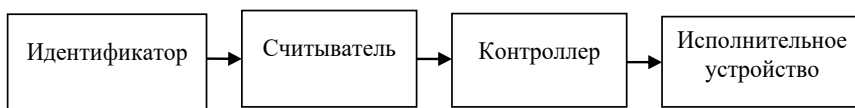


Рис. 3. Базовая структура системы контроля и управления доступом

Таким образом средства контроля и управления доступом по функциональному назначению подразделяют на:

- 1) устройства, преграждающие управляемые в составе преграждающих конструкций и исполнительных устройств;
- 2) устройства ввода идентификационных признаков в составе считывателей и идентификаторов;
- 3) устройства управления в составе аппаратных и программных средств.

Устройства, преграждающие управляемые – устройства, обеспечивающие физическое препятствие доступу людей, транспорта и других объектов и оборудованные исполнительными устройствами для управления их состоянием (двери, ворота, турникеты, шлюзы, проходные кабины и т. п. конструкции).

Устройства исполнительные – устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние устройства, преграждающие управляемые (электромеханические и электромагнитные замки, защелки, механизмы привода шлюзов, ворот, турникетов и т. д.).

Устройства ввода идентификационных признаков – электронные устройства, предназначенные для ввода запоминаемого кода, ввода биометрической информации, считывания кодовой информации с идентификаторов. В их состав входят считыватели и идентификаторы.

Считыватель – устройство, предназначенное для считывания (ввода) идентификационных признаков.

Идентификатор доступа, идентификатор (носитель идентификационного признака) – уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. *Идентификатор, использующий вещественный код* – это предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелки и т. д.)

Идентификация – процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку.

Устройства управления – устройства и программные средства, устанавливающие режим доступа и обеспечивающие прием и обработку информации с устройства ввода идентификационных признаков, управление преграждающими устройствами, отображение и регистрацию информации [18].

3.3. Система охранного телевидения

Системы охранного телевидения – это одно из наиболее бурно развивающихся направлений технических систем охраны [19–22]. Как и в случае системы контроля и управления доступом основной задачей систем охранного телевидения (СОТ) является реализация с использованием технических средств режимных мер охраны. Отличием от СКУД является тот факт, что применение охранного телевидения в основном нацелено на реализацию внутриобъектового режима, как элемента режимных мер, а не пропускного режима. Внутриобъектовый режим предполагает проведение контроля нахождения на территории учреждения или в отдельных его помещениях лиц и организаций, осуществляющих свою деятельность. Такой контроль, особенно в рабочее время, наиболее эффективно можно осуществ-

лять, используя визуальное наблюдение и тем более с использованием охранного телевидения. Внутриобъектовый режим предполагает также контроль или наблюдение за проведением тех или иных работ как в зданиях, так и на территории организации, а также обеспечение общественного порядка и режимов безопасности на ее территории.

Предотвратить преступление можно и в результате наблюдения за прилегающей к объекту территорией. Преступники могут готовиться к совершению преступления, не проникая на территорию или в помещения, а только наблюдая со стороны или изучая объект под видом посетителей без выполнения несанкционированных подготовительных действий. Очень полезна и возможность контролировать происходящее на объекте в процессе совершения преступления. Часто важен и последующий этап – анализ действий после произошедшего и использование данных телевизионных систем наблюдения для следствия и доказательной базы.

Таким образом, СОТ может быть эффективной на всех этапах противодействия несанкционированным действиям на объекте или вблизи него.

Система охранная телевизионная [21] – это телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений (со звуковым сопровождением или без него), служебной информации и извещений о тревоге с охраняемого объекта.

Существует два вида действий, связанных с наблюдением, **теленаблюдение** и **видеонаблюдение**.

Видеонаблюдение – это наблюдение, осуществляемое непосредственно (глазами человека) или с помощью дополнительных оптических средств (между глазами человека и наблюдаемым объектом), например бинокля. При этом оптический сигнал без принципиальных преобразований физической формы от объекта наблюдения попадает на сетчатку глаза.

При теленаблюдении оптический сигнал преобразуется в электрический, электрический сигнал передается по каналам связи и затем преобразуется снова в оптический, воспринимаемый глазом человека. Главная задача системы телевизионного наблюдения – дистанционное формирование видеосигнала и видеоизображения контролируемых зон, пригодное для дальнейшей обработки и анализа.

В результате анализа видеосигнала и видеоизображения контролируемых зон решаются следующие задачи:

1. Контроль и оценка текущей ситуации в местах наблюдения (например, в торговом зале магазина).
2. Контроль и оценка текущей ситуации в местах недоступных или опасных для присутствия человека.
3. Анализ ситуации, которая имела место в прошлом (информация, записанная на носителе).
4. Охрана объекта (обнаружение преступных действий или нападений).
5. Выявление нештатных ситуаций, требующих принятия определенных действий для их разрешения.
6. Обнаружение опасных ситуаций, требующих принятия безотлагательных мер (например, возгорание, отказ систем жизнеобеспечения зданий).
7. Идентификация объектов (например, личности людей, входящих на предприятие, въезжающего транспорта).
8. Оценка степени угрозы при возникновении нештатных или опасных ситуаций для принятия адекватных мер.
9. Обнаружение несанкционированных действий.
10. Осуществление визуальной проверки причины, которая вызвала срабатывание других подсистем интегрированной системы безопасности.
11. Архивирование видеоинформации о состоянии контролируемых зон, в том числе с обеспечением юридической законности использования этих архивных данных.

Системы телевизионного наблюдения должны обеспечивать выполнение следующих функций:

- 1) телевизионный анализ изображений с помощью одной или нескольких телевизионных камер:
 - а) обнаружение изменений в видеоизображении;
 - б) отслеживание движущихся объектов;
 - в) обнаружение оставленных объектов;
 - г) идентификация отдельных объектов (например, личности преступника);
 - д) распознавание образов (например, считывание номерных знаков автомашин);
- 2) синтез телевизионных изображений, полученных от всех камер;
- 3) сопровождение цели;

- 4) приоритетное отображение тревожных событий;
- 5) сигнализация о несанкционированных действиях.

Структурная схема телевизионной системы наблюдения включает в себя устройства формирования видеосигнала, каналы связи с передатчиками и приемниками видеосигнала (при необходимости), устройства отображения, анализа, регистрации видеосигналов и управления телевизионной системой. Структурная схема такой системы показана на рис. 4.

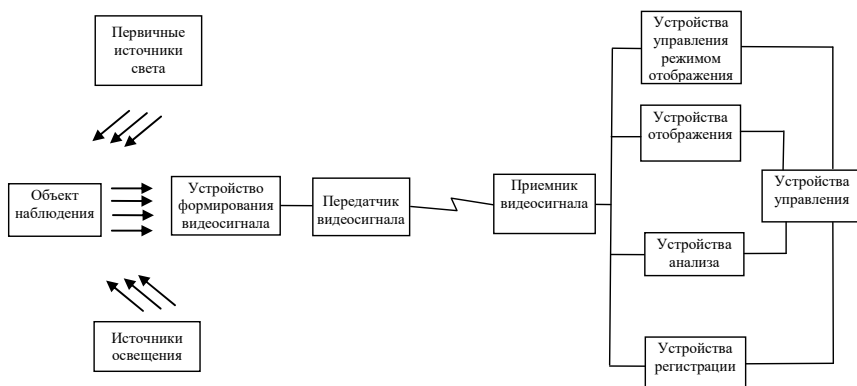


Рис. 4. Структурная схема телевизионной системы наблюдения

К устройствам формирования видеосигнала необходимо отнести устройства, решающие задачу преобразования оптического сигнала (изображения объекта) в электрический сигнал, пригодный для дальнейшей обработки, передачи его по каналам связи и обратного преобразования в видеоизображение. Такими устройствами являются:

- телевизионные камеры, осуществляющие задачу преобразования оптического сигнала в электрический;
- объективы, формирующие требуемый оптический сигнал, соответствующий изображению контролируемой зоны;
- светофильтры, ограничивающие спектральный состав оптического сигнала или его интенсивность.

Устройства отображения обеспечивают преобразование видеосигнала в видеоизображение для непосредственного наблюдения оператором. Самыми распространенными устройствами такого типа являются мониторы.

Устройства управления режимом отображения позволяют повысить эффективность восприятия видеоизображения. К ним относятся:

1) **последовательные коммутаторы**, осуществляющие последовательную смену изображений от различных телекамер на экране монитора;

2) **квадраторы**, формирующие на одном экране четыре изображения одновременно;

3) **видеомультимплексоры**, устройства формирования мультискринного отображения, позволяющие получать одновременно на экране изображение большого количества зон (обычно до 16) на одном экране;

4) **матричные коммутаторы**, устройства обеспечения многопользовательского доступа к видеоизображению (дающие возможность организовать несколько пунктов наблюдения изображения от одних и тех же источников сигнала), а также эффективно записывать видеосигналы от нескольких телекамер на один носитель информации;

5) **видеоменеджеры**, сочетающие в себе функции предыдущих устройств, а также ряд дополнительных, например, видеорегистрации или управления телекамерами.

Устройства регистрации служат для архивирования информации. Они различаются формой представления записываемого сигнала (аналоговой или цифровой) и видом носителя, на который записывается видеоизображение. Носителями, на которые записываются видеоизображения, могут быть:

- магнитная лента;
- магнитные диски;
- оптические носители;
- цифровые запоминающие устройства;
- бумага.

Такими устройствами являются:

1) специализированные видеомагнитофоны (аналоговые устройства регистрации видеосигнала);

2) цифровые видеорегистраторы;

3) видеопринтеры для печати видеоизображения на твердом носителе;

4) устройства формирования дополнительной информации на видеоизображении (например, генераторы титров) и т. п.

Устройства передачи видеосигналов. Состав и свойства системы передачи видеосигналов определяется, прежде всего, типом канала связи и необходимостью использования приемопередатчиков. Наиболее распространенными проводными каналами связи являются:

- 1) коаксиальный кабель;
- 2) оптоволоконные линии связи;
- 3) витые пары;
- 4) проводные телефонные линии;
- 5) линии связи компьютерных сетей.

К беспроводным каналам связи относят:

- 1) специализированные радиоканалы;
- 2) каналы радиотелефонии;
- 3) каналы связи беспроводных компьютерных сетей.

Установочные и защитные элементы обеспечивают установку и эксплуатацию телевизионных камер в различных условиях к таким устройствам относят:

- 1) **кронштейны** для крепления камер на стене, потолке, на специальных стойках;
- 2) **защитные корпуса** для эксплуатации в различных климатических условиях;
- 3) защитные корпуса обеспечивающие **вандалозащищенность**;
- 4) **поворотные устройства** для изменения положения телевизионных камер по углу наклона поворота;
- 5) **обогреватели**;
- 6) **вентиляторы**;
- 7) **стеклоомыватели и стеклоочистители.**

Средства управления позволяют оператору вручную или автоматически управлять положением телекамер, параметрами объективов, режимом отображения. Для этой цели обычно используются следующие аппаратные и программные средства:

- 1) специализированные клавиатуры;
- 2) устройства приема/передачи телеметрической информации;
- 3) экранные имитации клавиатур;
- 4) экранное меню.

Средствами анализа видеосигнала являются программные и аппаратные средства, выявляющие те или иные изменения в видеосигнале или выделяющие из видеосигнала определенные объекты. Это могут быть устройства или алгоритмы:

- 1) регистрирующие потерю ТВ-сигнала;
- 2) распознающие определенные объекты;
- 3) выполняющие видеообнаружение движения и т. д.

Устройства подсветки обеспечивают освещенность объекта наблюдения, необходимую для формирования видеосигнала требуемого качества. К ним относят:

- 1) осветительные приборы видимого спектрального диапазона;
- 2) источники инфракрасной подсветки, невидимой для человеческого глаза;
- 3) фотоэлектронные устройства включения/выключения подсветки.

Вспомогательное оборудование включает в себя различные устройства, обеспечивающие настройку и нормальное функционирование телевизионной системы:

- 1) устройства настройки ТВ-системы;
- 2) светофильтры для имитации низкой освещенности;
- 3) источники бесперебойного питания и т. д.

ЛИТЕРАТУРА

1. Волхонский, В. В Системы физической защиты. Основы теории : учебное пособие / В. В. Волхонский. – СПб. : Университет ИТМО, 2017. – 102 с.

2. Системы охраны и безопасности. Термины и определения : ГОСТ Р 52551-2016. – Введ. 22.11.2016. – М. : Стандартинформ, 2016. – 24 с.

3. О безопасности : Федеральный закон от 5 марта 2024 г. № 5. – М. : Кремль, 2024. – 4 с.

4. Концепция национальной безопасности Республики Беларусь : Решение Всебелорусского народного собрания от 25 апреля 2024 г. № 5 // Национальный правовой Интернет-портал Республики Беларусь. – URL : https://pravo.by/upload/docs/op/P924v0005_1714078800.pdf (дата обращения: 14.09.2024).

5. Гарсия, М. Проектирование и оценка систем физической защиты / М. Гарсия. – М. : ООО «Издательство АСТ», 2002. – 386 с.

6. Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения : учебное пособие / Р. Г. Магауенов. – 2-е изд., перераб. и доп. – М. : Горячая линия Телеком, 2008. – 496 с.

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

8. Об изменении Закона Республики Беларусь «О пожарной безопасности»: Закон Республики Беларусь от 11 нояб. 2019 г. № 251-З // Национальный правовой Интернет-портал Республики Беларусь. – URL : https://pravo.by/upload/docs/op/H11900251_1574456400.pdf (дата обращения: 14.09.2024).

9. Охрана объектов и физических лиц. Термины и определения : СТБ 1250-2000. – Введ. 01.04.2001. – Минск : Белорусский государственный институт стандартизации и сертификации, 2001. – 9 с.

10. Об охранной деятельности в Республике Беларусь : Закон Республики Беларусь от 8 нояб. 2006 г. № 175-З // pravo.by. URL : <https://www.google.com/url?client=internal-element-cse&cx=7a55abdc32296f8b4&q=https://pravo.by/document/%3Fguid%3D3961%26p0%3DH10600175&sa=U&ved=2ahUKEwitidLT6s2OAxVpBdsENaphCF0QFnoECAEQAQ&usg=AOvVawlj35tLf5iTIUURZf0RPHq0&fexp=72986053,72986052> (дата обращения: 14.09.2024).

11. Технический кодекс установившейся практики. Охрана объектов. Обеспечение технической укреплённости объектов : ТКП 652-2020 (33030). – Введ. 01.01.2021. – Минск : Министерство внутренних дел Республики Беларусь, 2020. – 51 с.

12. Технический кодекс установившейся практики. Охрана объектов. Требования по применению технических средств и систем охраны : ТКП 627-2018 (33030). – Введ. 01.01.2019. – Минск : Министерство внутренних дел Республики Беларусь, 2018. – 14 с.

13. Концепция борьбы с терроризмом в Республике Беларусь : Постановление Совета Министров Республики Беларусь от 25 июля 2013 г. № 658; в ред. от 27 июля 2015 г. № 631 // Национальный правовой Интернет-портал Республики Беларусь. – URL : <https://pravo.by/document/?guid=3871&p0=C21300658> (дата обращения: 14.09.2024).

14. Системы централизованного наблюдения. Общие положения : ГОСТ Р 56102.1-2014. – Введ. 01.01.2016. – М. : Стандартинформ, 2015. – 7 с.

15. Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры : ГОСТ 26342-84. – Введ. 01.01.1986. – М. : Издательство стандартов, 1984. – 18 с.

16. Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний : ГОСТ Р 52436-2005. – Введ. 01.09.2016. – М. : Стандартинформ, 2015. – 18 с.

17. Бондарев, П. В. Физическая защита ядерных объектов : учебное пособие для вузов / П. В. Бондарев, А. В. Измайлов, А. И. Толстой; под ред. Н. С. Погожина. – М. : МИФИ, 2008. – 584 с.

18. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний : СТБ ГОСТ Р 51241. – Введ. 11.01.2003. – Минск : Госстандарт, 2003. – 32 с.

19. Волхонский, В. В. Телевизионные системы наблюдения : учебное пособие / В. В. Волхонский. – 2-е изд., доп. и перераб. – СПб. : Экополипс и культура, 2005. – 167 с.

20. Проектирование систем охранного телевидения : учебное пособие / К. Л. Тявловский, Р. И. Воробей, О. К. Гусев [и др.]. – Минск : БНТУ, 2021. – 383 с.

21. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний : ГОСТ Р 51558-2014. – Введ. 01.01.2016. – М. : Стандартиформ, 2014. – 39 с.

22. О республиканской системе мониторинга общественной безопасности : Указ Президента Республики Беларусь от 25 мая 2017 г. № 187 // Национальный правовой Интернет-портал Республики Беларусь. – URL : https://pravo.by/upload/docs/op/P31700187_1496091600.pdf (дата обращения: 14.09.2024).

Учебное издание

ТЕОРИЯ СИСТЕМ БЕЗОПАСНОСТИ

Пособие

для обучающихся по специальности 6-05-0716-05
«Технические системы обеспечения безопасности»

С о с т а в и т е л ь

АНТОШИН Александр Анатольевич

Редактор *А. С. Быховцова*

Компьютерная верстка *Н. А. Школьниковой*

Подписано в печать 12.09.2025. Формат 60×84 $\frac{1}{16}$. Бумага офсетная. Ризография.

Усл. печ. л. 3,43. Уч.-изд. л. 2,68. Тираж 200. Заказ 757.

Издатель и полиграфическое исполнение: Белорусский национальный технический университет.

Свидетельство о государственной регистрации издателя, изготовителя, распространителя
печатных изданий № 1/173 от 12.02.2014. Пр. Независимости, 65. 220013, г. Минск.