

Воронежский институт МВД России

**МОДЕЛИРОВАНИЕ ПЕРИМЕТРАЛЬНЫХ СИСТЕМ
БЕЗОПАСНОСТИ ОБЪЕКТОВ**

Учебно-методическое пособие

**Воронеж
2020**

УДК 624.9
ББК 32.81
М 74

Коллектив авторов: С. А. Винокуров, С. А. Гречаный, И. В. Щербакова,
А. В. Сидоров, Е. С. Герасименко

Рецензенты: Р. О. Лисянский, начальник отдела организации, внедрения и эксплуатации инженерно-технических средств охраны и безопасности ФГКУ «УВО ВНГ России по Воронежской области»;
Ю. В. Харченко, заместитель начальника УВО по г. Воронежу – филиала ФГКУ «УВО ВНГ России по Воронежской области».

Моделирование периметральных систем безопасности объектов :
М74 учебно-методическое пособие / С. А. Винокуров [и др.]. – Воронеж :
Воронежский институт МВД России, 2020. – 104 с.

ISBN 978-5-88591-812-1

Учебно-методическое пособие содержит описание основных моделей, методик и алгоритмов, применяемых при разработке периметральных систем безопасности объектов.

Издание предназначено для курсантов и слушателей радиотехнического и юридического факультетов, слушателей факультета заочного обучения, факультета переподготовки и повышения квалификации и факультета профессиональной подготовки.

Пособие может быть использовано при самостоятельном изучении учебного материала по дисциплине «Организация периметральных систем безопасности объектов», при подготовке рефератов, курсовых работ, а также при написании выпускной квалификационной работы.

М $\frac{0203000000-41}{221-20}$ 17(I)-20

УДК 624.9

ББК 32.81

ISBN 978-5-88591-812-1

© Воронежский институт МВД России, 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	5
1. ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ ПЕРИМЕТРАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ	
1.1. Основы обнаружения нарушителя	6
1.1.1. Модель угроз	8
1.1.2. Модель нарушителя	9
1.2. Особенности организации периметральных систем безопасности	13
1.2.1. Назначение и общие требования к периметральным системам безопасности	13
1.2.2. Состав периметральных систем безопасности объектов	15
1.3. Классификация периметральных систем безопасности	17
1.4. Этапы моделирования периметральной системы охраны объектов с большой протяженностью периметра	18
1.4.1. Системный подход к проектированию систем охраны объектов с большой протяженностью периметра	18
1.4.2. Основные этапы построения периметральных систем охраны объектов	21
1.5. Типовые требования к ограждению периметров объектов	23
1.5.1. Ограждение периметра территории	23
1.5.2. Виды ограждений	23
1.5.3. Ворота и калитки	30
Вопросы для самоконтроля	33
2. МОДЕЛИРОВАНИЕ ПЕРИМЕТРАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ	
2.1. Оценка эффективности периметральных систем безопасности объектов	34
2.1.1. Сущность и методика применения обобщенной оценки эффективности периметральных систем безопасности объектов	34
2.1.2. Математические модели обобщенной оценки эффективности периметральных систем безопасности объектов	37
2.1.3. Параметры обобщенной оценки эффективности периметральных систем безопасности объектов	42
2.2. Система видеонаблюдения периметра объекта	43
2.3. Требования к системе охранного освещения на периметре объекта	51
2.3.1. Общие требования к охранному освещению	51
2.3.2. Расчет системы охранного освещения периметра	54
2.3.3. Подбор источников света по спектральным характеристикам	55
2.3.4. Расчет контраста объекта и фона	56
2.3.5. Применение инфракрасного освещения в охранных видеосистемах	57
Вопросы для самоконтроля	58

3. МОДЕЛИРОВАНИЕ КОМПЛЕКСА ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ ПЕРИМЕТРА ОБЪЕКТА	
3.1. Требования к размещению технических средств безопасности на периметре охраняемого объекта	59
3.2. Трибоэлектрические средства обнаружения.....	61
3.3. Однопозиционные радиоволновые средства обнаружения	76
3.4. Особенности применения интегрированных комплексов охраны периметра объекта.....	80
Вопросы для самоконтроля	84
4. ПРИМЕНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ ПЕРИМЕТРОВ ДЛЯ ОХРАНЫ ОБЪЕКТОВ РАЗНОГО УРОВНЯ СЛОЖНОСТИ.....	85
4.1. Оборудование техническими средствами охраны периметра промышленного предприятия	86
4.2. Оборудование техническими средствами охраны периметра нефтеперерабатывающего завода.....	90
4.3. Оборудование техническими средствами охраны открытых протяженных объектов государственной границы.....	92
4.4. Оборудование техническими средствами охраны периметра административного здания	94
4.5. Оборудование техническими средствами охраны периметра объектов культурного наследия	97
Вопросы для самоконтроля	98
ЗАКЛЮЧЕНИЕ.....	99
СПИСОК ЛИТЕРАТУРЫ	100

ВВЕДЕНИЕ

Показатели криминальной статистики и уровень террористической угрозы в последние годы имеют устойчивую тенденцию к росту. Это, в свою очередь, отражается и на требованиях, предъявляемых заказчиками к вновь создаваемым и модернизируемым системам физической защиты объектов. Поскольку система защиты периметра, как правило, располагается на внешних рубежах охраны объекта, ужесточение требований в первую очередь касается именно её. Именно здесь сосредоточены почти все критически важные компоненты комплекса инженерно-технических средств физической защиты.

Под системой защиты периметра (СЗП) понимают совокупность сложнейших технических устройств, находящихся в постоянном взаимодействии как между собой, так и с компонентами более высокого уровня системы безопасности объекта.

Эффективное функционирование всей системы физической защиты во многом определяется правильностью формирования СЗП: обоснованным выбором состава оборудования, продуманным его размещением по рубежам охраны, надлежащей организацией информационного взаимодействия. Чтобы спроектировать работоспособную и надёжную систему защиты периметра, специалист должен свободно ориентироваться в огромном количестве охранного оборудования, знать характеристики, принципы работы и условия применения каждого технического средства.

Несмотря на огромный опыт, накопленный российскими производителями охранного оборудования и проектировщиками комплексных систем физической защиты, набор печатных изданий по теории и практике создания систем физической защиты (СФЗ) весьма скуден. А список литературы по системам защиты периметра займёт всего лишь несколько строк. Тем не менее потребность в такого рода литературе растёт год от года.

Данное учебно-методическое пособие описывает подходы к моделированию различных составляющих системы безопасности периметра объекта.

Разработка типовых моделей периметральных систем безопасности позволяет организовать на их основе системы защиты периметра практически любого объекта. Кроме того, методы математического моделирования позволяют оценить эффективность предлагаемых вариантов оборудования периметра объекта техническими средствами охраны без проведения дорогостоящих натурных экспериментов.

1. ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ ПЕРИМЕТРАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ

1.1. Основы обнаружения нарушителя

В настоящее время антитеррористическая защита объектов становится одной из приоритетных задач правоохранительных органов.

Угроза объекту – это совокупность условий и факторов, создающих возможность нанесения ущерба охраняемому объекту.

Угроза носит вероятностный характер.

Угрозы можно классифицировать по нескольким основаниям:

- по месту возникновения:
 - внешние – угрозы, источник возникновения которых располагается вне зоны охраны (за ее пределами);
 - внутренние – угрозы, источник возникновения которых располагается на территории охраняемой зоны;
- по характеру:
 - искусственные – угрозы, возникновение которых сопряжено с антропогенным фактором (деятельностью человека);
 - естественные – угрозы, вызванные природными явлениями.

К наиболее вероятным угрозам можно отнести:

- Криминальные угрозы:
 - преднамеренные нападения – различные виды посягательств (покушение на жизнь и здоровье, различные разбои, грабежи, хищения, угоны транспортных средств, порча имущества, хулиганство);
 - другие виды правонарушений.
- Нарушения пропускного режима на объектах защиты.
- Технические неисправности:
 - возгорания: непреднамеренные, вызванные различными неисправностями технических систем, преднамеренные поджоги;
 - выход из строя техники в составе систем электроснабжения и газоснабжения, водопровода и канализации. Причинами могут служить случайные отказы в работе технического оборудования, ошибки обслуживающего персонала, преднамеренные воздействия.
 - Аварии на сетях электроснабжения. В связи с важностью отсутствия перебоев в электроснабжении для нормальной работы всех инженерных систем, включая технику, обеспечивающую безопасность, данная угроза была вынесена в отдельную группу.
 - Действия связанные с природными явлениями. В эту категорию входят: затопления нижних и цокольных этажей зданий, объектов инженерной инфраструктуры, кабельной канализации; различные повреждения от сильных ветров и другое.

В зависимости от возможных последствий и степени опасности

угрозы безопасности охраняемых объектов можно разделить на три вида:

- малоопасные (не причиняющие серьезного урона безопасности объекта);
- опасные (оказывающие значительное влияние);
- особо опасные (приводящие к неэффективности охранных мероприятий и нарушению целостности объекта, вызывающие серьезные последствия).

Вышеуказанные угрозы в обобщенном виде представлены на рисунке 1.1.



Рис. 1.1. Классификация угроз

Следует принять во внимание, что угрозы могут проявляться не только каждая в отдельности, но и в совокупности, таким образом ослабляя или усиливая воздействие.

Пути возникновения угроз:

- возникновение угроз, исключаящее проникновение на территорию, находящуюся под охраной (характерен для внутренних и внешних непреднамеренных угроз);
- возникновение угроз путем проникновения на территорию, находящуюся под охраной (характерен для внешних угроз искусственного происхождения).

Способы реализации угроз определяются категорией воздействия на объект охраны с целью причинения ему вреда. Наиболее характерными являются:

- причинение ущерба с применением поражающих факторов взрыва;
- причинение ущерба под воздействием открытого огня (пожара);
- причинение ущерба с помощью посягательств на материальные ценности и (или) информацию (похищение, повреждение или уничтожение таковых);
- причинение ущерба, путем посягательства на технические системы инженерной инфраструктуры с целью вывода их из строя и т.д.

1.1.1. Модель угроз

Меры по защите охраняемого объекта будут эффективными тогда и только тогда, когда система безопасности объекта сможет адекватно реагировать на все возможные угрозы. Поэтому разработка системы охраны объекта должна начинаться с построения модели угроз.

Модель угроз – это тщательный и подробный анализ всех путей и способов реализации угроз объекту охраны.

Модель угроз разрабатывается с целью:

- определения угроз безопасности охраняемого объекта;
- планирования мер по отражению угроз.

Модель угроз включает в себя:

- полный перечень угроз охраняемому объекту;
- модель нарушителя;
- полный перечень возможных действий (целей и способов их достижения) нарушителя после проникновения его на охраняемую территорию с целью реализации угроз.

Пути реализации угроз:

1. Реализация угроз без проникновения на охраняемую территорию (характерен для внутренних и внешних угроз естественного происхождения).

2. Реализация угроз посредством проникновения на охраняемую территорию (характерен для внешних угроз искусственного происхождения).

Способы реализации угроз

Определяются видами воздействия на охраняемый объект с целью причинения ему ущерба. Наиболее характерные из них:

1. Нанесение ущерба с помощью воздействия поражающих факторов взрыва.
2. Нанесение ущерба с помощью воздействия пожара.
3. Нанесение ущерба с помощью кражи материальных ценностей и (или) информации.
4. Нанесение ущерба с помощью вывода из строя технических систем инженерной инфраструктуры. В самом общем виде модель угроз можно представить следующим образом (рис. 1.2):

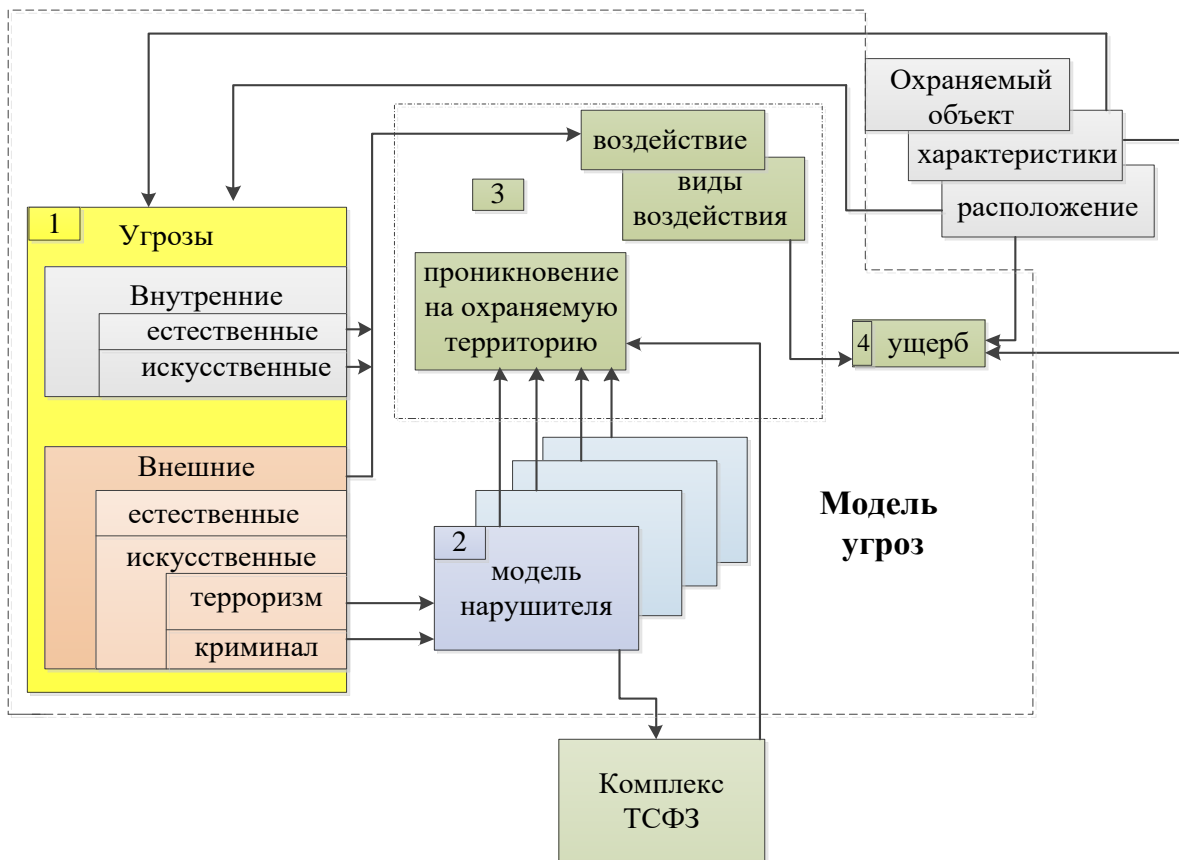


Рис. 1.2. Модель угроз

Таким образом, модель угроз – это детальная проработка всей совокупности путей и способов реализации угроз охраняемому объекту.

1.1.2. Модель нарушителя

Средством реализации внешних искусственных угроз охраняемому объекту является *нарушитель*.

Для определения требуемого уровня защищенности периметра объекта (способности его противостоять действиям нарушителя)

необходимо формирование модели нарушителя, на способности и возможности которого должна ориентироваться создаваемая система охраны периметра.

Модель нарушителей – совокупность сведений о численности, оснащенности, подготовленности, осведомленности и тактике действий нарушителей, их мотивации и преследуемых ими целях, которые используются при выработке требований к системе физической защиты и оценке ее эффективности.

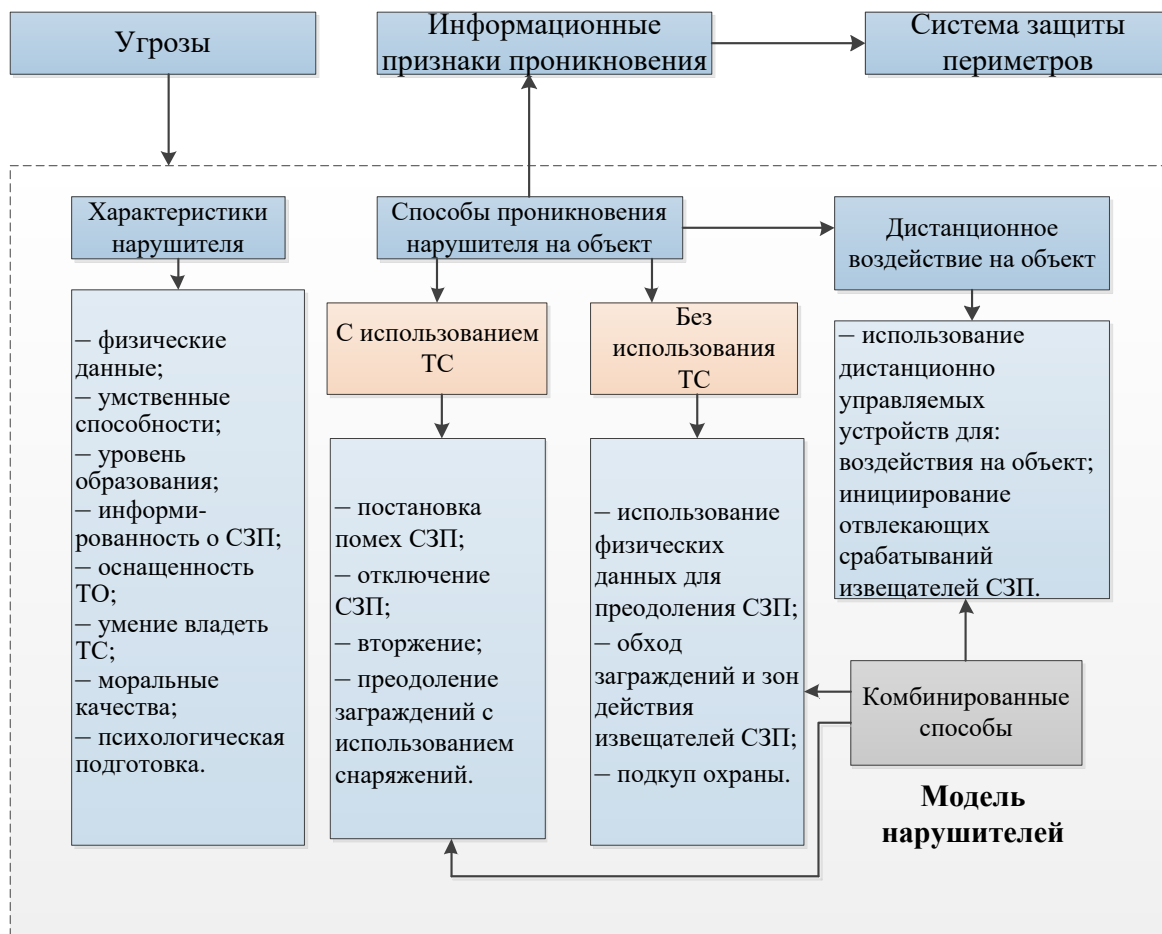


Рис. 1.3. Модель нарушителя

Способы проникновения нарушителя на объект обладают информационными признаками, которые должны использоваться для определения каналов проникновения.

Определение целей вторжения на территорию объекта, модели наиболее вероятного нарушителя и наиболее вероятных сценариев его действий дает возможность сформировать требования к инженерно-техническим средствам системы охраны периметра, при реализации которых возможно ее эффективное противостояние существующим угрозам.

Важное значение при разработке модели нарушителя имеет типология нарушителей по подготовленности к преодолению системы охраны.

Обобщенные типовые модели нарушителя приведены в табл. 1.

Таблица 1

Обобщенные типовые модели нарушителя

Тип	Категория	Подготовленность								
		Психофизическая			Техническая			Осведомленность		
		Высокая	Средняя	Низкая	Высокая	Средняя	Низкая	Высокая	Средняя	Низкая
Внешний	Специалист	+			+			+		
	Любитель		+			+			+	
	Дилетант			+			+			+
Внутренний	Сотрудник		+			+		+		

Тип нарушителя характеризует его отношение к защищаемому объекту и его возможности по преодолению системы охраны.

Категория отражает социальное положение нарушителя. Условно к категории «специалист» можно отнести людей, профессионально занимающихся данным видом деятельности и имеющих специальную подготовку. Они могут действовать в интересах государства или преследовать личные цели. К категории «любитель» относятся наемники или люди, остро нуждающиеся в средствах (например, безработные), обдуманно совершающие противоправные действия.

К категории «дилетант» относятся совершенно не подготовленные злоумышленники: хулиганы, наркоманы, алкоголики, совершающие проникновение без предварительной подготовки. Они преследуют, как правило, цель мелкого вредительства или имеют корыстную направленность. «Сотрудник» – непосредственно работающий на предприятии человек, чаще всего преследует корыстные цели.

Подготовленность нарушителя определяется многими параметрами, основными из которых являются психологическая подготовленность и физическое состояние, техническое обеспечение и осведомленность об объекте и системе охраны. Данные параметры находятся во взаимодействии, усиливая или ослабляя друг друга.

В формализованной модели нарушителя его параметры могут задаваться качественно (вербально), либо количественно (математически).

Общими подходами к математическому описанию параметров формализованной модели нарушителя являются вероятностный и детерминированный. Количественное описание ряда параметров

нарушителя является сложной задачей. Поэтому на практике чаще всего используется комбинированная модель, сочетающая элементы качественного и количественного описания вероятностного и детерминированного подходов.

Осведомленность нарушителя об объекте и системе охраны на нем существенно влияет на уровень его подготовленности. Можно выделить три уровня осведомленности нарушителя:

– высокая – нарушитель знает практически все об объекте и системе охраны, их уязвимых местах;

– средняя – нарушитель знает сравнительно много об объекте, но не знает его уязвимых мест, недостаточно знаний о системе охраны, значимости критических элементов объекта и точных местах их нахождения;

– низкая – нарушитель имеет общее представление о назначении объекта и системе его физической защиты, но практически ничего не знает об уязвимых местах объекта, значимости и местах нахождения его критических элементов.

Рассмотрим обобщенную модель возможных действий нарушителя (угроз объекту) в зависимости от уровня подготовленности, полученную на основе экспертного опроса специалистов вневедомственной охраны:

1. Квалифицированный нарушитель при подготовке проникновения проводит внешний осмотр здания на этапе подготовки кражи. Он визуально изучает внутри здания охраняемые помещения для определения мест расположения охранных извещателей с целью выбора такого способа проникновения внутрь здания или помещения, чтобы совершить обход выявленных им средств охранной сигнализации. Его квалификация позволяет ему применять любой способ проникновения. Однако особое внимание он уделяет возможности заблаговременного выведения из строя технических средств охраны на объекте (в том числе и путем сговора с персоналом объекта) или выбору объектов, на которых охранные извещатели временно находятся в неисправном состоянии. Как правило, он предварительно оценивает время оперативного реагирования групп задержания путем инициирования ложного сигнала тревоги (удары в дверь, окна, отключение электропитания и др.).

Квалифицированного нарушителя интересуют в первую очередь объекты с высокой стоимостью материальных ценностей, количество которых в регионе ограничено. Такие нарушители являются наиболее опасными, так как чаще всего успешно совершают кражи с большим ущербом. Однако в течение года большую серию краж они не реализуют из-за малого числа интересующих их объектов в одном регионе с допустимым для них риском неудачной кражи.

2. Подготовленный нарушитель проводит внешний осмотр с изучением объекта на этапе подготовки проникновения так же, как и

квалифицированный. Степень подготовленности позволяет ему реализовать квалифицированные способы проникновения, связанные с проломом стен, пола, потолка, подбором ключей, проникновением в здание до его сдачи под охрану. Количество замыслов кражи составляет 2–5 на одну попытку проникновения. Только часть таких нарушителей задерживаются, остальные в течение года могут совершить серию из нескольких краж.

3. Неподготовленный нарушитель при подготовке к краже ограничивается внешним осмотром здания, оценивает в основном техническую укрепленность окон и дверей и качество охранного освещения. Количество замыслов кражи редко превышает 1 на одну попытку проникновения на объект. Попытки проникновения совершает в основном путем битья стекол или выбивания дверей простых объектов в надежде совершить кражу «на рывок». В подавляющем большинстве нарушители этого типа задерживаются при совершении первой кражи на охраняемом объекте. При срабатывании автономной сигнализации (звонка «громкого боя») на объекте, расположенном в жилом массиве, такой нарушитель может прекратить дальнейшее проникновение [42].

На практике своевременно оказать сопротивление вооруженной преступной группе, имеющей высокий уровень подготовленности, в большинстве случаев бывает весьма сложно. Для быстрого отражения данной угрозы создается комплекс инженерно-технических средств физической защиты (КИТСФЗ) [10, 11, 12, 15].

Создание последовательных рубежей быстрого обнаружения угроз является основой разработки системы, защищающей территорию объекта охраны.

1.2. Особенности организации периметральных систем безопасности

1.2.1. Назначение и общие требования к периметральным системам безопасности

В настоящее время система защиты периметра – наиболее важный из элементов комплексной безопасности объекта и является обязательной для организации охраны объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации в соответствии с постановлением правительства Российской Федерации от 12 мая 2017 г. № 928-р.

Современные периметральные системы охраны, применяемые на объектах, представлены комплексом средств для оперативного обнаружения злоумышленников, мониторингом обстановки на объекте и его периметре, системами контроля управления доступом и физическими барьерами, которые объединяются общей информационной системой.

Периметр охраняемой территории является наилучшим местом для раннего обнаружения несанкционированного проникновения, потому что в данной ситуации силы охраны имеют наибольший временной запас для противодействия [16, 17, 18].

На периметре охраняемого объекта должны быть организованы специальные зоны для проезда железнодорожных или автомобильных транспортных средств (устройство ворот, преграждающих конструкций, площадок досмотра ТС).

К основным принципам разработки систем охраны периметра можно отнести:

- деление периметра на участки, что позволяет организовать контроль отдельных локальных зон и определение места несанкционированного проникновения на объект;
- интегральное обнаружение, использующее средства обнаружения, системы охранное телевизионные и охранное освещение;
- обеспечение защиты периметральной системы охраны (ПСО) от саботажа.

ПСО решает следующие задачи:

- своевременное обнаружение правонарушителя;
- создание препятствий для несанкционированного проникновения в охраняемую зону;
- быстрое задержание правонарушителя;
- отождествление личности правонарушителя.

Задержка обеспечивается внедрением такой системы, которая рассматривается потенциальными нарушителями как непреодолимое препятствие. Под непреодолимостью понимается невозможность преодоления преграды для нарушителя и наиболее вероятное обнаружение его техническими средствами.

Ограждение периметра территории представляет собой преграду в виде различных преграждающих устройств, защитных сооружений или конструкций, расположенных на поверхности или под землей.

Главной задачей, решаемой в процессе создания ПСО на объекте, является подбор необходимых сил и средств для защиты периметра этого объекта, обеспечивающих необходимый уровень защищенности территории при использовании оптимального количества финансовых ресурсов.

При создании ПСО следует учитывать особенности ее построения. К основным отличиям ПСО можно отнести следующие:

- зависимость конфигурации ПСО от особенностей строения инженерных средств охраны, от их расположения и состояния;
- зависимость конфигурации ПСО от особенностей местности, ландшафта охраняемой территории, климатической зоны ее расположения;
- влияние на ПСО различных электрических и электромагнитных

полей и других помех, таких как:

- а) помехи, вызываемые в процессе колебания земной поверхности вследствие движения тяжёлых крупногабаритных транспортных средств;
- б) помехи, создаваемые двигателями низко пролетающих вертолетов и самолетов;
- в) помехи, вызванные природными явлениями;
- г) помехи, связанные с биологическими единицами (мелкие птицы и животные);
- д) помехи, связанные с растительностью (ветви деревьев, крупные кустарники, высокая трава).

- постоянно изменяющаяся помеховая обстановка;
- необходимость передавать сигналы тревоги и питание для детекторов на большие расстояния (часто более чем 1 км).

При разработке периметральной системы безопасности необходимо одновременно обеспечить защиту от внешних и внутренних угроз. Задачу обнаружения угроз на периметре объекта решают средства обнаружения, предназначенные для блокировки периметра.

Для обеспечения слаженной работы системы безопасности ПСО должна основываться на следующих принципах:

1) принцип непрерывности зоны обнаружения и многозонности. Весь периметр следует разбить на независимые участки и не допускать разрывов между ними. Данное деление создается с целью оперативного реагирования силами наряда и дежурной смены;

2) комбинированное или комплексное обнаружение с использованием нескольких составляющих системы безопасности; средства обнаружения, охранное телевидение, охранное освещение. Данный принцип позволяет повысить надежность и отказоустойчивость системы и улучшить ее вероятностные характеристики;

3) принцип обеспечения защиты периметральных средств обнаружения от несанкционированного вмешательства путем постановки дополнительных извещателей [37, 39, 41].

Надежную защиту периметра объекта невозможно обеспечить только техническими средствами охраны (ТСО). ТСО должны быть интегрированы с инженерными средствами охраны периметра, важнейшим элементом которых являются ограждения.

1.2.2. Состав периметральных систем безопасности объектов

Периметральная система безопасности (ПСБ) объекта – это комплекс организационно-технических мероприятий, реализуемый администрацией объекта, службами безопасности, силовыми структурами с целью исключения угроз персоналу, хищений материальных ценностей и информации, нарушения технологических процессов [22].

Важнейшим элементом ПСБ является комплекс инженерно-технических средств охраны (ИТСО), в состав которого входят:

- технические средства охраны;
- инженерные средства охраны;
- охранное освещение;
- система электропитания.

Состав ПСБ объекта представлен на рисунке 1.4.



Рис. 1.4. Состав системы охраны периметра объекта

При построении модели системы безопасности периметра наиболее трудоемким является выбор технических средств охраны, что обусловлено необходимостью учета целого ряда факторов, влияющих на работу этого элемента системы охраны.

Основным компонентом технических средств охраны периметра является система сбора и обработки информации (ССОИ).

ССОИ – программно-аппаратный комплекс радиоканального или проводного типа, обеспечивающий передачу информационных сообщений с технических средств охраны и их прием на пульт централизованного наблюдения, обработку информации, а также выдачу сигналов управления техническим средствам.

ССОИ, являясь основой системы охраны периметра объекта, представляет собой основной объект атаки со стороны злоумышленников [30].

1.3. Классификация периметральных систем безопасности

При решении задач по обеспечению безопасности крупномасштабного объекта внешний периметр будет являться контуром защищаемой территории, т.е. первым рубежом охраны. Наиболее важной системой комплекса безопасности на первом рубеже объектов с большой протяженностью периметра является система периметральной сигнализации.

Рассмотрим основные технические средства охраны с различными физическими принципами функционирования, которые применяются для защиты периметра охраняемого объекта [38].

Классифицировать периметральные системы охраны можно в зависимости от применяемых в них средств обнаружения.

На рисунке 1.5 представлена классификация средств обнаружения в зависимости от вида регистрируемого воздействия.

Датчики обнаружения (ДО) призваны определять нарушение по демаскирующим признакам нарушителя.

Демаскирующий признак нарушителя (ДПН) – свойство человека-нарушителя, характеризующее его возможность вносить своими действиями изменения в физические параметры окружающей среды и конструкций на рубеже охраны, которые, будучи зафиксированными датчиками обнаружения, позволяют обнаружить пересечение нарушителем этого рубежа.

ДПН классифицируются в зависимости от способов преодоления периметра, а также объекта воздействия нарушителя.

Способы проникновения нарушителей:

- через наземный периметр объекта и вспомогательные помещения;
- путем подкопа;
- путем укрытия в автотранспортном средстве (АТС);
- путем саботажа (вывод из строя элементов ИТСО).



Рис. 1.5. Классификация периметральных систем охраны по виду регистрируемого воздействия

В зависимости от объекта воздействия можно выделить две категории ДПН: связанные с изменением параметров окружающей среды на рубеже охраны при движении в нем нарушителя и вызванные воздействием нарушителя на элементы конструкций на рубеже охраны.

Нарушитель путем оказания определенного воздействия на окружающие предметы в пространстве периметра вызывает некоторые возмущения, которые, в свою очередь, регистрируются специальными датчиками [30].

1.4. Этапы моделирования периметральной системы охраны объектов с большой протяженностью периметра

1.4.1. Системный подход к проектированию систем охраны объектов с большой протяженностью периметра

Системы охраны периметра являются сложными системами, представляющими собой совокупность большого количества

взаимосвязанных и взаимовлияющих элементов. Основной целью на этапе проектирования периметральной системы является обеспечение ее качественного функционирования в дальнейшем на этапе технической эксплуатации. Достижение данной цели возможно при системном подходе к проектированию, что предполагает изучение системы и ее поведения в целом как единого объекта, выполняющего определенные функции в конкретных условиях, с учетом взаимодействия и взаимного влияния отдельных частей, оказывающих наиболее существенное влияние на достижение конечных целей [40].

Системный подход может осуществляться на различных этапах разработки системы охраны периметра, однако наибольший эффект достигается на этапе предварительного моделирования, когда выбирается структурная схема системы и оцениваются ее основные параметры.

Основные принципы системного подхода в области оптимального проектирования могут быть сформулированы следующим образом:

1. Система, состоящая из оптимальных частей, в общем случае не является оптимальной.

2. Оптимизация системы должна проводиться по количественно определенному и единственному критерию, который в математической форме отражает цель оптимизации. Критерий оптимальности, представленный в виде функции оптимизируемых параметров системы, называется целевой функцией. Наличие нескольких критериев оптимальности, которые, как правило, тем или иным способом связаны между собой, не позволяет довести процесс до логического завершения, а отсутствие количественно определенного критерия свидетельствует о недостаточном понимании разработчиком поставленной перед ним задачи.

3. Система должна оптимизироваться в условиях количественно определенных ограничений на оптимизируемые параметры. Последнее обстоятельство свидетельствует о том, что оптимальность системы всегда относительна, условна, так как зависит от условий оптимизации. Поэтому условия оптимизации должны достаточно точно соответствовать реальным условиям.

Так как проектирование оптимальных систем осуществляется математическими методами, то возникает необходимость математического описания системы, т. е. разработки ее математической модели.

Основу математической модели составляют аналитические соотношения (уравнения связи) между внешними и внутренними параметрами системы. Внешние параметры описывают систему с точки зрения потребителя. Такими параметрами, в частности, могут быть помехоустойчивость, надежность, стоимость, габаритные размеры, масса и т. д. Внутренние параметры описывают систему с точки зрения разработчика. Такими параметрами являются: число рубежей обнаружения, тип применяемых датчиков и т. д. Уравнения связи между внешними и

внутренними параметрами системы в аналитической форме могут быть получены в результате:

- теоретических исследований (например, уравнения связи для помехозащищенности, надежности и т. д.);
- технико-экономических расчетов (например, уравнения связи для стоимости, приведенных затрат и т. д.);
- аппроксимации экспериментальных зависимостей или эмпирических данных (например, уравнения связи для вероятности ложных срабатываний);
- имитационного моделирования системы или ее подсистемы на ЭВМ (например, уравнения связи для параметров помехозащищенности в зависимости от типа используемых средств обнаружения).

Одной из наиболее важных задач, возникающих в процессе проектирования, является составление целевой функции, которое осуществляется по указаниям технического задания о критерии оптимизации путем анализа совокупности внешних параметров $x \in x_1, x_2, \dots, x_n$. Оптимизация по составленной целевой функции будет иметь смысл только в том случае, если она будет существенно зависеть от части или всех внешних параметров.

При этом целевая функция может быть представлена в различных формах. При проектировании периметральной системы охраны довольно часто используется целевая функция в виде упорядоченной совокупности целевых функций от одного внешнего параметра, все элементы которой размещены в соответствии с их значимостью, т. е. введен приоритет для некоторых внешних параметров:

$$\Phi(x) \rightarrow \begin{cases} \Phi_1(x) = f_1(y_i), \\ \Phi_2(x) = f_2(y_j), \\ \dots \\ \Phi_m(x) = f_m(y_k). \end{cases} \quad (1.1)$$

Процесс оптимизации при использовании целевой функции данного вида является многоступенчатым. Так, если в техническом задании в качестве критериев оптимизации указаны надежность и стоимость, то на первом этапе проектируются системы, обеспечивающие заданную надежность, а из последних предпочтение отдается проекту, которому соответствуют минимальные экономические затраты.

Сущность процесса проектирования периметральной системы объекта заключается в выборе аппаратуры и способов ее размещения на объекте. При этом разрабатываемая система должна с минимальными затратами и максимальной эффективностью выполнять предписанные ей функции в требуемых условиях.

1.4.2. Основные этапы построения периметральных систем охраны объектов

При создании периметральной системы охраны последовательно выполняется ряд этапов (рис. 1.6):

Этап 1. Предпроектное обследование объекта.

1. Обследование и изучение принципов жизнедеятельности объекта с точки зрения его безопасности (особенности функционирования объекта, его местоположение, рельеф местности, климатические условия, окружающая обстановка, наличие существующей системы безопасности, характеристика системы электроснабжения, помеховая обстановка и т.д.).

2. Аналитическая работа:

- оценка угроз;
- ранжирование по степени важности отдельных зон и направлений;
- выбор принципа построения комплекса;
- выбор схемы взаимодействия технических средств защиты и личного состава охраны.

3. Разработка технико-экономического обоснования (технико-экономических предложений, подробного технического задания на проектирование и т.п.).

Этап 2. Рабочее проектирование.

Разработка полного комплекта рабочей проектно-схемной, проектно-конструкторской и сметной документации.

Этап 3. Оснащение объекта.

1. Приобретение аппаратуры, кабельной продукции, коммутационных изделий, монтажных материалов (при необходимости – изготовление нестандартного оборудования) и т.п. Комплектование и поставка на объект.

2. Инженерное укрепление объекта, строительско-планировочные работы и т.п.

3. Установка и монтаж аппаратуры, оборудования, соединительных кабелей, кроссового оборудования, очагов заземления и т.п.

4. Наладка аппаратуры, комплексная проверка и апробирование.

5. Рабочий прогон смонтированного комплекса и предъявление к сдаче.

6. Выпуск всей исполнительной документации.

7. Сдача-приемка в эксплуатацию.

Этап 4. Подготовка персонала к эксплуатации.

1. Подбор кадров, формирование службы эксплуатации.

2. Обучение обслуживающего персонала правилам эксплуатации систем комплекса.



Рис. 1.6. Этапы построения периметральных систем охраны объектов

3. Разработка практических мер и сценариев действий личного состава службы безопасности и сотрудников объекта при штатных и нештатных ситуациях с использованием современных методов анализа и моделирования ситуаций.

Этап 5. Эксплуатация.

1. Грамотная техническая и оперативная эксплуатация комплекса.
2. Проведение плановых регламентных работ, технического обслуживания в соответствии с требованиями эксплуатационной документации на аппаратуру.
3. Проведение плановой оперативно-тактической учебы и практических занятий с личным составом по разработанным сценариям действий.

1.5. Типовые требования к ограждению периметров объектов

1.5.1. Ограждение периметра территории

Ограждение периметра территории представляет собой препятствие (физический барьер) в виде ограждений, других сооружений или конструкций, расположенных на поверхности или заглубленных в грунт.

В целях обеспечения надежной охраны территорий объектов необходимо, чтобы ограждения обладали следующими характеристиками:

- высокой механической прочностью (устойчивостью к внешним механическим воздействиям, направленным на разрушение);
- устойчивостью к различного рода климатическим воздействиям;
- простотой монтажа;
- высокой ремонтпригодностью и восстанавливаемостью;
- возможностью применения в различных геодезических условиях;
- совместимостью с различными видами ПСО;
- оптимальным сочетанием «цена-качество».

К ограждениям не должны примыкать какие-либо пристройки, кроме зданий, являющихся составной частью периметра.

1.5.2. Виды ограждений

Ограждения подразделяются на основное, дополнительное и предупредительное.

Основное ограждение должно иметь полотно ограждения высотой не менее 2 метров, а в районах с глубиной снежного покрова более 1 метра – не менее 2,5 метра.

По степени защиты основное ограждение подразделяется на:

- ограждение 1-го класса защиты (минимально необходимая степень защиты объекта (территории) от проникновения) – ограждение, из конструкций высотой не менее 2 метров;
- ограждение 2-го класса защиты (средняя степень защиты объекта (территории) от проникновения) – сплошное деревянное ограждение из

доски толщиной не менее 40 миллиметров, металлическое сетчатое либо решетчатое ограждение. Высота ограждения не менее 2 метров (рис. 1.7, 1.8);



Рис. 1.7. Основные ограждения с просматриваемым гибким полотном (гибкая сетка ССЦП)



Рис. 1.8. Колючая проволока и лента

– ограждение 3-го класса защиты (высокая степень защиты объекта (территории) от проникновения) – железобетонное ограждение толщиной не менее 100 миллиметров, каменное или кирпичное ограждение толщиной не менее 250 миллиметров, сплошное металлическое ограждение с толщиной листа не менее 2 миллиметров и усиленное ребрами жесткости, металлическое сетчатое ограждение, изготовленное из стальной проволоки диаметром 5-8 миллиметров, сваренной в перекрестиях и образующей ячейки размером не более 50x300 миллиметров, усиленное ребрами жесткости. Высота ограждения – не менее 2,5 метра с оборудованным дополнительным ограждением (рис. 1.9, 1.10, 1.11);

– ограждение 4-го класса защиты (специальная степень защиты объекта (территории) от проникновения) – монолитное железобетонное ограждение толщиной не менее 120 миллиметров, каменное или кирпичное ограждение толщиной не менее 380 миллиметров. Высота ограждения не менее 2,5 метра, а в районах с глубиной снежного покрова более 1 метра – не менее 3 метров с оборудованным дополнительным ограждением (рис. 1.12).

Дополнительное ограждение устанавливается сверху и внизу основного ограждения и предназначено для повышения сложности преодоления основного ограждения методом перелеза или подкопа, а также увеличения высоты основного ограждения.



Рис. 1.9. Основное ограждение с просматриваемым жестким полотном на ленточном фундаменте (сварная сетчатая панель)



Рис. 1.10. Основное ограждение с просматриваемым жестким полотном на ленточном фундаменте (просечно-вытяжной лист)



Рис. 1.11. Декоративное металлическое основное ограждение на ленточном фундаменте



Рис. 1.12. Основное ограждение сплошного заполнения
(железобетонное ограждение)

Дополнительное верхнее ограждение представляет собой козырек, препятствующий перелазу, на основе изделий из спиральной или плоской армированной колючей ленты и устанавливается на всех видах основного ограждения, а также на крышах одноэтажных зданий, примыкающих к основному ограждению и являющихся составной частью периметра охраняемого участка (рис 1.13, 1.14).



Рис.1.13. Наклонный козырек из колючей проволоки, скрученной колючей ленты (СКЛ), армированной скрученной колючей ленты (АСКЛ)

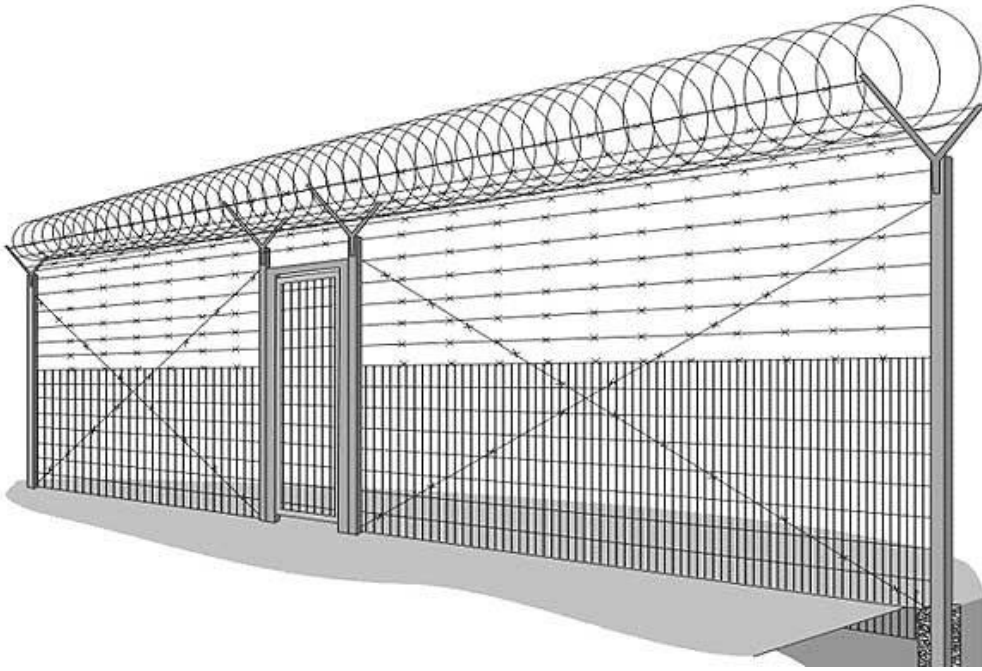


Рис 1.14. Козырек из спирального барьера безопасности

Дополнительное нижнее ограждение устанавливается под основным ограждением с заглублением в грунт не менее чем на 0,5 метра (рис. 1.15 – 1.17).



Рис. 1.15. Нижнее дополнительное ограждение в виде сварной решётки

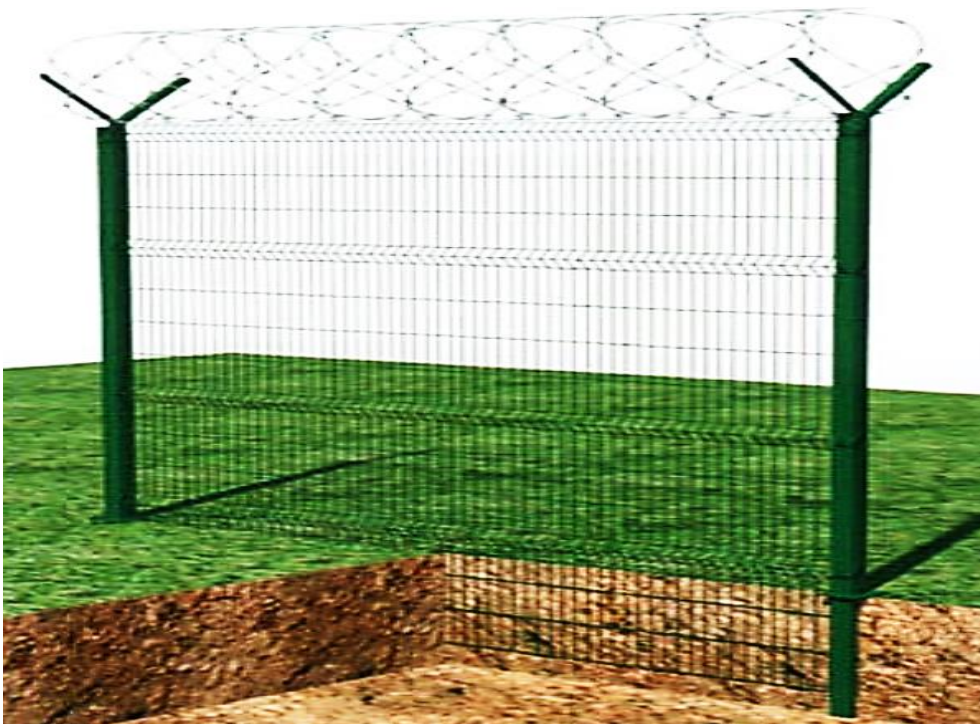


Рис. 1.16. Нижнее дополнительное ограждение в виде сварной сетчатой панели



Рис. 1.17. Нижнее дополнительное ограждение в виде барьера безопасности

Предупредительное ограждение предназначено для обозначения границы рубежа охраны и подразделяется на внешнее и внутреннее.

Высота предупредительного ограждения составляет не менее 1,5 метра, в районах с глубиной снежного покрова более 1 метра – не менее 2 метров.

При необходимости между основным ограждением и внутренним предупредительным ограждением оборудуется запретная зона, представляющая собой специально выделенную полосу местности, предназначенную для выполнения личным составом подразделения охраны служебных задач по защите объекта (территории) (рис. 1.18).

Запретная зона может быть использована для организации охраны объекта (территории) при помощи служебных собак. В этом случае предупредительное ограждение должно иметь высоту не менее 2,5 метра.



Рис. 1.18. Предупредительное ограждение

1.5.3. Ворота и калитки

По степени защиты от проникновения ворота (калитки) подразделяются на:

– ворота (калитки) 1-го класса защиты (минимально необходимая степень защиты), изготовленные из некапитальных конструкций высотой не менее 2 метров (рис. 1.19);



Рис. 1.19. Калитка 1-го класса защиты, выполненная из некапитальных конструкций высотой не менее 2 метров

– ворота (калитки) 2-го класса защиты (средняя степень защиты) представляющие собой:

а) комбинированные, решетчатые или реечные ворота (калитки) из металлоконструкций;

б) деревянные ворота (калитки) со сплошным заполнением полотен при их толщине не менее 40 миллиметров (рис. 1.20);

в) решетчатые металлические ворота (калитки), изготовленные из стальных прутьев диаметром не менее 16 миллиметров, сваренных в перекрестиях и образующих ячейки размером не более 150x150 миллиметров;

– ворота (калитки) 3-го класса защиты (высокая степень защиты) высотой не менее 2,5 метра, представляющие собой:

а) комбинированные или сплошные ворота (калитки) из металлоконструкций;

б) ворота (калитки) деревянные со сплошным заполнением полотен при их толщине не менее 40 миллиметров, обшитые с двух сторон стальным металлическим листом толщиной не менее 0,6 миллиметра;

в) комбинированные или сплошные ворота из стального листа толщиной не менее 2 миллиметров, усиленные дополнительными ребрами жесткости и обивкой изнутри доской толщиной не менее 40 миллиметров (рис 1.21);



Рис 1.20. Деревянные ворота 2-го класса защиты со сплошным заполнением полотен толщиной не менее 40 миллиметров



Рис. 1.21. Ворота 3-го класса защиты, выполненные из сплошного металлического листа высотой не менее 2,5 метра

– ворота (калитки) 4-го класса защиты (специальная степень защиты), представляющие собой сплошные ворота (калитки) из стального листа толщиной не менее 4 миллиметров, усиленные дополнительными ребрами жесткости, и высотой не менее 2,5 метра (рис 1.22).



Рис. 1.22. Ворота 4-го класса защиты

Конструкция ворот (калиток) должна обеспечивать их жесткую фиксацию в закрытом положении. Расстояние между дорожным покрытием и нижним краем ворот должно быть не более 0,1 метра.

Вопросы для самоконтроля

1. По каким признакам можно классифицировать угрозы безопасности объекта?
2. Способы реализации угроз безопасности объекта.
3. Что можно отнести к основным принципам разработки систем охраны периметра?
4. Что такое периметральная система безопасности объекта?
5. Из чего состоит система безопасности периметра объекта?
6. Как классифицируются периметральные системы безопасности по виду регистрируемого воздействия?
7. Какие принципы системного подхода в области оптимального проектирования вы знаете?
8. Перечислите основные этапы построения периметральной системы безопасности объектов.
9. Какими характеристиками должно обладать ограждение для надежной защиты периметра?
10. На какие классы по степени защиты делятся основные ограждения?

2. МОДЕЛИРОВАНИЕ ПЕРИМЕТРАЛЬНЫХ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ

2.1. Оценка эффективности периметральных систем безопасности объектов

2.1.1. Сущность и методика применения обобщенной оценки эффективности периметральных систем безопасности объектов

Одним из важных компонентов в охране объектов являются средства обнаружения. От их технических характеристик и правильной расстановки зависит эффективность системы по обеспечению охраны объектов в целом. Она характеризуется такими параметрами, как количество ложных сработок, время обнаружения и способность инженерных средств охраны задержать нарушителя на время, которое обеспечит прибытие группы задержания.

Система охраны должна обеспечивать обнаружение и задержание нарушителя. Требования к системе аналогичны требованиям к одному из ее компонентов – инженерным средствам охраны (рис. 2.1).

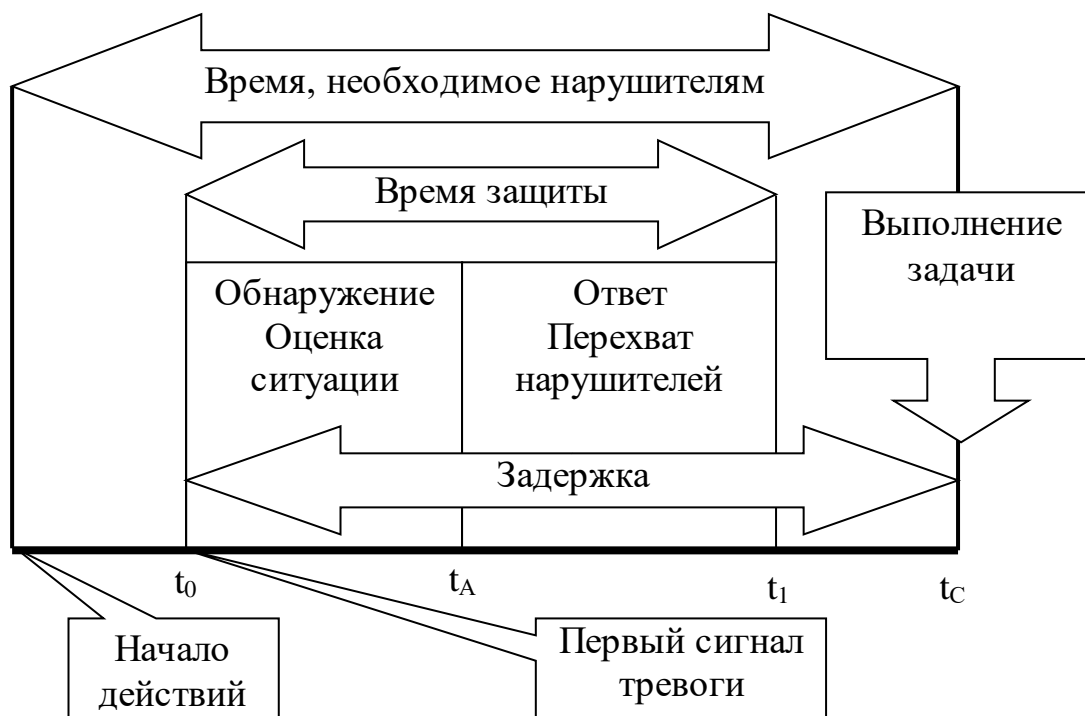


Рис. 2.1. Временная диаграмма функционирования системы охраны периметра

При неспособности обеспечить данные требования разработанная система безопасности станет неэффективной и совершенно бесполезной.

Продолжительность попытки проникновения нарушителем на охраняемый объект зависит от эффективности инженерных средств охраны, основная задача которых – задержать нарушителя до приезда группы задержания.

Момент времени, в который силы охраны нейтрализуют нарушителей – t_1 , а момент выполнения нарушителями их задачи – t_c . Только в случае, когда время защиты ($t_1 - t_0$) меньше времени выполнения задачи нарушителями ($t_c - t_0$), система охраны периметра выполняет свою функцию.

Для объектов с большой протяженностью периметра необходимо учитывать основные характеристики периметровых средств сигнализации, к числу которых можно отнести:

1. Уязвимость системы.
2. Частоту ложных срабатываний.
3. Вероятность обнаружения.
4. Надежность, долговечность, простоту монтажа и эксплуатации.

Параметр, определяющий возможность проникновения на охраняемый объект беспрепятственно, в том числе и с помощью специальных средств и методов блокирования системы охраны, называется уязвимостью системы. Термин «беспрепятственно» в этом контексте означает без сработки сигнала «тревога».

От частоты ложных срабатываний во многом зависит общая эффективность всего комплекса безопасности. На этот параметр значительно влияют индустриальные и климатические факторы. Для борьбы с данной проблемой рекомендуется использовать средства обнаружения с разными принципами действия. Требования к частоте ложных срабатываний: не больше одной сработки за 10 дней на участке длиной 250 м.

Вероятность обнаружения – это вероятность выдачи сигнала «тревога» при прохождении нарушителя в зоне действия датчика.

Рассмотрим факторы, влияющие на эффективность системы охраны периметра (рис. 2.2).

Согласно опросам сотрудников правоохранительных органов, большинство угроз охраняемым объектам реализуется по вине «человеческого фактора». Даже если объект будет оборудован самыми современными инженерными и техническими средствами охраны и они идеально выполняют свои функции предназначения, но при этом персонал объекта охраны не будет реагировать на соответствующие сигналы и сообщения, то, безусловно, угроза безопасности будет реализована. Это первый фактор, который необходимо учитывать при разработке и организации периметральной охраны объекта. Назовем его «*действия персонала*».



Рис. 2.2. Факторы, влияющие на эффективность системы охраны периметра

При длительном сроке эксплуатации или неудовлетворительном состоянии технических средств охраны, используемых на периметре объекта, вероятность невыдачи сигнала «тревога» при преодолении запретной зоны нарушителем безусловно возрастает. И, как следствие, факт нарушения запретной зоны может остаться необнаруженным. Данная проблема в современных периметральных системах решается на техническом уровне. Многие охранные системы производят мониторинг работоспособности шлейфов сигнализации в автоматическом режиме, моделируя сработку.

Состояние инженерно-технических средств в высокой степени влияет на эффективность периметральной системы охраны. Дело в том, что при неудовлетворительном состоянии инженерных средств охраны нарушитель затратит гораздо меньше времени на преодоление запретной зоны, чем предполагалось, а наряд охраны не успеет своевременно прибыть к месту нарушения. При невыполнении данного требования система станет абсолютно бесполезной. Назовем его фактором «*состояния инженерных средств охраны*».

Неправильная эксплуатация не менее влияет на эффективность системы охраны периметра, обычно из-за некачественного или несвоевременного их технического обслуживания. Обозначим его как фактор «*эксплуатации инженерно-технических средств охраны*».

Безусловно, роль освещенности в запретной зоне так же высока, как и состояния технических средств охраны. Фактор «*освещенности*» влияет на вероятность обнаружения нарушителя в запретной зоне в ночное время и качество работы элементов системы видеонаблюдения. Именно из этого вытекает зависимость: чем выше уровень освещенности в запретной зоне исследуемого объекта, тем выше вероятность пресечения попыток нарушения целостности периметра.

В настоящее время не создано абсолютной защиты от воздействия природно-климатических факторов, которые оказывают существенное влияние на состояние инженерных средств охраны. Однако данные факторы учитываются и частично компенсируются конструктивными и схемотехническими решениями при изготовлении технических средств охраны.

А состояние системы электропитания влияет на работоспособность технической аппаратуры. Нестабильное электропитание может приводить к выходу из строя технических средств или формированию ими большого количества ложных срабатываний. Назовем данный фактор фактором «*состояния системы электропитания*».

2.1.2. Математические модели обобщенной оценки эффективности периметральных систем безопасности объектов

Система охраны объекта с большой протяженностью периметра является сложной информационно-технической системой. Оценка эффективности системы охраны периметра по отдельным параметрам, как правило, не позволяет определить оптимальный вариант оборудования охраняемого объекта инженерно-техническими средствами безопасности. Решить задачу выбора элементов системы охраны периметра можно на основе системного подхода к оценке эффективности, основанного на том, что сравнение и анализ осуществляются в целом по совокупности параметров.

Система охраны объекта функционирует главным образом в режиме ожидания. В момент реализации угрозы охраняемому объекту (т.е. в момент воздействия нарушителя на систему) она переходит в режим использования по назначению.

Основная цель режима ожидания – поддержание постоянной работоспособности системы охраны объекта и готовности к внезапному использованию по прямому назначению

Главная цель режима использования по назначению – предотвращение попытки нарушения целостности охраняемого объекта, которая достигается выполнением следующих функций:

- обнаружение нарушителя;
- формирование тревожного извещения о возможной угрозе объекту;

- задержание нарушителя в пределах запретной зоны объекта на время, необходимое для нейтрализации угрозы силами охраны;
- предотвращение проникновения на охраняемый объект силами охраны.

Выполнение первых двух функций обеспечивают технические средства охранной сигнализации объекта, обязательными элементами которой являются средства обнаружения и система сбора и обработки информации, а также средства видеонаблюдения.

Выполнение третьей функции обеспечивают инженерные средства охраны, установленные на периметре охраняемого объекта.

Эффективность системы охраны периметра объекта будет определяться ее способностью выполнять свое целевое предназначение – предотвращать попытки несанкционированного проникновения на охраняемый объект. При этом в качестве показателя эффективности системы охраны периметра можно использовать вероятность предотвращения всех попыток преодоления охраняемого периметра за рассматриваемый промежуток времени [2]:

$$\Phi = P(N > 0, n = 0, t > 0), \quad (2.1)$$

где N – количество попыток преодоления охраняемого периметра за промежуток времени t ; n – количество непредотвращенных нарушений за промежуток времени t ; t – рассматриваемый промежуток времени.

Очевидно, что эффективность системы охраны периметра в целом будет складываться из эффективности функционирования её отдельных участков. При этом на величину показателя эффективности Φ влияет каждый участок системы охраны периметра объекта пропорционально величине его весового коэффициента k_i , который показывает относительное количество попыток проникновения на объект на данном участке:

$$k_i = \frac{N_i}{N}, \quad (2.2)$$

где N_i – количество попыток преодоления периметра на i -м участке; N – общее количество попыток преодоления периметра.

Введем обозначение вероятности предотвращения попыток преодоления охраняемого периметра за рассматриваемый промежуток времени на i -м участке:

$$\Phi_i = P(N_i > 0, n = 0, t > 0). \quad (2.3)$$

Тогда показатель эффективности всей системы охраны периметра будет иметь вид

$$\Phi = \sum_{i=1}^m k_i \Phi_i, \quad (2.4)$$

где m – количество участков периметра.

Нарушитель может преодолеть периметр охраняемого объекта двумя основными способами: наземным (через верх или сквозь полотно ограждений) и подземным (подкопом). Эффективная система охраны периметра объекта должна предотвращать попытки несанкционированного проникновения на объект, совершаемые как наземным, так и подземным способом. Поэтому показатель эффективности системы охраны периметра на i -м участке Φ_i будет определяться вероятностью совершения такого события на этом участке:

$$\Phi_i = \gamma_{ii} P_{ii} + \gamma_{iii} P_{iii}, \quad (2.5)$$

где γ_{ii} ; γ_{iii} – вероятности попыток совершения нарушений на i -м участке системы охраны периметра соответственно на поверхности земли и под землей;

P_{ii} ; P_{iii} – вероятности предотвращения попыток совершения нарушений на i -м участке системы охраны периметра соответственно на поверхности земли и под землей.

Чтобы параметр Φ_i достигал своего максимального значения, требуется выполнение следующих условий:

1. Обеспечение высокой вероятности обнаружения, достоверности выдачи сигнала и передачи информации об обнаружении.
2. Обеспечение необходимого времени задержания нарушителя в пределах запретной зоны объекта.

Для количественной оценки эффективности инженерных средств охраны можно ввести специальный показатель – плотность инженерных средств охраны:

$$\rho_{исо} = \sum_{i=1}^n t_i, \quad (2.6)$$

где t_i – время задержания нарушителя i -м средством охраны.

Таким образом, под плотностью инженерных средств охраны понимается суммарное время задержания нарушителя на периметре объекта всеми имеющимися инженерными средствами охраны.

Плотность инженерных средств охраны – это комплексное понятие, которое определяет насыщенность запретной зоны объекта инженерными средствами.

Однако одного значения плотности инженерных средств охраны недостаточно для оценки надежности и эффективности системы охраны периметра объекта, так как оно не позволяет судить о возможности (или невозможности) предотвращения силами охраны преступных посягательств на объект. Для того чтобы оценить надежность охраны объекта, необходимо сопоставить значения плотности инженерных средств охраны и времени, необходимого силам охраны для нейтрализации угрозы. Очевидно, что время, необходимое нарушителю для преодоления всех инженерных средств охраны, должно быть больше времени, затрачиваемого силами охраны на его нейтрализацию:

$$\rho_{исо} > T_{п}, \quad (2.7)$$

где $T_{п}$ – время, необходимое для предотвращения нарушения.

Плотность инженерных средств охраны (ИСО) можно считать достаточной, если она обеспечивает гарантированное задержание нарушителя в пределах запретной зоны охраняемого объекта.

Важно заметить, что применение формулы (2.7) для оценки эффективности системы охраны периметра имеет смысл только в случае достоверности подачи сигнала «тревога» техническими средствами охраны, установленными на периметре объекта.

Инженерно-технические средства охраны, установленные на периметре объекта, должны обеспечивать достаточно большую вероятность обнаружения, подачи сигнала тревоги и задержания нарушителя. В идеальном случае каждый участок системы охраны должен иметь показатель эффективности $\Phi_i = 1$. Тогда можно говорить о непреодолимости данного участка и всего периметра охраняемого объекта в целом.

Для организации эффективной системы охраны периметра, а именно для ее корректной работы к датчику (или к системе датчиков) предъявляются следующие требования:

- высокая вероятность обнаружения для всех видов нарушителей;
- малое количество ложных тревог при любых вариантах эксплуатации.

В этом и заключается проблема: ни один отдельно взятый датчик не может удовлетворять одновременно этим двум требованиям.

По этой причине используются оптический и акустический, инфракрасный и радиоволновый сигналы. Для получения сведений о действительном вторжении нарушителя на объект (как мы уже знаем, возможны ложные тревоги) используются различные виды комбинирования сигналов от рубежей охраны.

Если сигнал объединяется по схеме «И», вероятность ложной тревоги в системе (P_A) и вероятность пропуска нарушителя системой (P_M):

$$P_A = P_{A1} \wedge P_{A2}, \quad (2.8)$$

$$P_M = P_{M1} \vee P_{M2} \vee \overline{P_{M1} \wedge P_{M2}}, \quad (2.9)$$

где P_{Ai} и P_{Mi} – вероятность ложной тревоги и вероятность пропуска нарушителя i -м средством обнаружения соответственно.

При появлении тревоги по схеме «ИЛИ» вероятность ложной тревоги в системе (P_A) и вероятность пропуска нарушителя системой (P_M):

$$P_A = P_{A1} \vee P_{A2} \vee \overline{P_{A1} \wedge P_{A2}}, \quad (2.10)$$

$$P_M = P_{M1} \wedge P_{M2}. \quad (2.11)$$

И вот к какому выводу мы приходим: при использовании схемы «И» снижается вероятность ложной тревоги, а схема «ИЛИ» обеспечивает снижение вероятности пропуска нарушителей. Вероятности ошибок системы с двумя ортогональными рубежами обнаружения приведены в табл. 2.

Таблица 2

Вероятности ошибок системы с двумя ортогональными рубежами обнаружения

Вероятность	Способ объединения сигналов	
	Схема «И»	Схема «ИЛИ»
Ложная тревога в системе	$P_{A1}P_{A2} \ll P_{A1}; P_{A2}$	$P_{A1}+P_{A2}-P_{A1}P_{A2} \gg P_{A1}; P_{A2}$
Пропуск нарушителя системой	$P_{M1}+P_{M2}-P_{M1}P_{M2} \gg P_{M1}; P_{M2}$	$P_{M1}P_{M2} \ll P_{M1}; P_{M2}$

Более того, необходимо обратить внимание на то, что при использовании двух и более рубежей возможны более сложные комбинации, которые уменьшают и вероятность ложной тревоги, и вероятность пропуска нарушителей.

Таким образом, вследствие изменяющихся по длине рубежа обнаружения и во времени условий функционирования средств вероятность обнаружения является неоднородной в пространстве и во времени. С целью повышения данной вероятности устанавливают несколько рубежей обнаружения. Вероятность обнаружения нарушителя такой комбинированной системой определяют по различным решающим правилам: по схеме «И», «ИЛИ», «2 из 3-х» и т.п.

2.1.3. Параметры обобщенной оценки эффективности периметральных систем безопасности объектов

В ходе различного рода проверок, проверяющие обращают внимание на мероприятия, направленные на предотвращение ложных срабатываний технических средств охраны. Как мы поняли из вышесказанного, и это более чем логично: чем меньше ложных срабатываний, тем меньше выездов групп задержания. С одной стороны, кажется, что ложные срабатывания не влияют на работу вневедомственной охраны и те же самые «сработки» являются своеобразной тренировкой оперативного реагирования групп задержания, но, с другой стороны, надо учитывать, что под охраной данного подразделения стоит большое количество объектов и в таком случае деятельность вневедомственной охраны по обеспечению охраны объектов станет совсем неэффективной. В этом и заключается причина пристального внимания в ходе инспекторских, контрольных или целевых проверок к таким мероприятиям.

Ложные тревоги появляются из-за отказа ретрансляционного оборудования систем передачи извещений и неправильных указаний оператора, связанных с неграмотной оценкой состояния технических средств охраны и недостаточным набором знаний об оборудовании, установленном на охраняемом объекте.

Работа по снижению количества ложных срабатываний ТСО проводится подразделениями вневедомственной охраны на плановой основе в соответствии с требованиями нормативных документов.

Рассмотрим показатели, характеризующие работу по снижению количества ложных срабатываний ТСО.

Месячный коэффициент ложных срабатываний ($K_{\text{лс.мес}}$) – это количество ложных срабатываний в месяц на тысячу номеров задействованной пультовой ёмкости:

$$K_{\text{лс.мес}} = T_{\text{мес.}} / E_{\text{зад.}} \quad (2.12)$$

Под текущим коэффициентом ложных срабатываний ($K_{\text{лс.тек}}$) следует понимать отношение количества ложных срабатываний ТСО ($T_{\text{общ}}$) с начала года к задействованной пультовой емкости системы передачи извещений (СПИ) ($E_{\text{зад}}$) в тысячах единиц, поделенных на номер отчетного месяца N (от 1 до 12):

$$K_{\text{лс.тек}} = (T_{\text{общ}} / E_{\text{зад}}) / N. \quad (2.13)$$

Соответственно, годовой коэффициент ложных срабатываний ($K_{\text{лс.год}}$):

$$K_{\text{лс.год}} = (T_{12\text{мес}} / E_{\text{год}}) / 12, \quad (2.14)$$

где $T_{12\text{мес}}$ – количество ложных срабатываний за 12 месяцев отчётного года; $E_{\text{год}}$ – задействованная емкость СПИ на 1 января года, следующего за отчётным.

Инженерно-техническая служба оценивает работу по устранению срабатываний на основе их текущего коэффициента и годового.

При уменьшении коэффициента текущего года в сравнении с таким же периодом предыдущего года работа технической службы вневедомственной охраны считается удовлетворительной.

При обратной ситуации – работа получает неудовлетворительную оценку.

Любые охранные организации и технические работники стремятся к уменьшению количества ложных срабатываний технических систем охранной и тревожной сигнализации, ведь данный показатель не только характеризует точность определения, но и позволяет экономить время на проверку ложных срабатываний [30].

2.2. Система видеонаблюдения периметра объекта

Согласно ГОСТ 51558–2014 система охранного телевидения должна выполнять следующие функции:

- получение локального отображения (воспроизведения) и локального сохранения аудио- и видеопотоков от одной или нескольких видеокамер;
- связь автоматически регистрируемых событий с действиями видеосервера;
- наличие энергонезависимой памяти для хранения установленных параметров при пропадании напряжения питания;
- размер объектов на изображении должен быть не менее 5% высоты изображения (или не более 80 мм на пиксель изображения).

Для каждого охраняемого объекта с учетом его особенностей процесс разработки системы видеонаблюдения будет строго индивидуальным. С целью формализации процесса проектирования, основанной на принципах унификации, может быть использован обобщенный тактический алгоритм разработки системы видеонаблюдения, представленный на рис. 2.3.

Важным свойством системы видеонаблюдения на периметре охраняемого объекта является не только способность увидеть нарушителя, но и возможность приблизить его изображение без потери качества. При этом необходимо обеспечить контроль участка периметра с определенными размерами в зависимости от поставленных задач.

Многолетний опыт применения видеокамер для охраны периметра объекта позволил выявить следующую зависимость: чем шире поле зрения видеокамеры, тем менее надежно такое видеонаблюдение. Можно

констатировать, что для гарантированного обнаружения нарушителя достаточным является поле зрения в 50 м при условии, что обеспечена необходимая освещенность.



Рис. 2.3. Обобщенный тактический алгоритм разработки системы видеонаблюдения

При организации видеонаблюдения на периметре рассматриваемого объекта можно использовать следующие способы видеонаблюдения:

- 1) видеонаблюдение контролируемой зоны одной телекамерой;
- 2) видеонаблюдение контролируемой зоны двумя видеокамерами.

В настоящее время предпочтительным является первый способ. В этом случае должно соблюдаться следующее требование: камеры устанавливаются «в затылок» друг другу.

Рассмотрим несколько примеров.

Камера с форматом матрицы 1/3" при фокусном расстоянии 12 мм на расстоянии 100 м «видит» другую камеру периметра (при стандартных размерах внешней камеры ~ 200 мм x 80 мм (D)). На рис 2.4. представлено схематическое изображение зоны видеоконтроля для камеры с указанными параметрами.

При выборе места установки видеокamеры по высоте необходимо учитывать углы обзора: угол горизонтального обзора ~ 22°, угол вертикального обзора ~ 16,5°.

Чем ниже устанавливается камера, тем зона наблюдения более эффективна. Естественно, тем проще нарушителю ее украсть или вывести из строя, но при соблюдении принципа «камера видит камеру» ее «охраняет» другая, установленная сзади.

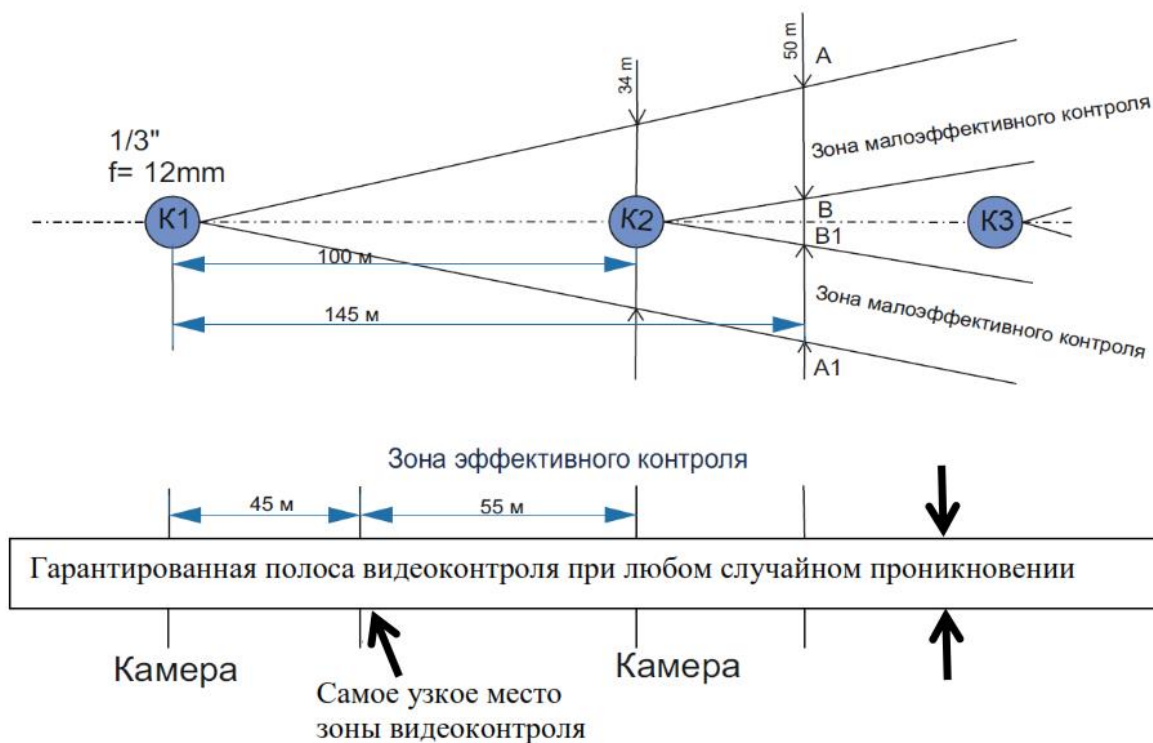


Рис. 2.4. Зона видеоконтроля камеры при $f = 12\text{ мм}$ и расстоянии между камерами в 100 м

Разберем ситуацию только с учетом горизонтальных углов. Если условия объекта потребуют установки камер на высоте так, что необходимо учитывать вертикальные углы обзора, можно проанализировать обстановку аналогичным образом.

Сектор обзора в 22° является весьма узким, и если место установки одной камеры «не закрыто» другой, то поле зрения в непосредственной близости от камеры практически равно нулю – если в этой точке пересекать периметр, «моргнет» экран, и не более того. Детектор движения, если таковой имеется, сработает, но никакого события ни на какой записи не останется.

На расстоянии 100 м (K2 – место установки следующей камеры) поле зрения составляет ~ 34 м. При таком поле можно увидеть следующую камеру K2, любые действия с этой камерой незамеченными не останутся. Сама камера K2 имеет вблизи этой точки поле зрения, близкое к нулю, т. е. практически не работает, зато продолжает «работать» камера K1 вплоть до дистанции потери распознаваемости. Потерю надежной распознаваемости считаем при поле зрения более 50 м. Для $f = 12$ мм поле зрения 50 м (A A1 на рис. 2.4.) находится на расстоянии ~ 145 м от камеры. Можно считать, что в этой точке камера K1 полностью «передает эстафету» камере K2. Ее поле зрения ВВ1 в этой точке (45 м от K2) составляет ~ 15 м. И так далее по всему периметру.

Схематично зона эффективного контроля, построенная исходя из условия максимального поля зрения в 50 м для обнаружения человека, показана на рисунке 2.4. Анализ рисунка показывает, что зона контроля не однородна по ширине вдоль всей протяженности периметра.

При моделировании системы безопасности на периметре объекта необходимо учитывать полный спектр угроз. Если исходить из условия, что потенциальный нарушитель осведомлен о схеме построения системы видеонаблюдения, можно предположить, что нарушитель будет проникать на охраняемый объект в самых узких местах зоны эффективного контроля, которая, как следует из построений, составляет ~ 15 м.

Таким образом, можно гарантировать, что при указанных выше условиях (формат матрицы $1/3''$, фокусное расстояние объектива 12 мм, расстояние между камерами 100 м, камеры смотрят «в затылок» друг другу, задача – обнаружение человека) полоса видеоконтроля при любом случайном проникновении будет иметь ширину не менее 15 м.

Аналогично проводятся рассуждения при определении параметров поворотов периметра. Важно обеспечить за счет сзади стоящей камеры контроль участка от камеры на углу до точки, с которой та начинает «видеть» поле, равное ширине гарантированной полосы контроля.

Особенности установки поворотных камер на периметре показаны на рис. 2.4. Как видно из рисунка, поворот камеры всего на $\sim 11^\circ$ «ломает» полосу гарантированного контроля, и чем больше будет поворот, тем шире «откроются ворота» для не обнаруженного видеосистемой проникновения. Такой поворот легко спровоцировать, например, созданием отвлекающей ситуации.

Детектор движения или дополнительная сигнализация позволяют подать сигнал тревоги с указанием места нарушения (в зоне какой камеры

произошло событие). Поэтому помимо видеокамер периметр охраняемых объектов должен быть в первую очередь защищен труднопреодолимыми препятствиями – инженерными ограждениями и заграждениями. В этом случае при своевременном обнаружении попытки проникновения и объявления тревоги время преодоления периметра охраняемого объекта нарушителем окажется больше времени, необходимого для реагирования сил охраны.

Увеличение дистанции между камерами за счет увеличения фокусного расстояния объективов, а значит, уменьшения угла обзора, приведет к еще большему уменьшению ширины полосы контроля, что снизит практическую эффективность такого контроля. Цифровые значения для любого выбранного варианта можно получить, выполнив аналогичные построения. Если рассчитанной ширины полосы недостаточно, необходимо уменьшать дистанцию между камерами. Простое увеличение угла обзора объектива на более широкий дает обратный эффект при прочих равных условиях.

Проиллюстрируем это на примере, представленном на рисунке 2.5.

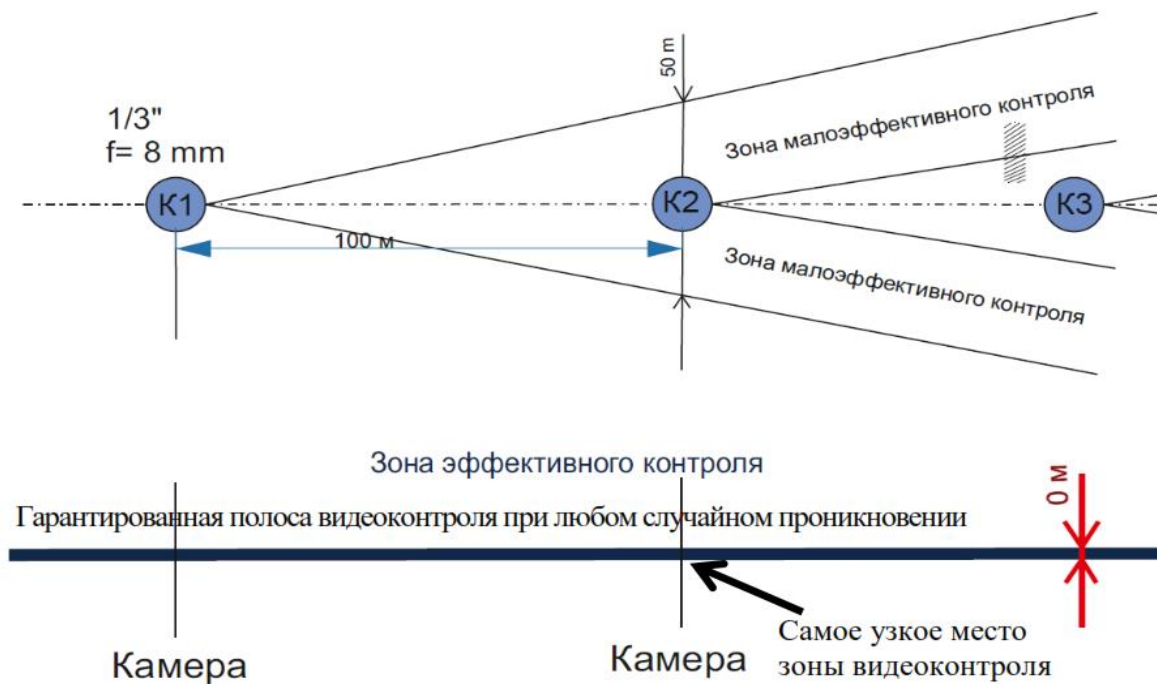


Рис. 2.5. Зона видеоконтроля при $f = 8$ мм и расстоянии между камерами в 100 м

Заменим для нашего случая (100 м между камерами) объектив с $f = 12$ мм на $f = 8$ мм. Угол горизонтального обзора увеличится с $\sim 22^\circ$ до $\sim 33^\circ$. Но поскольку каждая последующая видеокамера от предыдущей установлена на предельной дистанции распознавания объекта, то, как следует из построения, гарантированная полоса видеоконтроля

вырождается в линию, теоретическая толщина которой равна нулю. Если же камеры установлены не вровень с периметром, а имеют какую-либо «мертвую зону» по вертикальному обзору, то система видеонаблюдения на периметре будет иметь множество «мертвых» зон.

На рисунке 2.6. показан пример установки камер с $f = 8$ мм через 50 м. При условии обнаружения объекта на максимальном поле зрения в 50 м, как видно из построения, ширина гарантированной полосы видеоконтроля составляет ~ 34 м, т. е. более чем в 2 раза превышает полосу варианта $f = 12$ мм через 100 м.

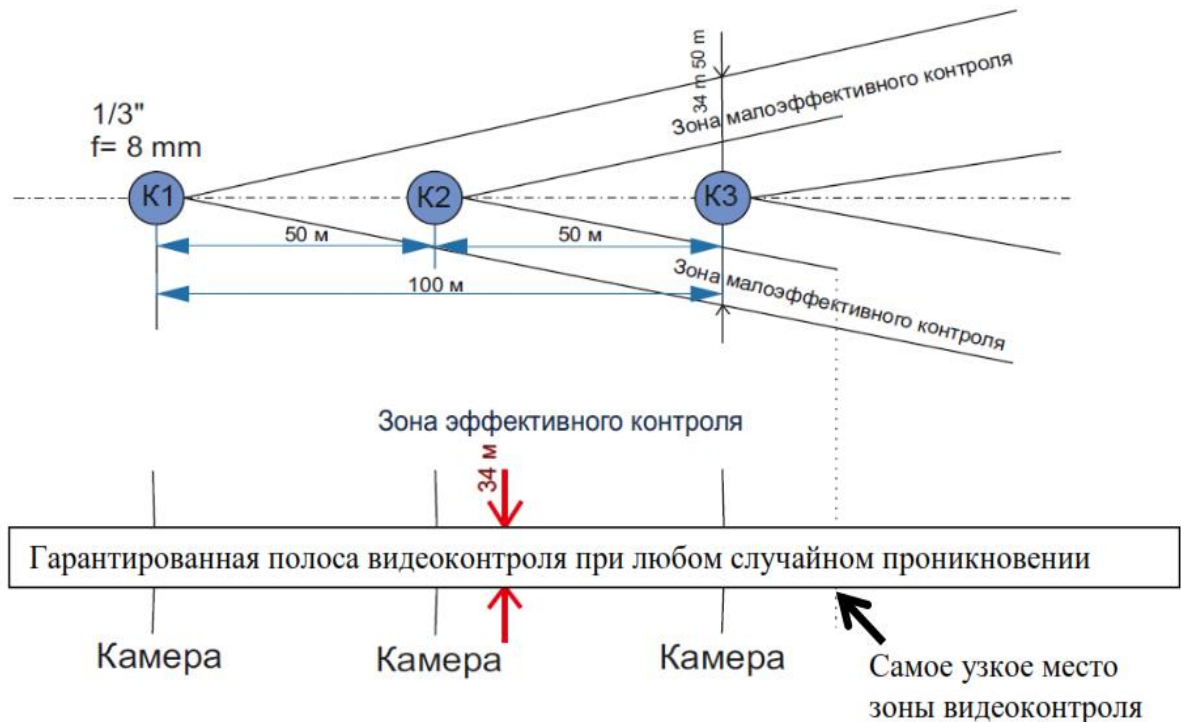


Рис. 2.6. Зона видеоконтроля при $f = 8$ мм и расстоянии между камерами в 50 м

Почти аналогичный результат будет получен для $f = 12$ мм через 50 м (~ 32 м), однако иметь более широкий угол обзора для каждой камеры при прочих равных условиях всегда предпочтительнее. С одной стороны, резко повышается вероятность обнаружения: даже в чистом поле бегом пересечение займет минимум 4-5 секунд. С другой стороны, потребуется в два раза больше камер, что повлечет за собой нагрузку на операторов системы видеонаблюдения и существенное увеличение финансовых затрат.

При невозможности выполнения этого правила возможна установка видеокамер навстречу друг другу с перекрытием зон обзора. При этом сами места их установки должны находиться в зонах обзора других камер.

Для этого применяют видеонаблюдение с двух концов выделенного участка периметра, то есть устанавливают две видеокамеры с противоположных концов наблюдаемого участка периметра (рис. 2.7).

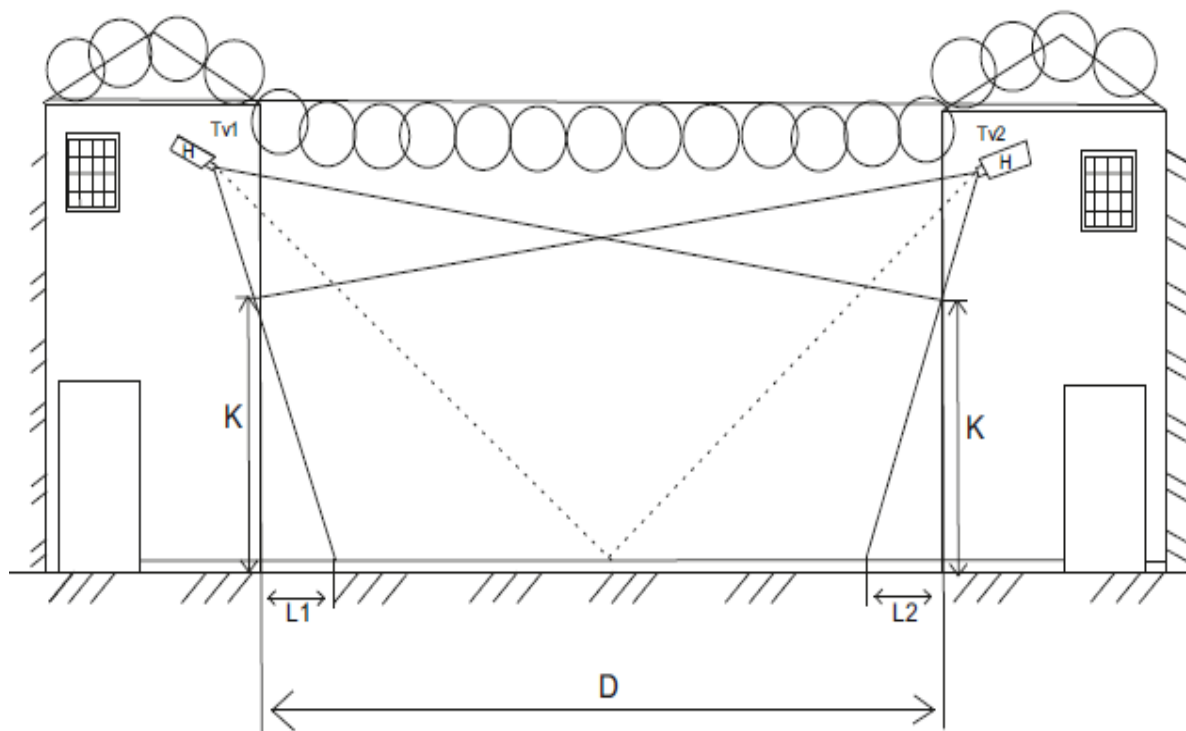


Рис. 2.7. Способ перекрытия «мертвых зон» видеокамер на периметре

В этом случае осуществляется полное «закрытие» всего участка периметра без «мертвых зон» за счет взаимного перекрытия всей контролируемой зоны двумя простыми видеокамерами с фиксированным фокусом и жесткой установкой. Однако данный способ требует увеличения количества применяемых видеокамер в два раза, что ведет к негативным последствиям, о которых говорилось при описании первого способа установки видеокамер.

Не рекомендуется устанавливать в одной точке две камеры, «смотрящие» в разные стороны. Эта точка будет самой уязвимой в системе охраны периметра.

Отдельной задачей является оборудование видеокамерами контрольно-пропускных пунктов охраняемых объектов.

Рассмотрим контрольную площадку для досмотра автотранспорта. Для удобства вычислений в качестве контролируемой зоны выберем квадратную площадку.

Очевидно, что видеонаблюдение надо производить из угла площадки, так как видеонаблюдение, например, из центра боковой стороны квадрата не позволит оператору эффективно контролировать углы площадки под видеокамерой.

При этом если необходимо наблюдать всю площадку, то следует использовать видеокамеру с углом обзора $85^\circ - 90^\circ$ в горизонтальной плоскости.

Однако при видеонаблюдении всей площадки зона контроля будет далеко выходить за ее пределы (заштрихованные участки), что создает трудности для видеонаблюдения заданного пространства, так как в поле зрения видеокамеры будут попадать участки территории за пределами площадки, на которых могут происходить любые события (рис. 2.8).

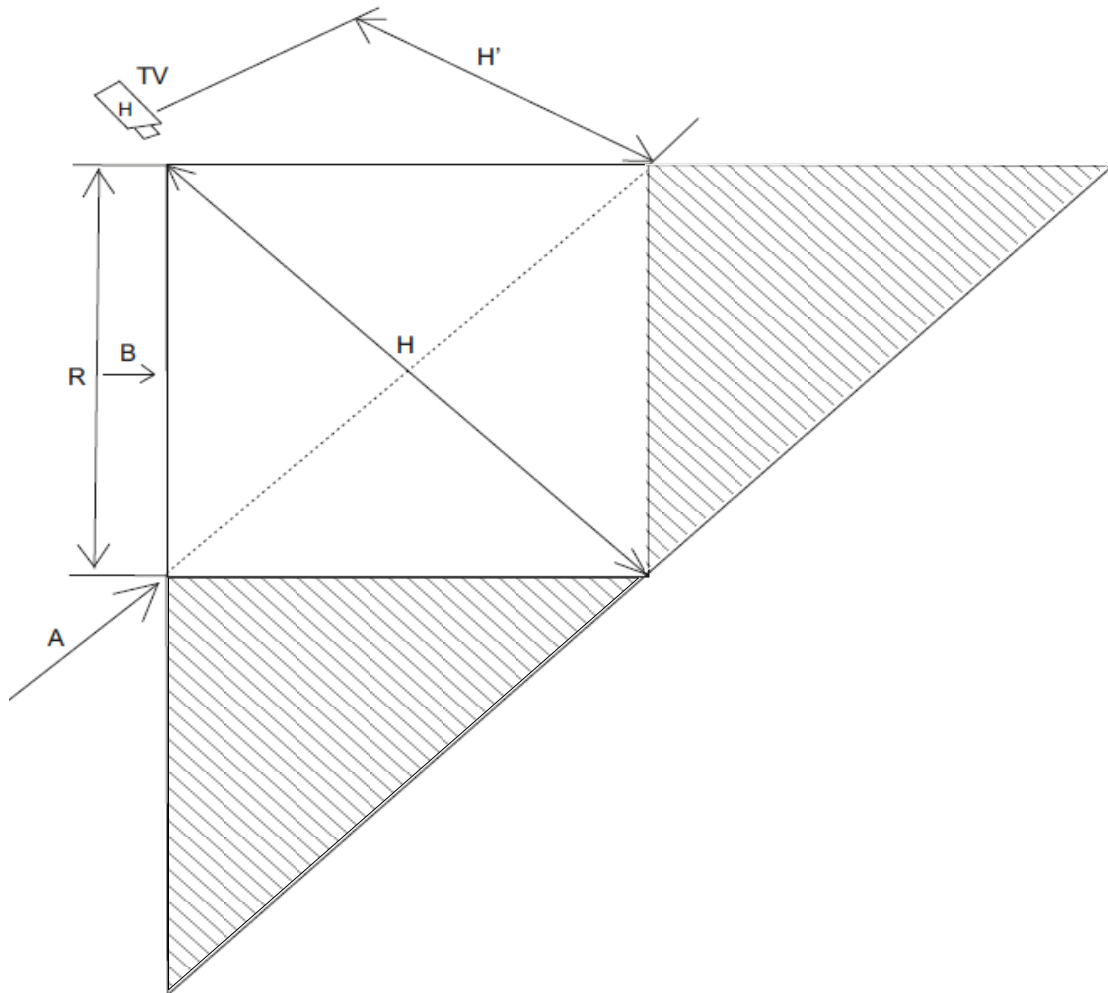


Рис. 2.8. Использование видеокамеры на контрольной площадке (вид сверху)

Для устранения отмеченного выше недостатка необходимо ограничить зону контроля видеокамеры, наклонив ее при установке таким образом, чтобы базой зоны контроля была диагональ H площадки и она не выходила за ее пределы.

Однако в этом случае под наблюдением окажется только половина площадки с дальностью по диагонали H' , поэтому на противоположном углу по диагонали необходимо установить симметрично вторую видеокамеру с теми же характеристиками таким образом, чтобы охватить наблюдением всю площадку (рис. 2.9).

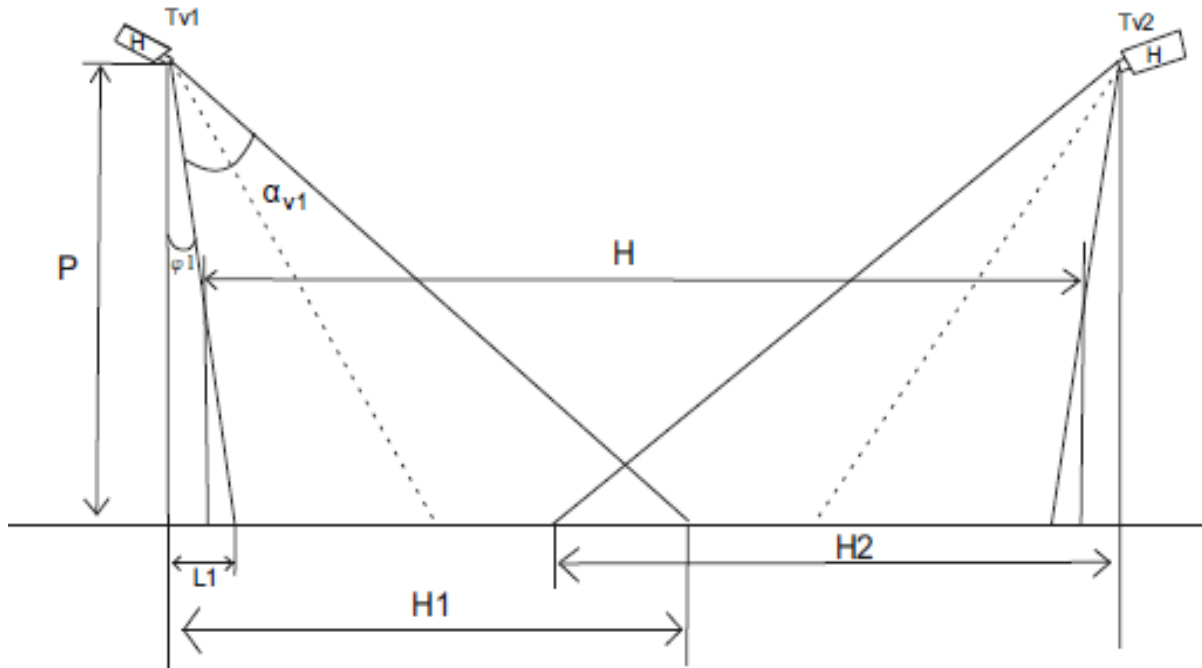


Рис. 2.9. Организация видеонаблюдения контрольной площадки с использованием двух видеокамер (вид с угла А)

Анализ рисунка 2.9 позволяет сделать вывод: для того чтобы образуемая под камерой «мертвая зона» не попадала на контролируемую площадку, необходимо мачту, на которой устанавливается видеокамера, отодвинуть от ограждения, ограничивающего площадку, на размер «мертвой зоны».

Естественно, на периметре реального охраняемого объекта возможны комбинации различных расстояний между камерами и различных фокусных расстояний объективов, которые могут быть смоделированы по аналогии с вышеизложенными примерами [34].

2.3. Требования к системе охранного освещения на периметре объекта

2.3.1. Общие требования к охранному освещению

Система освещения – это комплекс технических средств, состоящий из осветительных приборов (светильники, прожекторы), линий электропередачи и программно-аппаратных средств, обеспечивающий устойчивое и бесперебойное освещение в темное время суток охраняемых зданий, строений, сооружений, иных объектов (помещения, отдельные технические устройства и узлы), а также прилегающих к ним территорий и

акваторий в пределах границ, установленных в соответствии с законодательством Российской Федерации.

В настоящее время системе охранного освещения недостаточно обеспечивать возможность контроля видимости происходящего на территории объекта для человека, осуществляющего охранную деятельность. Такие системы должны удовлетворять более жестким требованиям, поскольку имеется необходимость не просто обеспечить видимость в охраняемой зоне, а сделать ее оптимальной в зависимости от характеристик используемых камер видеонаблюдения, устанавливаемых в совокупности с осветительными приборами.

Система охранного освещения должна обладать улучшенными характеристиками и более расширенным функционалом по сравнению с обычным уличным или декоративным освещением. Охранное освещение проектируется как самостоятельный элемент системы безопасности объекта, и для него определены нормативы, предусмотренные СП 52.13330.2016 «Естественное и искусственное освещение. Актуализированная редакция СНиП 23–05–95».

Обязательным элементом системы охранного освещения является аварийное освещение, включающееся автоматически при получении сигнала тревоги от датчиков системы охраны периметра. Для управления аварийным освещением может использоваться система сбора и обработки информации. В этом случае указывается зона, из которой поступил сигнал тревоги, или две соседние. Осветительные приборы, используемые для осуществления аварийного освещения, должны обеспечивать освещенность от 10 до 50 люксов, поэтому чаще всего применяются прожектора, построенные на основе ПЗС матрицы (прибор с зарядовой связью).

Освещенность зон контрольно-пропускных пунктов в любое время суток составляет не менее 20 люксов – для прохода людей, не менее 75 люксов – для проходных коридоров и будок охраны, не менее 3 люксов – для досмотровой площадки.

В состав системы охранного освещения объекта входят:

- осветительные приборы (светильники);
- кабельные и проводные сети;
- аппаратура управления.

Охранное освещение объекта должно состоять из основного и дополнительного освещения.

Охранное освещение должно обеспечивать гарантированную освещенность не менее 10 люксов во всех контролируемых зонах.

Дополнительное охранное освещение предназначено для улучшения эксплуатационных качеств системы охранной телевизионной и расширения возможности визуального контроля. Оно должно включаться при фиксации нарушения на соответствующем охраняемом участке в

ночное время, а при плохой видимости и в дневное.

Система охранного освещения объекта должна обеспечивать:

- освещенность на уровне земли в горизонтальной плоскости или на уровне 0,5 метра от земли на одной стороне вертикальной плоскости, перпендикулярной к линии границы, не менее 0,5 люкса (в темное время суток);
- равномерно освещенную сплошную полосу шириной не менее 3 метров по периметру объекта;
- возможность автоматического включения дополнительных источников света на отдельных зонах охраняемой территории (периметра) при срабатывании системы охранной сигнализации;
- ручное управление аппаратурой освещения из помещения охраны;
- совместимость с техническими средствами системы охранной сигнализации и системы охранной телевизионной.

Сеть охранного освещения по периметру и на территории объекта должна разделяться на самостоятельные участки в соответствии с зонами системы охранной сигнализации и (или) зонами наблюдения системы охранной телевизионной. Она должна подключаться к отдельной группе распределительного щита, расположенного в помещении охраны, закрытого на замок и оборудованного охранной сигнализацией.

Светильники наружного охранного освещения должны быть защищены от механических повреждений, иметь рабочий диапазон температур, соответствующий климатической зоне, и обеспечивать световую эффективность не менее 100 люмен/ватт.

Конструкции светильников должны иметь класс защиты не ниже IP56.

Для организации системы охранного освещения на периметре объекта применяются различные конструктивные решения, основанные на использовании определенного типа осветительных приборов: консольных светильников, прожекторов, подъемных светильников и т.д. Общим правилом для любого варианта оборудования периметра средствами охранного освещения является то, что системы, монтируемые на ограждениях, не должны превышать уровень ограждения.

Чтобы избежать механических повреждений ламп, необходимо оборудовать их защитной металлической сеткой. Включение системы аварийного освещения осуществляется из помещения охраны.

Подсистема освещения, включающая в себя наружное освещение, освещение самого объекта и внутреннее освещение на объекте, является одним из важнейших элементов системы инженерно-технических средств охраны.

Применение телевидения в составе системы физической защиты объекта ужесточает требования к уровню освещенности контролируемых зон, поскольку задачу классификации малоконтрастных объектов

зрительный анализатор человека решает лучше стандартной ТВ-аппаратуры.

2.3.2. Расчет системы охранного освещения периметра

Рассмотрим особенности размещения источников освещения на периметре объекта в зависимости от взаимного расположения охраняемого рубежа и пункта охраны.

В случае, когда пункт охраны располагается на охраняемой территории, освещение направляют за пределы периметра под небольшим углом к линии горизонта. При таком размещении осветительных приборов сотрудники охраны хорошо видят потенциальных нарушителей, а сами при этом остаются в тени.

При расположении пункта охраны за периметром объекта, чаще всего, освещение направляется внутрь охраняемой зоны, непосредственно на объект. При таком варианте системы охранного освещения в зоне видимости сотрудников будет находиться любой объект, который пытается пересечь освещенное охраняемое пространство.

Для обеспечения эффективной реализации системы освещения необходимо руководствоваться правилом, что такая система должна обеспечивать обнаружение и постоянную видимость нарушителя с расстояния не менее 200 м.

Чтобы рассчитать освещенность от N источников в определенной точке, необходимо знать световую отдачу источников света; расстояние между каждым из них и освещаемым объектом; угол падения света. Светотехнический расчет основывается на законах распространения, отражения и поглощения излучения различных длин волн (лампы при этом рассматриваются как точечные источники света, а освещенные стены – как вторичные распределенные источники). Его проводят для группы характерных точек в несколько итераций с учетом чувствительности телекамер.

Освещенность в данной точке рассчитывают по следующей формуле:

$$E = \sum_i^N \frac{I_i \cos \varphi_i}{4\pi R_j^2}, \quad (2.15)$$

где:

- E – освещенность в данной точке,
- i – номер источника света,
- N – общее количество источников света,
- I – световая отдача источника,
- φ_i – угол падения света от источника (угол между направлением на источник света и перпендикуляром к освещаемой поверхности),
- R – расстояние от источника света до выбранной точки.

Световая отдача источника I (лм) определяется следующим образом:

$$I = \eta P, \quad (2.16)$$

где η (лм/Вт) – коэффициент светоотдачи источника, P (Вт) – мощность лампы.

Коэффициент η зависит от типа и мощности ламп. Некоторые его значения приведены в табл. 3.

Таблица 3

Значение светоотдачи от некоторых типов ламп

Мощность лампы	Коэффициент светоотдачи
Лампы накаливания	
60 Вт	12 лм/Вт
150 Вт	14 лм/Вт
Ртутные лампы высокого давления	
125 Вт	от 38 лм/Вт
1000 Вт	до 50 лм/Вт

Расчет освещенности в поле зрения каждой камеры по формуле (2.15) проводят только для тех источников света, которые находятся между камерой и освещаемым объектом.

2.3.3. Подбор источников света по спектральным характеристикам

Важной характеристикой источников света является спектральная характеристика ПЗС-матрицы, которая, как и характеристика человеческого глаза, имеет максимум на длине волны 0,55 мкм и может распространяться в ИК-область (от 0,7 до 1,1 мкм). Поэтому для освещения объектов применяются газоразрядные лампы (чаще всего ртутные лампы высокого давления типа ДРЛ), имеющие максимум спектральной характеристики на длине волны около 0,5 мкм (то есть близко к максимуму характеристики ПЗС-матрицы), и лампы накаливания (у них максимум приходится на 1,1 мкм). Однако лампы накаливания обладают низким КПД, поэтому в системах охранного освещения чаще применяют газоразрядные лампы, в частности ДРЛ.

При маркировке ламп ДРЛ указывается номинальная мощность и красное отношение. Например, ДРЛ125(15), лампа ДРЛ с мощностью 125 Вт и красным отношением 15%.

Красное отношение $r_{кр}$ – это характеристика источника света, показывающая его близость к естественному свету. Эта величина рассчитывается как отношение красного светового потока к общему световому потоку источника света (в процентах).

$$r_{кр} = \frac{\int S(\lambda)K(\lambda)d\lambda}{\int K(\lambda)S(\lambda)d\lambda} \quad (2.17)$$

где $S(\lambda)$ – спектральная характеристика излучения,

$K(\lambda)$ – спектральная характеристика зрения.

Лучше всего использовать газоразрядные лампы с маленьким значением красного отношения (около 6%), они дают оптимальное согласование спектра излучения с характеристиками зрения. Однако для камер на ПЗС лучше подходят лампы с $r_{кр}=12-15\%$, поскольку они дают большую эффективную облученность объекта.

Стробоскопический эффект, возникающий при кратности кадровой частоты камер и частоты электропитания осветительного прибора, необходимо принимать во внимание при использовании газоразрядных ламп. Стробэффект можно устранить, синхронизировав кадрovou частоту с фазой питающего напряжения.

2.3.4. Расчет контраста объекта и фона

Важной характеристикой системы охраны является вероятность обнаружения нарушителя, которая зависит от его контраста относительно фона (охраняемого объекта). Необходимо спроектировать систему охранного освещения таким образом, чтобы обеспечить максимальную видимость объекта на фоне с учетом чувствительности камер видеонаблюдения.

Как правило, в паспортных характеристиках камеры указывают ее чувствительность для больших значений контрастности (около 85%). В реальных условиях контрастность объекта относительно фона значительно ниже, за счет чего снижается и значение чувствительности камеры на объекте. Это можно компенсировать дополнительным, более ярким освещением.

Расчет контраста K производят по следующей формуле:

$$K = \frac{(K_o - K_\phi)}{(K_o + K_\phi)}, \quad (2.18)$$

где k_o – коэффициент отражения объекта, k_ϕ – коэффициент отражения фона.

Таблица 4

Некоторые значения коэффициента отражения фона
и коэффициента отражения объекта

Контраст объекта относительно фона		Фон	
$K < 0,2$	Малый	$k_{\phi} < 0,2$	Темный
$0,2 < K < 0,5$	Средний	$0,2 < k_{\phi} < 0,4$	Средний
$K > 0,5$	Большой	$k_{\phi} > 0,4$	Светлый
Коэффициенты отражения для некоторых поверхностей			
Зеленая трава	0,14	Суглинистая почва	0,15
Желтая трава	0,22	Бетон	0,1... 0,19
Песок	0,15... 0,35	Светлый трикотаж	0,25... 0,35

Расчет контраста для разных сочетаний объекта и фона показывает, что среднее его значение в реальных условиях приблизительно равно 15%, т.е. примерно в 6 раз ниже того значения, для которого указаны паспортные характеристики камер.

2.3.5. Применение инфракрасного освещения в охранных видеосистемах

ИК-подсветка применяется совместно с черно-белыми камерами и камерами «день/ночь». Различают ИК-излучатели с видимым и невидимым свечением в зависимости от выполняемых задач. В первом случае длины излучаемых волн будут находиться в пределах от 715 до 800 нм, во втором случае – около 830 нм.

В качестве ИК-подсветки используются два типа осветителей: прожекторы с галогенными лампами накаливания и полупроводниковые ИК-осветители. При расчете ИК-подсветки следует принимать во внимание, что ПЗС-матрицами разных типов используется лишь до 15% световой энергии ИК-прожектора.

Таблица 5

Зависимость дальности наблюдения от мощности ИК-подсветки

Мощность ИК-прожектора	Дальность наблюдения
500 Вт	150–200 м
300 Вт	80–120 м
50 Вт	15–30 м
20 Вт	5–15 м

Галогенные лампы (с вольфрамовым излучателем) имеют спектральный максимум на длине волны 1 мкм, чем объясняется их довольно высокая эффективность. Для подавления видимой части спектра излучения можно использовать дисперсионные фильтры на основе ИК-стекол или (реже) интерференционные фильтры.

Полупроводниковые ИК-осветители по сравнению с галогенными лампами обладают большей спектральной яркостью на рабочей длине волны. Основной трудностью при использовании таких излучателей является эффективный отвод тепла от площадки светодиода. Чаще всего при проектировании ИК-подсветки полагаются на указанный в паспорте ИК-осветителя диапазон возможных предельных дальностей при использовании осветителя совместно с типовой телекамерой. Это связано с тем, что проведение теоретического расчета для каждого конкретного случая представляет весьма сложную математическую задачу.

Вопросы для самоконтроля

1. Что такое ложная тревога?
2. Перечислите основные характеристики периметровых средств сигнализации.
3. Какие факторы влияют на эффективность функционирования системы охраны периметра?
4. Причины ложных срабатываний.
5. Каким документом регламентируется применение системы охранного телевидения?
6. Какие функции у системы охранного телевидения?
7. Каким документом регламентируется применение охранного освещения?
8. Применение каких осветительных приборов наиболее целесообразно на периметре охраняемого объекта?
9. Требование к системе охранного освещения на периметре объекта.
10. Решите типовую задачу:

Контролируемая зона шириной $b = 12$ м освещается светильниками типа СПО-200. Расстояние между светильниками $L = 9$ м. Высота установки светильников $H_c = 3,5$ м. Рассчитать освещенность запретной зоны для рассматриваемого объекта и сделать вывод о возможности использования на периметре объекта светильников выбранного типа.

3. МОДЕЛИРОВАНИЕ КОМПЛЕКСА ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ ПЕРИМЕТРА ОБЪЕКТА

3.1. Требования к размещению технических средств безопасности на периметре охраняемого объекта

Для эффективного функционирования охраняемых объектов должна быть обеспечена безопасность периметра, наиболее важной составляющей которой является техническая система безопасности, которая позволяет обеспечить надежную защиту любого объекта, а также обнаружить угрозы практически при любых условиях и сценариях развития событий. Применение надежных технических средств охраны, созданных на базе новейших технологий, позволяет существенно снизить процент террористических посягательств на охраняемые объекты.

Распоряжением Правительства Российской Федерации от 15 мая 2017 г. № 928-р утвержден перечень объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации.

Учитывая, что одной из приоритетных задач Главного управления вневедомственной охраны Росгвардии является защита особо важных объектов, основной упор в деятельности НИЦ «Охрана» делается на решение задач, связанных с организацией охраны именно этой категории объектов.

Основная задача охраны периметра – обнаружить нарушителя (группы) во время преодоления линии периметра, как можно точнее определить место проникновения и локализовать нарушителя до того, как его действия смогут нанести вред охраняемому объекту.

Датчики обнаружения (ДО) многообразны. Они различаются по физическим принципам действия, схемной реализации и способам оперативного применения. Однако общий принцип их действия одинаков. Он состоит в постоянном измерении величины какого-либо физического параметра окружающей среды или элемента конструкции на рубеже охраны и формировании тревожного извещения в случае, когда зарегистрировано изменение этого параметра, соответствующее пересечению нарушителем рубежа охраны (наличию недозволенного предмета).

В зависимости от способа измерения различают пассивные и активные датчики обнаружения.

В активном ДО осуществляется воздействие на окружающую среду (элемент конструкции) при помощи зондирующего сигнала или излучения, вырабатываемого в самом приборе, а информация о наличии или отсутствии нарушителя получается из формы и величины ответного сигнала (излучения).

Обобщенная схема активного датчика обнаружения содержит следующие основные блоки (рис. 3.1):

Источник зондирующего сигнала (излучения) состоит, как правило, из *генератора*, формирующего электрический сигнал с заданными параметрами, а также *излучателя*, преобразующего этот электрический сигнал в излучение определенного вида, частоты и направленности. В случае, когда зондирование производится электрическим сигналом (например, в емкостных ДО), излучатель не используется.

Преобразованное внешней средой излучение (сигнал) поступает на *приемник ДО*, состоящий из *блока формирования (БФ)* и *чувствительного элемента (ЧЭ)*. Вид этого сигнала определяется характеристиками среды распространения сигнала на рубеже охраны, существующими источниками фоновых сигналов и помех, а также наличием или отсутствием нарушителя. Чувствительный элемент преобразует сигнал, содержащийся в принятом излучении, в электрический. В случае, когда зондирование производится электрическим сигналом, чувствительный элемент представляет собой элемент конструкции на рубеже охраны и сигнал с генератора подается непосредственно на него. Для ЧЭ характерно наличие внутренних шумов, добавляющихся к преобразованному сигналу и являющихся помехами.

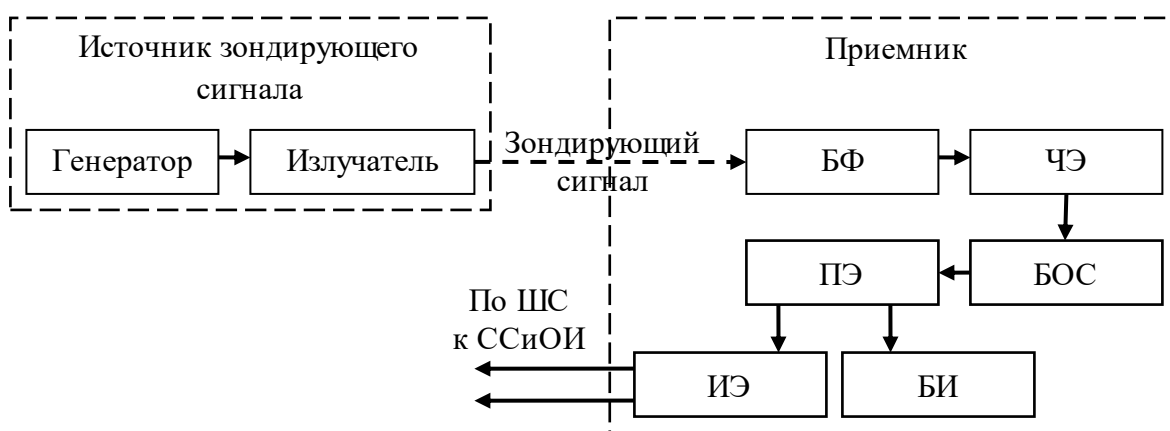


Рис. 3.1. Структурная схема активного датчика обнаружения

Таким образом, на выходе ЧЭ существует электрический сигнал, содержащий информацию о наличии или отсутствии нарушителя на рубеже охраны, в смеси с мешающими сигналами (помехами и фоновыми). Для выделения полезного сигнала из этой смеси предназначен *блок обработки сигналов (БОС)*. В БОС осуществляется аналоговое или цифровое преобразование поступающего сигнала, при котором полезные составляющие сигнала усиливаются, а доля помеховых снижается. Селекция полезных сигналов возможна ввиду отличия их по величине параметров.

Используемые при обработке параметры сигналов определяют виды обработки сигналов: *частотную; временную; частотно-временную; амплитудную; пространственную.*

В общем случае БОС осуществляет несколько видов обработки сигналов. Следует отметить, что пространственная обработка осуществляется излучателем и ЧЭ.

Таким образом, значение сигнала на выходе БОС зависит от факта наличия или отсутствия нарушителя на рубеже охраны. Этот сигнал поступает на *пороговый элемент (ПЭ)*, в котором производится сравнение его величины (напряжения) с пороговым, соответствующим факту наличия нарушителя. При превышении этого порогового значения с ПЭ на блок индикации и исполнительный элемент поступает сигнал заданной длительности и формы.

В свою очередь, *блок индикации (БИ)* формирует световой и (или) звуковой сигнал тревожного оповещения для л/с охраны или службы режима.

Исполнительный элемент (ИЭ) формирует тревожное извещение в виде электрического сигнала для передачи на систему сбора и обработки информации.

Пассивные ДО отличаются от активных отсутствием встроенных источников зондирующих сигналов. Информация о наличии или отсутствии нарушителя на рубеже охраны при этом получается путем преобразования энергии внешних источников излучения средой распространения на рубеже охраны или энергии механических воздействий нарушителя на элементы ограждения или грунт.

Рассмотрим основные типы технических средств и систем безопасности, используемых в настоящее время для охраны периметров объектов [1, 2, 3, 4].

3.2. Трибоэлектрические средства обнаружения

Среди различных типов извещателей по критерию эффективности охраны (надежность обнаружения / погонная стоимость) трибоэлектрические извещатели занимают ведущую позицию. Трибоэлектрические извещатели еще называют вибрационными. Термин «вибрационные» относится к характеру внешнего воздействия, вызывающего извещение о тревоге.

Трибоэлектричество, или трибоэлектрический эффект (от греч. *tribos* – трение), – явление возникновения электрических зарядов при трении. Наблюдается при взаимном трении двух диэлектриков, полупроводников или металлов различного химического состава или одинакового состава, но разной плотности, при трении металлов о диэлектрики, при трении двух одинаковых диэлектриков, при трении жидких диэлектриков друг о

друга или о поверхность твёрдых тел и др. При этом электризуются оба тела; их заряды одинаковы по величине и противоположны по знаку.

Датчики на основе трибоэлектрических кабелей предназначены для регистрации сейсмических колебаний и деформаций различного рода инженерных сооружений.

В отечественных извещателях в качестве чувствительных элементов (ЧЭ) используются специальные кабели со спиралевидным центральным проводником (типа КТВ). Также широко применяются телефонные экранированные кабели (типа ТПП 10×2×0,5), обладающие выраженным «паразитным» трибоэффектом.

Принцип действия датчиков основан на контактных явлениях между поверхностями проводников и диэлектриков, распределенных по всей длине кабеля. При механическом воздействии на трибоэлектрический кабель (деформации) наблюдается эффект перераспределения зарядов между металлическими и диэлектрическими элементами кабеля. Таким образом, трибоэлектрические датчики обнаружения в своей работе используют трибоэлектрический эффект, т. е. возникновение ЭДС между проводниками в специально изготовленном кабеле (чувствительном элементе) при его деформации. Полученный от чувствительного элемента сигнал усиливается, селектируется и обрабатывается, на основании чего принимается решение о выдаче сигналов тревоги.

Рассмотрим особенности работы трибоэлектрических извещателей на примере средств обнаружения «Годограф – Универсал» и «Гюрза-035ПЗ».

1. Прибор «Годограф – Универсал» относится к пассивным средствам обнаружения и функционирует на основе трибоэлектрического эффекта.

«Годограф – Универсал» предназначен для организации рубежей охраны протяженных участков местности, периметров объектов, малоразмерных объектов (крановых узлов, резервуарных парков, трансформаторных подстанций и т. п.), въезда и выезда на объект охраны, подъезда и подхода к объекту охраны.

Конструктивно прибор состоит из:

- блока электронного (БЭ);
- комплекта вибрационных чувствительных элементов (ВЧЭ) и сейсмических чувствительных элементов (СЧЭ).

В зависимости от подключаемых к БЭ чувствительных элементов прибор может использоваться в качестве:

- сейсмического средства обнаружения для выявления нарушителя, движущегося по поверхности земли;
- вибрационного средства обнаружения для выявления нарушителя, преодолевающего ограждение путем перелезания, разрушения или подкопа;

– комбинированного вибросейсмического средства обнаружения.

Также возможно расположение на одном участке рубежа охраны двух ВЧЭ, например, один ВЧЭ для обнаружения подкопа под заграждение, другой – для обнаружения перелезания или разрушения заграждения. Чувствительные элементы обеспечивают обнаружение преодолений рубежа охраны, выполняемых различными способами.

Блок электронный предназначен для обработки сигналов, поступающих с чувствительных элементов, и передачи сигнала срабатывания и сигнала неисправности на систему сбора и обработки информации (ССОИ). БЭ относится к группе исполнения 1.10.2 УХЛ по ГОСТ Р 52860–2007 и предназначен для эксплуатации на открытом воздухе. По степени защиты от воздействия окружающей среды БЭ имеет исполнение IP64 по ГОСТ 14254–96 (МЭК 529–89).

Работоспособность БЭ при температуре окружающей среды от минус 50 до минус 40 °С обеспечивается путем подогрева внутреннего объема БЭ. Для крепления БЭ на сетчатом заграждении, заграждении из железобетонных плит, столбе диаметром от 80 до 160 мм, кирпичной или деревянной стене используется комплект монтажных частей (КМЧ–БЭ).

Внешний вид устройства представлен на рисунке 3.2.



Рис. 3.2. Внешний вид блока электронного «Годограф – Универсал»

Панель управления предназначена для задания конфигурации участков рубежа охраны, настройки параметров алгоритма обнаружения нарушителя, просмотра уровня входных сигналов с чувствительных

элементов и состояния составных частей изделия. Клавиатура панели управления представляет собой гибкую пленочную клавиатуру с тактильным эффектом и имеет 18 кнопок. Внешняя сторона клавиатуры антибликовая, устойчивая к агрессивным средам. Дисплей панели представляет собой алфавитно-цифровой четырехстрочный люминесцентный дисплей с 20 символами в каждой строке.

Элемент вибрационный чувствительный (ВЧЭ) предназначен для преобразование механических колебаний заграждения или козырька в электрические сигналы и передачу сигналов в БЭ. ВЧЭ относится к группе исполнения 1.10.2 УХЛ по ГОСТ Р 52860–2007 и предназначен для эксплуатации на открытом воздухе. По степени защиты от воздействия окружающей среды ВЧЭ имеет исполнение IP67 по ГОСТ 14254–96 (МЭК 529–89).

Устройство «Годограф – Универсал» способно определять различные методы проникновения на охраняемый объект [46].

Таблица 6

Обнаруживающая способность чувствительных элементов

Чувствительный элемент, подключаемый к БЭ	Тип блокируемого заграждения (козырька) или участок местности	Блокируемая длина участка рубежа охраны	Зона обнаружения	Тип обнаруживаемого нарушителя
Элемент вибрационный чувствительный БАЖК. 468239.013 БАЖК. 468239.013–01, БАЖК. 468239.013–02	Заграждение высотой от 2 до 3 м, выполненное из стальной сварной оцинкованной проволоки диаметром от 2,5 до 3,0 мм, например, заграждение из сетки ССЦП 250/50 ТУ 14-4-647-75 (далее по тексту – сетка ССЦП). ВЧЭ располагается на заграждении или в коробе, установленном на заграждении.	От 3 до 250 м	Область пространства, совпадающая с полотном заграждения или козырька, вторжение в которую нарушителя приводит к формированию изделием сигнала срабатывания	Человек массой не менее 50 кг или группа людей, преодолевающие заграждения путем разрушения или перелезания без подручных средств
	Заграждение высотой от 2 до 3 м, выполненное из стальной сварной с полимерным покрытием проволоки диаметром от 3 до 5 мм. ВЧЭ располагается на заграждении или в коробе, установленном на заграждении.			

Продолжение таблицы 6

Чувствительный элемент, подключаемый к БЭ	Тип блокируемого заграждения (козырька) или участок местности	Блокируемая длина участка рубежа охраны	Зона обнаружения	Тип обнаруживаемого нарушителя
	<p>Козырек из объемной или плоской спирали на основе армированной колючей ленты (далее по тексту – спираль АКЛ) диаметром 500, 600, 955 мм, установленный по верху железобетонного заграждения или любой жестко закрепленной конструкции. ВЧЭ располагается на козырьке.</p>			
	<p>Козырек из сетки ССЦП или стальной сварной с полимерным покрытием проволоки диаметром от 3 до 5 мм, установленный по верху железобетонного заграждения или любой жестко закрепленной конструкции. Высота козырька от 0,5 до 1,0 м. ВЧЭ располагается на козырьке.</p>			
	<p>Заграждение высотой от 2,0 до 2,5 м, выполненное из стандартных железобетонных плит толщиной не более 0,15 м (допускаются кирпичные вставки толщиной не более 0,15 м и длиной не более 3 м). ВЧЭ располагается на заграждении.</p>			
	<p>Заграждение высотой от 1,5 до 3,0 м, выполненное на основе объемной спирали АКЛ диаметром до 1000 мм.</p>	<p>От 3 до 250 м При прокладке ВЧЭ в две линии</p>	<p>Область пространства, совпадающая с полотном заграждения</p>	<p>Человек массой не менее 50 кг или группа людей,</p>

Продолжение таблицы 6

Чувствительный элемент, подключаемый к БЭ	Тип блокируемого ограждения (козырька) или участок местности	Блокируемая длина участка рубежа охраны	Зона обнаружения	Тип обнаруживаемого нарушителя
	ВЧЭ располагается на ограждении. Прокладка ВЧЭ выполняется в одну линию, если ограждение состоит из 3 рядов АКЛ и в две линии, если ограждение состоит из 4-6 рядов АКЛ. При прокладке ВЧЭ в две линии максимальное расстояние между линиями – 2 ряда АКЛ.	блокируемая длина участка рубежа охраны уменьшится в 2 раза	или козырька, вторжение в которую нарушителя приводит к формированию изделия сигнала срабатывания	преодолевающие ограждения путем разрушения или перелезания без подручных средств
	Плоское колюче-ленточное ограждение (далее по тексту – ПКЛЗ) высотой от 2 до 2,5 м и ограждение высотой от 1,5 до 2,7 м, выполненное на основе плоской спирали АКЛ диаметром от 500 до 1000 мм, состоящей из 3 рядов АКЛ. ВЧЭ располагается на ограждении.	От 3 до 250 м		
	Ограждение высотой от 2 до 2,5 м, выполненное на основе металлического профилированного листа. ВЧЭ располагается на ограждении.			
	Ограждение, представляющее собой литую или сварную конструкцию, выполненную из прутьев из арматурной стали или труб. Применение изделия на подобном ограждении рекомендуется согласовывать с			

Продолжение таблицы 6

Чувствительный элемент, подключаемый к БЭ	Тип блокируемого заграждения (козырька) или участок местности	Блокируемая длина участка рубежа охраны	Зона обнаружения	Тип обнаруживаемого нарушителя
	предприятием-изготовителем в каждом конкретном случае.			
Элемент вибрационный чувствительный БАЖК. 468239.014	Грунт под заграждением на глубину до 1 м. ВЧЭ располагается в грунте под заграждением на глубине от 0,3 до 0,6 м.	От 3 до 250 м	Область в грунте под заграждением, вторжение внутрь которой нарушителя приводит к формированию изделия сигнала срабатывания	Человек или группа людей, ведущие подкоп под заграждение
Комплект сейсмического чувствительного элемента БАЖК. 433649.006	Поверхность грунта. СЧЭ располагается в грунте на глубине от 0,2 до 0,3 м	Полоса длиной от 20 до 250 метров (зависит от количества звеньев: от 1 до 12) и шириной от 5 до 10 м	Область на поверхности грунта шириной от 5 до 10 метров и длиной равной расстоянию от первого до последнего звена плюс от 10 до 20 м (для человека) и от 75 до 150 м (для транспорта) с каждой стороны, пересечение которой приводит к формированию изделия сигнала срабатывания.	Человек массой не менее 50 кг или группа людей (до 3 человек) пересекающие зону обнаружения
Комплект вибрационного чувствительного элемента БАЖК. 468229.003	Заграждение высотой от 2 до 3 м, выполненное из стальной сварной оцинкованной проволоки диаметром от 2,5 до 3,0 мм, например,	От 10 до 1000 м (зависит от длины и количества звеньев: от 1 до 20)	Область пространства, совпадающая с полотном заграждения или козырька,	Человек массой не менее 50 кг или группа людей, преодолева-

Продолжение таблицы 6

Чувствительный элемент, подключаемый к БЭ	Тип блокируемого ограждения (козырька) или участок местности	Блокируемая длина участка рубежа охраны	Зона обнаружения	Тип обнаруживаемого нарушителя
	<p>ограждение из сетки ССЦП 250/50 ТУ 14-4-647-75 (далее по тексту – сетка ССЦП). ВЧЭ располагается на ограждении или в коробе, установленном на ограждении</p> <p>Ограждение высотой от 2 до 3 м, выполненное из стальной сварной с полимерным покрытием проволоки диаметром от 3 до 5 мм. ВЧЭ располагается на ограждении или в коробе, установленном на ограждении.</p>		вторжение в которую нарушителя приводит к формированию изделия сигнала срабатывания	ющие ограждения путем разрушения или перелезания без подручных средств
	Козырек из объемной или плоской спирали на основе армированной колючей ленты (далее по тексту – спираль АКЛ) диаметром 500, 600, 955 мм, установленный по верху железобетонного ограждения или любой жестко закрепленной конструкции. ВЧЭ располагается на козырьке.			
	Козырек из сетки ССЦП или стальной сварной с полимерным покрытием проволоки диаметром от 3 до 5 мм, установленный по верху железобетонного ограждения или любой жестко закрепленной конструкции. Высота козырька от 0,5 до 1,0 м. ВЧЭ располагается на козырьке.			

Продолжение таблицы 6

Чувствительный элемент, подключаемый к БЭ	Тип блокируемого ограждения (козырька) или участок местности	Блокируемая длина участка рубежа охраны	Зона обнаружения	Тип обнаруживаемого нарушителя
	Заграждение высотой от 2,0 до 2,5 м, выполненное из стандартных железобетонных плит толщиной не более 0,15 м (допускаются кирпичные вставки толщиной не более 0,15 м и длиной не более 3 м). ВЧЭ располагается на заграждении.			
	Заграждение высотой от 1,5 до 3,0 м, выполненное на основе объемной спирали АКЛ диаметром до 1000 мм. ВЧЭ располагается на заграждении. Прокладка ВЧЭ выполняется в одну линию, если заграждение состоит из 3 рядов АКЛ, и в две линии, если заграждение состоит из от 4 до 6 рядов АКЛ. При прокладке ВЧЭ в две линии максимальное расстояние между линиями – 2 ряда АКЛ.			
	Плоское колюче-ленточное заграждение (далее по тексту – ПКЛЗ) высотой от 2 до 2,5 м и заграждение высотой от 1,5 до 2,7 м, выполненное на основе плоской спирали АКЛ диаметром от 500 до 1000 мм, состоящей из 3 рядов АКЛ. ВЧЭ располагается на заграждении.			

Продолжение таблицы 6

Чувствительный элемент, подключаемый к БЭ	Тип блокируемого ограждения (козырька) или участок местности	Блокируемая длина участка рубежа охраны	Зона обнаружения	Тип обнаруживаемого нарушителя
	Заграждение высотой от 2 до 2,5 м, выполненное на основе металлического профилированного листа. ВЧЭ располагается на заграждении.			
	Заграждение, представляющее собой литую или сварную конструкцию, выполненную из прутьев из арматурной стали или труб. Применение изделия на подобном заграждении рекомендуется согласовывать с предприятием-изготовителем в каждом конкретном случае.			

Основные тактико-технические и эксплуатационные характеристики прибора «Годограф – Универсал»:

– длина зоны обнаружения: один или два участка длиной до 250 м каждый для СЧЭ, до 1000 м каждый для ВЧЭ;

– прибор обеспечивает непрерывную круглосуточную работу и сохраняет свои характеристики при температуре окружающей среды от минус 50 до плюс 50 °С и относительной влажности воздуха 98 % при температуре 35 °С;

– напряжение питания от 20 В до 30 В.

2. Трибоэлектрический охранный извещатель «Гюрза-035ПЗ» является пассивным средством обнаружения, в основе работы которого лежит трибоэлектрический эффект.

Извещатель «Гюрза-035ПЗ» предназначен для охраны ограждений периметров на разрушение и перелаз.

Конструктивно прибор состоит из:

– блока обработки сигналов (БОС);
– чувствительного элемента (трибоэлектрического кабеля, прокладываемого по элементам ограждения);

– муфты переходной;

– устройства оконечного;

– соединительного кабеля.

Элементы БОС представлены на рис. 3.3.

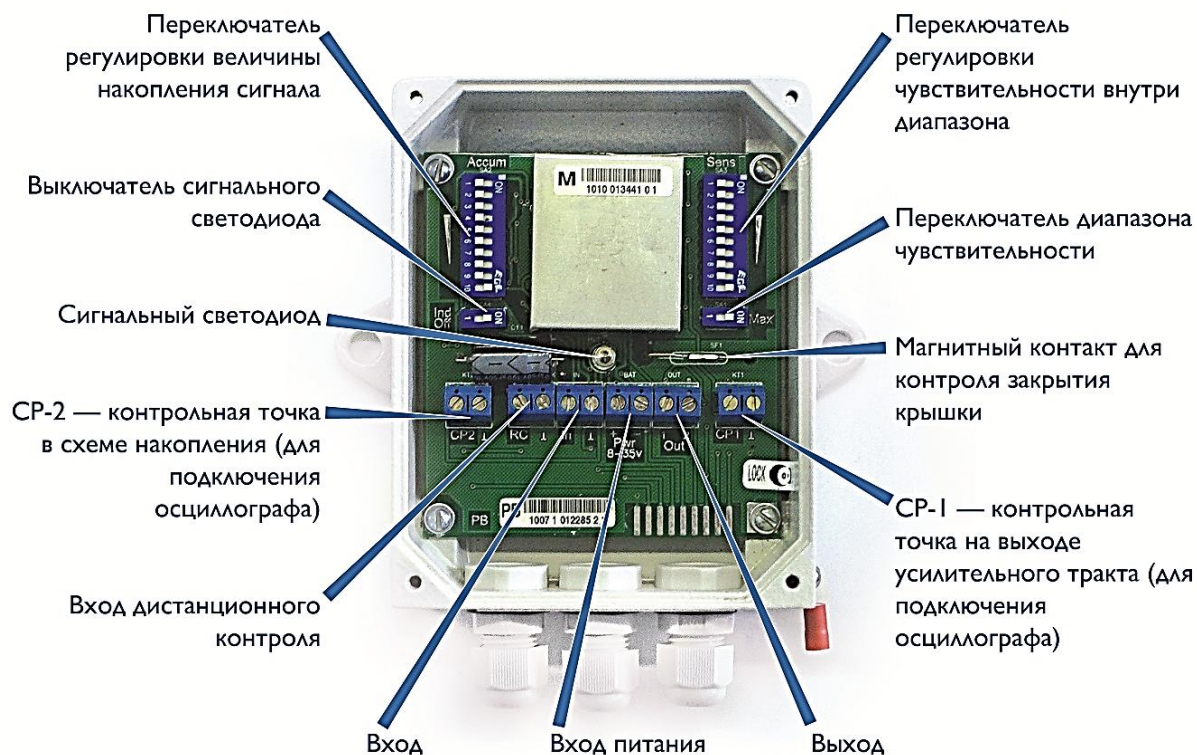


Рис. 3.3. Блок обработки сигналов извещателя «Гюрза-035ПЗ»

Принцип действия извещателя основан на регистрации блоком обработки сигналов извещателя электрических сигналов, возникающих в чувствительном элементе и его узлах напряжения (местах жесткого крепления чувствительного элемента к ограждению), при механическом воздействии на элементы ограждения.

В блоке обработки сигналов происходит фильтрация, обработка и усиление сигналов. В случае превышения порогового значения сигналом, прошедшим обработку, происходит формирование тревожного извещения в виде размыкания контактов выходного оптореле.

«Нарушитель» при преодолении ограждения создает малые деформации отдельных элементов ограждения. При этом происходит деформация трибоэлектрического кабеля и в нем происходит разделение зарядов за счет «трибоэффекта» (электризации трением между жилой и изоляцией). В результате формируется аналоговый сигнал, который поступает на вход БОС.

Муфта переходная предназначена для электрического соединения чувствительного элемента с линией подключения к блоку обработки сигналов (кабель РК 50-2-16), а также для экранирования и герметизации места соединения.

Муфта соединительная предназначена для соединения (при необходимости) двух отдельных отрезков чувствительного элемента друг с другом, а также для экранирования и герметизации места соединения.

Оконечное устройство предназначено для обеспечения постоянного контроля целостности чувствительного элемента и линии подключения его к БОС, а также для экранирования и герметизации конца чувствительного элемента.

Основные тактико-технические и эксплуатационные характеристики прибора «Гюрза-035ПЗ»:

– длина зоны обнаружения зависит от применяемого типа ограждения (табл. 7);

– прибор обеспечивает непрерывную круглосуточную работу и сохраняет свои характеристики при температуре окружающей среды от минус 50 до плюс 50 °С и относительной влажности воздуха 98 % при температуре 35 °С;

– напряжение питания от 8 В до 35 В.

К достоинствам извещателя «Гюрза-035ПЗ» можно отнести возможность организации рубежей обнаружения на периметре охраняемого объекта, оборудованного различными типами инженерных ограждений.

С помощью извещателя реализуется:

– охрана гибких ограждений (АКЛ, «Егоза», ПЗ, ССЦП, «Рабица», «Махаон», колючая проволока);

– охрана жестких ограждений, выполненных из металлических конструкций (сварных и кованых решеток, цельных металлических листов, гофролистов и т.п.), а также ограждений из дерева;

– охрана жестких монолитных ограждений, выполненных из бетона, кирпича, камня и т.п.;

– охрана дополнительных гибких ограждений (козырьков);

– охрана ворот, калиток и т.п.

Таблица 7

Характеристики зоны обнаружения в зависимости от применяемого типа ограждения

Тип ограждения	Способ установки ЧЭ	Максимальная длина зоны охраны
Основное ограждение		
Сетка типа ССЦП (высота Н=2,5 м) Плоская спираль АКЛ (высота Н=2,7 м) Решетка (высота Н=2,5 м)	В три линии	160 м
Ограждение типа «МАХАОН» (высота Н=2 м, без заглубления нижней части полотна в грунт)	В две линии	210 м
Сетка «Рабица» без каркаса (высота Н=1,8 м)	В две линии	210 м
Сетка «Рабица» в рамочной конструкции из уголка (высота Н=2,5 м)	В четыре линии	120 м
Колючая проволока (высота Н=2,5 м)	Синусоидой	130 м
Инженерное ограждение из плоской спирали типа ПЗ (ИЗ-ПЗ 95/12 производства ЗАО «НПП «СКИЗЭЛ»)	В две линии	230 м

Тип ограждения	Способ установки ЧЭ	Максимальная длина зоны охраны
Металлический лист (высотой до 4 м)	В две линии	240 м
Деревянное ограждение (высотой до 3 м)	В две линии	240 м
Дополнительное ограждение (козырек)		
Колючая проволока (высотой $H=80\div 90$ см)	Синусоидой	270 м
Спираль АКЛ (диаметром $40\div 95$ см)	В одну линию	500 м
Сетка типа ССЦП (высотой $H=80\div 90$ см)	В одну линию	500 м
Нажимной козырек	В одну линию	500 м

Чувствительный элемент монтируют непосредственно на гибких элементах ограждения, а при наличии опор, позволяющих нарушительно преодолеть ограждение, не касаясь гибких элементов ограждения, чувствительный элемент монтируют и на опорах. На гибких ограждениях сигнал тревоги формируется вследствие локальной деформации ограждения и закрепленного на нем чувствительного элемента при несанкционированном проникновении методом перелеза и методом нарушения целостности ограждения, чувствительного элемента и элементов, создающих узлы напряжения.

Рассмотрим варианты оборудования извещателем «Гюрза-035ПЗ» периметровых ограждений различного типа.

Схема расположения чувствительного элемента извещателя на ограждении из проволочной сетки ССЦП представлена на рис. 3.4.

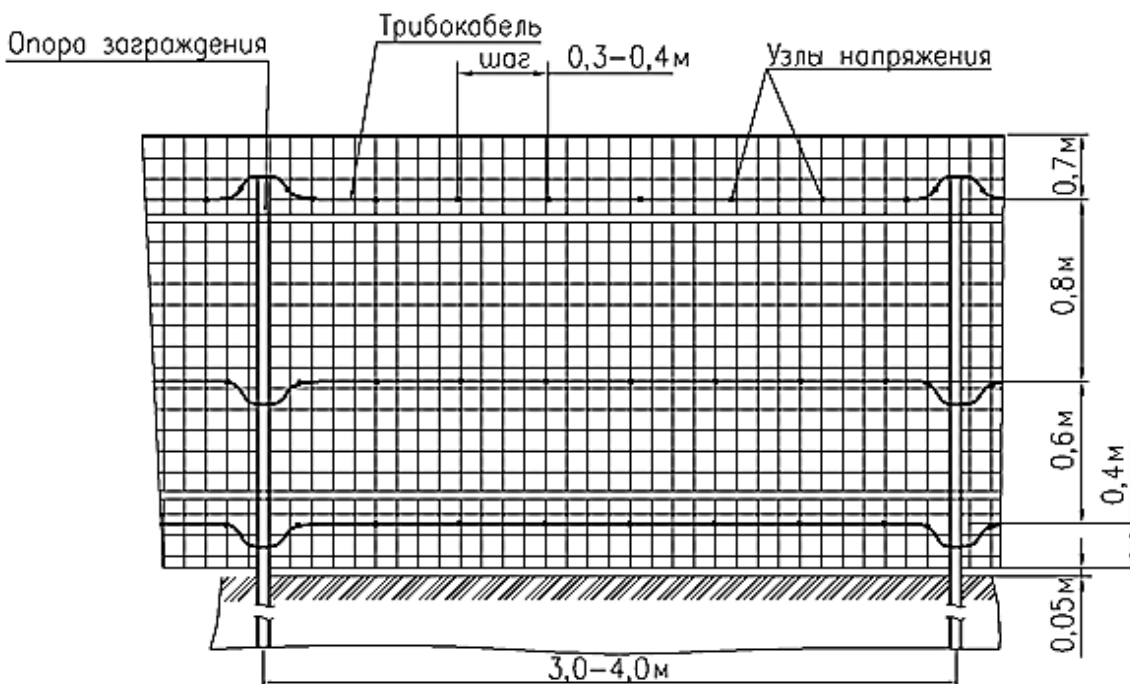


Рис. 3.4. Оборудование ограждения из проволочной сетки ССЦП

Схема расположения чувствительного элемента извещателя на ограждении из проволочной сетки типа «Рабица» представлена на рис. 3.5.

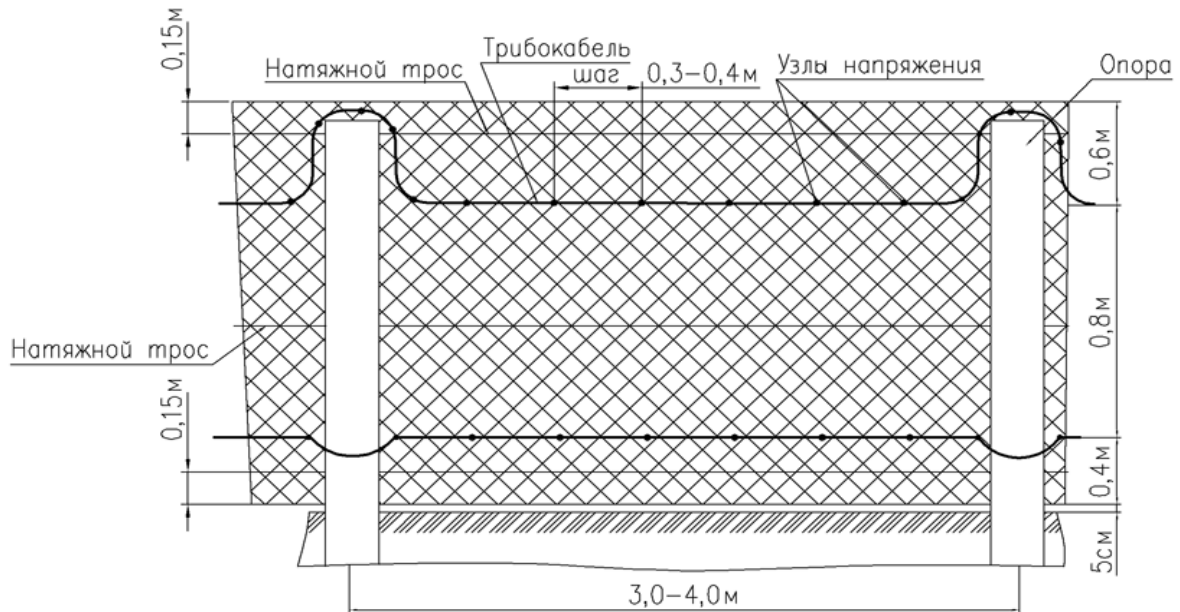


Рис. 3.5. Оборудование ограждения из проволочной сетки типа «Рабица»

Ограждение из колючей проволоки (рис. 3.6) представляет собой несколько горизонтальных линий колючей проволоки, натянутой между жесткими опорами. По диагоналям протянута колючая проволока, скрепленная с каждой горизонтальной линией проволоки, которые должны быть жестко прикреплены к каждой опоре ограждения.

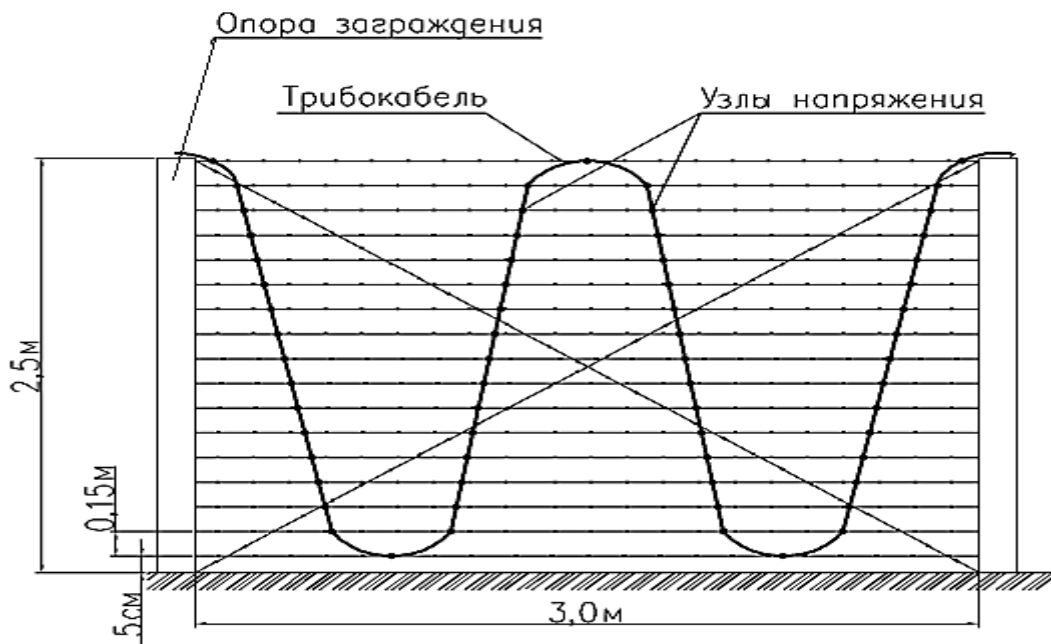


Рис. 3.6. Оборудование ограждения из колючей проволоки

Схема расположения чувствительного элемента извещателя на ограждении из плоской спирали АКЛ представлена на рис. 3.7.

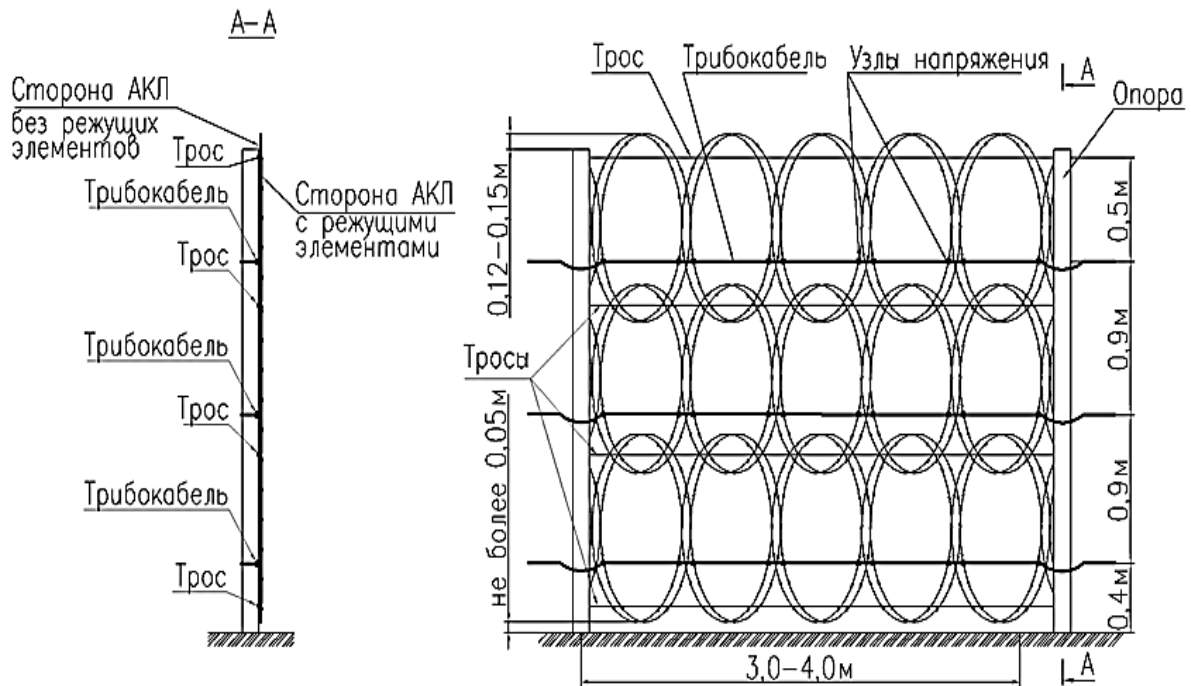


Рис. 3.7. Оборудование ограждения из плоской спирали АКЛ

Для оборудования жесткого ограждения из сварных и кованых решеток чувствительный элемент прокладывают с созданием узлов напряжения на каждом прутке (рис. 3.8).

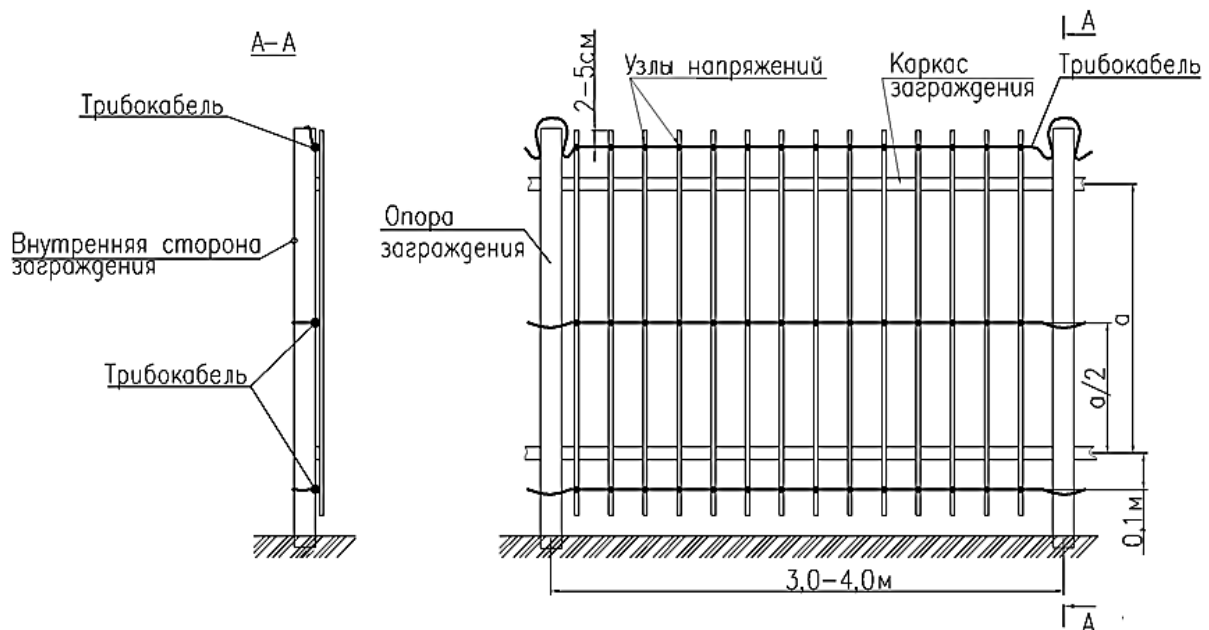


Рис. 3.8. Оборудование ограждения из сварных (кованых) решеток

При наличии гибких дополнительных ограждений над жесткими монолитными ограждениями чувствительный элемент прокладывают по гибкому ограждению (рис. 3.9).

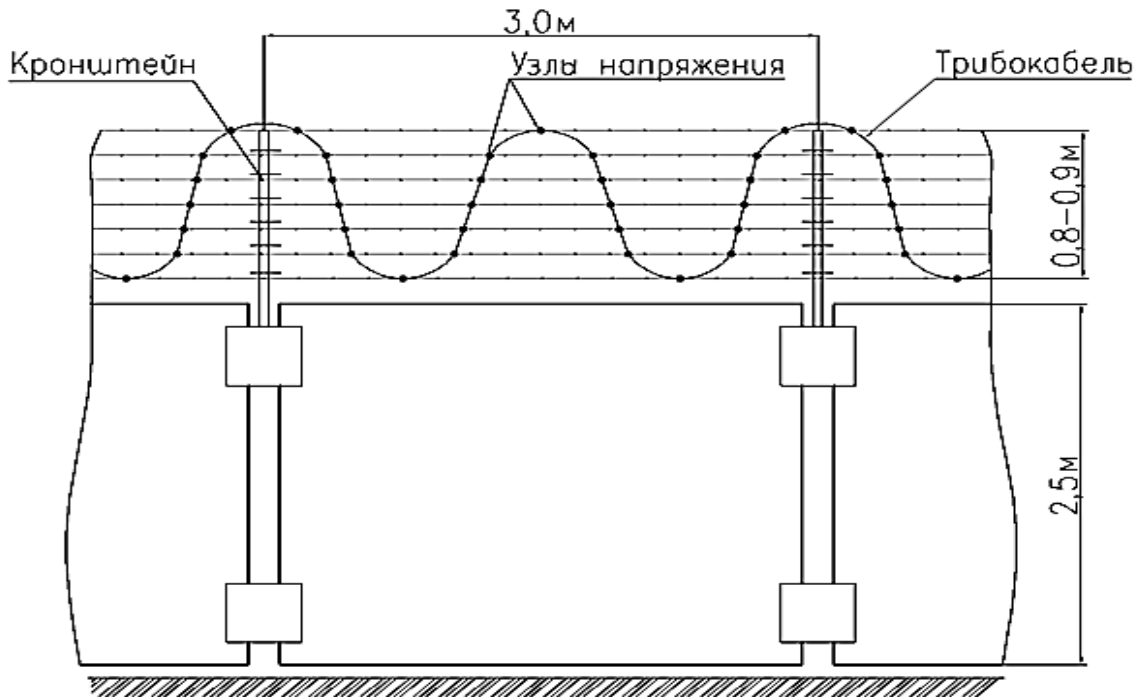


Рис. 3.9. Оборудование гибкого дополнительного ограждения

3.3. Однопозиционные радиоволновые средства обнаружения

Однопозиционные радиоволновые извещатели являются активными средствами обнаружения.

Отличительным признаком однопозиционных радиоволновых извещателей является принцип действия, основанный на использовании эффекта Доплера при излучении и приеме электромагнитных волн сверхвысокой частоты (СВЧ).

Согласно эффекту Доплера, отраженные от движущегося объекта радиоволновые сигналы изменяют частоту относительно частоты излучения. Для электромагнитной волны, распространяющейся в среде со скоростью c , частота ν , регистрируемая приемником при движении источника со скоростью u , излучающего частоту ν_0 , запишется следующим образом:

$$- \text{при приближении источника } \nu = \frac{\nu_0}{1 - \frac{u}{c}}, \quad \nu = \nu_0 \left(1 + \frac{u}{c} \right);$$

$$- \text{при удалении источника } \nu = \frac{\nu_0}{1 + \frac{u}{c}}, \quad \nu = \nu_0 \left(1 - \frac{u}{c} \right).$$

Для релятивистского случая, т.е. когда скорость распространения волны равна скорости света, справедливы следующие формулы:

$$\begin{aligned} \text{– при приближении источника } \nu &= \frac{\nu_0 \sqrt{1 - \frac{u^2}{c^2}}}{1 - \frac{u}{c}}; \\ \text{– при удалении источника } \nu &= \frac{\nu_0 \sqrt{1 - \frac{u^2}{c^2}}}{1 + \frac{u}{c}}. \end{aligned}$$

В радиоволновых извещателях сигнал СВЧ-генератора подается на передающую антенну и излучается в охраняемое пространство. Отражения от объектов сигнала через приемную антенну поступают в приемный блок извещателя. Если в охраняемой зоне появляется движущийся объект, то отраженный от него сигнал будет иметь частоту, отличную от частоты источника. Изменение частоты сигнала свидетельствует о наличии в охраняемой зоне нарушителя.

Доплеровские и разностные частоты, соответствующие минимальной и максимальной скорости движения источника излучения, приведены в таблице 8.

Анализ табличных данных позволяет сделать вывод о необходимости обнаружения частот в диапазоне от 35 Гц до 200 Гц.

Удвоение частоты происходит потому, что движущийся объект (нарушитель) является и приемником и источником излучения.

Таблица 8

Расчет частоты Доплера для движущегося источника излучения

Параметр	Значение	
Частота источника, Гц	1055000000	
Скорость волны, м/с	300000000	
Скорость источника, м/с	0,5	3
Доплеровская частота, Гц	10550000017,58	10550000105,50
Разностная частота, Гц	17,58	105,50

Рассмотрим особенности работы радиоволновых извещателей на примере средства обнаружения «Фон-3Т».

Извещатель «Фон-3Т» предназначен для создания сплошной объемной зоны обнаружения на периметре охраняемого объекта и формирования сигнала тревоги путем размыкания выходных контактов исполнительного реле при движении постороннего объекта в зоне обнаружения.

Конструктивно прибор состоит из:

- извещателя;
- блока программирования.

Блок программирования извещателя «Фон-3Т» представлен на рисунке 3.10.

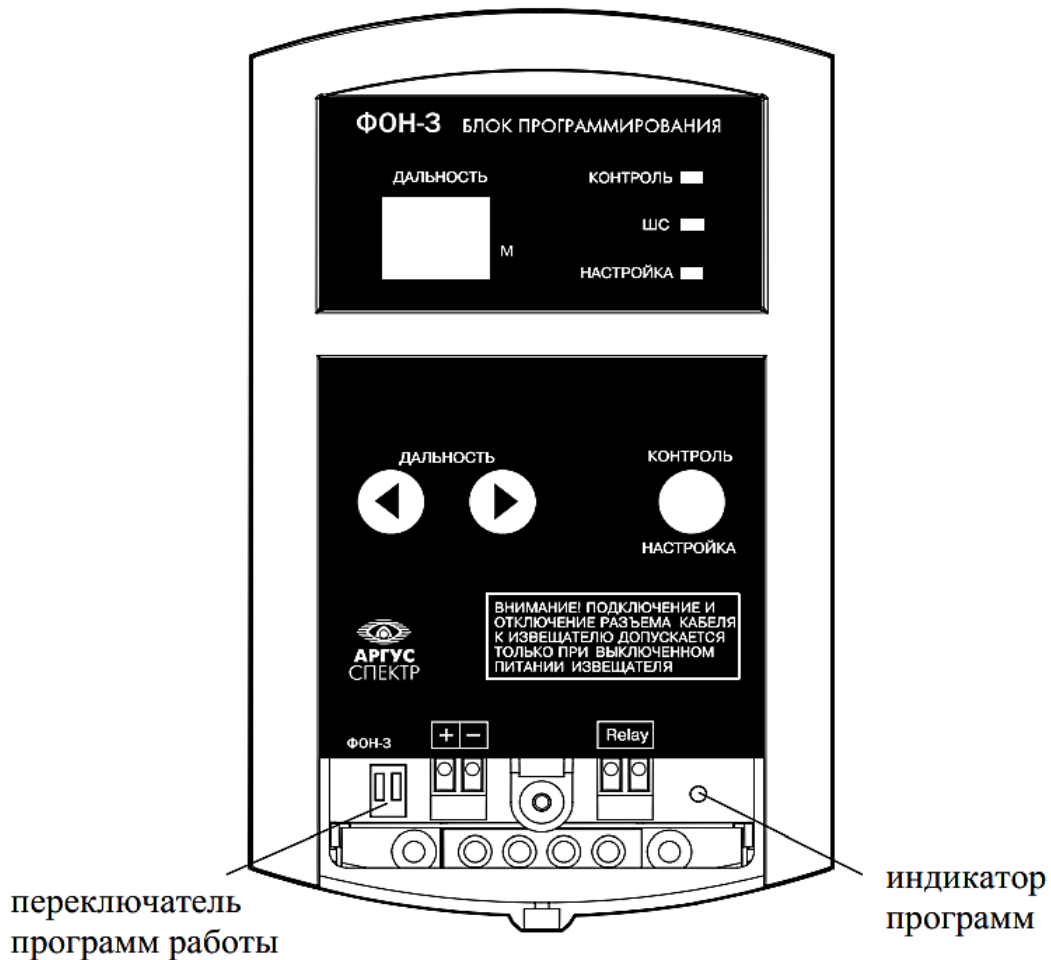


Рис 3.10. Внешний вид блока программирования извещателя «Фон-3Т» (со снятой нижней крышкой)

Принцип действия извещателя базируется на регистрации доплеровской составляющей в спектре отраженного сверхвысокочастотного сигнала, появляющейся при движении объекта в зоне действия электромагнитного поля, образуемого модулем извещателя «Фон 3Т».

СВЧ модуль имеет три антенны. Первая антенна излучающая, остальные две принимают отраженный сигнал. Применение нескольких приемных антенн, находящихся в горизонтальной плоскости, позволяет устойчиво фиксировать перемещение объекта при поперечных траекториях движения.

СВЧ модуль последовательно излучает энергию на трех фиксированных частотах с небольшим разносом. При малых разносах частот доплеровские сигналы почти совпадают по частоте, но имеют отличия по фазе. Величина разности фаз доплеровских сигналов зависит от расстояния между движущимся объектом и извещателем. Тем не менее величина разности фаз меняется и при вибрации предметов. Величины изменения разности фаз определяются в микропроцессоре, и при совпадении их с критериями, соответствующими перемещению объекта в зоне действия, выдается сигнал тревоги.

Значение изменения разности фаз доплеровских сигналов при перемещении объекта существенно выше, чем при разностных вибрациях и колебаниях предметов, что позволяет отделить помехи.

При использовании радиоволновых извещателей на периметре охраняемого объекта следует учитывать, что они обладают более низкой помехозащищенностью по сравнению с пассивными трибоэлектрическими извещателями. Это накладывает дополнительные ограничения на возможности применения данного типа извещателей.

Извещатель «Фон 3Т» устойчив к воздействию следующих видов помех:

- а) ветра скоростью до 30 м/с;
- б) атмосферных осадков интенсивностью до 3 мм/мин;
- в) движения транспорта в границах зоны обнаружения;
- г) колебаний травы высотой до 0,2 м в пределах всей зоны обнаружения, деревьев и кустарника – за границей зоны обнаружения.

Для защиты от колебаний кустов, деревьев и т.п. извещатель может быть поставлен в «помехозащищенный» режим работы, в котором по виду спектров доплеровских сигналов происходит дополнительная селекция помех. Но при этом необходимо учитывать, что устройство, работающее в «помехозащищенном» режиме, обладает низкой обнаружительной способностью при поперечных траекториях движения.

Рассмотрим основные эксплуатационные ограничения работы извещателя.

1. Извещатель должен устанавливаться на жестких не подверженных постоянным вибрациям опорах (капитальные стены, столбы, и т. п.) на высоте $(4 \pm 0,2)$ м. При эксплуатации ограждения из радионепрозрачных материалов допускается установка извещателя на высоте меньше 4 м [45].

2. Поставленные на охраняемом объекте извещатели не должны создавать помех радиоэлектронным средствам, работающим в соответствии с Таблицей распределения полос частот между радиослужбами РФ. Для того чтобы использовать извещатель за пределами зданий и сооружений, его необходимо устанавливать на высоте, не превышающей высоту соседних зданий и сооружений.

3. При установке извещателя вблизи крупных металлических поверхностей или конструкций необходимо учитывать, что они могут отражать СВЧ энергию. Это может привести:

- к образованию «мертвых зон» за металлическими предметами и к выдаче сигнала о тревоге при движении объектов вне охраняемой зоны;
- к переотражению СВЧ энергии в направлении на приемные станции других радиослужб и созданию для них недопустимых помех.

4. Охраняемые открытые площадки должны иметь ограждение высотой не менее 1 м, препятствующее случайному попаданию на площадку посторонних людей и животных. Зона обнаружения не должна быть больше размера площадки.

5. В зоне обнаружения извещателя не должны находиться:

- заросли кустов и деревьев;
- травяной покров высотой более 0,2 м.

3.4. Особенности применения интегрированных комплексов охраны периметра объекта

Центральное место в комплексе технических средств охраны периметра занимает система сбора и обработки информации, которая позволяет создать единую аппаратно-программную платформу для интеграции всех технических подсистем охраны периметра. В настоящее время в качестве таких систем на объектах с протяженным периметром применяют интегрированные комплексы технических средств охраны периметра.

Интегрированные системы должны обеспечивать комплексную безопасность объекта посредством контроля состояния шлейфов охранной и тревожной сигнализации, контроля и управления доступом, видеонаблюдения, связи с постами, участками периметра и помещениями, контроля несения службы.

Рассмотрим особенности применения интегрированных систем безопасности на периметре объекта на примере электронного комплекса охраны «Стрелец – Часовой».

Интегрированный комплекс технических средств охраны «Стрелец – Часовой» предназначен для охраны объектов и обеспечения безопасности личного состава службы охраны.

В структуру комплекса входят:

- пульт управления системой охраны периметра с монитором отображения местонахождения личного состава;
- система радиодатчиков, позволяющих контролировать охраняемый периметр;
- специальные браслеты для личного состава с тревожной кнопкой, дисплеем для приема сообщений и контролем состояния (неподвижности).

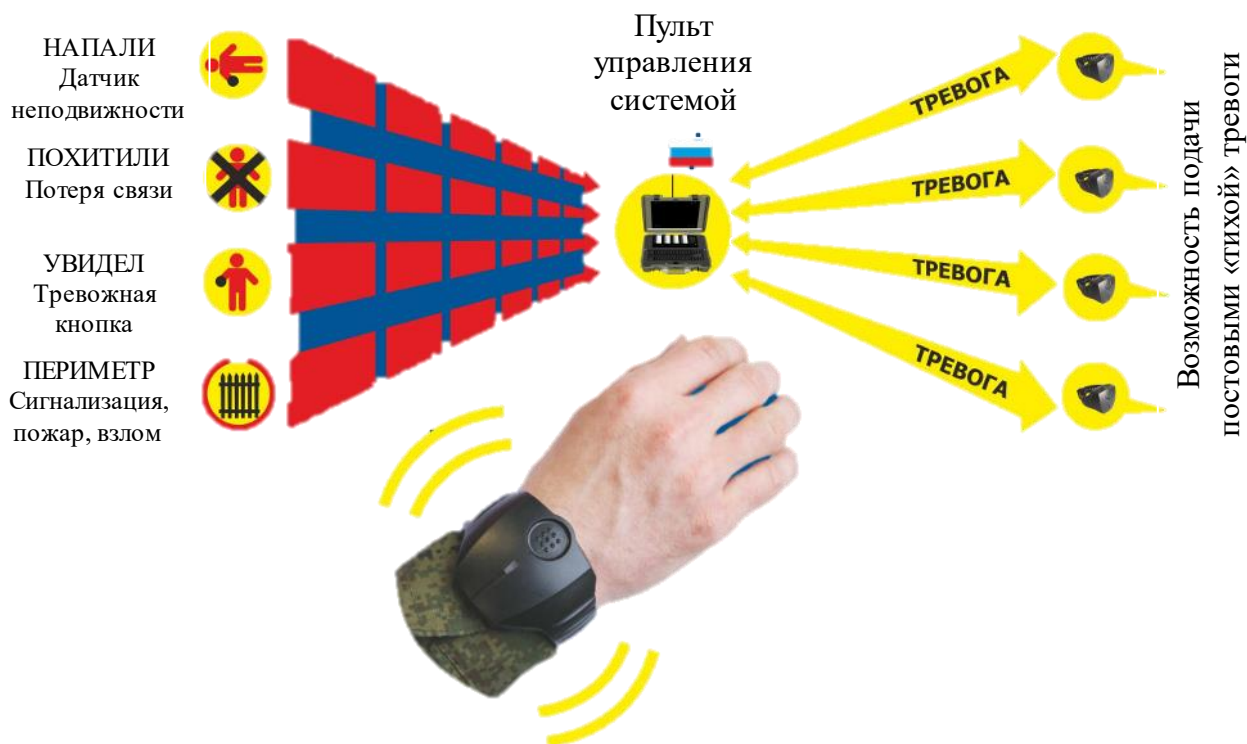


Рис. 3.11. Структура электронного комплекса охраны «Стрелец – Часовой»

Рассмотрим подсистемы охранной сигнализации и тревожно-вызывной сигнализации комплекса «Стрелец – Часовой».

1. Подсистемы охранной сигнализации

Периметровые средства обнаружения интегрированной системы безопасности «Стрелец – Часовой» предназначены для организации охраняемого периметрового рубежа и регистрируют преодоление его нарушителем следующими способами:

- путем пересечения по земле;
- перелаза заграждения через верх без подручных средств или с их применением (доска, приставная лестница);
- подкопа под заглубленный в грунт участок полотна заграждения не более чем на глубину заглубления полотна;
- пролаза с разрушением полотна заграждения (перекусывание, перепиливание, отгиб) или чувствительного элемента;
- подъема или раздвигания нитей полотна заграждения;
- демонтажа, повреждения или разрушения ЧЭ.

В качестве датчиков обнаружения в комплексе «Стрелец – Часовой» могут применяться извещатели с разными физическими принципами действия. Наиболее распространенным является вариант оборудования

периметра объекта двухпозиционными радиоволновыми извещателями, которые создают сплошную объемную зону обнаружения.

Принцип действия радиоволновых периметровых средств обнаружения интегрированной системы безопасности «Стрелец – Часовой» основан на регистрации и анализе сигнала при пересечении зоны обнаружения. Передатчик излучает электромагнитные колебания в направлении приемника. Приемник принимает колебания, излучаемые передатчиком, преобразует их в электрический сигнал и обрабатывает его. При изменении параметров электромагнитного поля на входе приемного устройства датчик формирует сигнал тревоги.

Появление нарушителя в зоне обнаружения вызывает изменение параметров электромагнитного поля на входе приемного устройства. До появления нарушителя в зоне обнаружения амплитуда принимаемых радиоимпульсов практически постоянна. Сигнал тревоги датчик не подает.

Когда в зону обнаружения входит нарушитель, то в приемную антенну будут попадать еще и отраженные от него радиоволны (рис. 3.12).

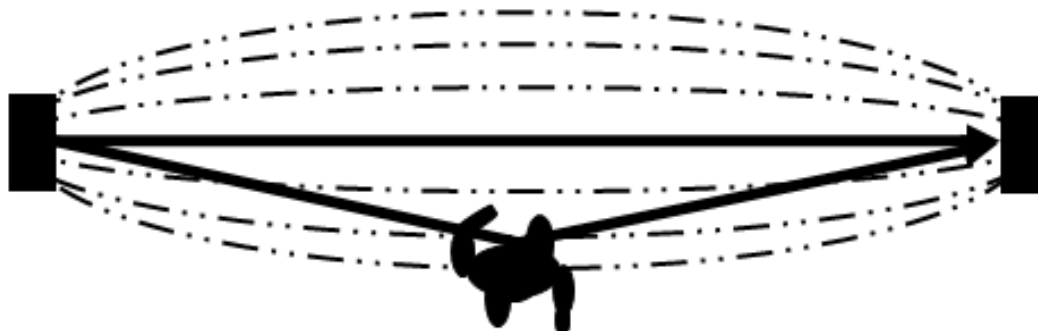


Рис. 3.12. Влияние нарушителя на амплитуду радиоимпульсов

В приемной антенне отраженные и прямые радиоволны либо складываются, либо вычитаются. Все зависит от разности хода прямых и отраженных радиоволн.

Если эта разность равна целому числу длин волн, то фазы радиоволн совпадают. При этом радиоволны складываются, т.е. амплитуда радиоимпульсов на входе ПРМ максимально возрастает. Если разность хода радиоволн равна нечетному числу полуволен, то результирующая амплитуда радиоимпульсов максимально уменьшается.

В зоне обнаружения существуют области, в которых появление нарушителя приводит к увеличению либо уменьшению результирующей амплитуды.

На пути движения нарушителя у границы зоны обнаружения первой может оказаться любая из указанных областей. Следовательно, амплитуда

результатирующих радиоимпульсов может либо увеличиться, либо уменьшиться. Изменения амплитуды в приемной антенне и является первичным электрическим сигналом о появлении нарушителя.

Сигнал тревоги от средств обнаружения на аппаратуру сбора и обработки информации передается по радиоканалу.

Основные тактико-технические и эксплуатационные характеристики подсистемы охранной сигнализации:

- микропроцессорная обработка сигнала с цифровой настройкой;
- несколько уровней чувствительности акустического канала;
- изменяемая чувствительность инфракрасного канала;
- криптографическое закрытие передаваемой информации.

2. Подсистемы тревожно-вызывной сигнализации

Система тревожно-вызывной сигнализации предназначена для дистанционного контроля за действиями должностных лиц наряда, контроля нахождения их в месте несения службы, передачи тревожных сигналов о нападении от личного состава на центральный пульт для вызова групп усиления и обратной передачи тревожных сигналов часовым (оповещение), контроля прохода нарядом контрольных точек по заданному маршруту.

В основе системы лежат носимые устройства персонального оповещения и вызова (браслеты).

Передача информации между составными частями комплекта системы тревожно-вызывной сигнализации производится по самоорганизующейся радиосети.

Комплект тревожно-вызывной сигнализации обеспечивает:

- круглосуточный режим работы;
- формирование тревожных и информационных сигналов на пульт управления;
- автоматический контроль работоспособности составных частей комплекса;
- контроль степени разряда источников питания.

Система тревожно-вызывной сигнализации формирует сообщение «Тревога» при:

- угле отклонения часового от исходного положения более 50 ± 5 градусов «назад», «влево», «вправо»;
- нажатии часовым на кнопку «Тревога»;
- неподвижности часового более 30 с.

Кроме того, система позволяет в режиме реального времени отслеживать местонахождение и все перемещения часового по охраняемой им зоне.

Браслет с помощью вмонтированного модуля навигационной спутниковой системы ГЛОНАСС может запомнить точку и время сбора патрульного и в нужный момент проложить до него самый оптимальный маршрут.

Основные тактико-технические и эксплуатационные характеристики подсистемы тревожно-вызывной сигнализации:

- максимальная мощность радиоизлучения передающих устройств 10 мВт;
- автоматическая смена рабочего частотного канала при помехах;
- рабочие дальности связи устройств до 1 км;
- криптографическое закрытие передаваемой информации;
- аутентификация для исключения подмены радиоустройств и несанкционированного управления состоянием системы;
- устройства сохраняют работоспособность при температуре окружающей среды от минус 50 до плюс 50°С;
- уровень помех, создаваемых устройствами, не превышает норм, установленных ГОСТ Р 50009–2000;
- устройства сохраняют работоспособность и не выдают ложных извещений при воздействии электромагнитных помех УК2, УЭ1 и УИ1 третьей степени жесткости по ГОСТ Р 60009–2000;
- средняя наработка на отказ не менее 60000 часов;
- срок службы приборов 10 лет.

Вопросы для самоконтроля

1. Каким документом регламентируется перечень объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации?

2. Расскажите об устройстве и особенностях применения охранного прибора «Годограф – Универсал».

3. Расскажите о назначении и особенностях работы охранного комплекса «Стрелец – Часовой».

4. Расскажите об устройстве и назначении охранного извещателя «ФОН-3Т».

5. Какие физические воздействия регистрирует охранный прибор «Гюрза»?

6. На каком физическом принципе основана работа трибоэлектрических охранных извещателей?

7. На каком физическом принципе основана работа радиоволновых охранных извещателей?

4. ПРИМЕНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ ПЕРИМЕТРОВ ДЛЯ ОХРАНЫ ОБЪЕКТОВ РАЗНОГО УРОВНЯ СЛОЖНОСТИ

Надежность охраны объектов всегда является главным приоритетом для всех контрагентов и производителей технических средств обеспечения безопасности объектов.

Новые разработки технических средств охраны периметров призваны содействовать улучшению качества охраны и предоставлению дополнительных возможностей.

В настоящее время модельный ряд технических средств охраны периметров предоставляет большие возможности для контроля различных участков периметра объекта. Рассмотрим основные типы извещателей, применяемых на объектах охраны.

1. Двухпозиционные радиоволновые извещатели серии «Призма» для прямолинейных участков периметра:

– «Призма-1» – извещатели для контроля открытых участков, в зоне обнаружения не должны находиться заграждения, столбы и другие сооружения.

– «Призма-2» – извещатели, не имеющие аналогов, для контроля участков, расположенных вплотную к заграждениям, объемная зона обнаружения формируется непосредственно на полотне заграждения и не переходит на сопредельную территорию.

Допускается наличие в зоне обнаружения столбов и других предметов и сооружений.

– «Призма-3» – универсальные извещатели, совмещающие возможности извещателей «Призма-1» и «Призма-2», нужные свойства выбираются непосредственно на объекте [50].

2. Проводноволновые извещатели серии «Импульс» для участков с поворотами и перепадами высот и на пересеченной местности.

– «Импульс-12» – однофланговые извещатели, зарекомендовавшие себя многолетней эксплуатацией, наиболее популярные в своем классе.

– «Импульс-14» – двухфланговая версия извещателя «Импульс-12».

– «Импульс-20» – универсальные извещатели, который могут функционировать в двух режимах:

а) в двухрубежном с определением направления пересечения рубежа охраны;

б) в однофланговом или двухфланговом, однорубежном или двухрубежном без определения направления пересечения.

Кратко остановимся на некоторых типовых решениях для объектов со своими особенностями, размерами и протяженностью периметра. В типовых решениях учтены требования к организации охраны, в том числе рекомендации по выбору модификаций охранного оборудования.

4.1. Оборудование техническими средствами охраны периметра промышленного предприятия

Объект представляет собой комплекс зданий и сооружений, расположенных на общей территории, огороженной заграждением.



Рис. 4.1. Объект – промышленное предприятие

Периметр заграждения оборудован дополнительным инженерным средством защиты – колючей проволокой типа АСКЛ.

Основными вероятными видами угроз безопасности объекта являются:

- угроза хищения, порчи материальных и информационных ценностей, находящихся на территории объекта;
- угроза несанкционированного проникновения на защищаемый объект;
- угроза террористического акта.

Особенности объекта:

- большая протяженность периметра;
- наличие прямолинейных участков большой и малой протяженности;
- заграждение выполнено из разнородных материалов (ж/б плиты, металлический профлист, металлическая сетка);
- наличие зон проезда автотранспорта и ж/д составов.

В качестве основного средства охраны периметра заграждения применяются радиоволновые извещатели «Призма-2/300НР» и «Призма-3-10/100МР»:

- извещатель «Призма-2/300НР» (рис. 4.2) размещается непосредственно на полотне ограждения и применяется на участках более 50 м;
- извещатель «Призма-3-10/100МР» (рис. 4.3) размещается на полотне ограждения и применяется на участках менее 50 м.



Рис. 4.2. Внешний вид радиоволнового извещателя «Призма-2/300НР»



Рис. 4.3. Внешний вид радиоволнового извещателя «Призма-3-10/100МР»

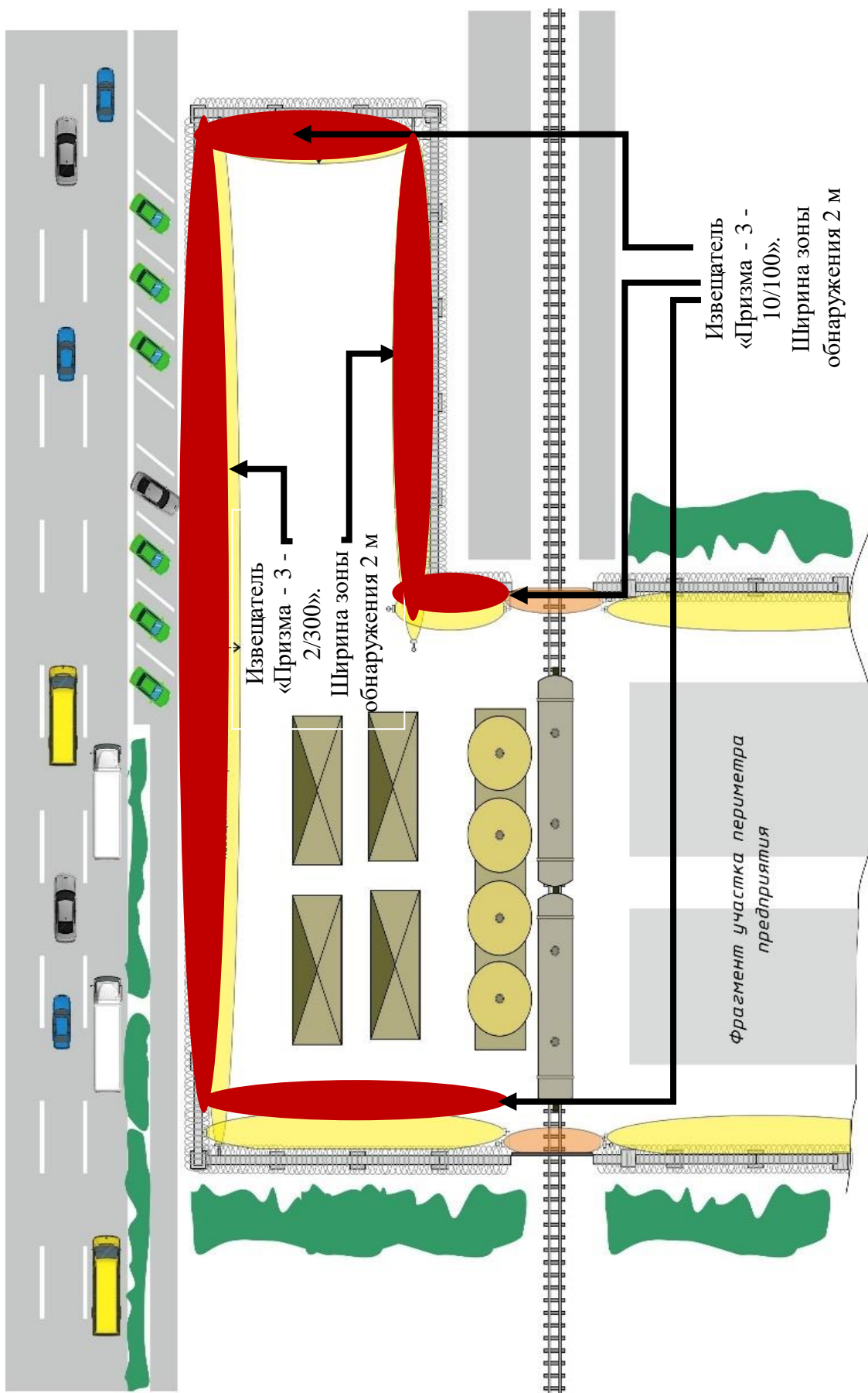


Рис. 4.4. Пример установки изрецагелей на коротких участках

На схеме участка периметра (рис. 4.4.) видно, что, применяя извещатель «Призма-3-10/100», можно на более коротких участках добиться такой же ширины объемной зоны обнаружения, какую формирует извещатель «Призма-2/300» на участках до 200 м. Это обуславливается тем, что угол раскрыва антенн у извещателей серии «Призма-2», составляет 8° , а извещателей серии «Призма-3-10» – 16° [8, 9]. Извещатели успешно функционируют при формировании зоны обнаружения непосредственно на полотне заграждений различного типа.

Так как угол раскрыва антенн извещателей серии «Призма-3-10» равен 16° , то при установке блоков непосредственно на заграждении (применяется наклонная поляризация – антенны расположены под углом 45° , рис 4.5), чувствительная зона раскрывается сразу на большой угол. При этом «мертвые зоны» вблизи блоков практически сводятся к нулю.

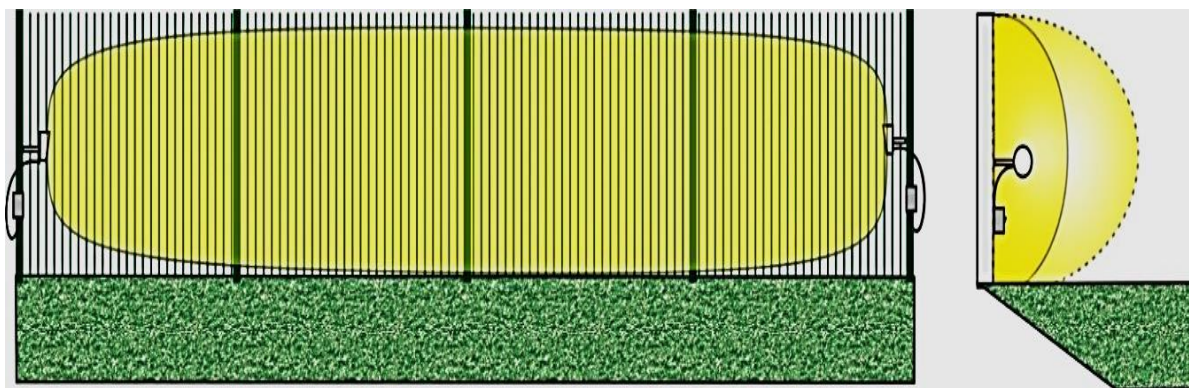


Рис. 4.5. Зона обнаружения извещателя «Призма-3-10»

Для охраны створов ворот для проезда автотранспорта и железнодорожных составов применяются извещатели «Призма-3-10/40М» (рис. 4.6).

Данные извещатели, как правило, устанавливаются на телескопических стойках СТ2. Высота установки блоков регулируется от 0,8 до 1,4 м. В зависимости от вида ворот (распашные либо откатные) извещатели на стойках могут устанавливаться на разном расстоянии от ворот и заграждения.

При установке в непосредственной близости от заграждения для эффективной работы извещателя достаточно выбрать правильный угол наклона поляризации.

Если блоки извещателя установлены вертикально (поляризация антенн 45°), то формируется узкая объемная зона обнаружения, если блоки извещателя установлены под углом 45° (вертикальная или горизонтальная поляризация антенн), то зона обнаружения будет широкой.



Рис. 4.6. Пример установки извещателя «Призма-3-10/40М» для охраны створов ворот

4.2. Оборудование техническими средствами охраны периметра нефтеперерабатывающего завода

Объект представляет собой комплекс зданий и сооружений, расположенных на общей территории, огороженной инженерным заграждением.

Периметровое заграждение выполнено из железобетонных плит.

Основными вероятными видами угроз безопасности объекта являются:

- угроза хищения, порчи материальных и информационных ценностей, находящихся на территории объекта;
- угроза несанкционированного проникновения на защищаемый объект;
- угроза террористического акта.

Особенности объекта:

- необходимость формирования двухрубежной зоны обнаружения, основанной на разных физических принципах действия;
- первая зона обнаружения – по верху заграждения;

– вторая зона обнаружения на сетчатом ограждении не должна «перетекать» на внутреннюю территорию объекта.

Первый рубеж охраняется извещателем «Импульс-20/350ТПМ» (рис. 4.7, 4.8) по верху внешнего железобетонного ограждения способом «козырек».



Рис. 4.7. Внешний вид извещателя «Импульс-20/350ТПМ»



Рис. 4.8. Пример установки извещателя «Импульс-20»

Второй рубеж на участках менее 50 м на внутреннем сетчатом заграждении охраняется радиоволновым извещателем «Призма-2-300Н» (рис. 4.9).



Рис. 4.9. Пример установки на втором рубеже радиоволнового извещателя «Призма-2/300Н»

4.3. Оборудование техническими средствами охраны открытых протяженных объектов государственной границы

Объект представляет собой приграничную территорию, пограничные заставы и пункты пропуска.

Основными вероятными видами угроз безопасности объекта являются:

- угроза проникновения террористических организаций;
- разведывательная и подрывная деятельность;
- незаконный оборот оружия и иных материальных и ценностей;
- незаконная миграция населения [48, 50].



Рис. 4.10. Пример применения охранных извещателей для защиты государственной границы

Особенности объекта:

- большая протяженность периметра на участках пересеченной местности со сложным рельефом;
- сложный рельеф местности.

Для охраны периметра приграничной территории применяется проводно-волновой извещатель «Импульс-20/350ТПМ» в варианте с определением направления движения нарушителей (рис. 4.11).



Рис. 4.11. Пример установки проводно-волнового извещателя «Импульс-20/350ТПМ»

Периметр пограничной заставы охраняется радиоволновыми извещателями «Призма-3-24/250НР1» и «Призма-3-10/100МР» (рис. 4.12).



Рис. 4.12. Вариант установки радиоволнового извещателя «Призма-3-10/100МР»

4.4. Оборудование техническими средствами охраны периметра административного здания

Объект представляет собой комплекс частных владений, расположенных на общей территории, огороженной инженерным заграждением.

Периметр заграждения выполнен из металлического профлиста.

Основной угрозой безопасности объекта является угроза хищения, порчи материальных ценностей собственников.

Особенности объекта:

- близость лесного массива и прилегающие частные постройки с внешней стороны периметра;
- необходимость создания узкой зоны обнаружения.

Для охраны периметра административного здания применяется радиоволновой извещатель «Призма-3-24/250НР1» (рис. 4.13), расположенный по верху заграждения из металлопрофиля.



Рис 4.13. Установка радиоволнового извещателя «Призма-3-24/250НР1» на заграждение

Внутренние периметры административных зданий охраняются с помощью извещателей «Сегмент-3-10» (рис. 4.14).



Рис. 4.14. Пример применения двухпозиционного радиоволнового извещателя «Сегмент-3-10», выполненного в виде уличного светильника, для охраны периметра территории административного здания

Извещатели серии «Сегмент» конструктивно внешне неотличимы от стандартных садово-парковых фонарей. Главное отличие в том, что внутри стойки светильника расположены антенны датчиков. Донором извещателей «Сегмент» стали двухпозиционные радиоволновые извещатели «Призма-3-10».

Придомовую территорию также возможно охранять радиоволновыми извещателями серии «Фонарь» и «Светильник» (рис. 4.15).



Рис. 4.15. Внешний вид радиоволновых извещателей серии «Фонарь» (а и б) и «Светильник» (в)

Извещатели применяются для охраны административных зданий, парковых территорий, коттеджей и других объектов, где предъявляются повышенные требования к внешнему виду территории или скрытности охранной сигнализации.

Принцип действия аналогичен принципу действия двухпозиционных радиоволновых извещателей. Зона обнаружения имеет объемный вид и формируется между передатчиком и приемником, расположенными в корпусе извещателей «Фонарь» и «Светильник». При пересечении этой зоны нарушителем приемник формирует сигнал тревоги.

Извещатели выполняют две функции: охрана объекта и декоративное освещение, при этом освещение может включаться и выключаться вручную или автоматически.

В корпусе одного извещателя смонтированы один или два приемника или передатчика, что исключает избыточность корпусов и уменьшает количество монтажных работ.

Извещатели имеют несколько частотных литер, что позволяет устойчиво работать нескольким извещателям в непосредственной близости друг от друга.

4.5. Оборудование техническими средствами охраны периметра объектов культурного наследия

Объект представляет собой комплекс сооружений, расположенных на общей территории, огороженной декоративным заграждением.

Основными вероятными видами угроз безопасности объекта являются:

- угроза хищения, порчи материальных ценностей, находящихся на территории объекта;
- угроза несанкционированного проникновения на защищаемый объект.

Особенности объекта:

- повышенные эстетические требования к внешнему виду охранных приборов;
- расположение охраняемых объектов в условиях плотной городской застройки;
- отсутствие выделенных зон отчуждения.

Рубежи охраны организуются с помощью радиоволновых извещателей «Призма-3-24/250HE». Датчики могут размещаться на различных поверхностях, в разных плоскостях, включая элементы архитектурных строений, не нарушая внешнего вида архитектурных ансамблей и сооружений.

Оптимальный выбор типа извещателей и вариантов их расположения на периметре позволяет создать качественную систему безопасности [5, 7].

Вопросы для самоконтроля

1. Какие охранные приборы целесообразно применять на периметре промышленных предприятий?
2. Какие охранные приборы целесообразно применять на периметре нефтеперерабатывающего завода?
3. Основные характеристики охранного прибора «Импульс-20».
4. Основные характеристики и назначение охранного прибора «Призма-3-10».
5. Основные характеристики и назначение охранного прибора «Сегмент-3-10».
6. Какие охранные приборы целесообразно применять на периметре частного домовладения?
7. Какие особенности необходимо учитывать при разработке системы безопасности объектов культурного наследия?
8. Какие особенности необходимо учитывать при организации охраны объектов топливно-энергетического комплекса?
9. Какие особенности необходимо учитывать при организации охраны частных домовладений?

ЗАКЛЮЧЕНИЕ

В современном представлении система защиты периметра является составной частью общего комплекса инженерно-технических средств физической защиты. Такая системность отражена в структуре пособия: материал изложен по принципу «от общего к частному».

Моделирование систем безопасности объектов является одним из перспективных направлений повышения качества их функционирования и позволяет разработать надежную систему охраны с минимальными затратами финансовых и временных ресурсов.

В настоящее время все большую актуальность приобретает задача моделирования и построения эффективной системы периметральной охраны объекта, расположенного на достаточно большой площади. Для таких объектов организация охраны периметра, безусловно, является одной из главных составляющих системы безопасности.

Интерес к исследованию проблем, связанных с обеспечением комплексной безопасности объектов, обусловлен увеличением количества объектов, подлежащих обязательной государственной охране подразделениями вневедомственной охраны. Среди них особое место занимают критически важные объекты, объекты особой важности и повышенной опасности, а также объекты топливно-энергетического комплекса, многие из которых имеют протяженный периметр. Между тем защита территорий большой площади (нефтехранилища, аэропорты, склады готовой продукции, большие автостоянки и т. п.) – задача достаточно сложная и на данный момент не имеющая однозначного решения.

В данном пособии описаны вопросы, касающиеся организации периметральных систем безопасности объектов. В первой главе описаны общие вопросы организации и функционирования периметральных систем безопасности объектов. Во второй главе рассказано о том, как можно моделировать различные составляющие системы безопасности периметра объекта, например охранное освещение, систему охранного телевидения и другие. В третьей главе рассмотрены технические средства охраны. В четвертой главе описаны возможные технические решения, которые позволяют обеспечить безопасность объектов различного функционального назначения.

Проектирование систем защиты периметров требует использования комплексного подхода, предполагающего анализ и учет всех возможных угроз охраняемому объекту. Применяемые средства и методы должны быть разумно достаточны, адекватны возможной угрозе, а меры противодействия должны быть сбалансированы, т.е. распределены по возможности в соответствии с вероятностью угроз и важностью защищаемой зоны.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты:

1. О войсках национальной гвардии Российской Федерации : федеральный закон от 3 июля 2016 г. № 226-ФЗ [Электронный ресурс]. – Режим доступа: [http:// garant.ru/](http://garant.ru/)

2. О перечне объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации : распоряжение Правительства Российской Федерации от 15 мая 2017 г. № 928-р [Электронный ресурс]. – Режим доступа: [http:// garant.ru/](http://garant.ru/)

3. Об утверждении правил охраны имущества физических и юридических лиц по договорам войсками национальной гвардии Российской Федерации: приказ Росгвардии от 28 декабря 2018 г. № 669 [Электронный ресурс]. – Режим доступа: [http:// garant.ru/](http://garant.ru/)

4. Об утверждении руководства по организации службы пунктов централизованной охраны подразделений вневедомственной охраны войск национальной гвардии Российской Федерации : приказ Росгвардии от 25 февраля 2019 г. № 59 [Электронный ресурс]. – Режим доступа: [http:// garant.ru/](http://garant.ru/)

5. Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий): постановление Правительства Российской Федерации от 11 февраля 2017 г. № 176 [Электронный ресурс]. – Режим доступа: [http:// garant.ru/](http://garant.ru/)

6. Об утверждении правил охраны объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации, в соответствии с перечнем, утвержденным Правительством Российской Федерации : приказ Росгвардии от 27 сентября 2018 № 427 (зарегистрировано в Минюсте РФ 26.10.2018 № 52529) [Электронный ресурс]. – Режим доступа: [http:// garant.ru/](http://garant.ru/)

7. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ МВД России от 31 декабря 2014 № 1152 (ред. 06.02.2018) [Электронный ресурс]. – Режим доступа: [http:// garant.ru/](http://garant.ru/)

8. Об утверждении Административного регламента исполнения Федеральной службой войск национальной гвардии Российской Федерации государственной функции по осуществлению федерального государственного контроля (надзора) за обеспечением безопасности объектов топливно-энергетического комплекса: приказ Федеральной службы войск национальной гвардии Российской Федерации от 3 октября

2017 года № 418 [Электронный ресурс]. – Режим доступа: <http://docs.cntd.ru/document/>

9. О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам антитеррористической защищенности объектов : федеральный закон Российской Федерации от 23 июля 2013 года № 208-ФЗ (ред. от 23 июля 2013 г.) [Электронный ресурс]. – Режим доступа: <http://garant.ru/>

10. ГОСТ Р 57674-2017. Интегрированные системы безопасности. Общие положения [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

11. ГОСТ 28195-89. Оценка качества программных средств. Общие положения [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

12. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

13. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

14. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

15. ГОСТ Р 52551-2016. Системы охраны и безопасности. Термины и определения. [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

16. ГОСТ Р 53195.1-2008. Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

17. ГОСТ Р 54126-2010. Оповещатели охранные. Классификация. Общие технические требования и методы испытаний [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

18. ГОСТ Р 54830-2011. Системы охранные телевизионные. Компрессия оцифрованных видеоданных. Общие технические требования и методы оценки алгоритмов [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

19. ГОСТ Р 54831-2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

20. ГОСТ Р 56035-2014. Системы охранные телевизионные. Защита оцифрованных видеоданных от случайного и преднамеренного искажения. Общие требования [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

21. ГОСТ Р 56047-2014. Системы охранные телевизионные. Компрессия оцифрованных аудиоданных. Классификация. Общие требования и методы оценки алгоритмов [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

22. ГОСТ Р 56102.1.-2014. Системы централизованного наблюдения. Часть 1. Общие положения [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

23. ГОСТ Р 52860-2007. Технические средства физической защиты. Общие технические требования [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

24. ГОСТ 14254-2015. (IEC 60529:2013) Степени защиты, обеспечиваемые оболочками (Код IP) (с Поправкой) [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

25. ГОСТ Р 50009-2000. Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний [Электронный ресурс]. – Режим доступа: <https://rags.ru/gosts/>

26. СП 52.13330.2016. Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95 [Электронный ресурс]. – Режим доступа: <https://rags.ru/>

Основная литература:

27. Системы защиты периметра / под ред. С. И. Корчагина. – 2-е изд. – Москва: Секьюрити Фокус, 2019. – 282 с.: цв. ил. (Энциклопедия безопасности).

28. Организация использования систем охраны периметра объектов : учебно-методическое пособие [Электронное издание] / С. А. Винокуров [и др.]. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2018. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

29. Обеспечение комплексной системы охраны объектов с большой протяженностью периметра : методические рекомендации / С. А. Винокуров [и др.]. – Воронеж : Воронежский институт МВД России, 2011. – 87 с.

30. Щербакова И. В. Организация периметральных систем безопасности объектов : учебное пособие / И. В. Щербакова, С. А. Гречаный, С. В. Шишкин. – Воронеж : Воронежский институт МВД России, 2014. – 94 с.

31. Ворона В. А. Теоретические основы обеспечения безопасности объектов информатизации : учебное пособие / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. – Москва : Горячая линия – Телеком, 2016. – 304 с.

32. Ворона В. А. Технические системы охранной и пожарной сигнализации / В.А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 374 с.

33. Ворона В. А. Технические системы охранной и пожарной сигнализации / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 376 с.

34. Мальцев А. Методика оценки состояния инженерно-технической защищенности объектов / А. Мальцев // Технологии защиты. – 2010. – № 4. – С. 15–21.

35. Попов А. Л. Система видеонаблюдения для стационаров – общие моменты / А. Л. Попов // Алгоритм Безопасности. – 2017. – № 3. – С. 60–64.

Дополнительная литература:

36. Применение радиоволновых и комбинированных извещателей с целью повышения обнаруживающей способности и помехозащищенности : методическое пособие (Р 78.36.022–2013). – Москва : НИЦ «Охрана», 2012. – 120 с.

37. Технические средства обнаружения проникновения и угроз различных видов. Особенности выбора, эксплуатации и применения в зависимости от степени важности и опасности объектов : рекомендации (Р 78.36.028–2012). – Москва : НИЦ «Охрана», 2012. – 359 с.

38. Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации : методические рекомендации (Р 078–2019). – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2019. – 84 с.

39. Мониторинг применения и сравнительный анализ испытаний различных видов периметрового ограждения (основного ограждения, дополнительного ограждения, предупредительного внешнего и внутреннего ограждения). Классификация : рекомендации (Р 78.36.034–2013). – Москва : НИЦ «Охрана», 2012. – 56 с.

40. Участие подразделений вневедомственной охраны Росгвардии в мероприятиях по антитеррористической защищенности объектов различной ведомственной принадлежности в рамках реализации федеральных законов от 21 июля 2011 года № 256-ФЗ, от 9 февраля 2007 года № 16-ФЗ, от 6 марта 2006 года № 35-ФЗ, а также подзаконных актов, изданных в рамках их реализации : методические рекомендации (Р 075–2018). – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2018. – 35 с.

41. Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны огражденных территорий и открытых площадок (Р 068–2017). – Москва : ФКУ «НИЦ «Охрана» Росгвардии; Саратов : Амирит, 2017. – 110 с.

42. Дровникова И. Г. Модель нарушителя в системе безопасности. – И. Г. Дровникова, Т. А. Буцынская // Системы безопасности. – 2008. – № 5. – С. 144–147.

43. СТФВ.425624.056 РЭ. ред. 1.0. Комплекс технических средств охраны «Стрелец-Часовой-1-СВ» : руководство по эксплуатации на периметровые средства охраны. – Санкт-Петербург, 2017. – 29 с.

44. СТФВ.425624.049 РЭ. ред. 1.0. Комплекс технических средств охраны «Стрелец-Часовой-1-СВ» : руководство по эксплуатации на систему тревожно-вызывной сигнализации. – Санкт-Петербург, 2017. – 42 с.

45. ЯЛКГ.425144.001 РЭ. Версия 1.6. Извещатели охранные объемные радиоволновые ИО-407-14 «ФОН-3»: руководство по эксплуатации. – Санкт-Петербург : Аргус-Спектр, 2012. – 41 с.

Электронные ресурсы:

46. Безопасность периметра [Официальный сайт]. – URL: <http://perimetr.3dn.ru/> (дата обращения: 25.02.2020).

47. Охрана периметра [Официальный сайт]. – URL: <https://vashtvmir.ru/uslugi/oxrana-perimetra/> (дата обращения: 07.03.2020)

48. НИЦ «Охрана» [Официальный сайт]. – URL: <http://www.nicohrana.ru/> (дата обращения: 25.02.2020).

49. ЗАО «НПП «СКИЗЭЛ» [Официальный сайт]. – URL: <http://skichel.ru/ru/main> (дата обращения: 12.02.2020).

50. Группа компаний «Омега-Микродизайн» [Официальный сайт]. – URL: <https://www.tso-perimetr.ru/> (дата обращения: 21.02.2020).

Учебное издание

Винокуров Станислав Анатольевич
Гречаный Сергей Анатольевич
Щербакова Ирина Владимировна
Сидоров Александр Викторович
Герасименко Евгений Сергеевич

**МОДЕЛИРОВАНИЕ ПЕРИМЕТРАЛЬНЫХ СИСТЕМ
БЕЗОПАСНОСТИ ОБЪЕКТОВ**

Учебно-методическое пособие

Редактор Н. Ф. Палихова
Компьютерная верстка А. В. Сидоров

Подписано в печать 25.12.2020. Формат 60×84 ¹/₁₆
Усл. печ. л. 6,04
Тираж 50 экз. Заказ № 224

Воронежский институт МВД России
394065 Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53