Утверждены
постановлением Правительства
Республики Казахстан
от « 3 » апреля 2015 года
№ 191

Требования
к системе антитеррористической защиты объектов,
уязвимых в террористическом отношении

1. Общие положения

1. Каждый объект, уязвимый в террористическом отношении, включенный в перечень объектов Республики Казахстан, уязвимых в террористическом отношении, должен иметь систему антитеррористической защиты в соответствии с настоящими требованиями к системе антитеррористической защиты объектов, уязвимых в террористическом отношении (далее – требования).

2. Целью создания системы антитеррористической защиты объектов, уязвимых в террористическом отношении (далее – система), является обеспечение их безопасности от воздействия террористических угроз.

3. Понятия и термины, применяемые в настоящих требованиях:

1) система антитеррористической защиты объектов, уязвимых в террористическом отношении, – совокупность компонентов инженерно-технической укрепленности, системы контроля и управления доступом, системы связи и оповещения, телевизионной системы видеонаблюдения, а также освещения, используемых в зданиях, строениях, сооружениях и иных объектах для обеспечения их антитеррористической безопасности;

2) инженерно-техническая укрепленность – конструктивные элементы, обеспечивающие необходимое противодействие несанкционированному проникновению в охраняемые зоны и другим преступным посягательствам;

3) периметр – граница охраняемой территории (зоны), оборудованная ограждающими строительными конструкциями (барьерами) и контрольно-пропускными пунктами;

4) контрольно-пропускной пункт – специальное помещение, предназначенное для обеспечения пропуска людей и разрешенного вида транспортных средств;

5) критическая зона – помещение, участки и конструктивные элементы, реализация террористической угрозы в отношении которых может привести к негативным последствиям;

6) охраняемая зона – часть здания и/или территории (объекта), в которой может (должно) быть обнаружено изменение контролируемых параметров с помощью системы охранной сигнализации;

7) рубеж охраны – совокупность инженерно-технических средств и систем безопасности, контролирующих определенную зону объекта или помещения (периметр, объем и подходы к ним), при преодолении которых выдается соответствующее извещение на оборудование контроля состояния объекта или выносные оповещатели (звуковая, световая индикация);

8) система охранной сигнализации – совокупность совместно действующих технических средств для обнаружения несанкционированного проникновения на объект охраны, нарушения целостности охраняемого объекта, сбора, обработки, передачи и представления информации в заданном виде о нарушении целостности объекта;

9) рубеж охранной сигнализации – совокупность совместно действующих технических средств охранной сигнализации, последовательно объединенных электрической цепью, позволяющих выдать извещение о проникновении (попытке проникновения) в охраняемую зону (зоны), независимо от других технических средств, не входящих в данную цепь;

10) пульт централизованного наблюдения – самостоятельное техническое средство (совокупность технических средств) или составная часть системы передачи извещений, устанавливаемые в пункте централизованной охраны для приема тревожных извещений о проникновении на охраняемые объекты, служебных и контрольно-диагностических извещений, обработки, отображения, регистрации полученной информации и представления ее в заданном виде для дальнейшей обработки, а также (при наличии обратного канала) для передачи команд телеуправления;

11) система контроля и управления доступом – совокупность совместно действующих технических средств контроля и управления (механические, электромеханические, электрические, электронные устройства, конструкции и программные средства), обладающих технической, информационной, программной, эксплуатационной совместимостью и осуществляющих контроль и управление доступом людей и транспорта;

12) система связи – система оперативной связи, предназначенная для обеспечения оперативного управления деятельностью служб охраны объекта;

13) система оповещения – совокупность технических средств, предназначенных для оперативного информирования (светового и/или звукового оповещения) находящихся на объекте, уязвимом в террористическом отношении, лиц о тревоге при чрезвычайных происшествиях (аварии, пожаре, стихийном бедствии, нападении, террористическом акте) и действиях в сложившейся обстановке;

14) телевизионная система видеонаблюдения – совокупность совместно действующих технических средств, обладающих технической,

информационной, программной и эксплуатационной совместимостью, предназначенных для получения изображений о состоянии объекта;

15) подразделения охраны – субъекты охранной деятельности, обеспечивающие охрану объектов, уязвимых в террористическом отношении.

4. Настоящие требования распространяются на действующие, вновь проектируемые, реконструируемые и технически модернизированные объекты, уязвимые в террористическом отношении, независимо от формы собственности и ведомственной принадлежности, расположенные на территории Республики Казахстан, а также устанавливают порядок оснащения инженерно-техническими средствами и системами безопасности объектов с целью противодействия преступным посягательствам на них.

5. Инженерно-техническая укрепленность объектов, подлежащих государственной охране, обеспечивается в соответствии с требованиями, утвержденными постановлением Правительства Республики Казахстан от 7 октября 2011 года № 1151.

Требования к инженерно-технической укрепленности объектов Вооруженных Сил определяются в соответствии с Указом Президента Республики Казахстан от 5 июля 2007 года № 364 «Об утверждении общевоинских уставов Вооруженных Сил, других войск и воинских формирований Республики Казахстан», а также приказами Министра обороны Республики Казахстан.

Службой государственной охраны Республики Казахстан устанавливаются дополнительные требования к системе антитеррористической защиты объектов, уязвимых в террористическом отношении, предназначенных для пребывания охраняемых лиц, с учетом настоящих требований, объема и специфики организационных, охранных, режимных и иных мер, обеспечивающих необходимые уровни их безопасности.

2. Требования к системе антитеррористической защиты особо важных государственных, стратегических, опасных производственных объектов

Требования к инженерно-технической укрепленности периметра

6. Объект, имеющий территорию, оборудуется по периметру ограждением, препятствующим свободному проходу лиц и проезду транспортных средств на объект и с объекта, минуя контрольно-пропускной пункт.

Магистральные трубопроводы и территории месторождений также могут оборудоваться ограждением, препятствующим свободному проходу лиц и проезду транспортных средств в охраняемые зоны.

7. Ограждение является капитальным сооружением и строится по типовым проектам.

8. Ограждение должно иметь:

1) высоту и заглубленность в грунт, исключающие свободное преодоление и удовлетворяющие режимным условиям объекта;

2) простоту в конструкции, высокую прочность и долговечность;

3) отсутствие узлов и конструкций, облегчающих его преодоление.

9. Не допускается во внешнем ограждении наличие незапираемых дверей, ворот, калиток, а также лазов, проломов и других повреждений.

10. На участках с повышенной опасностью периметр может укрепляться путем установки противотаранных и (или) иных дополнительных заградительных устройств.

Помимо инженерно-технических конструкций периметр оснащается средствами освещения, связи и телевизионной системы наблюдения.

11. Инженерно-технические конструкции для обеспечения безопасности периметра объектов должны соответствовать следующим характеристикам:

1) устойчивость к внешним климатическим факторам всех сезонов и соответствующих климатических зон;

2) защищенность от индустриальных помех и помех, вызываемых транспортными средствами, воздействия птиц и животных.

12. К внешнему ограждению объектов и помещений организаций, занятых проведением работ по разработке, производству, испытанию, хранению взрывчатых, особо опасных, бактериологических, биологических веществ, источников ионизирующего излучения, радиоактивных и двойного назначения материалов, применяются специальные требования в соответствии с Положением о физической защите ядерных материалов и ядерных установок, а также санитарно-гигиеническими требованиями по обеспечению радиационной безопасности, другими нормативными правовыми актами в соответствующей области применения.

13. Особо важные государственные, стратегические, опасные производственные объекты, на которых установлен пропускной режим, оснащаются контрольно-пропускными пунктами.

14. Количество контрольно-пропускных пунктов определяется с учетом обеспечения необходимой пропускной способности людей и транспортных средств.

Автотранспортный контрольно-пропускной пункт должен располагаться вблизи центрального контрольно-пропускного пункта для прохода людей.

Контрольно-пропускной пункт для проезда автомобильного и железнодорожного транспорта допускается делать совмещенным.

15. Наружные ограждающие конструкции (стены и перекрытия) зданий (помещений) контрольно-пропускных пунктов должны быть устойчивыми к внешним воздействиям, включая действия противоправного характера, и иметь хороший обзор.

16. Контрольно-пропускной пункт оборудуется камерой хранения личных вещей рабочих и служащих, комнатой досмотра, служебным помещением для размещения сотрудников подразделений охраны, техническими системами безопасности (концентраторами, пультами, видеоконтрольными устройствами охранного телевидения и т.п.), устройствами управления механизма открывания прохода (проезда), охранного освещения и санузлом.

В контрольно-пропускном пункте устанавливаются автоматизированные или механические ручные устройства, турникеты, калитки для предотвращения несанкционированного прохода людей.

Допускается оборудовать контрольно-пропускной пункт стационарными и ручными средствами для производства досмотра, способными распознавать различные типы металлов в зависимости от необходимости или служебной потребности.

17. Контрольно-пропускной пункт для транспортных средств оборудуется типовыми раздвижными или распашными воротами с электроприводом и дистанционным управлением, устройствами для их аварийной остановки и открытия вручную. Ворота оснащаются ограничителями или стопорами для предотвращения произвольного открывания (движения). Контрольно-пропускной пункт для автотранспортных средств оборудуется смотровыми площадками или эстакадами для их осмотра, шлагбаумами, а контрольно-пропускной пункт для железнодорожного транспорта – вышкой и площадкой для осмотра подвижного железнодорожного состава.

18. Пульт управления воротами располагается в местах, исключающих доступ к ним посторонних лиц.

19. Помещение контрольно-пропускного пункта оснащается средствами связи, пожаротушения и оборудуется системой тревожной сигнализации с подключением на пульт централизованного наблюдения.

Требования к инженерно-технической укрепленности зданий и сооружений

20. Размещение на территории особо важных государственных, стратегических, опасных производственных объектов зданий и сооружений, включая корпусы с оборудованием непрерывного производственного цикла, необходимо обеспечивать на максимально возможном удалении от периметра с учетом прикрытия их близлежащими зданиями и сооружениями.

21. Наружные стены зданий и сооружений должны быть капитальными и соответствовать утвержденным нормам и правилам Республики Казахстан.

22. При установке запирающихся устройств в зданиях и сооружениях необходимо выполнять условия противопожарной безопасности:

1) наружные эвакуационные двери зданий и сооружений не должны иметь запоров, которые не могут быть открыты изнутри без ключа;

2) двери лестничных клеток, ведущие в общие коридоры, двери лифтовых холлов и тамбуров-шлюзов оборудуются приспособлениями для самозакрывания и уплотнения в притворах и не должны иметь запоров, препятствующих их открыванию без ключа.

23. Подземные и наземные коммуникации, имеющие входы или выходы в виде колодцев, люков, лазов, шахт, открытых трубопроводов, каналов и других подобных сооружений, через которые можно проникнуть в здания и сооружения, оборудуются постоянными или съемными решетками, крышками, дверями с запирающими устройствами.

Постоянные устройства должны устанавливаться на все коммуникации, не подлежащие открыванию, а также проемы, имеющие диаметр более 250 миллиметров (сечением более 250х250 миллиметров).

Требования к инженерно-технической укрепленности помещений подразделений охраны

24. Помещения подразделений охраны следует размещать, как правило, на первом этаже зданий, при этом требования к конструкции помещений должны соответствовать требованиям, предъявляемым к конструкции соответствующей категории зданий.

25. Инженерные конструкции постов охраны, к которым относятся наблюдательные вышки, постовые грибки и будки, изгородки в виде барьеров, должны соответствовать следующим характеристикам:

1) наблюдательные вышки делаются из кирпича, дерева, металла или сборного железобетона и устанавливаются для увеличения обзора и просмотра охранниками территории и подступов к объекту. Высота вышки и место ее установки определяются в зависимости от рельефа местности, конфигурации и местных условий;

2) состав технических средств для оборудования вышек определяется заданием на проектирование;

3) конструкция вышки должна обеспечивать защиту охранника от поражения огнестрельным оружием;

4) постовые грибы устанавливаются, как правило, в центре участков постов на расстоянии не более 1-го метра от тропы нарядов;

5) постовые будки делаются из кирпича, дерева, сборного железобетона, металлоконструкций, пластика, прессованных и деревянных деталей. В районах, где температура опускается ниже минус 30°С, в постовых будках предусматривается отопление. Размеры и типы постовых будок определяются проектной организацией;

6) для обозначения границ участков постов применяются разграничительные знаки. Они нумеруются и последовательно устанавливаются таким образом, чтобы хорошо были видны нарядам и не просматривались посторонними лицами с внешней стороны участка.

Требования к системе охранной сигнализации

26. Системой охранной сигнализации оборудуются все помещения с постоянным или временным хранением секретной информации или материальных ценностей, а также все смежные с ними помещения, комнаты и уязвимые места (окна, двери, люки, вентиляционные шахты и короба), расположенные на первом и последнем этажах по периметру здания объекта.

27. Система охранной сигнализации в установленном порядке проходит сертификацию в органах по сертификации, испытательных лабораториях (центрах), аккредитованных и зарегистрированных в Государственном реестре Государственной системы сертификации Республики Казахстан.

28. На объектах, где требуется исключительно высокая наработка на ложное срабатывание и вероятность обнаружения, необходимо использовать комбинированные системы, сочетающие в себе несколько датчиков различного физического принципа действия. Расположение чувствительных элементов выбирается таким образом, чтобы сигнал о проникновении человека возникал одновременно в нескольких датчиках, тогда как помехи были разнесены во времени.

29. Системой охранной сигнализации оборудуются три рубежа охраны.

Первым рубежом охраны защищаются:

1) строительные конструкции по периметру зданий или помещений объекта;

2) места ввода коммуникаций, вентиляционные каналы и другие;

3) выходы к пожарным лестницам;

4) некапитальные и капитальные (если необходима их защита) стены.

Вторым рубежом охраны защищаются объемы помещений.

Третьим рубежом охраны защищаются хранилища, сейфы, шкафы или подходы к ним.

30. Строительные конструкции по периметру здания (помещения) объекта блокируют:

1) дверные проемы, погрузочно-разгрузочные люки – на открывание и пролом;

2) остекленные конструкции – на «открывание» и «разрушение» стекла;

3) места ввода коммуникаций, некапитальные и капитальные (если это необходимо) – на «пролом»;

4) вентиляционные короба, дымоходы и другое – на «разрушение» и «ударное воздействие».

31. Структура системы охранной сигнализации для повышения безопасности объекта определяется, исходя из:

1) режима работы этого объекта;

2) особенностей расположения помещений внутри зданий;

3) количества охраняемых зон.

32. Охраняемые зоны размещают таким образом, чтобы при подходе к критическим зонам с любой стороны нарушение было зафиксировано не менее чем двумя рубежами охраны.

33. Тревожные извещения с каждого рубежа охраны выводятся на пульт централизованного наблюдения или пульт внутренней охраны объекта.

34. Помещение, где организован пульт централизованного наблюдения, необходимо размещать на вторых или третьих этажах здания. В случае размещения помещения пульта централизованного наблюдения в одноэтажном здании, строительные конструкции (стены, двери и окна) помещения должны соответствовать утвержденным нормам и правилам Республики Казахстан.

35. Пульты внутренней охраны располагаются в служебных помещениях подразделений охраны или специально оборудованных для этих целей помещениях.

Требования к системе контроля и управления доступом

36. Система контроля и управления доступом должна обеспечивать:

1) ограничение доступа сотрудников и посетителей объекта в охраняемые помещения через пункты контроля;

2) фиксацию времени прихода и ухода каждого сотрудника и посетителя объекта;

3) получение информации об открывании внутренних помещений;

4) открывание преграждающего устройства после считывания идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение) в заданный временной интервал или по команде оператора;

5) запрет открывания преграждающего устройства после считывания идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;

6) санкционированное изменение (добавление, удаление) идентификационных признаков в устройствах управления и обеспечение связи их с зонами доступа (помещениями) и временными интервалами доступа;

7) защиту от несанкционированного доступа к программным средствам устройства управления для изменения (добавления, удаления) идентификационных признаков;

8) защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и информации;

9) сохранение настроек и базы данных идентификационных признаков при отключении электропитания;

10) ручное, полуавтоматическое или автоматическое открывание преграждающих устройств для прохода при чрезвычайных ситуациях, пожаре,

технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

11) открывание или блокировку любых дверей, оборудованных системой доступа, с рабочего места оператора системы;

12) автоматическое закрытие преграждающего устройства при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;

13) закрывание преграждающего устройства на определенное время и выдачу сигнала тревоги при попытках подбора идентификационных признаков (кода);

14) регистрацию и протоколирование текущих и тревожных событий;

15) автономную работу считывателя с преграждающего устройства в каждой точке доступа при отказе связи с устройства управления.

37. Считыватели должны выполнять следующие функции:

1) считывание идентификационного признака с идентификаторов;

2) сравнение введенного идентификационного признака с хранящимся в памяти или базе данных устройства управления;

3) формирование сигнала на открывание преграждающего устройства при идентификации пользователя;

4) обмен информацией с устройством управления.

38. Устройства управления должны выполнять следующие функции:

1) прием информации от считывателей, ее обработку, отображение в заданном виде и выработку сигналов управления преграждающими устройствами;

2) введение баз данных работников объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и другие);

3) ведение электронного журнала регистрации прохода работников через точки доступа;

4) приоритетный вывод информации о тревожных ситуациях в точках доступа;

5) контроль исправности состояния преграждающих устройств, считывателей и линий связи.

39. Система контроля и управления доступом должна быть защищена от манипулирования путем перебора или подбора идентификационных признаков, а конструкция, внешний вид и надписи на составных частях не должны приводить к раскрытию применяемых кодов.

40. Оснащение объекта системой контроля и управления доступом производится в трех основных зонах доступа:

1) первая зона – здания, территории, помещения, доступ в которые персоналу и посетителям не ограничен;

2) вторая зона – помещения, доступ в которые разрешен ограниченному составу персонала, а также посетителям объекта по разовым пропускам или в сопровождении персонала объекта;

3) третья зона – специальные помещения объекта, доступ в которые имеют строго определенные сотрудники и руководители.

Пропуск лиц на объект через пункты контроля должен осуществляться:

1) в первой зоне доступа по одному признаку идентификации;

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

3) в третьей зоне доступа – по двум и более признакам идентификации.

41. Системой контроля и управления доступом необходимо оборудовать:

1) главный и служебные входы на объект;

2) наружную дверь для входа в здание;

3) двери в служебные помещения;

4) двери помещений подразделений охраны;

5) двери помещений пульта централизованного наблюдения;

6) другие помещения по усмотрению руководства.

Требования к телевизионной системе видеонаблюдения

42. Телевизионная система видеонаблюдения должна обеспечивать:

1) передачу визуальной информации о состоянии охраняемых зон, помещений, периметра и территории объекта на мониторы локального пункта наблюдения в специально выделенном помещении подразделения охраны либо пункта централизованной охраны в автоматизированном режиме;

2) архивирование видеоинформации для последующего анализа событий;

3) видеодокументирование событий в автоматическом режиме или по команде оператора;

4) воспроизведение ранее записанной информации;

5) оперативный доступ к видеозаписи путем задания времени, даты и идентификатора телекамеры.

43. На объекте телевизионной системой видеонаблюдения оборудуются:

1) периметр территории;

2) контрольно-пропускные пункты;

3) досмотровые помещения (комнаты), зоны досмотра транспорта;

4) главные и запасные входы;

5) территория и помещения с критическими зонами, коридоры к ним;

6) другие помещения по усмотрению руководителя (собственника) объекта.

44. Видеокамеры, предназначенные для контроля территории объекта или периметра, должны работать при условиях воздействия климатических факторов для наружных установок в соответствии с климатической зоной либо

размещаться в герметичных термокожухах, обеспечивающих работоспособность при воздействии климатических факторов.

45. В темное время суток, если освещенность охраняемой зоны ниже чувствительности телекамер, должно включаться охранное освещение видимого или инфракрасного диапазона света. Зоны охранного освещения должны совпадать с зоной обзора телекамер.

46. Не рекомендуется объединение телевизионной системы видеонаблюдения, системы контроля и управления доступом, а также систем обнаружения и тушения пожаров в автоматизированный охранный комплекс.

Требования к системе оперативной связи

47. Система оперативной связи должна обеспечивать:

1) работу в диапазонах частот, выделенных в установленном порядке для систем оперативной связи;

2) двустороннюю радиосвязь между дежурным на пункте охраны и нарядами охраны на территории обслуживания;

3) двустороннюю радиосвязь между нарядами охраны в пределах территории обслуживания;

4) емкость и зону обслуживания, достаточные для обеспечения установленной связи на охраняемых объектах и прилегающей территории;

5) защиту передаваемой информации;

6) возможность автоматического перехода базового оборудования, центра коммутации и диспетчерского центра системы на резервное электропитание при отключении основного (и наоборот). Время работы от резервного источника питания – не менее 2 часов.

48. Конструкция компонентов системы оперативной связи должна обеспечивать электробезопасность обслуживающего персонала при их эксплуатации, обслуживании и ремонте.

Требования к системе оповещения

49. Система оповещения должна осуществлять:

1) подачу звуковых и (или) световых сигналов в здания, помещения, на участки территории объекта с постоянным или временным пребыванием людей;

2) трансляцию речевой информации о характере опасности, необходимости и путях эвакуации, других действиях, направленных на обеспечение безопасности людей;

3) доведение сигналов оповещения согласно нормам Закона Республики Казахстан «О гражданской защите».

50. На объекте должен быть разработан план оповещения, который включает в себя:

1) схему вызова сотрудников, должностными обязанностями которых предусмотрено участие в мероприятиях по предотвращению или устранению последствий внештатных ситуаций;

2) инструкции, регламентирующие действия сотрудников при внештатных ситуациях;

3) планы эвакуации;

4) систему сигналов оповещения.

51. Эвакуация людей в ходе действия системы оповещения должна сопровождаться:

1) включением аварийного и охранного освещения;

2) передачей по системе оповещения специально разработанных текстов, направленных на предотвращение паники и других явлений, усложняющих процесс эвакуации (скопление людей в проходах, тамбурах, на лестничных клетках и в других местах);

3) автоматическим включением световых указателей направления и путей эвакуации;

4) автоматическим открыванием дверей дополнительных эвакуационных выходов (например, оборудованных электромагнитными замками).

52. Сигналы оповещения должны отличаться от сигналов другого назначения.

Количество оповещателей и их мощность должны обеспечивать необходимую слышимость во всех местах постоянного или временного пребывания людей.

53. На охраняемой территории следует применять рупорные громкоговорители. Они могут устанавливаться на опорах освещения, стенах зданий и других конструкциях.

Правильность расстановки и количество громкоговорителей на объекте определяются и уточняются на месте экспериментальным путем на разборчивость передаваемых речевых сообщений.

54. Коммуникации систем оповещения допускается проектировать совмещенными с радиотрансляционной сетью объекта.

Требования к охранному освещению

55. Сеть охранного освещения по периметру выполняется отдельно от сети наружного освещения и разделяется на самостоятельные участки.

56. Освещение основного и внутреннего вспомогательного ограждения (освещенностью не менее 100 люкс) должно иметь возможность включения от систем охраны периметра, с учетом локальных участков обнаружения.

57. В качестве приборов охранного освещения должны применяться прожекторы заливающего света, светильники с лампами накаливания или аналогичного типа.

Приборы освещения необходимо располагать таким образом, чтобы не ослеплять постовых охранников и контролеров контрольно-пропускного пункта.

В полосу освещения не должны попадать посты охраны, тропа нарядов, постовые грибки.

Расстояние между светильниками, их мощность и конструкция должны выбираться из расчета создания сплошной, равномерной полосы света, необходимой по нормам освещенности.

58. Определение норм освещенности для служебных помещений охраны должно производиться на основании действующих норм и правил.

59. Охранное освещение обеспечивается:

1) необходимой равномерной освещенностью с расчетом, чтобы светоточки от светильников перекрывались и образовывали сплошную полосу шириной не менее 3-х метров;

2) возможностью автоматического включения освещения на одном участке или по всему периметру при срабатывании технических средств;

3) возможностью управления освещением – включение освещения любого участка или всего периметра.

60. Светильники охранного освещения устанавливаются в непосредственной близости к линии ограждения внутри территории, в местах, удобных и безопасных для обслуживания.

61. Помещения караулов, контрольно-пропускных пунктов, входы в здания, коридоры категорированных помещений должны дополнительно оборудоваться аварийным освещением. Переход рабочего освещения на аварийное и обратно должен осуществляться автоматически.

62. Освещение автотранспортных и железнодорожных контрольно-пропускных пунктов должно обеспечивать досмотр транспорта и провозимых грузов. Осветительные приборы должны располагаться таким образом, чтобы осуществлялось равномерное освещение досматриваемого транспорта, в том числе и снизу. В необходимых случаях следует предусмотреть возможность использования переносного освещения.

Требования к электропитанию систем охранной сигнализации, контроля и управления доступом, телевизионной системы видеонаблюдения и освещения

63. Системы охранной сигнализации, контроля и управления доступом должны содержать источники бесперебойного питания с аккумуляторной поддержкой, обеспечивающие работу оборудования не менее 12-ти часов при отсутствии основного сетевого питания.

64. Автономные резервные источники электрического питания должны обеспечивать работу системы контроля и управления доступом, телевизионной системы видеонаблюдения, охранного и дежурного освещения:

1) в городах и поселках городского типа – не менее 24-х часов;
2) в сельских районах – не менее 48-ми часов;
3) в труднодоступных районах – не менее 72-х часов.

3. Требования к системе антитеррористической защиты объектов массового скопления людей

65. Объекты массового скопления людей, включенные в приложение 1, в обязательном порядке оснащаются телевизионной системой видеонаблюдения.

66. Объекты массового скопления людей, включенные в приложение 2, в обязательном порядке оснащаются системой и средствами охранной сигнализации, системой контроля и управления доступом (за исключением первой зоны), системой и средствами оповещения, телевизионной системой видеонаблюдения.

67. На всех объектах массового скопления людей устанавливаются системы и технические средства, прошедшие в установленном порядке сертификацию в органах по сертификации, испытательных лабораториях (центрах), аккредитованных и зарегистрированных в Государственном реестре Государственной системы сертификации Республики Казахстан.

Требования к системе охранной сигнализации

68. Системы охранной сигнализации должны извещать о несанкционированном проникновении.

69. Системы охранной сигнализации не должны выдавать ложных тревог при переключениях источников электропитания с основного на резервный и обратно.

70. Системы охранной сигнализации защищаются от несанкционированного доступа к их управлению.

Требования к системе контроля и управления доступом

71. Система контроля и управления доступом должна обеспечивать организацию пропускного и внутриобъектового режима на объектах и предусматривать разделение объекта на три основные зоны доступа:

1) первая зона – здания, территории, помещения, доступ в которые персоналу и посетителям не ограничен;

2) вторая зона – помещения, доступ в которые разрешен ограниченному составу персонала, а также посетителям объекта по разовым пропускам или в сопровождении персонала объекта;

3) третья зона – специальные помещения объекта, доступ в которые имеют строго определенные сотрудники и руководители.

72. Система контроля и управления доступом обеспечивает предотвращение несанкционированного входа в помещения ограниченного доступа второй и третьей зон.

73. Система контроля и управления доступом должна быть защищена от манипулирования путем перебора или подбора идентификационных признаков, а конструкция, внешний вид и надписи на ее составных частях не должны приводить к раскрытию применяемых кодов.

Требования к телевизионной системе видеонаблюдения

74. Телевизионная система видеонаблюдения должна обеспечивать передачу визуальной информации на техническое средство или совокупность технических средств сбора, обработки, отображения и регистрации полученной информации, установленные в специально выделенном помещении для подразделения охраны (при наличии) либо на пункт централизованной охраны.

Срок хранения информации должен составлять не менее 30-ти суток.

75. Телевизионная система видеонаблюдения позволяет вести наблюдение за обстановкой в охраняемых зонах (территории, помещениях), а также визуально подтверждать факт несанкционированного проникновения для оценки ситуации и идентификации нарушителей.

76. Телевизионная система видеонаблюдения обеспечивает работу в автоматизированном режиме.

77. На объекте, занимающем отдельное здание (комплекс зданий), телевизионной системой видеонаблюдения оборудуются:

1) периметр территории, прилегающий к объекту;
2) контрольно-пропускные пункты (при наличии);
3) досмотровые помещения (комнаты) и зоны досмотра транспорта (при наличии);
4) главный и запасные входы;
5) помещения (места) массового скопления людей.

На объекте, занимающем часть здания, телевизионной системой видеонаблюдения необходимо оборудовать:

1) помещения (места) массового скопления людей;
2) главный и запасные входы (при наличии).

78. В темное время суток, если освещенность охраняемой зоны ниже чувствительности телекамер, должно включаться охранное освещение видимого или инфракрасного диапазона света. Зоны охранного освещения должны совпадать с зоной обзора телекамер.

Требования к системе оповещения

79. Система оповещения на объекте и его территории создается для оперативного информирования персонала и посетителей при чрезвычайных

происшествиях (аварии, пожаре, стихийном бедствии, нападении, террористическом акте) и действий в сложившейся обстановке.

80. На объекте должен быть разработан план оповещения, который включает в себя:

1) схему вызова сотрудников, должностными обязанностями которых предусмотрено участие в мероприятиях по предотвращению или устранению последствий внештатных ситуаций;

2) инструкции, регламентирующие действия сотрудников при внештатных ситуациях;

3) планы эвакуации;

4) систему сигналов оповещения.

81. Система оповещения должна обеспечивать выполнение следующих требований (характеристик):

1) подачу звуковых и (или) световых сигналов в здания, помещения, на участки территории объекта с постоянным или временным пребыванием людей;

2) трансляцию речевой информации о характере опасности, необходимости и путях эвакуации, других действиях, направленных на обеспечение безопасности людей;

3) доведение сигналов оповещения согласно нормам Закона Республики Казахстан «О гражданской защите».

82. Эвакуация людей по сигналам оповещения должна сопровождаться:

1) включением аварийного и охранного освещения;

2) передачей специально разработанных текстов, направленных на предотвращение паники и других явлений, усложняющих процесс эвакуации (скопление людей в проходах, тамбурах, на лестничных клетках и в других местах);

3) включением световых указателей направления и путей эвакуации;

4) дистанционным открыванием дверей дополнительных эвакуационных выходов (например, оборудованных электромагнитными замками).

83. Коммуникации систем оповещения в отдельных случаях допускается проектировать совмещенными с радиотрансляционной сетью объекта.