

РЕКОМЕНДАЦИИ

по оснащению объектов водоснабжения и водоотведения инженерно-техническими средствами охраны

1. Для целей реализации требований к антитеррористической защищенности объектов водоснабжения и водоотведения, утвержденных постановлением Правительства Российской Федерации от 23 декабря 2016 г. № 1467 (Собрание законодательства Российской Федерации, 2017, № 2, ст. 335), объекты водоснабжения и водоотведения (далее – объекты) рекомендуется оснащать инженерными средствами защиты, техническими средствами охраны и вспомогательными системами (далее - инженерно-технические средства охраны) в соответствии с категориями, присвоенными данным объектам в порядке, установленном вышеуказанными требованиями.

2. Перечень рекомендуемых инженерно-технических средств охраны для объектов различных категорий приведен в следующей таблице:

Вид инженерно-технического средства	1 категория	2 категория	3 категория	4 категория
1) основное ограждение внешнего периметра объекта	+(3м)	+(2,5м)	+(2,5м)	+(2м)
2) дополнительное ограждение внешнего периметра объекта:				
- верхнее	+	+	+	+/-
- нижнее	+	+/-	-	-
3) предупредительное ограждение внешнего периметра объекта:				
- внешнее	+	-	-	-
- внутреннее	+	+/-	-	-
4) средства ограничения скорости движения и (или)	+	+	+/-	-

принудительной остановки транспортных средств при въезде на объект				
5) средства защиты и (или) контроля пересекающих периметр объекта наземных и подземных коммуникаций	+	+	+/-	-
6) контрольно-пропускные пункты: - на объект - в места размещения критических элементов	+ +	+ +/-	+ -	+/- -
7) пункты управления безопасностью объекта	+	+	+	+/-
8) помещения для размещения подразделений охраны объекта	+	+	+	+/-
9) система тревожно-вызывной сигнализации с выводом сигнала тревоги в: - дежурную часть территориального органа Росгвардии (его отделов, отделений, районных и других подразделений) - дежурное подразделение с круглосуточным режимом работы частной охранной организации или ведомственной охраны	+ -	+ -	- +	- +/-
10) система охранной				

сигнализации: - по внешнему периметру объекта: а) два рубежа охраны (различных видов) б) один рубеж охраны - по периметру и (или) внутри мест размещения критических элементов - по периметру и (или) внутри пунктов управления безопасностью - по периметру и (или) внутри контрольно- пропускных пунктов	+	-	-	-
	-	+	+/-	-
	+	+	+	+
	+	+/-	-	-
	+	+	+	+/-
11) система охранная телевизионная: - по внешнему периметру объекта - по периметру и (или) внутри мест размещения критических элементов - по периметру и (или) внутри пунктов управления безопасностью - по периметру и (или) внутри контрольно- пропускных пунктов	+	+	+/-	-
	+	+	+	+
	+	+/-	-	-
	+	+	+	+/-
12) система охранного освещения: - по периметру и на территории объекта - по периметру и (или) внутри мест размещения критических элементов	+	+	+/-	-
	+	+	+	+

- по периметру и (или) внутри пунктов управления безопасностью	+	+	+	+/-
- по периметру и (или) внутри контрольно-пропускных пунктов	+	+	+	+/-
13) технические средства досмотра на контрольно-пропускных пунктах на объект:				
- стационарные	+	+/-	-	-
- мобильные	+	+	+/-	-
14) система контроля и управления доступом на контрольно-пропускных пунктах:				
- на объект	+	+	+/-	-
- в места размещения критических элементов	+	+/-	-	-
15) система оперативной связи:				
- стационарные и мобильные средства связи и обмена информацией общего пользования	+	+	+	+
- стационарные и мобильные средства внутриобъектовой связи	+	+/-	-	-
16) система оповещения:				
- речевая	+	+/-	-	-
- звуковая	+	+	+/-	-
17) система бесперебойного энергоснабжения инженерно-технических средств охраны	+	+	+	+/-

Примечания к таблице:

а. Знак «+» означает, что соответствующие инженерно-технические средства охраны на объекте рекомендуются к применению (при наличии технической возможности).

б. Знак «+/-» означает, что решение о целесообразности применения (при наличии технической возможности) соответствующих инженерно-технических средств охраны на объекте рекомендуется принимать комиссией по его обследованию и категорированию.

в. Знак «-» означает, что решение о целесообразности применения (при наличии технической возможности) соответствующих инженерно-технических средств охраны на объекте рекомендуется принимать руководству эксплуатирующей организации.

3. Таблица, содержащаяся в пункте 1 настоящих рекомендаций, содержит общий перечень рекомендуемых инженерно-технических средств охраны объектов в зависимости от их категории. При этом следует отметить, что объекты одной категории могут значительно различаться по своему функциональному назначению, архитектурно-планировочным решениям, характеристикам строительных конструкций, площади, периметру, месту расположения, уязвимости и другим параметрам, что рекомендуется учитывать при формировании системы инженерно-технических мер их антитеррористической защищенности.

Окончательно состав комплекса инженерно-технических средства охраны каждого конкретного объекта рекомендуется определять:

на стадии его проектирования – заказчиком (в техническом задании на проектирование объекта капитального строительства или в отдельном техническом задании на проектирование комплекса инженерно-технических средств охраны объекта, определяющем перечень, а также количественные и качественные характеристики (при необходимости – тип и тактико-технические данные) инженерно-технических средств охраны, которыми будет оснащен объект);

на стадии его функционирования – руководством организации, осуществляющей эксплуатацию объекта в соответствии с Федеральным законом от 7 декабря 2011 г. № 416-ФЗ «О водоснабжении, и водоотведении» (Собрание законодательства Российской Федерации, 2011, № 50, ст. 7358; 2012, № 53, ст. 7614, 7616, 7643; 2013, № 19, ст. 2330; № 30, ст. 4077; № 52, ст. 6976, 6982; 2014, № 26, ст. 3366, ст. 3406; № 30, ст. 4218; № 42, ст. 5615; 2015, № 1, ст. 11, ст. 38; № 29, ст. 4347; №45, ст. 6208; №48, ст. 6723; 2016, №1, ст. 24; № 27, ст. 4288; № 52, ст. 7507), с учетом предписаний, указанных в акте обследования и категорирования объекта и (или) в акте контроля за обеспечением антитеррористической защищенности объекта (в техническом задании на проектирование комплекса инженерно-технических средства охраны объекта, определяющем перечень, а также количественные и качественные характеристики (при необходимости – тип и тактико-технические данные) инженерно-технических средств охраны, которыми будет оснащен объект).

4. Функциональное назначение, способы использования (применения), типы и примерные тактико-технические характеристики рекомендуемых инженерно-технических средств охраны описаны в разделах I, II и III настоящих рекомендаций.

I. Инженерные средства защиты

Инженерные средства защиты рекомендуется применять в целях:

- защиты объекта и мест размещения его основных элементов от несанкционированного проникновения нарушителя;
- создания препятствий на пути движения нарушителя с целью затруднения (задержки) его проникновения на объект и продвижения к критическим элементам объекта на время, достаточное для его своевременной нейтрализации;
- защиты сотрудников подразделения охраны объекта от физического воздействия (нападения) и иных действий нарушителя при исполнении ими должностных обязанностей по обеспечению антитеррористической защищенности объекта;
- защиты работников и посетителей объекта, а также комплексов оборудования, зданий и сооружений объекта от действий нарушителя;
- предотвращения силового прорыва транспортных средств на объект;
- обеспечения контролируемого доступа работников, посетителей и транспортных средств на объект через установленные места пропуска;
- обеспечения благоприятных условий сотрудникам подразделения охраны объекта для выполнения возложенных на них задач.

В состав инженерных средств защиты рекомендуется включать:

5. Основное, дополнительное и предупредительное ограждение внешнего периметра и мест размещения критических элементов объекта.

5.1. При оборудовании основного ограждения внешнего периметра объекта рекомендуется обеспечить:

- препятствование несанкционированному проникновению нарушителей путем перелеза или подлаза (подкопа), взлома (разрушения), в том числе путем нанесения таранного удара автотранспортным средством;
- его высокую прочность и долговечность;
- его замкнутый характер;
- отсутствие у него конструктивных повреждений, позволяющих осуществить несанкционированное проникновение на ограждаемую территорию;
- отсутствие у него незапираемых ворот, дверей, калиток, а также конструкций, облегчающих его преодоление.

Основное ограждение внешнего периметра рекомендуется выполнять в виде стационарного капитального сооружения высотой 2 – 3 метра, состоящего из:

- железобетонных секций (толщиной не менее 100 миллиметров);
- каменной или кирпичной кладки (толщиной не менее 250 миллиметров);
- сплошных стальных секций (толщиной листа не менее 2 миллиметров, усиленных ребрами жесткости, или из аналогичного по прочности материала);
- имеющих антикоррозионную защиту усиленных ребрами жесткости секций сваренной в перекрестиях стальной сетки или решетки (с прутками диаметром не менее 5 миллиметров, размер двух параллельных земле сторон одной ячейки не должен превышать 50 миллиметров, а перпендикулярной – 300 миллиметров).

Для усиления просматриваемых ограждений рекомендуется устанавливать их на фундамент в виде сплошного железобетонного цоколя высотой до 300 миллиметров и толщиной 200 миллиметров и более.

Основное ограждение внешнего периметра объекта рекомендуется выполнять в виде прямолинейных участков, с минимальным количеством изгибов и поворотов, ограничивающих наблюдение и затрудняющих применение технических средств охраны. Не рекомендуется выполнять данное ограждение (при наличии возможности) примыкающим к каким-либо зданиям и сооружениям (кроме контрольно-пропускного пункта, и иных зданий и сооружений, запроектированных в составе периметра объекта), площадкам для складирования оборудования и материалов, а также лесонасаждениям, высота которых превышает расстояние от них до ограждения.

При отсутствии технической возможности размещения на отдельных опорах, на основном ограждении рекомендуется размещать:

- систему охранной сигнализации;
- систему охранную телевизионную;
- систему охранного освещения;
- систему оперативной связи;
- систему оповещения;
- систему тревожно-вызывной сигнализации.

5.2 Дополнительное ограждение рекомендуется устанавливать для усиления основного ограждения.

Верхнее (противоперелазное) дополнительное ограждение рекомендуется выполнять высотой не менее 500 миллиметров и устанавливать на основное ограждение внешнего периметра объекта, въездные ворота, крыши одноэтажных зданий и сооружений, являющихся частью основного ограждения внешнего периметра объекта, а также в местах примыкания с внешней стороны к периметру объекта принадлежащих сторонним организациям зданий и сооружений (если высота последних равна или больше высоты сооружений внешнего периметра объекта в данном месте рекомендуется применять дополнительное ограждение высотой не менее 1 метра и технические средства охраны раннего обнаружения).

Верхнее дополнительное ограждение рекомендуется выполнять в виде противоперелазного козырька (выполненного из сварного сеточного или решетчатого полотна либо 4 и более рядов колючей проволоки), спирали из колючей проволоки (ленты) или иного аналогичного устройства.

Нижнее (противоподкопное) дополнительное ограждение рекомендуется устанавливать под основным ограждением внешнего периметра объекта с заглублением в грунт не менее 500 миллиметров.

Нижнее дополнительное ограждение рекомендуется выполнять в виде бетонированного цоколя толщиной не менее 200 миллиметров или сварной решетки из прутков арматурной стали диаметром не менее 16 миллиметров, с ячейками размерами не более 150×150 миллиметров, сваренной в перекрестиях (или иным аналогичным по надежности способом).

Также (при необходимости) рекомендуются к применению временные дополнительные ограждения в виде переносных ограждений и барьеров, проволочных ежей, рогаток, спиралей из колючей проволоки (ленты), проволочных гирлянд, малозаметных препятствий и других аналогичных устройств.

5.3 Предупредительное ограждение рекомендуется устанавливать для обозначения границ охраняемой территории (периметра) и предотвращения бесконтрольного или случайного прохода лиц и проезда транспорта в места размещения критических элементов объекта и иные зоны объекта, проход (проезд) на территорию которых ограничен и контролируется.

Рекомендуется выполнять предупредительное ограждение просматриваемым (из металлической сварной или витой сетки, или решетки, гладкой, колючей проволоки или иного аналогичного материала) и устанавливать его рядом с основным ограждением (с внутренней или внешней стороны) либо по периметру мест размещения критических элементов объекта или досмотровых площадок автомобильного и железнодорожного транспорта.

Предупредительное ограждение рекомендуется выполнять высотой не менее 1,5 метров. При необходимости на нем могут быть размещены предупредительные, разграничительные и запрещающие знаки.

5.4 Между основным ограждением внешнего периметра и внутренним предупредительным ограждением рекомендуется (при необходимости) оборудовать запретную зону, представляющую собой специально выделенную полосу местности, предназначенную для выполнения сотрудниками подразделения охраны объекта служебных задач по обеспечению антитеррористической защищенности объекта и размещения технических средств охраны.

В запретной зоне не рекомендуется размещать какие-либо строения и предметы, затрудняющие применение технических средств охраны и действия подразделения охраны объекта. К границе запретной зоны не рекомендуется примыкать зданиям, сооружениям, площадям для складирования, а также лесонасаждениям.

При использовании запретной зоны для охраны объекта при помощи служебных собак рекомендуется выполнять предупредительное ограждение высотой не менее 2,5 метра, либо подвижность собаки рекомендуется ограничить тросом.

Рекомендуемая ширина запретной зоны - не менее 3 метров, а при размещении в ней технических средств охраны - превышающая ширину их зоны обнаружения.

5.5 Ограждения рекомендуется выполнять с не летальным травмирующим эффектом (характером воздействия) для нарушителя.

6. Стены, перекрытия и перегородки зданий, сооружений и отдельных помещений.

Стены зданий и сооружений, перекрытия пола и потолка, а также перегородки отдельных помещений рекомендуется выполнять в виде капитальных конструкций, представляющих собой труднопреодолимые препятствия для несанкционированного проникновения нарушителей путем их взлома и разрушения.

Стены зданий и сооружений, являющихся частью внешнего периметра объекта или местами размещения его критических элементов, рекомендуется выполнять в виде стационарных капитальных сооружений (из кирпичной кладки толщиной не менее 380 миллиметров, железобетонных панелей толщиной не менее 160 миллиметров или из иного аналогичного по прочности материала) устойчивыми

к пролому путем нанесения таранного удара автотранспортным средством. В этих целях на тараноопасных направлениях (при необходимости) рекомендуется усиливать стены зданий и сооружений путем размещения перед ними бетонных блоков со сторонами не менее 1000×500×500 миллиметров или иным аналогичным по надежности способом.

Меньшие по прочностным характеристикам стены вышеуказанных зданий, сооружений и отдельных помещений рекомендуется усиливать стальными решетками по всей площади с внутренней стороны помещения (толщина прутьев решеток зависит от требуемой надежности конструкции). После установки данные решетки рекомендуется маскировать штукатуркой или облицовочными панелями.

Стены находящихся внутри периметра объекта зданий, сооружений и отдельных помещений, в которых размещаются критические элементы объекта, не рекомендуется выполнять из материалов, имеющих меньшие, чем указано выше прочностные характеристики, при отсутствии надежного обеспечения их антитеррористической защищенности путем реализации других дополнительных мер.

7. Средства запираания, защиты и усиления въездных ворот, дверей, окон, а также дверных и оконных проемов зданий, сооружений и отдельных помещений.

7.1 Въездные ворота, устанавливаемые на автомобильных и железнодорожных въездах на территорию объекта в целях создания труднопреодолимого препятствия для несанкционированного проникновения нарушителей путем перелазы или подлаза (подкопа), взлома (разрушения), рекомендуется выполнять в виде стационарных капитальных конструкций высотой 2 – 2,5 метра (из стального листа толщиной не менее 2 миллиметров, усиленных ребрами жесткости, из дерева со сплошным заполнением доской толщиной не менее 40 миллиметров, обшитым с двух сторон стальным листом толщиной не менее 0,6 миллиметров или аналогичных по прочности конструкций) с предусмотренной конструкцией жесткой фиксации в закрытом положении. Рекомендованное расстояние между дорожным покрытием и нижним краем въездных ворот в высоту - не более 100 миллиметров.

В целях предотвращения разрушения автомобильных въездных ворот путем нанесения таранного удара автотранспортным средством перед ними рекомендуется устанавливать средства ограничения скорости движения и (или) принудительной остановки транспортных средств (в виде расположенных в шахматном порядке на определенном расстоянии друг от друга бетонных блоков со сторонами не менее 1000×500×500 миллиметров, автоматических или механических понимающихся стальных барьеров, противотаранных шлагбаумов либо аналогичных устройств).

Ворота с электроприводом и дистанционным управлением рекомендуется оборудовать устройствами аварийной остановки и открытия вручную на случай неисправности или отключения электропитания, а также ограничителями или стопорами для предотвращения произвольного открывания (движения).

Во внешнем периметре объекта помимо основных въездных ворот при наличии технической возможности рекомендуется устанавливать запасные и (или) аварийные въездные ворота. В качестве запирающих устройств основных въездных ворот рекомендуется устанавливать замки гаражного типа либо навесные

замки или аналогичные по надежности запирающие устройства. Редко открываемые запасные или аварийные ворота со стороны охраняемой территории рекомендуется запиравать на засовы и навесные замки или аналогичные по надежности запирающие устройства.

При выполнении калиток в основном ограждении, выходящих на внешнюю сторону периметра объекта, рекомендуется применять конструкции, аналогичные по прочности въездным воротам, и оборудовать их двумя врезными (накладными) замками, установленными на расстоянии не менее 300 миллиметров друг от друга или одним врезным (накладным) и одним навесным замками либо аналогичными по надежности запирающими устройствами.

Рекомендуется обеспечить устойчивость к разрушающим воздействиям запирающих и блокирующих устройств въездных ворот и калиток при закрытом состоянии, а также сохранение их работоспособности при повышенной влажности в широком диапазоне температур окружающего воздуха (в соответствии с климатической зоной использования), прямом воздействии воды, снега, града, песка и других факторов окружающей среды.

7.2 Рекомендуется устанавливать исправные двери (подогнанные под дверную коробку) и запирающие их устройства в зданиях, сооружениях и отдельных помещениях объекта, представляющие собой труднопреодолимое препятствие для несанкционированного проникновения через них нарушителей на объект и в его отдельные помещения путем их взлома (разрушения), а также вскрытия запирающих устройств.

Двери зданий и сооружений, выходящие на внешнюю сторону периметра объекта, а также двери мест размещения критических элементов объекта, контрольно-пропускных пунктов, помещений для размещения подразделения охраны, пунктов управления безопасностью рекомендуется выполнять в защищенном варианте (в виде металлических дверных конструкций с полотном из стального листа толщиной не менее 2 миллиметров, усиленного ребрами жесткости, деревянных дверных конструкций, со сплошным заполнением доской толщиной не менее 40 миллиметров, обшитых с двух сторон стальным листом толщиной не менее 0,6 миллиметра, либо аналогичными по надежности) со стальной или усиленной стальными листами дверной коробкой (либо изготовленной из других материалов, обеспечивающих необходимую надежность) и, по возможности, открываться наружу.

Вышеуказанные двери рекомендуется оборудовать не менее чем двумя врезными (накладными) замками, установленными на расстоянии не менее 300 миллиметров друг от друга или одним врезным (накладным) и одним навесным замками либо аналогичными по надежности запирающими устройствами. Двухстворчатые двери также рекомендуется оборудовать двумя стопорными задвижками (шпингалетами), устанавливаемыми в верхней и нижней части одного дверного полотна.

Входы (выходы) в здания и сооружения объекта с внешней стороны периметра (при отсутствии возле них постоянных постов подразделения охраны) рекомендуется оборудовать тамбуром с дополнительной внутренней дверью, аналогичной по надежности с основной дверью, или оснастить системой охранной

сигнализации, выдающей соответствующий сигнал подразделению охраны объекта при попытке подбора ключей или взлома, а также системой охранной телевизионной.

Дверные проемы входов (выходов) в здания, сооружения и отдельные помещения, в которых размещаются критические элементы объекта, также рекомендуется оборудовать дополнительной внутренней запирающейся стальной решетчатой дверью.

Двери (люки) и запирающие их устройства, а также, дверные коробки чердаков и подвалов зданий и сооружений, являющихся частью внешнего периметра объекта или местами размещения его критических элементов, по прочности конструкций рекомендуется устанавливать в соответствии с вышеуказанными требованиями.

7.3 Рекомендуется устанавливать в зданиях, сооружениях и отдельных помещениях объекта, исправные окна, подогнанные под оконные проемы, остекленные (стекла должны быть жестко закреплены в пазах) и оборудованные исправными и надежными запирающими устройствами.

Выходящие на внешнюю сторону объекта окна первых этажей зданий, являющихся частью внешнего периметра объекта, а также мест размещения критических элементов объекта, контрольно-пропускных пунктов, помещений для размещения подразделения охраны, пунктов управления безопасностью и иные уязвимые окна, независимо от этажности зданий и их размещения, рекомендуется выполнять в защищенном варианте (с усиленной рамой и оконными конструкциями, с защитным остеклением или композицией из обычного стекла и полимерных пленок, оснащенные противовзломной фурнитурой, либо в стандартной комплектации с применением защитных решеток либо ставней (рольставней), жалюзи и аналогичных конструкций, находящихся закрытом состоянии в ночное и нерабочее время либо при длительном отсутствии в соответствующем помещении работников или сотрудников подразделения охраны объекта) и быть труднопреодолимыми для несанкционированного проникновения через них нарушителей на объект и в его отдельные помещения путем их взлома (разрушения), а также вскрытия запирающих устройств.

8. Средства защиты пересекающих внешний периметр объекта наземных и подземных коммуникаций.

8.1 Не относящиеся к основному технологическому оборудованию объекта водопропуски сточных или проточных вод, подземные коллекторы (кабельные, канализационные и т.п.) при диаметре труб или коллектора 300 миллиметров и более, выходящие с территории объекта, на выходе рекомендуется оборудовать не препятствующими течению воды металлическими решетками из прутков арматурной стали диаметром не менее 16 миллиметров, образующих ячейки размером не более чем 150×150 миллиметров, сваренных в перекрестиях (или иным аналогичным по надежности способом), и (или) средствами охранной сигнализации на случай попытки несанкционированного проникновения.

Для очистки от сплавляемого по указанным трубам и коллекторам мусора данные инженерные средства защиты рекомендуется оборудовать подъемными и иными аналогичными устройствами.

В трубе или коллекторе диаметром более 500 миллиметров, где есть возможность применения инструмента взлома, рекомендуется устанавливать решетки, заблокированные системой охранной сигнализации.

Инженерно-техническое оснащение коллекторов основного технологического оборудования объекта рекомендуется осуществлять способами, исключающими создание препятствий (затруднений) в его работе, с учетом наличия объективно подтвержденных угроз использования нарушителями данных коммуникаций для проникновения на объект.

Устройства паводкового водосброса в местах пересечения периметра объекта реками, ручьями, оврагами и т.п. элементами местности рекомендуется оборудовать стальными решетками, спиралями из колючей проволоки (ленты), проволочными гирляндами или аналогичными устройствами над и под водой.

8.2 Воздушные трубопроводы, кабельные линии и т.п., в местах пересечения периметра объекта рекомендуется оборудовать сверху (при необходимости – вокруг) дополнительным ограждением (козырьком из колючей проволоки, спиралью из колючей проволоки (ленты) или иным аналогичным устройством).

8.3 Вентиляционные шахты, коробка, дымоходы и другие технологические каналы и отверстия диаметром 200 миллиметров и более, имеющие выход на улицу, крышу или в смежные не относящиеся к охраняемому объекту помещения, рекомендуется оборудовать на выходе с территории объекта стальными решетками, располагающимися от внутренней поверхности стены (перекрытия) не более чем на 100 миллиметров со стороны охраняемого помещения (при необходимости данные решетки надлежит заблокировать средствами охранной сигнализации)

9. Контрольно-пропускные пункты.

Для осуществления пропускного режима (контролируемого входа (выхода) на объект работников и посетителей, въезда (выезда) транспортных средств, а также досмотра лиц, транспорта и перемещаемых ими материальных ценностей) предотвращения несанкционированного проникновения на объект (с объекта) людей и транспортных средств, а также для обеспечения условий для выполнения вышеуказанных задач сотрудниками подразделения охраны объекта рекомендуется оборудовать объекты контрольно-пропускными пунктами, обеспечивающими необходимую пропускную способность для прохода людей и проезда транспорта.

Контрольно-пропускные пункты для прохода людей (проходные при наличии технической возможности не рекомендуется совмещать с контрольно-пропускными пунктами для транспорта, с помещением для размещения подразделения охраны объекта и (или) с пунктом управления безопасностью).

Контрольно-пропускные пункты рекомендуется оборудовать:

проходными;

помещениями для хранения и оформления пропусков (бюро пропусков);

камерами хранения личных вещей работников и посетителей объекта;

комнатами досмотра людей и досмотровыми площадками для транспортных средств;

помещениями для несения службы сотрудниками подразделения охраны а также размещения технических средств охраны.

Въездные ворота, двери и окна зданий контрольно-пропускных пунктов рекомендуется оборудовать средствами охранной сигнализации, которые выдают извещение о тревоге при попытке их вскрытия и разрушения.

Въездные ворота на территорию объекта и входные двери контрольно-пропускных пунктов рекомендуется оборудовать смотровым окошком (глазком) или переговорным устройством с находящимися с внешней стороны людьми, охранным освещением, а также телевизионной камерой системы охранной телевизионной для наблюдения за подступами к этим воротам и дверям (рекомендуется обеспечивать подсветку зон наблюдения и устанавливать камеры с необходимым разрешением которые настроены таким образом, чтобы в любое время суток отчетливо фиксировать лица входящих на объект людей и государственные регистрационные номера въезжающих транспортных средств)

Проходные рекомендуется оборудовать огороженным коридором для прохода людей с установленной в них системой контроля и управления доступом или местом несения службы сотрудника подразделения охраны осуществляющего пропускной режим.

На рабочих местах операторов технических средств охраны и (или) контролеров (постовых) на контрольно-пропускных пунктах рекомендуется обеспечить хороший обзор, и оборудовать инженерные средства защиты от нападения, а также устройства тревожно-вызывной сигнализации.

Контрольно-пропускные пункты также рекомендуется оборудовать стационарными и мобильными техническими средствами досмотра лиц и транспортных средств, стационарными и мобильными средствами оперативной связи, системами оповещения, а также охранного освещения.

Устройства управления механизмами открывания прохода (проезда) на территорию объекта, тревожно-вызывной сигнализацией, охранным освещением оповещением и стационарными техническими средствами досмотра лиц и транспортных средств при отсутствии иной технической возможности рекомендуется размещать на наружной стене контрольно-пропускных пунктов со стороны внутренней территории объекта в находящихся под постоянным контролем сотрудников подразделения охраны объекта местах, исключая доступ к ним посторонних лиц.

При наличии технической возможности рекомендуется оборудовать контрольно-пропускные пункты при входе (выходе) в места размещения критических элементов объекта, а также в отдельные здания, сооружения и помещения.

10. Помещения для размещения подразделения охраны объекта.

Для обеспечения благоприятных условий сотрудникам подразделения охраны объекта при выполнении возложенных на них задач рекомендуется организовать отдельное помещение для размещения подразделения охраны в расположенном на территории объекта здании, в составе которого оборудуются:

караульное помещение (для несения службы и отдыха не находящихся в постах сотрудников подразделения охраны объекта);

комната начальника караула (руководителя подразделения охраны, заступившего на смену для несения службы – при численности смены более 3 человек);

комната для хранения оружия, боеприпасов и специальных средств подразделения охраны (при их использовании).

Все двери и окна помещения для размещения подразделения охраны рекомендуется оборудовать аналогично дверям и окнам контрольно-пропускных пунктов.

Помещение для размещения подразделения охраны также рекомендуется оборудовать стационарными и мобильными средствами оперативной связи, системами оповещения, охранного освещения, тревожно-вызывной сигнализацией.

11. Пункт управления безопасностью объекта.

Для обеспечения оперативности в работе подразделения охраны объекта при выполнении возложенных на них задач управление их действиями по обеспечению антитеррористической защищенности объекта, а также работой инженерно-технических средств охраны рекомендуется осуществлять из пункта управления безопасностью объекта, размещаемого в отдельном помещении расположенного на территории объекта здания.

Все двери и окна пункта управления безопасностью рекомендуется оборудовать аналогично дверям и окнам контрольно-пропускного пункта.

Пункт управления безопасностью также рекомендуется оборудовать стационарными и мобильными средствами оперативной связи, системами оповещения, охранного освещения, тревожно-вызывной сигнализацией.

На рабочее место оператора технических средств охраны на пункте управления безопасностью рекомендуется вывести контроль и управление (пультами централизованного наблюдения) системами охранной и тревожно-вызывной сигнализации, системой охранной телевизионной, а также системами оперативной связи, охранного освещения, оповещения и энергоснабжения технических средств охраны.

II. Технические средства охраны

12. Система охранной сигнализации.

В целях обнаружения нарушителя при попытке несанкционированного проникновения на объект, в места размещения его критических элементов и иные охраняемые здания, сооружения и отдельные помещения, а также обнаружения его действий на территории объекта и передачи соответствующего сигнала сотрудникам подразделения охраны объекта и (или) уполномоченным государственным органам, объект рекомендуется оборудовать системой охранной сигнализации, состоящей из:

а) периметральных извещателей для обнаружения проникновения нарушителей на открытых площадках (рекомендуется устанавливать для контроля ограждения внешнего периметра объекта, мест размещения критических элементов объекта, въездных ворот и т.п.);

б) внутренних извещателей для обнаружения проникновения нарушителей в здания, сооружения и отдельные помещения (рекомендуется устанавливать для

контроля дверей, окон люков, коллекторов, вентиляционных шахт и т.п., мест размещения критических элементов объекта, контрольно-пропускных пунктов, помещений для размещения подразделения охраны, пунктов управления безопасностью, а также контроля состояния отдельных помещений, критических элементов объекта и отдельных предметов);

в) средств сбора и обработки информации (приемно-контрольные приборы, блоки, устройства и модули, обеспечивающие прием сигналов от извещателей, обработку, хранение и отображение информации в виде, удобном для принятия управленческих решений, осуществление местного звукового и светового оповещения, управление взятием (снятием) под охрану, передачу информации о состоянии охраняемой зоны на пульт централизованного наблюдения).

Управление системой охранной сигнализации рекомендуется осуществлять с применением административного пароля от несанкционированного доступа к управлению. Всему оборудованию, входящему в систему охранной сигнализации, рекомендуется иметь защиту от внешнего воздействия и несанкционированного доступа.

Посредством извещателей в автоматическом режиме работы рекомендуется обеспечивать:

- а) с заданной вероятностью обнаружение действия нарушителя и выдачу сигнала срабатывания (извещение) о его проникновении;
- б) выдачу сигнала о неисправности при отказе или взломе;
- в) с заданной достоверностью (вероятностью, средней наработкой на ложную тревогу) не выдачу ложных сигналов при воздействии негативных факторов природного и техногенного характера;

Рекомендуемые характеристики извещателей:

наличие электромагнитной совместимости с технологическим оборудованием охраняемого объекта и другими системами комплекса инженерно-технических средств охраны;

отсутствие необходимости обслуживания и настройки в течение срока эксплуатации, за исключением периодических регламентных и ремонтных работ.

Количество извещателей рекомендуется определять с учетом тактики охраны объекта, протяженности охраняемого периметра, размеров и этажности охраняемых зданий, сооружений и отдельных помещений, количества уязвимых мест, а также требуемой точности определения места срабатывания для оптимального реагирования подразделения охраны.

Рекомендуется обеспечивать возможность доступа к управлению системой сбора и обработки информации только с пульта централизованного наблюдения. Дистанционное вмешательство в работу системы сбора и обработки информации через какой-либо другой внешний канал связи и интерфейс рекомендуется полностью исключить.

Посредством пульта централизованного наблюдения рекомендуется обеспечивать:

- а) прием тревожных извещений о проникновении на охраняемые объекты, а также прием служебных и контрольно-диагностических извещений;

б) обработку, отображение, регистрацию полученной информации, представление ее в виде, удобном для дальнейшей обработки, а также (при наличии обратного канала) для передачи команд управления на объектовое оборудование технических средств охраны;

в) управление взятием (снятием) объекта (зоны) с охраны.

Рекомендуется обеспечить сопряжение системы охранной сигнализации с системами тревожно-вызывной сигнализации, охранной телевизионной, охранного освещения, оповещения, а также контроля и управления доступом.

Выходящие на внешнюю сторону объекта окна и двери первых этажей зданий, являющихся частью внешнего периметра объекта, а также окна и двери мест размещения критических элементов объекта рекомендуется оснащать средствами охранной сигнализации, которые выдают извещение о тревоге при попытке их вскрытия и разрушения.

13. Система тревожно-вызывной сигнализации.

В целях оперативной передачи сигнала тревоги в дежурную часть территориального органа Росгвардии (его отделов, отделений, районных и других подразделений по месту нахождения объекта), а также в дежурное подразделение с круглосуточным режимом работы частной охранной организации или ведомственной охраны в случае угрозы совершения или совершения террористического акта на объекте, объект рекомендуется оснащать системой тревожно-вызывной сигнализации (стационарными кнопками и педалями, а также носимыми сотрудниками подразделения охраны объекта и работниками объекта радиобрелоками и другими аналогичными устройствами).

Систему тревожно-вызывной сигнализации рекомендуется организовать «без права отключения».

Стационарные устройства тревожно-вызывной сигнализации ручного и ногого приведения в действие рекомендуется устанавливать в местах, обеспечивающих скрытность их использования.

При необходимости рекомендуется дополнительно устанавливать на объекте отдельную систему тревожно-вызывной сигнализации с выводом либо дублированием ее сигналов на пульт централизованного наблюдения пункта управления безопасностью.

14. Система охранная телевизионная.

В целях оптико-электронного визуального наблюдения за состоянием внешнего периметра и внутренней территории объекта, мест размещения его критических элементов, а также отдельных охраняемых зданий, сооружений и помещений, оценки складывающейся ситуации, фиксации попыток и фактов несанкционированного проникновения нарушителя и его действий, последующей идентификации нарушителя, а также сохранения полученной визуальной информации, объект рекомендуется оснащать системой охранной телевизионной в состав которой входят:

- телевизионные камеры;
- телевизионные мониторы;
- цифровые накопители информации;
- устройства управления и коммутации видеосигналов.

Телевизионные камеры рекомендуется устанавливать на отдельных опорах, кронштейнах, закрепленных на основном ограждении, опорах охранного освещения, зданиях и сооружениях объекта и внутри его помещений, вне прямой досягаемости для их выведения из строя нарушителями или выполнять в защищенном варианте.

Место и высота установки каждой телевизионной камеры, тип объектива и угол наклона его оптической оси рекомендуется определять исходя из условия формирования необходимой зоны наблюдения, в том числе непрерывной зоны для наблюдения периметра объекта и мест размещения критических элементов объекта.

Рекомендуется, чтобы зоны обзора телевизионных камер совпадали по габаритам с зонами охранного освещения. При необходимости наблюдения больших территорий рекомендуется применять объективы с переменным фокусным расстоянием, а телевизионные камеры устанавливать на дистанционно управляемых поворотных платформах. Вне помещений объекта рекомендуется комплектовать телевизионные камеры объективом с автоматической регулировкой диафрагмы.

Рекомендуется обеспечить защиту оборудования, входящего в состав системы охранной телевизионной, от внешнего воздействия и несанкционированного доступа.

Посредством системы охранной телевизионной объекта рекомендуется обеспечивать:

- а) передачу визуальной информации о состоянии внешнего периметра и мест размещения критических элементов объекта, а также отдельных охраняемых зданий, сооружений и помещений объекта на назначенные посты охраны и на пульт централизованного наблюдения пункта управления безопасностью объекта;
- б) работу в автоматизированном режиме;
- в) предоставление оператору пульта централизованного наблюдения дополнительной информации о состоянии наблюдаемой (охраняемой) зоны с целью исключения ложных тревог;
- г) визуальный контроль объекта и прилегающей к нему территории;
- д) визуальный контроль за действиями подразделений охраны при несении ими службы, предоставление необходимой информации для координации их действий;
- е) архивирование и последующее воспроизведение записей для их анализа в автоматическом режиме или по команде оператора;
- ж) оперативный доступ к видеоархиву путем задания времени, даты и идентификатора телевизионной камеры;
- з) совместную работу с системами контроля и управления доступом, охранной сигнализацией и охранного освещения;
- и) разграничение доступа к управлению и видеоинформации с целью предотвращения несанкционированных действий.

Для повышения надежности обеспечения антитеррористической защищенности объекта рекомендуется применять технические средства системы охранной телевизионной со встроенной функцией обнаружения движущихся объектов (видеодетектор), а также с автоматическим выводом изображений с телевизионных камер по сигналам технических средств охраны.

Всю видеоинформацию рекомендуется хранить на цифровых накопителях не менее 15 суток.

Качество записанной информации рекомендуется определять значимостью изображения для обеспечения антитеррористической защищенности объекта, рекомендованные параметры качества которого составляют не менее 380 телевизионных линий с частотой 6 кадров в секунду.

15. Система контроля и управления доступом.

В целях обеспечения контролируемого доступа на объект и в места размещения его критических элементов работников, посетителей и транспортных средств, объект рекомендуется оборудовать системой контроля и управления доступом.

Посредством системы контроля и управления доступом объекта рекомендуется обеспечивать:

а) санкционированный доступ и предотвращение несанкционированного доступа людей и транспорта на объект, в места размещения критических элементов объекта, а также отдельные охраняемые здания, сооружения и помещения;

б) выдачу информации на пульт централизованного наблюдения о попытках несанкционированного проникновения на объект, в места размещения критических элементов объекта, а также в отдельные охраняемые здания, сооружения и помещения;

в) работоспособность в автономном и сетевом режиме с автоматическим переходом из первого во второй при обрыве связи и нарушении локальной вычислительной сети.

Рекомендуется включать в состав системы контроля и управления доступом объекта:

устройства преграждающие с ручным, полуавтоматическим или автоматическим управлением в составе преграждающих конструкций и исполнительных устройств, обеспечивающие перекрытие проема прохода (частичное (турникет), полное (дверь), с блокированием субъекта в проеме (шлюз));

устройства для ввода идентификационных признаков в составе считывателей и идентификаторов личности;

периферийные программно-аппаратные устройства управления и центральные программно-аппаратные устройства управления, располагаемые на пульте централизованного наблюдения.

Посредством системы контроля и управления доступом рекомендуется обеспечивать выполнение следующих функциональных требований:

исключение возможности прохода через одно преграждающее устройство 2 или более человек одновременно;

открытие преграждающих устройств при считывании зарегистрированного в памяти системы идентификационного признака, запрет открывания при считывании незарегистрированного идентификационного признака;

санкционированная запись идентификационных признаков идентификатора в память системы;

защита от манипулирования путем перебора или подбора идентификационных признаков;

сохранение идентификационных признаков в памяти при отказе и отключении электропитания;

ручное и автоматическое аварийное открывание преграждающих устройств для прохода при авариях, чрезвычайных ситуациях, отключении электропитания и технических неисправностях;

защита системы аварийного открывания преграждающих устройств от возможности использования ее для несанкционированного проникновения;

выдача извещения о тревоге при аварийном открывании преграждающих устройств в случае несанкционированного проникновения;

регистрация и протоколирование текущих (штатных) и тревожных событий, приоритетное отображение тревожных событий на пульте централизованного наблюдения;

задание временных режимов действия идентификаторов и уровней доступа по командам оператора;

защита программно-аппаратных средств от несанкционированного доступа к элементам управления, информации и базам данных;

автоматический контроль исправности технических средств и линий передачи информации;

возможность автономной работы периферийных технических средств с сохранением ими основных функций при отказе связи с пультом централизованного наблюдения;

установка с пульта централизованного наблюдения режима свободного доступа при аварийных и чрезвычайных ситуациях, блокировка прохода по точкам доступа в случае нападения на объект;

возможность подключения дополнительных программно-аппаратных технических средств контроля и досмотра;

возможность интегрирования с системой охранной сигнализации и системой охранной телевизионной.

Посредством считывателей или идентификаторов (устройств ввода идентификационных признаков личности) рекомендуется обеспечивать:

надежное считывание идентификационного признака с идентификатора;

передачу идентификационного признака на устройства управления и обмена информацией.

Не рекомендуется использовать конструкцию и внешний вид считывателя (идентификатора), которые могут приводить к раскрытию применяемых кодов.

Рекомендуется обеспечить устойчивость программного обеспечения устройств управления системы контроля и управления доступом к случайным или преднамеренным воздействиям, которые могут приводить к открыванию управляемых преграждающих устройств и изменению действующих кодов доступа, следующего вида:

отключение питания аппаратных средств;

программный перезапуск аппаратных средств;

аппаратный перезапуск аппаратных средств;

случайное нажатие клавиш на клавиатуре;
случайный перебор пунктов меню программы.

После перезапуска программы рекомендуется предусмотреть возможность сохранения работоспособности системы контроля и управления доступом и сохранность установленных данных.

16. Технические средства досмотра.

В целях обнаружения взрывных устройств, оружия, токсичных веществ и других средств совершения террористического акта, а также иных запрещенных к свободному обороту предметов и веществ при проходе работников и посетителей или въезде транспортных средств на объект его рекомендуется оборудовать стационарными и мобильными техническими средствами досмотра:

а) металлообнаружителями (металлодетекторами), осуществляющими обнаружение металлических объектов, поиск холодного и огнестрельного оружия, металлосодержащих взрывчатых устройств и других видов металлосодержащей продукции, запрещенной к проносу на объект (рекомендуется выполнять в виде стационарных устройств арочного типа (порталы) либо в виде портативных переносных приборов);

б) досмотровыми эндоскопами и зеркалами, применяемыми для визуального осмотра труднодоступных мест грузов и транспортных средств, обеспечивающими возможность подсветки осматриваемого пространства;

в) рентгеновскими и рентгенотелевизионными досмотровыми комплексами, применяемыми для бесконтактного персонального досмотра лиц, определения внутреннего содержимого ручной клади, оргтехники и других предметов, оставленных без присмотра вещей, а также крупногабаритных грузов и транспортных средств (при наличии объективно подтвержденной необходимости в таком оборудовании);

г) индикаторами и комплектами для экспресс-анализа токсичных и иных опасных веществ, которые могут быть использованы для отравления питьевой воды (при наличии объективно подтвержденной необходимости в таком оборудовании);

д) другие технические средства досмотра.

Рекомендуется обеспечить возможность интеграции стационарных технических средств досмотра с системами охранной сигнализации, контроля и управления доступом и системой охранной телевизионной

III. Вспомогательные системы

17. Система оперативной связи.

Для обеспечения информирования органов государственной власти об угрозе совершения или о совершении террористического акта, а также координации и управления действиями подразделения охраны объекта и работников объекта по обеспечению антитеррористической защищенности объекта, его рекомендуется оборудовать системой оперативной связи, в состав которой входят:

стационарные и носимые средства связи общего пользования (использующие городскую телефонную сеть, сеть мобильной сотовой связи, работающую в зоне размещения объекта, сеть Интернет, сеть космической связи и т.п.);

стационарные и мобильные средства внутриобъектовой связи (использующие коммутируемую техническими средствами объекта проводную сеть и радиосвязь).

18. Система охранного освещения.

Для обеспечения необходимых условий видимости ограждений внешнего периметра объекта и мест размещения критических элементов объекта (прилегающей к ним территории), отдельных критических элементов, периметров и внутренних помещений охраняемых зданий, сооружений и отдельных помещений, а также мест несения службы сотрудниками подразделения охраны объекта, его рекомендуется оборудовать системой охранного освещения, в состав которой входят:

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

Светильники охранного освещения рекомендуется устанавливать на кронштейнах на основном ограждении или на отдельных опорах. Их количество, высоту установки и мощность ламп рекомендуется определять с учетом необходимого уровня освещенности. Лампы охранного освещения рекомендуется защищать от механических повреждений.

Посредством системы охранного освещения объекта рекомендуется обеспечивать:

а) освещенность горизонтальную на уровне земли или вертикальную на плоскости ограждений либо стен зданий или сооружений не менее 10 люкс в темное время суток во всех контролируемых (освещенных) зонах территории и периметра объекта;

б) равномерно освещенную сплошную полосу шириной не менее 3 – 4 метра по внешнему периметру объекта;

в) освещенность контролируемых (освещенных) коридоров и помещений зданий и сооружений, а также расположенных в них мест несения службы сотрудниками подразделения охраны объекта не менее 75 люкс.

г) ручное управление аппаратурой освещения из пункта управления безопасностью;

д) совместимость с техническими средствами системы охранной сигнализации и системы охранной телевизионной.

Для повышения надежности обеспечения антитеррористической защищенности объекта рекомендуется применять технические средства системы охранного освещения с возможностью автоматического включения дополнительных источников света на отдельных зонах охраняемой территории и периметра при срабатывании системы охранной сигнализации.

Рекомендуемая освещенность коридоров для прохода людей на контрольно-пропускных пунктах - не менее 100 люкс, досмотровых комнат людей и досмотровых площадок транспортных средств – не менее 200 люкс, а мест проверки пропусков – не менее 300 люкс.

Сеть охранного освещения по периметру и на территории объекта рекомендуется разделять на самостоятельные участки в соответствии с зонами системы охранной сигнализации и (или) зонами наблюдения системы охранной телевизионной.

19. Система оповещения.

Для оперативного доведения до сотрудников подразделения охраны объекта, а также до работников и посетителей объекта информации об угрозе совершения или о совершении террористического акта на объекте и координации их действий, объект рекомендуется оборудовать системой оповещения.

Посредством системы оповещения рекомендуется обеспечивать выполнение следующих функциональных требований:

подача звуковых и световых сигналов на территории объекта, а также в его отдельные здания, сооружения и помещения;

трансляция речевой информации о характере опасности, необходимости и путях эвакуации, действиях по обеспечению безопасности людей (в автоматическом режиме или в ручном режиме через микрофон).

На объекте рекомендуется разработать план оповещения, включающий в себя:

а) схему вызова сотрудников, должностными обязанностями которых предусмотрено обеспечение антитеррористической защищенности объекта, а также участие в мероприятиях по предотвращению или устранению последствий аварий и чрезвычайных ситуаций;

б) систему сигналов оповещения;

в) инструкции, регламентирующие действия при внештатных ситуациях;

г) планы эвакуации.

Эвакуацию людей по сигналам оповещения рекомендуется сопровождать:

а) включением аварийного и охранного освещения;

б) 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);

в) включением световых указателей направления и путей эвакуации;

г) дистанционным открыванием преграждающих устройств контрольно-пропускных пунктов и дверей дополнительных эвакуационных выходов, оборудованных электромагнитными замками.

Сигналы оповещения рекомендуется устанавливать отличающимися от сигналов другого назначения.

Звуковую и световую сигнализации рекомендуется устанавливать способом, обеспечивающим оповещение во всех местах постоянного или временного пребывания работников и посетителей объекта, а также сотрудников подразделений охраны объекта, разборчивость передаваемых речевых сообщений. Рекомендуется использовать громкоговорители без регуляторов громкости и разъемных соединений.

Коммуникации системы оповещения при необходимости рекомендуется совмещать с радиотрансляционной сетью объекта, либо иными системами со сходными задачами (например, системами ГО, ЧС и т.п.).

20. Система энергоснабжения.

Бесперебойное энергоснабжение, обеспечивающее работу инженерно-технических средств охраны объекта, рекомендуется осуществлять либо от двух независимых источников переменного тока, либо от одного источника переменного тока с автоматическим переключением на резервное питание (в аварийном режиме) и оповещением о переходе на электропитание от резервного источника.

Основное электропитание рекомендуется осуществлять от электрической сети переменного тока номинальным напряжением 220 или 380 вольт.

Резервное электропитание рекомендуется осуществлять от резервного ввода электрической сети переменного тока (независимый фидер) либо от аккумуляторных батарей.

Электропитание от сети переменного тока рекомендуется подавать на технические средства охраны от отдельной группы электропитания с помощью линейно-кабельной сети.

При прокладке линейно-кабельной сети комплекса инженерно-технических средств охраны, представляющей собой совокупность кабельных линий, кабельного оборудования (боксы, шкафы, коробки) и линейно-кабельных устройств (кабельная канализация, вводы, распределительные шкафы), предназначенных для передачи в системах инженерно-технических средств охраны энергии электропитания, сигнальной, речевой и видеоинформации, а также сигналов управления, рекомендуется обеспечить:

скрытность прокладки проводных линий, кабелей связи и электропитания (или их выполнение в защищенном варианте);

резервирование линий, кабелей и коммутационного оборудования;

автономность от технологических кабельных сетей объекта.

Кабельную сеть, проложенную по периметру объекта, в целях повышения надежности обеспечения электроэнергией технических средств охраны рекомендуется электрически замыкать в кольцо.

Распределительные щиты, шкафы, коробки и боксы кабельной сети инженерно-технических средств охраны, а также люки кабельных колодцев на территории объекта, рекомендуется оборудовать средствами запирания и охранной сигнализации.

При работе от резервного источника рекомендуется обеспечивать функционирование инженерно-технических средств охраны в течение не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги.

Изменения, которые вносятся в рекомендации по оснащению объектов водоснабжения и водоотведения инженерно-техническими средствами

1. В пункте 2 дополнить таблицу «Перечень рекомендуемых инженерно-технических средств охраны для объектов различных категорий» следующими позициями:

«

18) средства обнаружения радиосигналов	+	+	+	+
19) средства радиоподавления	+	+	+	+
20) средства радиолокационного обнаружения и сопровождения	+	+/-	+/-	-
21) средства видеообнаружения	+	+	+/-	-

».

2. Дополнить пунктом 16.1 следующего содержания:

«16.1 Система пресечения функционирования беспилотных воздушных судов.

В целях защиты охраняемых объектов, работников и (или) лиц, находящихся на этих объектах, от угрозы совершения террористического акта с применением беспилотного воздушного судна объект рекомендуется оборудовать системой пресечения функционирования беспилотных воздушных судов, состоящей из:

- а) средств обнаружения радиосигналов;
- б) средств радиоподавления;
- в) средств радиолокационного обнаружения и сопровождения;
- г) средств видеообнаружения.

Управление системой пресечения функционирования беспилотных воздушных судов рекомендуется осуществлять по защищенным каналам связи из единого пункта управления, обеспечивающего:

- а) отображение достоверной информации о воздушной обстановке в воздушном пространстве над прилегающей к объекту территории;
- б) траекторное сопровождение беспилотных воздушных судов в случаях их радиолокационного и (или) видеообнаружения;

в) выдачу сигнала о радиоподавлении каналов управления и сигналов радионавигационных систем беспилотного воздушного судна;

г) автоматическую фиксацию даты и времени инцидента в системном журнале событий.

Рекомендуется обеспечить защиту средств и пункта управления, входящих в систему пресечения функционирования беспилотных воздушных судов, от внешнего воздействия и несанкционированного доступа.

Посредством системы пресечения функционирования беспилотных воздушных судов рекомендуется обеспечивать:

а) определение факта запуска с прилегающей к объекту территории беспилотного воздушного судна;

б) обнаружение радиосигналов канала управления передачи данных беспилотного воздушного судна;

в) идентификацию сигналов канала управления передачи данных беспилотного воздушного судна, включая распознавание вида передачи и оценки основных параметров сигналов, необходимых для создания помех;

г) получение информации о типе беспилотного воздушного судна, его координатах и координатах точки старта посредством вскрытия радиопотокола обмена данными между беспилотного воздушного судна и пультом управления (при отсутствии криптографической защиты информации каналов управления передачи данных беспилотных воздушных судов);

д) радиолокационное обнаружение беспилотного воздушного судна, в том числе летящего в режиме радиомолчания, определение траектории его полета;

е) радиоподавление каналов управления и передачи данных беспилотного воздушного судна, а также радиоподавление сигналов бортовых спутниковых радионавигационных систем беспилотного воздушного судна;

ж) автоматическое видеообнаружение и сопровождение беспилотного воздушного судна;

з) обеспечение в непрерывном круглосуточном режиме комплексной обработки, отображения и хранения данных об обнаружении и выдачи команды на радиоэлектронное подавление беспилотного воздушного судна.

Состав и количество средств обнаружения и радиоподавления, входящих в систему пресечения функционирования беспилотных воздушных судов, а также место и высоту их установки рекомендуется определять по результатам инженерно-технического обследования объекта».