Об утверждении Инструкции по организации антитеррористической защиты объектов Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан и его ведомств, уязвимых в террористическом отношении

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 12 июня 2024 года № 316/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 18 июня 2024 года № 34506

В соответствии с пунктом 1 статьи 10-2 Закона Республики Казахстан "О противодействии терроризму", ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую инструкцию по организации антитеррористической защиты объектов Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан и его ведомств, уязвимых в террористическом отношении.

2. Управлению мобилизационной подготовки, гражданской защиты и антитерроризма Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на руководителя аппарата Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие после истечения десяти календарных дней после дня его первого официального опубликования.

Министр цифрового развития,
инноваций и аэрокосмической промышленности *Ж. Мадиев*
Республики Казахстан

"СОГЛАСОВАН"

Министерство внутренних дел
Республики Казахстан
"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Утверждена приказом
Министр цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 12 июня 2024 года № 316/НҚ

Инструкция по организации антитеррористической защиты объектов Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан и его ведомств, уязвимых в террористическом отношении

Глава 1. Общие положения

1. Настоящая Инструкция по организации антитеррористической защиты объектов Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан и его ведомств, уязвимых в террористическом отношении, разработана в соответствии с пунктом 1 статьи 10-2 Закона Республики Казахстан "О противодействии терроризму" и определяет требования по организации антитеррористической защиты объектов Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (далее – Министерство) и его ведомств, уязвимых в террористическом отношении.

2. Настоящая Инструкция распространяется на объекты Министерства и его ведомств, отнесенных к объектам, уязвимым в террористическом отношении, в соответствии с Правилами и критериями отнесения объектов к уязвимым в террористическом отношении, утвержденными постановлением Правительства Республики Казахстан от 12 апреля 2021 года № 234, (объекты связи и телекоммуникаций (АО "Казпочта", АО "Казахтелеком"), государственных услуг (Центры обслуживания населения, Специализированные центры обслуживания населения) и объекты наземной космической инфраструктуры (объекты комплексов управления космическими аппаратами и системы мониторинга связи аэрокосмической промышленности и его ведомств).

3. Настоящая инструкция предназначена для использования руководителями и другими должностными лицами, обеспечивающими проведение мероприятий по антитеррористической защищенности объектов Министерства, а также для сотрудников контролирующих и исполнительных органов при изучении и проверке состояния антитеррористической защищенности объектов Министерства. Инструкция детализирует общие подходы к обеспечению защищенности объектов Министерства,

их инженерно-технической укрепленности, порядку организации охраны, осуществления пропускного и внутриобъектового режимов, а также ведению соответствующей документации.

4. При эксплуатации объектов Министерства обеспечивается соблюдение Требований к организации антитеррористической защиты объектов, уязвимых в террористическом отношении, утвержденных постановлением Правительства Республики Казахстан от 6 мая 2021 года № 305 (далее – Требования к организации антитеррористической защиты объектов, уязвимых в террористическом отношении), а также настоящей Инструкции.

5. В настоящей Инструкции используются следующие основные понятия:

1) система связи – совокупность технических средств и специально выделенных каналов связи, предназначенных для передачи (обмена) информации (информацией), оперативного управления деятельностью служб охраны объекта;

2) контрольно-пропускной пункт – специально оборудованное место, предназначенное для обеспечения контроля, пропуска, досмотра людей и транспортных средств;

3) система видеонаблюдения – совокупность функционирующих видеоканалов, программных и технических средств записи и хранения видеоданных, а также программных и (или) технических средств управления, осуществляющих информационный обмен между собой;

4) система освещения – совокупность технических средств, позволяющих обеспечить необходимый уровень освещенности для системы видеонаблюдения, видимость людей и транспортных средств на объекте в темное время суток;

5) инженерно-техническая укрепленность – конструктивные элементы, инженерные , технические средства и (или) их совокупность, обеспечивающие необходимое противодействие несанкционированному проникновению на объект либо его части;

6) система контроля и управления доступом – совокупность технически совместимых аппаратных средств и (или) программного обеспечения, предназначенных для контроля доступа, разграничения прав на вход и (или) выход на объект и (или) его отдельные зоны персонала и посетителей, сбора и хранения информации;

7) периметр объекта – граница объекта согласно правоустанавливающим документам;

8) профилактические и учебные мероприятия – превентивные способы обучения персонала и охраны, реализуемые в виде инструктажей и занятий в целях привития навыков первичного реагирования;

9) пропускной режим – совокупность правил, регламентирующих установленный порядок, исключающий возможность несанкционированного входа (выхода) лиц, въезда (выезда) транспортных средств, вноса (выноса), ввоза (вывоза) имущества;

10) противотаранные устройства (заграждения) – инженерно-технические изделия, предназначенные для принудительного замедления и (или) остановки транспортных средств;

11) паспорт антитеррористической защищенности – информационно-справочный документ, содержащий общие и инженерно-технические сведения об объекте, отражающие состояние его антитеррористической защищенности, и предназначенный для планирования мероприятий по предупреждению, пресечению, минимизации и (или) ликвидации последствий актов терроризма на объекте, уязвимом в террористическом отношении;

12) система охранная телевизионная – система видеонаблюдения, представляющая собой телевизионную систему замкнутого типа, предназначенную для выявления и фиксирования нарушений;

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, акте терроризма) и действиях в сложившейся обстановке.

6. Воспрепятствование совершению акта терроризма (снижение риска совершения акта терроризма) на объектах Министерства обеспечивается выполнением комплекса мер и соблюдением условий, включающих в себя:

1) проведение организационных мероприятий по обеспечению антитеррористической защищенности объекта с учетом характера и специфики возможных террористических угроз, определяемых органами национальной безопасности, и их возможных последствий;

2) определение возможных причин и условий, способствующих совершению акта терроризма на объекте и их устранение;

3) оснащение необходимыми инженерно-техническими средствами;

4) обеспечение установленного пропускного режима;

5) организация подготовки (обучения) персонала объектов Министерства и сотрудников субъектов охранной деятельности к первичному реагированию на угрозы совершения акта терроризма (выявление признаков совершения акта терроризма, информирование об этом руководства, правоохранительных и (или) специальных государственных органов);

6) контроль за соблюдением требований обеспечения антитеррористической защищенности.

7. Минимизация и (или) ликвидация последствий возможных террористических угроз на объектах Министерства обеспечивается выполнением комплекса мер и соблюдении условий, включающих в себя:

1) своевременное информирование органов национальной безопасности и (или) внутренних дел Республики Казахстан о совершенном акте терроризма;

2) участие персонала объекта Министерства в учениях, тренировках и экспериментах по вопросам реагирования на террористические проявления, а также минимизация и (или) ликвидация угроз техногенного характера, возникших в результате совершенного акта терроризма, при проведении их уполномоченными государственными органами и организациями, органами оперативного управления;

3) обучение персонала объекта Министерства и сотрудников субъектов охранной деятельности навыкам первичного реагирования на угрозы террористического характера;

4) организация оповещения и эвакуации персонала и посетителей в случае совершения акта терроризма на объекте Министерства;

5) своевременное составление и поддержание в актуальном состоянии паспорта антитеррористической защищенности объекта Министерства, его надлежащее хранение;

6) формирование сил и средств, необходимых для организации мер первичного реагирования, направленных на ликвидацию и минимизацию последствий акта терроризма, за исключением случаев, прямо угрожающих жизни и здоровью людей, до прибытия основных спасательных, аварийных и иных служб;

7) подготовка и организация экстренных мер по обеспечению безопасности систем жизнеобеспечения и безопасности объекта Министерства (водоснабжения, электроснабжения, газового оборудования, пожаротушения), персонала и посетителей объекта Министерства, определением путей эвакуации, обеспечением персонала средствами защиты, определением ответственных лиц за указанные участки деятельности.

Глава 2. Требование организации пропускного режима на объекты Министерства

8. Пропускной режим предназначен для:

1) организации санкционированного допуска лиц и транспортных средств на объект или его части (зоны);

2) выявления лиц с противоправными намерениями, а также предметов и веществ, которые используются для их реализации;

3) охраны объекта, защиты потенциально опасных участков объекта и критических зон, исключения бесконтрольного пребывания на них посторонних лиц.

9. Пропускной режим на объектах подлежащих государственной охране осуществляется в соответствии Требований к организации антитеррористической защиты объектов, уязвимых в террористическом отношении.

10. Основными мероприятиями по обеспечению пропускного режима на объектах Министерства являются:

1) проверка у лиц, прибывших на объект, документа, удостоверяющего личность, также документа, дающего право на вход (выход) лиц, въезд (выезд) транспортных средств, внос (вынос), ввоз (вывоз) имущества;

2) проведение осмотра и досмотра транспортных средств при их въезде (выезде);

3) проведение визуального осмотра охраняемой территорий и ограждения на наличие посторонних лиц и неизвестных предметов;

4) задержание лиц, проникших на охраняемую территорию незаконным путем, до выявления обстоятельств и вызов сотрудников правоохранительных органов;

5) обеспечение порядка на охраняемой территории, применение физической силы, специальных средств и/или табельного оружия против лиц, совершающих явное нападение на объект Министерства или противоправные действия, угрожающие жизни людей или безопасности объекта Министерства, в соответствии с требованиями законодательства Республики Казахстан;

6) оперативное реагирование на признаки актов терроризма (попытка провести на территорию запрещенные предметы, появление вблизи объекта подозрительных лиц) и доведение необходимой информации до правоохранительных органов.

11. Для непосредственной организации пропускного режима на охраняемой территории объекта определяется должностное лицо, ответственное за организацию пропускного режима и подразделение, поддерживающее соответствующий пропускной режим.

Должностное лицо, ответственное за организацию пропускного режима, назначается из числа штатных сотрудников объекта, имеющих полномочия по даче указании и распоряжений от имени руководства объекта по вопросам пропускного режима.

В подразделении, поддерживающем соответствующий пропускной режим, назначаются штатные сотрудники объекта. Окончательное решение о привлечении сотрудника к мероприятиям по обеспечению пропускного режима объекта принимается руководителем объекта.

Состав подразделения, обеспечивающего пропускной режим предусматривает заступление на дежурство необходимого количества сотрудников в зависимости от охраняемой территорий, но не менее двух сотрудников, а также наличие не менее трех смен.

Порядок заступления на дежурство и мероприятия по приему и передаче дежурства определяется руководителем объекта.

12. В целях обеспечения пропускного режима руководство объектов Министерства, не подлежащих государственной охране, с соблюдением требований законодательства о государственных закупках и о закупках отдельных субъектов квазигосударственного

сектора, заключает договор об оказании охранных услуг с частными охранными организациями, имеющими лицензию по подвиду деятельности: "Все виды охранных услуг, в том числе охрана объектов, уязвимых в террористическом отношении".

В случае заключения договора об оказании охранной услуги с субъектом охранной деятельности в договоре оговариваются обязанности субъекта охранной деятельности по обеспечению антитеррористической защищенности объекта.

Глава 3. Требования к организации профилактических и учебных мероприятий

13. Профилактические и учебные мероприятия проводятся с целью доведения до сотрудников объектов Министерства об основных особенностях объекта, возможных последствиях в случае совершения акта терроризма на нем, порядка проведения мероприятий по предотвращению актов терроризма и недопущения проникновения на территорию объекта посторонних лиц, а также об ответственности за упущения при исполнении служебных обязанностей, если по их вине допущено совершение акта терроризма по вариантам тематик занятий согласно приложению 1 к настоящей Инструкции.

14. Учебные мероприятия организуются руководителями объектов Министерства с персоналом, а также руководителями субъектов охранной деятельности с привлекаемыми к охране объекта работниками.

Занятия с сотрудниками проводится индивидуально или с группой работников однотипных объектов в виде лекции, инструктажа, тренировок с выполнением практических действий, также используются видео уроки.

15. Учебные мероприятия обеспечивают обучение персонала выявлению подозрительных лиц и предметов, действиям в условиях совершения или угрозы совершения акта (актов) терроризма по предотвращению или минимизации ущерба, способам защиты от его последствий, безопасной и своевременной эвакуации с объекта посетителей и персонала.

16. В ходе теоретических занятий (лекций) доводится необходимая информация (требования регламентирующих нормативных правовых актов, инструкций, алгоритм действий, особенности объекта Министерства), а в ходе практических занятий отрабатываются действия персонала:

1) по проведению безопасной и беспрепятственной эвакуации;

2) в случае угрозы акта терроризма;

3) при обнаружении на объекте подозрительных лиц и предметов, а также иных сценариев совершения актов терроризма, характерных для объекта.

17. Во время инструктажа до персонала доводятся наиболее вероятные для объекта характер и специфика террористических угроз и правила поведения при их возникновении, способы минимизации и ликвидации последствий.

18. С сотрудниками, привлекаемыми к мероприятиям по обеспечению пропускного режима объекта, проводятся дополнительные занятия по приобретению и (или) совершенствованию навыков использования инженерно-технических средств антитеррористической защиты, технике осмотра помещений, выявлению возможных мест закладки взрывных устройств.

19. По характеру и времени проведения инструктаж подразделяется на плановый и внеплановый.

Плановый инструктаж проводится не реже одного раза в год согласно приложению 2 к настоящей Инструкции.

Внеплановый инструктаж проводится руководителями или иными должностными лицами объектов Министерства, руководителями субъектов охранной деятельности либо представителями государственных органов, задействованных в проводимых учениях, тренировках и экспериментах в случаях:

1) введения в регионе, где находится объект, уровня террористической опасности;

2) наличия информации о возможной угрозе совершения акта терроризма;

3) подготовки к учениям, тренировкам, экспериментам;

4) подготовки к проведению охранных мероприятий.

Внеплановый инструктаж проводится индивидуально или с группой работников. Содержание внепланового инструктажа определяется в каждом конкретном случае в зависимости от причин и обстоятельств, вызвавших необходимость его проведения.

20. Практические и теоретические занятия проводятся в соответствии с графиком проведения, утвержденным руководителем объекта Министерства, уязвимого в террористическом отношении, (руководителем субъекта охранной деятельности) с периодичностью не реже одного раза в год.

21. Со всеми сотрудниками, впервые принятыми на работу, проводятся занятия по ознакомлению с требованиями о запрете разглашений информаций по порядку охраны объекта и другой информации, которая используется для совершения акта терроризма, порядку действии при нападении на объект.

22. Инструктаж с сотрудниками, заступающими на дежурство по организации пропускного режима проводятся не реже одного раза в месяц. Также в обязательном порядке проходят инструктаж лица, прибывшие из отпусков, командировок и излечения сроком более 10 (десять) суток.

23. Тренировки с выполнением практических действий сотрудников, привлекаемых к охране объекта, при угрозе нападения или его совершении проводятся не менее одного раза в месяц с каждым составом дежурной смены.

24. О проведении инструктажей и занятий производится запись в журнале учета учебных мероприятий по антитеррористической защите согласно приложению 3 настоящей Инструкции.

Для объектов с большим количеством персонала (более 20 двадцати человек) документирование проведения указанных мероприятий осуществляется в виде протокола или справки.

Глава 4. Требования к организации взаимодействия по вопросам реагирования на террористические проявления, а также ликвидации угроз техногенного характера, возникших в результате совершенного акта терроризма

25. Руководители объектов Министерства при получении информации об угрозе совершения или о совершении акта терроризма на объекте (и/или анонимного характера) незамедлительно лично или через уполномоченного им лица посредством имеющихся в его распоряжении средств связи доводит (дублирует) информацию в территориальные органы национальной безопасности, внутренних дел, а также государственному органу (организации), в ведении которого находится объект.

26. При представлении информации с помощью средств телефонной связи или радиосвязи лицо, передающее информацию, представляется назвав свои фамилию, имя, отчество (при наличии), должность, наименование объекта и сообщает имеющуюся информацию об угрозе совершения или о совершении акта терроризма на объекте.

27. К угрозе совершения акта терроризма на объект относятся:

1) получение (и/или анонимно) сообщения о готовящемся акте терроризма на объект;

2) попытки незаконного заноса (завоза) на охраняемую территорию запрещенных веществ;

3) обнаружение на территории объекта заложенных устройств или веществ неизвестного предназначения;

4) сбор возле объекта Министерства группы неизвестных подозрительных лиц, не реагирующих на замечания сотрудников объекта.

28. Руководители и (или) уполномоченные лица объектов Министерства после информирования соответствующих государственных органов по безопасности о выявленном факте правонарушения, лично являются на объект, с представлением документов, подтверждающих свое полномочие сотрудникам силовых структур, прибывшим для предотвращения акта терроризма или ликвидации ее последствий и оказывают им помощь в предоставлении необходимой для проведения антитеррористической операции информации.

29. В случае совершения акта терроризма или возникновения кризисных ситуаций в рабочее время ответственным за организацию первичных мер реагирования является должностное лицо, назначенное руководителем объекта Министерства ответственным за обеспечение безопасности объекта.

30. В случае совершения акта терроризма или возникновения кризисных ситуаций в нерабочее время ответственным за организацию первичных мер реагирования является

старший дежурной смены, который до прибытия руководства объекта или представителей силовых структур по ликвидации кризисной ситуации организует выполнение первичных мер реагирования.

31. При установлении уровней террористической опасности, осуществляемом в соответствии с указом Президента Республики Казахстан от 9 августа 2013 года № 611 "Об утверждении Правил организации и функционирования государственной системы мониторинга информации и оповещения населения о возникновении угрозы акта терроризма" руководителями или иными должностными лицами объектов Министерства применяются следующие меры безопасности:

1) при "желтом" уровне террористической опасности:

усиление пропускного режима на объекте;

проверка и обеспечение работоспособности систем безопасности, оповещения, видеонаблюдения и охранной сигнализации;

досмотр посетителей, персонала и транспортных средств, с использованием специальных технических средств;

инструктаж субъектов охранной деятельности, заключивших договор об оказании охранных услуг, персонала, служащих и работников объектов, осуществляющих функции по локализации кризисных ситуаций с привлечением в зависимости от полученной информации специалистов в соответствующей сфере;

проведение учебных мероприятий с персоналом по действиям при совершении или угрозе совершения акта (актов) терроризма;

отработка вопросов экстренной эвакуации объектов, с определением мест временного нахождения эвакуированных людей, материальных ценностей и документации;

2) при "оранжевом" уровне террористической опасности (наряду с мерами, принимаемыми при установлении "желтого" уровня террористической опасности):

отработка совместных действий с уполномоченными государственными органами и организациями, республиканского, областного, города республиканского значения, столицы, района (города областного значения) и морского оперативного штаба по борьбе с терроризмом по вопросам реагирования на акты терроризма, а также ликвидации угроз техногенного характера, возникших в результате совершенного акта терроризма;

приведение в состояние режима повышенной готовности субъектов охранной деятельности, заключивших договор об оказании охранных услуг, персонала, служащих и работников объектов, осуществляющих функции по локализации кризисных ситуаций;

приостановление деятельности опасных производственных объектов и охранной деятельности;

3) при установлении "красного" уровня террористической опасности (наряду с мерами, применяемыми при введении "желтого" и "оранжевого" уровней террористической опасности):

принятие неотложных мер по спасению людей, содействие бесперебойной работе спасательных служб и формирований;

приостановление деятельности объектов Министерства;

приостановление охранной деятельности.

Глава 5. Требования к разработке и обращению паспорта антитеррористической защищенности объекта, уязвимого в террористическом отношении

32. Паспорт антитеррористической защищенности объекта составляется согласно типовому паспорту антитеррористической защищенности объектов, уязвимых в террористическом отношении, утвержденному совместным приказом Министра внутренних дел Республики Казахстан от 14 июня 2023 года № 481 и Председателя Комитета национальной безопасности Республики Казахстан от 26 июня 2023 года № 51 (зарегистрирован в реестре государственной регистрации нормативных правовых актов за № 32950), в двух экземплярах с одновременной разработкой электронного варианта.

33. Проект паспорта составляется в течение сорока пяти рабочих дней с момента получения руководителями объектов или лицами, их замещающими соответствующего уведомления о включении объекта в перечень объектов, уязвимых в террористическом отношении, области, города республиканского значения или столицы.

34. Проект паспорта объекта, включенного в перечень объектов, уязвимых в террористическом отношении, области, города республиканского значения или столицы, направляется на согласование должностному лицу, указанному в типовом паспорте, в течение десяти календарных дней после составления.

Срок согласования проекта паспорта не должен превышать пятнадцати рабочих дней со дня поступления паспорта должностному лицу, указанному в типовом паспорте .

35. В случае наличия замечаний к проекту паспорта, он возвращается лицу, направившему проект паспорта, с указанием причин, послуживших причиной возврата.

Проект паспорта дорабатывается в срок не более пятнадцати рабочих дней со дня возврата.

Срок согласования проекта паспорта, поступившего повторно, (во исполнение ранее указанных замечаний) не должен превышать семь рабочих дней.

36. Проект паспорта объекта, включенного в ведомственный перечень, согласовывается должностным лицом, определенным в настоящей Инструкции, если иное не установлено законодательством Республики Казахстан.

В течение десяти рабочих дней после согласования паспорт утверждается (и/или при его обновлении) собственником, владельцем или руководителем организации, подразделения организации, являющейся правообладателем объекта.

37. В случаях, когда здание, сооружение (комплекс зданий и сооружений) используются для размещения объектов, принадлежащих нескольким правообладателям, составление паспорта осуществляется по письменному соглашению между ними совместно всеми правообладателями объектов или одним из них.

38. При совместном составлении паспорт подлежит утверждению всеми правообладателями объектов, уязвимых в террористическом отношении.

При составлении одним правообладателем паспорт утверждается руководителем объекта по согласованию с другими правообладателями объекта.

Количество копий (электронных копий) паспорта и их направление другим правообладателям объекта определяется письменным соглашением между их правообладателями.

39. Первый экземпляр паспорта антитеррористической защищенности объекта (оригинал) хранится у ответственного лица или в подразделении объекта, определенного приказом руководителя организации, являющейся правообладателем объекта.

Второй экземпляр паспорта и электронный вариант паспорта (в формате PDF на электронном носителе информации) в срок не позднее десяти календарных дней со дня его утверждения или корректировки направляются в территориальные подразделения органов внутренних дел Республики Казахстан для хранения.

40. Паспорт корректируется в случаях изменения:

1) прав собственности,

2) руководителя объекта;

3) наименования объекта;

4) основного предназначения объекта;

5) общей площади и периметра объекта, застройки прилегающей территории или после завершения капитального ремонта, реконструкции зданий (строений и сооружений) и инженерных систем, если были произведены изменения в конструкции;

6) потенциально опасных участков объекта;

7) технических средств, привлекаемых для обеспечения антитеррористической защищенности объекта.

Внесение корректив в паспорт осуществляется в течение двадцати рабочих дней с момента возникновения причины его изменения. В отдельных случаях по решению антитеррористической комиссии могут устанавливаться иные сроки исходя из сложности объекта и вносимых изменений.

41. В паспорт вносятся изменения, заверенные подписью руководителя организации , являющейся правообладателем объекта, или лица, уполномоченного организацией

подписывать паспорт. Замене подлежат только те элементы паспорта, где произошли изменения. Одновременно информация о соответствующих изменениях за подписью руководителя организации, являющейся правообладателем объекта, направляется в органы внутренних дел Республики Казахстан для приобщения ко второму экземпляру паспорта.

42. Паспорт подлежит полной замене:

1) не реже одного раза в пять лет;

2) в случае внесения корректив в более чем половину пунктов текста паспорта.

Утративший силу паспорт подлежит уничтожению в комиссионном порядке с составлением соответствующего акта.

Акт остается в организации, являющейся правообладателем объекта. Копия акта направляется по месту хранения второго экземпляра паспорта.

43. Сведения паспорта носят ограниченный характер согласно Правилам отнесения сведений к служебной информации ограниченного распространения и работы с ней, утвержденным Правительством Республики Казахстан от 24 июня 2022 года № 429.

Глава 6. Требования к оснащению объектов, уязвимых в террористическом отношении, инженерно-техническим оборудованием

Параграф 1. Требования к оснащению объектов, уязвимых в террористическом отношении, инженерно-техническим оборудованием в области государственных услуг

44. В целях установления дифференцированных требований к антитеррористической защищенности объектов в зависимости от возможных последствий совершения акта терроризма и на основании его значимости для устойчивого функционирования отраслей в сфере компетенции Министерства проводится разделение объектов Министерства на группы:

первая группа – объекты, подлежащие государственной охране (включенные в Перечень объектов Республики Казахстан, подлежащих государственной охране);

вторая группа – объекты некоммерческого акционерного общества " Государственная корпорация "Правительство для граждан" и его филиалов.

третья группа – объекты наземных комплексов управления космическими аппаратами и системы мониторинга связи аэрокосмической промышленности Республики Казахстан, объекты почтовой связи и телекоммуникаций.

45. Объекты Министерства (первая, вторая и третья группы), уязвимые в террористическом отношении оснащаются системой видеонаблюдения с передачей видеоизображения в Центры оперативного управления полиции либо в дежурные части территориальных органов внутренних дел.

Объекты первой, второй и третьей группы оснащаются инженерно-техническим оборудованием в соответствии с требованиями настоящей Главы.

46. Для оснащения объектов Некоммерческого акционерного общества " Государственная корпорация "Правительство для граждан" и его филиалов используются следующие инженерно-технические средства:

1) по оборудованию периметра объекта:

- системы контроля и управления доступом;
- средства охранного и системы освещения;

2) по контролю за обстановкой на объекте:

- средства и системы связи;
- системы и средства оповещения;
- системы охранной, пожарной и тревожной сигнализации;
- технические средства досмотра;

3) обеспечивающие работу системы безопасности:

Допускается оснащение объектов, уязвимых в террористическом отношении, иным инженерно-техническим оборудованием, прямо не указанным в настоящем пункте, но выполняющим те же задачи и функции или отвечающие тем же целям.

47. Инженерно-технические оборудования необходимо привести в соответствие с требованиями пунктов 49, 50, 51, 52, 53, 54, 55, 56, 57 настоящей Инструкции.

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

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

Наружные ограждающие конструкции (стены и перекрытия) зданий (помещений) контрольно-пропускных пунктов обеспечиваются устойчивыми к внешним воздействиям, включая действия противоправного характера, конструкциями и иметь круговой обзор.

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.

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

В случае размещения объекта в одном здании контрольно-пропускной пункт оборудуется внутри здания вблизи центрального входа, а автотранспортный контрольно-пропускной пункт оборудуется со стороны заезда транспортных средств к зданию.

При отсутствии прилегающей территории автотранспортный контрольно-пропускной пункт не оборудуется.

На объектах Некоммерческого акционерного общества "Государственная корпорация "Правительство для граждан" и его филиалов за поддержание соответствующего пропускного и внутриобъектового режима ответственность возлагается в рамках компетенций на Службу безопасности, Службу по защите государственных секретов, Департамент административно-хозяйственной деятельности , структурные подразделения Некоммерческого акционерного общества " Государственная корпорация "Правительство для граждан" и его филиалов, а также на субъект охранной деятельности, заключивший договор по охране объекта.

На объектах Некоммерческого акционерного общества "Государственная корпорация "Правительство для граждан" и его филиалов обеспечение пропускного и внутриобъектового режима осуществляется сотрудниками частных охранных организаций, имеющих соответствующие лицензии.

49. Система контроля и управления доступом обеспечивает:

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

2) фиксацию времени прихода и ухода каждого сотрудника объекта;

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 обязан 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.

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.

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

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

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

Приборы освещения необходимо располагать так, чтобы не ослеплять контролеров контрольно-пропускного пункта.

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

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

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 управления освещением - включение освещения любого участка или всего периметра.

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

Помещения контрольно-пропускных пунктов, входы в здания, коридоры категорированных помещений дополнительно оборудуются аварийным освещением. Переход рабочего освещения на аварийное и обратно обязан осуществляться автоматически.

51. Система связи оперативной обеспечивает:

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

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

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

4) защиту передаваемой информации;

5) 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.

Конструкция компонентов системы связи оперативно обеспечивает электробезопасность обслуживающего персонала при их эксплуатации, обслуживании и ремонте.

52. Система оповещения осуществляет:

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" (далее – Закон о гражданской защите).

На объекте разрабатывается 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) алгоритмы действия сотрудников при внештатных ситуациях;

3) планы эвакуации;

4) систему сигналов оповещения.

Эвакуация людей в ходе действия системы оповещения сопровождается:

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).

Сигналы оповещения отличаются от сигналов другого назначения.

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

На охраняемой территории применять рупорные громкоговорители. Они устанавливаются 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.

Коммуникации систем оповещения допускается проектировать совмещенными с радиотрансляционной сетью объекта.

53. 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.

Система охранной сигнализации, являющаяся объектом технического регламента (технических регламентов) Евразийского экономического союза или Республики Казахстан проходит оценку соответствия требованиям данного технического регламента (технических регламентов).

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.

Системой охранной сигнализации оборудуются три рубежа охраны.

Первым рубежом охраны защищаются:

1) строительные конструкции по периметру зданий или помещении 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.

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".

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.

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

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

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

54. Телевизионная система видеонаблюдения обеспечивает:

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) сохранение видеоинформации для последующего анализа событий (срок хранения информации обязан составлять не менее 30 (тридцать) суток);

3) видео документирование 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;

6) возможность подключения к информационным подсистемам Центров оперативного управления, либо передачу видеоизображения в дежурные части территориальных органов полиции.

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.

Видеокамеры, предназначенные для контроля территории объекта или периметра обеспечиваются в рабочем состоянии, с учетом условий воздействия климатических факторов для наружных установок в соответствии с климатической зоной, с размещением в герметичных термокожухах, обеспечивающих работоспособность при воздействии климатических факторов.

В темное время суток, если освещенность охраняемой зоны ниже чувствительности телекамер, включается охранное освещение видимого или инфракрасного диапазона света. Зоны охранного освещения совпадают с зоной обзора телекамер.

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

Технические требования к системам видеонаблюдения, входящим в систему охранную телевизионную объекта и минимальные технические возможности систем видеонаблюдения соответствуют требованиям, предусмотренным Правилами функционирования Национальной системы видеомониторинга, утвержденными

приказом Председателя Комитета национальной безопасности Республики Казахстан от 27 октября 2020 года№ 69-қе "Об утверждении Правил функционирования Национальной системы видеомониторинга" (зарегистрированный в Реестре государственной регистрации нормативных правовых актов за № 21693) (далее – Правила национальной системы видеомониторинга).

55. Технические средства досмотра применяются на объектах для обнаружения оружия, других предметов и веществ, запрещенных к несанкционированному вносу (выносу), ввозу (вывозу) на объект и с объекта. Перечень запрещенных к проносу предметов на объекты Министерства указан в приложении 4 к настоящей Инструкции.

Оснащение объекта техническими средствами досмотра соответствует угрозам, характерным для объектов, особенностям его функционирования.

В перечень технических средств досмотра входят металлообнаружители.

Металлообнаружители (металлодетекторы) обеспечивают обнаружение холодного и огнестрельного оружия, металлосодержащих взрывных устройств (гранат), запрещенных к проносу различных видов металлосодержащей продукции производства и быть выполнены в виде стационарных устройств арочного или стоечного типа, либо в виде портативных приборов.

Технические средства досмотра обеспечивают выполнение возможности перенастройки на обнаружение различных масс металла.

56. В случае невозможности оснастить объекты необходимым инженерно-техническим оборудованием, за исключением систем охранных телевизионных и систем оповещения, принимаются иные инженерно-технические решения и (или) меры безопасности, компенсирующие их отсутствие, в соответствии с настоящей Инструкцией.

Срок завершения мероприятий по оснащению объекта инженерно-техническим оборудованием составляет не более 6 (шести) месяцев с момента получения уведомления о придании объекту статуса уязвимого в террористическом отношении.

Инженерно-техническое оборудование объекта поддерживается в рабочем состоянии.

По решению собственника, владельца, руководителя или иных должностных лиц объектов, уязвимых в террористическом отношении, на объекте устанавливаются дополнительные инженерно-технические оборудования.

Параграф 2. Требования к оснащению объектов, уязвимых в террористическом отношении, инженерно-техническим оборудованием в области наземной космической инфраструктуры

57. К объектам наземной космической инфраструктуры относятся:

1) научно-технологическая и опытно-экспериментальная база космических исследований;

2) средства производства космической техники и космических ракетных комплексов, предназначенных для обеспечения космической деятельности;

3) космодромы;

4) районы падения отделяющихся частей ракет-носителей;

5) наземные комплексы управления космическими объектами;

6) наземные целевые комплексы для приема информации от космических объектов, ее обработки и распространения.

58. В соответствии с подпунктом 2) пункта 1 статьи 20 Закона Республики Казахстан "О космической деятельности" (далее – Закон о космической деятельности) объекты наземной космической инфраструктуры являются объектами космической инфраструктуры Республики Казахстан.

Согласно пункту 2 статьи 20 Закона о космической деятельности, объекты космической инфраструктуры являются стратегическими объектами.

В соответствии с пунктом 2 статьи 193-1 Гражданского кодекса Республики Казахстан объекты космической инфраструктуры включаются в Перечень стратегических объектов.

В соответствии с подпунктом 4-3) пункта 6 Правил определения объектов, подлежащих государственной охране, утвержденных постановлением Правительства Республики Казахстан от 7 октября 2011 года № 1151 (далее – Правила определения объектов, подлежащих государственной охране), объекты космической инфраструктуры подлежат государственной охране.

59. Объекты наземной космической инфраструктуры, включенные в Перечень объектов Республики Казахстан, подлежащих государственной охране, охраняются специализированными охранными подразделения Министерства внутренних дел Республики Казахстан.

Для охраны объектов наземной космической инфраструктуры, не включенных в Перечень объектов Республики Казахстан, подлежащих государственной охране, заключаются договоры об оказании охранных услуг с частными охранными организациями, имеющими лицензию по подвиду деятельности: "Все виды охранных услуг, в том числе охрана объектов, уязвимых в террористическом отношении".

60. Объекты космической инфраструктуры, включенные в Перечень объектов Республики Казахстан, подлежащих государственной охране, оснащаются инженерно-техническим оборудованием в соответствии с Правилами определения объектов, подлежащих государственной охране, а также Требований к организации антитеррористической защиты объектов, уязвимых в террористическом отношении.

Объекты космической инфраструктуры, не включенные в Перечень объектов Республики Казахстан, подлежащих государственной охране, оснащаются инженерно-техническим оборудованием в соответствии с Требованиями.

61. В случае невозможности оснастить объекты наземной космической инфраструктуры необходимым инженерно-техническим оборудованием, за исключением охранных систем и систем оповещения, принимаются иные инженерно-технические решения и (или) меры безопасности, компенсирующие их отсутствие.

62. Срок завершения мероприятий по оснащению объекта инженерно-техническим оборудованием составляет не более 6 (шести) месяцев с момента получения уведомления о придании объекту статуса уязвимого в террористическом отношении.

По решению собственника, владельца, руководителя или иных должностных лиц объектов космической инфраструктуры, уязвимых в террористическом отношении, на объектах устанавливается дополнительное инженерно-техническое оборудование.

63. Для оснащения объектов используются инженерно-технические средства:

1) по оборудованию периметра объекта, исключающие несанкционированный доступ и удовлетворяющие режимным условиям объекта: ограждение (физический барьер) периметра, зон и отдельных участков объекта; контрольно-пропускные пункты; противотаранные устройства, укрепленность стен зданий, сооружений объекта, его оконных проемов; средства контроля и управления доступом, ограничения доступа, системы и средства досмотра, освещения;

2) по контролю за обстановкой на объекте: системы и средства связи, оповещения, охранной и тревожной (и/или мобильные либо стационарные средства подачи тревоги – "тревожные кнопки") сигнализации, системы охранные телевизионные, системы противодействия беспилотным летательным аппаратам;

3) обеспечивающие работу систем безопасности: системы и средства резервного, бесперебойного электроснабжения.

Допускается оснащение объектов, уязвимых в террористическом отношении, иным инженерно-техническим оборудованием, прямо не указанным в настоящем пункте, но выполняющим те же задачи и функции или отвечающие тем же целям.

64. Все объекты, уязвимые в террористическом отношении, в обязательном порядке оснащаются системами охранными телевизионными и системами оповещения. Технические требования к системам видеонаблюдения, входящим в систему охранную телевизионную объекта, соответствуют минимальным техническим возможностям систем видеонаблюдения, предусмотренным Правилами национальной системы видеомониторинга.

65. В случае невозможности оснастить объекты инженерно-техническим оборудованием, предусмотренным настоящей главой, за исключением систем, указанных в пункте 66 настоящей Инструкции, принимаются иные инженерно-технические решения и (или) меры безопасности, компенсирующие их отсутствие.

66. По решению руководителя или иных должностных лиц объектов, уязвимых в террористическом отношении, на объекте устанавливается дополнительное инженерно-техническое оборудование.

67. Объекты, имеющие территорию, оборудуются по периметру ограждением, препятствующим свободному проходу лиц и проезду транспортных средств на объект и с объекта.

1) устойчивость к внешним климатическим факторам всех сезонов;

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

68. Объекты с пропускным режимом, предусматривающим ограничение входа (выхода), въезда (выезда) на объект персоналу, посетителям и транспортным средствам, оснащаются контрольно-пропускными пунктами в целях осуществления санкционированного пропуска лиц и транспортных средств.

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

Существуют внешние и (или) внутренние контрольно-пропускные пункты.

Внешний контрольно-пропускной пункт оборудуется ограждением.

69. Объекты оснащаются системами контроля и управления доступом и (или) средствами ограничения доступа в целях обеспечения санкционированного входа в здания, помещения и зоны объекта и (или) выхода из них.

Оснащение объекта системой контроля и управления доступом производится по зонам, предусматривающим различный уровень доступа персонала и посетителей на объект и (или) его зоны (участки).

Системы контроля и управления доступом обеспечивают автоматическую запись и сохранение в течение одного года на носителях информации архива всех событий для их последующей однозначной классификации с целью обеспечения объективного расследования при попытке или возможном совершении акта терроризма, формирования доказательственной базы, проведения расследований при несанкционированных действиях персонала объекта или посторонних лиц.

70. Объекты оснащаются системами охранными телевизионными в целях ведения наблюдения за обстановкой на объекте, а также визуального подтверждения факта несанкционированного проникновения для оценки ситуации и фиксирования действий нарушителей.

Системой охранной телевизионной оборудуются:

1) периметр территории;

2) контрольно-пропускные пункты;

3) зоны досмотра транспорта

4) главные и запасные входы;

5) территория и помещения с потенциально опасными участками, помещения (места), коридоры, ведущие к ним;

Система охранная телевизионная обеспечивает:

1) передачу визуальной информации на мониторы локального пункта наблюдения в специально выделенном помещении подразделения охраны либо пункта централизованной охраны в автоматизированном режиме;

2) сохранение видеоинформации для последующего анализа событий (срок хранения информации составляет не менее 30 суток);

3) оперативный доступ к видеозаписи.

71. Объекты оснащаются системами и средствами охранной и тревожной сигнализации в целях выявления и выдачи извещений о несанкционированном проникновении или попытки проникновения на объект и (или) охраняемую зону объекта.

Структура системы охранной сигнализации определяется исходя из:

1) режима работы объекта;

2) особенностей расположения помещений внутри зданий;

3) количества охраняемых зон.

72. Объекты оборудуются системами и средствами охранного освещения в целях обеспечения их антитеррористической защищенности в темное время суток.

Охранное освещение обеспечивает освещенность объекта в темное время суток в любой точке периметра, образовывая сплошную полосу шириной 3-4 метра, освещенностью не менее 10 люкс.

73. Объекты, находящиеся под охраной, оснащаются системами и средствами связи в целях обмена информацией для управления силами и средствами подразделений охраны.

Система связи обеспечивает двустороннюю радиосвязь между дежурным на пункте охраны и нарядами охраны на территории обслуживания, между нарядами охраны в пределах территории обслуживания.

74. Объекты оснащаются системами и средствами оповещения в целях оперативного информирования персонала и посетителей объекта о возникновении внештатной ситуации (об угрозе совершения или совершения акта терроризма и возникших последствиях) и координации их действий.

Оповещение персонала и посетителей объекта осуществляется с помощью технических средств, которые обеспечивают:

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 персонала и посетителей объекта.

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

75. Объекты оснащаются системами и средствами резервного электроснабжения для обеспечения бесперебойной работы системы охранной и тревожной сигнализации, контроля и управления доступом, освещения, видеонаблюдения. Системы охранной и тревожной сигнализации, контроля и управления доступом содержат источники бесперебойного питания с аккумуляторной поддержкой, обеспечивающие работу оборудования не менее 2 часов при отсутствии основного сетевого питания.

Автономные резервные источники электрического питания обеспечивают работу системы контроля и управления доступом, телевизионной системы видеонаблюдения, охранного и дежурного освещения не менее 24 часов;

76. Инженерно-техническая укрепленность зданий и сооружений объектов обеспечивают труднопреодолимость проникновения нарушителей на объект и внутри него.

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, а также оборудуются другими техническими средствами охраны.

77. На объектах применение средств защиты оконных, дверных проемов зданий (оборудование пулестойкими стеклами, взрывозащитной пленкой, решетками), сооружений, помещений, замков и запирающих устройств, иных инженерно-технических решений обусловлено повышением уровня защищенности объектов, а также компенсировать отсутствие иных инженерно-технических средств.

На транспортных контрольно-пропускных пунктах и иных въездах на территорию объекта в ограждении оборудуются ворота с конструкцией, обеспечивающей их жесткую фиксацию в закрытом положении.

Запирающие и фиксирующие устройства ворот и калиток обеспечивают требуемую защиту от разрушающих воздействий, сохранять работоспособность в диапазонах температур и влажности окружающего воздуха, при прямом воздействии воды, снега, града, песка и других факторов.

78. Технические средства досмотра применяются на объектах для обнаружения оружия, других предметов и веществ, запрещенных к несанкционированному вносу (выносу), ввозу (вывозу) на объект и с объекта.

Оснащение объекта техническими средствами досмотра соответствуют угрозам, характерным для объектов, особенностям его функционирования.

79. По периметру объекты участков с повышенной опасностью оборудуются противотаранными устройствами в целях принудительной остановки транспортных средств.

80. На объектах помещения подразделений охраны рекомендуется размещать на первом этаже зданий. При этом конструкция помещения соответствует требованиям, предъявляемым к конструкции соответствующей категории зданий.

81. Объектам, для которых актуальны угрозы, связанные с доставкой и применением средств террора посредством беспилотных летательных аппаратов (квадрокоптерами), рекомендуется предусматривать системы противодействия беспилотным летательным аппаратам.

Глава 7. Требования к оснащению объектов, уязвимых в террористическом отношении, инженерно-техническим оборудованием в области телекоммуникационных услуг и связи

Параграф 1. Требования к оснащению объектов, уязвимых в террористическом отношении, инженерно-техническим оборудованием в области телекоммуникационных услуг и связи по объектам АО "Казахтелеком"

82. Для акционерного общества "Казахтелеком" и его филиалов используются следующие инженерно-технические средства:

1) по оборудованию периметра объекта:

- системы, компенсирующие отсутствие ограждения по периметру;
- контрольно-пропускные пункты;
- противотаранные устройства;
- системы контроля и управления доступом;
- средства охранного и системы освещения;

2) по контролю за обстановкой на объекте:

- средства и системы связи;
- системы и средства оповещения;
- системы охранной, пожарной и тревожной сигнализации;
- средства и системы охранные телевизионные;
- технические средства досмотра;

3) обеспечивающие работу системы безопасности:

- системы и средства резервного, бесперебойного электроснабжения.

Допускается оснащение объектов, уязвимых в террористическом отношении, иным инженерно-техническим оборудованием, прямо не указанным в настоящем пункте, но выполняющим те же задачи и функции или отвечающие тем же целям.

Системы, компенсирующие отсутствующие ограждения периметра оборудуются для препятствования бесконтрольному проходу лиц и/или проезду транспортных средств в виде инженерно-технической укрепленности самого здания объекта, обеспечивающий барьер для проникновения нарушителей на объект и непосредственно в здание.

Инженерно-техническое укрепление здания включает в себя оборудование постоянными или съемными решетками, крышками, дверями с запирающими устройствами или другими техническими средствами охраны, все подземные и надземные коммуникации, имеющие входы или выходы в виде колодцев, люков, шахт, открытых трубопроводов, каналов и других подобных сооружений, через которые можно проникнуть в здание и сооружения объекта.

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

Автотранспортный контрольно-пропускной пункт располагается при въезде на территорию объектов акционерного общества "Казахтелеком" и его филиалов и имеет круговой обзор.

Контрольно-пропускной пункт оборудуется техническими системами безопасности (пультами, видеоконтрольными устройствами охранного телевидения), устройствами управления механизма открывания прохода (проезда).

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 наличие металлов.

Контрольно-пропускной пункт для транспортных средств оборудуется типовыми раздвижными или распашными воротами и, или, шлагбаумами с электроприводом и дистанционным управлением, для их аварийной остановки и открытия вручную.

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

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

В случае размещения объекта в одном здании контрольно-пропускной пункт оборудуется внутри здания вблизи центрального входа, а автотранспортный контрольно-пропускной пункт оборудуется со стороны заезда транспортных средств к зданию.

При отсутствии прилегающей территории автотранспортный контрольно-пропускной пункт не оборудуется.

На объектах акционерного общества "Казахтелеком" и его филиалов за поддержание соответствующего пропускного и внутриобъектового режима ответственность возлагается, в рамках компетенций, на Службу внутренней безопасности, Департамент административно-хозяйственной деятельности, структурные подразделения акционерного общества "Казахтелеком" и его филиалов, а также на субъект охранной деятельности, заключивший договор по охране объекта.

На объектах акционерного общества "Казахтелеком" и его филиалов обеспечение пропускного и внутриобъектового режима осуществляется сотрудниками частных охранных организаций, имеющих соответствующие лицензии.

84. Система контроля и управления доступом обеспечивает:

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

2) фиксацию времени прихода и ухода каждого сотрудника;

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

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

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

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

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

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

9) 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;

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

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

12) регистрацию и протоколирование текущих и тревожных событий в система контроля и управления доступом.

Считыватели выполняют 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.

Устройства управления выполняют следующие функции:

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

2) введение базы 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) контроль исправности состояния преграждающих устройств, считывателей и линий связи;

Оснащение объекта система контроля и управления доступом производится во второй и третьей зонах доступа, из трех основных:

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 обязан осуществляться:

1) в первой зоне доступа – неограниченно;

2) во второй зоне доступа – по одному признаку идентификации (например, электронная карточка);

3) в третьей зоне доступа – по двум и более признакам идентификации (например, электронная карточка, механический ключ).

Системой контроля и управления доступом необходимо оборудовать:

1) главный и служебные входы на объект;

2) другие помещения (по усмотрению руководства).

85. Сеть охранного освещения по периметру разделяется на самостоятельные участки.

Приборы освещения необходимо располагать так, чтобы не ослеплять контролеров контрольно-пропускного пункта.

Расстояние между светильниками, их мощность и конструкция выбираются из расчета норм освещенности.

Охранное освещение обеспечивается:

1)необходимой равномерной освещенностью охраняемой территории;

2) возможностью управления освещением - включение освещения любого участка или всего периметра.

Светильники охранного освещения устанавливаются в удобных и безопасных местах для их обслуживания.

86. Система оперативной связи обеспечивает:

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

2) двустороннюю радиосвязь между дежурным на пунктах 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 объектах акционерного общества "Казахтелеком" и его филиалов 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.

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

87. Система оповещения осуществляет:

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 о гражданской защите.

На объекте разрабатывается 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) алгоритмы действия сотрудников при внештатных ситуациях;

3) планы эвакуации;

4) систему сигналов оповещения.

Эвакуация людей в ходе действия системы оповещения сопровождается:

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.

Сигналы оповещения отличаются от сигналов другого назначения.

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

На охраняемой территории применять рупорные громкоговорители. Они устанавливаются 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.

Коммуникации систем оповещения допускается проектировать совмещенными с радиотрансляционной сетью объекта.

88. 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), расположенные на первом и последнем этажах по периметру здания объекта.

Система охранной сигнализации, являющаяся объектом технического регламента (технических регламентов) Евразийского экономического союза или Республики Казахстан проходит оценку соответствия требованиям данного технического регламента (технических регламентов).

Системой охранной сигнализации оборудуются объемы помещений.

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.

Тревожные извещения выводятся на пульт централизованного наблюдения или пульт внутренней охраны объекта.

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

89. Телевизионная система видеонаблюдения обеспечивает:

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) сохранение видеоинформации для последующего анализа событий (срок хранения информации обязан составлять не менее 30 (тридцать) суток);

3) видеофиксация событий в автоматическом режиме;

4) воспроизведение ранее записанной информации;

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

На объекте телевизионной системой видеонаблюдения оборудуются:

1) периметр территории;

2) контрольно-пропускные пункты;

3) главные и запасные входы;

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

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

Видеокамеры, предназначенные для контроля территории объекта или периметра находятся в функциональном состоянии, с учетом условий воздействия климатических факторов для наружных установок в соответствии с климатической зоной, с размещением в герметичных термокожухах, обеспечивающих работоспособность при воздействии климатических факторов.

В темное время суток, если освещенность охраняемой зоны ниже чувствительности телекамер, включается охранное освещение видимого диапазона света. Зоны охранного освещения совпадают с зоной обзора телекамер.

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

Технические требования к системам видеонаблюдения, входящим в систему охранную телевизионную объекта и минимальные технические возможности систем видеонаблюдения соответствуют требованиям, предусмотренным Правилами национальной системы видеомониторинга.

90. Технические средства досмотра применяются на объектах для обнаружения оружия, других предметов и веществ, запрещенных к несанкционированному вносу/выносу, ввозу/вывозу на объект и с объекта.

Оснащение объекта техническими средствами досмотра соответствует угрозам, характерным для объектов, особенностям его функционирования.

В перечень технических средств досмотра входят:

1) металлодетекторы ручные;

2) металлодетекторы арочного или стоечного типа.

Металлодетекторы обеспечивают обнаружение холодного и огнестрельного оружия , металлосодержащих взрывных устройств (гранат), запрещенных к проносу различных видов металлосодержащих предметов и выполнены в виде стационарных устройств арочного или стоечного типа, либо в виде портативных ручных приборов.

91. В случае невозможности оснастить объекты необходимым инженерно-техническим оборудованием, за исключением систем охранных

телевизионных и систем оповещения, принимаются иные инженерно-технические решения и (или) меры безопасности, компенсирующие их отсутствие, в соответствии с инструкцией.

Срок завершения мероприятий по оснащению объекта инженерно-техническим оборудованием составляет не более 6 (шести) месяцев с момента получения уведомления о придании объекту статуса уязвимого в террористическом отношении.

Инженерно-техническое оборудование объекта поддерживается в рабочем состоянии.

По решению собственника, владельца, руководителя или иных должностных лиц объектов, уязвимых в террористическом отношении, на объекте устанавливается дополнительное инженерно-техническое оборудование.

Параграф 2. Требования к оснащению объектов, уязвимых в террористическом отношении, инженерно-техническим оборудованием в области телекоммуникационных услуг и связи по объектам АО "Казпочта"

92. Для оснащения объектов акционерного общества "Казпочта" и его филиалов используются следующие инженерно-технические средства:

1) по контролю за обстановкой на объекте:

системы контроля и управления доступом;

средства и системы связи;

системы и средства оповещения;

системы охранной, пожарной и тревожной сигнализации;

средства и системы охранные телевизионные;

технические средства досмотра;

2) обеспечивающие работу системы безопасности:

системы и средства резервного, бесперебойного электроснабжения.

Допускается оснащение объектов акционерного общества "Казпочта" и его филиалов, уязвимых в террористическом отношении, иным инженерно-техническим оборудованием, прямо не указанным в настоящем пункте, но выполняющим те же задачи и функции или отвечающие тем же целям.

93. Инженерно-техническое укрепление здания включает в себя оборудование с постоянными или съемными решетками, крышками, дверями с запирающими устройствами или другими техническими средствами охраны для помещений расчҰтных касс и оружейных комнат.

94. Количество контрольно-пропускных пунктов определяется с учетом обеспечения необходимой пропускной способности людей.

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

несанкционированного прохода людей с возможностью использования функции "FACE ID".

Допускается оборудовать контрольно-пропускной пункт стационарными и ручными средствами для производства досмотра, способными распознавать различные типы металлов.

Контрольно-пропускной пункт для автотранспортных 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).

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

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

В случае размещения объекта в одном здании контрольно-пропускной пункт оборудуется внутри здания вблизи центрального входа, а автотранспортный контрольно-пропускной пункт оборудуется со стороны заезда автотранспортных средств к зданию.

При отсутствии прилегающей территории автотранспортный контрольно-пропускной пункт не оборудуется.

На объектах акционерного общества "Казпочта" и его филиалов за поддержание соответствующего пропускного и внутриобъектового режима ответственность возлагается в рамках компетенций на Службу внутренней безопасности, Подразделение по защите государственных секретов, Департамент административно-хозяйственной деятельности, структурные подразделения акционерного общества "Казпочта" и его филиалов, а также на субъект охранной деятельности, заключивший договор по охране объекта.

95. Система контроля и управления доступом обеспечивает:

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.

Считыватели выполняют 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.

Устройства управления выполняют следующие функции:

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

2) введение базы 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.

Система контроля и управления доступом обеспечивается защитой от манипулирования путем перебора или подбора идентификационных признаков, а конструкция, внешний вид и надписи на составных частях не приводят к раскрытию применяемых кодов.

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.

Системой контроля и управления доступом необходимо оборудовать:

1) служебные входы на объект;

2) двери в специальные служебные помещения;

3) двери помещений пульта централизованного наблюдения;

4) другие помещения по усмотрению руководства.

96. Система оперативной связи обеспечивает:

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 объектах акционерного общества "Казпочта" и его филиалов 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.

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

97. Система оповещения осуществляет:

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 о гражданской защите.

На объекте разрабатывается 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) алгоритмы действия сотрудников при внештатных ситуациях;

3) планы эвакуации;

4) систему сигналов оповещения.

Эвакуация людей в ходе действия системы оповещения сопровождается:

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).

Сигналы оповещения отличаются от сигналов другого назначения.

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

На охраняемой территории применяются рупорные громкоговорители. Они устанавливаются 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.

Коммуникации систем оповещения допускается проектировать совмещенными с радиотрансляционной сетью объекта.

98. Системой охранной сигнализации оборудуются все помещения с постоянным или временным хранением секретной информации, конфиденциальной информации и 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.

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.

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.

Тревожные извещения с охраняемых зон выводятся на пульт централизованного наблюдения или пульт внутренней охраны объекта.

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

99. Телевизионная система видеонаблюдения обеспечивает:

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) сохранение видеоинформации для последующего анализа событий (срок хранения информации обязан составлять не менее 30 (тридцать) суток);

3) видео документирование 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;

6) возможность подключения к информационным подсистемам Центров оперативного управления, либо передачу видеоизображения в дежурные части территориальных органов полиции.

На объекте телевизионной системой видеонаблюдения оборудуются:

1) периметр территории;

2) контрольно-пропускные пункты;

3) главные и запасные входы;

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

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

Видеокамеры, предназначенные для контроля территории объекта или периметра обеспечиваются в рабочем состоянии, с учетом условий воздействия климатических факторов для наружных установок в соответствии с климатической зоной расположения объекта.

100. Технические средства досмотра применяются на объектах для обнаружения оружия, других предметов и веществ, запрещенных к несанкционированному вносу (выносу), ввозу (вывозу) на объект и с объекта.

Оснащение объекта техническими средствами досмотра соответствует угрозам, характерным для объектов, особенностям его функционирования. Перечень объектов акционерного общества "Казпочта" и его филиалов, подлежащих оснащению средствами досмотра, разрабатывается Управлением внутренней безопасности и утверждается Председателем Правления акционерного общества "Казпочта" и его филиалов.

101. Системы и средства резервного, бесперебойного электроснабжения обеспечивает системы охранной сигнализации, контроля и управления доступом источниками бесперебойного питания с аккумуляторной поддержкой, обеспечивающие работу оборудования не менее 12 (двенадцати) часов при отсутствии основного сетевого питания.

Автономные резервные источники электрического питания обеспечивают работу системы контроля и управления доступом, телевизионной системы видеонаблюдения, охранного и дежурного освещения - в городах и поселках городского типа – не менее 24 (двадцати четырех) часов.

102. В случае невозможности оснастить объекты необходимым инженерно-техническим оборудованием, за исключением систем охранных телевизионных и систем оповещения, принимаются иные инженерно-технические решения и (или) меры безопасности, компенсирующие их отсутствие, в соответствии с инструкцией.

Срок завершения мероприятий по оснащению объекта инженерно-техническим оборудованием составляет не более 6 (шести) месяцев с момента получения уведомления о придании объекту статуса уязвимого в террористическом отношении.

Инженерно-техническое оборудование объекта в обязательном порядке поддерживается в рабочем состоянии, путҰм проведения регламентных работ по техническому обслуживания.

По решению собственника, владельца, руководителя или иных должностных лиц объектов, уязвимых в террористическом отношении, на объекте устанавливается дополнительное инженерно-техническое оборудование.

Приложение 1
к Инструкции по организации
антитеррористической защиты
объектов Министерства
цифрового развития,
инноваций и аэрокосмической
промышленности

Республики Казахстан
и его ведомств, уязвимых в
террористическом отношении

Варианты тематик занятий

1. В рамках проведения теоретических занятий:

1) основные принципы и методы деятельности экстремистских организаций и течений;

2) современный терроризм: формы и методы совершения актов терроризма;

3) государственная система противодействия терроризму;

4) тактика подготовки и совершения актов терроризма;

5) требования законодательства к антитеррористической защите объектов, уязвимых в террористическом отношении;

6) общие признаки взрывных устройств;

2. В рамках проведения инструктажей:

1) детализированное ознакомление служащих, работников объекта службы с порядком действий в обстановке угрозы акта терроризма и (или) его совершения в пределах территории объекта: действия при захвате заложников; Действия при обнаружении подозрительного предмета, похожего на взрывное устройство; Порядок действий при получении анонимного звонка о минировании объекта; Порядок действий при получении устного сообщения о минировании объекта и т.д.

1) порядок использования инженерно-технических средств антитеррористической защиты (для сотрудников, ответственных за обеспечение пропускного режима);

2) порядок техники осмотра помещений, выявления возможных мест закладки взрывных устройств, меры безопасности (для сотрудников, ответственных за обеспечение пропускного режима).

3. В рамках проведения практических занятий:

1) организация оповещения сотрудников, работников, служащих объектов;

2) эвакуация сотрудников, служащих, работников, посетителей объекта и меры безопасности при проведении эвакуации;

3) действия при обнаружении бесхозных вещей, подозрительных предметов;

4) действия сотрудников по информированию территориальных органов внутренних дел и национальной безопасности об угрозе совершения или совершении акта (актов) терроризма;

5) осмотр помещений, выявление возможных мест закладки взрывных устройств (для сотрудников, ответственных за обеспечение пропускного режима).

Примечание: данный перечень не является исчерпывающим.

Руководство объектов при проведении занятий учитывает специфику объекта, включает дополнительные мероприятия или исключает такие, без которых, по его

мнению, не пострадает способность служащих и работников решать задачи при возникновении террористической угрозы.

При выборе темы практических занятий необходимо оценить возможность ее проведения без привлечения специалистов правоохранительных органов и органов национальной безопасности.

Приложение 2
к Инструкции по организации
антитеррористической защиты
объектов Министерства
цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
и его ведомств, уязвимых в
террористическом отношении

Алгоритмы действий различного круга лиц объекта на возможные угрозы террористического характера

Алгоритм по незамедлительному информированию территориальных органов внутренних дел и национальной безопасности Республики Казахстан об угрозе совершения или совершении акта (актов) терроризма

При выявлении основных признаков возможной подготовки и осуществления террористической деятельности:

1) немедленно сообщается в территориальные органы Комитета национальной безопасности или Министерства внутренних дел Республики Казахстан.

Телефон дежурной службы Комитета национальной безопасности: 110.

Телефон единой дежурно-диспетчерской службы: 112.

Телефон дежурной службы органов внутренних дел: 102.

При представлении информации указывают полученные сведения о совершении акта терроризма или об угрозе его совершения, наименование и адрес объекта, время происшествия, наличие пострадавших, их местонахождение и состояние, фамилия, имя и отчество (при его наличии) лица, передающего сообщение, и занимаемая им должность;

2) одновременно подается сигнал посредством нажатия "тревожной кнопки" взаимодействующей охранной организации, которая незамедлительно информирует территориальный орган внутренних дел;

Примечание: отсутствие полных данных не освобождает ответственных лиц от немедленного доклада.

Для оперативного доведения информации уточняются номера телефонов территориальных органов внутренних дел, национальной безопасности, а также Министерства по чрезвычайным пришествиям, аварийно-спасательных и медицинских

учреждений. Обговаривается содержание и форма сообщения о ставших известными фактах готовящихся актов терроризма, подозрительных действиях лиц.

Раздел 1. Алгоритм действий при вооруженном нападении на посетителей и персонал объекта

1. Действия посетителей:

защититься: незаметно покинуть здание или укрыться в помещении, заблокировать дверь, дождаться прибытия сотрудников правопорядка;

по возможности информировать любым способом правоохранительные и (или) специальные государственные органы, охрану, персонал, руководство объекта о факте и обстоятельствах вооруженного нападения.

2. Действия служащих, работников:

по возможности информировать любым способом правоохранительные и (или) специальные государственные органы, охрану, персонал, руководство объекта о факте и обстоятельствах вооруженного нападения;

по возможности провести эвакуацию посетителей, услугополучателей;

защититься: незаметно покинуть здание или укрыться в помещении, заблокировать дверь, дождаться прибытия сотрудников правопорядка.

3. Действия дежурного подразделения:

выявить вооруженного злоумышленника;

по возможности блокировать его продвижение к местам массового пребывания людей на объекте;

информировать любым способом руководство объекта, правоохранительных и (или) специальных государственных органов о факте вооруженного нападения;

принять меры к обеспечению безопасности людей временно/постоянно находящихся на объекте (эвакуация, блокирование внутренних барьеров и другие);

обеспечить собственную безопасность.

4. Действия руководства объекта:

незамедлительное информирование правоохранительных и (или) специальных государственных органов о фактах и обстоятельствах вооруженного нападения;

организация мер обеспечения безопасности людей на объекте (эвакуация, блокирование внутренних барьеров, оповещение о внештатной ситуации на объекте и другие);

взаимодействие с прибывающими силами оперативного штаба по борьбе с терроризмом.

Раздел 2. Алгоритм действий при захвате заложников

5. Действия посетителей:

защититься: избежать попадания в заложники, незаметно покинуть здание или укрыться в помещении, заблокировать дверь, продержаться до прибытия сотрудников правопорядка или возможности безопасности покинуть здание;

по возможности информировать любым доступным способом и только при условии гарантированного обеспечения собственной безопасности правоохранительные и (или) специальные государственные органы об обстоятельствах захвата заложников и злоумышленниках (количество, вооружение, оснащение, возраст, клички, национальность и другие).

6. Действия сотрудников, служащих, работников:

защититься: избежать попадания в заложники, незаметно покинуть здание или укрыться в помещении, заблокировать дверь, продержаться до прибытия сотрудников правопорядка или возможности безопасности покинуть здание;

по возможности информировать любым доступным способом и только при условии гарантированного обеспечения собственной безопасности правоохранительные и (или) специальные государственные органы об обстоятельствах захвата заложников и злоумышленниках (количество, вооружение, оснащение, возраст, клички, национальность и другие).

7. Действия дежурного подразделения:

выявить вооруженного (-ых) злоумышленника (-ов);

по возможности блокировать его/их продвижение к местам массового пребывания людей на объекте;

информировать любым доступным способом руководство объекта, правоохранительные и (или) специальные государственных органов о фактах и обстоятельствах покушения на захват заложников;

принять меры к обеспечению безопасности людей на объекте (эвакуация, блокирование внутренних барьеров на пути злоумышленников и другие);

обеспечить собственную безопасность (избежать попадания в заложники и другие).

8. Действия руководства объекта:

незамедлительное информирование правоохранительных, специальных государственных органов и (или) третьих лиц доступным способом о фактах и обстоятельствах попытки захвата заложников;

по возможности организация мер обеспечения безопасности людей на объекте (эвакуация, блокирование внутренних барьеров, оповещение о внештатной ситуации на объекте и другие);

по возможности организация взаимодействия с прибывающими силами оперативного штаба по борьбе с терроризмом.

9. Действия при захвате в заложники:

успокоится, не паниковать, разговаривать спокойным голосом;

не смотреть в глаза захватчиков, не вести себя вызывающе. Не допускать действий, которые спровоцируют захватчиков к применению физической силы или оружия;

выполнять требования захватчиков, не противоречить им, не допускать истерик и паники;

подготовится физически и морально к возможному суровому испытанию;

не высказывать ненависть и пренебрежение к захватчикам;

с самого начала (особенно в первый час) выполнять все указания захватчиков. Спрашивать разрешения у захватчиков на совершение любых действий;

не привлекать внимания захватчиков своим поведением, не оказывайте активного сопротивления. Это усугубит Ваше положение;

не пытаться бежать, если нет полной уверенности в успехе побега;

запомнить, как можно больше информации о захватчиков (количество, вооружение, как выглядят, особенно внешности, телосложения, акцент, тематика разговора, темперамент, манера поведения);

постараться определить место своего нахождения (заточения);

при наличии возможности, используя любой доступный способ связи, без риска для жизни, проявляя осторожность, попытаться сообщить о произошедшем в правоохранительные или специальные органы, подразделение безопасности или службу охраны объекта;

не пренебрегать пищей, какой бы она ни была. Это поможет сохранить силы и здоровье;

при ранении постараться самостоятельно оказать себе первую медицинскую помощь;

главное не паниковать, даже если захватчики перестали себя контролировать;

расположится подальше от окон, дверей и самих захватчиков. Это обеспечит Вашу безопасность в случае штурма помещения, стрельбы снайперов на поражение захватчиков;

при проведении сотрудниками спецподразделений операции по освобождению заложников целесообразно соблюдать следующие требования:

лечь на пол лицом вниз, по возможности прижавшись к стене, голову закрыть руками и не двигаться;

ни в коем случае не бежать навстречу сотрудникам спецподразделений или от них, так как существует риск принять бегущего заложника за захватчика;

если есть возможность, держитесь подальше от проҰмов дверей и окон;

не возмущаться, если при штурме и захвате с заложниками (до установления личности) поступают некорректно, как с вероятным захватчиком. Отнеситесь с пониманием в случае, если освобожденного заложника обыскивают, связывают, допрашивают. Такие действия спецподразделений (до окончательной идентификации всех лиц и выявления истинных преступников) оправданы.

Раздел 3. Алгоритм действий при закладке взрывных устройств и взрывчатых веществ

10. Признаки, указывающие на взрывное устройство:

наличие на обнаруженном предмете проводов, веревок, изоленты;

подозрительные звуки, щелчки, тиканье часов, издаваемые предметом;

от предмета исходит характерный запах миндаля или другой необычный запах;

необычное размещение обнаруженного предмета;

установленные на обнаруженном предмете различных видов источников питания, проволока, по внешним признакам, схожая с антенной и другие.

11. Действия посетителей при обнаружении подозрительного предмета:

не трогать, не подходить, не передвигать;

опросить окружающих для установления возможного владельца бесхозного предмета;

воздержаться от использования средств радиосвязи, в том числе и мобильных, вблизи данного предмета;

по возможности зафиксировать время и место обнаружения;

немедленно сообщить об обнаружении подозрительного предмета охране, персоналу объекта либо в дежурные части территориальных органов внутренних дел и национальной безопасности;

быть готовым описать внешний вид предмета, похожего на взрывное устройство и значимые обстоятельства его обнаружения;

не сообщать об угрозе взрыва никому, кроме тех, кому необходимо знать о случившемся, чтобы не создавать панику;

укрыться за предметами, обеспечивающими защиту (угол здания, колона, толстое дерево, автомашина и другие);

информирование охраны объекта, правоохранительных и (или) специальных государственных органов о подозрительных лице/ах (количество, внешние признаки наличия самодельного взрывного устройства, оружия, оснащение, возраст, клички, национальность и другие);

покинуть объект, при невозможности – укрыться за капитальным сооружением и на необходимом удалении.

12. Действия сотрудников, работников, служащих при обнаружении подозрительного предмета:

не трогать, не подходить, не передвигать;

опросить окружающих для установления возможного владельца бесхозного предмета;

воздержаться от использования средств радиосвязи, в том числе и мобильных, вблизи данного предмета;

по возможности зафиксировать время и место обнаружения;

немедленно сообщить об обнаружении подозрительного предмета в охране, персоналу объекта либо в дежурные части территориальных органов национальной безопасности и внутренних дел;

быть готовым описать внешний вид предмета, похожего на взрывное устройство и значимые обстоятельства его обнаружения;

не сообщать об угрозе взрыва никому, кроме тех, кому необходимо знать о случившемся, чтобы не создавать панику;

по возможности организовать с охраной ограничение доступа посторонних лиц к подозрительному предмету и опасной зоне;

помочь обеспечить организованную эвакуацию людей с территории, прилегающей к опасной зоне;

укрыться за предметами, обеспечивающими защиту (угол здания, колона, толстое дерево, автомашина и другие), вести наблюдение;

информирование охраны объекта, правоохранительных и (или) специальных государственных органов в случае выявления подозрительного лица или группы лиц, возможно имеющих при себе взрывные устройства или взрывчатые вещества (количество, внешние признаки наличия самодельного взрывного устройства, оружия, оснащение, возраст, клички, национальность и другие);

оказать содействие руководству и охране в организации эвакуации посетителей;

покинуть объект, при невозможности – укрыться за капитальным сооружением и на необходимом удалении.

13. Действия дежурного подразделения при обнаружении подозрительного предмета:

не трогать, не подходить, не передвигать;

опросить окружающих для установления возможного владельца бесхозного предмета;

воздержаться от использования средств радиосвязи, в том числе и мобильных, вблизи данного предмета;

по возможности зафиксировать время и место обнаружения;

немедленно сообщить об обнаружении подозрительного предмета охране, персоналу объекта либо в дежурные части территориальных органов национальной безопасности и внутренних дел;

быть готовым описать внешний вид предмета, похожего на взрывное устройство и значимые обстоятельства его обнаружения;

не сообщать об угрозе взрыва никому, кроме тех, кому необходимо знать о случившемся, чтобы не создавать панику;

обеспечить ограничение доступа посторонних лиц к подозрительному предмету и опасной зоне на необходимом удалении;

обеспечить организованную эвакуацию людей с территории, прилегающей к опасной зоне;

укрыться за предметами, обеспечивающими защиту (угол здания, колона, толстое дерево, автомашина и другие), вести наблюдение;

информирование охраны объекта, правоохранительных и (или) специальных государственных органов в случае выявления подозрительного лица или группы лиц, возможно имеющих при себе взрывные устройства или взрывчатые вещества (количество, внешние признаки наличия самодельного взрывного устройства, оружия, оснащение возраст, клички, национальность и другие).

14. Действия руководства:

незамедлительное информирование правоохранительных, специальных государственных органов о выявлении подозрительного человека или об обнаружении бесхозного предмета;

организация оцепления места обнаружения бесхозного подозрительного предмета на необходимом удалении;

организация эвакуации людей с объекта, оповещение о внештатной ситуации на объекте и другие;

обеспечение обхода помещений и осмотра территорий с целью обнаружения подозрительных предметов;

организация взаимодействия с прибывающими силами оперативного штаба по борьбе с терроризмом, представление необходимой информации.

15. При обнаружении взрывного устройства или предмета, похожего на него, соблюдают следующие расстояния при удалении и организации оцепления:

граната РГД-5 – 50 метров;

граната Ф-1 – 200 метров;

тротиловая шашка массой 200 грамм – 45 метров;

тротиловая шашка массой 400 грамм – 55 метров;

дипломат (кейс) – 230 метров;

дорожный чемодан – 350 метров;

а/машина "легковая" - 460-580 метров;

автобус – 920 метров;

грузовая машина (фургон) – 1240 метров.

Раздел 4. Алгоритм действий при атаке с применением террористов-смертников

16. Действия посетителей:

защититься: незаметно покинуть здание или укрыться в помещении, заблокировать дверь, дождаться прибытия сотрудников правопорядка;

по возможности информировать любым способом правоохранительные и (или) специальные государственные органы, охрану, персонал, руководство объекта о факте и обстоятельствах вооруженного нападения.

17. Действия сотрудников, служащих, работников:

защититься: незаметно покинуть здание или укрыться в помещении, заблокировать дверь, дождаться прибытия сотрудников правопорядка;

по возможности информировать любым способом правоохранительные и (или) специальные государственные органы, охрану, персонал, руководство объекта о факте и обстоятельствах вооруженного нападения.

18. Действия охраны:

по возможности блокировать его/их продвижение к местам массового пребывания людей на объекте;

информировать любым способом руководство объекта, правоохранительные и (или) специальные государственных органов о выявлении подозрительного лица или группы лиц;

принять меры к обеспечению безопасности людей на объекте (эвакуация, блокирование внутренних барьеров);

организовать наблюдение передвижений подозрительного лица или группы лиц по объекту (лично либо через систему видеонаблюдения);

обеспечить собственную безопасность.

19. Действия руководства:

незамедлительная передача информации в правоохранительные и (или) специальные государственные органы о выявлении на объекте подозрительного лица или группы лиц;

предоставление сотрудникам правоохранительных органов максимально полной информации о подозрительном лице, которая сокращает время выявления и задержания злоумышленника;

обеспечение организованной эвакуации людей;

обеспечение собственной безопасности.

Раздел 5. Алгоритм действий при поступлении сообщений о готовящемся акте терроризма

20. Действия получателя угрозы по телефону (руководитель, сотрудник, сотрудник дежурного подразделения):

1) по ходу разговора отметьте пол, возраст звонившего и особенности его речи:

голос (громкий или тихий, низкий или высокий);

темп речи (быстрый или медленный);

произношение (отчетливое, искаженное, с заиканием, шепелявое, с акцентом или диалектом);

манера речи (развязная, с издевкой, с нецензурными выражениями);

2) обратить внимание на звуковой фон (шум автомашин или железнодорожного транспорта, звук теле-или радиоаппаратуры, голоса, другое), характер звонка (городской, междугородный);

3) зафиксируйте точное время начала разговора и его продолжительность;

4) постарайтесь в ходе разговора получить ответы на следующие вопросы:

куда, кому, по какому телефону звонит данный человек?

какие конкретные требования он выдвигает?

выдвигает требования лично или выступает в роли посредника и представляет какую-то группу лиц?

на каких условиях он или они согласны отказаться от задуманного?

как и когда с ним можно связаться?

кому вам необходимо сообщить об этом звонке?

5) постарайтесь добиться от звонящего максимально возможного промежутка времени для принятия вами и руководством решений или совершения каких-либо действий;

6) в процессе разговора или немедленно после окончания разговора сообщить на канал "102" органов внутренних дел или единую дежурно-диспетчерскую службу "112" и руководству организации о телефонной угрозе.

21. В случае поступления в письменном (электронном) виде анонимных сообщений о готовящемся акте терроризма сотрудникам необходимо:

принять меры к сохранности и быстрой передаче письма (записки, электронного носителя) уполномоченному должностному лицу;

по возможности письмо (записку, электронный носитель) положить в полиэтиленовый пакет;

постараться не оставлять на документе отпечатки своих пальцев;

сохранить все: сам документ, конверт, упаковку, любые вложения. Ничего не выбрасывать;

запомнить обстоятельства получения или обнаружения письма (записки, электронного носителя);

незамедлительно информировать дежурного (ответственного, оперативного дежурного).

после получения сообщения незамедлительно сообщить на канал "102" органов внутренних дел или единую дежурно-диспетчерскую службу "112" и руководству организации о информационной угрозе.

Раздел 6. Алгоритм действий в случае получения подозрительных почтовых отправлений

В случае выявления подозрительного почтового отправления сотрудникам Министерства (объекта) необходимо:

не пытаться самостоятельно вскрыть Ұмкость, пакет, контейнер и другие подозрительные предметы;

по возможности не брать в руки подозрительное письмо или бандероль;

сообщить об этом факте руководству Министерства (объекта), территориальным органам санэпиднадзора;

убедиться, что подозрительная почта отделена от других писем и бандеролей;

предпринять меры, исключающие возможность попадания неизвестного вещества из вскрытого отправления в вентиляционную систему здания;

до приезда специалистов поместить подозрительные отправления в герметичную тару (стеклянный сосуд с плотно прилегающей крышкой или в многослойные пластиковые пакеты). При этом следует пользоваться подручными средствами индивидуальной защиты кожи (резиновые перчатки, полиэтиленовые пакеты) и дыхательных путей (респиратор, ватно-марлевая повязка);

до приезда специалистов герметично закрытую тару хранить в недоступном для посторонних людей месте;

составить список всех лиц, кто непосредственно контактировал с подозрительной корреспонденцией (их адреса, телефоны);

лицам, контактировавшим с подозрительной корреспонденцией, неукоснительно выполнить мероприятия личной гигиены (вымыть руки с мылом, по возможности принять душ) и рекомендации медицинских работников по предупреждению заболевания.

Раздел 7. Алгоритм действий должностных лиц объектов Министерства при получении информации от уполномоченных государственных органов об угрозе совершения или совершении акта (актов) терроризма

Наряду с мерами, принимаемыми при установлении уровней террористической опасности в соответствии с Указом Президента Республики Казахстан от 9 августа 2013 года № 611 "Об утверждении Правил организации и функционирования государственной системы мониторинга информации и оповещения населения о возникновении угрозы акта терроризма", руководителями объектов и/или ответственным лицом Министерства применяются следующие меры безопасности:

1) при умеренном ("желтом") уровне террористической опасности:

усиление пропускного режима на объектах Министерства;

усиление режимных мер в ходе проведения досмотровых мероприятий посетителей, персонала и транспортных средств с использованием специальных технических средств;

инструктаж сотрудников, служащих и работников, осуществляющих функции по локализации кризисных ситуаций, с привлечением в зависимости от полученной информации специалистов в соответствующей сфере;

информирование, служащих и работников о возможной угрозе совершений акта терроризма и необходимых действиях;

установление связи (дополнительно по специально выделенным каналам связи) с взаимодействующими правоохранительными и специальными органами;

2) при высоком ("оранжевом") уровне террористической опасности (наряду с мерами, принимаемыми при установлении "желтого" уровня террористической опасности):

проверка готовности служащих и работников, осуществляющих функции по локализации кризисных ситуаций, и отработка их возможных действий по пресечению акта терроризма и спасению людей;

усиление охраны объектов Министерства;

усиление контроля за передвижением транспортных средств по территории объекта , проведение досмотра транспортных средств с применением технических средств обнаружения оружия и взрывчатых веществ;

установление связи (дополнительно по специально выделенным каналам связи) с взаимодействующими правоохранительными и специальными государственными органами;

3) при установлении критического ("красного") уровня террористической опасности (наряду с мерами, применяемыми при введении "желтого" и "оранжевого" уровней террористической опасности):

принятие неотложных мер по спасению людей, содействия бесперебойной работе спасательных служб и формирований;

установление связи (дополнительно по специально выделенным каналам связи) с взаимодействующими правоохранительными и специальными органами;

перевод объекта в чрезвычайный режим или прекращение функционирования объекта Министерства (при необходимости);

прекращение охранной деятельности на объекте (при необходимости).

Приложение 3
к Инструкции по организации
антитеррористической защиты
объектов Министерства
цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
и его ведомств, уязвимых в
террористическом отношении
Форма

Журнал учета учебных мероприятий по антитеррористической подготовке (титульный лист)

_____

(наименование организации)

Журнал № __
учета проведения учебных мероприятий по антитеррористической подготовке

Дата начала ведения журнала "_ "___ 20___ г.
Дата окончания ведения журнала "_ "___20___г. (внутренняя сторона)

Раздел 1. Инструктажи

№ п/п	Дата проведения инструктажа	Ф.И.О.(отчество при наличии) и должность инструктируемого	Вид инструктажа	Ф.И.О. (отчество при наличии)и должность лица, проводившего инструктаж	Подпись инструктируемого	Подпись лица, проводившего инструктаж
1	2	3	4	5	6	7

Раздел 2. Занятия

1. Дата проведения занятия.
2. Тема занятия.
3. Учебные вопросы.
4. Количество присутствующих работников.
5. Подпись лица, проводившего занятия.

Приложение 4
к Инструкции по организации
антитеррористической защиты
объектов Министерства
цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
и его ведомств, уязвимых в
террористическом отношении

Перечень предметов, запрещенных к проносу на объекты, уязвимых в террористическом отношении

1. Взрывчатые вещества, средства взрывания и предметы, ими начиненные:
1) пороха всякие, в любой упаковке и в любом количестве;
2) патроны боевые (в том числе малокалиберные);
3) патроны к газовому оружию;
4) капсюли (пистоны) охотничьи;

5) пиротехнические средства: сигнальные и осветительные ракеты, патроны сигнальные, посадочные шашки, дымовые патроны (шашки), спички подрывника, бенгальские огни, петарды железнодорожные;

6) тротил, динамит, тол, аммонал и другие взрывчатые вещества;

7) капсюли-детонаторы, электродетонаторы, электровоспламенители, детонирующий и огнепроводный шнур и другие.

2. Сжатые и сжиженные газы:

1) газы для бытового пользования (бутан-пропан) и другие газы;

2) газовые баллончики с наполнением нервнопаралитического и слезоточивого воздействия и другие.

3. Воспламеняющиеся твердые вещества:

1) вещества, подверженные самопроизвольному возгоранию;

2) вещества, выделяющие легковоспламеняющиеся газы при взаимодействии с водой: калий, натрий, кальций металлический и их сплавы, кальций фосфористый и другие;

3) фосфор белый, желтый и красный и все другие вещества, относящиеся к категории воспламеняющихся твердых веществ.

4. Едкие и коррозирующие вещества:

1) сильные неорганические кислоты: соляная, серная, азотная и другие;

2) фтористоводородная (плавиковая) кислота и другие сильные кислоты и коррозирующие вещества.

5. Ядовитые и отравляющие вещества:

1) любые ядовитые сильнодействующие и отравляющие вещества в жидком или твердом состоянии, упакованные в любую тару;

2) все соли синильной кислоты и цианистые препараты;

3) циклон, цианплав, мышьяковистый ангидрид и другие;

4) другие опасные вещества, предметы и грузы, которые могут быть использованы в качестве орудия нападения на сотрудников объекта, а также создающие угрозу для объекта.

6. Оружие: пистолеты, револьверы, винтовки, карабины и другое огнестрельное, газовое, пневматическое оружие, электрошоковые устройства, кортики, стилеты, десантные штык-ножи.