

Об утверждении требований к антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федерального агентства связи, Федерального агентства по печати и массовым коммуникациям, а также подведомственных им организаций, и формы паспорта безопасности таких объектов (территорий)

Постановление Правительства Российской Федерации · № 1130 · от 30.10.2014 · Правительство Российской Федерации · Утратил силу

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОСТАНОВЛЕНИЕ
ОТ 30 ОКТЯБРЯ 2014 Г. № 1130
МОСКВА

Утратило силу - Постановление Правительства Российской Федерации от 08.06.2023 № 944

Об утверждении требований к антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также подведомственных им организаций, и формы паспорта безопасности таких объектов (территорий)

В соответствии с пунктом 4 части 2 статьи 5 Федерального закона "О противодействии терроризму" Правительство Российской Федерации постановляет:

Утвердить прилагаемые:

требования к антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также подведомственных им организаций;

форму паспорта безопасности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также подведомственных им организаций.

Председатель Правительства
Российской Федерации Д.Медведев

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от 30 октября 2014 г. № 1130

ТРЕБОВАНИЯ

к антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых

коммуникаций, а также подведомственных им организаций

I. Общие положения

1. Настоящие требования определяют порядок обеспечения антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, их территориальных органов и подведомственных им организаций (далее соответственно - органы (организации), объекты (территории), включая вопросы инженерно-технической укреплённости объектов (территорий), оснащения их техническими средствами и иные вопросы, влияющие на уровень антитеррористической защищенности объектов (территорий).

2. Для целей настоящих требований под объектами (территориями) понимаются комплексы технологически и технически связанных между собой зданий, строений, сооружений и систем, отдельные здания, строения и сооружения, линии связи, правообладателем которых являются органы (организации).

3. Настоящие требования распространяются на объекты (территории) организаций, относящихся к сфере деятельности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

4. Настоящие требования не распространяются:

на объекты (территории), подлежащие обязательной охране войсками национальной гвардии Российской Федерации;

на важные государственные объекты, специальные грузы, сооружения на коммуникациях, подлежащие охране войсками национальной гвардии Российской Федерации, в части их оборудования инженерно-техническими средствами охраны, порядка контроля за оборудованием и эксплуатацией указанных инженерно-технических средств охраны.

(Пункт в редакции Постановления Правительства Российской Федерации от 22.03.2018 № 319)

II. Категорирование объектов (территорий) и порядок его проведения

5. В целях установления дифференцированных требований по обеспечению антитеррористической защищенности объектов (территорий) осуществляется их категорирование.

6. Категорирование объектов (территорий) осуществляется на основании оценки состояния защищенности объектов (территорий), учитывающей их значимость для инфраструктуры и жизнеобеспечения, степень потенциальной опасности и угрозы совершения террористического акта на объектах (территориях), а также возможных последствий его совершения.

Степень угрозы совершения террористического акта определяется на основании данных о совершенных и предотвращенных террористических актах. Возможные последствия совершения террористического акта на объекте (территории) определяются на основании прогнозных показателей о количестве работников органа (организации), эксплуатирующих объект (территорию), и количестве людей, которые могут погибнуть или получить вред здоровью, о возможном материальном ущербе и ущербе окружающей природной среде в районе нахождения объекта (территории).

7. Категорирование объекта (территории) организуется руководителем органа (организации), являющегося правообладателем объекта (территории).

8. Руководителем органа (организации), являющегося правообладателем объекта (территории), назначается комиссия по категорированию объекта (территории) (далее - комиссия). В состав комиссии включаются работники органа (организации), являющегося правообладателем объекта (территории), представители территориального органа безопасности и территориального органа Федеральной службы войск национальной гвардии Российской Федерации или подразделения

вневедомственной охраны войск национальной гвардии Российской Федерации (по согласованию). К работе комиссии могут привлекаться эксперты из числа работников специализированных организаций в области проектирования и эксплуатации технологических систем и специализированных организаций, имеющих право осуществлять экспертизу безопасности объектов (территорий).

9. Результаты работы комиссии оформляются актом категорирования объекта (территории), который составляется в одном экземпляре, подписывается всеми членами комиссии и хранится вместе с первым экземпляром паспорта безопасности объекта (территории).

10. В зависимости от степени угрозы совершения на объектах (территориях) террористических актов и возможных последствий их совершения и с учетом оценки состояния защищенности объектов (территорий) устанавливаются следующие категории объектов (территорий):

а) объекты (территории) категории 1 - объекты (территории) федерального и межрегионального значения, противоправные действия на которых могут нанести ущерб государственной безопасности страны, привести к особо крупному экономическому ущербу, в том числе:

административные здания, занимаемые центральным аппаратом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций;

узлы связи сетей междугородной и международной связи;

узлы связи в составе наземных станций сопряжения сети подвижной спутниковой радиосвязи, объекты космической связи;

международные транзитные узлы связи (сети передачи данных);

международные транзитные узлы телеграфной связи;

центры обработки данных, обеспечивающие обработку и хранение данных государственных информационных систем класса K1;

эксплуатационно-технические здания и линейно-кабельные сооружения объектов (территорий), обеспечивающих работу телекоммуникационных сетей и систем на территории более одного субъекта Российской Федерации;

главпочтамты и иные объекты почтовой связи, на территории которых при определенных условиях могут одновременно находиться более 400 человек;

объекты телерадиовещания и средств массовой информации, осуществляющие (обеспечивающие) вещание и эфирную наземную трансляцию общероссийских обязательных общедоступных телерадиоканалов на территории 2 и более субъектов Российской Федерации;

объекты средств массовой информации, осуществляющие (обеспечивающие) вещание общероссийских обязательных общедоступных телерадиоканалов на территории 2 и более субъектов Российской Федерации;

эксплуатационно-технические здания и линейно-кабельные сооружения режимных объектов связи;

представительства международных организаций;

хранилища секретных документации, изделий;

комнаты хранения оружия;

б) объекты (территории) категории 2 - объекты (территории) регионального значения, противоправные действия на которых могут привести к экономическому ущербу в отношении промышленных предприятий, организаций социальной сферы и других организаций, в том числе: административные здания, сооружения и территория, занимаемые территориальными органами Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также организациями, находящимися в ведении указанных федеральных органов исполнительной власти;

сети зоновой телефонной связи, узлы связи сетей местной телефонной связи с количеством портов

от 5000, а также транзитные и оконечно-транзитные узлы связи сетей местной телефонной связи, которые соединяются с узлами обслуживания вызовов экстренных оперативных служб;

узлы связи сети подвижной радиосвязи, узлы связи сети подвижной радиотелефонной связи;

транзитные узлы связи;

узлы сети передачи данных суммарной емкостью более 100 Гбит/с;

междугородные узлы телеграфной связи;

центры обработки данных, обеспечивающие обработку и хранение данных государственных информационных систем класса К2;

объекты почтовой связи, на территории которых при определенных условиях могут одновременно находиться от 100 до 400 человек;

объекты телерадиовещания и средств массовой информации, осуществляющие (обеспечивающие) вещание и эфирную наземную трансляцию общероссийских обязательных общедоступных телерадиоканалов на территории одного субъекта Российской Федерации с охватом населения свыше 100 тыс. человек;

объекты средств массовой информации, осуществляющие (обеспечивающие) вещание общероссийских обязательных общедоступных телерадиоканалов на территории одного субъекта Российской Федерации;

объекты, в которых хранятся или размещаются денежные средства и (или) товарно-материальные ценности на сумму более 10 млн. рублей;

в) объекты (территории) категории 3 - локальные объекты (территории), противоправные действия на которых могут привести к выводу из строя или ограничению деятельности объектов категории 1 и 2, в том числе:

узлы связи сети местной телефонной связи с количеством портов до 5000;

оконечные узлы связи, оконечно-транзитные узлы связи (сети передачи данных);

зоновые узлы телеграфной связи;

центры обработки данных, обеспечивающие обработку и хранение данных государственных информационных систем класса К3;

объекты почтовой связи, на территории которых при определенных условиях может одновременно находиться от 50 до 100 человек;

объекты телерадиовещания и средств массовой информации, осуществляющие (обеспечивающие) вещание и эфирную наземную трансляцию общероссийских обязательных общедоступных телерадиоканалов, не вошедшие в 1 и 2 категории;

объекты, предназначенные для хранения денежных средств, в том числе кассы предприятий и учреждений;

линейно-кабельные сооружения объектов связи общего назначения;

вспомогательно-технические здания;

складские помещения для оборудования, содержащего драгоценные металлы;

автономные (не обслуживаемые) объекты;

объекты, в которых хранятся или размещаются изделия технологического назначения, нормативно-техническая документация и другое имущество;

объекты, в которых хранятся или размещаются компьютерная техника, оргтехника, видео- и аудиотехника, автомобили и запасные части к ним, и другое аналогичное имущество.

11. Объекты (территории), не указанные в пункте 10 настоящих требований, категоризируются по ближайшему аналогу с учетом степени их потенциальной опасности и возможных последствий совершения на них террористических актов.

12. В случае если в составе одного объекта (территории) находятся несколько объектов (территорий), отнесенных к различным категориям, либо сам объект (территорию) можно отнести к различным категориям, такой объект (территория) относится к наиболее высокой категории.

13. Потенциально опасные объекты (территории), совершение террористического акта на которых может привести к возникновению чрезвычайных ситуаций с опасными социально-экономическими последствиями, относятся к объектам категории 1.

14. На каждом объекте (территории) независимо от его категории выделяются критические элементы, совершение террористического акта на которых приведет к прекращению нормального функционирования объекта (территории), его повреждению или аварии на объекте (территории).

III. Мероприятия по обеспечению антитеррористической защищенности объектов (территорий)

15. Ответственность за обеспечение антитеррористической защищенности объектов (территорий) возлагается на руководителей органов (организаций), являющихся правообладателями объектов (территорий).

16. Антитеррористическая защищенность объектов (территорий) обеспечивается путем осуществления мероприятий в целях:

а) воспрепятствования неправомерному проникновению на объекты (территории), что достигается посредством:

установления пропускного и внутриобъектового режимов;

обеспечения установленных требований по инженерно-технической оснащенности и укреплённости объектов (территорий);

проведения иных мероприятий, направленных на предупреждение и пресечение преступлений и административных правонарушений на объектах (территориях);

б) выявления потенциальных нарушителей режимов, установленных на объектах (территориях), и (или) признаков подготовки или совершения террористического акта, что достигается посредством: неукоснительного соблюдения на объектах (территориях) пропускного и внутриобъектового режимов;

контроля за текущей обстановкой на объектах (территориях) и близлежащей территории на предмет выявления посторонних лиц и подозрительных предметов, лиц, осуществляющих наблюдение за объектами (территориями), сбор сведений об объектах (территориях);

постоянного анализа поступающей информации о социально-политической, криминогенной обстановке в регионе, сведений об угрозах совершения или о совершении террористических актов на территории региона;

в) пресечения попыток совершения террористических актов на объектах (территориях), что достигается посредством:

проведения специальных занятий с работниками объектов (территорий) о порядке действий при появлении признаков совершения террористического акта или возникновении угрозы его совершения;

взаимодействия с территориальными органами безопасности, территориальными органами Министерства внутренних дел Российской Федерации и территориальными органами Федеральной службы войск национальной гвардии Российской Федерации, а также с подразделениями охраны объектов (территорий) по вопросам антитеррористической защищенности;

постоянного контроля за установленным порядком доступа на объекты (территории) посетителей и транспортных средств;

г) минимизации возможных последствий и ликвидации угроз террористических актов на объектах (территориях), что достигается посредством:

обеспечения достаточного уровня подготовки работников объектов (территорий) по вопросам антитеррористической защищенности объектов (территорий);

неукоснительного соблюдения настоящих требований;

своевременного информирования органов (организаций), в ведении которых находятся объекты (территории), территориальных органов безопасности, территориальных органов Министерства

внутренних дел Российской Федерации и территориальных органов Федеральной службы войск национальной гвардии Российской Федерации (далее - уполномоченные органы) об угрозе или совершении террористического акта;

оперативного оповещения и проведения эвакуации работников и посетителей объектов (территорий);

слаженного взаимодействия в работе с уполномоченными органами, территориальными органами Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, а также с подразделениями охраны объектов (территорий);

д) обеспечения защиты служебной информации ограниченного распространения, содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации, в том числе служебной информации ограниченного распространения о принимаемых мерах по антитеррористической защищенности объекта (территории), что достигается посредством:

установления порядка работы со служебной информацией ограниченного распространения;

ограничения доступа должностных лиц (работников) и иных лиц к служебной информации ограниченного распространения, содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации;

определения обязанностей лиц, допущенных к служебной информации ограниченного распространения, в том числе лиц, ответственных за хранение паспорта безопасности объекта (территории), иных документов и других материальных носителей информации, содержащих сведения о состоянии антитеррористической защищенности объекта (территории) и принимаемых мерах по ее усилению;

обеспечения надлежащего хранения и использования служебной информации ограниченного распространения, в том числе содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации;

организации и осуществления контроля за обеспечением установленного порядка работы со служебной информацией ограниченного распространения и ее хранения в целях выявления и предупреждения возможной утечки служебной информации ограниченного распространения, в том числе содержащейся в паспорте безопасности объекта (территории), иных документах и на других материальных носителях информации;

подготовки и переподготовки должностных лиц (работников) по вопросам работы со служебной информацией ограниченного распространения;

(Подпункт дополнен - Постановление Правительства Российской Федерации от 22.03.2018 № 319)

е) выявления и предотвращения несанкционированного проноса (провоза) и применения на объекте (территории) токсичных химикатов, отравляющих веществ и патогенных биологических агентов, в том числе при их получении посредством почтовых отправлений, что достигается посредством: определения и оборудования техническими средствами специальных мест для проверки вносимого (ввозимого) имущества и почтовых отправлений;

установления порядка проведения проверки и действий в случае выявления токсичных химикатов, отравляющих веществ и патогенных биологических агентов и назначения лиц, ответственных за проведение проверки;

оборудования карантинного хранилища для размещения обнаруженных подозрительных предметов и корреспонденции;

подготовки и переподготовки должностных лиц (работников) по вопросам работы по выявлению и предотвращению несанкционированного проноса (провоза) и применения на объекте (территории) токсичных химикатов, отравляющих веществ и патогенных биологических агентов, в том числе при их получении посредством почтовых отправлений.

(Дополнено подпунктом - Постановление Правительства Российской Федерации от 22.01.2020 № 30)

17. В целях обеспечения необходимой степени антитеррористической защищенности объектов (территорий) с учетом присвоенной им категории осуществляются следующие мероприятия:

а) в отношении объектов (территорий) категории 3:

организация охраны объекта (территории) с использованием технических средств и групп быстрого реагирования;
обеспечение инженерно-технической укреплённости зданий, строений и сооружений;
организация внутриобъектового режима;
оборудование зданий, строений и сооружений, включая периметр объекта (территории), техническими системами охранной и тревожной сигнализации;
оборудование зданий, строений и сооружений техническими системами пожарной сигнализации;
оборудование зданий, строений и сооружений системой видеонаблюдения (охранного телевидения);
подготовка персонала к действиям в условиях угрозы и совершения террористического акта;
обмен информацией и оперативное оповещение уполномоченных органов и территориальных органов Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий об угрозе и (или) о совершении террористического акта, а также о действиях по минимизации и (или) ликвидации последствий совершения террористического акта;
проведение совместных учений (тренировок) с уполномоченными органами (по согласованию) по отработке действий при получении информации об угрозе или о совершении на объекте (территории) террористического акта;

б) в отношении объектов (территорий) категории 2 дополнительно к мероприятиям, предусмотренным подпунктом "а" настоящего пункта:

организация физической защиты объекта (территории) с использованием специальных средств;
организация пропускного режима;
оборудование ограждения периметра объекта (территории);
оборудование системы контроля управления доступом;
оборудование охранного освещения;
оборудование системы оповещения (извещения);

в) в отношении объектов (территорий) категории 1 дополнительно к мероприятиям, предусмотренным подпунктами "а" и "б" настоящего пункта:

организация вооруженной охраны объекта (территории);
оборудование подъездов (дороги, участки местности) к периметру объекта (территории) и (или) контрольно-пропускным пунктам, через которые может быть совершен прорыв транспортных средств, противотаранными устройствами и иными заградительными сооружениями.

18. Должностным лицом, осуществляющим руководство деятельностью объекта (территории) (далее - руководитель объекта) может быть принято решение об использовании мер антитеррористической защищенности объекта (территории) по более высокой категории.

19. Система антитеррористической защищенности объектов (территорий) должна обеспечивать возможность:

а) проверки у лиц, находящихся на объектах (территориях), документов, удостоверяющих их личность, а также документов, дающих право на вход (выход) лиц, въезд (выезд) транспортных средств, внос (вынос), ввоз (вывоз) имущества;

б) проведения осмотра и досмотра транспортных средств при их въезде (выезде);

в) задержания и доставления в служебное помещение охраны организации, находящейся в ведении Федеральной службы войск национальной гвардии Российской Федерации, или орган внутренних дел лиц, совершивших преступления или административные правонарушения;

г) применения физической силы, специальных средств и огнестрельного оружия в случаях и в

порядке, которые установлены законодательством Российской Федерации;

д) беспрепятственного входа в помещения объектов (территорий) и осмотра их при преследовании лиц, незаконно проникших на объекты (территории), а также для задержания лиц, подозреваемых в совершении преступлений;

е) оперативной ликвидации последствий террористических актов.

20. К инженерно-технической укрепленности объектов (территорий), применяемым на объектах (территориях) техническим средствам охранной, тревожной и пожарной сигнализации, контроля и управления доступом, систем оповещения и охранного освещения, а также к электроснабжению технических систем безопасности объектов (территорий) предъявляются требования согласно приложению.

21. При получении информации об угрозе совершения террористического акта для своевременного и адекватного реагирования на возникающие террористические угрозы, предупреждения совершения террористических актов, направленных против объектов (территорий), осуществляются мероприятия, предусмотренные соответствующим режимом усиления противодействия терроризму.

22. Режимы усиления противодействия терроризму предусматривают выполнение мероприятий, указанных в настоящих требованиях, в зависимости от степени угрозы совершения террористического акта и его возможных последствий, уровня террористической опасности, вводимого в пределах субъектов Российской Федерации и отдельных местностей (объектов) Российской Федерации в соответствии с Порядком установления уровней террористической опасности, предусматривающих принятие дополнительных мер по обеспечению безопасности личности, общества и государства, утвержденным Указом Президента Российской Федерации от 14 июня 2012 г. № 851 "О порядке установления уровней террористической опасности, предусматривающих принятие дополнительных мер по обеспечению безопасности личности, общества и государства".

IV. Порядок информирования об угрозе совершения или о совершении террористического акта на объекте

23. Информация об угрозе совершения или о совершении террористического акта на объекте (территории) (в том числе анонимного характера) незамедлительно направляется ответственным за обеспечение антитеррористической защищенности объекта (территории), назначенным приказом руководителя объекта, посредством имеющихся в его распоряжении средств связи в уполномоченные органы.

В случае отсутствия на момент представления в уполномоченные органы лицом, ответственным за обеспечение антитеррористической защищенности объекта (территории), информации в полном объеме, информация представляется в имеющемся объеме с последующим представлением дополнительной информации.

24. При представлении информации с помощью средств телефонной связи или радиосвязи лицо, ответственное за обеспечение антитеррористической защищенности объекта (территории), называет свои фамилию, имя, отчество, занимаемую должность, наименование объекта (территории), а также сообщают имеющуюся информацию об угрозе совершения или о совершении террористического акта на объекте (территории).

25. Лицо, передавшее информацию с помощью средств электронной или факсимильной связи, телефонной связи или радиосвязи фиксирует факт передачи, дату и время передачи информации имеющимися в его распоряжении средствами аудио- и (или) видеозаписи, программными и (или) техническими средствами.

26. Срок хранения носителей информации, подтверждающих факт ее передачи, дату и время, составляет не менее одного месяца.

V. Порядок осуществления контроля за выполнением требований к антитеррористической

защищенности объектов (территорий)

27. Контроль за выполнением настоящих требований заключается в проверке выполнения требований нормативных документов по защите объектов (территорий), а также в оценке обоснованности и эффективности принятых мер.

Проверки осуществляются руководителем объекта или лицом, ответственным за обеспечение антитеррористической защищенности объекта (территории), во взаимодействии с представителями уполномоченных органов (по согласованию).

28. Перечень лиц, уполномоченных на осуществление проверок, утверждается Министром цифрового развития, связи и массовых коммуникаций Российской Федерации (руководителем подведомственного Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации федерального органа исполнительной власти).

29. Мероприятия по контролю за выполнением настоящих требований включают в себя: внутренний контроль антитеррористической защищенности объектов (территорий) руководителем объекта;

контроль антитеррористической защищенности объектов (территорий), проводимый соответствующими подразделениями Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

30. Проверки антитеррористической защищенности объектов (территорий) могут быть плановыми и внеплановыми. Продолжительность проверки антитеррористической защищенности объекта (территории) не может превышать 3 рабочих дня.

31. Основанием для проведения проверки являются:

план проверки антитеррористической защищенности объекта (территории) (при плановой проверке), утверждаемый руководителем объекта или лицом, ответственным за обеспечение антитеррористической защищенности объекта (территории). Плановая проверка проводится не реже одного раза в 3 года;

поступившая в уполномоченные органы информация об угрозе совершения террористического акта или информация о нарушении требований к антитеррористической защищенности объекта (территории) (при внеплановой проверке). Внеплановая проверка проводится с учетом характера поступившей информации в течение 10 дней со дня ее поступления.

32. Акт проверки с указанием вида проверки, основания ее проведения, даты начала и окончания проверки, ее результатов, выявленных недостатков в антитеррористической защищенности объекта (территории) (при наличии) и сроков их устранения составляется в течение 10 дней со дня окончания проверки.

Акт проверки подписывается должностным лицом, осуществлявшим проверку, руководителем объекта или лицом, ответственным за обеспечение антитеррористической защищенности объекта (территории).

VI. Паспорт безопасности объекта (территории)

33. Паспорт безопасности объекта (территории) является информационно-справочным документом, определяющим состояние антитеррористической защищенности объекта (территории).

34. Паспорт безопасности объекта (территории) составляется лицом, ответственным за обеспечение антитеррористической защищенности объекта (территории), и утверждается руководителем органа (организации) или уполномоченным им должностным лицом.

35. Паспорт безопасности объекта (территории) составляется в 1 экземпляре и согласовывается (в том числе при его актуализации) с территориальным органом безопасности и территориальным органом Федеральной службы войск национальной гвардии Российской Федерации или подразделением вневедомственной охраны войск национальной гвардии Российской Федерации по

месту нахождения объекта (территории).

36. Паспорт безопасности объекта (территории) хранится в администрации объекта (территории), копии (электронные копии) паспорта безопасности объекта (территории) направляются в территориальный орган безопасности и территориальный орган Министерства внутренних дел Российской Федерации по месту нахождения объекта (территории).

37. Актуализация паспорта безопасности объекта (территории) осуществляется в порядке, установленном для его разработки, при изменении основного предназначения объекта (территории), общей площади и его периметра, количества потенциально опасных и критических элементов объекта (территории), сил и средств, привлекаемых для обеспечения антитеррористической защищенности объекта (территории), а также мер по физической, инженерно-технической защите объекта (территории) в течение 30 дней со дня таких изменений, но не реже одного раза в 5 лет.

38. Паспорт безопасности объекта (территории) является документом, содержащим служебную информацию ограниченного распространения, и имеет пометку "Для служебного пользования", если ему не присваивается гриф секретности.

Решение о присвоении паспорту безопасности грифа секретности принимается в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ

к требованиям к антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также подведомственных им организаций

ТРЕБОВАНИЯ

к инженерно-технической укреплённости объектов (территорий), применяемым на объектах (территориях) техническим средствам охраны, тревожной и пожарной сигнализации, контроля и управления доступом, систем оповещения и охранного освещения, а также к электроснабжению технических систем безопасности объектов (территорий)

1. Инженерно-техническая укреплённость объектов (территорий)

1. Ограждение периметра, зон и отдельных участков территории подразделяется на основное, дополнительное, предупредительное и ограждение локальных зон.

2. Ограждение должно исключать проход людей (животных), въезд транспорта и затруднять проникновение правонарушителей на объект (территорию), минуя контрольно-пропускной пункт.

3. Ограждение выполняется в виде прямолинейных участков с минимальным количеством изгибов и поворотов, ограничивающих наблюдение и затрудняющих применение технических систем безопасности.

4. К ограждению не должны примыкать какие-либо пристройки, кроме зданий, являющихся продолжением периметра объекта (территории). Окна первых этажей этих зданий, выходящие на неохраемую территорию, оборудуются металлическими решетками и металлическими сетками (при необходимости).

5. Ограждение не должно иметь лазов, проломов и других повреждений, а также незапираемых дверей, ворот и калиток.

6. Дополнительное ограждение устанавливается сверху и снизу основного для усиления основного ограждения. Верхнее дополнительное ограждение устанавливается на основное ограждение, если высота последнего менее 2,5 метра. Оно может представлять собой козырек, выполненный из 3 - 4 рядов колючей проволоки, инженерное средство защиты из армированной колючей ленты типа "Егоза" или иное устройство. Нижнее дополнительное ограждение для защиты от подкопа

устанавливается под основным ограждением с заглублением в грунт не менее 50 сантиметров. Оно может быть выполнено в виде бетонированного цоколя или сварной решетки из прутков арматурной стали диаметром не менее 16 миллиметров, сваренных в перекрестиях и образующих ячейки размером не более 150 x 150 миллиметров.

На крышах одноэтажных зданий, примыкающих к ограждению периметра объекта (территории), также устанавливается дополнительное ограждение.

7. Предупредительное ограждение устанавливается на объектах (территориях) категории 1. Оно может располагаться с внешней и (или) с внутренней стороны основного ограждения.

Высота предупредительного ограждения составляет не менее 1,5 метра.

На предупредительном ограждении через каждые 50 метров размещаются таблички (например, "Запретная зона! Проход запрещен", "Внимание! Охраняемая территория"), другие указательные и предупредительные знаки.

Предупредительное ограждение должно быть просматриваемым и выполняться из штакетника, металлической сетки, гладкой или колючей проволоки или другого материала.

8. Ограждение периметра объекта (территории) оборудуется системой охранного освещения, видеонаблюдения.

9. Места входа (въезда) на объект (территорию) оборудуются воротами и калитками.

10. Ворота устанавливаются на автомобильных и железнодорожных въездах на объект (территорию). По периметру объекта (территории) могут устанавливаться основные, запасные или аварийные ворота.

Конструкция ворот должна обеспечивать их жесткую фиксацию в закрытом положении.

Ворота с электроприводом и дистанционным управлением оборудуются устройствами аварийной остановки и открытия вручную на случай неисправности или отключения электропитания.

Ворота оборудуются ограничителями или стопорами для предотвращения произвольного открывания (движения).

11. Запирающие и блокирующие устройства при закрытом состоянии ворот должны обеспечивать соответствующую устойчивость к разрушающим воздействиям и сохранять работоспособность при повышенной влажности в широком диапазоне температур окружающего воздуха (от минус 40 до плюс 50 градусов Цельсия), прямом воздействии воды, снега, града, песка и других факторов.

12. При использовании замков в качестве запирающих устройств основных ворот устанавливаются замки гаражного типа или висячие (навесные). Редко открываемые ворота (запасные или аварийные) с внутренней стороны периметра объекта (территории) должны запираться на засовы и висячие (навесные) замки.

13. Калитка запирается на врезной, накладной замок или на засов с висячим замком. Усиление защиты калиток выполняется аналогично способам усиления дверей и их коробок.

14. На объекте (территории), на котором установлен пропускной режим или планируется его введение, оборудуется контрольно-пропускной пункт для прохода людей и проезда транспорта.

15. Контрольно-пропускной пункт должен обеспечивать необходимую пропускную способность прохода людей и проезда транспорта.

16. В зависимости от категории объекта (территории) на контрольно-пропускном пункте предусматриваются:

- а) помещение для хранения и оформления пропусков (карточек);
- б) помещение для зарядки оружия;
- в) камера хранения личных вещей персонала и посетителей объекта (территории);
- г) помещение для отдыха работников охраны и помещение для размещения технических систем безопасности.

17. Устройства управления механизмами открывания, прохода (проезда), охранным освещением и стационарными средствами досмотра размещаются в помещении контрольно-пропускного пункта

или на его наружной стене с внутренней стороны периметра объекта (территории). В последнем случае должен исключаться доступ посторонних лиц к устройствам управления.

18. Для осмотра транспорта на контрольно-пропускном пункте оборудуются смотровые площадки, эстакады, а для осмотра железнодорожного или крупногабаритного автотранспорта - вышки с площадками.

19. Окна и двери контрольно-пропускного пункта оборудуются защитными конструкциями соответствующего класса защищенности. Для контроля подъезжающего транспорта и прибывающих граждан сплошные ворота и входная дверь оборудуются смотровыми окошками или "глазками".

20. Для прохода людей через контрольно-пропускной пункт должен быть предусмотрен коридор, оборудованный турникетами.

21. Водопроемы сточных или проточных вод, подземные коллекторы (кабельные, канализационные) при диаметре трубы или коллектора от 300 до 500 миллиметров, выходящие с объекта (территории) категории 1, оборудуются на выходе решетками. Решетки изготавливаются из прутков арматурной стали диаметром не менее 16 миллиметров, сваренных в перекрестиях и образующих ячейки размером не более 150 x 150 миллиметров. В трубах или коллекторах большего диаметра, где есть возможность применения инструмента взлома, устанавливаются решетки, оборудованные охранной сигнализацией на разрушение или открывание.

22. Воздушные трубопроводы, пересекающие ограждение периметра объекта (территории), оборудуются элементами дополнительного ограждения - козырьком из колючей проволоки или инженерным средством защиты из армированной колючей ленты типа "Егоза", которое разворачивается по верху трубопровода или вокруг него.

23. Наружные и внутренние стены зданий, перекрытия пола и потолка помещений объектов должны быть труднопреодолимым препятствием для проникновения нарушителей.

24. Дверные конструкции, включая люки, должны обеспечивать надежную защиту помещений объекта (территории), быть исправными, хорошо подогнанными под дверную коробку. Во всех помещениях устанавливаются уплотнители на дверные притворы.

25. Входные наружные двери на объект (территорию) должны по возможности открываться наружу.

26. Двухстворчатые двери оборудуются 2 стопорными задвижками (шпингалетами), устанавливаемыми в верхней и нижней части каждого дверного полотна.

27. Двери и коробки чердачных и подвальных люков по конструкции и прочности должны быть аналогичны входным наружным дверям.

28. Двери погрузо-разгрузочных люков по конструкции и прочности должны быть аналогичны ставням и запираются изнутри на задвижку, а снаружи - на висячие (навесные) замки.

29. Деревянная обвязка погрузо-разгрузочного люка должна крепиться к фундаменту стальными скобами с внутренней стороны или ершами из стали диаметром не менее 16 миллиметров и забиваться в строительные конструкции на глубину не менее 150 миллиметров, а также закрываться изнутри на замки, задвижки, накладки и другие устройства.

30. При наличии в зданиях, строениях и сооружениях неиспользуемых или арендуемых подвальных помещений, граничащих с помещениями других организаций и собственников, необходимо при отсутствии двери на выходе из подвального помещения устанавливать металлическую открывающуюся решетчатую дверь, которая закрывается на висячий (навесной) замок.

31. Оконные конструкции (окна, форточки, фрамуги) во всех помещениях должны обеспечивать надежную защиту объекта (территории), должны быть остеклены, иметь надежные и исправные запирающие устройства. Стекла жестко закрепляются в пазах.

32. В случае если все оконные проемы помещения оборудуются решетками, одна из них делается открывающейся (распашной, раздвижной).

33. Для больших помещений с количеством окон более 5 количество открывающихся решеток определяется условиями быстрой эвакуации людей.

34. Для защиты оконных проемов первых этажей зданий, строений и сооружений допускается использовать рольставни, жалюзи, решетки.
35. Двери, ворота, калитки, люки, ставни, жалюзи и решетки являются надежной защитой только в том случае, когда на них установлены соответствующие по классу запирающие устройства.
36. Висячие (навесные) замки применяются для запираания ворот, чердачных и подвальных дверей, решеток, ставень и других конструкций. Данные замки должны иметь защитные пластины и кожухи.
37. Ключи от замков на оконных решетках и дверях запасных выходов размещаются в непосредственной близости или в специально выделенном помещении (в помещениях охраны) в ящиках, шкафах или нишах, заблокированных охранной сигнализацией.
38. Вентиляционные шахты, короба, дымоходы и другие технологические каналы и отверстия диаметром более 200 миллиметров, имеющие выход за границы объекта (территории), в том числе на крыши зданий и (или) в смежные неохраемые помещения, и входящие в охраняемые помещения, оборудуются на входе в эти помещения решетками, изготавливаемыми из прутков арматурной стали диаметром не менее 16 миллиметров, сваренных в перекрестиях и образующих ячейки размером не более 150 x 150 миллиметров.
39. Решетка в вентиляционных коробах, шахтах, дымоходах со стороны помещения должна отстоять от внутренней поверхности стены (перекрытия) не более чем на 100 миллиметров.
40. Для защиты вентиляционных шахт, коробов и дымоходов допускается использовать фальшрешетки из металлической трубки с диаметром отверстия не менее 6 миллиметров для протяжки провода шлейфа сигнализации с ячейкой 100 x 100 миллиметров.
41. В случае если вентиляционные короба и дымоходы диаметром более 200 миллиметров проходят в стенах помещений, такие стены с внутренней стороны помещения укрепляются по всей граничащей с коробом (дымоходом) площади решеткой, изготавливаемой из прутков арматурной стали диаметром не менее 8 миллиметров, сваренных в перекрестиях и образующих ячейки размером не более 100 x 100 миллиметров.
42. Защита кабельных линий связи и волноводов должна производиться в соответствии с установленными требованиями.
43. Места вывода (ввода) кабельных линий связи из распределительных шкафов в общественные или жилые здания, в подвальные или другие помещения должны быть защищены от посторонних лиц. Двери и оконные конструкции указанных помещений должны обеспечивать надежную защиту и обладать достаточным классом защищенности к разрушающим воздействиям.

II. Технические средства охранной и тревожной сигнализации

44. Технические средства охранной сигнализации периметра объекта (территории) выбираются в зависимости от вида предполагаемой угрозы объекту (территории), помеховой обстановки, рельефа местности, протяженности и технической укрепленности периметра объекта (территории), типа ограждения, наличия дорог вдоль периметра объекта (территории), зоны отторжения, ее ширины.
45. Охранная сигнализация периметра объекта (территории) проектируется, как правило, однорубежной. Для усиления охраны, определения направления движения нарушителя, блокировки уязвимых мест применяется многорубежная система охранной сигнализации.
46. Технические средства охранной сигнализации могут размещаться на ограждении, зданиях, строениях, сооружениях или в зоне отторжения. Охранные извещатели устанавливаются на стенах, специальных столбах или стойках, обеспечивающих отсутствие колебаний, вибраций.
47. Периметр объекта (территории) с входящими в него воротами и калитками разделяется на отдельные охраняемые участки (зоны) с подключением их отдельными шлейфами сигнализации к приемно-контрольному прибору малой емкости или к пульту внутренней охраны, которые устанавливаются на контрольно-пропускном пункте или в специально выделенном помещении охраны объекта (территории).

48. Технические устройства графического отображения охраняемого периметра (компьютер, световое табло с мнемосхемой охраняемого периметра и другие устройства) могут быть установлены в помещении дежурного персонала или помещении охраны объекта (территории).
49. Техническими средствами охранной сигнализации оборудуются все помещения с постоянным или временным хранением материальных ценностей, а также все уязвимые места здания (окна, двери, люки, вентиляционные шахты, короба и т. д.), через которые возможно несанкционированное проникновение в помещения объекта (территории).
50. Объекты (территории) категорий 1 и 2 оборудуются многорубежной системой охранной сигнализации.
51. Извещатели, блокирующие входные двери и неоткрываемые окна помещений, включаются в разные шлейфы сигнализации для возможности блокировки окон в дневное время при отключении охранной сигнализации дверей. Извещатели на входных дверях и открываемых окнах допускается включать в один шлейф сигнализации.
52. В помещениях больших размеров и (или) сложной конфигурации, для защиты которых требуется большое количество извещателей, допускается блокировать только локальные зоны (тамбуры между дверьми, коридоры, подходы к ценностям и другие уязвимые места).
53. На разных рубежах системы охранной сигнализации необходимо применять охранные извещатели, работающие на различных физических принципах действия.
54. Количество шлейфов охранной сигнализации должно определяться тактикой охраны, размерами зданий, строений, сооружений, этажностью, количеством уязвимых мест, а также точностью локализации места проникновения для оперативного реагирования на сигналы тревоги.
55. В помещениях, где круглосуточно находится персонал, охранной сигнализацией оборудуются отдельные участки периметра помещения, а также сейфы и металлические шкафы для хранения ценностей и документов.
56. Для оперативной передачи сообщений о противоправных действиях в отношении персонала или посетителей объекта (территории) на пункт централизованной охраны дежурной части охранной организации, осуществляющей охрану объекта (территории), объект (территория) оборудуется устройствами тревожной сигнализации (механическими кнопками, радиокнопками, радиобрелоками, педалями, оптико-электронными извещателями и другими устройствами). При организации системы тревожной сигнализации обеспечивается ее защита от несанкционированного отключения.
57. Устройства тревожной сигнализации на объекте (территории) в обязательном порядке устанавливаются на рабочих местах дежурного персонала, в помещениях охраны.
58. Ручные и ножные устройства тревожной сигнализации размещаются в местах, незаметных для посетителей и не мешающих нормальной работе персонала.
59. Работники охраны и дежурный персонал могут быть оснащены мобильными устройствами тревожной сигнализации, работающими по радиоканалу (радиокнопками или радиобрелоками) и установленными на отдельные шлейфы сигнализации.

III. Технические средства пожарной сигнализации

60. Технические средства пожарной сигнализации предназначены для круглосуточного автоматического контроля помещений и пожароопасных зон и автоматической индикации возникновения пожара.
61. К числу основных задач, возлагаемых на технические средства пожарной сигнализации, относятся:
эффективное и своевременное обнаружение очага возгорания с точным указанием места;
автоматическое оповещение подразделения охраны и дежурной диспетчерской службы о возгорании.
62. Для обнаружения возгорания используются пожарные датчики (извещатели) различных типов:

а) дымовые датчики (оптические, ионизационные, радиоизотопные, линейные и др.), которые устанавливаются в наиболее важных и (или) пожароопасных зонах, а при возможности во всех помещениях;

б) тепловые датчики (магнитные, с применением легкоплавких материалов, термометрические и др.), которые устанавливаются в менее ответственных зонах или как вспомогательные датчики;

в) комбинированные тепло-дымовые датчики.

63. Ручные пожарные извещатели устанавливаются на путях эвакуации людей (в коридорах, проходах, лестничных клетках и т.д.) и при необходимости в отдельных помещениях.

64. Организация и проведение противопожарных мероприятий, включая оснащение объекта системой пожарной сигнализации и огнетушителями, осуществляются в соответствии с нормативными документами по пожарной безопасности.

IV. Технические средства контроля и управления доступом

65. Система контроля и управления доступом предназначена:

а) для обеспечения санкционированного входа в здание и зоны ограниченного доступа и выхода из них путем идентификации личности по комбинации различных признаков:

вещественный код (карты с магнитной полосой, карты Виганда и др.);

запоминаемый код (клавиатуры, кодонаборные панели и др.);

биометрические признаки (отпечатки пальцев, сетчатка глаз и др.);

б) для предотвращения несанкционированного прохода в помещения и зоны ограниченного доступа объекта (территории).

66. Система контроля и управления доступом состоит из следующих технических средств:

а) преграждающие управляемые устройства в составе преграждающих конструкций и исполнительных устройств (турникеты, управляемые калитки, двери с электромагнитными замками или электромеханическими защелками и т.д.);

б) устройства для ввода идентификационных признаков в составе считывателей, кода наборных панелей, различных идентификаторов и т.д.;

в) устройства управления в составе аппаратных и программных средств.

67. Система контроля и управления доступом должна обеспечивать выполнение следующих основных функций:

а) открывание преграждающих управляемых устройств при считывании идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение) в заданный временной интервал или по команде оператора системы контроля и управления доступом;

б) запрет открывания преграждающих управляемых устройств при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;

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

г) защита от несанкционированного доступа к программным средствам устройств управления для изменения (добавления, удаления) идентификационных признаков;

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

е) сохранение настроек базы данных идентификационных признаков при отключении электропитания;

ж) ручное, полуавтоматическое или автоматическое открывание преграждающих управляемых устройств для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

- з) автоматическое закрытие преграждающих управляемых устройств при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;
- и) выдача сигнала тревоги или блокировка преграждающих управляемых устройств на определенное время при попытках подбора идентификационных признаков (кода) или открывания преграждающих управляемых устройств силой;
- к) регистрация и протоколирование текущих и тревожных событий;
- л) автономная работа считывателя с преграждающих управляемых устройств в каждой точке доступа при отказе связи с устройствами управления;
- м) возможность реализации функции контроля повторного входа (при необходимости).

V. Технические средства системы оповещения

68. Система оповещения на объекте (территории) создается для оперативного информирования людей о возникшей или приближающейся внештатной ситуации при угрозе или совершении террористического акта и координации их действий.

69. Для объекта (территории) разрабатывается план оповещения, который включает в себя:

- а) схему вызова сотрудников, должностными обязанностями которых предусмотрено участие в мероприятиях по предотвращению или устранению последствий внештатных ситуаций;
- б) инструкции, регламентирующие действия сотрудников при внештатных ситуациях;
- в) планы эвакуации;
- г) систему сигналов оповещения.

70. Оповещение людей, находящихся на объекте (территории), должно осуществляться с помощью технических средств, обеспечивающих:

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

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

71. Выбор варианта построения системы оповещения следует производить исходя из задач, стоящих перед системой, особенностей объекта управления и возможных способов реализации оповещения.

VI. Технические средства системы охранного освещения

72. Периметр объекта (территории), здания, строения и сооружения оборудуются системой охранного освещения.

73. Охранное освещение должно обеспечивать необходимые условия видимости ограждения территории, периметра здания и путей обхода.

74. В состав технических средств охранного освещения входят:

- а) осветительные приборы;
- б) кабельные и проводные сети;
- в) аппаратура управления.

75. Сеть охранного освещения по периметру объекта (территории) должна выполняться отдельно от сети наружного освещения и разделяться на самостоятельные участки в соответствии с участками охранной сигнализации периметра объекта (территории) и (или) охранного телевидения. Сеть охранного освещения должна подключаться к отдельной группе щита освещения, расположенного в помещении охраны или на контрольно-пропускном пункте. Допускается установка щита освещения на внешней стене контрольно-пропускного пункта с внутренней стороны периметра объекта (территории). Щит освещения должен закрываться на висячий (навесной) замок и блокироваться охранной сигнализацией.

76. Осветительные приборы охранного освещения могут быть любого типа (подвесные, консольные, прожекторы и др.).

77. В качестве источника света рекомендуется использовать лампы накаливания напряжением 220 В.

78. При использовании черно-белого охранного телевидения могут применяться инфракрасные прожекторы для подсветки периметра объекта (территории).

79. Магистральные и распределительные сети охранного освещения объекта (территории) прокладываются, как правило, под землей или по ограждению в трубах. Если указанное расположение воздушных сетей охранного освещения невозможно, они размещаются на объекте (территории) так, чтобы исключить возможность повреждения их из-за ограждения.

80. В ночное время охранное освещение должно работать постоянно. Дополнительное охранное освещение должно включаться только при нарушении охраняемых участков в ночное время, а при плохой видимости и в дневное.

VII. Электроснабжение технических систем безопасности

81. Установленные на объекте (территории) технические системы безопасности должны относиться к 1 категории электроприемников по надежности электроснабжения в соответствии с требованиями законодательства Российской Федерации, поэтому их электропитание должно быть бесперебойным (от 2 независимых источников переменного тока либо от одного источника переменного тока с автоматическим переключением в аварийном режиме на резервное питание от аккумуляторных батарей).

82. Рабочий ввод электропитания должен выполняться от электрической сети переменного тока напряжением 220 В.

83. Резервный ввод электропитания должен выполняться от одного из следующих источников питания или их любых сочетаний:

- а) электрическая сеть переменного тока напряжением 220 В (независимый фидер);
- б) аккумуляторные батареи;
- в) автономный электрогенератор.

84. Электроснабжение технических средств охраны от электрической сети переменного тока осуществляется от отдельной группы электрошита дежурного освещения.

85. При отсутствии на объекте (территории) электрошита дежурного освещения или отдельной группы на нем устанавливается самостоятельный электрошит на соответствующее количество групп. Вне охраняемого помещения электрошита размещаются в запираемых металлических шкафах.

86. Переход технических средств охраны на работу от резервного источника электропитания и обратно должен осуществляться автоматически с возможностью выдачи сигнала индикации перехода локально на объекте (территории).

87. Кабели электропитания технических средств охраны периметра объекта (территории) размещаются путем:

- а) прокладки в траншее, в подземном коллекторе или открыто по внутренней стороне бетонного ограждения (стене здания) с использованием бронированных кабелей. В обоснованных случаях допускается прокладка небронированных кабелей (проводов) по внутренней стороне бетонного ограждения (стене здания) в стальных трубах, металлорукавах и гофрированных поливинилхлоридных трубах;
- б) подвески на тросе на высоте не менее 3 метров или на отдельных участках на высоте до 2,5 метра при условии защиты кабеля от механических повреждений.

88. Соединительные или ответвительные коробки устанавливаются в охраняемых помещениях (зонах).

УТВЕРЖДЕНА
постановлением Правительства
Российской Федерации
от 30 октября 2014 г. № 1130

ФОРМА

паспорта безопасности объектов (территорий), находящихся в ведении Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также подведомственных им организаций

Срок действия паспорта

до " __ " _____ 20__ г.

(гриф по заполнении)

Экз. № _____

УТВЕРЖДАЮ _____ (руководитель Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (руководитель территориального органа, руководитель подведомственной организации) или уполномоченное им должностное лицо)

(подпись) (ф. и. о.)

" __ " _____ 20__ г.

СОГЛАСОВАНО

(руководитель территориального органа безопасности)

(подпись) (ф. и. о.)

" __ " _____ 20__ г.

СОГЛАСОВАНО

(руководитель территориального органа Росгвардии или подразделения вневедомственной охраны войск национальной гвардии Российской Федерации)

(подпись) (ф. и. о.)

" __ " _____ 20__ г.

ПАСПОРТ БЕЗОПАСНОСТИ _____ (наименование объекта (территории))

г. _____

20__ г.

(принадлежность, наименование вышестоящей организации, основной вид деятельности, наименование, адрес объекта (территории))

(ф. и. о. руководителя объекта, контактные телефоны)

(ф. и. о. лица, ответственного за обеспечение антитеррористической защищенности объекта (территории), контактные телефоны)

(наименование подразделений охраны, контактные телефоны)

I. Общие сведения об объекте (территории)

1. Категория объекта (территории) _____

2. Территория

(зоны, территории, административно-производственные здания и сооружения, конструктивные и технологические элементы объекта (территории))

(общая площадь)

(протяженность периметра)

II. Общие сведения о работниках (арендаторах)

1. Сведения о персонале объекта (территории)

(численность работающих на объекте (территории), из них арендаторов)

2. Режим работы объекта (территории)

(одно-, двух-, трехсменный режим работы, максимальная численность работников,

одновременное нахождение на объекте (территории) работников в дневное и ночное время)

III. Сведения о потенциально опасных участках и (или) критических элементах объекта (территории)

1. Потенциально опасные участки объекта (территории)\

№

п/п

Наименование потенциально опасного участка

Характер террористической угрозы

Численность работников, участвующих в деятельности на участке, человек

Общая площадь участка, кв. метров

Характер возможной чрезвычайной ситуации

1

2

3

4

5

6

2. Критические элементы объекта (территории)

№

п/п

Наименование критического элемента

Характер террористической угрозы

Численность работников, участвующих в деятельности критического элемента, человек

Оценка уязвимости критического элемента объекта (территории)

1

2

3

4

5

IV. Возможные социально-экономические последствия в результате совершения террористического акта на объекте

1. Людские потери

№

п/п

Наименование критического элемента

Количество человек, пострадавших в результате террористического акта

Количество человек, условия жизнедеятельности которых нарушены

Масштаб последствий террористического акта

персонал организации

персонал охраны

жители

1

2

3

4

5

6

7

2. Экономический ущерб

№

п/п

Наименование критического элемента

Собственный экономический ущерб, тыс. рублей

Сторонний экономический ущерб, тыс. рублей

Общий экономический ущерб, тыс. рублей

Масштаб последствий террористического акта

1

2

3

4

5

6

3. Нарушение инфраструктуры _____

V. Силы и средства, привлекаемые для обеспечения антитеррористической защищенности объекта

1. Принадлежность охраны

(вид охраны - организация, находящаяся в ведении Росгвардии, подразделения вневедомственной охраны войск национальной гвардии Российской Федерации, военизированные и сторожевые подразделения организации, подведомственной Росгвардии, и др.)

2. Структура и порядок организации охраны

(положение о подразделении охраны, вид подразделения - филиал, отряд, команда, отдельная группа)

3. Штат подразделения охраны

№

п/п

Наименование должности

Количество работников

Всего

4. Организационно-распорядительные документы

(инструкция по физической защите объекта (территории), договор, должностные инструкции охранников, акт технической укреплённости объекта (территории) и др.)

5. Организация пропускного и внутриобъектового режимов

(инструкции по пропускному и внутриобъектовому режимам, образцы пропускных документов, вспомогательные помещения для персонала охраны)

6. Контрольно-пропускные пункты:

а) всего _____

б) проходных _____

в) автотранспортных _____

г) смешанных _____

7. Дислокация постов охраны, режим работы

Вид поста

Количество

единиц

человек

Наружные посты

Внутренние посты

Круглосуточные посты

12-часовые посты

8-часовые посты

Посты с иным режимом работы (указать режим)

Всего

8. Экипировка охраны:

а) оружие _____
(наименование и количество единиц огнестрельного оружия и патронов к нему)

б) специальные средства

(вид и количество единиц специальных средств)

в) служебные собаки

(количество собак и вольеров для их содержания)

г) дополнительные силы, привлекаемые для обеспечения антитеррористической защищенности объекта (территории)

VI. Меры по инженерно-технической, физической защите и пожарной безопасности объекта (территории)

1. Общая протяженность периметра, подлежащего ограждению

(метров)

2. Характеристика ограждений

(капитальные, деревянные, из колючей проволоки, сетчатые и др., протяженность, состояние)

3. Освещение охраняемой территории и периметра ограждения

(наличие, краткая характеристика)

4. Охранная сигнализация

(участки, ограждение которых заблокировано сигнализацией, тип и количество приборов сигнализации, установленных по периметру ограждения)

5. Пожарная сигнализация

(тип, количество лучей)

6. Тревожная сигнализация, в том числе кнопка тревожной сигнализации

(тип, количество лучей, куда выведены)

7. Наличие средств радиосвязи

(количество постов, оборудованных радиосвязью, тип и количество радиостанций)

8. Наличие средств телефонной связи

(количество постов, оборудованных телефонной связью)

9. Наличие средств видеонаблюдения

(тип и количество видеокамер, контролируемые зоны)

10. Техника контрольно-пропускных пунктов

(тип и количество обычных турникетов, системы контроля и управления доступом, механизированных ворот, применяемых средств принудительной остановки транспорта)

11. Пожарная безопасность

а) наличие средств пожаротушения

(количество огнетушителей отдельно по каждому виду, типу, распределение по зданиям, этажам; наличие и расположение гидранта, наличие пожарных щитов, водоемов и т. д.)

б) наличие подразделений Государственной противопожарной службы

(наименование подразделения, порядок связи и номера телефонов)

VII. Выводы и рекомендации

1. Объект (территория) находится в ведении (сфере деятельности)

(федеральный орган исполнительной власти)

2. Эффективность сил и средств охраны для выполнения мероприятий по антитеррористической защищенности объекта (территории)

3. Необходимые дополнительные мероприятия по совершенствованию физической защиты и антитеррористической защищенности объекта (территории) с указанием срока их выполнения

4. Вывод о системе охраны объекта (территории)

VIII. Дополнительная информация с учетом особенностей объекта (территории)

(пояснения и другие сведения, в том числе информация о размещенных на объекте (территории) других организаций - размеры занимаемых площадей, основание размещения на объекте (территории), наличие самостоятельной охранной структуры (принадлежность, вид, численность, вооруженность, техническая оснащенность), состояние пропускного режима и др., порядок взаимодействия с подразделением охраны объекта (территории)

(подпись, ф. и. о. лица, ответственного за обеспечение антитеррористической защищенности объекта)

Составлен " __ " _____ 20__ г.

Актуализирован " __ " _____ 20__ г.
