ОБСЕ Организация по безопасности и сотрудничеству в Европе

PROTECT

ТЕХНИЧЕСКОЕ РУКОВОДСТВО

ВОПРОСЫ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ ОТ ТЕРРОРИСТИЧЕСКИХ АТАК

Проект ОБСЕ PROTECT получил финансовую поддержку от Соединенных Штатов Америки и Федеративной Республики Германия.

Дизайн и макет: Пено Мишоян
Печать: Druckerei Ferdinand Berger & Söhne GmbH
Источник изображения: Envato Elements Pty Ltd & Shutterstock, Inc.

Антитеррористическое подразделение
Департамент по противодействию транснациональным угрозам
Секретариат ОБСЕ
Wallnerstrasse 6 A.
1010 Vienna, Austria
Тел.: +43 1 514 360, atu@osce.org

Содержание

Выражение признательности

Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам ОБСЕ хотело бы выразить искреннюю благодарность различным государствам-участникам, экспертам, консультантам и сотрудникам, внесшим вклад в создание настоящего *Технического руководства.*

Консультативная группа экспертов по разработке технического руководства проекта PROTECT (2024–2025 гг.)[1]

Мэрибет Келлихер
Старший советник по вопросам политики
Бюро по борьбе с терроризмом
Государственный департамент
Соединенные Штаты Америки

Хайко Нильс Хюттер
Полковник, военный советник
Постоянное представительство Федеративной Республики Германия при ОБСЕ
Федеративная Республика Германия

Далер Валиев
Государственный комитет по национальной безопасности
Правительство Республики Таджикистан

Ерлан Батталов
Антитеррористический центр
Правительство Республики Казахстан

Асия Мергалиева
Антитеррористический центр
Правительство Республики Казахстана

Дэниел Голстон
Председатель экспертно-консультативной группы и руководитель проекта PROTECT
Антитеррористическое подразделение
Департамент по противодействию транснациональным угрозам
ОБСЕ

Дипак Чатурведи
Председатель
Сообщество физической безопасности
ASIS International

Джулиан Стаффорд
Генеральный секретарь
Европейский совет по телекоммуникациям и коммунальным услугам

Йоханнес Хайлер
Советник по вопросам борьбы с терроризмом
Бюро по демократическим институтам и правам человека
ОБСЕ

Максимилиан Шайд
Специалист по правам человека
Бюро по демократическим институтам и правам человека
ОБСЕ

Джулия Манкони
Старший специалист по энергетической безопасности
Экономическая и экологическая деятельность
ОБСЕ

д.т.н. Мартин Ларше
Старший научный сотрудник по безопасности и обороне
Подразделение космической, связной и экономической безопасности
Директорат по социальной устойчивости и безопасности
Объединенный исследовательский центр Европейской комиссии

Доктор Моника Кардарилли
Исследователь в области передовой науки для разработки политики
Отдел по вопросам безопасности космоса, связи и экономики
Директорат по социальной устойчивости и безопасности
Объединенный исследовательский центр Европейской комиссии

Амин Бутаган
Ведущий эксперт
Проект Civipol «Усиление защиты общественных пространств и критически важной инфраструктуры на Западных Балканах»

Кэтрин Пиана
Генеральный директор
Конфедерация европейских служб безопасности

Камиль Скотто де Сезар
Аналитик по вопросам политики, подразделение по химическим, биологическим, радиологическим, ядерным, взрывоопасным и уязвимым объектам
Управление по борьбе с терроризмом
ИНТЕРПОЛ

Глобальная программа Организации Объединенных Наций (ООН) по защите уязвимых целей от террористических угроз:

- Игнасио Ибаньес, координатор Управления ООН по борьбе с терроризмом
- Энн-Мария Сеесмаа, юрист, Исполнительный директорат Контртеррористического комитета Совета Безопасности, ООН
- Дуччо Мазарезе, сотрудник по управлению программами, Межрегиональный научно-исследовательский институт ООН по вопросам преступности и правосудия

Агнешка Мизгальска
Технический специалист по авиационной безопасности
Авиационная безопасность и упрощение формальностей, политика авиационной безопасности
Международная организация гражданской авиации

Национальная команда по критически важной инфраструктуре
Федеральная служба национальной безопасности
Королевская канадская конная полиция
Канада

1 Настоящее *Техническое руководство* не обязательно отражает национальные или институциональные позиции членов Экспертной консультативной группы.

Эксперты

Доктор Дэвид БаМаунг
Ведущий эксперт
Эксперт по физической безопасности и безопасности персонала
Директор, Консультант AbleSecurity
Почетный профессор Каледонского университета Глазго
Приглашенный профессор, Университет Ковентри

Стефано Бетти
Юридический эксперт

Бенджамин Гринакр
Эксперт по правам человека

Профессор Джон Каддихи, FRSA
Эксперт по угрозам и рискам
Лаборатория Защитной Безопасности
Университет Ковентри

Доктор Алессандро Лазари
Независимый эксперт-рецензент
Центр междисциплинарных исследований безопасности и устойчивости критически важной инфраструктуры
Департамент инжиниринга для инноваций
Университет Саленто
Италия

Сотрудники антитеррористического подразделения ОБСЕ

Дэниел Голстон
Руководитель проекта PROTECT

Анна Гусарова
Заместитель руководителя проекта

Камила Сабыррахим
Проектный ассистент

Элис Циммерманн
Проектный ассистент

Данное *Техническое руководство* было переведено на русский язык Ильей Даншиным, отредактировано Маликой Пулатовой, Анной Гусаровой и Камилой Сабыррахим.

ОБСЕ хотела бы выразить благодарность Отделу безопасности инфраструктуры Агентства по кибербезопасности и безопасности инфраструктуры Соединенных Штатов Америки за рецензирование.

Предисловие

Современный мир зависит от доступа к электричеству, энергии, воде, интернету и другим жизненно важным услугам. Эти услуги составляют основу повседневной жизни каждого государства-участника ОБСЕ, и правительства, тогда как владельцы/операторы критически важной инфраструктуры прилагают значительные усилия для обеспечения ежедневной доступности этих услуг для нас. Учитывая большое значение этих жизненно важных услуг для нашей жизни и экономики, террористы зачастую выбирают в качестве мишени критически важную инфраструктуру, чтобы нанести максимальный ущерб.

Террористическая угроза энергетической инфраструктуре, международным перевозкам и другим критически важным объектам инфраструктуры была признана 57 государствами-участниками ОБСЕ, Советом Безопасности ООН и Генеральной Ассамблеей ООН, что стало результатом более чем двадцатилетних целенаправленных усилий ОБСЕ в этой области.

Несколько десятилетий назад государства-участники ОБСЕ призвали Организацию к осуществлению мер по повышению безопасности международных перевозок и других критически важных объектов инфраструктуры. С тех пор ОБСЕ сотрудничает с государствами-участниками в целях усиления защиты критически важной инфраструктуры посредством наращивания потенциала стран, содействия региональному диалогу, а также консолидации передового опыта и обмена им.

Государства-участники ОБСЕ обладают обширным опытом в области защиты критически важной инфраструктуры, как показано в настоящем техническом руководстве. Многочисленные примеры передовой практики, представленные нашими участниками, свидетельствуют о глубине и широте этих знаний и опыта.

Мы надеемся, что данное *руководство* послужит источником ценной информации для политиков государств-участников, партнеров ОБСЕ по сотрудничеству, владельцев и операторов национальной критически важной инфраструктуры, а также для всех других субъектов, осуществляющих деятельность по защите критически важной инфраструктуры. Мы уверены, что благодаря обмену рекомендациями и передовой практикой, собранными в этом *руководстве*, как с государственными, так и с частными заинтересованными сторонами, мы сможем повысить нашу коллективную безопасность в условиях меняющихся террористических угроз и защитить жизненно важные службы, которым угрожают эти террористы.

Посол Алена Купчина
Координатор деятельности ОБСЕ по противодействию транснациональным угрозам
Секретариат ОБСЕ

Краткое содержание

Критически важная инфраструктура (КВИ) обеспечивает основные услуги, которые лежат в основе жизнедеятельности общества и экономики во всем регионе ОБСЕ. Вследствие своей первостепенной важности объекты КВИ всегда были и продолжают быть мишенью для насильственных экстремистских и террористических организаций. Взаимосвязанность сетей КВИ, обусловленная их природой, означает, что одна атака может иметь каскадные последствия для других систем и служб КВИ. Это не только усиливает разрушительное воздействие одной атаки, но и привлекает дополнительное внимание СМИ к самим злоумышленникам. Поэтому повышение безопасности КВИ является насущным приоритетом для всего региона ОБСЕ. И все же, хотя это важная конечная цель, путь к ней зачастую неочевиден.

За исключением строго регулируемых секторов КВИ, во многих государствах-участниках ОБСЕ отсутствуют подробные руководящие инструкции по мерам обеспечения физической безопасности, которые должны быть реализованы на уровне объектов. Вместо этого существует сложная система практических подходов, принципов и необязательных руководящих документов, которые должны изучаться правительствами, владельцами/операторами КВИ и лицами, отвечающими за безопасность на объектах КВИ, для обеспечения эффективной физической безопасности находящихся в их ведении объектов и предприятий.

Настоящее *Техническое руководство* содержит структурированные рекомендации по практическим подходам, принципам и соображениям, которые могут повысить физическую безопасность стационарных объектов и предприятий КВИ с целью предотвращения террористических атак, повышения уровня подготовки к ним и смягчения их последствий. Целевой аудиторией данного руководства являются лица, ответственные за разработку политики, с надзорными, консультативными и/или регулирующими функциями по отношению к владельцам/операторам КВИ в государствах-участниках ОБСЕ, сами владельцы/операторы КВИ, а также лица, отвечающие за обеспечение безопасности на объектах КВИ (включая частных поставщиков охранных услуг). Настоящее *руководство* было разработано с учетом потребностей различных секторов, объектов и предприятий КВИ, как в городских центрах, так и в отдаленных регионах.

Важно отметить, что вместо того, чтобы диктовать единый подход к обеспечению физической безопасности, данное *руководство* представляет ряд общедоступных практических методов, отражающих многообразие существующих подходов. Большинство упоминаемых в данном *руководстве* практических методов взяты из опыта государств-участников ОБСЕ. Это демонстрирует огромное богатство знаний, доступ к которым открывает членство в ОБСЕ, а также важность сбора данных об этих подходах и обмена ими на благо всех.

Руководство разделено на несколько глав, охватывающих стратегические вопросы, такие как политические и законодательные подходы к защите критически важной инфраструктуры (ЗКВИ), соблюдение рамочных положений в области прав человека

и технические аспекты, такие как проектирование систем обнаружения вторжений и контроля доступа. На протяжении всего документа особое внимание уделяется подготовке и планированию ряда сценариев террористических угроз, таких как ситуации с захватом заложников, нападение с использованием огнестрельного оружия и транспортных средств. Вопросам планирования также уделено внимание в разделах, посвященных кризисным коммуникациям, обеспечению непрерывности деятельности, обучению и учениям. В частности, в регионе ОБСЕ секторы КВИ имеют высокую степень проникновения частного сектора, поэтому вопросы частно-государственного партнерства также находят отражение во всех положениях *руководства.* По мере возможности также даются ссылки на международные и региональные стандарты для самостоятельного ознакомления.

Сокращения и аббревиатуры

БАС – беспилотные авиационные системы (дроны)

БДИПЧ (ОБСЕ) – Бюро по демократическим институтам и правам человека

ГА ООН – Генеральная Ассамблея Организации Объединенных Наций

ДОБ – Департамент ООН по вопросам охраны и безопасности

ЕС – Европейский Союз

ЕСПЧ – Европейский суд по правам человека

ЗКВИ – защита критически важной инфраструктуры

ИКАО – Международная организация гражданской авиации

ИМО – Международная морская организация

ИНТЕРПОЛ – Международная организация уголовной полиции

ИТ – информационные технологии

КВИ – критически важная инфраструктура

КПЧ – Комитет по правам человека ООН

МАГАТЭ – Международное агентство по атомной энергии

МоВ – меморандум о взаимопонимании

МПГПП – Международный пакт о гражданских и политических правах

НАТО – Организация Североатлантического договора

ОБСЕ – Организация по безопасности и сотрудничеству в Европе

ОВиК – отопление, вентиляция и кондиционирование воздуха

ООН – Организация Объединенных Наций

ОЭСР – Организация экономического сотрудничества и развития

ПДЧС – план действий при чрезвычайных ситуациях

ППД – парадигма правоохранительной деятельности

ПРООН – Программа развития ООН

ПСВУ – переносное самодельное взрывное устройство, носимое на теле человека

СБ ООН – Совет Безопасности ООН

СВУ – самодельные взрывные устройства

СВУТС – самодельные взрывные устройства, заложенные в транспортные средства

США – Соединенные Штаты Америки

УВКПЧ – Управление Верховного комиссара ООН по правам человека

УНП ООН – Управление ООН по наркотикам и преступности

ХБР – химическое, биологическое и радиологическое

ХБРВ – химическое, биологическое, радиологическое и взрывчатое

ХБРЯ – химическое, биологическое, радиологическое и ядерное

ЧГП – частно-государственное партнерство

ЮНИТАД – Следственная группа ООН по привлечению к ответственности за преступления, совершенные ИГИЛ/Исламским государством в Ираке и Леванте

ASF – противоосколочная пленка

CCTV – система видеонаблюдения

CEPES – критической объект, имеющий особое европейское значение

CER – Директива ЕС об устойчивости критически важных объектов [2022/2557]

CISA – Агентство по кибербезопасности и защите инфраструктуры США

CJEU – Суд Европейского Союза

CE – Совет Европейского Союза

CoESS – Конфедерация европейских служб безопасности

DCAF – Женевский центр управления сектором безопасности

DHS – Министерство внутренней безопасности США

EN – Европейский стандарт

FEMA – Федеральное агентство по чрезвычайным ситуациям США

ICoCA – Международная ассоциация кодексов поведения

IDS – система обнаружения вторжений

ISO – Международная организация по стандартизации

NNCEIP – защита критической неядерной энергетической инфраструктуры

NPSA – Национальное управление по защите и безопасности Великобритании

NSRA – Оценка рисков национальной безопасности Великобритании

PIDAS – система обнаружения и оценки вторжений на периметр

RBPS – стандарты эффективности, основанные на оценке риска

UNDRR – Управление ООН по снижению риска бедствий

UNOCT – Управление ООН по борьбе с терроризмом

VSS – система охранного видеонаблюдения

1 Введение

«Экстремистские и террористические организации на всей территории ОБСЕ рассматривают критически важную инфраструктуру в качестве своей главной цели. Их пропаганда, совершенные нападения и сорванные заговоры указывают на неизменное, если не возросшее, намерение и способность нарушать работу критически важных служб (также известных как системы жизнеобеспечения), необходимых для нашей повседневной социальной и экономической жизни.»

1 Введение

Экстремистские и террористические организации на всей территории ОБСЕ рассматривают критически важную инфраструктуру (КВИ) в качестве своей главной цели. Их пропаганда, совершенные нападения и сорванные заговоры указывают на неизменное, если не возросшее, намерение и способность нарушать работу критически важных служб (также известных как системы жизнеобеспечения), необходимых для нашей повседневной социальной и экономической жизни. Хотя идеологические мотивы этих злоумышленников разнообразны, многие в конечном итоге останавливают свой выбор на КВИ в качестве цели для нападений с применением насилия, поскольку они обеспечивают мощный эффект, привлекают внимание СМИ и имеют пропагандистскую ценность.

Системы КВИ взаимозависимы, поэтому одна атака может иметь каскадные, усиливающиеся последствия. Например, успешное нападение на электрическую подстанцию может последовательно распространиться на другие критически важные объекты и нарушить работу больниц, водоочистных сооружений, общественного транспорта, аварийной связи и т.д. Последствия могут варьироваться от гибели людей до крупных экономических и социальных издержек, снижения доверия общественности к правительству и придания смелости террористическим организациям как внутри страны, так и за рубежом. Таким образом, повышение безопасности КВИ является насущным приоритетом для всего региона ОБСЕ.

Хотя это важная конечная цель, путь к ней зачастую неочевиден. За исключением строго регулируемых секторов КВИ, таких как сектор ядерной энергетики, во многих государствах-участниках ОБСЕ отсутствует подробное руководство по мерам обеспечения физической безопасности, которые должны быть реализованы на уровне объектов. Вместо этого существует сложная система практических подходов, принципов и необязательных руководящих документов, которые должны изучаться правительствами, владельцами/операторами КВИ и лицами, отвечающими за безопасность на объектах КВИ, для обеспечения эффективной физической безопасности находящихся в их ведении объектов и предприятий. Данное *Техническое руководство* призвано оказать поддержку этим заинтересованным сторонам путем сбора информации об опыте и знаниях со всего региона ОБСЕ и за его пределами и объединения их в одной публикации.

Настоящее *Техническое руководство* содержит структурированные рекомендации по практическим подходам, принципам и соображениям, которые могут повысить физическую безопасность стационарных объектов и предприятий КВИ с целью предотвращения террористических атак, повышения уровня подготовки к ним и смягчения их последствий. Настоящее *руководство* было разработано с учетом потребностей различных секторов, объектов и предприятий КВИ, как в городских центрах, так и в отдаленных регионах.

Вместо того, чтобы диктовать единый подход к физической безопасности, это *руководство* представляет комплекс общедоступных практических методов, используемых в регионе ОБСЕ и за его пределами, в том числе правительствами, международными и региональными организациями и частным сектором. Таким образом, оно отражает широкий спектр точек зрения и подходов, принятых в регионе ОБСЕ для продвижения общей цели укрепления физической безопасности объектов и предприятий КВИ.

Хотя данный документ содержит необязательные рекомендации, фактические решения по мерам обеспечения физической безопасности и всем вопросам, рассматриваемым в настоящем *Техническом руководстве,* должны приниматься компетентными заинтересованными сторонами на междисциплинарной основе, то есть с привлечением для консультаций инженеров и экспертов в юридических вопросах, сферах прав человека, охраны правопорядка, борьбы с терроризмом и других соответствующих дисциплин, по мере необходимости. Кроме того, эти меры физической безопасности должны приниматься в соответствии с международным правом, включая международное право в области прав человека, национальные законы и местные нормативные акты. Ничто в настоящем *руководстве* не должно рассматриваться как отменяющее такие законы и нормативные акты.

Настоящее *Техническое руководство* предназначено для лиц, ответственных за разработку политики, с надзорными, консультативными и/или регулирующими функциями по отношению к владельцам/операторам КВИ в государствах-участниках ОБСЕ, владельцев/операторов КВИ, а также лиц, отвечающих за обеспечение безопасности на объектах КВИ (включая частных поставщиков охранных услуг). Однако часть его содержания может быть также полезна для лиц, заинтересованных

в повышении физической безопасности своих объектов, включая такие уязвимые объекты, такие как места поклонения, гостиницы, концертные залы и т. д.

В данном *Техническом руководстве* основное внимание уделяется соображениям физической безопасности. Однако, если объект КВИ подвергнется террористической атаке, одни только меры физической защиты не смогут обеспечить его безопасность; во многих случаях они представляют собой последнюю линию обороны после того, как другие меры не сработали. Меры физической защиты должны быть интегрированы с мерами безопасности персонала, процедурной безопасности и кибербезопасности, которые вместе создают комплексную и устойчивую систему безопасности для конкретного объекта. В этой связи иногда содержание руководства смещается в сторону более широких вопросов борьбы с терроризмом, управления кризисами, обучения и учений, а также других областей. Это связано с основной угрозой, которую данное *Техническое руководство* призвано снизить: терроризмом. Учитывая динамичный характер террористической угрозы и тот факт, что террористические организации могут быть очень изобретательными и инновационными в своих атаках, все системы физической безопасности должны работать как часть более широкой системы безопасности, чтобы обеспечить надлежащую защиту объекта КВИ. При необходимости данное *руководство* затрагивает и эту более широкую систему.

Важно отметить, что данное *Техническое руководство* не рассматривает физическую безопасность КВИ в ситуациях вооруженного конфликта. Оно также не предназначено для предоставления всеобъемлющих рекомендаций по созданию национальной системы защиты КВИ.

1.1 Мандат ОБСЕ по защите критически важной инфраструктуры от террористических атак

Защита КВИ от террористических атак прочно закреплена в мандате ОБСЕ, о чем свидетельствует почти два десятилетия политического внимания к этой теме со стороны 57 государств-участников ОБСЕ. Первое упоминание о защите критически важной инфраструктуры (ЗКВИ) содержится в Решении Совета министров № 5 (2007) о частно-государственном партнерстве в противодействии терроризму. В этом Решении ОБСЕ поручено содействовать роли частного сектора и гражданского общества в своей контртеррористической деятельности, уделяя особое внимание «определению объектов критически важной инфраструктуры, составлению соответствующих приоритетов и защите таких объектов, а также готовности к чрезвычайным ситуациям и ликвидации их последствий».[2] В том же году Совет министров принял Решение № 6 о защите критической энергетической инфраструктуры от террористических атак. Это Решение призывает к сотрудничеству с другими организациями, обмену передовым опытом и содействию частно-государственному партнерству.[3]

2 ОБСЕ (2007 г.), Решение Совета министров № 5/07: Частно-государственное партнерство в противодействии терроризму (MC.DEC/5/07). Доступно по адресу: https://www.osce.org/files/f/documents/c/a/29572.pdf [дата обращения: 21 июля 2025 г.].

3 ОБСЕ (2012 г.), Решение Постоянного совета № 1063: Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063). Доступно по адресу: https://www.osce.org/files/f/documents/f/3/98542.pdf [дата обращения: 21 июля 2025 г.].

Важно отметить, что в 2012 году государства-участники ОБСЕ согласовали Консолидированную концептуальную базу для борьбы с терроризмом. Именно в этом Решении заложена основа настоящего *Технического руководства* ОБСЕ:

> «осуществлять свою деятельность, направленную на расширение сотрудничества и укрепление потенциала на национальном, региональном и субрегиональном уровнях с целью предупреждения терроризма и борьбы с ним, в *частности*, в области уголовного правосудия, в правоохранительной сфере и в области пограничного режима и безопасности границ в рамках, основанных на верховенстве права и уважении прав человека, с тем чтобы: [...] повышать безопасность международной транспортной и других важнейших видов инфраструктуры».[4]

1.2 Мандат ООН по защите критически важной инфраструктуры от террористических атак

В качестве регионального механизма в соответствии с Главой VIII Устава Организации Объединенных Наций (ООН), ОБСЕ вносит вклад в реализацию решений ООН, в том числе по борьбе с терроризмом. Что касается защиты КВИ, то в 2017 году Совет Безопасности ООН принял Резолюцию 2341 (2017) о защите КВИ от террористических атак. Эта резолюция будет неоднократно упоминаться в данном *Техническом руководстве*.[5]

Кроме того, Добавление Совета Безопасности ООН от 2018 года к Мадридским руководящим принципам 2015 года в отношении иностранных боевиков-террористов содержит рекомендации, направленные на поддержку реализации Резолюции 2341. Эти Принципы и Добавление также упоминаются в настоящем *руководстве*.[6]

При этом в восьмом обзоре Глобальной контртеррористической стратегии ООН в 2023 году Генеральная Ассамблея ООН конкретно призывает к действиям в области КВИ в контексте борьбы с терроризмом:

> «Призывает далее государства-члены установить или укреплять сообразно обстоятельствам национальные, региональные и международные партнерские отношения с заинтересованными сторонами, как государственными, так и частными, для обмена информацией и опытом в целях предотвращения террористических нападений, защиты от них, смягчения их последствий, их расследования, реагирования на них и восстановления после таких нападений, подчеркивает необходимость того, чтобы государства, которые в состоянии

4 ОБСЕ (2012 г.), Решение Постоянного совета № 1063: Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063), стр. 4–5. Доступно по адресу: https://www.osce.org/files/f/documents/f/3/98542.pdf [дата обращения: 21 июля 2025 г.].

5 СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

6 Контртеррористический комитет Совета Безопасности ООН (2019 г.), *Руководящие принципы Совета Безопасности в отношении иностранных боевиков-террористов: Мадридские руководящие принципы 2015 г. + Дополнение 2018 г.* Доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/security-council-guiding-principles-on-foreign-terrorist-fig.pdf [дата обращения: 21 июля 2025 г.].

делать это, содействовали эффективному и целенаправленному наращиванию потенциала, организации учебной подготовки и предоставлению других необходимых ресурсов и технической помощи, когда это требуется, с тем чтобы у всех государств появился надлежащий потенциал для осуществления планов чрезвычайных мер и мер реагирования в случае нападения на критически важные объекты инфраструктуры и общественные места (слабозащищенные цели), и призывает структуры Глобального договора по координации контртеррористической деятельности продолжать оказывать запрашивающим государствам-членам поддержку в наращивании потенциала для обеспечения устойчивости уязвимых целей».[7]

1.3 Обзор проекта ОБСЕ PROTECT

В 2023 году Антитеррористическое подразделение ОБСЕ запустило проект PROTECT, направленный на совершенствование национальных подходов к защите уязвимых целей от террористических угроз и других опасностей в регионе ОБСЕ. Термин «уязвимые цели» относится как к КВИ, так и к слабозащищенным целям.[8]

Проект представляет собой многогранную инициативу, направленную на создание как национального потенциала, так и региональных сетей, ориентированных конкретно на защиту уязвимых целей, посредством трех компонентов:

- **Компонент 1:** Объединение и распространение специализированных рекомендаций и передовой практики по защите КВИ во всем регионе ОБСЕ. Настоящее *Техническое руководство* является результатом работы в рамках этого компонента.
- **Компонент 2:** Укрепление национального потенциала для эффективной защиты уязвимых целей от террористических атак и других опасностей посредством повышения осведомленности и обучения внутри стран.
- **Компонент 3:** Содействие региональному сотрудничеству и диалогу между государствами-участниками и другими заинтересованными сторонами по вопросам эффективной защиты уязвимых целей, в том числе посредством частно-государственного партнерства и взаимодействия с гражданским обществом.

7 Генеральная Ассамблея ООН (22 июня 2023 г.), *Глобальная контртеррористическая стратегия Организации Объединенных Наций: восьмой обзор.* Доступно по адресу: https://docs.un.org/ru/A/RES/77/298 [дата обращения: 21 июля 2025 г.].

8 В ОБСЕ не принято стандартное определение понятия «слабозащищенная цель». Однако в Глобальной программе ООН по противодействию террористическим угрозам в отношении уязвимых целей говорится: «В широком смысле под «слабозащищенными целями» понимаются такие виды уязвимых объектов, как стадионы, торговые центры, театры, религиозные учреждения, пешеходные зоны, которые легко доступны и открыты для общественности и по этим причинам намеренно не предусматривают никаких мер обеспечения безопасности или предусматривают ограниченные меры. Эта особенность, в сочетании с большим скоплением людей, которое часто отмечается в этих местах, делает их привлекательными целями для террористов, стремящихся вызвать массовые жертвы и/или масштабные разрушения таким образом, чтобы для этого не требовалось масштабного планирования и подготовки или значительных ресурсов, но чтобы это вызвало несоразмерно большое освещение в средствах массовой информации. Понятие «слабозащищенные цели» не поддается точному определению еще и потому, что места, которые обычно ассоциируются с ним, являются крайне неоднородными. «Слабозащищенными цели» могут быть крытые или открытые объекты постоянного или временного характера. Они могут иметь различные размеры, функции, физические характеристики, местоположение и профили пользователей». См. Управление ООН по борьбе с терроризмом (UNOCT) (2022 г.), *Защита уязвимых целей от террористических нападений: Руководство по передовой практике: Введение.* Доступно по адресу: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451r-vt-mod1-introduction_web.pdf [дата обращения: 21 июля 2025 г.].

1.4 Структура данного *Технического руководства*

Эффективная физическая безопасность на объектах КВИ требует поддержки и приверженности на уровне объекта, на корпоративном уровне владельца/оператора КВИ, а также со стороны государственных должностных лиц. Настоящее *Техническое руководство* содержит рекомендации для всех этих сторон, как на уровне высшего руководства, так и на уровне практикующих специалистов.

Хотя разработчики государственной политики зачастую не являются непосредственными исполнителями мер физической безопасности на уровне объекта, они обеспечивают правовую и стратегическую основу, на которой строится эффективная физическая безопасность. Они разрабатывают и принимают национальное законодательство о защите КВИ, имеют возможность регулировать деятельность владельцев/операторов КВИ из частного сектора и несут полную ответственность за безопасность своих граждан. Для этой аудитории в главе 2 **«Стратегические и правовые основы защиты объектов критически важной инфраструктуры»** представлены различные подходы, принятые государствами-участниками ОБСЕ, посредством обзора соответствующих законов, стратегий и мер политики и выявления ряда ключевых общих черт, включая процедуры определения КВИ, подходы к управлению рисками, управление чрезвычайными ситуациями и кризисами, а также компоненты международного сотрудничества. В следующей главе 3 **«Соображения в области прав человека»** права человека рассматриваются как важнейший компонент эффективной защиты КВИ от террористических атак. В защите КВИ зачастую участвуют частные субъекты – от владельцев/операторов КВИ до частных охранных компаний, поэтому в главе 4 рассматривается **частно-государственное партнерство**, а также даются рекомендации по установлению общих базовых ценностей для таких партнерств и обмену информацией по деликатным вопросам.

Вторая аудитория данного *Технического руководства* состоит из практикующих специалистов, ответственных за безопасность объектов КВИ. Оставшаяся часть *руководства* предназначена для таких специалистов. Тем не менее, им настоятельно рекомендуется также ознакомиться с тремя вышеупомянутыми главами.

Глава 5 **«Угроза терроризма и оценка рисков»** содержит общий обзор того, как террористическая угроза проявляется на объектах КВИ, а также рекомендации по способам управления риском терроризма на основе подхода, предполагающего учет «всех угроз и всех опасностей».

В центре внимания главы 6 находятся **меры физической безопасности,** рассмотрение которых начинается с концептуализации системы физической безопасности как части более крупной системы безопасности объекта КВИ. Затем подробно рассматриваются конкретные меры физической безопасности, включая системы обнаружения вторжений, охранное освещение, системы видеонаблюдения, системы контроля доступа и конструктивные решения для зданий.

В главе 7 **«Планирование безопасности и укрепление объекта»** представлен комплекс мер, направленных на противодействие различным способам, которыми террористы могут нарушить работу объекта КВИ, – от подрывов до нападений с использованием огнестрельного оружия. В этой главе особое внимание уделяется различным планам, которые владельцы/операторы КВИ должны учитывать в рамках своей миссии по обеспечению физической безопасности.

Хотя **управление внутренними угрозами,** которому посвящена глава 8, не является очевидной физической мерой безопасности, оно является важнейшим компонентом противодействия террористической угрозе для КВИ. В этой главе рассматриваются различные типы внутренних нарушителей, признаки враждебной инсайдерской деятельности, а также организационные меры реагирования на такие угрозы.

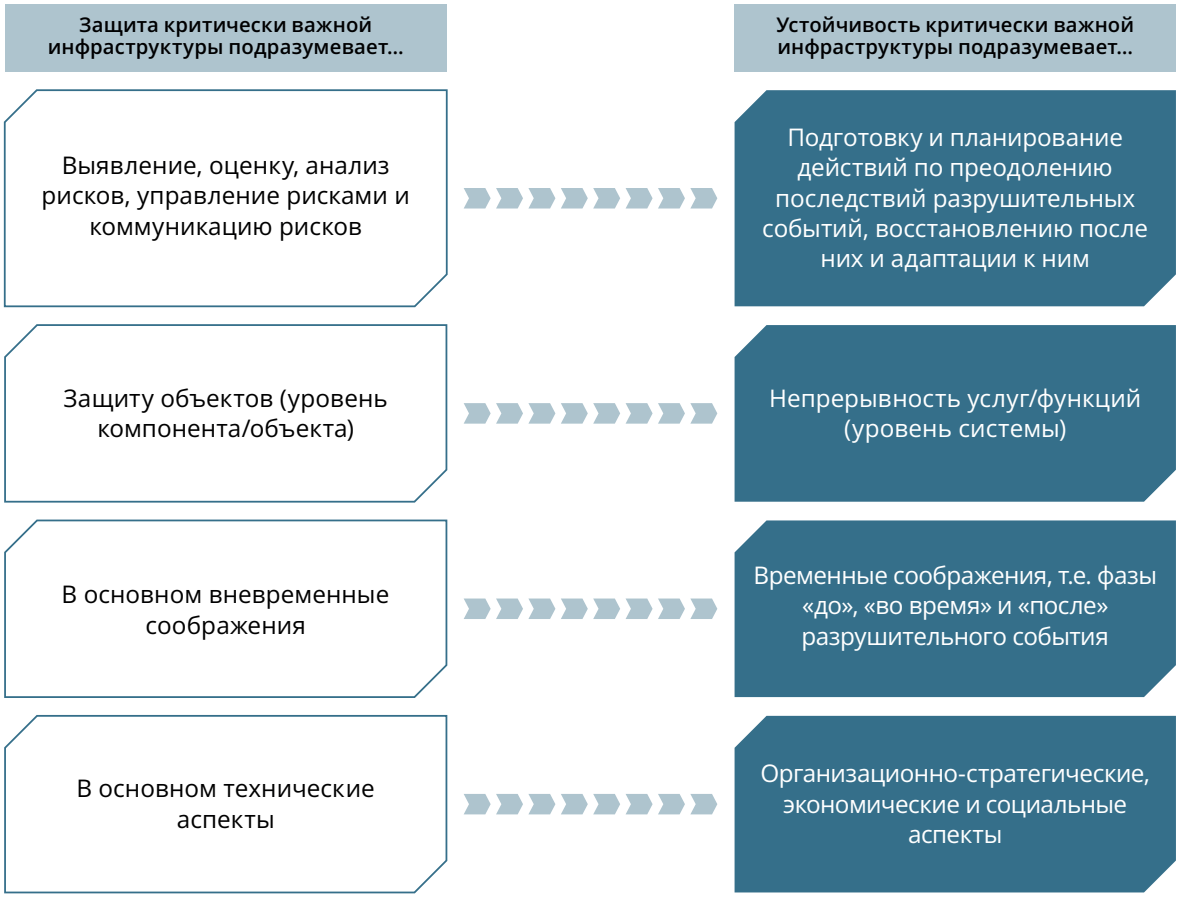
В главе **«Подготовка и учения»** подчеркивается важность подготовки персонала объекта к инцидентам, связанным с безопасностью, а также важность отработки действий в кризисных ситуациях, в том числе совместно с местными органами власти. Это может гарантировать, что в реальной чрезвычайной ситуации будут предприняты соответствующие и, возможно, спасающие жизни действия.

Поскольку террористическая угроза постоянно эволюционирует и затрагивает как локальную, так и региональную динамику, владельцы/операторы КВИ должны быть готовы адаптировать свои меры физической безопасности в ответ на это. Заключительная глава настоящего *Технического руководства*, **«Варианты существенной эскалации угроз»**, подробно рассматривает эту концепцию.

1.5 Пояснение к вопросу устойчивости критически важной инфраструктуры

Усилия по повышению физической безопасности КВИ обычно являются частью более широкого подхода владельцев/операторов КВИ и государственных структур к защите КВИ от различных угроз и опасностей. Одной из таких угроз является терроризм. В последние годы некоторые политики все чаще рассматривают ЗКВИ как часть более широкого подхода к устойчивости КВИ. Устойчивость КВИ включает в себя многие аспекты ЗКВИ, включая физическую безопасность, но также обеспечивает более широкую политическую и операционную основу, в центре которой находится непрерывность работы и функциональности КВИ, а не только защита объектов КВИ. Хотя настоящее *Техническое руководство* не содержит конкретных рекомендаций по способам повышения устойчивости объектов и секторов КВИ, при желании его содержание может быть использовано политиками государств-участников и другими лицами в качестве инструмента для содействия повышению устойчивости КВИ.

Ниже представлен полезный способ концептуализации некоторых различий между защитой КВИ и устойчивостью КВИ:[9]



9 Использовано с разрешения д-ра Бориса Петрень: Петрень, Б., «Повышение устойчивости критически важной инфраструктуры к террористическим угрозам» [презентация на конференции, 22 ноября 2024 г.]. См. также: Защита критически важной инфраструктуры ОБСЕ в Центральной Азии: укрепление устойчивости, усиление безопасности, Ашхабад 2024 [пресс-релиз]. Доступно по адресу: https://www.osce.org/secretariat/581707 [дата обращения: 21 июля 2025 г.].

Сам термин «устойчивость КВИ» по-разному определяется рядом заинтересованных сторон как в регионе ОБСЕ, так и за его пределами:

Правительство/Организация	Определение устойчивости
Организация экономического сотрудничества и развития (ОЭСР)	«Устойчивость можно определить как способность критически важной инфраструктуры выдержать неисправность, восстановиться после перебоев и адаптироваться к меняющимся условиям, сохраняя при этом ту же основную функцию, что и до деструктивного потрясения».[10]
Управление ООН по снижению риска бедствий	Устойчивость: «Способность системы, сообщества или общества, подверженного угрозам, противостоять последствиям угрозы, переносить их, приспосабливаться к ним и восстанавливаться своевременно и эффективно, в том числе посредством сохранения и восстановления своих основополагающих структур и функций».[11]
	«Устойчивость инфраструктуры является своевременным и эффективным средством профилактики, нейтрализации воздействий, восстановления и адаптации основных сооружений и функций национальной инфраструктуры, подвергшихся угрозам. Реализация устойчивости на всех этапах перебоев в работе должна осуществляться посредством совместного управления факторами риска и неопределенности, оценки множественных угроз и методов, учитывающих системный характер национальной инфраструктуры».[12]
Директива Европейского Союза (ЕС) об устойчивости критически важных объектов	«[Способность] критически важной организации предотвращать, защищаться, реагировать, противостоять воздействию, смягчать, нейтрализовать, улаживать инциденты и восстанавливаться после них».[13]
Австралия[14]	«Устойчивость критически важной инфраструктуры относится к тем аспектам организационной устойчивости, которые сосредоточены на мерах по повышению безопасности и устойчивости владельцев критически важной инфраструктуры, операторов и заинтересованных сторон в сетях поставок как коллектива и в масштабах всей экономики».[15]

Возможно, наиболее ярким свидетельством вышеупомянутого перехода от ЗКВИ к устойчивости КВИ со стороны политиков является Директива ЕС 2022 года об устойчивости критически важных объектов (2022/2557), известная как Директива об устойчивости критически важных объектов (CER). В преамбуле к Директиве, которая должна быть транспонирована во внутреннее законодательство всеми государствами-членами ЕС, предыдущая Директива ЕС о ЗКВИ (2008/114/ЕС) была

10 ОЭСР (2019 г.), *Эффективное управление для устойчивости критически важной инфраструктуры.* Доступно по адресу: https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html [дата обращения: 21 июля 2025 г.].

11 Управление ООН по снижению риска бедствий (UNDRR) (2017 г.), *Терминология Сендайской рамочной программы по снижению риска бедствий*, Определение: Устойчивость. Доступно по адресу: https://www.undrr.org/terminology/resilience [дата обращения: 21 июля 2025 г.].

12 UNDRR (2022 г.), *Принципы обеспечения устойчивости инфраструктуры,* стр. 16. Доступно по адресу: https://www.undrr.org/media/78694/download?startDownload=20250319 [дата обращения: 21 июля 2025 г.].

13 ЕС (2022 г.), Директива 2022/2557 Европейского парламента и Совета от 14 декабря 2022 года об устойчивости критически важных субъектов и отмене Директивы Совета 2008/114/ЕС, *OJ* L 333. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [дата обращения: 21 июля 2025 г.].

14 Данное определение дается только в контексте Стратегии Австралии по обеспечению устойчивости критически важной инфраструктуры.

15 Правительство Австралии – Министерство внутренних дел (февраль 2023 г.), *Стратегия устойчивости критически важной инфраструктуры.* Доступно по адресу: https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf [дата обращения: 21 июля 2025 г.].

отменена и заменена Директивой CER. Ниже приведено описание этого процесса, в котором подчеркивается различие между ЗКВИ и устойчивостью КВИ:

> «Директива Совета 2008/114/ЕС [...] предусматривает процедуру обозначения европейской критически важной инфраструктуры в секторах энергетики и транспорта, нарушение или разрушение которой будет иметь существенное трансграничное воздействие по крайней мере на два государства-члена. Эта Директива сосредоточена исключительно на защите такой инфраструктуры. Однако оценка Директивы 2008/114/ЕС, проведенная в 2019 году, показала, что из-за все более взаимосвязанного и трансграничного характера операций с использованием критически важной инфраструктуры защитные меры, касающиеся только отдельных объектов, недостаточны для предотвращения всех сбоев. Поэтому необходимо изменить подход в сторону обеспечения того, чтобы риски лучше учитывались, чтобы роль и обязанности критически важных субъектов как поставщиков услуг, необходимых для функционирования внутреннего рынка, были более четко определены и последовательны, и чтобы правила Союза были приняты для повышения устойчивости критически важных субъектов. Критически важные субъекты должны быть в состоянии усилить свою способность предотвращать, защищать, реагировать, противостоять, смягчать, нейтрализовать, приспосабливаться и восстанавливаться после инцидентов, которые могут нарушить предоставление основных услуг».

Практика: принципы обеспечения устойчивости инфраструктуры Управления ООН по снижению риска бедствий (2022 г.)[16]

В 2022 году Управление ООН по снижению риска бедствий (UNDRR) определило шесть принципов, дополненных целями и рекомендациями, для укрепления устойчивости КВИ и «обеспечения непрерывности предоставления критически важных услуг системами экономической инфраструктуры». Эти принципы применимы к деятельности «органов государственного управления любого уровня, учреждений, доноров, инвесторов, собственников, регуляторов, операторов, проектировщиков и подрядчиков, поставщиков услуг и международных организаций, которые заинтересованы в реализации комплекса действий по повышению устойчивости инфраструктуры, способствующих достижению положительных результатов в экономической, социальной и природоохранной сфере». UNDRR опубликовало руководство по внедрению этих принципов в 2023 году.[17]

Принцип	Описание	Цель
1	Непрерывное обучение	Развивать и обновлять понимание и видение устойчивости инфраструктуры.
2	Упреждающая защита	В упреждающем порядке планировать, проектировать, строить и эксплуатировать объекты инфраструктуры, готовые к текущим и будущим опасностям.
3	Экологическая интегрированность	Работать в позитивной интеграции с окружающей средой.
4	Социальная вовлеченность	Развивать активное взаимодействие, вовлеченность и участие на всех уровнях общества.
5	Совместная ответственность	Обмениваться информацией и опытом для получения скоординированных выгод.
6	Адаптивная трансформация	Адаптироваться и трансформироваться в соответствии с меняющимися потребностями.

Источник: UNDRR

1.6 Пояснение к вопросу кибербезопасности

Хотя настоящее *Техническое руководство* не содержит подробных ссылок на кибербезопасность, необходимо признать и подчеркнуть ее важность как составной части комплексного подхода к ЗКВИ. Многие инструменты и сервисы, облегчающие эксплуатацию КВИ – от промышленных систем управления до систем связи, отопления, вентиляции и кондиционирования воздуха (ОВиК), и других технологий – объединены в сеть или подключены к Интернету и, следовательно, уязвимы для кибератак. В результате локальные операции на объекте КВИ может быть скомпрометирована злоумышленниками, находящимися за тысячи километров.

16 UNDRR (2022 г.), *Принципы устойчивой инфраструктуры*. Доступно по адресу: https://www.undrr.org/publication/principles-resilient-infrastructure [дата обращения: 21 июля 2025 г.].

17 UNDRR (2023 г.), *Руководство по внедрению принципов устойчивой инфраструктуры*. Доступно по адресу: https://www.undrr.org/publication/handbook-implementing-principles-resilient-infrastructure [дата обращения: 21 июля 2025 г.].

Международная лига безопасности и Конфедерация европейских служб безопасности (CoESS) признают, что «когда устройства на местах обмениваются данными с сетевыми центрами обработки данных, а компьютерные системы подключаются к Интернету, площадь атаки расширяется экспоненциально».[18] Хотя настоящее *Техническое руководство* не рассматривает проблему кибербезопасности напрямую, по мере того, как владельцы/операторы КВИ внедряют все больше новых технологий для упрощения своей деятельности, управление как физическими рисками, так и киберрисками будет становиться все более сложным.

Во многих случаях государства-участники ОБСЕ и руководители служб безопасности, которым поручено заниматься ЗКВИ, подходят к обеспечению безопасности КВИ комплексно, то есть их политика и практика учитывают и устраняют как физические риски, так и киберриски. Хотя настоящее *Техническое руководство* сосредоточено на аспектах физической безопасности КВИ, это дает возможность проиллюстрировать важность и ценность комплексного подхода к безопасности и устойчивости, при котором определяются и интегрируются меры по обеспечению как кибербезопасности, так и физической безопасности. В 2023 году Международная лига безопасности и CoESS заявили:

> «Владельцы критически важных инфраструктурных объектов используют подключенные системы для повышения производительности и эффективности. Традиционно изолированные устройства в системах диспетчерского управления и сбора данных и промышленных системах управления теперь используют [промышленный Интернет вещей] для передачи данных от электростанций до водоочистных сооружений. Интеграция компьютеров и других технологий в конструкцию и функционирование физической инфраструктуры стала обычным явлением. Компьютеры [...] теперь интегрированы в физическую инфраструктуру,

18 *Международная лига безопасности*, CoESS (2023 г.), *Киберфизическая безопасность и критическая инфраструктура.* Доступно по адресу: https://www.bdsw.de/images/pdf/isl-coess-cyberphysicalsecurity-wp.pdf [дата обращения: 21 июля 2025 г.].

что наиболее отчетливо наблюдается в развитии технологии «умных сетей», где сетевые компьютеры и коммуникационные технологии работают автономно для решения проблем в электросети, управления потреблением энергии и ее выработкой. Автоматизированное управление дорожным движением стало частью транспортной инфраструктуры, а «умные» системы водоснабжения упреждающе отслеживают состояние своей собственной физической инфраструктуры».[19]

Физическая и кибербезопасность для объектов КВИ тесно переплетены: физическая безопасность на объекте КВИ может быть нарушена кибератакой, а кибербезопасность на объекте может быть подорвана физической террористической атакой. Это называется киберфизической конвергенцией и является областью, вызывающей все большую озабоченность у разработчиков политики и владельцев/операторов КВИ. Агентство по кибербезопасности и защите инфраструктуры (CISA) Министерства внутренней безопасности США (DHS) приводит примеры этого явления:

- «Пробелы в системе безопасности контроля доступа, такие как несанкционированный доступ к объектам или системные допуски, могут позволить человеку использовать USB-устройство [...] или другое съемное оборудование для внедрения вируса или вредоносного ПО в сеть.
- Системы отопления, вентиляции и кондиционирования воздуха (ОВиК) могут быть фактически выведены из строя, что приведет к повышению температуры и выходу из строя сетевых серверов.
- Кибератака на телекоммуникационные системы может нарушить связь с правоохранительными органами и аварийно-спасательными службами, что приведет к задержке реагирования.
- Беспилотная авиационная система (БАС) может скомпрометировать конфиденциальную информацию, получив доступ к незащищенной сети помощью технологии беспроводного взлома».[20]

Взаимодействие между физической безопасностью и кибербезопасностью признано на политическом уровне. Например, Директива Европейской комиссии (ЕС) 2022/2555 о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе (Директива NIS 2) гласит: «Учитывая взаимосвязь между кибербезопасностью и физической безопасностью субъектов, следует обеспечить согласованный подход между [Директивой (ЕС) 2022/2557 Европейского парламента и Совета от 14 декабря 2022 года об устойчивости критически важных организаций] и настоящей Директивой».[21]

19 Международная лига безопасности, CoESS (2023 г.), *Киберфизическая безопасность и критическая инфраструктура.* Доступно по адресу: https://www.bdsw.de/images/pdf/isl-coess-cyberphysicalsecurity-wp.pdf [дата обращения: 21 июля 2025 г.].

20 Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Конвергенция кибербезопасности и физической безопасности.* Доступно по адресу: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf [дата обращения: 21 июля 2025 г.].

21 Совет Европейского Союза (СЕ), Директива Совета 2008/114/ЕС от 14 декабря 2022 г. о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе, вносящая поправки в Регламент (ЕС) № 910/2014 и Директиву (ЕС) 2018/1972 и отменяющая Директиву (ЕС) 2016/1148 (Директива NIS 2), OJ L 333, пункт 30. Доступно по адресу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555 [дата обращения: 21 июля 2025 г.].

Таким образом, хотя настоящее *Техническое руководство* фокусируется на угрозах физической безопасности, связанных с террористическими атаками, оно призывает политиков, владельцев/операторов КВИ и других заинтересованных лиц укреплять сотрудничество со своими коллегами по кибербезопасности, поскольку «когда руководители служб безопасности действуют в изолированных областях [кибербезопасности и физической безопасности], у них отсутствует целостное представление об угрозах безопасности, направленных на их предприятие».[22] Поэтому государства-участники и владельцы/операторы КВИ могут извлечь пользу из устранения разобщенности между этими сообществами и разработки комплексного подхода к управлению рисками на уровне объекта, организации и сектора.

22 Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Конвергенция кибербезопасности и физической безопасности*. Доступно по адресу: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520and%2520Physical%2520Security%2520Convergence_508_01.05.2021.pdf [дата обращения: 21 июля 2025 г.].

2 Стратегические и правовые основы защиты объектов критически важной инфраструктуры

«

В государствах-участниках ОБСЕ основные концепции и подходы к защите критически важной инфраструктуры чаще всего определяются в правовых и политических документах, в рамках которых могут быть определены меры физической безопасности.

»

2 Стратегические и правовые основы защиты объектов критически важной инфраструктуры

В Резолюции 2341 (2017 г.) Совета Безопасности Организации Объединенных Наций (СБ ООН) Совет Безопасности ООН:[23]

> «призна[ет], что каждое государство само определяет, какие объекты его инфраструктуры являются критически важными и как обеспечить их эффективную защиту от террористических нападений, [...]
>
> «призывает государства-члены рассмотреть возможность разработки или дальнейшего совершенствования своих стратегий уменьшения рисков террористических нападений на критически важные объекты инфраструктуры — стратегий, которые должны предусматривать, в частности, оценку и улучшение понимания соответствующих рисков, принятие мер по обеспечению готовности, в том числе эффективного реагирования на такие нападения, а также содействие повышению оперативной совместимости в области безопасности и ликвидации последствий и поддержку эффективного взаимодействия всех заинтересованных сторон».

23 СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

В данной главе представлены различные подходы, применяемые государствами-участниками ОБСЕ. Они охватывают важные аспекты ЗКВИ, такие как процедуры определения КВИ, управление рисками, управление чрезвычайными ситуациями и кризисами, а также международное сотрудничество. Важно отметить, что данная глава не охватывает все соответствующие стратегические и правовые основы, которые могут повлиять на ЗКВИ в той или иной стране. Например, законы или нормативные акты, разрешающие или ограничивающие использование БАС (беспилотных авиационных систем), влияют на то, кто имеет доступ к этой технологии и для каких целей – все это может повлиять на безопасность КВИ.

Во многих случаях эти подходы обеспечивают основу для ЗКВИ на национальном уровне. Они представляют собой ключевой элемент многокомпонентной системы физической безопасности и обычно предоставляют стратегические рекомендации и инструкции соответствующим заинтересованным сторонам. Руководство по физической безопасности на уровне объекта (как представлено в настоящем *Техническом руководстве*), техническая поддержка владельцев/операторов КВИ и выделение государственных средств играют ключевую роль в содействии эффективной реализации этих стратегических и правовых основ ЗКВИ.

Обратите внимание, что многие европейские практические подходы, упомянутые в этом разделе, могут быть изменены после вступления в силу в 2023 году Директивы Европейского союза об устойчивости критически важных объектов (2022/2557).

В государствах-участниках ОБСЕ основные концепции и подходы к ЗКВИ чаще всего определяются в правовых и политических документах, обеспечивающих всеобъемлющую основу для защиты КВИ, в рамках которой могут быть определены меры физической безопасности. Это касается в первую очередь терминологии, определяющей саму КВИ, которая варьируется от критически важной инфраструктуры до «стратегических объектов»,[24] «жизненно важных установок»[25] и других терминов.[26] Учитывая такое разнообразие, настоящее *Техническое руководство* не претендует на единое определение КВИ. Эта прерогатива принадлежит каждому государству, как подтверждено в Резолюции Совета Безопасности ООН 2341 (2017 г.).

В некоторых случаях основные компоненты ЗКВИ содержатся в специализированных межсекторальных национальных стратегиях или планах действий. Эти документы зачастую устанавливают общие параметры для разработки подробных нормативных рамок.

24 Постановление Правительства Кыргызской Республики № 56/2015: Об утверждении Требований к режиму функционирования и эксплуатации стратегических объектов. Доступно по адресу: https://cbd.minjust.gov.kg/97305/edition/617411/ru [дата обращения: 21 июля 2025 г.].

25 Кодекс обороны, Глава II: Защита жизненно важных объектов, статьи R1332-1 и R1332-42. (2015 г., Франция). Доступно по адресу: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006574323 [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

26 В Законе Эстонии о государственной обороне используется термин «объект государственной обороны, связанный с предоставлением жизненно важной услуги». См.: Закон о государственной обороне (11 февраля 2015 г., Эстония). Доступно по адресу: https://www.riigiteataja.ee/en/eli/502042019010/consolide [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

В других случаях основные принципы ЗКВИ закрепляются в специальных законодательных актах. Уровень детализации этих законов существенно различается. Например, Закон Словении 2017 года о критической инфраструктуре[27] определяет понятие КВИ, регулирует критерии ее идентификации и обозначения, определяет задачи компетентных государственных органов и владельцев/операторов КВИ и рассматривает вопросы обмена информацией, защиты данных, а также санкций за несоблюдение требований законодательства. В Люксембурге задача регулирования обозначения КВИ и определения структуры безопасности владельцев/операторов и планирования непрерывности деятельности возложена на исполнительную ветвь власти.[28] В некоторых случаях основные политические документы по ЗКВИ прямо подчеркивают физическую безопасность как основополагающую цель. В стратегии национальной безопасности Нидерландов «обеспечение лучшей защиты критически важной инфраструктуры» является приоритетным направлением на 2023–2027 годы.[29]

27 Закон о критической инфраструктуре (22 декабря 2017 г., Словения). Доступно по адресу: https://pisrs.si/pregledPredpisa?id=ZAKO7106 [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

28 Закон от 23 июля 2016 года о создании Верховной комиссии по национальной защите (29 июля 2022 г., Люксембург). Доступно по адресу: http://data.legilux.public.lu/eli/etat/leg/loi/2016/07/23/n1 [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

29 Правительство Нидерландов (3 апреля 2023 г.) *Стратегия безопасности Королевства Нидерландов*. Доступно по адресу: https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands [дата обращения: 21 июля 2025 г.].

Национальная практика: стратегический акцент Канады на межсекторальном сотрудничестве (2009 г.)[30]

Особенностью Национальной стратегии Канады по защите критически важной инфраструктуры 2009 года является ее ориентация на межсекторальные подходы и инициативы. Поскольку Канада работает над укреплением своего подхода к КВИ, содействие межсекторальному сотрудничеству с учетом угроз для достижения общих целей остается ключевым элементом подхода Канады к обеспечению безопасности и устойчивости КВИ.

В соответствии с этим подходом Министерство общественной безопасности Канады – правительственное ведомство, отвечающее за вопросы общественной безопасности, управления чрезвычайными ситуациями, национальной безопасности и готовности к чрезвычайным ситуациям – сотрудничает с ключевыми секторами в целях разработки прочного, общего понимания угроз и взаимозависимостей как основы эффективного межсекторального сотрудничества. Одним из примеров успешного сотрудничества между секторами является межсекторальное исследование (под руководством финансового сектора) для оценки уровня взаимозависимости объектов критически важной инфраструктуры финансового, телекоммуникационного и электроэнергетического секторов. Исследование было проведено совместно экспертами из всех трех секторов и выявило возможности для повышения межсекторальной устойчивости, дополненные практическими рекомендациями. Уроки, извлеченные из этой и других подобных успешных инициатив, могут послужить стимулом и основой для будущего межсекторального сотрудничества.

Источник: Министерство общественной безопасности Канады

В ЕС существенный стимул законодательной деятельности изначально был создан Директивой 2008 года об идентификации и обозначении европейских критически важных инфраструктур и оценке необходимости улучшения их защиты.[31] Опираясь на Директиву 2008 года, Бельгия постепенно совершенствовала свое законодательство, связанное с ЗКВИ, расширяя его первоначальный охват с энергетики и транспорта (два основных сектора в Директиве 2008 года), до сфер финансов, здравоохранения, водоснабжения и критически важной информационной инфраструктуры.[32] Директива ЕС 2008 года также была транспонирована в национальное законодательство различными странами-кандидатами на вступление в ЕС в рамках их усилий по согласованию с законодательной базой ЕС (известной как *acquis communautaire*).

30 Министерство общественной безопасности Канады (2009 г.), *Национальная стратегия для критически важной инфраструктуры*. Доступно по адресу: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx#s0 [дата обращения: 21 июля 2025 г.].

31 CE 2008/114/EC от 8 декабря 2008 г. об идентификации и обозначении важнейшей европейской инфраструктуры и оценке необходимости улучшения ее защиты, *OJ* L 345. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2008/114/oj [дата обращения: 21 июля 2025 г.].

32 Противодействие нарушению функционирования критически важной инфраструктуры (15 июля 2011 г., Бельгия). Доступно по адресу: https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2011070108&table_name=wet [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

Например, в законодательстве Черногории 2019 года целая глава посвящена «Европейской критически важной инфраструктуре».[33]

Подобно импульсу, созданному Директивой 2008 года, вступление в силу Директивы CER в 2023 году вызвало волну законодательных реформ в государствах-членах ЕС.[34] Директива CER отменила вышеупомянутую Директиву 2008 года и заложила новую основу для ЗКВИ и устойчивости КВИ в Европейском союзе и за его пределами. Директива CER была принята вместе с директивой о кибербезопасности, известной как Директива NIS2.[35] Крайний срок для государств-членов по принятию и публикации мер, необходимых для соответствия этим двум инструментам, был установлен на октябрь 2024 года. Например, парламент Германии разрабатывает «Зонтичный закон KRITIS»[36], который направлен на реализацию Директивы CER путем усиления устойчивости и физической защиты КВИ, дополняя существующие правила кибербезопасности.[37]

Что касается физической безопасности КВИ, то Статья 13 Директивы CER гласит:

> «Государства-члены должны гарантировать, что критически важные организации принимают надлежащие и пропорциональные технические и организационные меры и меры безопасности для обеспечения их устойчивости, основываясь на соответствующей информации, предоставляемой государствами-членами ЕС об оценках рисков государств-членов ЕС и о результатах оценок рисков критически важных организаций, включая меры, необходимые для [...] обеспечения физической защиты их помещений и критически важной инфраструктуры, надлежащим образом рассматривая необходимость, например, ограждения забором, барьерами, средств и процедур наблюдения за периметром, оборудования обнаружения и контроля доступа».[38]

33 Закон о восстановлении и защите критически важной инфраструктуры, Закон о ЗКВИ, 72/19 (30 января 2020 г., Черногория). Доступно по адресу: https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e [дата обращения: 21 июля 2025 г.] неофициальный перевод.

34 ЕС (2022 г.), Директива 2022/2557 Европейского парламента и Совета от 14 декабря 2022 года об устойчивости критически важных субъектов и отмене Директивы Совета 2008/114/ЕС, *OJ* L 333. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [дата обращения: 21 июля 2025 г.].

35 ЕС (2022 г.), Директива 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности в Союзе, вносящая поправки в Регламент (ЕС) № 910/2014 и Директиву (ЕС) 2018/1972 и отменяющая Директиву (ЕС) 2016/1148 (Директива NIS2), *OJ* L 333. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng [дата обращения: 21 июля 2025 г.].

36 KRITIS расшифровывается как Kritische Infrastrukturen, что в переводе с немецкого означает «критически важная инфраструктура».

37 Некоторые страны могут столкнуться с институциональными проблемами при принятии межсекторальных мер по ЗКВИ. В Швейцарии в недавнем заключении Федерального совета подчеркнуто, что наличие существенных различий в регулировании в подсекторах ЗКВИ в стране «обусловлено, в частности, тем фактом, что [федеральный уровень правительства] не имеет общих регулирующих полномочий в этой области. Такая компетенция должна быть создана в рамках частичного пересмотра Федеральной конституции».

38 ЕС (2022 г.), Директива 2022/2557 Европейского парламента и Совета от 14 декабря 2022 года об устойчивости критически важных субъектов и отмене Директивы Совета 2008/114/ЕС, *OJ* L 333. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [дата обращения: 21 июля 2025 г.].

От защиты критически важной инфраструктуры к устойчивости: стратегический сдвиг в Европейском Союзе

В 2013 году в результате оценки хода реализации Директивы о КВИ 2008 года был выявлен ряд проблем. В частности, было отмечено, что «несмотря на то, что Директива способствовала укреплению европейского сотрудничества в процессе ЗКВИ, она в основном поощряла двустороннее взаимодействие государств-членов вместо создания реального европейского форума для сотрудничества. Секторально-ориентированный подход Директивы также представляет собой проблему для ряда государств-членов, поскольку на практике анализ критически важных факторов не ограничивается секторальными границами и следует скорее «системному» или «сервисному» подходу (например, больницы, финансовые услуги)».[39] Руководствуясь необходимостью перехода от секторальной к более системной модели, Европейская комиссия возглавила процесс разработки нового стратегического подхода.

Результатом этого процесса стало принятие Директивs ЕС об устойчивости критически важных объектов (Директивы CER), в которой подчеркивается широкая концепция «устойчивости». Она выходит за рамки технического понятия «защиты» и включает в себя общую непрерывность функционирования и способность готовиться к различным сбоям, противостоять им, адаптироваться к ним и восстанавливаться после них.

В соответствии с Директивой CER государства-члены ЕС теперь обязаны разрабатывать, внедрять и регулярно обновлять меры по повышению устойчивости, гарантируя, что критически важные субъекты, расположенные на их территориях, смогут быстро адаптироваться к меняющимся угрозам и обстоятельствам.

В некоторых случаях базовые подходы к ЗКВИ также встраиваются в более широкие рамочные основы национальной безопасности государств-участников. Например, ЗКВИ занимает центральное место в Стратегии безопасности Словацкой Республики 2021 года,[40] а в Норвегии Закон 2019 года предусматривает ключевую координирующую роль Управления национальной безопасности – межотраслевого профессионального и надзорного органа в составе Министерства обороны – в реализации главы 7 Закона «Национальные критически важные объекты и инфраструктура».[41]

Поскольку сбои в работе КВИ и их каскадные последствия могут привести к экономическому и социальному параличу или хаосу, некоторые государства-участники закрепили задачу ЗКВИ в законодательстве, касающемся стихийных

39 Европейская комиссия (2013 г.), Рабочий документ персонала комиссии о новом подходе к Европейской программе защиты критически важной инфраструктуры. Повышение безопасности европейской критически важной инфраструктуры. Доступно по адресу: https://home-affairs.ec.europa.eu/system/files/2020-09/swd_2013_318_on_epcip_en.pdf [дата обращения: 19 мая 2025 г.].

40 Правительство Словацкой Республики (2021 г.), *Стратегия безопасности Словацкой Республики*. Доступно по адресу: https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf [дата обращения: 4 мая 2025 г.].

41 Правительство Королевства Норвегия (2019 г.), Закон о национальной безопасности (Закон о безопасности). Доступно по адресу: https://lovdata.no/dokument/NLE/lov/2018-06-01-24 [дата обращения: 21 июля 2025 г.].

бедствий и чрезвычайных ситуаций. Например, в Польше правовая основа для национальной программы ЗКВИ разработана в соответствии с Законом об управлении кризисами 2007 года; программа обновляется каждые два года.[42]

В регионе ОБСЕ большое количество правовых и политических рамочных инструментов, связанных с КВИ, предусматривают применение «подхода, учитывающего все виды угроз и опасностей», то есть они обеспечивают защитные механизмы, направленные на смягчение различных угроз для КВИ, будь то природного (изменение климата, неблагоприятные погодные условия, землетрясения) или антропогенного (терроризм, преступная деятельность, халатность) происхождения. Более подробную информацию об этом подходе можно найти ниже в главе 5 «Угроза терроризма и оценка рисков».

В других государствах-участниках механизмы ЗКВИ строятся вокруг одного вида угроз, в частности, терроризма. Например, в Кыргызской Республике «разработка и реализация мер по минимизации последствий террористических актов для стратегических объектов» является центральным элементом Национальной программы по борьбе с терроризмом на 2023–2027 годы.[43]

При анализе различных подходов к определению ЗКВИ правительствами государств-участников ОБСЕ можно выделить несколько основных принципов. Они представлены в таблице ниже.

Принцип	Описание
Общая ответственность	Обеспечение безопасности объектов КВИ является общей ответственностью органов государственной власти (федерального, государственного или местного уровня) и владельцев/операторов объектов КВИ.
Выстраивание партнерских отношений	Повышение устойчивости защиты КВИ требует дополнительных и согласованных действий всех партнеров, как из частного, так и из государственного секторов.
Непрерывное планирование	ЗКВИ основана на непрерывном процессе управления рисками, включая оценку угроз и их смягчение.
Защита на всех этапах	Необходимо обеспечить защитные меры до, во время и после сбоев в работе КВИ, чтобы общество могло противостоять инцидентам, управлять ими, восстанавливаться и извлекать из них уроки.
Общесистемная защита	Эффективность ЗКВИ зависит от приверженности широкого круга заинтересованных сторон, включая общественность.
Пропорциональность	Защитные меры должны обеспечивать оптимальный баланс между затратами и предполагаемыми выгодами.
Обмен данными и защита данных	Обмен информацией с соответствующими заинтересованными сторонами и защита информации являются необходимыми и дополнительными предпосылками для устойчивости защиты КВИ.

42 Закон от 26 апреля 2007 г. об управлении кризисами, Законодательный вестник 2007 г. № 89, ст. 590 (26 апреля 2007 г., Польша). Доступно по адресу: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20070890590 [по состоянию на 21 июля 2025 г.] неофициальный перевод.

43 Кабинет Министров Кыргызской Республики (15 марта 2023 г.), Программа Кабинета Министров Кыргызской Республики по противодействию экстремизму и терроризму на 2023-2027 годы. Доступно по адресу: https://cbd.minjust.gov.kg/160032/edition/1241419/ru [дата обращения: 21 июля 2025 г.].

2.1 Определение критически важной инфраструктуры: критерии и процедуры

Процедура определения отдельных объектов, систем и процессов, которые считаются заслуживающими защиты, является сложной и специфичной для каждой страны. В большинстве случаев критерии, используемые для определения конкретных объектов и систем, являются строго конфиденциальными с ограниченным доступом. Однако на стратегическом уровне во многих государствах-участниках приняты рекомендации по процедуре определения КВИ. В качестве первого шага многие государства-участники выявляют или определяют секторы и подсекторы КВИ.

Во многих государствах-участниках зачастую встречаются несколько общих секторов, относящихся к КВИ: энергетика, коммуникационные/информационные технологии, транспорт, здравоохранение, управление водными ресурсами, продовольствие, финансы и государственное управление.[44]

Многие из европейских практических подходов, упомянутых в этом разделе, могут быть изменены после вступления в силу Директивы ЕС об устойчивости критически важных объектов в соответствии с ее статьей 6 «Определение критически важных субъектов».

В целом, государства-участники ОБСЕ используют различные институциональные процессы для идентификации и обозначения КВИ. Законодательство Черногории позволяет правительству определять КВИ, которые не включены в заранее установленные перечни критически важных секторов. Соответствующие министерства определяют, соответствуют ли системы, сети и объекты, относящиеся к их секторам, установленным критериям, и представляют свои предложения государственному органу, ответственному за внутренние дела. Этот орган представляет консолидированные предложения правительству, которое принимает окончательное решение. Владельцы/операторы КВИ обязаны информировать соответствующие министерства об изменениях, затрагивающих инфраструктуру, которая была обозначена как критически важная, что может привести, после принятия решения правительством, к внесению изменений в национальный перечень КВИ.[45] В Швеции этот процесс основан на совместном, горизонтальном и неиерархическом подходе с участием как центральных, так и местных органов власти. Ответственность за определение КВИ возлагается на муниципалитеты, окружные советы, окружные административные советы и национальные органы власти в соответствии с их сферами ответственности, включая географические районы, где расположены

44 Вместо того чтобы в целом определить «правительство/государственное управление» как критически важный сектор, некоторые страны предпочитают выделять только определенные государственные услуги как критически важные, например, «экстренные службы» (в Чешской Республике, Германии, Кыргызской Республике, Польше, Великобритания, США). В Швеции «социальное обеспечение» и «муниципальные технические услуги» считаются двумя автономными критически важными секторами.

45 Закон о назначении и защите критической инфраструктуры, Закон о КВИ, 72/19 (30 января 2020 г., Черногория) Доступно по адресу: https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e [дата обращения: 21 июля 2025 г.] неофициальный перевод.

объекты.[46] Во Франции правительство не определяет КВИ напрямую. Вместо этого оно назначает «операторов жизненно важных объектов», которые затем отвечают за определение конкретных объектов как критически важных.[47]

Национальная практика: жизненно важные объекты во Франции (2015 г.)[48]

Во Франции этапы обозначения КВИ, известных как «жизненно важные объекты», описаны в оборонном кодексе страны:

- Премьер-министр разрабатывает список «жизненно важных секторов» после консультаций с Межведомственной комиссией по обороне и безопасности и назначает «министра-координатора» для каждого определенного сектора.
- В каждом секторе, находящемся в их ведении, координирующие министры уведомляют операторов инфраструктуры о своем намерении обозначить их как «операторов жизненно важных объектов» на основе выполнения двух условий: i) их деятельность осуществляется полностью или частично в секторе жизненно важного значения; ii) они управляют или используют по крайней мере одно учреждение, сооружение или объект, повреждение, недоступность или разрушение которого в результате злонамеренных действий, саботажа или терроризма может иметь серьезные последствия для способности к выживанию нации или здоровья или жизни населения.
- Уведомленные операторы должны представить свои замечания в течение двух месяцев. После назначения они предлагают список «жизненно важных объектов» в качестве приложения к своим планам безопасности. Затем административный орган присваивает им статус «жизненно важных объектов».

Источник: Правительство Франции

Для определения отдельных объектов, систем или процессов в качестве критически важных многие государства-участники применяют как отраслевые, так и межотраслевые критерии. Отраслевые критерии обычно определяются министерствами, ответственными за отдельные секторы, и учитывают особенности этих секторов. Напротив, межотраслевые критерии основаны на оценке воздействия, вызванного нарушением или разрушением отдельного объекта инфраструктуры, обычно с точки зрения «ожидаемых» жертв, экономического воздействия или различных социальных последствий (например, влияния на общественное доверие, нарушения повседневной жизни, степени ухудшения состояния окружающей среды).

46 Шведское агентство по чрезвычайным ситуациям гражданского характера (MSB) (2014 г.), *План действий по защите жизненно важных социальных функций и критически важной инфраструктуры.* Доступно по адресу: https://www.msb.se/siteassets/dokument/publikationer/english-publications/action-plan-for-the-protection-of-vital-societal-functions--critical-infrastructure.pdf [дата обращения: 4 мая 2025 г.]. Этот практический подход может быть изменен после вступления в силу Директивы CER.

47 Правительство Французской Республики (2015 г.), Кодекс обороны, Глава II: Защита объектов жизненной важности, Статьи R1332-1 à R1332-42. Доступно по адресу: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006574323 [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

48 Правительство Французской Республики (2015 г.), Кодекс обороны, Глава II: Защита объектов жизненной важности, Статьи R1332-1 à R1332-42. Доступно по адресу: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006574323 [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

Ниже приведены два примера:

- В Германии используется «порог в 500 000 человек» в качестве ориентира. Например, электростанция считается критически важной, если ее установленная чистая номинальная мощность превышает 104 гигаватт, что соответствует электроснабжению более 500 000 человек. Обоснование заключается в том, что отключения, затрагивающие более 500 000 человек, невозможно эффективно устранить с помощью текущего аварийного планирования и эксплуатационных возможностей.[49]
- В Чешской Республике указ президента определяет критерии, используемые для идентификации КВИ в каждом критически важном секторе. Например, в разделе «Управление водными ресурсами» источник считается критически важным, если он незаменим и обеспечивает водой не менее 125 000 жителей. В секторе здравоохранения «статус критической важности» присваивается, в частности, медицинским учреждениям с общим числом коек в отделениях интенсивной терапии не менее 2 500.[50]

Как упоминалось выше, критерии, используемые правительствами для идентификации КВИ, не всегда находятся в открытом доступе. В Хорватии эти критерии отнесены к категории конфиденциальной информации и имеют соответствующий уровень секретности в соответствии со специальными правилами о секретности данных.[51]

Помимо секторов и подсекторов, в некоторых государствах-участниках существуют категории КВИ, отражающие различные потребности и административные механизмы. В соответствии с законом Латвии о национальной безопасности, основной причиной разграничения категории А («особо важная КВИ») и категорий В и С («важная КВИ» и «КВИ» соответственно) является необходимость регламентировать, какой субъект отвечает за реализацию мер физической безопасности.[52] В Нидерландах эти различия используются в качестве руководства для определения приоритетов в управлении определенными инцидентами и наращивания возможностей для повышения устойчивости. Категория А существенно отличается от категории В тем, что первая включает в себя инфраструктуру, нарушение, повреждение или отказ которой предположительно вызовут особенно серьезные экономические, физические или

49 Правительство Федеративной Республики Германия (2016 г.), Положение об определении критически важных инфраструктур в соответствии с Законом о безопасности и инфраструктуре (BSI). Часть 2: Расчетные формулы для определения порогового значения. Доступно по адресу: https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf [по состоянию на 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

50 Правительство Чешской Республики (22 декабря 2010 г.), Постановление правительства № 432/2010 о критериях определения критического элемента инфраструктуры. Доступно по адресу: https://nukib.gov.cz/download/publications_en/legislation/Order_432_2010_EN_v1.0_final.pdf [доступ 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

51 Закон о критически важной инфраструктуре (2 мая 2013 г., Хорватия). Доступно по адресу: https://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html [дата обращения: 21 июля 2025 г.] неофициальный перевод.

52 Латвия, Закон о национальной безопасности (2000 г.). Доступно по адресу: https://sab.gov.lv/files/uploads/2023/10/Law-on-National-Security.pdf [дата обращения: 18 мая 2025 г.] неофициальный перевод. Для категории А субъекты реализации определяются отдельным постановлением Кабинета министров. Для категорий В и С реализация мер физической безопасности ложится на операторов КВИ. Этот практический подход может быть изменен после вступления в силу Директивы CER.

социальные последствия, а также каскадные эффекты.[53] В Эстонии КВИ отнесены к объектам категории B (объекты, предоставляющие жизненно важные услуги); в результате Министерство внутренних дел определено как орган, отвечающий за координацию усилий по их защите. С другой стороны, объекты категории D (объекты, связанные с военными операциями) подпадают под прерогативу Министерства обороны.[54]

53 Королевство Нидерландов, Министерство юстиции и безопасности, Национальный координатор по борьбе с терроризмом и безопасности (без даты), Критическая инфраструктура (защита) [веб-страница]. Доступно по адресу https://english.nctv.nl/topics/critical-infrastructure-protection [дата обращения: 23 июля 2024 г.]. Этот практический подход может быть изменен после вступления в силу Директивы CER.

54 Закон о национальной обороне (11 февраля 2015 г., Эстония). Доступно по адресу: https://www.riigiteataja.ee/en/eli/502042019010/consolide [дата обращения: 21 июля 2025 г.]. Данная практика может быть изменена после вступления в силу Директивы CER.

Национальная практика: методология оценки критичности инфраструктуры в Ирландии (2020 г.)[55]

В принятом Министерством обороны Ирландии Руководстве по стратегическому управлению чрезвычайными ситуациями, затрагивающими устойчивость критически важной инфраструктуры, «критический порог» определяется как «уровень, выше которого последствия потерь считаются настолько серьезными, что национальная инфраструктура, подпадающая под эти уровни, должна считаться критически важной». В этом руководство также представлена шестиэтапная методология, подробно описывающая процесс определения уровня критичности инфраструктуры:

Шаг 1

Составьте «перечень основных услуг [...], которые в случае нарушения или уничтожения [...] могут оказать существенное воздействие на общество».

Шаг 2

«Определив основные услуги, задокументируйте объекты, «необходимые» для предоставления услуг [...]. Каждый такой объект называется «обозначенной инфраструктурой».

Шаг 3

«Определите другие объекты инфраструктуры, связанные с обозначенной инфраструктурой». Например, если электростанции («обозначенная инфраструктура») требуется природный газ для выработки электроэнергии, этот поставщик энергоносителя определяется как «необходимая инфраструктура». Если электростанция производит электроэнергию для водоснабжения и водоотведения, водоочистная станция определяется как «зависимая инфраструктура».

Шаг 4

«Используя сценарный подход, определите [разумный наихудший сценарий], при котором услуга недоступна из-за разрушительного воздействия».

Шаг 5

Оцените «рейтинг критичности, присвоив каждому фактору воздействия балл от 1 до 5. Факторы воздействия включают в себя:

- Масштаб воздействия: люди, концентрация людей, географический диапазон;
- Серьезность последствий: общественные, экономические, экологические, зависимость, политические, психологические, международные, «основные» услуги, безопасность;
- Временные факторы воздействия: время восстановления, продолжительность воздействия, пик воздействия

Шаг 6

После оценки и присвоения баллов от 1 до 5 каждому фактору воздействия рассчитайте показатель критичности следующим образом:

- Выберите «самый высокий балл воздействия из каждой категории воздействия (масштаб, серьезность и время)».
- Перемножьте «самые высокие баллы воздействия из каждой категории воздействия (т.е. масштаб X серьезность X время). Рассчитанный показатель критичности может находиться в диапазоне от 1 до 125».
- Постройте график «показателя критичности на соответствующем уровне для определения общего уровня критичности инфраструктуры».

Источник: Департамент обороны Ирландии

55 Министерство обороны Ирландии (12 октября 2020 г.), Стратегическое руководство по управлению чрезвычайными ситуациями 3 — Устойчивость критически важной инфраструктуры. Доступно по адресу: https://www.gov.ie/en/publication/7ff6f-strategic-emergency-management-sem-national-structures-and-framework/ [дата обращения: 21 июля 2025 г.]. Этот практический подход может быть изменен после вступления в силу Директивы CER.

В предлагаемом в Германии законе о КВИ (KRITIS-Dachgesetz) правительство подчеркивает, что сбои в отдельных секторах КВИ, особенно в тесно взаимосвязанных секторах с взаимозависимостью, могут привести к сбоям во многих других секторах, что может повлечь за собой каскадные сбоим в предоставлении услуг.[56] Этот пример показывает, что в каждой стране существует небольшая категория особо ценных секторов или объектов КВИ, которые являются едиными точками отказа, учитывая их центральную роль в сложных взаимосвязанных сетях КВИ. Даже если они не выделены в отдельную категорию в правовых или стратегических документах страны, важно, чтобы каждая страна определила такие секторы и объекты и приняла соответствующие меры для их защиты и обеспечения их устойчивости.

2.2 Рекомендации по вопросам политики в области управления рисками

Управление рисками является основополагающим компонентом защиты КВИ, включая их физическую безопасность. В данном разделе представлены рекомендации по различным аспектам управления рисками, определенным в национальных стратегических документах. Более подробную информацию о процессе управления рисками можно найти в главе 5 «Угроза терроризма и оценка рисков».

В процессе определения характера и масштаба угроз в отношении КВИ в рамках процесса управления рисками законодательство различных государств-участников предусматривает определенную роль для владельцев/операторов КВИ. Это подкреплено Решением Комитета министров ОБСЕ № 5/07 о частно-государственном партнерстве в борьбе с терроризмом, которое «призна[ет] полезность совместных контртеррористических усилий государственных органов и частного сектора (гражданского общества и делового сообщества) в форме добровольного сотрудничества [...]. В этой связи во всех мероприятиях необходимо, в частности, учитывать: [...] выявление, определение приоритетности и защиту критически важной инфраструктуры, а также решение вопросов готовности к чрезвычайным ситуациям и ликвидации их последствий».[57] Ниже приведены два соответствующих примера:

- В соответствии с Законом Словении о критически важной инфраструктуре 2017 года[58] владельцы/операторы готовят оценку рисков на основе методологии, принятой Министерством обороны, которое выступает координирующим органом в этой области, а также профессиональных руководств, разработанных отдельными министерствами в соответствующих областях их компетенции.
- В Эстонии ответственность за определение уровня угрозы для конкретных объектов инфраструктуры лежит на их владельцах/операторах. Однако

56 Проект закона Федерального правительства: Проект закона о реализации Директивы (ЕС) 2022/2557 и повышении устойчивости критически важных установок, Вестник 20/13961. Доступно по адресу: https://dserver.bundestag.de/btd/20/139/2013961.pdf [по состоянию на 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

57 ОБСЕ (30 ноября 2007 г.), Решение Совета министров № 5/07: Частно-государственное партнерство в противодействии терроризму (MC.DEC/5/07). Доступно по адресу: https://www.osce.org/files/f/documents/c/a/29572.pdf [дата обращения: 21 июля 2025 г.].

58 Закон о критической инфраструктуре (Словения, 2017 г.) Доступно по адресу: https://pisrs.si/pregledPredpisa?id=ZAKO7106 [дата обращения: 28 ноября] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

владельцы/операторы не могут устанавливать его ниже уровня, установленного компетентными государственными органами.[59]

Некоторые государства-участники призывают включить меры по снижению рисков в планы обеспечения безопасности, принимаемые на уровне владельцев/операторов КВИ:

- Порядок защиты объектов государственной обороны Эстонии 2016 года устанавливает минимальные требования, касающиеся конкретно физической защиты объектов государственной обороны.[60]
- В Кыргызской Республике подробные требования к безопасности для владельцев/операторов стратегических объектов включают в себя меры контроля доступа, в том числе физические меры, а также процедуры своевременного обнаружения уязвимостей и идентификации подозрительных лиц, пытающихся проникнуть в охраняемые помещения.[61]

В законодательстве ряда государств-участников обучение владельцев/операторов КВИ и соответствующего персонала рассматривается в качестве ключевого компонента процесса управления рисками:

- В Черногории задача планирования и проведения обучения входит в обязанности координатора по безопасности, назначаемого на уровне отдельного объекта КВИ.[62]
- В Национальной стратегии Швейцарии по защите КВИ 2023 года подготовка и учения определены в рамках «цикла устойчивости» в качестве ключевых инструментов консолидации предусмотренных мер защиты.[63]

2.3 Управление чрезвычайными и кризисными ситуациями

Применительно к КВИ процедуры управления чрезвычайными и кризисными ситуациями, как правило, относятся к процедурам реагирования и управления дестабилизирующими событиями или крупными инцидентами на объектах КВИ, которые влияют на предоставляемые ими услуги. В целом, в государствах-участниках было выработано три общих правовых подхода к решению кризисных ситуаций, затрагивающих КВИ. В рамках первого подхода отсутствуют отдельные положения об управлении кризисными ситуациями, специально предназначенные для КВИ.

59 Порядок защиты объектов государственной обороны (Эстония, 27 апреля 2016 г.). Доступно по адресу: https://www.riigiteataja.ee/akt/112032019033 [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

60 Порядок защиты объектов государственной обороны (Эстония, 27 апреля 2016 г.). Доступно по адресу: https://www.riigiteataja.ee/akt/112032019033 [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

61 Постановление Правительства КР № 56/2015: Об утверждении Требований к режиму функционирования и эксплуатации стратегических объектов. Доступно по адресу: https://cbd.minjust.gov.kg/97305/edition/617411/ru [дата обращения: 21 июля 2025 г.].

62 Закон о восстановлении и защите критически важной инфраструктуры, Закон о ЗКВИ, 72/19 (30 января 2020 г., Черногория). Доступно по адресу: https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e [дата обращения: 21 июля 2025 г.] неофициальный перевод. Этот практический подход может быть изменен после вступления в силу Директивы CER.

63 Национальная стратегия защиты критической инфраструктуры (16 июня 2023 г., Швейцария). Доступно по адресу: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/3159c04b-ffc8-4f4e-b72f-ccba6b6a800e.pdf [по состоянию на 2 мая 2025 г.] неофициальный перевод.

Таким образом, правовая база, в целом применимая к готовности к чрезвычайным ситуациям, охватывает кризисные сценарии, затрагивающие КВИ лишь косвенно.

Национальная практика: система планирования действий в чрезвычайных ситуациях в Швеции[64]

В Швеции система планирования действий в чрезвычайных ситуациях гражданского характера координируется Агентством по гражданским чрезвычайным ситуациям, которое использует подход, учитывающий все виды угроз, включая также угрозы КВИ. Этот подход предусматривает планирование действий в чрезвычайных ситуациях, обеспечение готовности, реагирование и восстановление. Для решения проблемы взаимозависимости КВИ процессы планирования и распределения ресурсов для обеспечения готовности к чрезвычайным ситуациям в мирное время основаны на принципе совместной ответственности заинтересованных сторон. Это означает, что любой субъект, отвечающий за деятельность в нормальных условиях, должен сохранять эту ответственность во время чрезвычайных ситуаций, а также инициировать любое межсекторальное сотрудничество.

Источник: Международная ассоциация менеджеров по чрезвычайным ситуациям

Например, Закон Венгрии о предотвращении стихийных бедствий ориентирован на операторов объектов[65] опасными веществами. Он обязывает их разрабатывать планы внутренней защиты, расследовать обстоятельства любых серьезных аварий, направлять отчеты об инцидентах в орган промышленной безопасности и выполнять другие задачи.

В рамках второго подхода положения об управлении кризисными ситуациями, затрагивающими КВИ, прямо включены в законодательство о готовности к чрезвычайным ситуациям/стихийным бедствиям. Например, Закон Эстонии о чрезвычайных ситуациях 2017 года[66] определяет соответствующие задачи центральных и местных органов власти по обеспечению непрерывности предоставления критически важных услуг и устанавливает координирующие, консультативные и надзорные функции этих органов в отношении владельцев/операторов КВИ.

В рамках третьего подхода положения об управлении кризисными ситуациями, применимые к КВИ, содержатся в законах, касающихся ЗКВИ, в дополнение к другим положениям, касающимся, *в частности*, идентификации и оценки рисков КВИ. Эти нормы зачастую дополняют текст общих законов об управлении кризисными ситуациями, например, регулируя разделение полномочий между ведомствами,

64 Международная ассоциация менеджеров по чрезвычайным ситуациям (IAEM) (без даты), Гражданское чрезвычайное планирование/Управление кризисами в Швеции. Доступно по адресу: https://www.iaem.org/portals/25/documents/CivilEmergencyPlanningSweden.pdf [дата обращения: 21 июля 2025 г.].

65 Закон CXXVIII 2011 года о борьбе со стихийными бедствиями и поправках к некоторым соответствующим законам (2011, Венгрия). Доступно по адресу: https://njt.hu/jogszabaly/2011-128-00-00 [дата обращения: 29 ноября 2024 г.] неофициальный перевод.

66 Закон о чрезвычайном положении (3 марта 2017 г., Эстония). Доступно по адресу: https://www.riigiteataja.ee/en/eli/511122019004/consolide [дата обращения: 29 ноября 2024 г.].

непосредственно отвечающими за ЗКВИ, и ведомствами, отвечающими в целом за управление чрезвычайными ситуациями. Например:

- Согласно Закону Сербии «О критической инфраструктуре» от 2018 года,[67] управление кризисными ситуациями осуществляет Штаб по чрезвычайным ситуациям, в то время как Министерство внутренних дел, которое выступает в качестве координирующего органа по критической инфраструктуре, играет содействующую роль, предоставляя профессиональную поддержку и необходимые данные и информацию.
- Приложение к Национальной программе по защите критически важной инфраструктуры Польши[68] содержит подробные рекомендации по подготовке планов обеспечения непрерывности бизнеса и восстановления. Практические рекомендации включают в себя хранение планов по защите КВИ в надежном и безопасном месте, координацию с другими владельцами/операторами КВИ по вопросам плановых ремонтов и простоев аналогичных объектов КВИ, а также периодическую проверку планов обеспечения непрерывности бизнеса и восстановления.

В некоторых случаях законодательство, касающееся КВИ, требует, чтобы положения о планировании действий в чрезвычайных ситуациях и реагировании на них включались в планы обеспечения безопасности владельцев/операторов КВИ:

- В соответствии с законодательством Черногории планы обеспечения безопасности владельцев/операторов должны включать в себя, помимо прочего, описание мер, направленных на обеспечение функционирования КВИ в случае перебоев в услугах, а также мер, направленных на смягчение последствий таких перебоев.[69]
- Правительство Латвии утвердило руководящие указания,[70] устанавливающие минимальные требования к планированию непрерывности функционирования КВИ в случае угрозы национальной безопасности. В руководящих принципах рассматриваются такие вопросы, как сроки и приоритеты восстановления критически важных услуг, минимальные человеческие ресурсы, необходимые для обеспечения критически важных функций, поиск альтернативных рабочих помещений и виды поддержки, требуемой со стороны государственных органов.

67 Закон о критически важной инфраструктуре: 87/2018-41, Официальный вестник РС, № 87 от 13 ноября 2018 г. (13 ноября 2018 г., Сербия), доступно по адресу: https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2018/87/8 [по состоянию на 29 ноября 2024 г.] неофициальный перевод.

68 Критическая инфраструктура (26 апреля 2007 г., Польша). Доступно по адресу: https://archiwum.rcb.gov.pl/en/critical-infrastructure [дата обращения: 29 ноября 2024 г.].

69 Закон о восстановлении и защите критически важной инфраструктуры, Закон о ЗКВИ, 72/19 (30 января 2020, Черногория) Доступно по адресу: https://www.gov.me/dokumenta/2585570a-cdff-420f-a7c4-0f67f19a6d8e [дата обращения: 21 июля 2025 г.] неофициальный перевод.

70 Процедуры обследования критически важной инфраструктуры, включая европейскую критическую инфраструктуру, а также планирования и внедрения мер безопасности и обеспечения непрерывности эксплуатации (Cab. Reg. No. 508) (6 июля 2021 г., Латвия) Доступно по адресу: https://www.vvc.gov.lv/en/laws-and-regulations-republic-latvia-english/cab-reg-no-508-procedures-surveying-critical-infrastructure-cluding-european-critical-infrastructure-and-planning-and-implementation-security-measures-and-continuity-operation-amendments-08032022 [дата обращения: 2 декабря 2024 г.]. Данная практика может быть изменена после вступления в силу Директивы CER.

Национальная практика: учения по планированию действий в чрезвычайных ситуациях и управлению ими в Кыргызской Республике (2024 г.)[71]

В 2024 году правительство Кыргызстана утвердило положение, определяющее виды обязательных учений, проводимых на уровне объекта КВИ. Один из видов учений предназначен для оценки уровня готовности к возможным террористическим актам. В ходе этого учения компетентные органы безопасности должны скрытно проникнуть на объект через обычные контрольно-пропускные пункты (например, используя поддельный документ об аккредитации) либо вне официальных контрольно-пропускных пунктов (например, используя уязвимость внешнего периметра). Для каждого учения организаторы разрабатывают сценарий, который не доводится до сведения сотрудников службы безопасности объекта. При необходимости по итогам учений руководителям соответствующих объектов направляются рекомендации по устранению выявленных недостатков.

Источник: Правительство Кыргызской Республики

Национальная практика: паспорт безопасности объектов критически важной инфраструктуры в Украине (2023 г.)[72]

Постановлением Кабинета Министров Украины установлен порядок разработки владельцами/операторами КВИ паспорта безопасности объектов КВИ и процедура его официального утверждения. Каждый паспорт объекта КВИ содержит титульный лист, общую характеристику объекта, планы его защиты и отчеты об оценке безопасности. Планы защиты объекта подлежат обязательному утверждению Министерством здравоохранения, Министерством обороны, Государственной службой специальной связи, Государственной службой по чрезвычайным ситуациям и Национальной полицией. В частности, в отношении террористических и иных угроз требуются дополнительные согласования: «В случае угрозы диверсий, террористических актов, актов кибертерроризма против систем управления, операционных и других систем объектов критической инфраструктуры, чрезвычайных ситуаций или других опасных событий на объектах критической инфраструктуры, инцидентов, связанных с нарушениями систем физической безопасности и кибербезопасности и других проектных угроз на общегосударственном, отраслевом и объектовом уровне и возможных негативных последствий для объектов критической инфраструктуры планы защиты подлежат обязательному согласованию Службой безопасности Украины, Национальной гвардией, другими государственными органами».

Источник: Правительство Украины

71 Постановление Кабинета Министров Кыргызской Республики от 7 марта 2024 года № 97 Об утверждении Положения об учебно-практических и профилактических мероприятиях, направленных на выявление состояния антитеррористической защиты объектов возможных террористических посягательств (7 марта 2024 г., Кыргызская Республика). Доступно по адресу: https://online.zakon.kz/Document/?doc_id=35699774&show_di=1 [дата обращения: 4 декабря 2024 г.].

72 Порядок разработки и согласования паспорта безопасности на объекте критической инфраструктуры (4 августа 2023 г., Украина) Доступно по адресу: https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#n9 [по состоянию на 4 декабря 2024 г.].

Национальная практика: паспорт антитеррористической защищенности объектов, уязвимых в террористическом отношении, в Республике Казахстан (2023 г.)[73]

В соответствии совместным приказом Министерства внутренних дел Республики Казахстан и председателя Комитета национальной безопасности был утвержден типовой паспорт антитеррористической защищенности объектов, уязвимых в террористическом отношении. Приказ был принят в июне 2023 года и поручает Министерству внутренних дел его реализацию. Паспорт содержит информацию о рассматриваемом объекте: его характеристики (общая площадь объекта, количество парковочных мест, количество зданий/сооружений), меры защиты, меры безопасности, поэтажные планы зданий и т. д.

Источник: Правительство Республики Казахстан

Неправительственные субъекты также предоставляют рекомендации по управлению кризисными ситуациями частным заинтересованным сторонам, таким как владельцы/операторы КВИ.

Практика: *Справочник по вопросам обеспечения готовности нефтяной и газовой промышленности* Американского института нефти: (2022 г.)[74]

В *Справочнике* Американского институт нефти содержится информация о том, как обеспечить готовность к кризисным ситуациям на государственном и местном уровнях для поддержки устойчивости и восстановления услуг:

- знать, кто что делает: устанавливать контакты и понимать обязанности в ходе подготовки;
- знать, чего не следует делать: не разглашать конфиденциальную или служебную информацию во время мероприятия;
- знать, что важно: понимать важность объектов и ресурсов для надежной работы системы;
- практика, практика и еще раз практика: тестировать процессы посредством тренировок и учений, чтобы убедиться, что установлены правильные взаимосвязи, собрана правильная информация и задействованы правильные механизмы.

Источник: Американский институт нефти

73 Об утверждении типового паспорта антитеррористической защищенности объектов, уязвимых в террористическом отношении (29 июня 2023, Казахстан). Доступно по адресу: https://adilet.zan.kz/rus/docs/V2300032950 [дата обращения: 4 декабря 2024 г.] неофициальный перевод.

74 Американский институт нефти (Вашингтон, округ Колумбия, 2022 г.), *Справочник по обеспечению готовности нефтяной и газовой промышленности*, стр. 24. Доступно по адресу: https://www.api.org/-/media/files/policy/safety/ong-industry-preparedness-handbook.pdf [дата обращения: 21 июля 2025 г.].

2.4 Международное сотрудничество

Экономики и общества государств-участников ОБСЕ тесно взаимосвязаны. Это означает, что сбои в работе КВИ, например, в транспортных сетях, энергетических сетях или финансовых системах, могут иметь каскадные эффекты, в том числе трансграничные. Это может происходить не только тогда, когда КВИ физически находится на территории двух или более стран, но и когда КВИ, полностью расположенная в одной стране, предоставляет критически важную услугу другой стране. Тем не менее, лишь в немногих случаях внутренняя политика/законодательство о КВИ содержат положения о международном сотрудничестве. При этом в большинстве случаев эти положения лишь в общих чертах подтверждают необходимость усиления мер защиты путем взаимодействия и координации с зарубежными странами. Например, в руководящих указаниях правительства Ирландии по обеспечению устойчивости КВИ подчеркивается важность международного сотрудничества для полного понимания уязвимостей цепочек поставок и реализации скоординированных, неконкурирующих мер глобальной безопасности и устойчивости.[75] Другим примером является Стратегия безопасности Нидерландов, в которой подчеркивается необходимость международных обязательств по выявлению и снижению зависимостей в производственных цепочках, услугах и секторах. Такие обязательства считаются неотъемлемой частью оценки рисков.[76]

Директива ЕС об устойчивости критически важных объектов (Директива CER) является важным шагом на пути к созданию совместной структуры по защите КВИ на уровне ЕС. Директива вводит понятие «критически важного субъекта особого европейского значения» (CEPES), который определяется как субъект, предоставляющий критически важные услуги шести или более государствам-членам ЕС. В связи с этим CEPES будет подчиняться режиму консультативных миссий (организуемых и финансируемых Европейской комиссией), целью которых является оценка мер, принятых этим критически важным субъектом для выполнения своих обязательств. Если субъект не соответствует критериям CEPES, Директива CER по-прежнему налагает обязательство консультироваться между государствами-членами в отношении совместно используемой КВИ, или КВИ, предоставляющей критически важные услуги через границы, или КВИ, связанной с критически важными субъектами в других государствах-членах. Директива CER также устанавливает режим уведомления об инцидентах внутри страны и между государствами-членами. Этот режим предусматривает строгие требования к срокам направления уведомлений.

На двустороннем уровне Канада и США связаны сложной системой соглашений, планов и процедур, устанавливающих различные типы и уровни взаимного сотрудничества в области защиты КВИ.[77] Эти договоренности свидетельствуют о

75 Министерство обороны Ирландии (2021 г.), *Стратегическое управление чрезвычайными ситуациями: Руководство 3 — Устойчивость критически важной инфраструктуры (Версия 2).* Доступно по адресу: https://assets.gov.ie/90683/7d83eda8-4ff1-4a42-9c22-2d614c8a2d28.pdf [дата обращения 21 июля 2025 г.] Этот практический подход может быть изменен после вступления в силу Директивы CER.

76 Правительство Нидерландов (3 апреля 2023 г.), *Стратегия безопасности Королевства Нидерландов.* Доступно по адресу: https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands [дата обращения: 4 декабря 2024 г.].

77 Министерство внутренней безопасности США и Министерство общественной безопасности Канады (2022), *Сборник механизмов помощи в управлении чрезвычайными ситуациями США и Канады*. Доступно по адресу: https://www.dhs.gov/sites/default/files/2022-03/22_0329_us-canada-em-assistance-mechanism-compendium.pdf [дата обращения: 21 июля 2025 г.].

постепенном и прагматичном подходе, принятом двумя странами, к расширению взаимной поддержки растущего числа критически важных секторов и видов деятельности. Ключевые документы включают в себя:

- Соглашение 2004 года о сотрудничестве в области науки и технологий для защиты критически важной инфраструктуры и безопасности границ (создание механизма для проведения совместных научных и технологических исследований и разработок);[78]
- Соглашение 2009 года о сотрудничестве в управлении чрезвычайными ситуациями (создание Консультативной группы);[79]
- Рамочная программа 2009 года о перемещении товаров и людей через границу во время и после чрезвычайных ситуаций (включая, в частности, чрезвычайные ситуации, связанные с нападением или угрозой нападения);[80]
- План действий 2010 года в отношении критически важной инфраструктуры (разработка комплексного трансграничного подхода к критически важной инфраструктуре и устойчивости).[81]

На субрегиональном уровне одним из примеров трансграничного механизма является меморандум о взаимопонимании (МОВ), подписанный в 2006 году странами Бенилюкса.[82] Этот инструмент направлен на улучшение координации в области управления рисками и кризисными ситуациями, включая информирование общественности и организацию совместных учений. МОВ распространяется на «инциденты или аварии, которые произошли или могут произойти на территории одной из Сторон и которые влекут или могут повлечь за собой трансграничные последствия, независимо от того, является ли кризис природным, техническим или антропогенным». Хотя МОВ был подписан странами Бенилюкса до того, как его подписавшие стороны приняли законы, касающиеся КВИ, он, тем не менее, распространяется на инциденты, затрагивающие объекты и сети, которые обычно считаются критически важными, особенно в транспортном и энергетическом секторах.

78 Соглашение между правительством Соединенных Штатов Америки и правительством Канады о сотрудничестве в области науки и технологий для защиты критически важной инфраструктуры и безопасности границ (1 июня 2004 г.). Доступно по адресу: https://www.dhs.gov/xlibrary/assets/agreement_us_canada_sciencetech_cooperation_2004-06-01.pdf [дата обращения: 21 июля 2025 г.].

79 Соглашение между правительством Соединенных Штатов Америки и правительством Канады о сотрудничестве в управлении чрезвычайными ситуациями (12 декабря 2008 г.). Доступно по адресу: https://www.state.gov/wp-content/uploads/2019/02/09-707-Canada-Emergency-Management-Cooperation.pdf [дата обращения: 21 июля 2025 г.].

80 Рамочное соглашение между Канадой и США о перемещении товаров и людей через границу во время и после чрезвычайной ситуации (17 мая 2009 г.). Доступно по адресу: https://www.dhs.gov/xlibrary/assets/border_management_framework_2009-05-27.pdf [дата обращения: 21 июля 2025 г.].

81 План действий Канады и США по критически важной инфраструктуре (2010). Доступно по адресу: https://www.cisa.gov/sites/default/files/publications/ip-canada-us-action-plan-2010-508.pdf [дата обращения: 21 июля 2025 г.].

82 Меморандум о взаимопонимании по сотрудничеству в области управления кризисами с потенциальными трансграничными последствиями между Королевством Бельгия, Королевством Нидерландов и Великим Герцогством Люксембург (1 июня 2006 г.). Доступно по адресу: https://wetten.overheid.nl/BWBV0003156/2012-03-01 [дата обращения: 4 декабря 2024 г.] неофициальный перевод.

Региональная практика: платформа сотрудничества стран Северной Европы (2020 г.)[83]

В 2017 году Финляндия, Норвегия и Швеция продолжили развивать трехстороннее сотрудничество в целях подготовки к возможным сбоям в трансграничных потоках критически важных товаров и услуг. Результатом стал отчет, охватывающий следующие «общественные секторы»: коммуникации и цифровые сети, энергетика, продовольствие, финансовая инфраструктура, фармацевтика и транспорт.

В отчете были определены различные действия, направленные на информирование политиков трех стран. Например:

- В энергетическом секторе было предложено расширить информационную базу, необходимую для улучшения последовательности в проведении политики, и участвовать в совместных мероприятиях по выявлению перекрестных зависимостей с другими секторами.
- В продовольственном секторе было предложено изучить, как Норвегия и Швеция могли бы перенять опыт Финляндии, которая повысила устойчивость своих каналов распределения продовольствия, обеспечив более чем тремстам (300) розничным магазинам доступ к электричеству во время отключений электроэнергии или других сбоев.
- Что касается управления кризисами, в отчете рекомендуется провести предварительное расследование с целью оценки взаимной доступности автоцистерн, грузовых контейнеров и другой транспортной инфраструктуры в различных видах чрезвычайных ситуаций.

Кроме того, международному сотрудничеству в области борьбы с терроризмом и преступностью могут содействовать международные и региональные организации. Например, Международная организация уголовной полиции (ИНТЕРПОЛ) «обеспечивает и поощряет максимально широкую взаимопомощь между всеми органами уголовной полиции в рамках законов, действующих в разных странах, и в духе Всеобщей декларации прав человека».[84] Часть этой взаимопомощи осуществляется в форме уведомлений ИНТЕРПОЛа, которые представляют собой «международные запросы о сотрудничестве или оповещения, позволяющие полиции стран-членов обмениваться важной информацией, связанной с преступностью».[85] Компетентные органы стран-членов ИНТЕРПОЛа могут получить доступ к этим уведомлениям, некоторые из которых могут содержать уникальную информацию, полезную для защиты КВИ. Такие уведомления могут включать в себя информацию, содержащуюся в Оранжевых Уведомлениях, используемых для «предупреждения о

83 Аула, И.; Амундсен, Р.; Буваро, П.; Харрами, О.; Линдгрен, Дж.; Сахлен, В.; Ведебранд, К. (2020), *Критические северные потоки: сотрудничество между Финляндией, Норвегией и Швецией по безопасности поставок и защите критически важной инфраструктуры.* Доступно по адресу: https://rib.msb.se/filer/pdf/29100.pdf [дата обращения: 4 декабря 2024 г.].

84 Устав МОУП-ИНТЕРПОЛ (2023 г.). Доступно по адресу: https://www.interpol.int/en/content/download/590/file/01%20E%20Constitution_2024.pdf [дата обращения: 21 июля 2025 г.].

85 ИНТЕРПОЛ (без даты), Уведомления. Доступно по адресу: https://www.interpol.int/en/How-we-work/Notices [дата обращения: 4 декабря 2024 г.].

событии, лице, объекте или процессе, представляющем серьезную и неминуемую угрозу общественной безопасности», или в Фиолетовых Уведомлениях, используемых для «поиска или распространения информации о методах работы преступников, объектах, устройствах и способах сокрытия, используемых преступниками».[86]

Обширная сеть полицейских баз данных Интерпола играет важнейшую роль в содействии международному сотрудничеству и обмену информацией. Интерпол управляет 19 полицейскими базами данных, содержащими обширный массив информации о преступниках и преступлениях,[87] включая персональные данные о физических лицах, сведения о террористических организациях и информацию об украденных и утерянных проездных документах. Эти базы данных доступны в режиме реального времени для стран-членов ИНТЕРПОЛ,[88] что позволяет им быстро и эффективно обмениваться сведениями и извлекать важную информацию. Эта информация может использоваться в качестве основы для оценки рисков, разработки целевых мер безопасности и повышения общей физической безопасности КВИ, что в конечном итоге снижает риск совершения успешного террористического акта.

86 ИНТЕРПОЛ (без даты), Об уведомлениях. Доступно по адресу: https://www.interpol.int/en/How-we-work/Notices/About-Notices [дата обращения: 4 декабря 2024 г.].

87 ИНТЕРПОЛ (без даты), Базы данных. Доступно по адресу: https://www.interpol.int/How-we-work/Databases [дата обращения: 4 декабря 2024 г.].

88 ИНТЕРПОЛ (без даты), Базы данных. Доступно по адресу: https://www.interpol.int/How-we-work/Databases [дата обращения: 4 декабря 2024 г.].

3 Соображения в области прав человека

«

Террористы представляют угрозу основным функциям критически важной инфраструктуры. Столкнувшись с этой угрозой, государства, владельцы/операторы критически важной инфраструктуры и частные охранные компании должны соблюдать обязательства, предусмотренные как национальным, так и международным правом, включая право в области прав человека.

»

3 Соображения в области прав человека

Террористы представляют угрозу основным функциям КВИ в регионе ОБСЕ. Они также являются «одной из наиболее значимых угроз миру, безопасности и стабильности, а также осуществлению прав человека и социально-экономическому развитию на пространстве ОБСЕ и за его пределами».[89] Противодействуя этой угрозе и разрабатывая необходимые механизмы защиты КВИ, государства, владельцы/операторы КВИ и частные поставщики услуг безопасности должны соблюдать обязательства, предусмотренные как национальным, так и международным законодательством, включая в области прав человека. Это право закреплено в различных международных документах, включая Обязательства ОБСЕ,[90] а также

89 ОБСЕ (2007 г.), Решение Постоянного совета № 1063: Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063), стр. 4–5. Доступно по адресу: https://www.osce.org/files/f/documents/f/3/98542.pdf [дата обращения: 21 июля 2025 г.].

90 См., например, ОБСЕ (2007 г.), Решение Совета министров № 6/07: Частно-государственно партнерство в противодействии терроризму (MC.DEC/5/07). Доступно по адресу: https://www.osce.org/files/f/documents/c/a/29572.pdf [доступ 21 июля 2025 г.] См. также: ОБСЕ (2015 г.), Декларация министров о предупреждении и противодействии насильственному экстремизму и радикализации, ведущим к терроризму (MC.DOC/4/15), преамбула, пункты 5 и 7, пункт 3, 2015 г. Доступно по адресу: https://www.osce.org/files/f/documents/b/e/212041.pdf [дата обращения: 21 июля 2025 г.].

в многочисленных резолюциях Совета ООН по правам человека,[91] Генеральной Ассамблеи ООН[92] и Совета Безопасности ООН.[93]

Постоянный совет ОБСЕ «[подтверждает] обязательство государств-участников принимать меры, необходимые для защиты каждого, кто находится под их юрисдикцией, от террористических актов, и необходимость того, чтобы все действия осуществлялись при соблюдении принципа верховенства права и всех обязательств по международному праву, включая международное право прав человека, беженское право и гуманитарное право».[94] Таким образом, управление обязательствами по правам человека в контексте ЗКВИ является необходимым условием для обеспечения эффективного реагирования государства на терроризм на основе верховенства права. Меры реагирования, несоразмерные террористической угрозе или лишающие людей их прав, могут подтолкнуть уязвимых лиц в объятия вербовщиков террористов.[95] Чтобы предотвратить подобные непреднамеренные последствия, права человека должны учитываться как на уровне политиков, так и исполнителями, такими как владельцы/операторы КВИ и частные поставщики услуг безопасности.

Будучи многообразной отраслью права, права человека включают в себя процессуальные, следственные гарантии, гарантии справедливого судебного разбирательства и права на неприкосновенность частной жизни, а также на защиту и безопасность данных. Каждое государство обязано уважать, защищать и осуществлять права человека, в том числе путем регулирования поведения негосударственных субъектов. Последнее особенно актуально в контексте КВИ, поскольку государственные органы зачастую участвуют наряду с частными поставщиками услуг безопасности в разработке и реализации мер безопасности и защиты или в реагировании на нападения на объекты КВИ. Государство может заключать контракты с частными организациями на определенные услуги (например, с частными охранными компаниями или компаниями по обработке данных). При этом некоторые объекты КВИ могут полностью находиться в частной собственности. Распространенность и значимость частных субъектов в этой области могут, таким образом, усложнить вопросы о том, кому разрешено что делать или кто несет ответственность во время кризисной ситуации, такой как террористическая атака и ее последствия.

91 Генеральная Ассамблея ООН (ГА ООН), Совет по правам человека (2022 г.), Резолюция 51/24: Терроризм и права человека (A/HRC/51/24), преамбула, пункты 2, 5, 6, 7 и 8; пункты 2 и 4. Доступно по адресу: https://docs.un.org/en/A/HRC/RES/51/24 [дата обращения: 21 июля 2025 г.].

92 См., например, ГА ООН (2018 г.), Резолюция 72/189: Защита прав человека и основных свобод в условиях борьбы с терроризмом (A/RES/72/180). Доступно по адресу: https://docs.un.org/ru/A/RES/72/180 [дата обращения: 21 июля 2025 г.]. См. также UNGA (2006 г.), Резолюция 60/288: Глобальная контртеррористическая стратегия Организации Объединенных Наций (A/RES/60/288). Доступно по адресу: https://docs.un.org/ru/A/RES/60/288 [дата обращения: 21 июля 2025 г.].

93 См., в частности, СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341), преамбула, пункт 5 о защите критически важной инфраструктуры от террористических атак. Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

94 ОБСЕ (2007 г.), Решение Постоянного совета № 1063: Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063), стр. 4–5. Доступно по адресу: https://www.osce.org/files/f/documents/f/3/98542.pdf [дата обращения: 21 июля 2025 г.].

95 См. ПРООН (2023 г.), *Путь к экстремизму в Африке: пути вербовки и выхода из состава вооруженных групп*, стр. 17–18. Доступно по адресу: https://www.undp.org/sites/g/files/zskgke326/files/2023-02/UNDP-JourneyToExtremism-summary-2023-english.pdf [дата обращения: 21 июля 2025 г.]. Здесь сообщается, что почти половина опрошенных лиц пережили определенное ключевое событие, которое подтолкнуло их к присоединению к воинствующим экстремистским группировкам, причем 71 процент описали таким триггером перенесенные насилие или несправедливость со стороны правительства.

Эта глава служит отправной точкой для понимания важнейшей роли обязательств в области прав человека в контексте защиты КВИ от террористических атак, а также содержит некоторые замечания об их актуальности при рассмотрении систем физической безопасности, частно-государственно партнерства (ЧГП) и других вопросов. В данной главе рассматриваются три основных вопроса:

1. Что такое права человека и как они применимы к мерам по обеспечению физической безопасности КВИ?
2. Какие насущные вопросы в области прав человека следует учитывать разработчикам политики и владельцам/операторам КВИ при создании структур ЗКВИ?
3. Каким образом требования в области прав человека могут по-разному применяться к государственному и негосударственному персоналу, работающему на объектах КВИ?

Эта глава не является всеобъемлющим или исчерпывающим изложением аспектов прав человека в данной теме. Тем не менее, в ней упоминаются продолжающиеся дискуссии, а дополнительные ссылки можно найти в сносках. Основным объектом анализа в данном разделе являются основные договоры ООН по правам человека,[96] поскольку они образуют общую основу правовых обязательств, разделяемых всеми государствами-участниками ОБСЕ. При необходимости также цитируются судебная практика, нормативные акты и рекомендации других соответствующих механизмов, включая региональные правозащитные механизмы, международные уголовные трибуналы и национальные суды. Наконец, в данной главе акцент делается на праве в области прав человека. В связи с этим другие отрасли права, такие как международное гуманитарное право, выходят за рамки данной главы.[97]

3.1 Права человека и их применение

Права человека налагают на государства юридические обязательства по защите людей и обеспечению определенных стандартов обращения и жизни. Они вытекают из нескольких источников, прежде всего из международных/региональных договоров, которые государства добровольно подписали и ратифицировали, таких как Международный пакт о гражданских и политических правах (МПГПП), Европейская конвенция о правах человека или Межамериканская конвенция о правах человека. Права человека также вытекают из обычного права, которое является обязательным для государств независимо от ратификации ими какого-либо договора.[98] В обоих случаях государства должны обеспечить наличие внутренней правовой и политической базы, которая практически и эффективно гарантирует осуществление прав человека.

96 См.: Организация Объединенных Наций (без даты), Основные международные документы по правам человека и их контрольные органы. Доступно по адресу: https://www.ohchr.org/en/core-international-human-rights-instruments-and-their-monitoring-bodies [дата обращения: 4 декабря 2024 г.].

97 Независимо от применимых сводов законов, ученые в области прав человека и эксперты ООН рекомендуют, чтобы терроризм «в первую очередь рассматривался как серьезная форма преступления и с ним боролись в рамках парадигмы правоохранительных органов», а не в рамках права вооруженного конфликта о ведении боевых действий. Источник: М. Шейнин (2022), «Терроризм», в *Международном праве прав человека*, четвертое издание, под редакцией Моэкли, Д.; Шаха, С.; Сивакумарана, С.; Харриса, Д. (Оксфорд: Издательство Оксфордского университета), стр. 608.

98 См., например, Шабас, В. (2021 г.), *Обычное международное право прав человека* (Оксфорд: Издательство Оксфордского университета).

Комментаторы часто описывают обязательства государств в области прав человека как трехсторонние, состоящие из обязанности защищать, обязанности соблюдать и обязанности осуществлять.[99] Проще говоря, это означает, что каждое право человека влечет за собой обязанность:

- Соблюдать: воздерживаться от действий, которые могут помешать осуществлению прав человека или нарушить их;
- Защищать: принимать все разумные меры для предотвращения нарушений и злоупотреблений правами человека, в том числе со стороны третьих лиц (например, частных предприятий);
- Осуществлять: принимать позитивные меры, такие как «соответствующие законодательные, административные, бюджетные, судебные и иные меры» для обеспечения полного осуществления прав человека.[100]

Права человека действуют на всей территории государства и всякий раз, когда государственные агенты осуществляют определенный уровень контроля.[101] Например, государство может нести ответственность за нарушение права на жизнь или права не подвергаться пыткам, когда его действие является «необходимым звеном в причинно-следственной цепочке», непосредственно ведущей к предсказуемому риску нарушения третьей стороной.[102] Государства также обязаны соблюдать международное право в области прав человека при выполнении резолюций Совета Безопасности ООН.[103]

Ограничения и отступления

Права человека защищают каждого; это касается как иностранных граждан, находящихся на территории государства, так и собственных агентов государства, таких как вооруженные силы, правоохранительные органы или сотрудники служб безопасности.[104] Хотя право в области прав человека применимо всегда, свод законов достаточно гибок, чтобы учитывать различные требования безопасности, с которыми могут столкнуться государства при защите КВИ. Основным способом обеспечения этой гибкости является законное *ограничение* неабсолютного права человека,

99 См., например, Комиссия ООН по правам человека (1987 г.), Доклад о праве на достаточное питание как праве человека, представленный г-ном Асбьерном Эйде, Специальным докладчиком (E/CN.4/Sub.2/1987/23). Доступно по адресу: https://documents.un.org/doc/undoc/gen/g87/120/48/pdf/g8712048.pdf [дата обращения: 21 июля 2025 г.].

100 Международная комиссия юристов (МКЮ) (1997 г.), Маастрихтские руководящие принципы по нарушениям экономических, социальных и культурных прав, пар. 6. Доступно по адресу: https://www.refworld.org/policy/legalguidance/icjurists/1997/en/63964 [дата обращения: 21 июля 2025 г.].

101 Комитет ООН по правам человека (2004), Замечание общего порядка № 31 [80]: Характер общего юридического обязательства, налагаемого на государства - участников Пакта (CCPR/C/21/Rev.1/Add.13), пар. 10. Доступно по адресу: https://www.refworld.org/legal/general/hrc/2004/en/52451 [дата обращения: 9 декабря 2024 года].

102 См., например, Комитет ООН по правам человека (2009 г.), Мохаммад Мунаф против Румынии (CCPR/C/96/D/1539/2006), пар. 14.2. Доступно по адресу: https://www.refworld.org/jurisprudence/caselaw/hrc/2009/en/70157 [по состоянию на 21 июля 2025 г.].

103 Кади против Совета Европейского Союза и Комиссии Европейских Сообществ, C-402/05 P и C-415/05 P, Европейский Союз: Суд Европейского Союза (CJEU), 3 сентября 2008 г. Доступно по адресу: https://www.refworld.org/jurisprudence/caselaw/ecj/2008/en/97735 [дата обращения 21 июля 2025 г.]; Аль-Джедда против Великобритании, заявление № 27021/08, Совет Европы: Европейский суд по правам человека (ЕСПЧ), 7 июля 2011 г. Доступно по адресу: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-105612%22]} [дата обращения 18 мая 2025 г.]; Нада против Швейцарии, решение от 12.9.2012 [GC], ЕСПЧ, август–сентябрь 2012 г. Доступно по адресу: https://hudoc.echr.coe.int/fre?i=002-6434 [дата обращения: 21 июля 2025 г.].

104 ОБСЕ (1994 г.), Кодекс поведения, касающийся военно-политических аспектов, параграф 32, доступно по адресу: https://www.osce.org/files/f/documents/d/f/41359.pdf [дата обращения: 21 июля 2025 г.]; Энгель против Нидерландов, ЕСПЧ, 8 июня 1976 г., п. 54. Доступно по адресу: https://hudoc.echr.coe.int/eng?i=001-57479 [дата обращения: 21 июля 2025 г.].

которое при определенных обстоятельствах сужает сферу применения одного права. В исключительных случаях государства могут более широко ограничивать определенные гражданские и политические права посредством *отступления* от них во время чрезвычайного положения. Ограничения и отступления подробно описаны в следующих двух разделах.

Ограничения

Ограничения представляют собой ограничения прав человека, предусмотренные соответствующим положением международного договора. Например, ограничение права на свободу и личную неприкосновенность, когда сотрудник правоохранительных органов производит законный арест. Ограничения, в отличие от отступлений, не требуют публичного объявления чрезвычайного положения. Однако они не предоставляют *карт-бланш* на ограничение прав человека. Законное ограничение прав человека должно быть:

Предусмотрено законом	Любое ограничение или вмешательство в права человека должно иметь достаточно ясную, доступную и предсказуемую основу во внутреннем праве (принцип законности).
Необходимым/ оправданным	Государство должно установить, что ограничение необходимо и оправдано в демократическом обществе для достижения законной цели, такой как защита национальной безопасности, общественного порядка, здоровья или нравственности населения или прав и свобод других лиц (принцип необходимости).
Соразмерным	Ограничение должно быть соразмерно законной цели. Это означает, что оно должно быть «наименее ограничительной мерой» для достижения законной цели (принцип соразмерности).
Недискриминационным	Любое ограничение, не имеющее разумного обоснования и являющееся несоразмерным, считается дискриминационным. В контексте борьбы с терроризмом особое внимание следует уделять тому, чтобы не принимались и/или не применялись меры, дискриминирующие исключительно по признаку расы, религии, национальности или этнической принадлежности.

Ограничения представляют собой исключительный режим. Следовательно, ограничение не должно применяться таким образом, чтобы осуществление данного права стало исключением, а не правилом. Кроме того, некоторые права не имеют действительных ограничений, перечисленных в устанавливающем их договоре, и, таким образом, могут быть ограничены только посредством законного отступления (см. ниже). Другие права, например, право не подвергаться пыткам или другим видам жестокого обращения, право на недискриминацию и некоторые элементы права на справедливое судебное разбирательство, такие как презумпция невиновности, являются абсолютными правами и не могут быть ограничены ни при каких обстоятельствах.

Отступления

В некоторых редких обстоятельствах лица, осуществляющих защиту КВИ, могут действовать вне строгих требований в области прав человека. Это является результатом отступления, которое представляет собой публичное уведомление о временном неприменении отдельных мер защиты прав человека, вынесенное в соответствии со строгой процедурой.

Обоснованное отступление допускается только в исключительной ситуации, возникшей в результате неминуемого чрезвычайного положения, угрожающего жизни нации.[105] Для отступления установлена высокая планка. Например, участие в вооружённом конфликте само по себе не является достаточным основанием для отступления,[106] поэтому единичное нападение на КВИ не обязательно может стать основанием для отступления. Отступление должно быть необходимым и соразмерным.

Кроме того, отступление является временной мерой. Действие прав может быть «приостановлено только в целях [...] скорейшего возвращения к нормальной жизни».[107] Для того, чтобы субъект действовал в соответствии с обоснованным отступлением, он должен быть явно и публично уполномочен на это. Международные документы по правам человека прямо указывают, что некоторые права, такие как право на жизнь, право не подвергаться пыткам и другим видам жестокого обращения, запрет рабства и принцип недопустимости наказания без закона, являются неотменяемыми и, следовательно, действуют всегда, даже во время чрезвычайного положения.[108]

Ограничения и отступления: террористические атаки

В каких случаях террористическая атака на КВИ дает основания для ограничения или отступления от норм права в области прав человека? Терроризм не имеет единого общепринятого определения в международном праве; в любом случае «террористический» характер атаки не меняет обязательств государства и его агентов в области прав человека.[109] Критерии оценки законности ограничения или отступления остаются неизменными независимо от характера угрозы. Поэтому любое предлагаемое ограничение норм международного права в области прав человека потребует индивидуальной оценки вероятности, неминуемости и серьезности вреда, а также законности, необходимости и соразмерности предлагаемых государством мер реагирования.

Однако атака на КВИ может служить законным основанием для ограничения некоторых прав. Например, если существует непосредственная угроза жизни, службы реагирования могут иметь право применить смертельную силу в целях самообороны. Отступления, напротив, требуют более высокой степени угрозы.

105 Трудно однозначно определить, что является или не является «чрезвычайной ситуацией, угрожающей жизни нации», поскольку это требует комплексной и индивидуальной оценки каждого случая. Однако международные судебные механизмы рассматривают, *среди прочего*, следующие критерии: (1) вероятность, неизбежность и тяжесть вреда; (2) влияет ли чрезвычайная ситуация или ее последствия на все население; (3) являются ли предлагаемые меры строго необходимыми для разрешения чрезвычайной ситуации. См., например, «Греческое дело» (Дания, Норвегия, Швеция и Нидерланды против Греции), ECHR, 1967 г. Доступно по адресу: https://hudoc.echr.coe.int/eng?i=001-167795 [дата обращения: 21 июля 2025 г.].

106 Комитет по правам человека (2001 г.), Замечание общего порядка № 29: Чрезвычайное положение (Статья 4) об отступлениях от прав в связи с чрезвычайным положением (CCPR/C/21/Rev.1/Add.11), пункт 3. Доступно по адресу: https://hrlibrary.umn.edu/russian/gencomm/Rhrcom29.html [дата обращения: 21 июля 2025 г.].

107 Бюро ОБСЕ по демократическим институтам и правам человека (БДИПЧ) (2007 г.), *Борьба с терроризмом и защита прав человека: Руководство*, стр. 87. Доступно по адресу: https://www.osce.org/files/f/documents/f/9/29104.pdf [дата обращения: 21 июля 2025 г.].

108 См. ГА ООН (1966 г.), Международный пакт о гражданских и политических правах, Treaty Series, 999, 171, ст. 4; Европейский суд по правам человека, Совет Европы (1950 г.), Конвенция о защите прав человека и основных свобод (Европейская конвенция о правах человека с поправками), European Treaty Series – № 5, Ст. 15; Комитет ООН по правам человека (2001 г.), Замечание общего порядка № 29, Ст. 4 об отступлениях во время чрезвычайного положения (CCPR/C/21/Rev.1/Add.11).

109 БДИПЧ (2007 г.), *Борьба с терроризмом и защита прав человека: Руководство*. Доступно по адресу: https://www.osce.org/files/f/documents/f/9/29104.pdf [дата обращения: 21 июля 2025 г.].

Например, Франция сделала отступление через МПГПП и Европейский суд по правам человека (ЕСПЧ) после нападения на театр Батаклан в 2015 году.[110] Первоначальное отступление длилось три месяца и было введено для расширения полномочий правоохранительных органов, жандармов и военных в борьбе с предполагаемой непосредственной угрозой дальнейших нападений. Великобритания сделала отступление от права на свободу от произвольного задержания после террористических атак 11 сентября 2001 года в Соединенных Штатах, предвидя аналогичное нападение в Великобритании. Такое отступление было признано британскими судами недействительным.[111] Это произошло потому, что нападение в Соединенных Штатах, в отсутствие конкретных разведданных о надвигающемся нападении на Великобританию, не оправдывало необходимость принятия таких радикальных ответных мер.[112]

3.2 Участие третьих лиц в защите критически важной инфраструктуры

Защита КВИ является сферой государственного управления, тесно связанной с частным сектором.[113] Это признано в Решении Совета министров ОБСЕ № 5 от 2007 года о частно-государственном партнерстве в борьбе с терроризмом:

> Государства-участники ОБСЕ «[признают] полезность совместных усилий органов власти и частного сектора (гражданского общества и делового сообщества) по противодействию терроризму в рамках добровольного сотрудничества, основанного на принципах партнерства и взаимного доверия, с целью укрепления безопасности и получения очевидных выгод для всех сторон. В этой связи во всех мероприятиях необходимо, в частности, учитывать вопросы: [...]

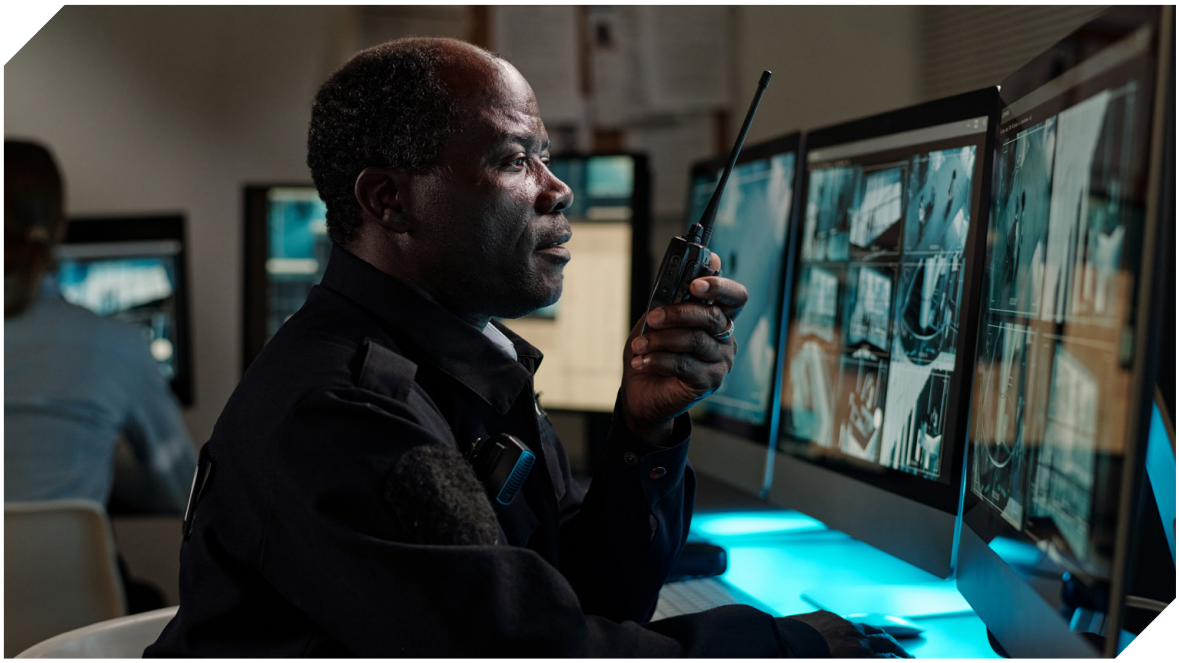
110 См. Совет Европы (1950 г.), Конвенция о защите прав человека и основных свобод (ETS № 005). Доступно по адресу: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005 [дата обращения: 21 июля 2025 г.] ; Указ № 2015-1475 от 14 ноября 2015 г. о применении Закона № 55-385 от 3 апреля 1955 г. о чрезвычайном положении во Франции. Доступно по адресу: https://treaties.un.org/doc/Publication/CN/2015/CN.703.2015-Eng.pdf [дата обращения: 21 июля 2025 г.].

111 См. Совет Европы (1950 г.), Конвенция о защите прав человека и основных свобод (ETS № 005). Доступно по адресу: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005 [дата обращения: 21 июля 2025 г.] ; Указ № 2015-1475 от 14 ноября 2015 г. о применении Закона № 55-385 от 3 апреля 1955 г. о чрезвычайном положении во Франции. Доступно по адресу: https://treaties.un.org/doc/Publication/CN/2015/CN.703.2015-Eng.pdf [дата обращения: 21 июля 2025 г.].

112 См.: A и другие против Государственного секретаря Министерства внутренних дел, Палата лордов Великобритании, 2005 г., UKHL 71, 2004 г. Доступно по адресу: https://publications.parliament.uk/pa/ld200506/ldjudgmt/jd051208/aand-1.htm [дата обращения 21 июля 2025 г.]. См. также: A. и другие против Великобритании, ЕСПЧ, 2009 г. Доступно по адресу: https://hudoc.echr.coe.int/eng?i=002-1647 [дата обращения: 21 июля 2025 г.].

113 См., например, ссылки на государственно-частное партнерство в преамбуле, а также в пункте 5 постановляющей части Резолюции 2341 (S/RES/2341) Совета Безопасности ООН (2017 г.).Доступно по адресу: https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2341(2017)&Language=E&DeviceType=Desktop&LangRequested=False [дата обращения 21 июля 2025 г.] ; ОБСЕ (2007), Решение Совета министров № 5/07: Частно-государственное партнерство в противодействии терроризму (MC.DEC/5/07). Доступно по адресу: https://www.osce.org/files/f/documents/c/a/29572.pdf [дата обращения 21 июля 2025 г.] ; ОБСЕ (2012 г.), Решение Постоянного совета № 1063: Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063), пункты 6, 12, 17. Доступно по адресу: https://www.osce.org/pc/98008 [дата обращения: 21 июля 2025 г.].

составления соответствующих приоритетов и защиты таких объектов, а также готовности к чрезвычайным ситуациям и ликвидации их последствий».[114]



Государства могут заключать контракты с частными поставщиками услуг безопасности для охраны объектов КВИ, привлекать компании для проведения проверок благонадежности потенциальных сотрудников объекта, осуществлять наблюдение за объектом и хранить или обрабатывать данные наблюдения. Некоторые объекты КВИ могут частично или полностью находиться в частной собственности и самостоятельно подбирать персонал. Распространенность и значимость негосударственных субъектов в этой сфере поднимают вопросы о том, какие полномочия государство может им делегировать и кто в конечном итоге несет ответственность в случае нарушения прав человека.

Ответственность государства

В общем международном праве подробно описаны конкретные обстоятельства, при которых государство несет ответственность за нарушение закона. Например, государство всегда несет ответственность за нарушение, совершенное одним из его агентов, даже если они действуют вне сферы своих законных полномочий.[115] Государство также всегда несет ответственность за субъект, осуществляющий элементы государственных полномочий (например, частного поставщика услуг безопасности, которому делегированы правоохранительные полномочия в целях защиты КВИ).[116]

114 ОБСЕ (2007 г.), Решение Совета министров № 5/07: Частно-государственное партнерство в противодействии терроризму (MC.DEC/4/07). Доступно по адресу: https://www.osce.org/files/f/documents/c/a/29572.pdf [дата обращения: 21 июля 2025 г.].

115 Комиссия международного права (ноябрь 2001 г.), Проект статей об ответственности государств за международно-противоправные деяния, Дополнение № 10 (A/56/10), гл. IV.E.1, Статья 4. Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/pdf/responsibility.pdf [дата обращения: 21 июля 2025 г.].

116 Комиссия международного права (ноябрь 2001 г.), Проект статей об ответственности государств за международно-противоправные деяния, Дополнение № 10 (A/56/10), гл. IV.E.1, Статья 4. Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/pdf/responsibility.pdf [дата обращения: 21 июля 2025 г.]. См. также: Комитет ООН по правам человека (2019 г.), Замечание общего порядка № 36, пар. 15. Доступно по адресу: https://docs.un.org/ru/CCPR/C/GC/36 [дата обращения: 21 июля 2025 г.].

Нормы права в области прав человека создают дополнительные параметры ответственности государства. Международное право в области прав человека создает презумпцию ответственности государства за все действия, совершаемые на его территории или под его юрисдикцией. Как правило, государство несет ответственность за нарушения, совершенные третьими лицами, если оно не предприняло разумные меры для «предупреждения и расследования таких нарушений, наказания за них и возмещения ущерба».[117] Это означает, что государство должно принимать разумные меры для пресечения и предотвращения нарушений прав человека, например, путем разработки внутреннего законодательства и политики, которые «устанавливают четкие границы для любого потенциального применения силы»[118] и обеспечивают, чтобы сотрудники, работающие на объектах КВИ, подлежали проверке благонадежности, проходили обучение в области прав человека и имели соответствующее оборудование. Эти основы защиты КВИ также должны регулярно совершенствоваться и оцениваться на предмет их соответствия нормам в области прав человека с использованием фактических данных, прозрачно и с участием всех заинтересованных сторон, чтобы гарантировать, что они не способствуют и не приводят к нарушениям прав человека или к изоляции, предубеждению или предвзятости в более широком смысле.

Во-вторых, государство обязано проводить независимое и беспристрастное расследование предполагаемых нарушений. В случае установления факта нарушения государство обязано обеспечить эффективное средство правовой защиты.[119] Если государство не принимает мер по защите и обеспечению стандартов прав человека, оно несет ответственным за действия третьих лиц.

Делегирование государственных полномочий

В международном праве нет положений, которые бы прямо запрещали государству делегировать свои полномочия частным организациям, в том числе связанные с законным применением силы.[120] Однако делегирование прерогатив не эквивалентно делегированию ответственности. Государство продолжает нести ответственность за нарушения, злоупотребления и/или неправомерное поведение третьих лиц, если оно не приняло меры, описанные выше. Учитывая преобладание частных организаций в управлении и защите КВИ, государство несет значительную обязанность проявлять должную осмотрительность для обеспечения законности деятельности третьих лиц, особенно когда организация напрямую нанимается государством для оказания услуг.

117 См.: ООН (2011 г.), *Руководящие принципы предпринимательской деятельности в аспекте прав человека,* Принцип 1. Доступно по адресу: https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_RU.pdf [дата обращения: 21 июля 2025 г.].

118 См.: Женевский центр по управлению сектором безопасности (DCAF) (2019 г.), *Регулирование применения силы частными поставщиками услуг безопасности: руководство для государств: основные принципы и требования к государственным нормативно-правовым базам по применению силы частными поставщиками услуг безопасности*, стр. 5. Доступно по адресу: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Toolkit_Use%20of%20Force.pdf [дата обращения: 21 июля 2025 г.].

119 См., например, Комиссия ООН по правам человека (2005 г.), Основные принципы и руководящие положения, касающиеся права на правовую защиту и возмещение ущерба для жертв грубых нарушений международных норм в области прав человека и серьезных нарушений международного гуманитарного права (E/CN.4/2005/L.4 8). Доступно по адресу: https://www.un.org/ru/documents/treaty/A-RES-60-147 [дата обращения: 21 июля 2025 г.]; ЕСПЧ (2025 г.), *Руководство по статье 13 Европейской конвенции о правах человека.* Доступно по адресу: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_13_eng [дата обращения: 21 июля 2025 г.].

120 DCAF (2019 г.), *Регулирование применения силы частными поставщиками услуг безопасности: руководство для государств: основные принципы и требования к государственным нормативно-правовым базам по применению силы частными поставщиками услуг безопасности.* Доступно по адресу: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Toolkit_Use%20of%20Force.pdf [дата обращения: 21 июля 2025 г.].

Некоторые полномочия государства требуют соблюдения стандартов прав человека, которые обычно обеспечиваются государством. Примерами могут служить общие полномочия правоохранительных органов, включающие в себя арест и задержание. Они должны защищать от произвольного ареста, например, предоставляя право оспорить задержание в суде, проводить непрерывный правовой надзор и иметь доступ к юридической помощи.[121] Несмотря на отсутствие прямого запрета, на практике государствам запрещено делегировать такие полномочия. Таким образом, службы безопасности КВИ, являющиеся частным поставщиком услуг безопасности, как правило, не могут осуществлять общие полномочия по аресту.

Ответственность частных субъектов

Непосредственная применимость права в области прав человека к негосударственным субъектам является предметом дискуссий.[122] Тем не менее, в большей части региона ОБСЕ наблюдается растущая тенденция к созданию механизмов корпоративной ответственности за нарушения прав человека, злоупотребления и/или неправомерное поведение.[123] IB соответствии с *Руководством по вопросам должной осмотрительности для ответственного ведения бизнеса* Организации экономического сотрудничества и развития (ОЭСР), такие механизмы, как правило, требуют от предприятия:

- интегрировать принципы должной осмотрительности в отношении прав человека в свою политику и системы управления;
- выявлять и оценивать фактическое или потенциальное неблагоприятное воздействие своей деятельности на права человека;
- пресекать, предотвращать и смягчать неблагоприятное воздействие на права человека;
- отслеживать ход осуществления таких мер и их результаты;
- информировать о способах устранения неблагоприятных последствий; и
- при необходимости принимать меры по возмещению ущерба.[124]

121 DCAF (2019 г.), *Регулирование применения силы частными поставщиками услуг безопасности: руководство для государств: основные принципы и требования к государственным нормативно-правовым базам по применению силы частными поставщиками услуг безопасности.* Доступно по адресу: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Toolkit_Use%20of%20Force.pdf [дата обращения: 21 июля 2025 г.]; ООН (1990 г.), Основные принципы роли юристов. Доступно по адресу: https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-role-lawyers [дата обращения: 21 июля 2025 г.]; Комитет ООН по правам человека (16 декабря 2014 г.), Замечание общего порядка № 35, Статья 9 (Свобода и личная неприкосновенность), CCPR/C/GC/35. Доступно по адресу: https://www.refworld.org/legal/general/hrc/2014/en/104763 [дата обращения: 21 июля 2025 г.].

122 В руководящих принципах предпринимательской деятельности в аспекте прав человека ООН подчеркивается «ответственность» предприятий, а не их «обязательства». Доступно по адресу: https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_RU.pdf [дата обращения: 21 июля 2025 г.]. См., однако, A. Clapham (2022 г.), «Негосударственные субъекты», в *Международном праве прав человека*, четвертое издание, под редакцией Моэкли, Д.; Шаха, С.; Сивакумарана, С.; Харриса, Д. (Оксфорд: Издательство Оксфордского университета) стр. 583; и BD Lepard (2019 г.), «Почему международное обычное право имеет значение в защите прав человека», Voelkerrechtsblog. Доступно по адресу: https://voelkerrechtsblog.org/de/why-customary-international-law-matters-in-protecting-human-rights/ [дата обращения: 11 декабря 2024 г.].

123 См., например, законопроект о коммерческих организациях и обязанностях государственных органов (права человека и окружающая среда) парламента Великобритании (2023–2024 гг.) [Палата лордов]. Доступно по адресу: https://bills.parliament.uk/bills/3527/publications [дата обращения 21 июля 2025 г.]; ЕС (2024 г.), Директива о комплексной проверке корпоративной устойчивости и внесение изменений в Директиву (ЕС) 2019/1937 и Регламент (ЕС) 2023/2859 (Директива 2024/1760). Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2024/1760/oj [дата обращения: 21 июля 2025 г.].

124 См. OECD (2018 г.), *Руководство ОЭСР по процедурам надлежащей проверки в практике ответственного ведения бизнеса*. Доступно по адресу: https://mneguidelines.oecd.org/due-diligence-guidance-for-responsible-business-conduct.html; см. также Директиву по процедурам надлежащей проверки в области корпоративной устойчивости (CSDDD) – Директива (ЕС) 2024/1760. Доступно по адресу: https://www.corporate-sustainability-due-diligence-directive.com [дата обращения: 21 июля 2025 г.].

Таким образом, независимо от того, связаны ли частные предприятия напрямую международным правом в области прав человека, они все в большей степени обязаны соблюдать стандарты прав человека косвенно, в соответствии с региональным и национальным законодательством. Несоблюдение этих стандартов может привести к штрафам[125] или уголовному преследованию,[126] а также может иметь более широкие последствия, связанные с общественным восприятием.[127]

Частные субъекты, и особенно частные поставщики услуг безопасности, также все чаще принимают добровольные меры для приведения своей практики в соответствие с международным правом. Примерами служат кодификация практики в области прав человека в отраслевых стандартных кодексах поведения[128] и критериях Международной организации по стандартизации (ИСО).[129] В процессе внедрения добровольных механизмов защиты прав человека частные субъекты взаимодействуют с гражданским обществом, которое осуществляет мониторинг их деятельности и предлагает свои технические возможности и помощь для обеспечения соответствия стандартам передовой практики в области прав человека.[130]

125 См., например, ЕС (2024 г.), Директива о комплексной проверке корпоративной устойчивости и вносящая поправки в Директиву (ЕС) 2019/1937 и Регламент (ЕС) 2023/2859 (Директива 2024/1760), Статья 27. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2024/1760/oj [дата обращения: 21 июля 2025 г.]; см. также Doe против Chiquita Brands International, Окружной суд США по Нью-Джерси, 2024 г. Доступно по адресу: https://earthrights.org/case/doe-v-chiquita-brands-international-en/#:~:text=On%20June%2010%2C%202024%2C%20a,murdered%20were%20awarded%20rightful%20compensation [дата обращения: 21 июля 2025 г.].

126 См., например, текущее дело Lafarge (Французский кассационный суд, № 22-83.681). Доступно по адресу: https://www.courdecassation.fr/en/decision/6411793925b075fb02f1b072 [дата обращения 21 июля 2025 г.]; Коссарт, С.; Шатлен, Л. (2021 г.), «Судебные разбирательства по правам человека против транснациональных компаний во Франции», в книге *«Судебные разбирательства по правам человека против транснациональных компаний на практике»*, под редакцией Р. Мирана и Дж. Мирана (Оксфорд; онлайн-издание Oxford Academic, 18 ноября 2021 г.).

127 См., например, различные исследования, связывающие обнародованные нарушения прав человека с отрицательной динамикой акций: Крайтмейр, Д.; Лейн, Н.; Рашки, П. (2020 г.), *«Ценность имен: гражданское общество, информация и управление транснациональными корпорациями на глобальной периферии»*; С. Штеблер (2020 г.), «Корпоративная социальная ответственность и реакция фондового рынка: критическая роль новостных СМИ», Принципы ответственного инвестирования. Доступно по адресу: https://www.unpri.org/pri-blog/corporate-social-irresponsibility-and-stock-market-reactions-the-critical-role-of-news-media/6008.article [дата обращения: 11 декабря 2024 г.]; Каппел, В.; Шмидт, П.; Циглер, А. (2009 г.), «Нарушение прав человека и эффективность корпоративных акций — анализ событийного исследования», *SSRN Electronic Journal.* Доступно по адресу: https://www.researchgate.net/publication/256000444_Human_Rights_Abuse_and_Corporate_Stock_Performance_-_An_Event_Study_Analysis [дата обращения: 21 июля 2025 г.].

128 См., например, Ассоциация международного кодекса поведения (ICoCA), Международный кодекс поведения для поставщиков частных охранных услуг [веб-страница]. Доступно по адресу: https://icoca.ch/the-code/ [дата обращения 21 июля 2025 г.]; Добровольные принципы безопасности и прав человека [веб-сайт]. Доступно по адресу: https://www.volunteerprinciples.org [дата обращения 11 декабря 2024 г.].

129 См., например, Международная организация по стандартизации, ISO 18788:2015 Система менеджмента для частных охранных предприятий. Требования и руководство по применению. Доступно по адресу: https://www.iso.org/obp/ui/en/#iso:std:iso:18788:ed-1:v1:en [дата обращения: 11 декабря 2024 г.].

130 ICoCA, Наращивание потенциала [веб-страница]. Доступно по адресу: https://icoca.ch/what-we-do/capacity-building/ [дата обращения 11 декабря 2024 г.]; DCAF, Управление безопасностью и защита прав [веб-страница]. Доступно по адресу: https://www.dcaf.ch/index.php/managing-security-and-protecting-rights [дата обращения: 11 декабря 2024 г.].

3.3 Применение силы и право на жизнь, безопасность и гуманное обращение

Ключевым элементом обеспечения физической безопасности КВИ является создание службы безопасности, способной реагировать на угрозы. Эта служба безопасности может быть вооружена и, при необходимости, должна будет применять силу для защиты себя, других людей или объекта КВИ. Поэтому обучение основам прав человека, регулирующих применение силы и право на жизнь, имеет важнейшее значение для всех работников службы безопасности.

Применение силы регулируется в первую очередь правом на жизнь и правом на безопасность. Право на жизнь имеет как негативный правовой элемент (согласно которому государственные агенты обязаны воздерживаться от произвольного лишения жизни), так и ряд позитивных правовых элементов, согласно которым государство обязано обеспечить правовую и политическую основу, способствующую уважению права на жизнь, должным образом обучать и оснащать своих агентов, расследовать и устранять нарушения и привлекать нарушителей к ответственности.[131] Право на жизнь требует, чтобы сила применялась только в самых исключительных обстоятельствах, когда это абсолютно необходимо для защиты жизни; такая сила подпадает под действие строгих правовых гарантий. Право на жизнь не допускает отступлений, то есть не может быть временно приостановлено в периоды кризиса.

Когда служба безопасности реагирует на угрозу безопасности, применение силы с ее стороны всегда должно регулироваться тремя основополагающими принципами: необходимостью, соразмерностью и мерами предосторожности.[132] Содержание этих принципов, за исключением ситуаций вооруженного конфликта, определяется парадигмой правоохранительной деятельности.

131 В юридическом смысле негативное обязательство – это обязательство, требующее от субъекта воздержаться от определенного поведения, в то время как позитивное обязательство – это обязательство, требующее от субъекта совершить определенное действие.

132 Женевская академия международного гуманитарного права и прав человека (2016 г.), *Применение силы в правоохранительной деятельности и право на жизнь: роль Совета по правам человека,* стр. 6. Доступно по адресу: https://www.geneva-academy.ch/joomlatools-files/docman-files/in-brief6_WEB.pdf [дата обращения: 21 июля 2025 г.].

Парадигма правоохранительной деятельности

Парадигма правоохранительной деятельности (ППД) защищает право каждого человека на жизнь. Это право включает в себя и возможность применения силы. На практике это означает, что службы реагирования, как правило, должны следовать строгим правилам, стремясь, насколько это возможно, избегать применения силы. Следовательно, ППД требует наличия четырех ключевых компонентов на тактическом уровне.

Компонент 1: Веское основание применения силы

Сотрудники службы безопасности могут быть вынуждены применять силу по разным причинам, например, в целях самообороны или в качестве государственных агентов, осуществляющих законный арест. Применение менее строгих мер, таких как физическое сдерживание, может быть разрешено, когда это абсолютно необходимо для достижения законной цели поддержания правопорядка. Такие меры могут включать в себя, например, задержание нарушителя до прибытия правоохранительных органов на место происшествия.[133]

133 ООН (1990 г.), Основные принципы применения силы и огнестрельного оружия должностными лицами по поддержанию правопорядка, принцип 4. Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/firearms.shtml [дата обращения 21 июля 2025 г.] ; ООН, Кодекс поведения должностных лиц по поддержанию правопорядка (резолюция ГА ООН 34/169) с комментариями (1979 г.), Ст. 3. Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/code_of_conduct.shtml [дата обращения: 21 июля 2025 г.].

Применение более жестких мер силового воздействия, в том числе с использованием огнестрельного оружия, более строго регулируется законодательством о правах человека. Основные принципы ООН по применению силы и огнестрельного оружия должностными лицами по поддержанию правопорядка («Основные принципы ООН») предусматривают три ситуации, в которых огнестрельное оружие может быть применено для остановки или задержания лица:

- Самооборона или защита других лиц от неминуемой угрозы смерти или серьезных телесных повреждений. Под неминуемостью в данном контексте понимается угроза, которая проявится в течение «секунд, а не часов»;[134]
- Предотвращение совершения особо тяжкого преступления, сопряженного с серьезной угрозой жизни;
- При задержании лица, представляющего такую угрозу и оказывающего сопротивление властям, или для предотвращения его побега.[135]

Обратите внимание, что во всех трех ситуациях требуется явная угроза причинения серьезного увечья или смерти идентифицируемому лицу.[136] Фактически это означает, что огнестрельное оружие ни при каких обстоятельствах не может быть использовано исключительно для защиты имущества.

Кроме того, вышеперечисленные ситуации применяются только к обстоятельствам, в которых намерение состоит в том, чтобы «остановить», а не «убить» цель. Применение преднамеренной летальной силы также ограничено. Например, беглец, даже если он считается склонным к насилию и опасным, но не представляет непосредственной и конкретной угрозы для жизни, не может быть убит. По мнению Европейского суда по правам человека и экспертов ООН, это применимо даже к случаям, «когда неприменение летальной силы может привести к утрате возможности задержания беглеца».[137]

В совокупности эти принципы означают, что службы охраны объекта КВИ будут иметь право применять огнестрельное оружие для отпора ведущему огонь стрелку, нападающему на персонал объекта, но не для предотвращения побега лица, проникшего на объект и уничтожающего имущество или скрывшегося, не представляя непосредственной угрозы для людей. Если подозреваемый мирно отступает, сотрудники службы безопасности могут применять только соответствующие нелетальные средства

134 К. Хейнс, Совет ООН по правам человека, Доклад Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях (A/HRC/26/36), пункт 50. Доступно по адресу: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F26%2F36&Language=E&DeviceType=Desktop&LangRequested=False [дата обращения: 21 июля 2025 г.].

135 См.: MD против Турции, ECHR, 1997 г. Доступно по адресу: https://hudoc.echr.coe.int/eng?i=001-113441 [дата обращения: 21 июля 2025 г.]. В данном случае стрельба по предполагаемому террористу-смертнику считалась законной, поскольку офицеры не «стреляли на поражение», а скорее чтобы обездвижить.

136 См.: ООН (1990 г.), Основные принципы применения силы и огнестрельного оружия должностными лицами по поддержанию правопорядка, принцип 9. Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/firearms.shtml [дата обращения: 11 декабря 2024 г.]. См. также: ООН, Кодекс поведения должностных лиц по поддержанию правопорядка (Резолюция ГА ООН 34/169) с комментариями (1979 г.). Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/code_of_conduct.shtml [дата обращения: 11 декабря 2024 г.].

137 Начова и другие против Болгарии, ЕСПЧ, 2005 г., п. 95. Доступно по адресу: https://hudoc.echr.coe.int/tur?i=001-69630 [дата обращения: 21 июля 2025 г.]. См. также: ООН (2006 г.), Доклад о гражданских и политических правах, включая вопрос об исчезновениях и казнях без надлежащего судебного рассмотрения, E/CN.4/2006/53/Add.4, пункт 47. Доступно по адресу: https://docs.un.org/ru/E/CN.4/2006/53/Add.4 [дата обращения: 21 июля 2025 г.].

для предотвращения его побега. Смертельная сила может применяться только в случае крайней необходимости для защиты жизни другого человека.[138]

Ситуация, изначально создавшая законные основания для применения силы, может со временем измениться. Если основания, приведшие к непосредственной угрозе жизни, исчезнут, применение силы, и особенно летальной, может стать незаконным. Примерами могут служить сдача нападающими в плен или их обезвреживание.

Компонент 2: Индивидуальная оценка угроз

В соответствии с нормами права в области прав человека человеку должна быть предоставлена индивидуальная оценка непосредственной угрозы, которую он представляет.[139] Это означает, что человек не может быть объектом нападения только потому, что он входит в состав вооруженной группы, участвующей в нападении на КВИ. Например, если оперативные данные показывают, что только двое из четырех человек, участвующих в нападении, вооружены, сотрудники службы безопасности не могут стрелять во всех четверых исключительно на основании их принадлежности к одной и той же группе или в силу «баланса вероятностей», что каждый из них представляет угрозу. Человек должен представлять прямую и непосредственную угрозу, чтобы применение силы против него было разрешено. В смешанных толпах людей применение силы должно быть ограничено именно теми, кто представляет такую угрозу.

Компонент 3: Предупреждение перед применением силы, когда это возможно

Применению силы сотрудниками службы безопасности должно предшествовать, когда это возможно, предупреждение и предоставление возможности сдаться. Предупреждение нецелесообразно, если оно подвергнет сотрудника службы безопасности неоправданному риску, создаст риск смерти или серьезного вреда другим людям или будет явно бессмысленным (например, если объект уже ведет огонь).[140]

138 ООН (1990 г.), Основные принципы применения силы и огнестрельного оружия должностными лицами по поддержанию правопорядка, принцип 9. Доступно по адресу: https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement [дата обращения: 11 декабря 2024 г.]; принцип 9, рассматриваемый совместно с принципами 4, 5 и 10. См. также: Совет ООН по правам человека, Доклад Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях Кристофа Хейнса (A/HRC/26/36), пункты 46–47. Доступно по адресу: https://docs.un.org/ru/A/HRC/26/36 [дата обращения: 21 июля 2025 г.].

139 УВКПЧ (1997 г.), *Права человека и правоохранительная деятельность: Руководство по подготовке в области прав человека для должностных лиц правоохранительных органов,* Глава 9. Доступно по адресу: https://www.ohchr.org/sites/default/files/Documents/Publications/training5en.pdf [дата обращения: 21 июля 2025 г.].

140 Управление ООН по наркотикам и преступности (УНП ООН) (2017 г.), *Справочник по применению силы и огнестрельного оружия в правоохранительной деятельности,* стр. 98. Доступно по адресу: https://www.ohchr.org/en/publications/policy-and-methodological-publications/resource-book-use-force-and-firearms-law [дата обращения: 21 июля 2025 г.].

Предупреждение должно быть устным, содержать четкую информацию о личности сотрудника службы безопасности, содержать четкие инструкции и указывать на последствия невыполнения требований.[141] Для того чтобы предупреждение было эффективным, лицу должно быть предоставлено достаточно времени для выполнения требований сотрудника службы безопасности. Предупредительные выстрелы не являются эффективным предупреждением, поскольку они не соответствуют этим критериям и могут быть ошибочно истолкованы как нападение. В любом случае предупредительные выстрелы должны быть запрещены в большинстве случаев из-за риска причинения случайного ущерба и травм.[142] Требование давать предупреждения, когда это возможно, является общепризнанным и применяется даже к целям, которые считаются вооруженными и опасными.

Компонент 4: Порядок эскалации силы

Согласно закону о защите прав человека, сотрудники службы безопасности могут применять силу только в той мере, в какой это строго необходимо и соразмерно устранению угрозы жизни. Применение нелетальной силы должно быть основным способом реагирования. Это не исключает сценариев, в которых летальная сила может быть применена немедленно, например, в случае законной самообороны от неминуемого или продолжающегося нападения. Однако это означает, что нелетальные и менее летальные меры реагирования должны быть предприняты в первую очередь, когда это возможно. Применение огнестрельного оружия является крайней мерой, а преднамеренное применение летальной силы всегда должно быть последним средством. Даже в операциях, сопряженных с высоким риском, порядок эскалации силы может предусматривать первоначальное контролируемое применение дезориентирующих устройств, таких как светошумовые гранаты, средства подавления массовых беспорядков,[143] зловонные вещества или звуковое оружие.[144]

141 ООН (1990 г.), Основные принципы применения силы и огнестрельного оружия должностными лицами по поддержанию правопорядка, принцип 10. Доступно по адресу: https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-use-force-and-firearms-law-enforcement#:~:text=4.,use%20of%20force%20and%20firearms [дата обращения: 11 декабря 2024 г.].

142 УНП ООН (2017 г.), *Справочник по применению силы и огнестрельного оружия в правоохранительной деятельности*, стр. 98. Доступно по адресу: https://www.ohchr.org/en/publications/policy-and-methodological-publications/resource-book-use-force-and-firearms-law [дата обращения: 21 июля 2025 г.]. См. также: Amnesty International (2015 г.), *Применение силы: Руководство по реализации Основных принципов ООН по применению силы и огнестрельного оружия должностными лицами по поддержанию правопорядка.* Доступно по адресу: https://www.amnesty.org.uk/files/use_of_force.pdf [дата обращения: 21 июля 2025 г.].

143 Как указано в Конвенции о запрещении разработки, производства, накопления и применения химического оружия (Конвенция о запрещении химического оружия). Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/chemweapons.shtml [дата обращения: 21 июля 2025 г.].

144 УВКПЧ (2020 г.). *Руководство ООН по соблюдению прав человека при применении менее смертоносного оружия в правоохранительной деятельности.* Доступно по адресу: https://www.ohchr.org/sites/default/files/Documents/Publications/LLW_Guidance_RU.pdf [дата обращения: 21 июля 2025 г.] ; см. также БДИПЧ (2021 г.). *Руководство по оборудованию правоохранительных органов, наиболее часто используемому при охране порядка на собраниях.* Доступно по адресу: https://www.osce.org/odihr/491551 [дата обращения: 21 июля 2025 г.].

Право на жизнь: позитивные правовые элементы

Позитивные элементы права на жизнь делятся на две категории: элементы, требующие от государства принятия мер до применения силы, и элементы, требующие принятия мер после применения силы.

Политика и планирование: Государство должно создать правовую и политическую основу, отражающую его обязательства в соответствии с международным правом в области прав человека. Эти меры предполагают, например, установление нормативных рамок, регулирующих деятельность сотрудников служб безопасности в соответствии с ППД, и установление надлежащих процедур надзора, расследования и правовой защиты.

При оперативном планировании также необходимо учитывать право на жизнь. Это означает, что лица, участвующие в планировании мер реагирования на террористическую атаку, должны всегда учитывать, является ли применение силы строго необходимым, и если да, то какой тип силы следует использовать.

Право на жизнь также распространяется на самих сотрудников служб безопасности. Государство может быть привлечено к ответственности за нарушение права на жизнь или права на личную безопасность, если оно допустило грубую халатность при планировании, обучении или оснащении сотрудников служб безопасности для противодействия конкретной угрозе, и эта халатность привела к смерти или ранению агента государства.[145]

Обучение и оборудование: Подготовка сотрудников служб безопасности должна основываться на соответствующих международных стандартах, особенно на Кодексе поведения должностных лиц по поддержанию правопорядка ООН и Основных принципах ООН по применению силы и огнестрельного оружия должностными лицами по поддержанию правопорядка.[146] Кроме того, сотрудники служб безопасности должны быть обучены методам деэскалации и методам пресечения, которые могут снизить необходимость применения силы.

Сотрудники службы безопасности, включая персонал объекта КВИ, также должны быть соответствующим образом оснащены. Обеспечение сотрудников службы безопасности средствами защиты, такими как шлемы, щиты и бронежилеты, может снизить угрозы, исходящие от нападающих, или даже предотвратить нападение, тем самым ограничивая необходимость применения силы.[147] Некоторые «наступательные» средства, такие как огнестрельное оружие, напротив, могут с большей вероятностью привести к нарушению прав. Поэтому сотрудники службы безопасности должны иметь доступ к «менее летальным» альтернативам

145 См., например, Смит и др. против Великобритании, Верховный суд Великобритании, 2013 г. Доступно по адресу: https://www.supremecourt.uk/cases/uksc-2012-0249 [дата обращения: 21 июля 2025 г.]. Это дело связано с ошибочным ведением огня «по своим» во время военной операции в Ираке. Поскольку суд установил ответственность в более сложной экстерриториальной ситуации, заведомо выдвигается аргумент, что дело будет применяться и к внутренним ситуациям.

146 Комитет ООН по правам человека (2018 г.), Замечание общего порядка № 36, п. 13. Доступно по адресу: https://docs.un.org/ru/CCPR/C/GC/36 [дата обращения: 21 июля 2025 г.].

147 УНП ООН (2018 г.), Поощрение и защита прав человека в контексте мирных протестов (A/HRC/RES/38/11), пункт 15. Доступно по адресу: https://documents.un.org/doc/undoc/gen/g18/213/58/pdf/g1821358.pdf [дата обращения: 21 июля 2025 г.].

огнестрельному оружию, таким как резиновые пули, пейнтбольные шары, электрошокеры, дубинки или парализующие аэрозоли.[148] В любом случае, для смешанной толпы людей, в которой присутствуют допустимые цели и другие лица, сотрудники службы безопасности должны использовать методы и средства, которые с наибольшей вероятностью гарантируют безопасность тех лиц, которые не являются допустимыми целями.

Однако менее смертоносное оружие также может наносить серьезные увечья или даже приводить к смерти как допустимых целей, так и окружающих. Поэтому доступ к такому оружию должен быть ограничен лицами, регулярно проходящими специальную подготовку. С оперативной точки зрения менее смертоносное оружие следует применять только в ситуациях, когда другие, причиняющие меньший вред меры кажутся неэффективными для устранения явной угрозы.[149]

3.4 Права на конфиденциальность, безопасность и защиту данных

Сбор данных с помощью технологий является ключевым компонентом обеспечения физической безопасности КВИ. Распространенные методы сбора данных включают в себя сети наблюдения за объектами, такие как системы видеонаблюдения, сбор биометрических данных для аутентификации, проверку персонала и меры по снижению внутренних угроз (для получения дополнительной информации см. главу 8 «Управление внутренними угрозами»). Эти меры могут повлечь за собой последствия для неприкосновенности частной жизни рядовых граждан или персонала объекта, либо и тех, и других.

148 УВКПЧ (2020 г.). *Руководство ООН по соблюдению прав человека при применении менее смертоносного оружия в правоохранительной деятельности*, стр. III. Доступно по адресу: https://www.ohchr.org/sites/default/files/Documents/Publications/LLW_Guidance_RU.pdf [дата обращения: 21 июля 2025 г.].

149 Комитет ООН по правам человека (2018 г.), Замечание общего порядка № 36, п. 14. Доступно по адресу: https://docs.un.org/ru/CCPR/C/GC/36 [дата обращения: 21 июля 2025 г.].

С 2013 года наблюдается значительный прогресс в нормативном регулировании права на неприкосновенность частной жизни в международном праве.[150] Сегодня право на неприкосновенность частной жизни охватывает не только частную и семейную жизнь, жилище и переписку, но и более широкие, эффективные меры защиты и обеспечения конфиденциальности персональных данных.[151] Все, что подпадает под действие права на неприкосновенность частной жизни, включая персональные данные, подлежит защите от «произвольного или незаконного вмешательства» со стороны «государственных органов или физических или юридических лиц».[152]

ООН и ОБСЕ определили расширенный мониторинг коммуникаций, системы наблюдения общего назначения и целевое цифровое наблюдение как одни из наиболее серьезных угроз праву на неприкосновенность частной жизни на сегодняшний день.[153] Однако вмешательство государства в право на неприкосновенность частной жизни может быть допустимо, если оно преследует четко определенную цель, например, национальную безопасность, и если оно необходимо и соразмерно, то есть если оно осуществляется в соответствии с принципами защиты данных, такими как минимизация данных (ограничение сбора данных теми данными, которые строго необходимы для первоначальной цели) и хранение данных (удаление данных после того, как они больше не нужны).[154] Например, сбор данных о человеке с целью выяснения того, имеет ли он/она право на доступ к секретной информации или доступ к объекту, как правило, является обоснованным ограничением права на неприкосновенность частной жизни, если объем собираемых данных ограничен в соответствии с принципами необходимости и соразмерности.[155]

150 Нист, К.; Фальчетта, Т. (2017 г.), «Право на неприкосновенность частной жизни в цифровую эпоху». *Журнал практики прав человека* 9(1), стр. 104–118. Доступно по адресу: https://www.researchgate.net/publication/317774145_The_Right_to_Privacy_in_the_Digital_Age [дата обращения: 21 июля 2025 г.].

151 См. последовательные резолюции Генеральной Ассамблеи ООН и Совета по правам человека: Генеральная Ассамблея ООН (2018 г.), Право на неприкосновенность частной жизни в цифровой век: Доклад Верховного комиссара Организации Объединенных Наций по правам человека (A/HRC/39/29). Доступно по адресу: https://docs.un.org/ru/A/HRC/39/29 [дата обращения: 21 июля 2025 г.]; Генеральная Ассамблея ООН (14 декабря 1990 г.) (45/95), Руководящие принципы регламентации компьютерных карточек, содержащих данные личного характера. Доступно по адресу: https://docs.un.org/ru/A/RES/73/179 [дата обращения: 21 июля 2025 г.]; Генеральная Ассамблея ООН (2022 г.), Право на неприкосновенность частной жизни (A/77/196). Доступно по адресу: https://docs.un.org/ru/A/77/196 [дата обращения: 21 июля 2025 г.]. По мнению автора, последнее может быть достаточно обширным исследованием для оценки практики государств и убежденности в правомерности в отношении обычного права на неприкосновенность частной жизни.

152 Комитет ООН по правам человека (1988 г.), Замечание общего порядка № 36: Статья 17 (Право на неприкосновенность частной жизни), пар. 1. Доступно по адресу: https://docs.un.org/ru/CCPR/C/GC/36 [дата обращения: 21 июля 2025 г.].

153 См.: ГА ООН (2018 г.), Право на неприкосновенность частной жизни в цифровой век: Доклад Верховного комиссара Организации Объединенных Наций по правам человека (A/HRC/39/29). Доступно по адресу: https://docs.un.org/ru/A/HRC/39/29 [дата обращения: 21 июля 2025 г.]. См. также: БДИПЧ ОБСЕ (2021 г.), *Управление границами и права человека: сбор, обработка и обмен персональными данными и использование новых технологий в контексте борьбы с терроризмом и обеспечения свободы передвижения.* Доступно по адресу: https://www.osce.org/files/f/documents/2/7/514237.pdf [дата обращения: 21 июля 2025 г.].

154 Полные «десять принципов», определенных Специальным докладчиком ООН по вопросу о неприкосновенности частной жизни, см. в Генеральной Ассамблее ООН (2024 г.), Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни Аны Браян Нугререс, A/79/173. Доступно по адресу: https://docs.un.org/ru/A/79/173 [дата обращения: 21 июля 2025 г.].

155 Парламент Великобритании (2024 г.), *Проверка на предмет национальной безопасности: ответы на ваши вопросы.* Доступно по адресу: https://www.parliament.uk/globalassets/mps-lords--offices/offices/pass-office/psd-national-security-vetting-booklet.pdf [дата обращения: 21 июля 2025 г.]. См. также: Михаэль Шварс против Stadt Bochum, CJEU, 2013, C-191/12, параграфы 63–64, где излагается точка зрения ЕС на удаление биометрических данных, законным образом собираемых и обрабатываемых в аэропортах.

Точно так же Европейский суд по правам человека отмечает, что наблюдение охранником за системой видеонаблюдения, охватывающей место общественного пользования, в целом является законным вмешательством в частную жизнь.[156] Венецианская комиссия пришла к выводу, что видеонаблюдение на рабочих местах, тем не менее, требует уважения права сотрудников на неприкосновенность частной жизни. Это означает, что следует избегать использования камер в туалетах, комнатах отдыха персонала или других местах, где человек ожидает отсутствия наблюдения, и что любое скрытое наблюдение за персоналом, например, для снижения внутренней угрозы, должно быть необходимым, соразмерным и применяться на временной основе.[157] Более инвазивные или широкомасштабные методы сбора данных требуют более веских оснований для их использования и более надежной защиты от неправомерного использования.

Использование БАС (дронов) позволяет вести наблюдение в режиме барражирования, которое может быть направлено на отдельного человека или охватывать обширную территорию, где у людей может не возникнуть обоснованного ощущения, что за ними ведется наблюдение. Эксперты ООН по правам человека отмечают, что БАС, как правило, требуют строгого правового регулирования для предотвращения злоупотреблений в большей степени, чем традиционные технологии наблюдения, такие как наземные системы видеонаблюдения.[158]

156 PG и JH против Великобритании, ЕСПЧ, 2001 г., п. 57.

157 Европейская комиссия за демократию через право (Венецианская комиссия) (2007 г.), Мнение о видеонаблюдении, осуществляемом частными операторами в общественной и частной сферах и государственными органами в частной сфере и защите прав человека, параграфы 53–54. Доступно по адресу: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)027-e [дата обращения: 21 июля 2025 г.].

158 См., например, Не Аолайн, Ф. (2022 г.), Замечания Специального докладчика ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом на Международном совещании экспертов по защите уязвимых целей и беспилотным авиационным системам. Доступно по адресу: https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2022-10-18/SR-CT%2520-HR-Drones-Remarks-6-Oct-2021.docx [дата обращения: 21 июля 2025 г.].

Аналогичным образом сбор и обработка биометрических данных,[159] таких как данные, полученные с помощью технологий распознавания лиц, вероятно, потребует гораздо более веских оснований и правовой защиты для получения разрешения. С этой новой технологией также связано быстрое развитие соответствующей области права.[160]

Как государственные субъекты, так и частные организации должны проявлять особую осмотрительность при сборе, обработке и хранении данных, чтобы гарантировать отсутствие произвольного или незаконного вмешательства в право на неприкосновенность частной жизни. Хотя может существовать предположение о том, что государственные агенты, выполняющие законные обязанности по обеспечению безопасности в соответствии с законом, не нарушают право на неприкосновенность частной жизни, неясно, применимы ли те же предположения и оценки необходимости и соразмерности к частным субъектам. Примеры сбора данных негосударственными субъектами с соблюдением права на неприкосновенность частной жизни основаны, главным образом, на получении «добровольного, конкретного и информированного согласия» субъекта данных или соблюдении национального законодательства.[161]

Некоторые государства могут считать, что хранилища данных подпадают под их определение КВИ.[162] Хотя в настоящем *Техническом руководстве* передовые практики в области кибербезопасности подробно не рассматриваются, кибербезопасность и физическая безопасность тесно взаимосвязаны. Например, хотя надежные методы защиты данных, такие как шифрование данных и контроль доступа, могут снизить вероятность несанкционированного доступа к данным, они будут неэффективны, если персонал не имеет достаточной подготовки в области кибербезопасности, или если данные физически хранятся в месте, доступном для злоумышленников.

Вопросы физического доступа к данным особенно важны, когда анализ или хранение данных передаются на подряд частным предприятиям или другим третьим лицам. Государства должны гарантировать, что объекты и программы обучения подрядчика соответствуют минимальным стандартам в отношении защиты данных, физической безопасности и кибербезопасности. Кроме того, частные организации могут передавать, хранить, резервировать или кэшировать данные в сетях, которые могут

159 Для получения дополнительной информации см.: БДИПЧ ОБСЕ (2021 г.), *Управление границами и права человека: сбор, обработка и обмен персональными данными и использование новых технологий в контексте борьбы с терроризмом и свободы передвижения.* Доступно по адресу: https://www.osce.org/files/f/documents/f/a/499777.pdf [дата обращения: 21 июля 2025 г.].

160 Мюррей, Д. (2023 г.), «Использование полицией технологии ретроспективного распознавания лиц: качественное изменение возможностей наблюдения, требующее эволюции правовой базы прав человека», *Modern Law Review* 87(4), стр. 833–863. Доступно по адресу: https://doi.org/10.1111/1468-2230.12862 [дата обращения: 21 июля 2025 г.].

161 См., например, ЕС, Общий регламент по защите данных (GDPR) 2016 г., статья 6(1), *OJ* L 119. Доступно по адресу: https://eur-lex.europa.eu/eli/reg/2016/679 [дата обращения 21 июля 2025 г.] См. также: GDPR, Статья 47: Преобладающий правовой интерес (доступно по адресу: https://gdpr-info.eu/recitals/no-47/ [дата обращения: 21 июля 2025 г.]) и его разъяснение в Meta Platforms Inc. и другие против Bundeskartellamt, Дело C-252/21, CJEU, 2023 г.; и Венецианская комиссия (2007 г.), Мнение о видеонаблюдении, осуществляемом частными операторами в государственной и частной сферах и государственными органами в частной сфере и защите прав человека, пункт 50. Доступно по адресу: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)027-e [дата обращения: 21 июля 2025 г.].

162 См., например, Министерство внутренних дел Австралии, Центр кибербезопасности и защиты инфраструктуры (CISC) (5 декабря 2023 г.), Закон 2018 г. о хранении и обработке данных. Доступно по адресу: https://www.cisc.gov.au/information-for-your-industry/data-storage-and-processing/legislation-regulation-and-compliance/soci-act-2018 [дата обращения: 21 июля 2025 г.].

включать в себя узлы в иностранных юрисдикциях. Государствам следует стремиться к сохранению суверенитета над персональными данными или данными высокого риска. Если это невозможно, государствам следует обеспечить соблюдение другими заинтересованными юрисдикциями строгих правил защиты данных. Это помогает обеспечить соблюдение и прямое применение обязательств в области прав человека, в том числе касающихся несанкционированного доступа, для смягчения последствий, связанных с законами третьих государств о защите данных или обмене данными.

Обмен данными между государствами и частными организациями в отношении групп и лиц, которые считаются представляющими угрозу для КВИ, все чаще рассматривается как часть планов по предотвращению инцидентов и обеспечению готовности к ним для защиты КВИ.[163] Однако «обмен данными является «черным ящиком» международной правовой практики, поскольку существует мало информации о в практике международного права, при этом имеется мало информации о том, происходит ли обмен биометрическими данными и какого типа, а также [...] о содержании соглашений об обмене данными» и о том, учитываются ли вообще соображения прав человека в таких соглашениях.[164] Государства и частные организации должны гарантировать, что данные передаются только в случае необходимости и соразмерно, а также с соблюдением обязательств в области прав человека, включая право на неприкосновенность частной жизни.[165] Учитывая, что такие системы обмена неизбежно действуют без согласия субъекта данных, обмен биометрическими данными, такими как изображение лиц или отпечатки пальцев, потребует более высокого бремени доказывания необходимости, например, наличия непосредственной и идентифицируемой угрозы, а также гарантий от злоупотреблений.[166]

163 См. СБООН, Исполнительный директорат Контртеррористического комитета (2017 г.), *Отчет о тенденциях ИДКТК: Физическая защита критически важной инфраструктуры от террористических атак*, стр. 11–12. Доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted-trends-report-march-2017-final.pdf [дата обращения: 21 июля 2025 г.].

164 ГА ООН (2023 г.), Последствия разработки, использования и передачи новых технологий в контексте борьбы с терроризмом и пресечения и предотвращения насильственного экстремизма (A/HRC/52/39), п. 26. Доступно по адресу: https://documents.un.org/doc/undoc/gen/g23/020/43/pdf/g2302043.pdf [дата обращения: 21 июля 2025 г.].

165 Для получения дополнительных рекомендаций см. Хусзти-Орба́н, К.; Ни Аола́н, Ф (2020 г.), *Использование биометрических данных для идентификации террористов: передовая практика или рискованное дело?* Центр по правам человека, Университет Миннесоты (2020 г.). Доступно по адресу: https://law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf [дата обращения: 21 июля 2025 г.]. См. также: ГА ООН (2023 г.), Последствия разработки, использования и передачи новых технологий для прав человека в контексте борьбы с терроризмом и пресечения и предотвращения насильственного экстремизма (A/HRC/52/39). Доступно по адресу: https://docs.un.org/ru/A/HRC/52/39 [дата обращения: 21 июля 2025 г.].

166 Для получения дополнительных рекомендаций см. БДИПЧ ОБСЕ (2021 г.), *Аналитическая записка: Управление границами и права человека,* стр. 16–20. Доступно по адресу: https://www.osce.org/files/f/documents/2/7/514237.pdf [дата обращения 21 июля 2025 г.] См. также: Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН и КТУ ООН (2018 г.), *Сборник рекомендуемых практик Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом*, в частности, стр. 37–38. Доступно по адресу: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf [дата обращения 21 июля 2025 г.].

4 Частно-государственное партнерство

«

Хотя структуры собственности объектов критически важной инфраструктуры различаются, ключевая реальность заключается в том, что многие частные владельцы/операторы критически важной инфраструктуры несут ответственность за защиту своих объектов/систем. Поэтому взаимодействие между государственным и частным секторами все чаще рассматривается как эффективная и даже необходимая практика.

»

4 Частно-государственное партнерство

В регионе ОБСЕ частный бизнес играет центральную роль во владении, эксплуатации и защите КВИ. Таким образом, он играет ключевую роль в обеспечении готовности к террористическим атакам на объекты КВИ и реагировании на них. Хотя структуры собственности объектов КВИ различаются в государствах-участниках ОБСЕ, ключевая реальность заключается в том, что многие частные владельцы/операторы КВИ несут ответственность за защиту своих объектов/систем КВИ. Это имеет место даже в тех случаях, когда предоставляемые ими услуги (например, электроэнергия, питьевая вода или транспорт) предназначены для общественного потребления. Во многих случаях обязанности по защите передаются на аутсорсинг частному поставщику услуг безопасности. В результате, в случае террористического акта на объекте КВИ жизненно важную роль играют частные заинтересованные стороны, включая частные охранные компании. Поэтому взаимодействие между государственным и частным секторами все чаще рассматривается как эффективная и даже необходимая практика.

Частно-государственное партнерство (ЧГП) – это формальные или неформальные соглашения о сотрудничестве между государственными органами и частными компаниями. Цель ЧГП –разделение нагрузки и содействие сотрудничеству между частными партнерами и государственными органами, при этом частный партнер берет на себя ответственность за предоставление эффективных услуг, а государственный орган гарантирует, что преследуемые цели соответствуют общественным интересам. Государственные органы ожидают, что партнерство с частным сектором снизит давление на государственный бюджет, поскольку частная компания должна сама предоставлять часть средств или все необходимые средства, а это значит, что она будет стремиться обеспечить экономическую эффективность проектов.[167]

В этой главе представлена международная структура для ЧГП в контексте ЗКВИ и рассматривается вопрос о том, как общие базовые ценности могут способствовать эффективности ЧГП. В заключении главы акцент делается на механизмах обмена информацией в рамках ЧГП – ключевой фактор противодействия террористическим угрозам КВИ.

167 ОБСЕ (2013 г.), *Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства.* Доступно по адресу: https://www.osce.org/files/f/documents/5/2/110472.pdf [дата обращения: 21 июля 2025 г.].

4.1 Рамочные механизмы ОБСЕ и ООН для частно-государственного партнерства по защите критически важной инфраструктуры

ОБСЕ в течение уже почти двух десятилетий признает и поощряет частно-государственное партнерство, особенно в усилиях по защите КВИ от террористических атак. В 2007 году в решении № 5 Совета министров государства-участники ОБСЕ признали:

> «полезность совместных усилий органов власти и частного сектора (гражданского общества и делового сообщества) по противодействию терроризму в рамках добровольного сотрудничества, основанного на принципах партнерства и взаимного доверия, с целью укрепления безопасности и получения очевидных выгод для всех сторон».[168]

В этой связи они призвали к усилиям, которые должным образом учитывают вопросы: «определения объектов критической инфраструктуры, составления соответствующих приоритетов и защиты таких объектов, а также готовности к чрезвычайным ситуациям и ликвидации их последствий».[169]

Эта позиция была впоследствии подкреплена Решением Совета министров ОБСЕ № 6 от 2007 года о защите критически важной энергетической инфраструктуры от террористических атак[170] и Консолидированной концептуальной базой ОБСЕ по борьбе с терроризмом от 2012 года.[171]

Генеральная Ассамблея ООН и ее Совет Безопасности подтвердили схожие взгляды относительно частно-государственного партнерства в рамках защиты КВИ от террористических атак. В восьмом обзоре Глобальной контртеррористической стратегии[172] Генеральная Ассамблея ООН:

> «Рекомендует Контртеррористическому управлению и структурам Глобального договора по координации контртеррористической деятельности тесно сотрудничать с государствами-членами и соответствующими международными, региональными и субрегиональными организациями в деле выявления и

168 ОБСЕ (2007 г.), Решение Совета министров № 5/07: Частно-государственное партнерство в противодействии терроризму (MC.DEC/5/07). Доступно по адресу: https://www.osce.org/files/f/documents/c/a/29572.pdf [дата обращения: 21 июля 2025 г.].

169 ОБСЕ (2007 г.), Решение Совета министров № 5/07: Частно-государственное партнерство в противодействии терроризму (MC.DEC/5/07). Доступно по адресу: https://www.osce.org/files/f/documents/c/a/29572.pdf [дата обращения: 21 июля 2025 г.].

170 ОБСЕ (2007 г.), Решение Совета министров № 6/07: Защита важнейших объектов энергетической инфраструктуры от террористических актов (MC.DEC/6/07). Здесь Совет министров «Побуждает государства-участники и далее развивать частно-государственное партнерство с деловыми кругами с целью усиления защиты жизненно важной энергетической инфраструктуры от террористических актов и эффективного решения вопросов готовности и преодоления последствий в этой сфере». Доступно по адресу: https://www.osce.org/files/f/documents/e/2/29485.pdf [дата обращения: 21 июля 2025 г.].

171 ОБСЕ (2007 г.), Решение Постоянного совета № 1063: Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063), II, пункт 6. Доступно по адресу: https://www.osce.org/files/f/documents/f/3/98542.pdf [дата обращения: 21 июля 2025 г.].

172 ГА ООН (2023 г.), Глобальная контртеррористическая стратегия Организации Объединенных Наций: восьмой обзор (A/RES/77/298). Доступно по адресу: https://docs.un.org/ru/A/RES/77/298 [дата обращения: 21 июля 2025 г.].

распространения передовых методов предотвращения террористических нападений на особо уязвимые цели, включая критически важные объекты инфраструктуры и общественные места (слабозащищенные цели), и признает важность развития государственно-частных партнерств в этой области».

В Резолюции 2341 (2017 г.) Совета Безопасности Организации Объединенных Наций Совет Безопасности:

«Признавая, что обеспечение готовности к террористическим нападениям охватывает их предотвращение, защиту от них, смягчение их последствий, реагирование на них и восстановление после них с уделением особого внимания повышению безопасности и устойчивости критически важных объектов инфраструктуры, в том числе, сообразно обстоятельствам, в рамках государственно-частного партнерства»;

«Призывает далее государства установить или укрепить национальные, региональные и международные партнерские отношения с заинтересованными сторонами, как государственными, так и частными, сообразно обстоятельствам, в целях обмена информацией и опытом и тем самым предотвращения террористических нападений на критически важные объекты инфраструктуры, обеспечения защиты от них, смягчения их последствий, их расследования, реагирования на них и восстановления после причиненного ими вреда, в том числе путем проведения совместных учебных мероприятий и применения или создания соответствующих сетей связи или экстренного оповещения».[173]

Кроме того, Добавление 2018 года к Мадридским руководящим принципам содержит ценные рекомендации Совета Безопасности ООН по ЧГП. Мадридские руководящие принципы Совета Безопасности ООН 2015 года в отношении иностранных боевиков-террористов[174] были разработаны как «практический инструмент для использования государствами-членами [ООН] в их усилиях по борьбе с терроризмом и, в частности, по пресечению потока иностранных боевиков-террористов в соответствии с Резолюцией 2178 (2014)». В 2018 году было выпущено Добавление к этим Руководящим принципам, которое включает в себя дополнительные Руководящие принципы. Два из них содержат конкретные рекомендации по ЧГП в контексте борьбы с терроризмом.[175]

173 СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

174 СБ ООН (2015 г.), Письмо Председателя Комитета Совета Безопасности, учрежденного Резолюцией 1373 (2001) о борьбе с терроризмом, от 28 февраля 2019 года на имя Председателя Совета Безопасности, (S/2015/939). Доступно по адресу: https://docs.un.org/ru/S/2019/192 [дата обращения: 21 июля 2025 г.].

175 Контртеррористический комитет Совета *Безопасности ООН (2019 г.), Руководящие принципы Совета Безопасности в отношении иностранных боевиков-террористов: Мадридские руководящие принципы 2015 г. + Добавление 2018 г.* Доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/security-council-guiding-principles-on-foreign-terrorist-fig.pdf [дата обращения: 21 июля 2025 г.].

Руководящий принцип	Официальный текст
Руководящий принцип 50	«В своих усилиях по разработке и осуществлению мер по защите важнейших объектов инфраструктуры и слабозащищенных целей от террористических нападений государства-члены, действуя в сотрудничестве с местными органами власти, должны: [...] ▸ разрабатывать, осуществлять и применять на практике такие стратегии и планы действий по снижению риска террористических нападений на важнейшие объекты инфраструктуры и слабозащищенные цели, которые предусматривают объединение и эффективное использование возможностей соответствующих государственных и частных заинтересованных сторон; ▸ создать или укрепить механизмы для обмена информацией, экспертными знаниями (включая инструментарий и руководящие указания) и опытом между государственными и частными заинтересованными сторонами в целях расследования террористических нападений на такие цели и реагирования на них».
Руководящий принцип 51	«В своих дальнейших усилиях по защите важнейших объектов инфраструктуры и уязвимых целей от террористических актов государствам-членам, действующим в сотрудничестве с местными органами власти, следует также рассмотреть возможность: [...] ▸ создания национальных структур и механизмов в поддержку принятия решений с учетом фактора риска, обмена информацией и государственно-частного партнерства как для правительства, так и для отраслевых ведомств, в том числе в целях налаживания совместной работы по определению приоритетов, и совместной разработки соответствующих материалов и инструментов, таких как общие руководящие принципы наблюдения или конкретные меры, предлагаемые для защиты объектов различных типов (например, стадионов, гостиниц, торговых центров или школ); ▸ внедрения процедур для обмена информацией об оценке рисков между правительством, отраслевыми ведомствами и частным сектором в интересах содействия повышению осведомленности о положении дел и укрепления безопасности слабозащищенных целей и повышения их устойчивости к внешним воздействиям; ▸ поощрения государственно-частных партнерств путем разработки механизмов сотрудничества, оказания поддержки владельцам предприятий и эксплуатирующим компаниям, а также управляющим объектами инфраструктуры и, в случае необходимости, обмена информацией о планах, политике и процедурах».

4.2 Общие ценности как основа частно-государственного партнерства

ЧГП между правительствами и владельцами/операторами КВИ существуют в разных формах и размерах. Эффективные ЧГП, достигающие конкретных, заранее определенных целей, требуют общего набора ценностей, разделяемых всеми сторонами. В 2016 году в рамках «Меридианского процесса» – форума для обмена идеями по защите критически важной информационной инфраструктуры и сотрудничества между высшими государственными деятелями, был определен ряд факторов, способствующих эффективности ЧГП:

- **Доверие:** поскольку ЧГП часто касается проблемных субъектов, важно создать атмосферу доверия, в которой все организации будут осознавать потребность друг друга в осмотрительности. Четкие руководящие принципы членства в оперативных правилах могут способствовать укреплению доверия.
- **Ценность:** участие в ЧГП должно приносить пользу, иначе энтузиазм к участию быстро угаснет;

- **Уважение:** все организации должны признавать и уважать добавленную стоимость, которую другие организации вносят в сотрудничество;
- **Кодекс поведения:** необходимо иметь четкие, конкретные и предсказуемые правила, которые не предоставляют возможности для разобщения и предотвращают любой конфликт интересов;
- **Осведомленность о возможностях и ограничениях друг друга:** это предотвращает конфликт через неправильное суждение о причине отрицательного ответа и позволяет оптимально окупить усилия альянса. Это означает, что обе организации должны быть осведомлены о деятельности друг друга;
- **Реалистичные ожидания:** все организации должны учитывать доступность ресурсов, бюджет развития и другие факторы, чтобы иметь возможность формировать реалистичные ожидания от ЧГП.[176]

В центре внимания: важность доверия

Хотя доверие уже упоминалось как фактор, поддерживающий эффективность ЧГП, его центральное значение для успеха ЧГП нельзя недооценивать. Готовность делиться информацией в рамках любых отношений тесно связана с уровнем доверия между вовлеченными сторонами. Ценная информация практически всегда является крайне чувствительной для держателя этой информации. Для владельцев/операторов частных КВИ и их частных поставщиков услуг безопасности (в соответствующих случаях) это может быть информация об уязвимостях объектов, жизненно важных узлах инфраструктуры, мерах безопасности на объектах, коммерческих секретах или интеллектуальной собственности. Для государственных субъектов это может быть конфиденциальная информация или оперативные данные, связанные с недавними или текущими уголовными расследованиями, террористическими или криминальными угрозами (включая субъектов угроз, их методы, возможности) или источниками оперативных данных. Для обеих сторон обмен такой конфиденциальной информацией может поставить под угрозу источники информации или методы ее сбора, раскрыть сильные или слабые стороны критически важного объекта и/или обеспечить возможность неправомерного использования информации для создания или подрыва конкурентных преимуществ.

В основе усилий по преодолению этих трудностей, таких как заключение официальных юридических соглашений, предоставление допуска к секретной информации представителям частного сектора или другие меры, лежит доверие. Стороны в ЧГП должны быть уверены, что все участники будут использовать предоставленную информацию по назначению и защищать ее от неправомерного использования. Доверие можно построить разными способами, включая регулярное личное взаимодействие.

176 Глобальный форум кибер-экспертизы (2017 г.), *Руководство по передовой практике GFCE-Meridian по защите критической информационной инфраструктуры для лиц, формирующих государственную политику.* Доступно по адресу: https://thegfce.org/wp-content/uploads/gfce-meridian-gpg-to-ciip-1.pdf [дата обращения: 21 июля 2025 г.].

Практика: ОБСЕ – восемь шагов к достижению эффективного государственно-частного партнерства (2013 г.)[177]

Эти шаги были взяты из *руководства ОБСЕ по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства,* опубликованного в 2013 году. Однако они актуальны и для более широкого спектра секторов КВИ, а также для противодействия физическим угрозам, таким как терроризм.

Шаг 1

Проанализировать и установить мотивацию каждого партнера, включение которого планируется в партнерство по защите важнейших объектов инфраструктуры. Это необходимо для выяснения взаимных ожиданий и вклада каждой стороны.

Шаг 2

Установить амбиции и цели партнерства на основе общих национальных целей в сфере защиты важнейших объектов инфраструктуры; прояснить цель партнерства и задач, которые оно должно выполнить.

Шаг 3

Проанализировать существующую нормативно-правовую базу, применимую к каждому важнейшему инфраструктурному сектору; выявить обязательные и самостоятельно установленные нормы, правила и принципы; оценить адекватность существующей нормативно-правовой базы в свете ожидаемых рисков и существующего уровня готовности; обсудить, как можно ликвидировать возможные пробелы.

Шаг 4

Предоставить механизмы, защиту и правовую определенность для обмена информацией, относящейся к защите важнейших объектов инфраструктуры, между всеми задействованными заинтересованными сторонами. Предоставить механизмы для добровольных инициатив, включая развитие образцов передовой практики и обмен ими, а также для консультаций и диалога в целях обеспечения постоянных и эффективных партнерских отношений.

Шаг 5

Создать институциональную структуру, поощряющую межорганизационное сотрудничество и обмен информацией; разъяснить роли и вклад каждого партнера (например, государственных органов, владельцев и операторов важнейших объектов инфраструктуры, поставщиков продукции, ассоциаций); выявить единые контактные точки для каждого партнера; установить рекомендации для сотрудничества.

Шаг 6

Начать с малого, сосредоточившись на одном или двух важнейших инфраструктурных секторах; постепенно развиваться на фоне обеспечения готовности всех заинтересованных сторон к сотрудничеству, рассматривая уровней угрозы.

Шаг 7

Определить важнейшие этапы для анализа достижений и определения потенциальных следующих действий.

Шаг 8

Предусмотреть постоянный процесс проверки для пересмотра и обновления отношений партнерства, чтобы обеспечить продолжающийся прогресс, соотносимый с общей средой риска и с мерами безопасности и защиты, которые требуются для обеспечения оптимального уровня защиты.

Источник: ОБСЕ

177 ОБСЕ (2013 г.), *Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространств.* Доступно по адресу: https://www.osce.org/files/f/documents/5/2/110472.pdf [дата обращения: 21 июля 2025 г.].

4.3 Обмен информацией в рамках частно-государственного партнерства

Правительства, в частности, их разведывательные и правоохранительные органы (как на национальном, так и на местном уровне), играют важную роль в обеспечении надлежащего распространения и понимания информации об угрозах в государственном секторе и в секторах КВИ, включая частные заинтересованные стороны. Если информация об угрозах не передается заинтересованным сторонам за пределами правительства, это может привести к тому, что владелец/оператор КВИ или его поставщик услуг безопасности проведет неточную или неполную оценку уязвимости объекта КВИ. Точно так же владельцы/операторы КВИ и частные поставщики услуг безопасности имеют все возможности для обмена информацией о мерах безопасности на конкретных объектах, областях, представляющих особый интерес для субъектов угроз, подозрительной деятельности и инцидентах, вызывающих беспокойство. Когда эта информация сводится воедино с должным уважением и соответствием местному законодательству, все заинтересованные стороны получают более четкое представление о текущей ситуации с угрозами и могут предпринять соответствующие действия. В результате в регионе ОБСЕ многие владельцы/операторы КВИ и государственные субъекты участвуют в ЧГП, в которых действуют положения об обмене информацией.

Обмен информацией может также осуществляться между субъектами частного сектора, такими как владельцы/операторы КВИ в одном секторе или даже между секторами. В регионе ОБСЕ существует множество секторальных и отраслевых ассоциаций и групп, предоставляющих дополнительные возможности для обучения и обмена экспертными знаниями и опытом, например, Национальный совет центров обмена информацией и анализа США,[178] CoESS[179] и Европейский совет по телекоммуникациям.[180]

Резолюция Совета Безопасности ООН 2341 (2017 г.) обеспечивает прочную основу для содействия обмену информацией между частными и государственными субъектами в целях защиты КВИ от террористических атак. В этой Резолюции Совет Безопасности:

> «4. Призывает государства-члены изыскать возможности для обмена соответствующей информацией и активно сотрудничать в деле предотвращения террористических нападений, планируемых в отношении критически важных объектов инфраструктуры, и обеспечения защиты от них и готовности к ним, а также смягчения последствий уже совершенных нападений, их расследования, реагирования на них и восстановления после них».
>
> «8. Подтверждает, что инициативы в области регионального и двустороннего экономического сотрудничества и развития играют ключевую роль в достижении стабильности и процветания, и в этой связи призывает все государства расширять свое сотрудничество в целях защиты критически важных

178 Национальный совет информационных центров обмена и анализа (ISAC) (без даты), About ISACs [веб-страница]. Доступно по адресу: https://www.nationalisacs.org/about-isacs [дата обращения: 25 марта 2025 г.].

179 CoESS (без даты) [веб-сайт]. Доступно по адресу: https://www.coess.org/ [дата обращения: 25 марта 2025 г.].

180 Европейский совет по телекоммуникациям и коммунальным услугам (EUTC) (без даты) [веб-сайт]. Доступно по адресу: https://eutc.org/ [дата обращения: 25 марта 2025 г.].

объектов инфраструктуры, в том числе региональных проектов развития сообщения и связанных с ними объектов трансграничной инфраструктуры, от террористических нападений путем использования, сообразно обстоятельствам, двусторонних и многосторонних механизмов обмена информацией, оценки рисков и совместной правоприменительной деятельности».[181]

В изданном Организацией Объединенных Наций в 2022 году *Сборнике передовой практики по защите критически важной инфраструктуры от террористических атак* выделены три категории для обмена информацией между государственными органами и владельцами/операторами КВИ:

- **«Оценка угроз:** правоохранительные органы и разведывательные службы должны предоставлять операторам КВИ результаты национальной оценки угроз, затрагивающие конкретные критически важные объекты и процессы, а также критически важные секторы. Эту информацию необходимо включать в оценки рисков, которые должны проводить операторы КВИ, зачастую в соответствии с нормативными требованиями, обязывающими их разрабатывать и предоставлять планы безопасности на уровне КВИ. В свою очередь, отдельным операторам КВИ важно предоставлять результаты своей оценки угроз компетентным государственным органам, чтобы они могли составить точное представление об угрозе как в рамках отдельного сектора КВИ, так и на межсекторальном уровне.
- **Подозрительная деятельность:** операторы КВИ играют важную роль в выявлении необычной деятельности, происходящей внутри или вокруг объектов и процессов, находящихся в их ведении, и информировании о ней соответствующих органов. Эта задача должна быть возложена не только на лиц, ответственных за безопасность, но и на тех, кто взаимодействует с объектами, процессами и системами КВИ, например, на сотрудников, подрядчиков, поставщиков и других заинтересованных лиц. Необходимо внедрить соответствующие программы повышения осведомленности и учебные мероприятия, чтобы эти сотрудники могли распознавать подозрительное поведение и знать, кому следует о нем сообщать.
- **Данные и соображения, связанные с инцидентами:** уроки, извлеченные из прошлых инцидентов (включая успешные методы, вмешательства и неудачи), дают важные знания о способах предотвращения повторения подобных ситуаций. Это, в свою очередь, создает основу для более эффективного управления рисками и действий по восстановлению».[182]

Некоторые из вышеперечисленных положений могут быть также полезны для частных охранных компаний, занимающихся защитой соответствующего объекта КВИ.

Важно отметить, что, учитывая конфиденциальность информации, касающейся защиты КВИ, в рамках любого ЧГП следует обращать внимание на следующие ключевые моменты:

181 СБ ООН (2017), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

182 UNOCT, Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (2022 г.), *Защита критически важных инфраструктур от террористических атак: Сборник передовой практики.* Доступно по адресу: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf [дата обращения: 21 июля 2025 г.].

- Соответствующая информация не должна использоваться иным образом, кроме как в целях защиты КВИ.
- Любой персонал, работающий с секретной или конфиденциальной информацией, должен пройти соответствующую проверку для оформления допуска к секретной информации со стороны соответствующих государственных органов для обеспечения должной осторожности при обращении с информацией.
- Заинтересованные стороны в рамках ЧГП должны осознавать, что определенная передаваемая информация, даже не являющаяся секретной, может быть *чувствительной* и, следовательно, требует осторожного обращения.
- Если соответствующая информация включает персональные данные, то их сбор, обработка, хранение и передача должны осуществляться в соответствии с национальным законодательством и международными стандартами.

Обмен информацией между организациями регулируется стандартом Международной организации по стандартизации № 22396:2020: «Безопасность и устойчивость – Устойчивость сообщества – Руководящие принципы обмена информацией между организациями».[183]

Национальная практика: Программа США по защите информации о критически важной инфраструктуре (2022 г.)[184]

Программа защиты информации о критически важной инфраструктуре была разработана Конгрессом США в 2002 году. Целью Программы является «защита информации, добровольно предоставленной правительству в отношении безопасности критически важной инфраструктуры частных компаний и государственных/местных органов власти». Программа устанавливает единые процедуры получения, проверки, обработки, хранения, маркировки и использования информации о КВИ, добровольно предоставленной в Агентство по кибербезопасности и защите инфраструктуры Министерства внутренней безопасности США. Она также обеспечивает защиту владельцев/операторов КВИ, что привело к расширению добровольного обмена информацией с правительством. Программа также дает владельцам КВИ уверенность в том, что любая предоставленная информация не приведет к раскрытию конфиденциальных или частных данных и не станет достоянием общественности.

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры США

183 ISO (2020 г.), *Безопасность и устойчивость — Устойчивость сообщества — Руководящие принципы обмена информацией между организациями* (Стандарт ISO № 22396:2020). Доступно по адресу: https://www.iso.org/standard/50292.html [дата обращения: 21 июля 2025 г.].

184 Агентство по кибербезопасности и защите инфраструктуры (без даты), Программа защищенной информации критически важной инфраструктуры (ЗИКВИ) [веб-сайт]. Доступно по адресу: https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program [дата обращения: 25 августа 2024 г.].

5 Угроза терроризма и оценка рисков

«Детальная оценка существующих угроз и рисков для конкретного объекта критически важной инфраструктуры имеет решающее значение для его защиты от террористических атак.»

5 Угроза терроризма и оценка рисков

К КВИ относятся секторы и объекты, которые являются неотъемлемой частью повседневной жизни и поддерживают критически важные услуги и функции, необходимые для обеспечения безопасности, экономической стабильности, прав человека и общего благополучия общества. Таким образом, объекты КВИ являются привлекательной целью для террористов из-за масштабных разрушений, страха и экономического ущерба, которые могут вызвать такие атаки. Террористы выбирают цели на основе широкого спектра стратегических, символических и оперативных факторов, которые затем сочетаются с характеристиками, мотивами и целями их террористической организации.[185] Поэтому бывает крайне сложно точно определить, кого, что и где террористы будут атаковать, особенно с учетом того, что многие государства сталкиваются с одновременными угрозами со стороны нескольких террористических организаций с различными идеологическими убеждениями.

В этой главе представлен обзор методов, используемых террористами для атак на объекты КВИ, а также основы процесса оценки риска, который является важнейшим предварительным шагом для определения мер физической безопасности для любого объекта КВИ. Особое внимание уделяется важности применения концепции, учитывающей все угрозы и опасности, к КВИ в соответствии с Резолюцией СБ ООН 2341 (2017 г.).

Существует несколько взаимосвязанных причин, по которым атака на объекты КВИ может быть привлекательной для террористических организаций. Некоторые из них представлены ниже.

Символическое значение

Террористы могут выбирать цели, имеющие символическое значение для своих противников. В некоторых случаях это могут быть объекты КВИ, такие как нефте- и газопроводы, транспортная инфраструктура или государственные учреждения.

Экономический ущерб

Повреждение и/или уничтожение объектов КВИ может привести к значительным финансовым потерям из-за расходов на ремонт, экономических сбоев и потери производительности. Длительные сбои, вызванные атаками такого рода, могут привести к долгосрочной экономической нестабильности, ослабляя экономику страны, ее устойчивость и инвестиционные механизмы.

185 Шмитт, К. (без даты), Цели террористов, Министерство юстиции США, номер NCJ 63429. Доступно по адресу: https://www.ojp.gov/ncjrs/virtual-library/abstracts/targets-terrorists [дата обращения: 21 июля 2025 г.].

Психологическое воздействие

Террористы выбирают своей целью КВИ отчасти для того, чтобы создать у населения всепроникающее чувство уязвимости и страха. Успешная атака на КВИ может создать у населения впечатление, что власти неспособны защитить критически важные службы, что, в свою очередь, может подорвать доверие общества к правительству и его способности поддерживать безопасность и порядок.

Пропагандистская ценность

Террористы могут выбирать цель на основе определенного послания, которое они хотят донести, или для продвижения определенного нарратива. Успешные атаки на КВИ также служат инструментом вербовки для террористических организаций, повышая их привлекательность для потенциальных новых членов, демонстрируя их возможности и преданность делу.

Возмездие

Террористические организации могут выбрать конкретный объект КВИ как часть более широкой стратегии возмездия в ответ на предыдущие инциденты или операции, проведенные против них.

Внимание СМИ

Террористы обычно выбирают целью место, которое может привлечь внимание СМИ, что усиливает их послание и способствует нагнетанию страха. Атаки на КВИ могут привлечь значительное внимание СМИ из-за их масштабных последствий.

Долгосрочные последствия

Атаки на КВИ могут вынудить правительства направлять значительные ресурсы на защиту и восстановление КВИ, что может привести к перенапряжению бюджета и затруднить властям ликвидацию непосредственных последствий атаки. Длительные сбои в работе КВИ, такие как масштабное отключение электроэнергии, могут привести к социальным волнениям, политической нестабильности и усилению поляризации общества, что, в свою очередь, может стать движущей силой радикализации, ведущей к терроризму и насилию.

Стремление к максимальному увеличению числа пострадавших

Террористические организации могут выбирать в качестве целей места массового скопления людей (например, общественный транспорт), чтобы максимизировать эффект от атаки. Такие инциденты также привлекают значительное внимание СМИ. В результате террористы могут планировать атаки, приурочивая их к событиям или периодам вероятного присутствия большего числа людей, например, к часам пик в метро.

5.1 Как террористы атакуют критически важную инфраструктуру?

Настоящее *Техническое руководство* сосредоточено на физической безопасности объектов КВИ с акцентом на террористические атаки. В этом разделе подробно методы, используемые террористами для совершения атак. Хотя он не дает исчерпывающего списка методов, он охватывает многие ключевые категории. В некоторых случаях террористы также комбинируют описанные здесь методы, например, совершают террористические атаки с использованием транспортных средств и взрывчатых веществ.

Взрывчатые вещества

Взрывчатые вещества и самодельные взрывные устройства (СВУ) широко используются террористами в качестве средства нападения благодаря своей разрушительной силе, относительной простоте изготовления и возможности вызывать массовые жертвы. СВУ могут быть изготовлены из легкодоступных материалов, что делает их доступными для широкого круга групп, независимо от их ресурсов. Их можно применять различными способами: устанавливать на человека, начинять транспортные средства, доставлять по воде, СВУ в виде придорожных бомб или скрытые и активируемые СВУ, такие как радиоуправляемые взрывные устройства. Это обеспечивает гибкость в их применении и возможность нацеливать их как на гражданских лиц, так и на объекты КВИ. Непредсказуемость и потенциальная опасность большого количества жертв делают взрывчатые вещества и СВУ высокоэффективным инструментом для устрашения, дестабилизации общества и привлечения внимания к мотивам террористов.

Огнестрельное оружие

Огнестрельное оружие является распространенным средством нападения для террористов благодаря своей доступности, простоте использования и летальной эффективности. Оно позволяет нападающим быстро наносить значительные потери, особенно в людных или замкнутых пространствах. Огнестрельное оружие можно приобрести как законным, так и незаконным путем, и его использование требует минимальной подготовки по сравнению с более сложным оружием. Мобильность и управляемость, обеспечиваемые огнестрельным оружием, позволяют террористам проводить скоординированные атаки, нацеливаться на конкретных людей или группы и поддерживать атаки в течение длительного времени для усиления эффекта. Кроме того, атаки с применением огнестрельного оружия часто привлекают значительное внимание средств массовой информации, что может способствовать усилению позиции террористов.

Транспортные средства

Террористы используют транспортные средства в качестве средства нападения, потому что они легкодоступны, такие атаки требуют минимального планирования и могут привести к значительным жертвам, особенно в густонаселенных городских районах. Транспортные средства можно превратить в смертоносные орудия, направив их на толпу людей, что делает их эффективными для совершения спонтанных или малозатратных атак. Этот метод не требует особых технических навыков или подготовки, что делает его привлекательным для одиночек или небольших групп. Непредсказуемость атак с использованием транспортных средств затрудняет их предотвращение.

Поджог

Террористы могут преднамеренно поджигать объекты критически важной инфраструктуры (заборы, сооружения, складские помещения и т.д.) с целью их повреждения или уничтожения. Поскольку это относительно недорогой метод атаки, его может использовать любое лицо на любом объекте. Поджог также можно сочетать с другими методами атаки, перечисленными здесь, включая огнестрельное оружие и/или похищение людей/захват заложников.

Похищение людей/захват заложников

Похищение людей и захват заложников используются террористами для оказания давления, получения рычагов влияния и привлечения внимания СМИ. Такая тактика позволяет террористам требовать выкуп, добиться освобождения заключенных членов своей группировки или принуждать правительства к политическим уступкам. Ситуации с захватом заложников порождают сильный страх и неопределенность, а также привлекает внимание общественности и СМИ. Длительный характер таких инцидентов может дестабилизировать общество, нагружать силы безопасности и оказывать сильное психологическое воздействие.

Беспилотные авиационные системы

Беспилотные авиационные системы (БАС), также известные как дроны, все чаще используются террористами в качестве средства нападения из-за их растущей доступности, снижения их стоимости и потенциальной способности обходить традиционные меры безопасности.[186] Поскольку БАС можно легко приобрести, потенциальная возможность злоумышленников атаковать КВИ, публичные собрания или военные объекты на расстоянии с минимальным риском для себя делает БАС технологией, вызывающей беспокойство. Кроме того, БАС можно эксплуатировать удаленно, что затрудняет отслеживание или перехват злоумышленников.

186 Информацию об угрозе, которую представляет использование БАС террористами, см., например, в документе Совета Безопасности ООН (2023 г.), Руководящие принципы для государств-членов, касающиеся противодействия применению новых и новейших технологий в террористических целях (S/2023/1035). Доступно по адресу: https://docs.un.org/ru/S/2023/1035 [дата обращения: 21 июля 2025 г.].

Химические, биологические, радиологические, ядерные материалы

Террористы могут использовать химические, биологические, радиологические и ядерные (ХБРЯ) материалы в качестве средства нападения из-за их способности вызывать массовые жертвы, всеобщий страх и долгосрочные перебои. ХБРЯ-оружие может быть невероятно смертоносным, его сложно обнаружить или защититься от него. Использование таких материалов может привести к заражению больших территорий, перегрузить медицинские системы и оказать разрушительное психологическое воздействие на население. Одна лишь угроза атаки с использованием ХБРЯ может вызвать серьезную панику и создать значительную нагрузку на правительства.

Способствующий фактор: привлечение инсайдеров

Террористы используют «инсайдеров» благодаря их авторизованному доступу к объектам КВИ, конфиденциальной информации и протоколам безопасности, что может быть полезным для планирования и проведения более эффективных атак. Инсайдеры могут помочь террористам обойти меры безопасности, предоставить оперативные данные о целях и даже напрямую участвовать в саботаже или атаках, увеличивая свои шансы на успех и сводя к минимуму риск обнаружения. Хотя привлечение инсайдеров не является строгим методом действий при атаках на объекты КВИ, он может рассматриваться как способ содействия атакам и поэтому включен в этот список.

5.2 Оценка угроз и рисков: факторы и различия

Детальная оценка существующих угроз и рисков для того или иного объекта КВИ имеет решающее значение для его защиты от террористических атак. Такие оценки определяют спектр мер безопасности, включая меры физической защиты. Неполные или неточные оценки могут подвергнуть опасности объекты КВИ, персонал или процессы.

Угроза: Система управления безопасностью ООН определяет угрозу как «потенциальное причинение вреда преднамеренными действиями».[187] Угрозы могут быть прямыми (т.е. четкое, выраженное намерение атаковать определенный объект) или обобщенными (т.е. широкое выражение намерения атаковать сектор, религиозную группу или всю страну). Оба типа угрозы следует воспринимать серьезно при выявлении и оценке угроз для конкретного объекта КВИ. При этом следует рассмотреть несколько ключевых оперативных вопросов, в том числе следующие:

КТО	Какой злоумышленник может начать атаку?
ЧТО	Какие объекты может попытаться атаковать злоумышленник? Что он может использовать для осуществления атаки?
ЗАЧЕМ	Какова цель атаки?
ГДЕ	Где может быть осуществлена атака?
КОГДА	В какой момент времени может произойти атака? Примечание: чем конкретнее ответ, тем лучше (например, час, день, месяц, год).
КАК	Как злоумышленники могут осуществить атаку? Каковы потенциальные методы атаки? Какова вероятность совершения атаки? Какова вероятность успеха атаки?

Рассмотрение таких вопросов способствует разработке оценки угроз, которая также включает в себя сведения о возможных методах атаки. Другой способ анализа угроз – визуализировать их в виде расчета:

угроза = намерения[188] *злоумышленников* x *их возможности*[189]

187 Департамент охраны и безопасности ООН (2017 г.), *Система управления безопасностью Организации Объединенных Наций: Руководство по политике безопасности*. Доступно по адресу: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [дата обращения: 21 июля 2025 г.].

188 Определено как «мотивация или склонность субъекта угрозы вызвать событие угрозы, как описано» в: Департамент охраны и безопасности Организации Объединенных Наций (2017 г.), *Руководство по политике безопасности системы управления безопасностью Организации Объединенных Наций*. Доступно по адресу: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [дата обращения: 21 июля 2025 г.].

189 Определяется как «способность или возможность субъектов угрозы вызвать событие угрозы, как описано» в: Департамент охраны и безопасности Организации Объединенных Наций (2017 г.), *Руководство по политике безопасности системы управления безопасностью Организации Объединенных Наций*. Доступно по адресу: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [дата обращения: 21 июля 2025 г.].

Проведение оценки угроз позволяет лицам, ответственным за безопасность объекта КВИ, понять и оценить потенциальных источников угроз и сценарии их возникновения, а также создать надежную основу для эффективной оценки рисков. Крайне важно, чтобы оценка угроз проводилась *до* проведения оценки рисков, поскольку угроза является ключевым компонентом риска (как показано в расчете риска ниже).

Риск: Риск определяется Организацией Объединенных Наций как «вероятность возникновения опасного события и последствия этого события в случае его возникновения».[190] Риск также можно визуализировать в виде расчета, например:

риск = *угроза* x *уязвимость*[191] x *последствия*[192]

Для того чтобы сформировать понимание риска для конкретного объекта КВИ и способов управления им, важны следующие вопросы и факторы:

Компонент	Определение ООН[193]	Основной вопрос	Факторы
Угроза	«Потенциальное причинение вреда преднамеренными действиями»	Что может поставить под угрозу функционирование?	▸ Прошлые события угрозы ▸ Модели угроз (локальные, региональные, глобальные) ▸ Моделирование и прогнозирование угроз
Уязвимость	«Слабая сторона, которая может позволить угрозе или опасности нанести вред»	Насколько подвержен объект угрозе нарушения его функционирования?	▸ Оценка текущих условий ▸ Недавние улучшения в системе безопасности ▸ Уроки, извлеченные из предыдущих сбоев (локальных, региональных, глобальных)
Воздействие (часто называемое последствием)	«Оценка потенциального вреда, который событие может нанести (если оно произойдет) организации»	Если функционирование объекта будет нарушено, каковы будут последствия?	▸ Анализ взаимозависимости ▸ Оценка воздействия ▸ Стратегии обеспечения устойчивости и планы обеспечения непрерывности деятельности

190 Департамент охраны и безопасности ООН (2017 г.), *Система управления безопасностью Организации Объединенных Наций*. Доступно по адресу: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [дата обращения: 21 июля 2025 г.].

191 Определяется как «слабое место, которое может позволить угрозе или опасности нанести вред» в: Департамент охраны и безопасности Организации Объединенных Наций (2017 г.), *Руководство по политике безопасности системы управления безопасностью Организации Объединенных Наций.* Доступно по адресу: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [дата обращения: 21 июля 2025 г.].

192 Часто также именуется «последствием».

193 Департамент охраны и безопасности ООН (2017 г.), *Система управления безопасностью Организации Объединенных Наций.* Доступно по адресу: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [дата обращения: 21 июля 2025 г.].

5.3 Важность «концепции, учитывающей все угрозы и опасности»

Чтобы противостоять вызовам, связанным как с текущими, так и с будущими угрозами, в 2017 году Совет Безопасности ООН призвал страны применять национальный подход к защите КВИ, учитывающий широкий спектр угроз и опасностей, влияющих на владельцев/операторов КВИ и более широкие слои населения. Как указано в Резолюции Совета Безопасности ООН 2341 (2017 г.),[194] посвященной защите КВИ от террористических атак, учет всех угроз и опасностей,[195] которым подвергается КВИ, имеет решающее значение для ее защиты от террористических атак:

> «Признавая в этой связи, что эффективность защиты критически важных объектов инфраструктуры значительно повышается, если защита осуществляется на основе концепции, учитывающей все угрозы и опасности, в частности связанные с террористическими нападениями, и когда при этом регулярно проводятся предметные консультации и обеспечивается сотрудничество с операторами критически важных объектов инфраструктуры и должностными лицами правоохранительных органов и служб безопасности, отвечающих за защиту критически важных объектов инфраструктуры, и, сообразно обстоятельствам, с другими заинтересованными сторонами, в том числе с владельцами частного бизнеса».

На практике это означает включение терроризма в число угроз КВИ в дополнение к другим угрозам и опасностям, таким как стихийные бедствия (экстремальная жара, извержения вулканов, землетрясения, засухи), инциденты в области кибербезопасности, технические сбои, разливы химических веществ, случайные взрывы, отключения электроэнергии, промышленный шпионаж, пожары, преступная деятельность, гражданские беспорядки и т. д.

5.4 Оценка риска

В Резолюции СБ ООН 2341 (2017 г.) Совет Безопасности ООН:

> «призывает государства-члены рассмотреть возможность разработки или дальнейшего совершенствования своих стратегий уменьшения рисков террористических нападений на критически важные объекты инфраструктуры – стратегий, которые должны предусматривать, в частности, **оценку и улучшение понимания соответствующих рисков, принятие мер по обеспечению готовности,** в том числе эффективного реагирования на такие нападения, а также содействие повышению оперативной совместимости в области безопасности

194 СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

195 Опасность определяется как «потенциальное причинение вреда в результате непреднамеренных действий» в документе Департамента охраны и безопасности ООН (2017 г.), *Руководство по политике безопасности системы управления безопасностью Организации Объединенных Наций*. Доступно по адресу: https://b2315f08-09cf-4a7a-b224-5b9df6403e51.usrfiles.com/ugd/b2315f_59d25533484d4430aede6ad4558aea66.pdf [дата обращения: 21 июля 2025 г.].

и ликвидации последствий и поддержку эффективного взаимодействия всех заинтересованных сторон».[196]

Учитывая деликатный характер процесса оценки рисков, в данном разделе будет приведено лишь несколько примеров передовой национальной практики. Вместо этого в нем содержатся рекомендации по оценке общих рисков, которые могут быть использованы для поддержки существующих процессов для государств-участников и владельцев/операторов КВИ. Для получения более подробных и целевых рекомендаций по управлению рисками владельцы/операторы КВИ могут обратиться к руководству по управлению рисками Международной организации по стандартизации (ISO 31000:2018).[197] Важно отметить, что оценка рисков является лишь частью процесса управления рисками. После оценки рисков в рамках четко определенного процесса следующим шагом является обработка рисков,[198] в ходе которой разрабатываются и реализуются организационные меры реагирования на выявленные риски.

Оценка рисков, связанных с террористическими атаками, не является точной наукой. Каждый, кто участвует в такой оценке, может интерпретировать ее по-своему. Важно обеспечить, чтобы команда, проводящая оценку риска, получила качественные данные (включая информацию об субъектах угрозы, их намерениях и возможностях, а также о предыдущих инцидентах), а также структурированную модель или шаблон.

Некоторые правительства и субъекты привлекают широкий круг заинтересованных сторон к процессу оценки рисков. Например, в Великобритании в рамках ежегодной Оценки рисков национальной безопасности (NSRA) оцениваются риски (такие как терроризм, аварии и системные сбои, природные и экологические опасности и т.д.) по семи основным направлениям: воздействие на благосостояние людей, воздействие на поведение, воздействие на основные услуги, экономический ущерб, воздействие на окружающую среду, воздействие на безопасность, международное воздействие. Эта оценка используется в качестве основы для разработки планов обеспечения устойчивости секторов, которые составляются каждым из правительственных ведомств, отвечающих за 13 критически важных секторов Великобритании.[199]

Кроме того, учитывая высокую степень использования частных охранных компаний для защиты КВИ, наиболее качественные оценки рисков, как правило, получаются в рамках частно-государственного партнерства, например, между правоохранительными органами и организациями, ответственными за безопасность объекта КВИ. Подробнее о создании эффективного партнерства см. в главе 4 «Частно-государственное партнерство».

196 СБ ООН (2017), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

197 ISO (2018 г.), *Управление рисками – Руководящие принципы* (Стандарт ISO № 31000:2018). Доступно по адресу: https://www.iso.org/standard/65694.html [дата обращения: 21 июля 2025 г.].

198 ISO (2018 г.), *Управление рисками – Руководящие принципы* (Стандарт ISO № 31000:2018). Доступно по адресу: https://www.iso.org/standard/65694.html [дата обращения: 21 июля 2025 г.].

199 Правительство Ее Величества (2023 г.), *Национальный реестр рисков 2023 г.* Доступно по адресу: https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf [дата обращения: 21 июля 2025 г.].

5.5 Управление рисками

Хотя в регионе ОБСЕ существует несколько различных моделей управления рисками, в соответствии со стандартом ISO 31000:2018 оно обычно состоит из следующих этапов, которые лучше всего рассматривать как итеративный и циклический процесс: выстраивание процесса, оценка риска, обработка риска, мониторинг и обзор.[200]

Цикл управления рисками лучше всего проводить регулярно, чтобы отслеживать меняющиеся угрозы, улучшения в системе безопасности и другие события, которые могут изменить профиль риска данного объекта. В большинстве случаев ответственность за процесс управления рисками возлагается на высшее руководство КВИ, поэтому его участие на всех этапах процесса является крайне важным.

Процесс управления рисками владельца/оператора КВИ должен быть документирован и контролироваться специалистами по безопасности, имеющими опыт управления рисками и знакомыми с объектом КВИ, при поддержке компетентных органов и других уполномоченных партнеров. Стандарт ISO 3100:2018 также поощряет предоставление

200 ISO (2018 г.), *Управление рисками – Руководящие принципы* (Стандарт ISO № 31000:2018). Доступно по адресу: https://www.iso.org/standard/65694.html [дата обращения: 21 июля 2025 г.].

отчетности о процессе управления рисками и его результатах всем сотрудникам организации по мере необходимости, а также другим заинтересованным сторонам в системе управления организацией.

Национальная практика: шаблон оценки рисков для предприятий, разработанный Управлением по охране труда и технике безопасности Великобритании[201]

Организация:						
Оценку провел:						
Дата следующего обзора:						
Дата проведения оценки:						
Какие опасности существуют?	Кто и каким образом может пострадать?	Что вы уже делаете для контроля рисков?	Какие дальнейшие действия вам необходимо предпринять для контроля рисков?	Кто должен предпринять действие?	Когда необходимо предпринять действия?	Сделано?

Источник: Управление по охране труда и технике безопасности Великобритании

Адаптация процесса управления рисками: Каждому владельцу/оператору КВИ необходимо адаптировать процесс управления рисками к своей уникальной ситуации и своим потребностям. На этом этапе принимаются решения о соответствующих критериях риска, объеме мероприятий по управлению рисками, целях процесса управления рисками и других ключевых параметрах.

Оценка рисков: Этап оценки рисков включает в себя выявление и оценку потенциальных рисков, которые могут повлиять на объект КВИ и его функционирование. Он включает в себя сбор информации обо всех возможных внутренних и внешних угрозах, таких как описанные выше. Методы, используемые на этом этапе, могут включать в себя исследования в открытых источниках, сессии фокус-групп, интервью с ключевыми заинтересованными сторонами, анализ исторических данных, отраслевые отчеты и консультации с местными и национальными службами безопасности. Одна из целей этого этапа – составить

201 Этот образец шаблона оценки рисков был взят из документа Health and Safety Executive правительства Великобритании, разработанного для предприятий в Великобритании. Health and Safety Executive (2019), Risk assessment template [веб-страница]. Доступно по адресу: https://www.hse.gov.uk/simple-health-safety/risk/risk-assessment-template-and-examples.html [дата обращения: 16 декабря 2024 г.].

полный список угроз и сценариев угроз, которые могут повлиять на объект КВИ. После выявления угроз анализируется вероятность реализации каждого сценария угрозы и серьезность его воздействия (или последствий). Затем риски оцениваются по существующим критериям риска с учетом принятия решений и готовности к риску владельца/оператора КВИ (т.е. уровня риска, который владелец/оператор КВИ готов принять). Такие инструменты, как матрицы рисков, могут помочь приоритизировать риски, чтобы выявить риски, требующие немедленного внимания, а также риски, которые можно отслеживать в динамике.

Обработка рисков: Затем разрабатываются и внедряются стратегии для снижения или обработки выявленных рисков. Меры по снижению рисков могут быть *превентивными*, такими как внедрение мер безопасности или принятие новых стратегий, или *корректирующими*, такими как разработка планов реагирования на инциденты и программ обучения для повышения эффективности подготовки персонала к таким инцидентам. В конечном счете, ключевой задачей владельца/оператора КВИ является принятие обоснованных решений о действиях в отношении конкретных рисков с использованием практичных и экономически эффективных решений.

Мониторинг и обзор: Этот этап цикла управления рисками включает в себя мониторинг рисков и обзор реализации стратегий обработки рисков, чтобы удостовериться в том, что они соответствуют поставленным задачам. Эти меры включают в себя оценку успешности мер по снижению рисков, точности оценок рисков и эффективности процессов мониторинга. Инструментами мониторинга рисков могут быть аудиты и инспекции, проводимые внешними экспертами. Регулярные обзоры, зачастую проводимые ежегодно или после серьезных инцидентов, гарантируют актуальность и эффективность результатов управления рисками (часто в форме плана управления рисками). Полученные на этом этапе замечания и предложения используются для улучшения и разработки будущих мер по управлению рисками, что создает непрерывный цикл обратной связи, обеспечивающий последовательное совершенствование.

6 Меры физической безопасности

«

Очевидно, что террористические организации располагают целым рядом методов атак, начиная от взрывчатых веществ, огнестрельного оружия, беспилотных летательных аппаратов, химических, биологических, радиологических и ядерных материалов и транспортных средств до похищения людей или захвата заложников. Это означает, что разработка эффективных мер по обеспечению физической безопасности жизненно важна для защиты любого объекта критически важной инфраструктуры.

»

6 Меры физической безопасности

Существует множество злоумышленников, включая террористов, которые представляют физическую угрозу объектам КВИ с намерением вывести их из строя (полностью или частично) путем их уничтожения или повреждения. Понимание характера террористической угрозы для конкретного объекта КВИ требует комплексной оценки намерений и возможностей террористических организаций, а также рисков, которые они представляют, как подробно описано выше в главе 5 «Угроза терроризма и оценка рисков». Очевидно, что террористические организации располагают целым рядом методов атак, начиная от взрывчатых веществ, огнестрельного оружия, БАС,[202] ХБРЯ материалов и транспортных средств до похищения людей или захвата заложников. Это означает, что разработка эффективных мер по обеспечению физической безопасности жизненно важна для защиты любого объекта КВИ. В главе 5 концепция *риска* была представлена в виде формулы: *угроза* x *уязвимость* x *воздействие.* В данной главе рассматриваются потенциальные меры по снижению уязвимости объектов КВИ с акцентом на физическую безопасность.

Важность повышения безопасности на объектах КВИ признана как ООН, так и ОБСЕ. В Консолидированной концептуальной базе ОБСЕ для борьбы с терроризмом, принятой в декабре 2012 года, говорится, что ОБСЕ должна укреплять сотрудничество

202 Дополнительные рекомендации в отношении мер по предотвращению приобретения террористами оружия, такого как взрывные устройства, беспилотные летательные аппараты и огнестрельное оружие, можно найти в *Технических руководящих принципах по содействию выполнению Резолюции 2370 (2017 г.) Совета Безопасности и связанных с ней международных стандартов и передовой практики по предотвращению приобретения террористами оружия*, опубликованных КТУ ООН, Исполнительным директоратом Контртеррористического управления Совета Безопасности ООН, Институтом ООН по исследованию проблем разоружения и Глобальным договором ООН по координации борьбы с терроризмом.

и наращивать потенциал для предотвращения терроризма и борьбы с ним, в том числе в отношении повышения «безопасности международных перевозок и другой критически важной инфраструктуры».[203] Что касается критически важной энергетической инфраструктуры, то в 2007 году Совет министров ОБСЕ призвал все государства-участники «рассмотреть на национальном уровне все необходимые меры для обеспечения адекватной защиты жизненно важной энергетической инфраструктуры от террористических актов».[204] А Совет Безопасности ООН в своей Резолюции 2341 (2017 г.) признал, что многочисленные усилия, необходимые для защиты КВИ, должны включать в себя «меры физической защиты».[205]

В данной главе рассматриваются различные способы повышения физической безопасности и шаги, необходимые для разработки системы безопасности (включая примеры различных национальных подходов и моделей). Затем будут рассмотрены различные меры по обеспечению физической безопасности, которые входят в состав системы физической безопасности, включая системы обнаружения вторжений, освещение, системы видеонаблюдения, охрану периметра, системы контроля доступа, досмотр и использование зон ограниченного доступа. Наконец, будут рассмотрены методы проектирования и строительства, способные повысить физическую безопасность зданий объектов КВИ, включая строительные материалы, установку защищенного уличного оборудования, а также формы и расположение различных мер по обеспечению безопасности.

Реализация мер по обеспечению физической безопасности должна также подкрепляться соответствующими кадровыми ресурсами и процедурными мерами, гарантирующими их выполнение уполномоченными лицами и регулярную проверку. Такие меры должны осуществляться персоналом, прошедшим надлежащую проверку и обучение. Они также должны подкрепляться комплексными планами действий в чрезвычайных ситуациях и планами обеспечения безопасности, разработанными на уровне оператора КВИ, и быть пригодными для применения на объекте КВИ. Эти планы должны регулярно отрабатываться и обновляться по мере необходимости (см. главу 9 «Подготовка и учения»).

203 ОБСЕ (2012 г.), Решение Постоянного совета № 1063: Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом (PC.DEC/1063). Доступно по адресу: https://www.osce.org/files/f/documents/f/3/98542.pdf [дата обращения: 21 июля 2025 г.].

204 ОБСЕ (2007 г.), Решение Совета министров № 6/07: Защита важнейших объектов энергетической инфраструктуры от террористических актов (MC.DEC/6/07). Доступно по адресу: https://www.osce.org/files/f/documents/e/2/29485.pdf [дата обращения: 21 июля 2025 г.].

205 СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

Национальная практика: общие меры реагирования на чрезвычайные ситуации, рекомендуемые компаниям Национальным агентством экстренного реагирования Финляндии (2022 г.)[206]

Национальное агентство по экстренному реагированию Финляндии предоставляет следующие рекомендации по защите критически важной инфраструктуры компаний:

- Проверяйте контроль доступа, замки, видеонаблюдение, физическую защиту и другие меры в зависимости от потребностей физических объектов.
- В частности, пересмотрите меры защиты от киберугроз и методы управления инцидентами для важнейших основных бизнес-функций.
- Обеспечьте достаточно надежные телекоммуникационные соединения для критически важных операций с точки зрения эксплуатационной устойчивости.
- Обеспечьте энергоснабжение критически важных операций, т.е. обеспечьте наличие альтернативных источников энергии и оцените способность операций выдерживать перебои в энергоснабжении.
- Проанализируйте меры и планы организации по обеспечению непрерывности деятельности организации, а также меры по обеспечению готовности.
- Поощряйте бдительность персонала и обеспечьте получение сотрудниками актуальной информации.
- Уведомляйте органы власти и сеть наблюдений, не создавая излишних ограничений, чтобы формировалась общая картина ситуации и, при необходимости, инициировались возможные меры поддержки.

Источник: Национальное агентство по экстренному реагированию Финляндии

6.1 Концептуализация физической безопасности

Целью систем физической безопасности является защита объектов КВИ, включая оборудование и сотрудников, от несанкционированного физического проникновения, повреждения, уничтожения или нарушения функционирования. Меры по обеспечению физической безопасности могут включать в себя как активные, так и пассивные меры, направленные на сдерживание злоумышленников и защиту объектов[207] от различных угроз, включая несанкционированный доступ, кражу и повреждение. Ответственность за определение состава систем физической безопасности несут как владелец/оператор КВИ, так и соответствующие национальные органы.

206 Национальное агентство по чрезвычайным ситуациям (12 октября 2023 г.): В распоряжении компаний есть много способов защитить критически важную инфраструктуру [веб-страница]. Доступно по адресу https://www.huoltovarmuuskeskus.fi/en/a/companies-have-many-ways-of-protecting-critical-infrastructure [дата обращения: 21 июля 2025 г.].

207 Например, персонал, оборудование, установки, материалы и информация.

В изданном Организацией Объединенных Наций в 2022 году *Сборнике передовой практики по защите критически важной инфраструктуры от террористических атак* перечислены примеры мер по обеспечению физической безопасности, в том числе:

- определение периметра зоны КВИ и его защита с помощью физических барьеров;
- патрулирование и наблюдение силами правоохранительных органов и операторов КВИ с целью быстрого выявления подозрительной активности, происходящей вокруг критически важного объекта (например, проведение разведки злоумышленниками), и информирования о ней соответствующих органов;
- контроль доступа с использованием средств безопасности для повышения его эффективности (например, колючая проволока на заборах, системы обнаружения вторжений по периметру, освещение или система видеонаблюдения);
- использование таких технологий, как досмотр и другие средства обеспечения безопасности (например, обычное или высокоточное рентгеновское оборудование, собаки-детекторы для обнаружения взрывчатых веществ, ручные металлоискатели и технология обнаружения следов взрывчатых веществ).[208]

Национальная практика: Руководство по обеспечению физической безопасности Управления национальной безопасности Норвегии (2020 г.)[209]

В 2020 году Управление национальной безопасности Норвегии опубликовало публичные, необязательные основные принципы обеспечения физической безопасности. Они предназначены для предприятий всех секторов, желающих защитить свои объекты от различных преднамеренных и непреднамеренных угроз. Эти рекомендации не ограничиваются критически важными инфраструктурными секторами или компаниями. Управление национальной безопасности представляет четыре основных принципа обеспечения физической безопасности: (1) идентификация и картирование, (2) защита, (3) поддержание и обнаружение и (4) управление и восстановление. Эти принципы охватывают различные меры, такие как освещение и видимые средства сдерживания (заборы, барьеры, вывески), а также рекомендуемые процедуры, такие как эвакуация, изоляция и информирование о нарушениях. Управление национальной безопасности рекомендует проводить регулярные учебно-тренировочные занятия для персонала объектов, а также уделять особое внимание постоянному поддержанию механизмов обеспечения безопасности, включая как средства защиты, так и стратегии.

Источник: Управление национальной безопасности Норвегии

208 UNOCT и Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (2022 г.), *Защита критически важных объектов инфраструктуры от террористических атак: сборник передового опыта.* Доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf [дата обращения: 21 июля 2025 г.].

209 Управление национальной безопасности Норвегии (NSM) (2 октября 2020 г.), Grunnprinsipper for fysisk sikkerhet [веб-страница]. Доступно по адресу: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-fysisk-sikkerhet/introduksjon [дата обращения: 21 июля 2025 г.] неофициальный перевод.

Программа обеспечения физической безопасности Министерства обороны США определяет физическую безопасность как использование «материальных защитных и процедурных мер безопасности в сочетании с активными или пассивными системами, технологиями, устройствами и персоналом службы безопасности, используемыми для защиты объектов от возможных угроз».[210] Программа определяет следующие ключевые компоненты систем безопасности:

- силы безопасности и персонал, находящиеся под контролем владельца или пользователя;
- физические барьеры, системы защиты объектов и активные системы задержки или воспрепятствования;
- надежные системы запирания, контейнеры и хранилища;
- электронные системы безопасности, такие как системы обнаружения вторжений, радиочастотные детекторы или детекторы электронного излучения;
- оценка систем наблюдения (например, системы видеонаблюдения, тепловизоры, радары миллиметрового диапазона);
- защитное освещение;
- технологии идентификации, устройства контроля доступа, биометрия, системы маркировки материалов или объектов, а также оборудование для обнаружения запрещенных предметов и веществ;
- собаки с лицензированными кинологами (например, собаки-детекторы для обнаружения взрывчатых веществ, патрульные собаки и т.д.).[211]

210 Министерство обороны США (2007 г.), *Программа физической безопасности: Министерство обороны США, Руководство DoD 5200.08-R (С учетом изменения 2, 19 октября 2020 г.)* (Вашингтон, округ Колумбия: Министерство обороны США).

211 Министерство обороны США (2007 г.), *Программа физической безопасности. Министерство обороны США, Руководство DoD 5200.08-R (включая изменение 2, 19 октября 2020 г.)* (Вашингтон, округ Колумбия: Министерство обороны США).

Национальная практика: примеры мер по обеспечению физическойбезопасности, рекомендуемых Федеральным ведомством по гражданской обороне Швейцарии (2018 г.)[212]

Федеральное ведомство по гражданской обороне Швейцарии разработало руководство по защите критически важной инфраструктуры, в котором содержатся положения, которые следует учитывать владельцам/операторам КВИ при строительстве и защите своих объектов, в том числе:

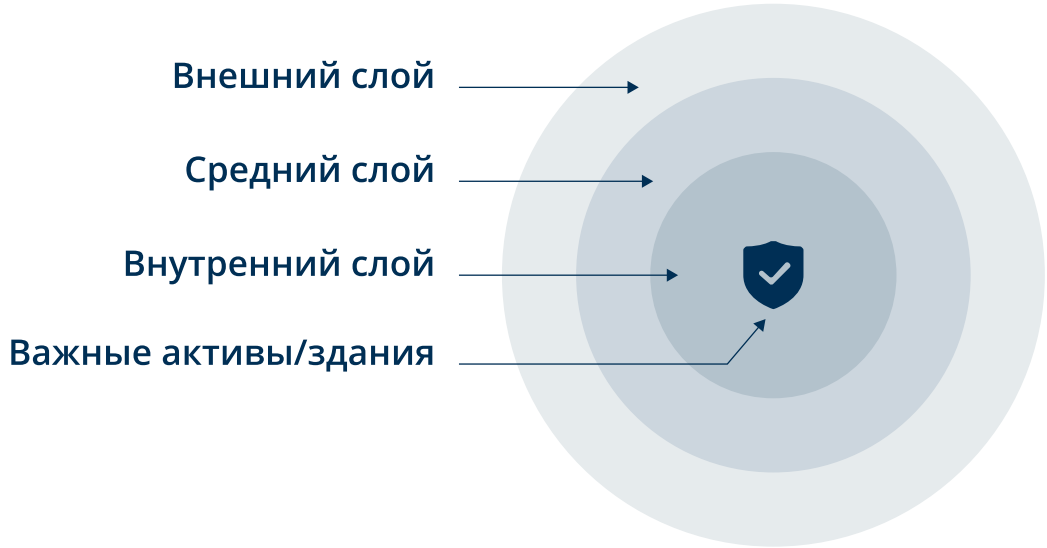
Охрана периметра	▸ Ограждение (сплошное, с защитой от прорыва, с минимальными требованиями к высоте, с защитой от прохода через ограждение или под ним [например, колючая проволока], видеонаблюдение) ▸ Двери и ворота, прочные на пробой ▸ Технический контроль доступа (домофоны, видеотехника, системы поэтапного доступа, считыватели идентификационных карт, клавиатуры и т.д.) ▸ Автоматическое электронное обнаружение (охранные ограждения и ворота, видеотехника с датчиками, защищённые верхние части стен, радиолокационное наблюдение, высокочастотные световые барьеры, тревожная сигнализация) ▸ Наружное освещение (по возможности, без резких теней, с защитой от взлома)
Защита зданий	▸ Защита охраняемых зон (электронная, механическая, контроль доступа, специальное наблюдение) ▸ Зарешеченные окна ▸ Защитное остекление в охраняемых зонах ▸ Защита окон (остекление, прочное на пробой, ударопрочное многослойное безопасное стекло, запираемые петли, фиксирующие планки на болтах) ▸ Ограниченное количество наружных дверей ▸ Защита главного входа (считыватель карт или чипов, замки с автоматической блокировкой, электрические устройства открывания дверей, автоматические запирающие устройства, домофон с видеонаблюдением, системы поэтапного доступа, разделение входа и выхода) ▸ Защита аварийных выходов (самозапирающиеся, автоматические замки, двери с сигнализацией) ▸ Выдача ключей только уполномоченным лицам ▸ Безопасное хранение запасных ключей
Меры по обеспечению безопасности персонала	Для персонала (внутреннего и внешнего): ▸ Проверка безопасности внутренних и внешних сотрудников ▸ Соблюдение персоналом законов, обязательств, положений, внутренних правил и т. д. ▸ Повышение осведомленности персонала в вопросах безопасности (курсы, учения, семинары, командные тренировки и т.д.) ▸ Подбор персонала с учетом требований безопасности: опыт, знания, проверка биографических данных (наличие судимости и т. д.), репутация, проверка рекомендаций ▸ Обеспечение безопасности при увольнении (возврат всех документов, офисных принадлежностей, ключей, паролей, бейджей и т.д.; соглашения о неразглашении и т.д.) ▸ Защита персонала (личная безопасность и т.д.)
Внешний персонал	▸ Регистрация: журнал входа и выхода посетителей ▸ Быстрая идентификация посетителей (например, по бейджам) ▸ Обеспечение сопровождения/контроля посетителей ▸ Контроль доставки и товаров

Источник: Федеральное ведомство по гражданской обороне Швейцарии

212 Федеральное ведомство по гражданской обороне Швейцарии (BABS), *Leitfaden Schutz kritischer Infrastrukturen* (Берн: BABS, 2018 г.). Доступно по адресу: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2023/12/12/27228b5a-2d7c-4c17-9df6-42e105197465.pdf [по состоянию на 21 июля 2025 г.] неофициальный перевод.

6.2 Эшелоны защиты или глубоко эшелонированная защита

Физическую безопасность можно обеспечить с помощью различных подходов и технологий. Одним из эффективных подходов является концепция глубоко эшелонированной защиты, которая состоит из нескольких последовательных уровней различных мер безопасности, образующих систему обнаружения вторжений (IDS) и основанных на основополагающем принципе, согласно которому общая безопасность объекта не снижается существенно при потере любого отдельного эшелона защиты. Ключевое преимущество этого подхода с последовательными эшелонами защиты, каждый из которых все сложнее преодолеть, заключается в том, что он предоставляет дополнительное время для обнаружения, оценки и реагирования службой безопасности, а также дает персоналу объекта время для перемещения в безопасные зоны на объекте в случае, если эвакуация невозможна.[213]



Эшелоны защиты могут начинаться с внешнего периметра объекта или площадки КВИ и продвигаться внутрь к зданию (зданиям) с наибольшей потребностью в защите. В качестве альтернативы эшелоны можно рассматривать в обратном порядке: начиная с того, что требует наибольшей защиты, и продвигаясь наружу.[214] В частности, если террористические организации используют «инсайдера» для содействия атаке, он может помочь им преодолеть некоторые или все эшелоны защиты изнутри. Более подробную информацию можно найти в главе 8 «Управление внутренними угрозами».

213 UNOCT и Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (2022 г.), *Защита критически важных объектов инфраструктуры от террористических атак: сборник передового опыта.* Доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf [дата обращения: 21 июля 2025 г.].

214 Министерство внутренней безопасности США (2011 г.), *Справочное руководство по снижению воздействия потенциальных террористических атак на здания: FEMA-426/BIPS-06/октябрь 2011 г. Издание 2*. Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

Национальная практика: концепция глубокоэшелонированной защиты зданий от террористических атак Министерства внутренней безопасности США (2011 г.)[215]

1. Первый или внешний эшелон: естественные или искусственные барьеры, обычно расположенные по границе участка или периметру объекта.
2. Второй или средний эшелон: обычно от периметра до внешней поверхности объекта. Защитные меры могут включать в себя естественные или искусственные барьеры, а также стратегию проектирования объекта, направленную на предотвращение доступа злоумышленников к ключевым объектам.
3. Третий или внутренний эшелон: относится к фасаду и/или внутренней части объекта и отделяет незащищенные зоны от защищенных. Ключевая концепция третьего эшелона – «укрепление» или повышение защищенности здания.

Источник: Министерство внутренней безопасности США

Для усиления эшелонов защиты заинтересованные стороны КВИ все чаще применяют концепции так называемой «безопасности по замыслу» на этапе проектирования и строительства (или реконструкции) зданий. Это помогает минимизировать будущие расходы, связанные с обеспечением физической безопасности. Примеры применения такого подхода приведены в справочнике *«Безопасность по замыслу: защита мест общественного пользования от террористических атак»*, опубликованном в 2022 году Объединенным исследовательским центром Европейской комиссии.[216] Хотя этот справочник посвящен защите общественных пространств, многие принципы безопасности по проектированию могут применяться и к КВИ.

6.3 Разработка системы безопасности

Реализация мер физической безопасности на объекте КВИ начинается с разработки системы безопасности, адаптированной к уникальному профилю и потребностям этого объекта. Системы безопасности должны включать в себя компоненты, которые эффективно взаимодействуют друг с другом, обеспечивая необходимый уровень защиты объекта и позволяя ему противостоять угрозам, адаптироваться к ним и/или быстро восстанавливаться после них, например, при террористической атаке. Практически в каждом случае система безопасности объекта КВИ будет включать в себя не только меры физической безопасности. Например, может быть полезно рассматривать безопасность персонала как ключевой компонент системы безопасности, если она направлена на снижение риска внутренних угроз на данном объекте (подробнее см. главу 8 «Управление внутренними угрозами»).

215 Министерство внутренней безопасности США (2011 г.), *Справочное руководство по снижению воздействия потенциальных террористических атак на здания: FEMA-426/BIPS-06/октябрь 2011 г. Издание 2.* Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

216 Бюро публикаций Европейского Союза (2024 г.), *Проектируемая безопасность: защита мест общественного пользования от террористических атак.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC131172 [дата обращения: 21 июля 2025 г.].

Национальная практика: пять компонентов системы безопасности Министерства внутренней безопасности США (2011 г.)[217]

1. *Политика, планы и процедуры безопасности,* включая планы действий в чрезвычайных ситуациях, планы обеспечения безопасности, процедуры обучения и тестирования, а также меры реагирования, общие рекомендации по процедурам, рекомендации по итогам процедур и рекомендации по привлечению внешних ресурсов.
2. *Операции по обеспечению безопасности и сбору оперативных данных,* определяющие потребности в обеспечении безопасности и включающие в себя обязанности охранников, сбор оперативных данных и обмен информацией.
3. *Физические барьеры,* включая ограждения, ворота и шлагбаумы для транспортных средств.
4. *Системы и оборудование безопасности,* включая электронные устройства, компьютерные системы и электронные системы контроля доступа.
5. *Кибербезопасность,* включая меры по защите операционных систем и данных КВИ от киберугроз и несанкционированных вторжений.

Источник: Министерство внутренней безопасности США

Модели систем безопасности

Существует множество различных, но схожих моделей систем безопасности, например:

Международное агентство по атомной энергии[218]	Сдерживание, обнаружение, задержка, реагирование
Национальное управление по защите и безопасности Великобритании[219]	Сдерживание, обнаружение, задержка, ослабление, реагирование
Австралия[220]	Сдерживание, обнаружение, задержка, реагирование, восстановление
Сингапур[221]	Сдерживание, обнаружение, задержка, недопущение, реагирование

217 Министерство внутренней безопасности США (2011 г.), *Справочное руководство по снижению потенциальных террористических атак на здания : FEMA-426/BIPS-06/октябрь 2011 г. Издание 2.* Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

218 Международное агентство по атомной энергии (МАГАТЭ) (2021 г.), *Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Серия изданий МАГАТЭ по физической ядерной безопасности № 40-Т.* Доступно по адресу: https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities [дата обращения: 21 июля 2025 г.].

219 Национальное управление по защите и безопасности Великобритании (2021 г.), Активы – Принципы [веб-страница, последнее обновление 18 марта 2021 г.]. Доступно по адресу: https://www.npsa.gov.uk/asset-0 [дата обращения 12 января 2024 г.].

220 Правительство Австралии – Министерство внутренних дел (2018 г.), *Основы политики защитной безопасности. Раздел 15: Физическая безопасность ресурсов организации. V2018.3* (Белконнен: Министерство внутренних дел).

221 Объединенная оперативная группа – Министерство внутренних дел (без даты), *Рекомендации по повышению безопасности зданий в Сингапуре.* Доступно по адресу: https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security [дата обращения: 21 июля 2025 г.]

Ключом к разработке и внедрению системы безопасности и определению ее модели является определение каждого компонента. Примеры определений вышеуказанных терминов приведены ниже:

Сдерживание	Меры, которые приводят к тому, что «потенциальные злоумышленники рассматривают объект как непривлекательную цель и решают не атаковать его, поскольку считают, что вероятность успеха слишком низка или риски для них самих слишком высоки».[222]
Обнаружение	Меры, которые «[начинаются] с обнаружения потенциально вредоносного или иного несанкционированного действия и которые [завершаются] оценкой причины сигнала тревоги».[223]
Задержка	Меры, которые «[направлены] на замедление продвижения злоумышленника к цели, тем самым предоставляя больше времени для эффективного реагирования».[224]
Недопущение	Меры, которые «[обеспечивают], что только уполномоченным лицам разрешен вход в охраняемые зоны».[225]
Ослабление	Меры, которые «[направлены] на прерывание и нейтрализацию действий злоумышленника, чтобы предотвратить завершение злонамеренного действия».[226]
Реагирование	Меры, направленные на «предотвращение, противодействие или ослабление атаки или события при их обнаружении».[227]
Восстановление	Меры, направленные на «восстановление работы до нормального уровня (в кратчайшие возможные сроки) после события».[228]

Структура той или иной системы безопасности определяется компетентными органами и/или владельцем/оператором КВИ. Как было продемонстрировано, существуют различные формы и размеры систем безопасности. Они должны быть адаптированы к уровню угроз и оценке рисков в секторе или на объекте. Важно определить структуру системы безопасности и использовать ее в качестве основы для интеграции всех компонентов системы, чтобы они работали на общую цель обеспечения надлежащего уровня защиты объекта.

222 МАГАТЭ (2021 г.), *Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Серия МАГАТЭ по физической безопасности № 40-Т.* Доступно по адресу: https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities [дата обращения: 21 июля 2025 г.].

223 МАГАТЭ (2021 г.), *Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Серия МАГАТЭ по физической безопасности № 40-Т.* Доступно по адресу: https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities [дата обращения: 21 июля 2025 г.].

224 МАГАТЭ (2021 г.), *Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Серия МАГАТЭ по физической безопасности № 40-Т.* Доступно по адресу: https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities [дата обращения: 21 июля 2025 г.].

225 Совместная оперативная группа – Министерство внутренних дел (без даты), *Руководство по повышению безопасности зданий в Сингапуре*. Доступно по адресу: https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security [дата обращения: 21 июля 2025 г.].

226 МАГАТЭ (2021 г.), *Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок. Серия МАГАТЭ по физической безопасности № 40-Т.* Доступно по адресу: https://www.iaea.org/publications/13459/handbook-on-the-design-of-physical-protection-systems-for-nuclear-material-and-nuclear-facilities [дата обращения: 21 июля 2025 г.].

227 Правительство Австралии – Министерство внутренних дел (2018 г.), *Основы политики защиты и безопасности. Раздел 15: Физическая безопасность ресурсов организации. V2018.3* (Белконнен: Министерство внутренних дел).

228 Правительство Австралии – Министерство внутренних дел (2018 г.), *Основы политики защиты и безопасности. Раздел 15: Физическая безопасность ресурсов организации. V2018.3* (Белконнен: Министерство внутренних дел).

6.4 Системы обнаружения вторжений

Независимо от модели системы безопасности, выбранной для объекта, контроль и обнаружение санкционированного и несанкционированного проникновения всегда будут ее ключевым компонентом. Такие меры осуществляются с помощью системы обнаружения вторжений (IDS). Используя средства видеонаблюдения, IDS обнаруживает изменения в целевой среде, например, появление нарушителя, а затем оповещает о несанкционированном проникновении (с помощью сигнализации). Помимо функций видеонаблюдения и сигнализации, эффективная IDS дополняется функциями мониторинга и реагирования как на объекте, так и за его пределами.

Обычно IDS включает в себя внутренние и внешние устройства срабатывания сигнализации, такие как датчики движения и дверные контакты. В рамках своих основных функций IDS отслеживает такие действия, как открытие/закрытие дверей доступа или перемещение персонала в целевой зоне. Система может также осуществлять мониторинг окружающей среды целевой зоны, такой как периметра объекта или других сооружений. Это позволяет IDS, например, обнаружить попытку злоумышленника прорвать ограждение периметра.

При обнаружении несанкционированного проникновения IDS подаст сигнал тревоги либо на пункт охраны на объекте, либо в удаленный центр мониторинга для последующего реагирования силами уполномоченных сотрудников службы безопасности. Учитывая секретность объектов КВИ и их защиту, владельцы/операторы КВИ могут рассмотреть возможность создания резервных каналов связи для оповещения о тревоге, а также резервных источников питания для обеспечения бесперебойной работы систем, например, в случае отключения электроэнергии.[229]

229 Ассоциация банков Сингапура (2018 г.), *Руководство по физической безопасности для финансовых учреждений.* Доступно по адресу: https://abs.org.sg/docs/library/abs-scps-guidelines.pdf [дата обращения: 21 июля 2025 г.].

В рамках системы IDS объекты могут применять стандартные средства в обычные периоды работы, а также дополнительные меры в период повышенной угрозы. Такие меры могут включать в себя дополнительные средства наблюдения и планы по активизации мер, информирующие персонал объекта о необходимых действиях в случае обнаружения угрозы.

Технологии обнаружения вторжений

Системы IDS могут включать в себя ряд технологических средств для обнаружения санкционированных и несанкционированных перемещений. Во многих случаях технологии, выбранные владельцами/операторами КВИ, могут основываться на местных, национальных или отраслевых стандартах эффективности или рекомендациях компетентных органов. Технологические средства, доступные владельцам/операторам КВИ, различаются в разных странах региона ОБСЕ. Однако Центр по защите национальной критически важной инфраструктуры Великобритании (ныне Национальное управление по защите и безопасности [NPSA]) представил краткий список основных категорий доступных технологий обнаружения в своих добровольных рекомендаций по системам обнаружения вторжений для руководителей служб безопасности объектов КВИ, как представлено в таблице ниже:[230]

Технологии	Принцип работы
Пассивное инфракрасное обнаружение движения	Пассивные инфракрасные датчики обнаруживают присутствие злоумышленника, улавливая тепловое (инфракрасное) излучение от человеческого тела.
Микроволновое обнаружение движения	Микроволновые датчики движения излучают электромагнитные радиоволны. При контакте с объектом часть волн поглощается, часть отражается и рассеивается во всех направлениях, а часть отражается обратно к детектору.
Комбинированные детекторы	Детекторы, объединяющие две или более технологий обнаружения в одном корпусе (например, пассивное инфракрасное в сочетании с микроволновым), приобрели популярность благодаря повышенной стабильности в условиях эксплуатации. Сочетание различных технологий обеспечивает повышенную устойчивость к ложным срабатываниям по сравнению с детекторами, использующими только одну технологию.
Детекторы разбития стекла	При разбивании стекла генерируется широкий диапазон частот. В зависимости от типа, детекторы разбития стекла используют частоты в одном или нескольких из этих диапазонов для обнаружения разбития.
Детекторы вибрации и ударов	Детекторы вибрации и удара используются в случаях, когда ожидаемая попытка проникновения приведет к проникновению через плоскую поверхность (например, стену) или другое препятствие. Способы проникновения могут включать в себя сверление, удары кувалдой, киркой или аналогичным инструментом, резку пилой, шлифовальной машиной или кислородно-ацетиленовой горелкой/электродами, а также подрыв с использованием взрывчатых веществ.
Сейсмические детекторы	Сейсмические вибрационные детекторы способны обнаруживать широкий спектр силовых воздействий: от мощных ударных импульсов до мельчайших вибрационных толчков.
Инерционные детекторы	Инерционные детекторы предназначены для общего применения. Они могут стать надежным и экономичным решением для обнаружения большинства способов силового проникновения.

230 Центр защиты национальной инфраструктуры (2013 г.), *Системы обнаружения вторжений: руководство для менеджеров по безопасности,* стр. 59, 70, 75, 81, 86–88, 91, 96. Доступно по адресу: https://www.npsa.gov.uk/resources/intrusion-detection-systems-guidance-security-managers [дата обращения: 21 июля 2025 г.].

Датчики удара	Датчики удара обычно реагируют на вибрации, вызванные силовыми методами проникновения, например, при таране двери и снятии ее с петель.
Защитные выключатели	Защитные выключатели используются для обнаружения открытия двери, окна или другого проема.
Активные инфракрасные детекторы	Активные инфракрасные детекторы излучают один или несколько инфракрасных лучей, которые можно настроить так, чтобы создать «барьер обнаружения», невидимый для человеческого глаза. Если лучи прерываются, например, когда через них проходит злоумышленник, приемник обнаруживает потерю инфракрасного сигнала и активирует сигнал тревоги.

Типы систем обнаружения вторжений

Для обнаружения несанкционированных проникновений на объекте КВИ системы IDS могут применяться двумя способами: для внешнего и внутреннего использования. Каждое тип применения предъявляет свои системные требования и имеет различные технологические решения. При проектировании внешних систем IDS, которые потенциально могут осуществлять наблюдение за лицами, не являющимися сотрудниками объекта КВИ, важно учитывать влияние таких действий на права человека, включая сбор и хранение данных (подробнее см. в главе 3 «Соображения в области прав человека»). Общепринятой практикой защиты объекта КВИ является использование как внешних, так и внутренних элементов IDS. Ниже представлено описание каждого варианта применения.

Внешние системы обнаружения вторжений. Внешние эшелоны системы безопасности часто являются наиболее важным компонентом, поскольку они обеспечивают самое раннее обнаружение и реагирование. Как правило, что чем дальше внешний эшелон IDS находится от цели (например, входа или периметра объекта КВИ), тем лучше. Это означает, что внешние IDS обычно используются для обнаружения вторжений на периметре объекта или за его пределами. Однако в Директиве НАТО по физической безопасности 2020 года признается, что внешние IDS «по своей природе склонны к ложным срабатываниям и поэтому обычно должны использоваться только с системой проверки сигналов тревоги, такой как CCTV [система видеонаблюдения]».[231] Таким образом, система безопасности, включающая в себя внешнюю IDS, должна обеспечивать быструю проверку срабатываний сигналов тревоги для подтверждения наличия опасной или санкционированной активности.

Внутренние системы обнаружения вторжений. Внутренние IDS обычно предполагают сочетание датчиков и устройств видеонаблюдения, предназначенных для обнаружения несанкционированных проникновений на объект. В отличие от

231 Крискуоло, М. (2020 г.), Директива по физической безопасности, документ НАТО AC/35-D/2001-REV3 (Брюссель: Организация Североатлантического договора).

внешних IDS, внутренние IDS считаются менее дорогостоящими, поскольку они зачастую лучше защищены, в том числе от неблагоприятных погодных условий. Выбор конкретных датчиков или сочетания датчиков для системы IDS определяется руководителями служб безопасности и компетентными органами на основе соответствующих инструкций и стандартов эффективности. Во многих случаях используются датчики проникновения, которые обнаруживают успешное или предпринятое проникновение на объект через его периметр.[232]

Национальная практика: Программа обеспечения физической защиты Министерства энергетики США – базовые требования к физической защите: выборочные требования для тестирования внутренней системы обнаружения вторжений (2021 г.)[233]

Руководящие принципы Министерства энергетики США разработаны для установления базовых требований к физической защите объектов, находящихся под контролем Министерства энергетики США. Ниже приведены требования к тестированию внутренних систем обнаружений вторжений:

- Система обнаружения и оценки вторжений по периметру (PIDAS) должна быть способна обнаруживать человека, пересекающего зону обнаружения путем ходьбы, ползания, прыжка, бега, перекатывания и/или восхождения на ограждение в любой точке зоны обнаружения, с вероятностью обнаружения 90 процентов и уровнем достоверности 95 процентов.
- После установки и затем ежегодно (не реже одного раза в 12 месяцев) необходимо проводить проверку работоспособности системы обнаружения вторжений, чтобы подтвердить ее соответствие требованиям к вероятности обнаружения и уровню достоверности.
- Если вероятность обнаружения в системе обнаружений вторжений падает ниже требуемой, ее необходимо отремонтировать и повторно протестировать.
- При расчете вероятности обнаружения для систем с несколькими датчиками предполагается, что обнаружение произошло, если хотя бы один из датчиков оповестил о вторжении.
- Необходимо провести испытание производительности, чтобы определить правильные настройки, обеспечивающие высокий уровень обнаружения с минимальным количеством ложных срабатываний сигнализации.
- Испытания необходимо проводить как с малозаметной целью (ползущей), так и с более скоростной (идущею, бегущей, быстро ползающей, катящейся).
- Испытания должны проводиться в погодных и световых условиях, типичных для данной местности.

Источник: Министерство энергетики США

232 Министерство национальной безопасности США (2011 г.), *Справочное руководство по снижению потенциальных террористических атак на здания : FEMA-426/BIPS-06/октябрь 2011 г. Издание 2*. Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

233 Министерство энергетики США, Программа физической защиты 473.1A, Приложение 2: Базовые требования физической защиты. Доступно по адресу: https://www.directives.doe.gov/directives-documents/400-series/0473.1-BOrder-a/@@images/file [дата обращения: 21 июля 2025 г.].

6.5 Освещение

Освещение на объекте КВИ (как внутреннее, так и внешнее) является основным компонентом эффективной системы обеспечения физической безопасности. Вопросы использования освещения в целях безопасности кратко изложены в *Сборнике руководств ОБСЕ по лучшей практике в области обычных боеприпасов* 2008 года:

> «Освещение охраняемой зоны помогает в обнаружении, оценке и пресечении угрозы безопасности. Освещение может также служить для посторонних дополнительным отпугивающим фактором. Освещение охраняемого объекта повышает результативность работы охраны и CCTV, улучшая видимость в темное время суток или освещая участок, куда не всегда проникает естественный свет. Средства наружного освещения охраняемого объекта, как правило, размещаются вдоль внешнего периметра объекта и пропускных пунктов».[234]

Конкретные требования к освещению будут различаться для каждого объекта КВИ в зависимости от потребностей и оцененных угроз, с которыми он сталкивается. В некоторых случаях международные или национальные стандарты, такие как ISO 8995-1:2002 «Освещение рабочих мест» или Единые критерии Министерства обороны США по системам внутреннего и наружного освещения (UFC 3-530-01 (C4-2019)),[235] содержат ценные рекомендации. Системы освещения не следует проектировать отдельно от других аспектов системы безопасности объекта КВИ. Например, в США Министерство национальной безопасности подчеркивает, что системы освещения должны быть

234 ОБСЕ (2008 г.), *Сборник руководств ОБСЕ по лучшей практике в области обычных боеприпасов* (Вена: ОБСЕ). Доступно по адресу: https://www.osce.org/files/f/documents/5/6/33375.pdf [дата обращения: 21 июля 2025 г.].

235 Министерство обороны США (2023 г.), *Единые критерии объектов (UFC): Системы внутреннего и внешнего освещения.* Доступно по адресу: https://www.wbdg.org/FFC/DOD/UFC/ufc_3_530_01_2023_c1.pdf [дата обращения: 21 июля 2025 г.].

спроектированы с учетом работы систем видеонаблюдения или постов охраны, которым обычно требуется более высокий уровень освещения.[236]

Рассмотрение различных стратегий освещения для отдельных частей объекта КВИ считается хорошей практикой. Общество инженеров-светотехников в своем *Руководстве по охранному освещению для людей, имущества и критически важной инфраструктуры* 2016 года утверждает: «При планировании или оценке охранного освещения проектировщикам будет полезно разделить объект на зоны, такие как периметр, пешеходная зона, здание, транспортное средство, склад, оборудование и зоны ограниченного доступа. В процессе планирования проектировщики могут определить и спланировать различные другие зоны для оценки конкретного охранного освещения в соответствии с требованиями проекта. Для каждой зоны может потребоваться учет различных факторов уязвимости и реагирования».[237]

Стратегии освещения также должны включать в себя меры защиты от злонамеренных действий, таких как несанкционированное вмешательство или повреждение светильников. Руководители по безопасности могут устанавливать светильники высоко, вне досягаемости потенциальных злоумышленников, и обеспечивать их защиту с помощью антивандальных материалов, таких как проволочная сетка или металлический/пластиковый кожух.

Наконец, хорошей практикой считается обеспечение резервных источников питания для наиболее важных систем охранного освещения на объекте КВИ, при этом панель управления такими системами должна размещаться в безопасной зоне с контролируемым доступом.

236 Министерство национальной безопасности США (2011 г.), *Справочное руководство по снижению потенциальных террористических атак на здания. FEMA-426/BIPS-06/октябрь 2011 г. Издание 2.* Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

237 Светотехническое инженерное общество (2016 г.), *Руководство по безопасному освещению для людей, имущества и критически важной инфраструктуры.* Доступно по адресу: https://cdn.fedweb.org/fed-96/2/IES%2520Security%2520Lightingn%2520G-1_web.pdf [дата обращения: 21 июля 2025 г.].

Типы охранного освещения

Как указано выше, требования к освещению будут различаться для каждого объекта КВИ в зависимости от потребностей и оцененных угроз, с которыми он сталкивается. Охранное освещение существует в нескольких различных вариантах, как вкратце описано в рекомендациях Министерства внутренней безопасности США, представленных ниже[238]:

Непрерывное освещение	Непрерывное освещение – наиболее распространенная система охранного освещения. Эта система состоит из ряда стационарных светильников, расположенных таким образом, чтобы непрерывно освещать определенную зону в темное время суток перекрывающимися конусами света.
Резервное освещение	Резервное освещение имеет схему, схожую со схемой непрерывного освещения; однако свет не горит постоянно, а включается автоматически или вручную при обнаружении или подозрении со стороны сотрудников службы безопасности или системами сигнализации подозрительной активности.
Передвижное освещение	Передвижное освещение состоит из управляемых вручную передвижных прожекторов, которые могут включаться в темное время суток или по мере необходимости. Система обычно используется в качестве дополнения к непрерывному или резервному освещению. Передвижное освещение также используется для облегчения досмотра транспортных средств во временных и постоянных зонах досмотра транспортных средств.
Аварийное освещение	Аварийное освещение – это резервная система питания освещения, которая может дублировать любую или все из вышеперечисленных систем. Ее использование ограничено временем отключения электроэнергии или другими чрезвычайными ситуациями, при которых основная система не работает. Она зависит от альтернативного источника питания, например, стационарных или переносных генераторов или аккумуляторов. Для охранного освещения следует рассмотреть возможность аварийного резервного питания.

6.6 Системы видеонаблюдения

Одним из компонентов системы обнаружения вторжений является система охранного видеонаблюдения (VSS), которая обычно стратегически удобно размещается по всему объекту КВИ для отслеживания подозрительного поведения и других факторов. Европейский инспектор по защите данных определяет видеонаблюдение как «мониторинг определенной зоны, события, деятельности или лица с помощью электронного устройства или системы визуального наблюдения».[239] Ассоциация банков Сингапура описывает VSS как «неотъемлемую часть мониторинга безопасности, поскольку она предоставляет информацию для проведения расследований, когда это необходимо. Система видеонаблюдения CCTV также может отпугнуть злоумышленников, если они считают, что их действия отслеживаются и записываются»[240]. Система VSS должна соответствовать местным законам о сборе, хранении и защите данных, а также быть необходимой и соразмерной (см. главу 3 «Соображения в области прав человека»). Как и в других разделах настоящего *Технического руководства*, в некоторых случаях международные или национальные

238 Министерство национальной безопасности США (2011 г.), *Справочное руководство по снижению потенциальных террористических атак на здания : FEMA-426/BIPS-06/октябрь 2011 г. Издание 2*. Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

239 Европейский инспектор по защите данных (без даты), Видеонаблюдение [веб-страница]. Доступно по адресу: https://www.edps.europa.eu/data-protection/data-protection/glossary/v_en#video_surveillance [дата обращения: 30 ноября 2024 г.].

240 Ассоциация банков Сингапура (2018 г.), *Руководство по физической безопасности для финансовых учреждений.* Доступно по адресу: https://abs.org.sg/docs/library/abs-scps-guidelines.pdf [дата обращения: 21 июля 2025 г.].

стандарты содержат ценные рекомендации, например, Европейский стандарт 50132-1 «Системы тревожной сигнализации – Системы видеонаблюдения CCTV для использования в целях безопасности – Часть 1: Требования к системе».

При правильном использовании VSS оказывают ценную помощь сотрудникам службы безопасности в проверке инцидентов и активации как внутренних, так и внешних систем обнаружения вторжений. Однако эффективность VSS зависит от типов используемых камер и их установки, а также процесса мониторинга видеоданных VSS.

Места установки камер

Система VSS включает в себя несколько камер, стратегически удобно размещенных для обеспечения возможностей видеонаблюдения в заданном месте. Они могут быть установлены в точках доступа к объекту КВИ, на периметре, зонах критически важных бизнес-операций и/или зонах, содержащих ценное или критически важное имущество. Правильное размещение камер должно основываться на заранее определенной функции.

Национальная практика: примеры функций системы видеонаблюдения, рекомендуемые Национальным управлением по защите и безопасности Великобритании[241]

- предотвращение попытки вторжения, заставляя злоумышленника пересмотреть свое решение в отношении объекта из-за повышенной вероятности обнаружения;
- обнаружение попытки вторжения на объект с помощью видеоаналитики;
- проверка и расследование тревожного события от системы обнаружения вторжений на периметре;
- отслеживание нарушителя при пересечении им периметра;
- запись цифровых изображений, пригодных для использования в качестве доказательств в ходе расследования или судебного разбирательства;
- наблюдение за зонами контроля доступа.

Источник: Национальное управление по защите и безопасности Великобритании

Национальная практика: категории полей обзора стандартной системы видеонаблюдения для зданий, установленные полицией Сингапура (2022 г.)[242]

Категория поля обзора	Описание
Обнаружение	Фигура занимает не менее 10% доступной высоты экрана (или более 40 мм на пиксель), а изображаемая область не перегружена. После срабатывания сигнала тревоги сотрудник может, проведя поиск, с высокой степенью уверенности установить, виден ли человек на отображаемых изображениях.
Наблюдение	Фигура должна занимать от 25% до 30% высоты экрана (или более 16 мм на пиксель). При таком масштабе можно различить отдельные характерные детали человека, например, отличительные черты одежды, при этом обзор остается достаточно широким, чтобы отслеживать некоторые события, происходящие вокруг инцидента.
Распознавание	Когда фигура занимает не менее 50% высоты экрана (или более 8 мм на пиксель), сотрудник может с высокой степенью уверенности сказать, является ли показанный человек тем же самым человеком, которого он видел раньше.[243]
Идентификация	Поскольку теперь фигура занимает не менее 120% высоты экрана (или более 4 мм на пиксель), качество изображения и детализация должны быть достаточными для того, чтобы идентифицировать личность человека без обоснованных сомнений.

Источник: Полиция Сингапура

241 Национальное управление по защите и безопасности Великобритании (без даты), CCTV. Обзор [веб-страница]. Доступно по адресу: https://www.npsa.gov.uk/cctv [дата обращения: 30 ноября 2024 г.].

242 Полиция Сингапура (2022 г.), *Стандарт системы видеонаблюдения (VSS) для зданий, версия 2.0*. Доступно по адресу: https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security [дата обращения: 21 июля 2025 г.].

243 Полиция Сингапура делает дополнительный комментарий: «Следует отметить, что на данном этапе, когда эти руководящие принципы были впервые разработаны, все системы использовали общую полностью аналоговую систему [Phase Alternate Line] с фиксированным разрешением 576 строк для захвата и отображения видео. С приходом цифровых систем на рынок [VSS] у нас появилось больше возможностей для захвата, записи и отображения в более высоком разрешении. Поэтому требование «Распознавания» больше не приравнивается к размеру фигуры в 50% высоты экрана. Например, благодаря использованию мегапиксельных камер и дисплеев с высоким разрешением теперь можно обеспечить то же разрешение изображения, что и раньше, используя гораздо меньший физический процент экрана».

Типы камер

Система VSS состоит из ряда камер, размещенных в стратегических точках для выполнения заранее определенной функции. В зависимости от функции могут использоваться различные камеры. Например, камеры могут быть стационарными (неподвижными) или гибкими (с возможностью направления в разные стороны). Камеры могут иметь функцию масштабирования, обеспечивающую крупный план или широкоугольный обзор, а также могут быть оснащены дополнительными технологиями, позволяющими, например, записывать номерные знаки и другую информацию. В рамках комплексной системы безопасности крайне важно учитывать взаимодействие между освещением, размещением камер и выбором камер.

Мониторинг системы видеонаблюдения

Помимо камер, еще одним ключевым компонентом системы VSS является ее функция мониторинга. Если видеосигналы с камер не отслеживается сотрудниками службы безопасности, предшествующее нападению подозрительное поведения или преступная деятельность могут остаться незамеченными, или меры реагирования на инцидент будут приняты с задержкой.

Мониторинг видеосигнала VSS обычно осуществляется в диспетчерской на объекте КВИ, где работают сотрудники службы безопасности, прошедшие подготовку по реагированию на различные инциденты, включая вооруженные вторжения, угрозы взрыва, взрывы и т.д. Такая подготовка должна сопровождаться письменными инструкциями, которые помогут этим сотрудникам в чрезвычайных ситуациях и позволят им оповестить все необходимые заинтересованные стороны на объекте и за его пределами, включая местные правоохранительные органы и службы быстрого реагирования.

Национальная практика: стандарт системы видеонаблюдения для зданий, рекомендованный полицией Сингапура (2022 г.)[244]

- Операторы в диспетчерской службы безопасности, пожарном командном центре или других местах (пунктах просмотра сигнала VSS) в здании должны контролировать изображения VSS в режиме реального времени.
- В пункте просмотра сигнала VSS оператор должен иметь возможность выбрать изображение с любой камеры для отображения на любом мониторе в любое время или настроить последовательность сканирования с желаемым временем задержки.
- Система управления выбором камеры должна обеспечивать быстрый выбор изображения с любой камеры с минимальными ручными усилиями и быть единообразной во всей сети VSS.
- В случае любого инцидента каждый монитор в диспетчерской должен иметь возможность вывода изображения с любой камеры в системе VSS здания. Система должна обеспечивать многооконный режим отображения на мониторах VSS.
- Выбор одним пользователем изображения в режиме реального времени (потока) не должен мешать другим пользователям выбрать то же изображение в режиме реального времени (потока) или любые другие изображения в той же системе.
- Все изображения с камер, отображаемые на мониторах, должны представлять собой единое наложение с идентификационными кодами камер, датой и временем.
- Для облегчения общего наблюдения за безопасностью и сохранностью здания, а также управления инцидентами необходимо тщательно спланировать маркировку и нумерацию камер, а также соответствующую последовательность записи, чтобы обеспечить быстрый поиск записанных изображений.

Источник: Полиция Сингапура

Мониторинг VSS предполагает запись данных, включая данные о персонале и посетителях объекта. Поэтому сбор, хранение, использование и раскрытие записей VSS должны осуществляться в соответствии с соответствующими национальными законами и политикой в области защиты данных.

Видеозапись и хранение записей

Мониторинг видеонаблюдения важен для немедленного реагирования, в то время как запись и хранение материалов видеонаблюдения поддерживают следственные и другие действия правоохранительных органов. Важно иметь возможность сохранять записи видеонаблюдения в целях безопасности. Меры по хранению записей должны соответствовать национальным законам и процедурам, в том числе в области защиты данных и конфиденциальности (для получения дополнительной информации см. главу 3 «Соображения в области прав человека»). Все камеры, входящие в систему VSS, должны иметь возможность записывать и хранить изображения в течение срока, установленного национальными законами и процедурами. Не существует международного стандарта, установленного для срока хранения записей VSS; этот срок в значительной степени зависит от национального контекста. Например, Национальное управление по защите и

244 Полиция Сингапура (2022 г.), *Стандарт системы видеонаблюдения (VSS) для зданий, Версия 2.0*. Доступно по адресу: https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security [дата обращения: 21 июля 2025 г.].

безопасности Великобритании рекомендует хранить записи в течение 30 дней,[245, 246] в то время как полиция Сингапура рекомендует 31 день и более.[247]

6.7 Охрана периметра

Определение границ и поддержание безопасности периметра вокруг объекта КВИ имеют решающее значение для его эффективной защиты. Периметр представляет собой внешнюю линию обороны системы безопасности объекта. Он служит для контроля доступа транспортных средств и людей, задержки несанкционированного проникновения и сдерживания потенциальных злоумышленников. Периметры могут состоять из заборов, барьеров (естественных или искусственных), густой растительности или других сооружений.

Национальная практика: функции правильно спроектированного периметра, рекомендуемые Национальным управлением по защите и безопасности Великобритании (2011 г.)[248]

Правильно спроектированный и созданный периметр должен:

- Способствовать предотвращению потенциальных атак;
- Обеспечивать санкционированный доступ на объект как пешеходам, так и транспортным средствам через предусмотренные точки доступа;
- Предотвращать несанкционированный доступ через предусмотренные точки доступа;
- Обеспечивать контролируемое расстояние для снижения эффективности угроз, расположенных по периметру, таких как самодельные взрывные устройства, установленные на транспортных средствах;
- Способствовать задержке, обнаружению и пресечению несанкционированных попыток нарушения безопасности объекта;
- Обеспечивать соответствующие условия для выполнения сотрудниками службы безопасности своих обязанностей, включая обеспечение защиты в случае нападения;
- Способствовать минимизации риска сопутствующего ущерба для людей, объектов и инфраструктуры;
- Эффективно взаимодействовать с другими системами безопасности на объекте и вокруг него.

Источник: Национальное управление по защите и безопасности Великобритании

245 Центр защиты национальной инфраструктуры (2020 г.), *Хранение и сохранение записанных изображений видеонаблюдения. Версия 2.0.* Доступно по адресу: https://www.npsa.gov.uk/resources/storage-and-retention-recorded-cctv-images-2020 [дата обращения: 21 июля 2025 г.].

246 Служба тюрем и пробации Ее Величества (без даты), Сохранение записей видеонаблюдения [веб-страница]. Доступно по адресу: https://assets.publishing.service.gov.uk/media/619b92788fa8f503780c1b5f/annex-f-at-compliant-version-retention-cctv-footage.pdf [дата обращения: 21 июля 2025 г.].

247 Полиция Сингапура (2022 г.), *Стандарт системы видеонаблюдения (VSS) для зданий,* версия 2.0. Доступно по адресу: https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security [дата обращения: 21 июля 2025 г.].

248 Национальное управление по защите и безопасности Великобритании (2021 г.): Строительство и инфраструктура [веб-страница]. Доступно по адресу: https://www.npsa.gov.uk/building-infrastructure [дата обращения: 30 ноября 2024 г.].

Если в ходе оценки риска для объекта КВИ предполагается вероятность угрозы со стороны вражеских транспортных средств, следует рассмотреть возможность установки сертифицированных противотаранных заграждений по всему периметру. Важно отметить, что стоимость сертифицированных систем защиты от вражеских транспортных средств, рассчитанных на столкновение, намного выше, чем стоимость обычных систем ограждения (подробнее см. в главе 7 «Планирование безопасности и укрепление объекта»).

Ограждения и барьеры

Периметральные ограждения или барьеры, хотя и необходимы, могут лишь на время *задержать* решительного нарушителя. В *Сборнике руководств ОБСЕ по лучшей практике в области обычных боеприпасов* говорится, что «ограждения (так со средствами, так и без средств усиления) зачастую позволяют выиграть менее одной минуты при противодействии угрозам низкого уровня и всего 3-8 секунд при противодействии попыткам проникновения со стороны опытных и мотивированных групп высокопрофессиональных злоумышленников».[249]

В большинстве случаев периметр объекта КВИ включает в себя охранное ограждение, предназначенное для разделения защищенного пространства от незащищенного. Такое ограждение может включать в себя металлическую сетку-рабицу, сетчатые панели или другие типы ограждений и может быть дополнено колючей проволокой или другими физическими средствами сдерживания. Важно, чтобы несущественные конструкции, такие как фонарные столбы или телефонные столбы, располагались вдали от охранного ограждения, поскольку они могут служить средством для преодоления забора злоумышленником. В идеале нижняя часть ограждения должна быть расположена ниже уровня земли. Система обнаружения вторжений (IDS) также может быть интегрирована в охранное ограждение, например, для включения сигнализации при несанкционированном доступе к ограждению.

249 ОБСЕ (2008 г.), *Сборник руководств ОБСЕ по лучшей практике в области обычных боеприпасов*. Доступно по адресу: https://www.osce.org/files/f/documents/5/6/33375.pdf [дата обращения: 21 июля 2025 г.].

Барьеры также могут использоваться вместо охранных ограждений в особых случаях, в соответствии с потребностями объекта и окружающей средой. Барьеры могут состоять из земляных насыпей, литого бетона или других искусственных материалов, таких как сталь.

При наличии актуальной угрозы использования БАС следует рассмотреть возможность использования сетей или ограждений против БАС в составе зданий или периметральных конструкций.[250] В таких случаях также могут быть рассмотрены возможности использования технологий противодействия БАС.

Ворота в периметральном ограждении
Безопасность ворот объекта КВИ оказывает значительное влияние на общую безопасность его периметра, поскольку ворота, как правило, считаются самым слабым звеном периметра с точки зрения несанкционированного доступа. Ворота должны быть сконструированы в соответствии с теми же стандартами безопасности, что и сам периметр, и должны иметь систему контроля доступа.

Как правило, количество ворот в периметре объекта КВИ должно быть сведено к минимуму, чтобы сократить ресурсы, необходимые для их патрулирования и мониторинга. Это особенно актуально для участков периметра, расположенных вдали от основной точки доступа, где может находиться постоянная группа охраны.

Важно осуществлять постоянный мониторинг периметра и его ворот с помощью системы VSS для обнаружения опасной активности.

6.8 Системы контроля доступа

Учитывая, что ключевым компонентом физической безопасности является предотвращение несанкционированного доступа на объект, владельцы/операторы КВИ применяют ряд средств контроля доступа. Они могут быть расположены как снаружи (по периметру объекта), так и внутри (для обеспечения доступа к определенным частям объекта только авторизованным лицам). Они могут включать в себя электронные системы доступа с определенными процедурами для доступа к чувствительным зонам объекта. Важно, чтобы все системы контроля доступа соответствовали действующим нормам охраны труда и техники безопасности, включая противопожарную безопасность, для обеспечения безопасности персонала объекта КВИ.

250 См. также: *Объединенный исследовательский центр Европейской комиссии (2023 г.), Защита от беспилотных летательных аппаратов: Руководство по оценке риска беспилотных летательных аппаратов и принципам физического укрепления зданий и объектов.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC132967 [дата обращения: 21 июля 2025 г.].

Национальная практика: инструкции по обеспечению безопасности для владельцев/ операторов критически важной инфраструктуры в Республике Казахстан (1999/2023 гг.)[251]

На основании Закона Республики Казахстан «О противодействии терроризму» 1999 года[252] отдельные министерства выпустили инструкции по организации антитеррористической защиты стратегических объектов, находящихся в их ведении. В 2023 году министр индустрии и инфраструктурного развития издал Приказ № 508 о защите объектов питьевого водоснабжения. Инструкции разделены на различные тематические категории и главы, в том числе:

- пропускной режим;
- профилактические и образовательные мероприятия;
- инженерно-техническое оборудование (ворота, ограждения, системы видеонаблюдения, контрольно-пропускные пункты, досмотр транспортных средств);
- предметы и вещества, запрещенные к проносу на территорию соответствующих объектов;
- документы, которые должны храниться у руководителей объектов (например, планы охраны, должностные инструкции сотрудников подразделения охраны);
- учебные программы по вопросам безопасности, связанным с борьбой с терроризмом;
- контрольные списки действий при различных сценариях угроз (например, обнаружение подозрительных предметов, угроза захвата заложников, получение анонимных сообщений о взрывном устройстве).

Источник: Правительство Республики Казахстан

Внешний контроль доступа

Меры внешнего контроля доступа по периметру объекта используются для предотвращения доступа неавторизованных лиц и для облегчения доступа аккредитованного персонала и авторизованных посетителей. Они также предотвращают пронос СВУ или других опасных материалов и устройств на объект потенциальными злоумышленниками. Входящие посылки и личные вещи могут контролироваться и проверяться на входе в объект КВИ (например, с помощью рентгеновских аппаратов). Уровень внешнего контроля доступа, требуемый для конкретного объекта КВИ, будет варьироваться в зависимости от уровня угроз и оценки рисков. Тем не менее, следует рассмотреть возможность разработки стандартных мер внешнего контроля доступа в периоды нормальной работы и усиленных мер в периоды повышенной угрозы (подробнее об этом см. главу 10 «Варианты существенной эскалации угроз»).

251 *Об утверждении инструкции по организации антитеррористической защиты объектов питьевого водоснабжения населенных пунктов, уязвимых в террористическом отношении* (20 июля 2023 г., Казахстан). Доступно по адресу: https://adilet.zan.kz/rus/docs/V2300033119 [дата обращения: 21 июля 2025 г.] неофициальный перевод.

252 *Закон Республики Казахстан от 13 июля 1999 года № 416-ИО противодействия терроризму* (13 июля 1999 г., Казахстан). Доступно по адресу: https://online.zakon.kz/Document/?doc_id=1013957&pos=3;-106#pos=3;-106 [дата обращения: 21 июля 2025 г.] неофициальный перевод.

В большинстве систем внешнего контроля доступа доступ предоставляется сотрудникам службы безопасности объекта через централизованную диспетчерскую или автоматизированную систему. Внешние пропускные пункты могут быть оборудованы системами видеонаблюдения, металлоискателями, досмотровыми сканерами и/или средствами связи в зависимости от оцененных потребностей объекта КВИ (см. рисунок ниже).

В более критически важных или охраняемых помещениях может потребоваться использование нескольких форм контроля доступа. Например, Ассоциация банков Сингапура рекомендует использовать для этой цели ряд систем контроля доступа с двухфакторной аутентификацией.[253] Одним из примеров передовой практики является зонирование по уровням безопасности с системой управления доступом на основе ролей. Ниже приведен пример практики зонирования по уровням безопасности, применяемой в Сингапуре.[254]

Контроль доступа	Зона	Кто может получить доступ
Нет	Зоны общего пользования	Все сотрудники и общественность
Ограниченный	Зоны для посетителей	Все сотрудники и посетители, чьи имена предварительно зарегистрированы в службе безопасности
Умеренный	Общие помещения/офисы для сотрудников и т.д.	Все сотрудники
Высокий	Зоны ограниченного доступа	Авторизованные сотрудники

253 Ассоциация банков Сингапура (2018 г.), *Руководство по физической безопасности для финансовых учреждений*. Доступно по адресу: https://abs.org.sg/docs/library/abs-scps-guidelines.pdf [дата обращения: 21 июля 2025 г.].

254 Ассоциация банков Сингапура (2018 г.), *Руководство по физической безопасности для финансовых учреждений*. Доступно по адресу: https://abs.org.sg/docs/library/abs-scps-guidelines.pdf [дата обращения: 21 июля 2025 г.].

Еще одной передовой практикой является требование заблаговременного уведомления о планируемом посещении объекта КВИ, при этом количество дней, необходимых для обработки личных данных посетителей, должно быть четко указано соответствующему персоналу. Это позволяет заранее проверить личность посетителей, в том числе путем предъявления удостоверения личности с фотографией до и по прибытии. Это также ускоряет процесс входа и снижает риск нападений на посетителей, ожидающих входа за пределами периметра объекта КВИ.

Внутренний контроль доступа

После того, как лицо получило доступ на объект КВИ, применяются внутренние средства контроля доступа, гарантирующие, что доступ к различным зонам объекта получат только авторизованные лица. В Директиве НАТО по обеспечению физической безопасности более подробно описывается этот аспект:

> «Контроль доступа может осуществляться внутри объекта, на предприятии, расположенном внутри объекта, а также в зонах или помещениях внутри предприятия. Механизм контроля может быть электронным, электромеханическим или физическим. Он также может контролироваться охранником или администратором. Для контроля входа в охраняемые зоны или зоны ограниченного доступа может использоваться система пропусков или распознавания личности штатного персонала. В случаях, когда в учреждении действует система распознавания пропусков, пропуска следует носить на видном месте постоянно, чтобы обеспечить распознавание, идентификацию и проверку, если сотрудник не уверен в полномочиях лица на доступ».[255]

Все внутренние точки доступа должны быть спроектированы с учетом уровня безопасности, соответствующего секретности зоны. Как и внешние точки доступа, внутренние точки доступа должны быть дополнены другими средствами, такими как освещение, видеонаблюдение и оборудование для контроля доступа к дверям, включая надежные запирающие механизмы.

255 Крискуоло, М. (2020 г.), Директива по обеспечению физической безопасности. Документ НАТО AC/35-D/2001-REV3 (Брюссель: НАТО).

Автоматизированные электронные системы контроля доступа

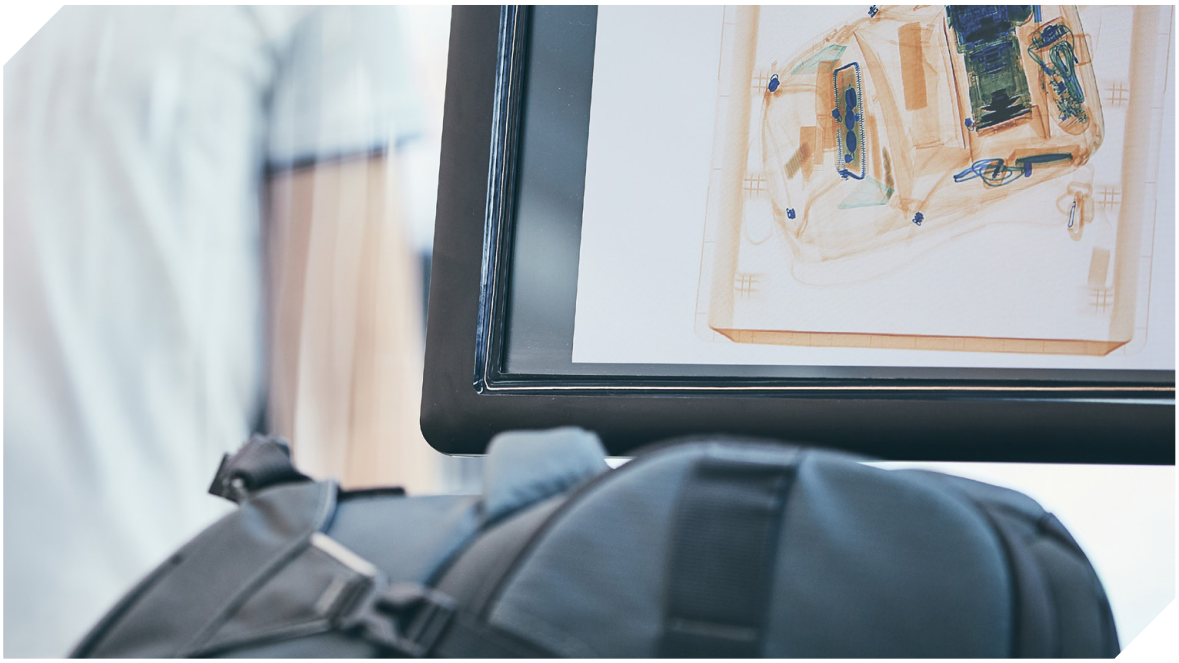
Электронные системы контроля доступа используются для обеспечения входа в контролируемую зону и выхода из нее только авторизованных лиц. Они функционируют как автоматизированная система. В таких случаях авторизованные лица аккредитуются и получают код, бейдж или другое устройство, содержащее аутентификационную информацию и распознаваемое автоматизированной системой. При использовании биометрических систем контроля доступа авторизованные лица предоставляют необходимые биометрические данные для получения доступа. Министерство внутренней безопасности США выделяет как минимум три категории автоматизированного контроля доступа, представленные в следующей таблице[256]:

Категория автоматизированного контроля доступа	Описание
Кодовые устройства	Кодовые устройства требуют от пользователя ввести известный ему код для доступа через устройство контроля доступа. Для контроля доступа в более важные зоны обычно требуются индивидуальные коды. Кодовые устройства проверяют подлинность введенного кода; устройства с электронным кодированием включают в себя электронные и управляемые компьютером клавиатуры.
Устройства управления учетными данными	Устройства управления учетными данными идентифицируют лицо, использующее учетные данные (например, имеющуюся у него пластиковую карту или ключ), которые содержат предварительно записанный код, разрешающий вход в контролируемую зону. Эти устройства аутентифицируют учетные данные только при условии, что пользователь учетных данных имеет право входа. К наиболее распространенным картам доступа относятся карты с магнитной полосой, бесконтактные карты, смарт-карты и имплантированные чипы.
Биометрические устройства	Биометрические устройства основаны на измерении одной или нескольких физических или личностных характеристик лица (его особенностей или действий). Для контроля доступа используются устройства, распознающие такие характеристики, как отпечатки пальцев, геометрия руки, голосовой отпечаток, почерк и рисунок кровеносных сосудов сетчатки глаза. Наиболее распространенными биометрическими устройствами являются устройства проверки отпечатков пальцев, сетчатки глаза, геометрии руки и устройства распознавания лиц.

256 Министерство национальной безопасности США (2011 г.), *Справочное руководство по смягчению последствий потенциальных террористических атак на здания: FEMA-426/BIPS-06/октябрь 2011 г. Издание 2.* Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

6.9 Процедуры досмотра

Строгие меры досмотра товаров и людей имеют решающее значение на входе на объект КВИ. Неавторизованные лица могут попытаться проникнуть на объект открыто, используя в своих целях законные процедуры, установленные для посетителей (включая тайный пронос оружия или взрывных устройств), или запланировать нападение удаленно, например, доставив взрывное устройство по почте.



Досмотр персонала и грузов

В докладе Европейской комиссии за 2020 год о защите периметра зданий подчеркивается важность досмотра как людей, так и грузов перед входом на объект из-за риска наличия у лица огнестрельного оружия или взрывного устройства.[257] Для критически важных объектов в докладе рекомендуется использовать полномасштабные сканеры тела для обнаружения металлических или неметаллических предметов, спрятанных на человеке, или рамочные и ручные металлоискатели. Для досмотра грузов могут использоваться рентгеновские аппараты, позволяющие сотрудникам службы безопасности визуально осматривать их содержимое с помощью программного обеспечения для обработки изображений, а детекторы взрывчатых веществ могут использоваться в качестве дополнительного инструмента для повышения общей эффективности.

Если это возможно, рекомендуется организовать отдел корреспонденции или помещение для досмотра посылок за пределами объекта. Это может снизить перебои в работе объекта КВИ в случае обнаружения подозрительного отправления. Если это невозможно и отдел корреспонденции или помещение для досмотра посылок находится на объекте КВИ, обеспечение независимой циркуляции воздуха в этом

257 Василис, К.; Ларчер, М. (2020 г.), *Рекомендации, Защита периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак*, Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

помещении от остальной части объекта КВИ поможет снизить перебои в работе в случае доставки неопознанного порошка или вещества.

Досмотр посетителей
Доступ посетителей к объектам КВИ может контролироваться с помощью бейджей, электронных турникетов или других средств. Пункты доступа посетителей должны располагаться рядом с сотрудниками службы безопасности, что обеспечит им хорошую видимость попыток обхода турникетов или других установленных средств безопасности.

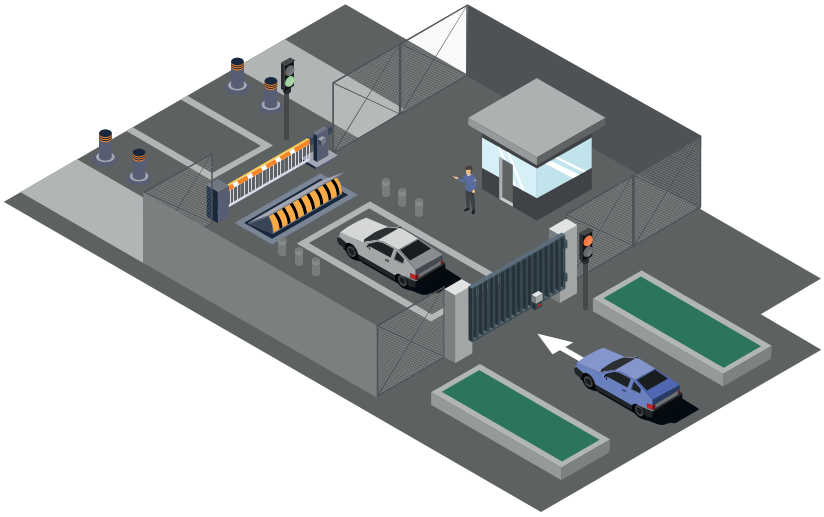
Хотя процедуры контроля посетителей на объекте КВИ могут различаться в зависимости от местных требований безопасности (т.е. посетители могут быть как сопровождаемыми, так и несопровождаемыми), необходимо поддерживать соответствующий уровень контроля за посетителями. В каждом случае к сопровождаемым и несопровождаемым посетителям должны применяться следующие минимальные требования:

- *Сопровождаемые посетители* должны постоянно сопровождаться персоналом с соответствующим уровнем авторизованного доступа. Они должны носить пропуск, который идентифицирует их как посетителя, и не должны оставаться одни на территории объекта.
- *Несопровождаемым посетителям* может быть предоставлено временное разрешение на вход на объект КВИ или его части без сопровождения. Тем не менее, посетители без сопровождения должны иметь при себе пропуск, который идентифицирует их как посетителя, и сдать его сразу по завершении своих дел на объекте.

Сотрудникам службы безопасности рекомендуется регистрировать время входа и выхода посетителей, как сопровождаемых, так и несопровождаемых, фотографировать их и хранить эту информацию в течение определенного периода времени в соответствии с местными законами и правилами защиты данных.

В рамках мероприятий по повышению осведомленности персонала объекта КВИ в вопросах безопасности следует поощрять среди персонала *культуру требования пояснений,* чтобы к любому посетителю на объекте КВИ, не носящему свой пропуск на видном месте, предъявлялись требования пояснения причины отсутствия пропуска на видном месте.

Досмотр транспортных средств
Пункты досмотра транспортных средств позволяют сотрудникам службы безопасности проверять и разрешать доступ транспортных средств на территорию КВИ, что снижает вероятность несанкционированного доступа лиц, представляющих угрозу, и их оружия. С контрольно-пропускного пункта сотрудники службы безопасности могут контролировать подъезд и направление движения транспортных средств, регулировать очереди (включая полосу для разворота) и оказывать поддержку другим сотрудникам службы безопасности.



Одним из эффективных методов безопасного управления доступом транспортных средств на территорию КВИ является контролируемый въезд с так называемыми «тигровыми ловушками» (см. рисунок выше). Они обычно используются в зонах повышенного риска и представляют собой ограждение с двумя электроприводными шлагбаумами, из которых одновременно может открываться только один. Первый шлагбаум открывается только после получения разрешения на въезд и закрывается после въезда транспортного средства. Второй шлагбаум открывается после завершения проверки компетентными сотрудниками службы безопасности и закрывается после выезда транспортного средства. Это гарантирует, что следующее транспортное средство не сможет «подъехать впритык» к идущему впереди транспортному средству и проникнуть на территорию без проверки.

6.10 Зоны ограниченного доступа

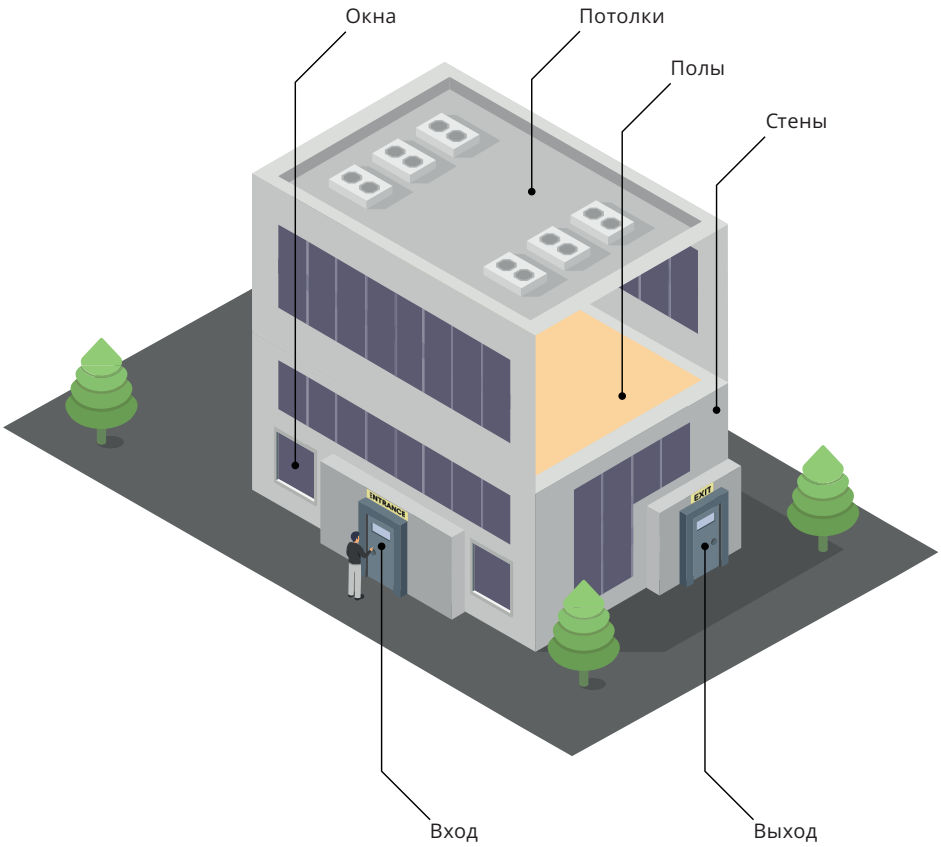
В дополнение к общей системе безопасности периметра объекта КВИ и системе контроля доступа, любой объект КВИ, вероятно, имеет также зоны с повышенным уровнем ограничений, доступ к которым дополнительно ограничен и разрешен только уполномоченному персоналу. Зоны ограниченного доступа обычно используются для обеспечения безопасности или сохранности ценного имущества или материалов, размещения средств управления системой охранного видеонаблюдения или других средств безопасности. Однако это может быть любое пространство, обозначенное владельцами/операторами КВИ. Такие зоны требуют дополнительной защиты, поскольку они могут стать целью террористов, если они преодолеют периметр объекта КВИ и другие эшелоны защиты. Дополнительные меры защиты включают в себя, помимо прочего, следующее:

- ограничение количества входов и выходов до необходимого минимума;
- минимизация количества дверей, поскольку двери, как правило, менее прочны, чем конструкция здания, что делает их менее устойчивыми к атакам;
- запрет доступа для всех внешних транспортных средств и использование специального парка транспортных средств;
- установка дверей, открывающихся наружу, так как они более прочны и лучше защищены от внешних атак.

Предупреждающие знаки с надписью «Зона ограниченного доступа» или другой аналогичной надписью также должны быть размещены на границе каждой зоны ограниченного доступа, чтобы их могли легко прочитать люди, приближающиеся пешком или на транспортном средстве.

6.11 Конструкция здания

На объекте КВИ конструкция и целостность здания имеют основополагающее значение для физической безопасности защиты объекта от различных угроз и опасностей, включая террористические атаки. Это важно как с точки зрения проектных решений, так и с точки зрения строительных материалов, чтобы исключить возможность использования уязвимостей.



Входы и выходы

Двери являются важнейшим элементом физической безопасности объекта. Как указано в рекомендациях Национального управления по защите и безопасности Великобритании, двери выполняют ряд ключевых функций, в том числе:

- контроль санкционированного доступа и предотвращение несанкционированного доступа;
- содействие потоку людей без создания узких мест для доступа;
- обеспечение защиты от взрывной волны или баллистических угроз (при использовании дверей повышенной безопасности);
- защита от проникновения огня и/или дыма;
- создание барьера, задерживающего продвижение злоумышленника;

- обеспечение возможности эвакуации в чрезвычайной ситуации (например, в ситуациях с активным применением огнестрельного оружия).[258]

Двери, ведущие наружу здания, должны быть оснащены надежными замками, но при этом должны легко открываться в случае эвакуации. Все двери и фасады должны быть устойчивы к физическому воздействию. В особых случаях может быть установлено пуленепробиваемое остекление для предотвращения определенных угроз. Независимо от способа защиты дверей, они должны соответствовать действующим нормам пожарной безопасности.

Министерство внутренних дел Сингапура разработало дополнительные указания: «Внешние двери должны открываться наружу, в сторону возможной угрозы. В этом случае дверная рама может защитить дверь от взлома или взрывной волны снаружи. Однако в этом случае петли должны быть укреплены от взлома, поскольку они будут расположены снаружи здания. Точки крепления рамы к стене должны быть укреплены на том же уровне, что и дверь».[259]

Стены, потолки и полы

Стены – это физические барьеры, отделяющие одну часть здания от другой (или внутреннюю часть здания от внешней). Они играют важную роль в общей физической безопасности здания. Внешняя часть всех зданий на объекте КВИ должна быть защищена от несанкционированного доступа, особенно в случаях отсутствия окружающего периметра/забора или в случае повреждения забора. В руководстве Министерства энергетики США подчеркивается, что стены, полы и потолки по периметру «должны иметь капитальную конструкцию и быть соединены друг с другом», и что «все строительные работы должны быть выполнены таким образом, чтобы обеспечить визуальное подтверждение несанкционированного проникновения».[260]

Прочные, укрепленные стены защищают от взрывов, огня из стрелкового оружия, проникновения с применением силы и других угроз безопасности. Владельцы/операторы КВИ также могут рассмотреть возможность установки взрывозащитной стены или усиления стеклянных фасадов и конструкций в определенных частях соответствующих зданий в зависимости от угроз, которым они подвергаются.

Если в здание можно попасть через стену, можно установить систему обнаружения вторжений, чтобы исключить возможность проникновения нарушителя незамеченным.

Потолки и полы должны быть изготовлены из материалов, обеспечивающих стойкость к проникновению, чтобы задержать несанкционированное проникновение в здание и обеспечить наличие доказательств попыток несанкционированного проникновения (например, следов применения силы или повреждений потолка или конструкции пола).

258 Национальное управление по защите и безопасности Великобритании (2021 г.), Безопасность дверей. Доступно по адресу: https://www.npsa.gov.uk/door-security [дата обращения: 3 марта 2024 г.].

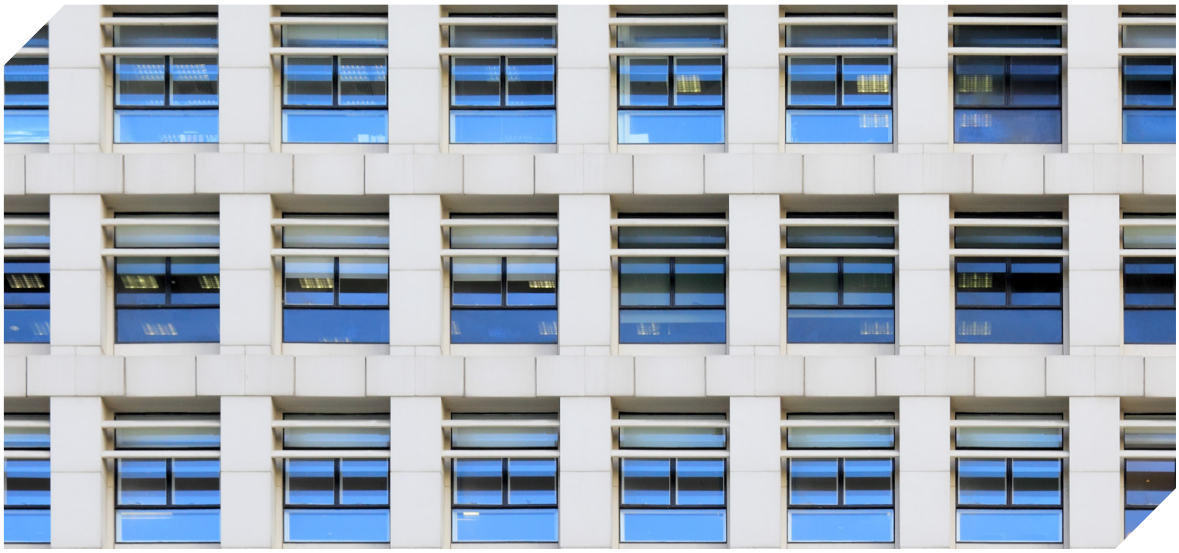
259 Совместная оперативная группа — Министерство внутренних дел (без даты), *Рекомендации по повышению безопасности зданий в Сингапуре*. Доступно по адресу: https://www.police.gov.sg/Advisories/Infrastructure-Protection/Building-Security [дата обращения: 21 июля 2025 г.].

260 Министерство энергетики США (2021 г.), Программа физической защиты, DOE O 473.1A, Приложение 2: Базовые требования к физической защите. Доступно по адресу: https://www.directives.doe.gov/directives-documents/400-series/0473.1-BOrder-a/@@images/file [дата обращения: 21 июля 2025 г.].

Окна

Окна представляют собой более легкую возможность проникновения на объект, чем двери или стены, поскольку они зачастую не обладают тем же уровнем физической прочности. Поэтому окнам необходимы интегрированные функции безопасности:

- Окна должны обеспечивать защиту от несанкционированного проникновения и фиксировать факт несанкционированного проникновения.
- Оконные рамы должны быть надежно закреплены в стенах, а окна должны быть заперты изнутри или установлены в неподвижные рамы, что исключает возможность выноса оконных стекол снаружи.
- Если визуальный доступ является фактором, определяющим возможность визуального контроля, следует использовать визуальные барьеры. Например, все окна, через которые можно визуально наблюдать за секретной деятельностью, должны быть непрозрачными или снабжены жалюзи, шторами или другими покрытиями.



При оценке защищенности окна от вооруженного проникновения или нападения с использованием взрывчатых веществ необходимо оценить всю оконную систему (а не только остекление) для обеспечения ее надежности.[261]

Окна на уровне земли или другие легкодоступные окна должны быть изготовлены из материалов, обеспечивающих защиту от взлома. Уровень защиты окон должен соответствовать прочности прилегающих к ним стен, а также прочности крепления окон к стене, которое должно выдерживать такую же прилагаемую силу.

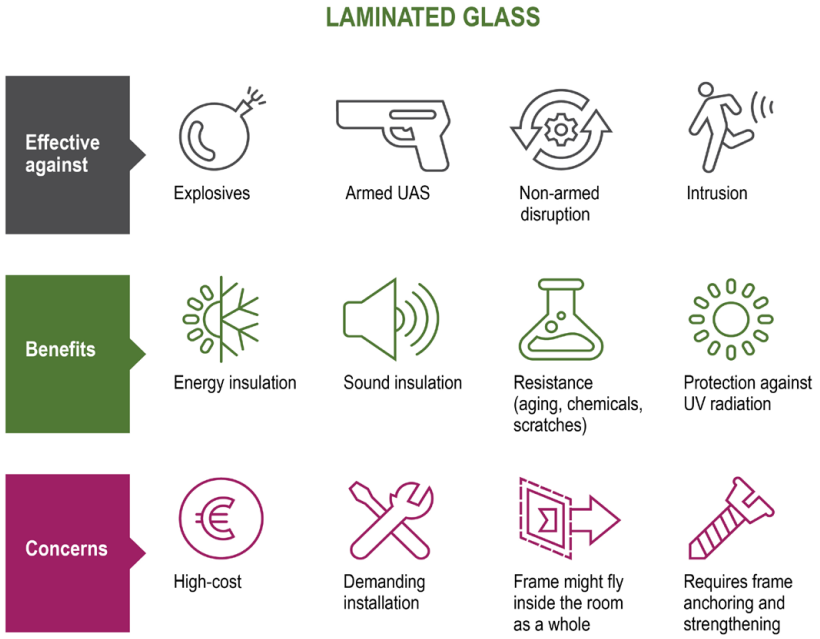
Окна: остекление

Помимо того, что окна облегчают проникновение злоумышленника, они также представляют угрозу безопасности в случае нападения с использованием взрывчатых веществ. По данным Министерства обороны США, «[в] прошлых инцидентах с использованием взрывчатых веществ, когда здания не обрушивались, большое количество травм было вызвано разлетающимися осколками стекла и обломками

261 ДОБ (без даты), *Защита окон от взрыва*. Доступно по адресу: https://www.unicef.org/jordan/media/5951/file/LRFP-2021-9166373-Annex_4-Blast_Protection_for_Windows.pdf [дата обращения: 21 июля 2025 г.].

стен, потолков и арматуры (неконструктивными элементами)».[262] По данным Департамента ООН по вопросам охраны и безопасности (ДОБ), до 80 процентов жертв крупных терактов с подрывом взрывного устройства погибают или получают ранения из-за осколков стекла.[263] При оценке расположения окон на предмет уязвимости для подрыва взрывного устройства ДОБ отмечает, что чем меньше остекление, тем ниже риск попадания осколков в случае взрыва.[264] Испытание окон на взрывостойкость регламентируются стандартом ISO 16933:2007 «Стекло в строительстве: взрывостойкое безопасное остекление».[265]

Существует несколько основных типов остекления, которые обычно используются в системах защитного остекления: термически упрочненное стекло, полностью термически закаленное стекло и многослойное стекло. Все они обладают разной степенью устойчивости к разрушению при взрыве. Поэтому владельцам/операторам КВИ и компетентным органам следует выбирать их исходя из потребностей и оценки рисков.



Эффективность и особенности использования многослойного стекла против атак с использованием БАС. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[266]

262 Министерство обороны США (2018 г.), *Единые критерии объектов (UFC): Минимальные антитеррористические стандарты Министерства обороны для зданий,* стр. 18. Доступно по адресу: https://www.wbdg.org/FFC/DOD/UFC/ARCHIVES/ufc_4_010_01_2018_c1.pdf [дата обращения: 21 июля 2025 г.].

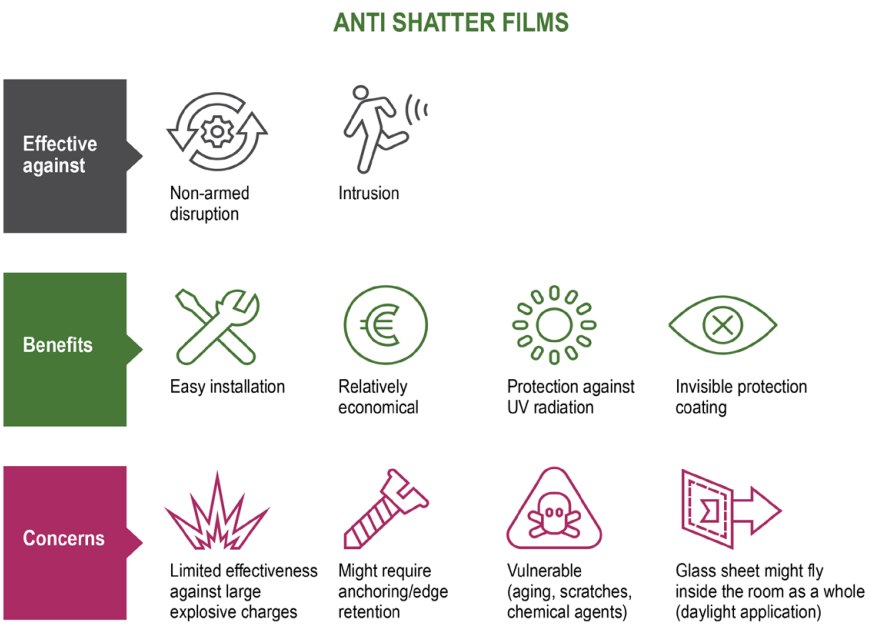
263 ДОБ (без даты), *Защита окон от взрыва.* Доступно по адресу: https://www.unicef.org/jordan/media/5951/file/LRFP-2021-9166373-Annex_4-Blast_Protection_for_Windows.pdf [дата обращения: 21 июля 2025 г.].

264 ДОБ (без даты), *Защита окон от взрыва.* Доступно по адресу: https://www.unicef.org/jordan/media/5951/file/LRFP-2021-9166373-Annex_4-Blast_Protection_for_Windows.pdf [дата обращения: 21 июля 2025 г.].

265 ISO (2007 г.), Стекло в строительстве — Взрывостойкое безопасное остекление — Испытания и классификация при полигонных испытаниях на устойчивость к действию воздушной ударной волны (испытания «арена») (Стандарт ISO № 16933:2007). Доступно по адресу: https://www.iso.org/standard/38166.html [дата обращения: 16 мая 2025 г.]. Для получения дополнительной информации о различных типах остекления и стандартах окон см., например, Европейская справочная сеть по защите критически важной инфраструктуры (2014 г.), *Сравнение существующих стандартов для испытания взрывостойкого остекления и окон.* Доступно по адресу: https://erncip-project.jrc.ec.europa.eu/sites/default/files/ReqNo_JRC94930_A%20comparison%20of%20existing%20standards%20for%20testing%20blast%20resistant%20glazing%20and%20windows.pdf [дата обращения: 21 июля 2025 г.].

266 Объединенный исследовательский центр Европейской комиссии (2023 г.), *Защита от беспилотных авиационных систем: Справочник по оценке риска БАС и принципам физического укрепления зданий и объектов.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC132967 [дата обращения: 21 июля 2025 г.].

Хотя для остекления чаще всего используют отожженное и термически упрочненное стекло, любой тип остекления можно покрыть противоосколочной пленкой, чтобы снизить риск разлета осколков стекла и, таким образом, снизить риск получения травм.



Эффективность и особенности использования противоосколочной пленки против атак с использованием БАС. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[267]

Окна: пуленепробиваемое стекло

Обычное пуленепробиваемое стекло изготавливается путем ламинирования слоев стекла поливинилбутиралем. В некоторых случаях пули останавливаются стеклом, но осколки могут разлетаться. Хотя они вряд ли нанесут серьезную травму, они все же могут повредить глаза или кожу. Поэтому может потребоваться более толстое стекло.

Для идентификации изделий, которые достигают соответствующих уровней пулестойкости, следует обратиться к европейскому стандарту (EN) 1522:2000, который устанавливает требования к пулестойкости и классификацию окон, дверей, ставней и жалюзи.

Взрывозащитные шторы

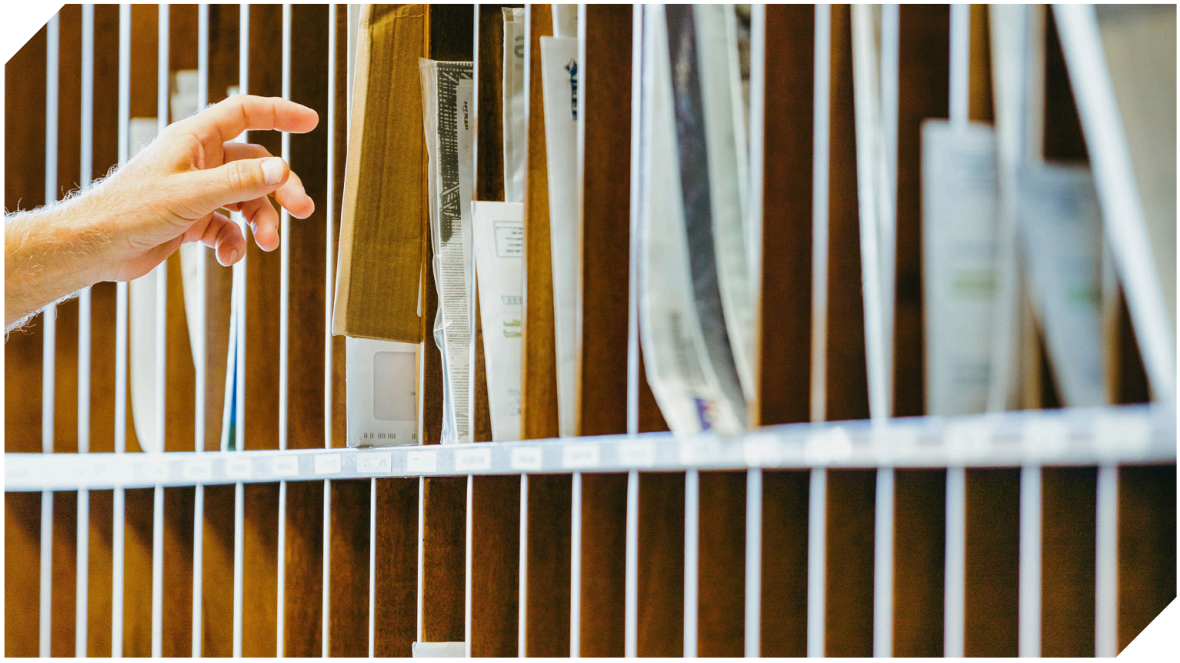
Для объектов, которые считаются подверженными повышенному риску террористических атак, или для окон объектов, которые оцениваются как более подверженные взрывоопасным событиям (например, окна, выходящие на улицу), следует рассмотреть дополнительные меры по предотвращению разлета осколков стекла или других обломков в случае взрыва. Одним из решений является установка взрывозащитных штор. По данным Объединенного исследовательского центра Европейской комиссии, основная цель таких мер – «уловить разлетающиеся осколки, образующиеся при разрушении окон в результате распространения взрывной волны,

267 Объединенный исследовательский центр Европейской комиссии (2023 г.), *Защита от беспилотных авиационных систем: Справочник по оценке риска БАС и принципам физического укрепления зданий и объектов.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC132967 [дата обращения: 21 июля 2025 г.].

и обычно они устанавливаются за фасадом здания».[268] Хотя все еще сохраняется возможность попадания осколков внутрь помещения и причинения травм, взрывозащитная штора значительно сокращает дальность разлета фрагментов.

Взрывозащитные шторы могут быть изготовлены из полиэфирных материалов или стали. Каждый материал по-разному ведет себя во время взрыва и более или менее эффективно улавливает осколки стекла. Поэтому необходимо провести соответствующие испытания и выбрать материал на основе оценки риска для конкретного окна. Взрывозащитные шторы могут использоваться как самостоятельная мера, так и в сочетании с противоосколочными пленками или многослойными защитными стеклами.[269]

Отделы корреспонденции



Отделы корреспонденции могут представлять собой значительную уязвимость объекта КВИ, если они неудачно расположены или некачественно построены и спроектированы для предотвращения потенциальных угроз, связанных, например, с СВУ, доставляемыми по почте. Следует учитывать расположение отделов корреспонденции для вновь строящихся объектов КВИ, отдавая предпочтение их размещению вблизи периметра объекта КВИ, чтобы избежать транспортировки СВУ, доставляемых по почте, через объект КВИ для последующей обработки в отделе корреспонденции.[270] Для существующих объектов КВИ со стационарными отделами корреспонденции,

268 Василис, К.; Ларчер, М. (2020 г.), *Рекомендации, Защита периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак,* Бюро публикаций Европейского Союза, стр. 45. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

269 Василис, К.; Ларчер, М. (2020 г.), *Рекомендации, Защита периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак*, Бюро публикаций Европейского Союза, стр. 45. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

270 Министерство обороны США (2018 г.), *Единые критерии объектов (UFC): Минимальные антитеррористические стандарты Министерства обороны для зданий*, стр. 27. Доступно по адресу: https://www.wbdg.org/FFC/DOD/UFC/ARCHIVES/ufc_4_010_01_2018_c1.pdf [дата обращения: 21 июля 2025 г.].

расположенными не вблизи периметра здания, следует принять меры для обеспечения надлежащего уровня взрывобезопасности помещения и отдельной системы вентиляции на случай химической или биологической атаки. Эти положения подробно разъяснены в следующих рекомендациях Ассоциации банков Сингапура:

> «Если помещения отделов корреспонденции не спроектированы и не расположены должным образом, они могут представлять угрозу зданию и его обитателям при использовании почты в качестве средства химической, биологической, радиологической атаки или атаки с использованием взрывчатых веществ (ХБРВ). В идеале отделы корреспонденции должны располагаться рядом со входом в здание или в отдельной части здания вдали от критически важных зон и ключевых конструктивных элементов здания. Для предотвращения угроз, передающихся по воздуху, отделы корреспонденции также должны быть оборудованы отдельной/независимой системой кондиционирования воздуха или вентиляции с учетом особенностей конструкции и затрат. Зона проверки входящей почты и посылок должна быть спроектирована таким образом, чтобы минимизировать последствия взрыва».

> «Поскольку отделы корреспонденции являются зонами повышенного риска, они должны быть оборудованы надлежащими средствами обеспечения безопасности, такими как системы видеонаблюдения и контроля доступа к дверям. Кроме того, доступ в отделы корреспонденции должен быть ограничен только уполномоченным персоналом. В некоторых случаях объекты критически важной инфраструктуры могут не иметь собственного отдела корреспонденции и могут получать почту от сторонних поставщиков услуг или курьерских служб. Эти поставщики и курьерские службы могут подвергаться такому же уровню угрозы от входящей почты, и любое соответствующее обучение по вопросам безопасности взаимодействующего с почтой персонала должно быть частью упреждающих действий для выявления и обнаружения таких угроз для последующей эскалации мер и реагирования».[271]

Персонал, обрабатывающий почту на объекте КВИ, должен быть обучен процедурам работы с почтой, включая соответствующие действия в случае получения подозрительных писем или посылок. Такое обучение должно включать в себя регулярную актуализацию знаний и навыков, чтобы сотрудники были осведомлены о текущих методах действий субъектов угрозы. Для этого может потребоваться тесное сотрудничество и взаимодействие с местными и национальными правоохранительными органами и другими службами безопасности.

Также должна быть разработана организационная политика для объекта, позволяющая принимать различные ответные меры как внутри объекта КВИ (включая отчеты для служб безопасности объекта КВИ), так и за его пределами (например, контакты с правоохранительными органами или подразделениями по обезвреживанию взрывных устройств).

271 Ассоциация банков Сингапура (2018 г.), *Руководство по физической безопасности для финансовых учреждений.* Доступно по адресу: https://abs.org.sg/docs/library/abs-scps-guidelines.pdf [дата обращения: 21 июля 2025 г.].

7 Планирование безопасности и укрепление объекта

«Для снижения риска, связанного с различными видами террористических атак, необходимы общие меры физической безопасности, подобные тем, что описаны в предыдущих главах, а также конкретные планы и шаги. В данной главе представлены рекомендации по таким планам и действиям.»

7 Планирование безопасности и укрепление объекта

Объекты КВИ сталкиваются с различными угрозами со стороны субъектов угроз, включая террористов. Субъекты угроз могут быть терпеливыми, гибкими и, в некоторых случаях, хорошо обеспеченными ресурсами. Если они решат атаковать объект КВИ, учитывая вероятность серьезных последствий, они, вероятно, тщательно спланируют свою атаку. Чтобы понять угрозы, исходящие от субъектов угроз, владелец/оператор КВИ должен сначала оценить окружающую среду угроз, а затем риск(и) для рассматриваемого объекта (подробнее см. главу 5 «Угроза терроризма и оценка рисков»). Этот процесс позволит глубже понять уязвимости объектов КВИ, а также определить вероятные сценарии угроз, с учетом которых можно будет подготовить план действий. Хотя многие субъекты угроз могут иметь схожие намерения (например, повредить объект КВИ или снизить его работоспособность), их возможности могут существенно различаться. Некоторые из них в состоянии проводить сложные и скоординированные атаки с использованием современного оружия, в то время как другие могут осуществлять только более простые атаки, например, с использованием транспортных средств. Для снижения риска, связанного с каждым типом атак, необходимо принять общие меры обеспечения физической безопасности, подобные тем, что описаны в предыдущей главе, а также разработать планы и конкретные действия для различных типов атак. В данной главе представлены рекомендации по таким планам и действиям.

В данной главе сначала будет рассмотрен вопрос подготовки террористических организаций к атакам, с акцентом на их разведывательные действия. Затем будут рассмотрены различные типы террористических атак, включая использование транспортных средств, взрывчатых веществ, ХБР материалов, огнестрельного оружия и захват заложников, а также меры, которые владельцы/операторы КВИ могут предпринять для соответствующей подготовки своих объектов. В заключение главы рассматриваются практические методы эвакуации, укрытия и изоляции персонала, необходимые в кризисных ситуациях. Также будет подчеркнута важность внедрения системы управления непрерывностью деятельности и системы кризисных коммуникаций.

7.1 Планирование террористической атаки посредством разведывательной деятельности

Хотя последовательность действий не является строгой, существуют общие этапы, которые террорист должен пройти для успешного осуществления атаки. Эти этапы включают в себя ряд мероприятий по планированию и подготовке, особенно в случаях, когда цель хорошо укреплена (например, объект КВИ) или когда будет использоваться сложная методология атаки.[272] Существует множество различных концепций цикла планирования террористической атаки, при этом все они, как правило, решают следующие ключевые задачи (не обязательно в указанном порядке):

- Поиск необходимых материалов и средств (вооружение, финансы, люди и т.д.);
- Определение потенциальных целей;
- Сбор информации о потенциальных целях для планирования атак и выявления уязвимостей, которые можно использовать (как онлайн, так и оффлайн);
- Выбор цели;
- Определение методологии атаки;
- Осуществление атаки (включая варианты отступления, если это не атака смертника);
- Определение возможностей для освещения в прессе и пропаганды после атаки.

Как показано выше, существует множество задач, предшествующих атаке, для решения которых злоумышленнику потребуется информация, касающаяся непосредственно предполагаемой цели или целей. В таких случаях ему может потребоваться провести разведывательные операции. Разведывательная деятельность, как правило, включает в себя действия, предпринимаемые злоумышленником для получения информации в рамках подготовительной фазы атаки на определенную цель. В случае атаки на объект КВИ тип информации, которую злоумышленник может захотеть получить посредством собственных разведывательных действий, может включать, *среди прочего*, следующее:

272 Смит, Б. Л.; Дамфусс, К. Р.; Пакстон, Р. (2006 г.), *Предварительные показатели террористических инцидентов: идентификация поведенческих, географических и временных моделей поведения при подготовке,* стр. 7 (Вашингтон, округ Колумбия: Национальный институт юстиции, Министерство юстиции). Доступно по адресу: https://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf [дата обращения: 21 июля 2025 г.].

- Информация, касающаяся конкретного объекта (например, схемы движения пешеходов и транспорта, точки входа и выхода, полученные с помощью фотографий/видео, поэтажных планов, планов обеспечения безопасности, планов эвакуации);
- Информация о безопасности (например, применяемые меры безопасности, местоположение сотрудников службы безопасности, процедуры въезда, графи и порядок патрулирования);
- Установление полномочий персонала или транспортных средств (например, через изображения на веб-сайтах, в социальных сетях);
- Корпоративная информация (например, организационные структуры, контактные данные персонала, местоположение офисов);
- Информация о планировании (например, планы нового строительства/расширения, меры по модернизации систем безопасности и т.д.).

В процессе осуществления этих разведывательных действий злоумышленник стремится проверить уже собранную информацию о потенциальной цели, собрать новую информацию, исключить цели из своего списка и, в конечном итоге, определить окончательную цель. Разведывательные действия злоумышленников на объекте КВИ могут проводиться на месте или виртуально. Виртуальные действия могут включать в себя посещение веб-сайта объекта КВИ для получения информации о его периметре, физических мерах безопасности или процессе входа и аккредитации. Они также могут включать в себя выявление критически важных служб за пределами периметра объекта КВИ, таких как электрические подстанции, линии электропередач и трубопроводы, которые могут быть более уязвимы для атак, чем сам объект КВИ. Разведывательные действия, проводимые на месте, предоставляют злоумышленнику возможность непосредственного ознакомления с внешними мерами безопасности (например, постами охраны и патрулями) или контрмерами (например, проверкой удостоверений личности или сумок), что может помочь ему определить осуществимость атаки на рассматриваемую цель (или цели).[273]

Разведывательная деятельность злоумышленников может включать в себя видео- или фотосъемку объекта или ведение заметок. В некоторых случаях злоумышленник может расспрашивать персонал объекта КВИ о мерах безопасности, применяемых на объекте, или даже проверять меры безопасности, оставляя подозрительные предметы без присмотра, пытаясь пронести запрещенные предметы на территорию или паркуясь в запрещенных зонах. Злоумышленник также может проводить репетицию атаки. Такая репетиция может включать в себя прохождение через точки входа и выхода, транспортировку предметов, которые имитируют оружие или бомбы, или отработку времени и последовательности событий. Репетиция атаки, скорее всего, будет проводиться для атаки на слабозащищенную цель или место общественного пользования. Однако возможно, что злоумышленник может захотеть провести репетицию на объекте КВИ, даже если это осуществимо лишь частично (например, репетиция атаки вплоть до точки входа на объект).

273 Паундер, Д. (2018 г.), «Взгляд: цикл атак враждебных событий начинается с выбора цели и наблюдения», Homeland Security Today [веб-страница]. Доступно по адресу: https://www.hstoday.us/subject-matter-areas/counterterrorism/perspective-picking-target-surveillance-begins-the-hostile-events-attack-cycle [дата обращения: 10 декабря 2024 г.].

В ходе проведения разведывательной деятельности злоумышленники могут стать уязвимыми для обнаружения службами безопасности или владельцами/операторами КВИ. Например, они могут непреднамеренно раскрыть информацию о своих потенциальных намерениях или выборе цели, осуществляя поиск информации в Интернете, лично посещая предполагаемую цель или задавая вопросы персоналу объекта. Поэтому крайне важно, чтобы владельцы/операторы КВИ повышали осведомленность персонала объекта о разведывательной деятельности злоумышленников как о явлении, предшествующем атаке, и обеспечивали наличие адекватных механизмов для передачи сообщений и информации соответствующим координаторам по вопросам безопасности.

Обнаружение разведывательной деятельности и подозрительной активности злоумышленников

Учитывая, что разведывательные действия являются ключевой задачей, которую большинство злоумышленников, включая террористов, выполняют перед совершением террористической атаки, крайне важно обеспечить наличие мер по обнаружению такой деятельности на объекте КВИ. Разведывательные действия редко удается распознать как таковые в момент их проведения. Более вероятно их выявить по многочисленным подозрительным, необычным или несоответствующим обстоятельствам инцидентам, происходящим в течение определенного периода времени. При анализе компетентными сотрудниками службы безопасности эти инциденты могут быть расценены как часть разведывательной кампании, проводимой злоумышленником. Таким образом, выявление подозрительной деятельности напрямую связано с обнаружением разведывательных действий злоумышленников.

Для выявления подозрительной активности, которая может представлять собой разведывательные действия злоумышленников, владелец/оператор КВИ может рассмотреть возможность внедрения целевой многогранной программы, позволяющей персоналу объекта КВИ выявлять подозрительную деятельность и сообщать о ней. В свою очередь, компетентные сотрудники службы безопасности могут реагировать по мере необходимости. В некоторых случаях это может быть частью более масштабной программы, направленной на формирование *культуры безопасности* среди персонала объекта КВИ.

Практика: Руководство Международной организации гражданской авиации по формированию культуры безопасности (2022 г.)[274]

«Культура безопасности – это организационная культура, способствующая оптимальному обеспечению безопасности. Культура безопасности обычно понимается это набор связанных с безопасностью норм, ценностей, взглядов и предположений, которые присущи повседневной работе организации и отражаются в действиях и поведении всех подразделений и персонала внутри организации. Культуру безопасности нельзя рассматривать изолированно от организационной культуры в целом».

274 Международная организация гражданской авиации (ИКАО) (2022 г.), Материалы руководства ИКАО по культуре безопасности. Доступно по адресу: https://www.icao.int/Security/Security-Culture/Documents/ICAO%20-%20Security%20Culture%20Guidance%20Material.pdf [дата обращения: 21 июля 2025 г.].

«Для формирования или повышения культуры безопасности в организациях следует разработать меры по укреплению этих норм, убеждений, ценностей, установок и предположений. Эти меры должны быть направлены на продвижение следующих принципов:

1. постоянное повышение уровня безопасности, признавая, что культура безопасности в организации является важнейшим компонентом эффективного, упреждающего и реактивного режима безопасности, который поддерживает и сохраняет устойчивую к рискам структуру, помогающую эффективно управлять как внутренними, так и внешними рисками;
2. поощрение осведомленности и бдительности в отношении рисков безопасности со стороны всего персонала и той роли, которую они лично играют в выявлении, устранении или снижении этих рисков;
3. поощрение ознакомления с вопросами безопасности, процедурами и механизмами реагирования (например, кому звонить или о каких процессах сообщать в случае подозрительной активности);
4. признание важности безопасности на всех уровнях организации, включая руководство, и отражение этого посредством наблюдения и участия во всех мерах безопасности;
5. предоставление необходимого времени и приложение необходимых усилий для соблюдения мер безопасности даже в стрессовой ситуации;
6. поощрение готовности брать на себя ответственность, проявлять инициативу и самостоятельно принимать решения в случае возникновения проблем безопасности, включая инциденты, недостатки и нарушения;
7. подвергать критике действия других сотрудников в случае нарушений и допускать критику в свой адрес (т.е. поощрять высказывание мнения, признавать различные точки зрения);
8. немедленно сообщать о происшествиях или любых подозрительных в плане безопасности действиях – независимо от того, кто совершает указанные действия;
9. развитие критического мышления в отношении авиационной безопасности и интереса к выявлению потенциальных источников уязвимости безопасности, отклонений от применимых процедур и решений; и
10. надлежащее обращение с конфиденциальной информацией, касающейся авиационной безопасности».

Источник: Международная организация гражданской авиации

Ключевые соображения относительно программы владельца/оператора КВИ, направленной на обнаружение разведывательных действий злоумышленников и подозрительной активности, включают в себя:

- Выявление подозрительной активности;
- Сообщение о подозрительной активности;
- Анализ информации для выявления закономерностей и других важных сведений;
- Предоставление информации соответствующим заинтересованным сторонам.

Выявление подозрительной активности: Персонал объекта КВИ должен иметь надлежащую подготовку, чтобы отслеживать окружающую обстановку на предмет подозрительной активности и, при необходимости, немедленно сообщать о ней соответствующему координатору по безопасности. Такая подготовка может включать в себя обучение методам поведенческого анализа для выявления лиц с враждебными намерениями путем наблюдения за их поведением и действиями.[275] Меры по повышению уровня осведомленности персонала объекта КВИ в вопросах безопасности могут включать в себя проведение инструктажей по угрозам для более широкого круга сотрудников и распространение материалов о субъектах угроз и общепринятых методах действий. Инструктажи важны для того, чтобы помочь персоналу распознавать модели поведения и формировать целостное представление о спектре возможных подозрительных действий.

Национальная практика: рекомендации Федерального управления гражданской авиации Швейцарии по разработке кампаний по повышению осведомленности с целью укрепления культуры безопасности в секторе гражданской авиации (2020 г.)[276]

- «Кампания по повышению осведомленности является одним из возможных способов обеспечить знание или понимание культуры безопасности или ее элементов. Для того чтобы кампания была плодотворной, она должна быть конкретной, эффективной и целенаправленной. Кампания должна не только информировать об угрозах и рисках, но и обеспечивать понимание ее содержания теми, кому она адресована, и мотивацию к достижению поставленных целей.
- Еще одним важным фактором является способ коммуникации. Коммуникация, направленная на создание атмосферы страха или запугивание, часто контрпродуктивна, поскольку она скорее напугает в тех, к кому она адресована, чем мотивирует их. Риски в идеале следует представлять на примерах из практики, а информация, как правило, должна быть простой и краткой.
- Кампания должна сопровождаться соответствующими сопутствующими мерами. Среди прочего, это могут быть плакаты и листовки, электронные рассылки или специальные мероприятия, такие как тематические или целевые встречи.
- Также полезно установить эмоциональную связь с кампанией. Это можно сделать, например, с помощью брендинга. Использование впечатляющего названия бренда и/или логотипа создает положительные эмоции, мотивацию и доверие».

Источник: Федеральное управление гражданской авиации Швейцарии

275 Национальное управление по защите и безопасности Великобритании (27 февраля 2023 г.), Поведенческое выявление [веб-страница]. Доступно по адресу: https://www.npsa.gov.uk/behavioural-detection-0 [дата обращения: 10 декабря 2024 г.].

276 Швейцарское федеральное управление гражданской авиации (2020 г.), *Культура безопасности: Руководство по развитию и расширению культуры безопасности и потенциальной кампании по повышению осведомленности.* Доступно по адресу: https://www.icao.int/Security/Security-Culture/Documents/Switzerland%20FOCA%20-%20Guidance%20on%20development%20and%20expansion%20of%20SC%20and%20awareness%20raising.pdf [дата обращения: 21 июля 2025 г.].

Помимо повышения осведомленности, персонал также должен быть уполномочен выявлять подозрительную активность и сообщать о ней координатору по безопасности на объекте. Сообщая о подозрительной активности, персонал должен понимать, какие ключевые сведения будут полезны для последующих действий, например:

- что было ненормальным/подозрительным/необычным в поведении лица/лиц;
- откуда лицо/лица прибыли и куда ушли после обнаружения подозрительной активности;
- количество подозрительных лиц;
- подробное описание лица/лиц, например, пол, возраст, рост, вес, стрижка/ цвет волос, шрамы, татуировки и этническая принадлежность;
- описание одежды подозрительных лиц;
- описание предметов, находящихся при лице/лицах (применимо);
- описание транспортного средства (тип транспортного средства, цвет, отличительные черты, регистрационный номер, местонахождение) (если применимо);
- реакция лица/лиц на вопросы (если применимо).

Персоналу объекта КВИ (включая персонал службы безопасности) следует рекомендовать обращаться к незнакомым лицам на территории объекта, если их поведение кажется подозрительным, вежливо спрашивать о причинах их присутствия и задавать открытые вопросы, например: «Могу ли я вам помочь?» или «К кому вы сегодня идете?». Это демонстрирует, что персонал объекта не только умеет замечать незнакомые лица, но и способен реагировать на необычную активность. Однако обращаться к незнакомым лицам следует с осторожностью и только при отсутствии непосредственной или очевидной угрозы. Если опасения персонала объекта не будут развеяны в результате этих действий, он должен следовать процедуре уведомления о подозрительной активности.

Важно, чтобы весь персонал также знал местные законы. Например, сотрудники службы безопасности объекта КВИ не всегда имеют законные полномочия конфисковать камеру у подозрительного лица, запретить ему фотографировать или потребовать удалить фотографии.

Сообщение о подозрительной активности: Если сотрудники объекта КВИ остались не удовлетворены после обращения к неизвестному лицу на территории или вблизи объекта, или они не чувствуют себя в безопасности, они должны по поручению руководства владельца/оператора КВИ обратиться к координатору по безопасности и сообщить ему ключевые сведения о неизвестном лице. Для координатора по безопасности также должна быть предусмотрена четкая процедура составления отчета об инциденте после получения уведомления от персонала. Отчет о подозрительной активности должен содержать перечисленные выше ключевые сведения и должен быть составлен координатором по безопасности как можно скорее, чтобы обеспечить актуальность и точность этих сведений.

Эффективная программа такого рода может также предусматривать сбор всех сообщений о подозрительной активности (включая любые соответствующие изображения и другую информацию) в едином хранилище для последующего использования. Это позволяет создать «институциональную память» (включая

извлеченные уроки) и провести дальнейший анализ. При работе с персональными данными необходимо соблюдать местные и национальные законы, а также международные стандарты. Подробнее об этом см. в главе 3 «Соображения в области прав человека».

Анализ информации для выявления закономерностей и других важных сведений: Координатор по вопросам безопасности объекта КВИ должен иметь общее представление о подозрительной активности на объекте или связанной с объектом за определенный период времени. Эту информацию следует регулярно анализировать для выявления закономерностей в инцидентах подозрительной активности, определения масштабом подозрительной активности на данном объекте и установления любых связей с реальной угрозой.

Предоставление информации соответствующим заинтересованным сторонам: Информация о подозрительной активности также должна предоставляться соответствующим заинтересованным сторонам в сфере безопасности. Решение о том, кто должен иметь доступ к этой информации, может приниматься отдельными владельцами/операторами КВИ, предписываться государственными регулирующими органами или определяться специальными соглашениями между владельцами/операторами КВИ и государственными заинтересованными сторонами.

Меры реагирования на разведывательную деятельность злоумышленников и подозрительную активность

Помимо разработки и внедрения программы, способствующей выявлению разведывательных действий или подозрительной активности и уведомлению о них, владельцы/операторы КВИ могут предпринять ряд мер для сдерживания разведывательной деятельности злоумышленников. Один из подходов заключается в организации информационно-разъяснительной работы по вопросам безопасности. Такая работа направлена на сдерживание злоумышленников на этапе разведывательной деятельности путем убеждения его в том, что объект слишком хорошо укреплен, слишком хорошо охраняется или иным образом представляет собой слишком сложную для атаки цель.

Помимо информационно-разъяснительной работы по вопросам безопасности, этой цели можно достичь посредством эффективных и видимых мер по обеспечению физической безопасности и усиления защиты (включая описанные в главе 6 «Меры физической безопасности» и этой главе). Владелец/оператор КВИ может сдерживать злоумышленников, например, минимизируя объем общедоступной информации об объекте (включая меры безопасности, организационную структуру и изображения объекта и его окрестностей в Интернете).

Национальная практика: примеры информационно-разъяснительной работы по вопросам безопасности, рекомендуемые Национальным управлением по защите и безопасности Великобритании[277]

- «Убедитесь, что на вашем веб-сайте действует надежная и актуальная политика в отношении файлов cookie и конфиденциальности, чтобы злоумышленники знали, что вы записываете данные об использовании ими вашего веб-сайта, например их IP-адрес.
- Убедитесь, что на вашем веб-сайте есть отдельная страница, посвященная безопасности, на которой подробно описывается спектр мер безопасности, принимаемых в вашем учреждении (не раскрывая при этом деталей, которые могут быть полезны для злоумышленников). Вам следует освещать только те меры безопасности, которые действительно применяются.
- Проверьте свои сообщения и убедитесь, что вы случайно не разглашаете информацию, которая может быть полезна злоумышленникам, например, точные карты/планы этажей, точное количество посетителей или часы пик и тишины.
- Используйте социальные сети, пресс-релизы и другие каналы коммуникации, чтобы сообщать о том, что на вашем объекте приняты меры безопасности, но не раскрывайте подробности, которые могут быть полезны злоумышленникам.
- Подумайте об используемых изображениях. Не содержат ли они информацию о местоположении и типе системы видеонаблюдения, установленной на вашем объекте, или о внешнем виде и содержании пропусков сотрудников? Если да, удалите или отредактируйте изображение».

Источник: Национальное управление по защите и безопасности Великобритании

Еще одной полезной мерой, которую владельцы/операторы КВИ могут использовать для разработки мер в ответ на разведывательные действия злоумышленников или подозрительную активность, является организация учений, в ходе которых внутренние команды имитируют роль злоумышленников, стремящихся проверить состояние безопасности объекта. Результаты этих учений затем можно оценить, проанализировать и использовать для определения мер, которые позволят повысить уровень безопасности объекта или сделать реагирование более эффективным и действенным.

277 Национальное управление по защите и безопасности Великобритании (2024 г.), *Коммуникация с учетом вопросов безопасности. 5-минутное резюме.* Доступно по адресу: https://www.npsa.gov.uk/resources/security-minded-communications-5-minute-read [дата обращения: 10 декабря 2024 г.].

7.2 Планирование мер безопасности на случай нападения с использованием транспортных средств

Распространенным и особенно разрушительным методом атак, используемым террористами для уязвимых целей и общественных мест, является таран целей крупногабаритными транспортными средствами на высокой скорости для максимального увеличения человеческих жертв и ущерба. Террористы также используют транспортные средства для подвоза взрывных устройств ближе к площадке или объекту. Хотя эта угроза исторически ограничивалась атаками на уязвимые цели, ее потенциальную угрозу для объектов КВИ, *в том числе* в качестве способа преодоления периметра объекта или доставки взрывного устройства или группы вооруженных злоумышленников к намеченной цели, нельзя недооценивать.

Национальная практика: вопросы Агентства по кибербезопасности и защите инфраструктуры США для оценки рисков использования транспортных средств в качестве тарана (2024 г.)[278]

«Первым шагом в планировании мер по снижению рисков является проведение оценки рисков, связанных с использованием транспортного средства в качестве тарана. Эта оценка помогает владельцам критически важной инфраструктуры, операторам, их персоналу и организаторам массовых мероприятий выявлять уязвимости, расставлять приоритеты в усилиях по снижению рисков и внедрять меры по обеспечению безопасности пешеходов и зданий. [...] Оценка угроз, исходящих от транспортных средств, уникальна тем, что пользователь оценивает, может ли территория, непосредственно окружающая, прилегающая и граничащая с его объектом или инфраструктурой, стать путем для совершения нападения с использованием транспортного средства. Вопросы, которые следует задать во время оценки, могут быть следующими:

- Можно ли проехать по моей территории, прилегающей территории или окружающей территории?
- Какие типы транспортных средств могут передвигаться по этой территории?
- Какую максимальную скорость может развить транспортное средство при движении по этой территории?
- Есть ли контрольно-пропускной пункт для транспортных средств? Если да, то как далеко он расположен от объектов инфраструктуры?
- Есть ли охрана на контрольно-пропускных пунктах?
- Где находятся парковочные места, стоянки или гаражи для транспортных средств?
- Имеются ли подъездные пути для транспортных средств доставки?
- Имеются ли какие-либо естественные барьеры для транспортных средств?
- Под какими углами атаки транспортное средство может нанести ущерб моей инфраструктуре?

278 Агентство кибербезопасности и защите инфраструктуры США (2024 г.), *Предотвращение и смягчение последствий инцидентов с использованием транспортных средств: руководство по безопасности.* Доступно по адресу: https://www.cisa.gov/sites/default/files/2024-04/Vehicle_Incident_Prevention_and_Mitigation_Security_Guide_508_20240418.pdf [дата обращения: 21 июля 2025 г.].

- Есть ли зоны, позволяющие замедлить движение?
- Имеются ли камеры видеонаблюдения, охватывающие территории, где находятся или будут/могут проезжать транспортные средства?
- Отделено ли надлежащим образом пешеходное движение, будь то с парковок или вблизи въездов/выездов на объекты, от движения транспортных средств?»

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры

Многие варианты ограждения, подробно описанные в этом разделе, имеют «рейтинг ударопрочности», что означает их способность до определенной степени выдерживать удар движущегося транспортного средства, оцененную поставщиком. Существует множество факторов, которые влияют на этот рейтинг того или иного варианта ограждения, включая вес потенциально опасного транспортного средства (например, мотоцикла или большого грузовика), а также скорость и угол, под которым оно ударяется об ограждение или объект. Поэтому владельцам/операторам КВИ рекомендуется учитывать этот диапазон факторов при выборе предпочтительного метода или методов защиты объекта КВИ от транспортных средств злоумышленников. Ниже приведены некоторые примеры национальных и международных стандартов, используемых для определения рейтингов ударопрочности:

- ISO 22343-1:2023 «Безопасность и устойчивость. Барьеры безопасности транспортных средств. Часть 1. Требования к эксплуатационным характеристикам, метод испытания транспортного средства на удар и оценка эксплуатационных характеристик»;[279]
- Американское общество по испытаниям и материалам F2656: Стандартный метод испытаний методом «краш-теста» с участием защитных транспортных средств и защитных ограждений;[280]
- Публично доступная Спецификация 68 Британского института стандартов.[281]

279 ISO (2023 г.) *Безопасность и устойчивость. Защитные барьеры от транспортных средств, Часть 1: Требования к эксплуатационным характеристикам, метод испытания на удар транспортного средства и оценка характеристик.* Доступно по адресу: https://www.iso.org/standard/50080.html [дата обращения: 21 июля 2025 г.].

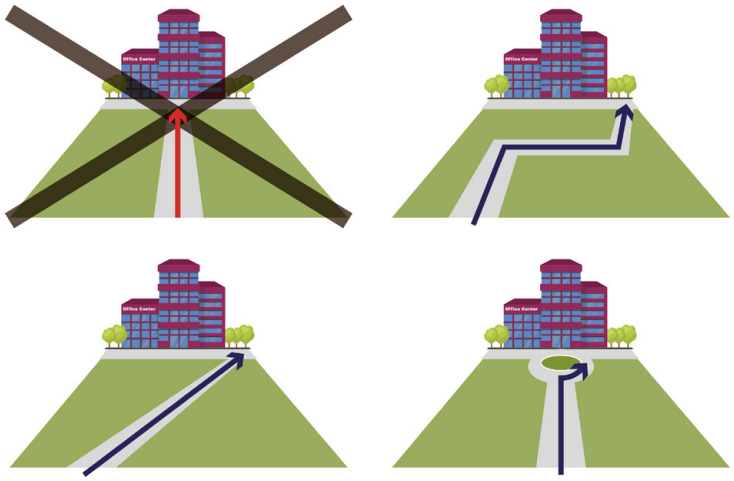
280 ASTM International (ноябрь 2023 г.), *Стандартный метод испытаний методом «краш-теста» защитных ограждений от транспортных средств*, ASTM F2656/F2656M-23.

281 Британский институт стандартов (август 2013 г.), *Технические условия на ударные испытания систем ограждений от транспортных средств, третье издание.*

Контроль скорости транспортного средства

Угрозу атаки с использованием транспортного средства можно значительно снизить, контролируя скорость транспортного средства при приближении к объекту КВИ и исключая возможность прямого столкновения транспортного средства со зданием КВИ. Проектирование подъездных путей к объекту КВИ без прямого или прямолинейного доступа делает невозможным набор скорости транспортным средством при приближении. Такое проектирование, в сочетании с соответствующим ландшафтным дизайном, снижает эффективность любой потенциальной атаки злоумышленника с использованием транспортного средства.

В случаях, когда на въезде на объект КВИ используется дорожное ограждение, требования к ударопрочности определяются такими факторами, как скорость транспортного средства при приближении и угол его удара об ограждение. Размер транспортного средства также имеет значение не только из-за силы, с которой более крупное транспортное средство может ударить по цели, но и потому, что более крупные транспортные средства, движущиеся с той же скоростью, могут содержать больше взрывчатого вещества и, следовательно, вызвать более мощный взрыв, который повредит близлежащие здания. Для объектов КВИ можно могут рассмотреть возможность использования отдельных подъездных путей для более крупных транспортных средств с дополнительными мерами снижения скорости.



Различные меры по ограничению скорости движения транспортных средств, включая непрямой доступ к объекту. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[282]

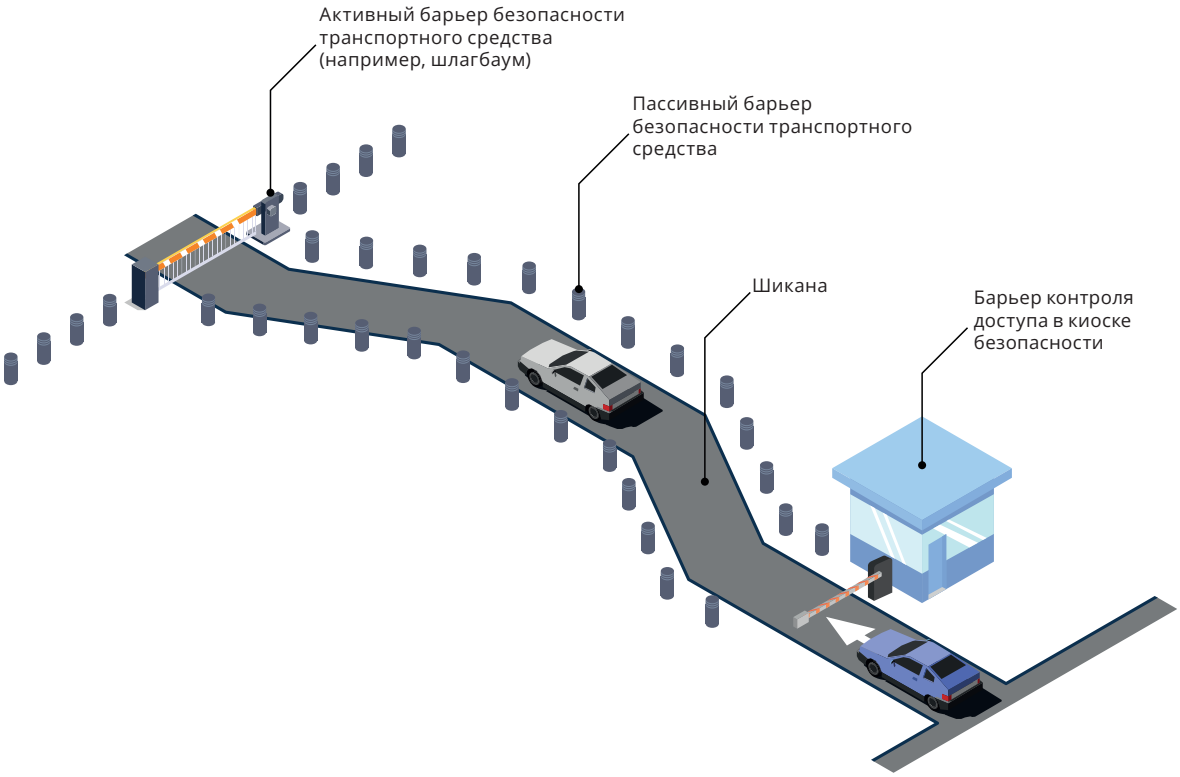
Другими потенциальными вариантами снижения скорости транспортных средств посредством проектирования дорог являются использование криволинейных участков дороги, параллельных подъездных путей и шикан:

- *Криволинейные участки дороги.* Прямые и перпендикулярные подъездные пути к объекту КВИ позволяют транспортному средству набирать скорость и потенциально проникать на объект КВИ или за его периметр. Однако, при движении по криволинейному участку дороги к объекту КВИ транспортное

282 Бюро публикаций Европейского Союза (2024 г.), *Безопасность по проектированию: защита общественных пространств от террористических атак.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC131172 [дата обращения: 21 июля 2025 г.].

средство злоумышленника, движущееся с высокой скоростью, может занести или перевернуться. Чтобы снизить риск потери управления, водителям придется снизить скорость.[283]

- *Параллельные подъездные пути.* Параллельные дороги вдоль периметра объекта могут помешать транспортному средству набрать достаточную скорость для прямой атаки или преодоления периметра объекта.[284]
- *Шиканы.* Шикана – это двойной изгиб дороги, созданный намеренно для снижения скорости транспортного средства и контроля его въезда или выезда (см. рисунок ниже). Постоянные шиканы могут состоять из дорожных барьеров, размещенных по краям дороги, чтобы вынудить транспортное средство следовать траектории шиканы. Временные шиканы могут состоять из больших бетонных блоков, служащих той же цели. Объекты КВИ могут устанавливать как временные, так и постоянные шиканы на основе своей оценки степени угрозы.[285]



Дорожные барьеры: пассивные и активные барьеры

Дорожные барьеры, используемые для снижения угроз со стороны транспортных средств злоумышленников, могут быть (стационарными) или активными (управляемыми). Решение о том, какой барьер наиболее подходит для конкретного объекта КВИ, должно основываться на оценке рисков, в рамках которой отдельно рассматриваются угрозы со стороны транспортных средств и потенциальные

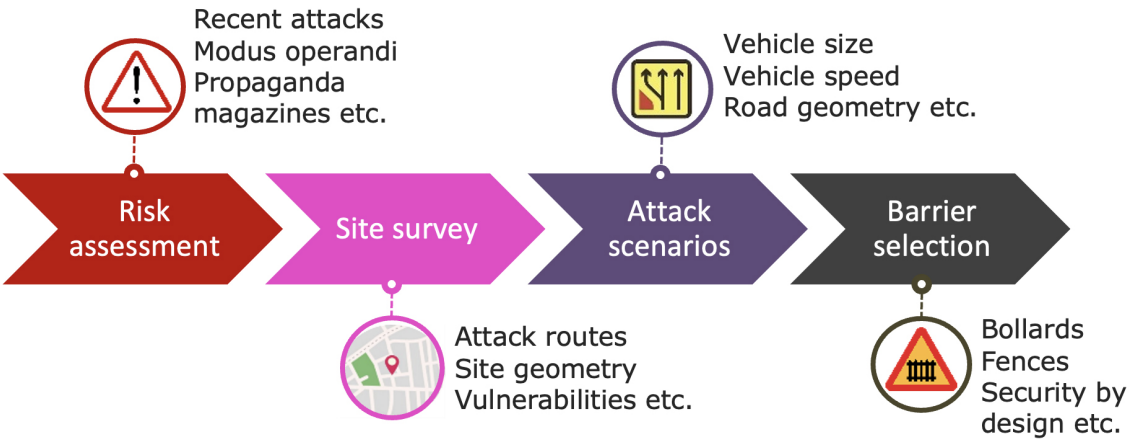
283 Бейкер, П.; Бенни, Дж. Д. (2013 г.), *Полное руководство по физической безопасности* (Бока-Ратон: CRC Press).

284 Бейкер, П.; Бенни, Дж. Д. (2013 г.), *Полное руководство по физической безопасности* (Бока-Ратон: CRC Press).

285 Комри, Д., Мейс, Г., Смит, П. (2009 г.) «Угрозы, исходящие от транспортных средств, и принципы смягчения последствий воздействия враждебных транспортных средств», в книге Комри, Д.; Мейс, Г.; Смит, П., *Воздействие взрывной волны на здания* (2-е издание) (Лондон: ICE Publishing).

сценарии угроз. В любом случае барьеры должны быть надлежащим образом спроектированы, изготовлены и регулярно обслуживаться для обеспечения их корректной работы. Это особенно актуально для активных барьеров с подвижными частями.

Требования к эксплуатационным характеристикам ограждений транспортных средств изложены в стандарте ISO 22343:1:2023 «Безопасность и устойчивость. Барьеры безопасности транспортных средств, Часть 1: Требования к эксплуатационным характеристикам, метод испытания транспортного средства на удар и оценка эксплуатационных характеристик».[286]



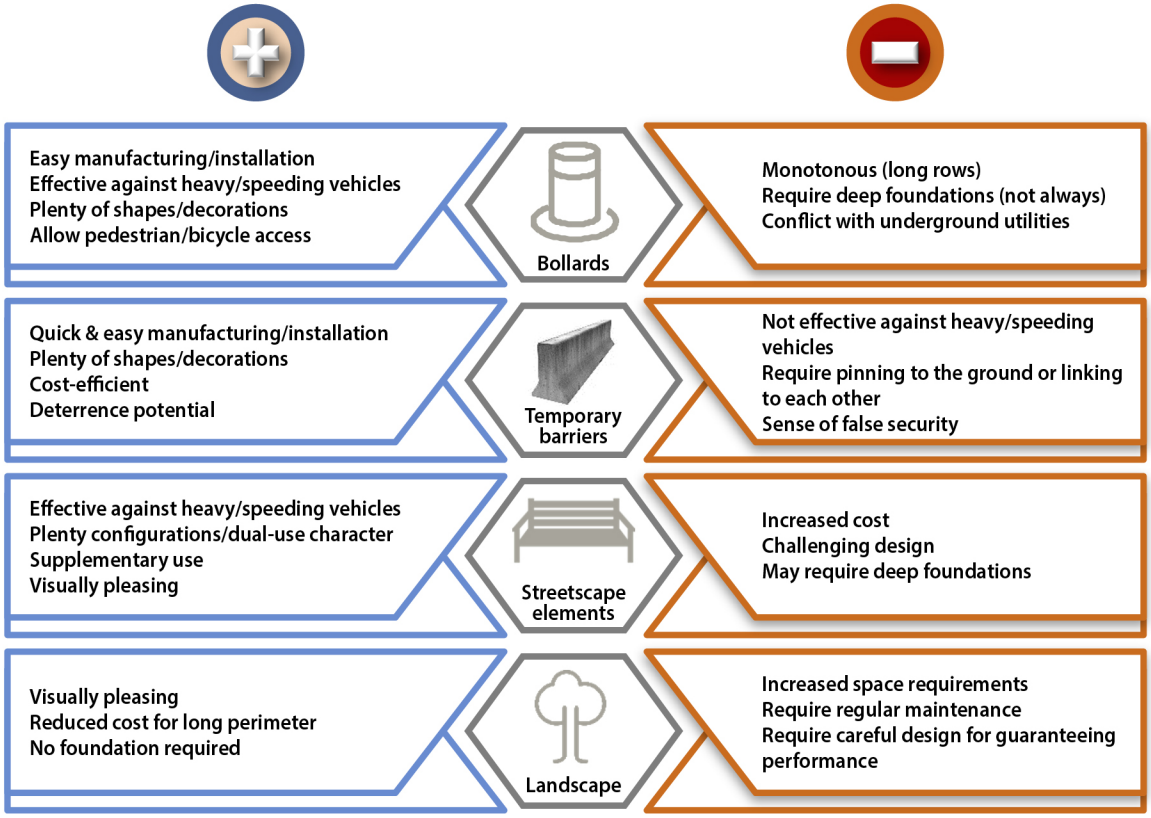
Технологическая схема выбора противотаранных заграждений. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[287]

286 ISO (2023 г.) *Безопасность и устойчивость. Защитные барьеры от транспортных средств, Часть 1: Требования к эксплуатационным характеристикам, метод испытания на удар транспортного средства и оценка характеристик*. Доступно по адресу: https://www.iso.org/standard/50080.html [дата обращения: 21 июля 2025 г.].

287 Василис, К.; Ларчер, М. (2020 г.), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак,* Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

Пассивные дорожные барьеры

Пассивные барьеры представляют собой цельные конструкции, которые фактически блокируют въезд транспортных средств и тем самым защищают периметр объекта или площадки.[288] Они предназначены для поглощения удара транспортного средства за счет прочного основания или сочетания веса конструкции и трения, возникающего при ее движении по дорожному покрытию.[289] Примерами пассивных барьеров являются стационарные столбы, искусственные клумбы, тяжелые предметы, деревья, стены, водные преграды и заборы.[290, 291]



Преимущества и недостатки пассивных дорожных барьеров. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[292]

288 US DHS FEMA (2007 г.), *Проектирование территорий и городов для обеспечения безопасности: Руководство по борьбе с потенциальными террористическими атаками.* Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

289 Василис, К.; Ларчер, М. (2020), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак, Бюро публикаций Европейского Союза.* Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

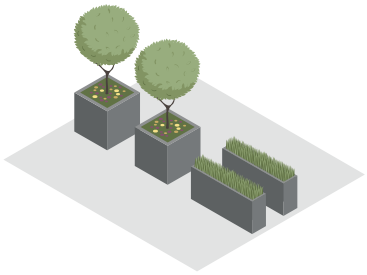
290 Министерство национальной безопасности США (2011 г.), *Справочное руководство по снижению потенциальных террористических атак на здания: FEMA-426/BIPS-06/октябрь 2011 г. Издание 2.* Доступно по адресу: https://www.dhs.gov/xlibrary/assets/st/st-bips-06.pdf [дата обращения: 21 июля 2025 г.].

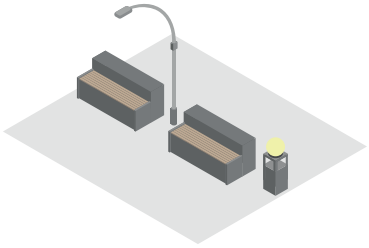
291 US DHS FEMA (2007 г.), *Проектирование площадок и городов для обеспечения безопасности: руководство по предотвращению потенциальных террористических атак.* Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

292 Василис, К.; Ларчер, М. (2020), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак,* Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

Различные варианты пассивного барьера (неисчерпывающий список)

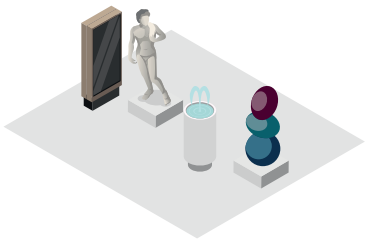
Искусственные клумбы: Грамотно спроектированная клумба может стать эффективным барьером для транспортных средств и эстетичным дополнением к периметру объекта КВИ. Клумбы могут быть либо закреплены на земле, либо быть достаточно тяжелыми, чтобы за счет трения остановить или задержать транспортное средство злоумышленника. В последнем случае клумбы могут быть отброшены в сторону тяжелыми или быстро движущимися транспортными средствами. Клумбы, закрепленные на земле с помощью достаточного количества подземных укреплений, могут обеспечить более надежную защиту от транспортных средств различных размеров и скоростей.[293]

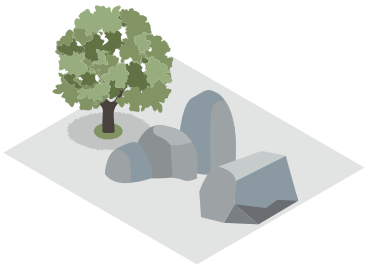




***Усиленная уличная мебель и инвентарь*:** Элементы уличного ландшафта, такие как скамейки и уличные фонари, можно укрепить или усилить, чтобы они служили пассивными барьерами. При надлежащем проектировании они могут служить одновременно и элементами благоустройства, и элементами периметральной безопасности.[294] Стратегическое размещение их по периметру объекта КВИ, где присутствуют транспортные средства, может также служить эстетическим целям.

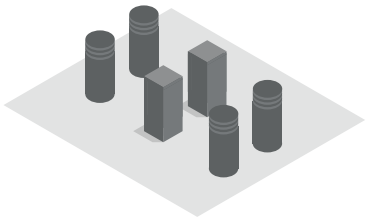
Тяжелые предметы: Тяжелые предметы, такие как скульптуры и валуны, также могут выполнять двойную функцию: эстетических элементов и пассивных барьеров. Чтобы обеспечить их эффективность в снижении выявленной угрозы, необходимо инженерное проектирование и/или оценка.[295]





Элементы ландшафта, деревья: В зависимости от местоположения объекта КВИ, элементы ландшафта, такие как скальные образования, водные объекты, возвышенности или деревья, также могут использоваться для защиты от транспортных средств злоумышленников.[296] В некоторых случаях такие элементы также могут быть усилены для обеспечения дополнительной защиты.

Специально разработанные барьеры для смягчения последствий воздействия транспортных средств: Дорожные столбы являются одним из самых популярных решений для предотвращения несанкционированного доступа транспортных средств. Обычно они изготавливаются из стали, железобетона или их сочетания (бетонный сердечник в стальном кожухе). Их узкая форма и компактный размер делают их более привлекательными для использования, например, в местах общественного пользования, чем другие решения. Как правило, эффективность дорожного столба зависит от глубины залегания его фундамента под землей и его общих размеров.[297]



293 US DHS FEMA (2007 г.), *Проектирование площадок и городов для обеспечения безопасности: руководство по борьбе с потенциальными террористическими атаками. Серия «Управление рисками»*. Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

294 US DHS FEMA (2007 г.), *Проектирование площадок и городов для обеспечения безопасности: руководство по борьбе с потенциальными террористическими атаками. Серия «Управление рисками»*. Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

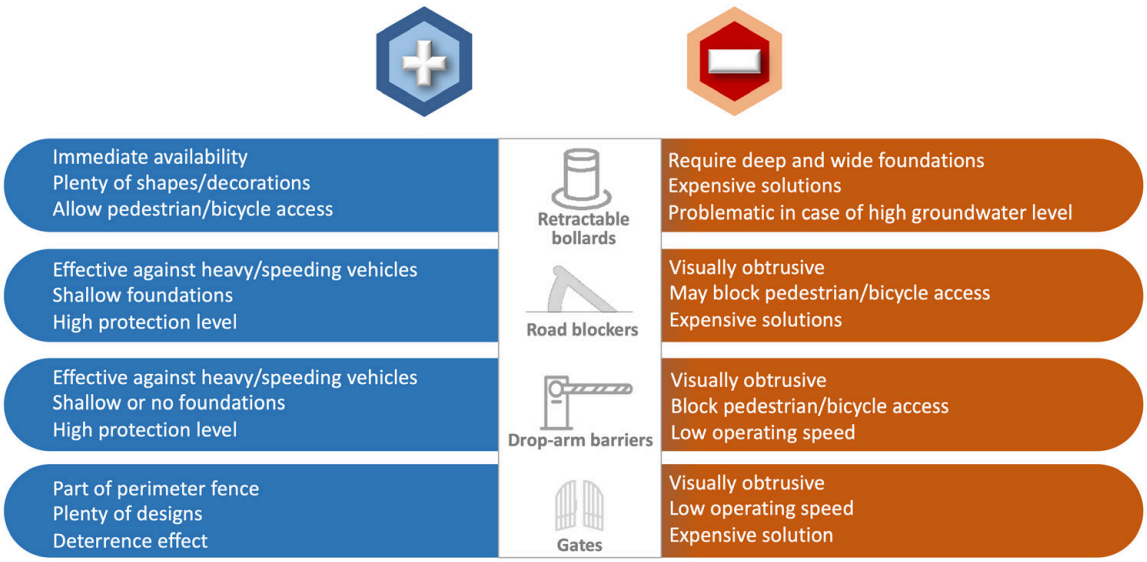
295 US DHS FEMA (2007 г.), *Проектирование площадок и городов для обеспечения безопасности: руководство по борьбе с потенциальными террористическими атаками. Серия «Управление рисками»*. Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

296 Василис, К.; Ларчер, М. (2020 г.), *Рекомендации, Защита периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак,* Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

297 US DHS FEMA (2007 г.), *Проектирование территорий и городов для обеспечения безопасности: руководство по борьбе с потенциальными террористическими атаками. Серия «Управление рисками»*. Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

Активные заграждения

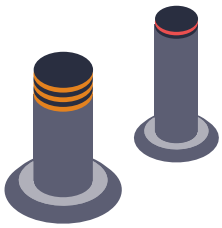
Активные заграждения могут использоваться в пунктах контроля доступа транспортных средств по периметру объекта КВИ или на въезде в определенное здание на территории объекта. В последнем случае они могут служить заграждением для проверки или досмотра транспортных средств. Их открытие может контролироваться различными способами, например, водителем транспортного средства с разрешенным доступом, автоматизированной электронной системой или сотрудниками службы безопасности, ответственными за досмотр въезжающего транспорта. Системы активных заграждений имеют как преимущества, так и недостатки, как показано ниже. Из-за наличия в их конструкции подвижных частей механические системы активных заграждений требуют технического обслуживания для обеспечения их работоспособности.



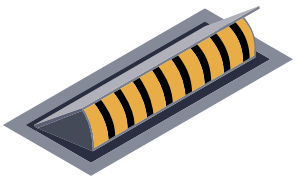
Преимущества и недостатки активных заграждений. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[298]

298 Карлос, В.; Ларчер, М. (2020 г.), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак,* Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

Различные варианты активных заграждений[299]

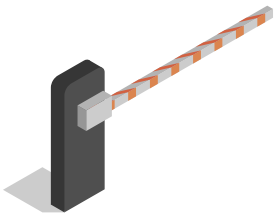


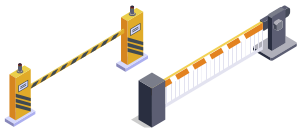
Выдвижные столбы: Система выдвижных столбов состоит из одного или нескольких поднимающихся столбов, работающих независимо или группами по два или более.[300] Они остаются в поднятом положении, блокируя проезд транспортных средств, и опускаются только для проезда разрешенных транспортных средств. Обычно их считают дорогостоящим вариантом активного барьера, учитывая высокую стоимость их установки и необходимость обеспечения достаточно глубокого фундамента для предотвращения транспортных угроз.[301]



Пандусы или дорожные блокираторы: Дорожные блокираторы представляют собой усиленный барьер, обычно изготавливаемый из стали, который устанавливается в поднятом положении для блокировки проезда транспортных средств. При необходимости их можно опустить с помощью гидравлической или электрической системы, чтобы они полностью прилегали к земле, обеспечивая проезд транспортных средств.[302] В поднятом положении некоторые дорожные блокираторы можно дополнительно усилить шипами для прокола шин транспортных средств, пытающихся преодолеть барьер.

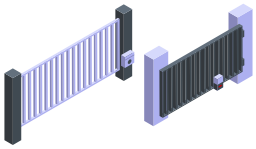
Шлагбаумы: Шлагбаумы обычно устанавливаются на контрольно-пропускных пунктах или въездах на охраняемую территорию и часто используются персоналом службы безопасности или управляются автоматизированной системой контроля доступа. Такой барьер состоит из металлической штанги, которая находится в горизонтальном положении, блокируя проезд транспортных средств,[303] и затем поднимается, позволяя транспортным средствам проехать.





Усиленные шлагбаумы: Усиленные шлагбаумы обычно рассматриваются как более прочная версия простых шлагбаумов. Они обычно сертифицированы в соответствии с определенными стандартами безопасности транспортных средств и изготавливаются из стали с достаточным армированием и других материалов.[304] Эта система работает аналогично обычным шлагбаумам, но обычно имеет бетонные или иные армированные конструкции по обе стороны металлической балки для обеспечения более высокой ударопрочности.

Ворота: Ворота обычно являются частью более крупного периметрального ограждения и используют колеса или петли для открывания и пропуска транспортных средств. Существует несколько типов ворот с различными рейтингами ударопрочности.[305] В зависимости от типа ворот, быстро движущееся транспортное средство может прорваться сквозь них, разбрасывая опасные осколки в разных направлениях.



299 Типы «различных вариантов активного барьера» взяты из: Карлос, В.; Ларчер, М. (2020 г.), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак*, Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

300 US DHS FEMA (2007 г.), *Проектирование территорий и городов для обеспечения безопасности: руководство по борьбе с потенциальными террористическими атаками.* Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

301 Карлос, В.; Ларчер, М. (2020 г.), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак*, Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

302 Карлос, В.; Ларчер, М. (2020 г.), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак*, Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

303 Карлос, В.; Ларчер, М. (2020 г.), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак*, Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

304 US DHS FEMA (2007 г.), *Проектирование территорий и городов для обеспечения безопасности: руководство по борьбе с потенциальными террористическими атаками.* Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

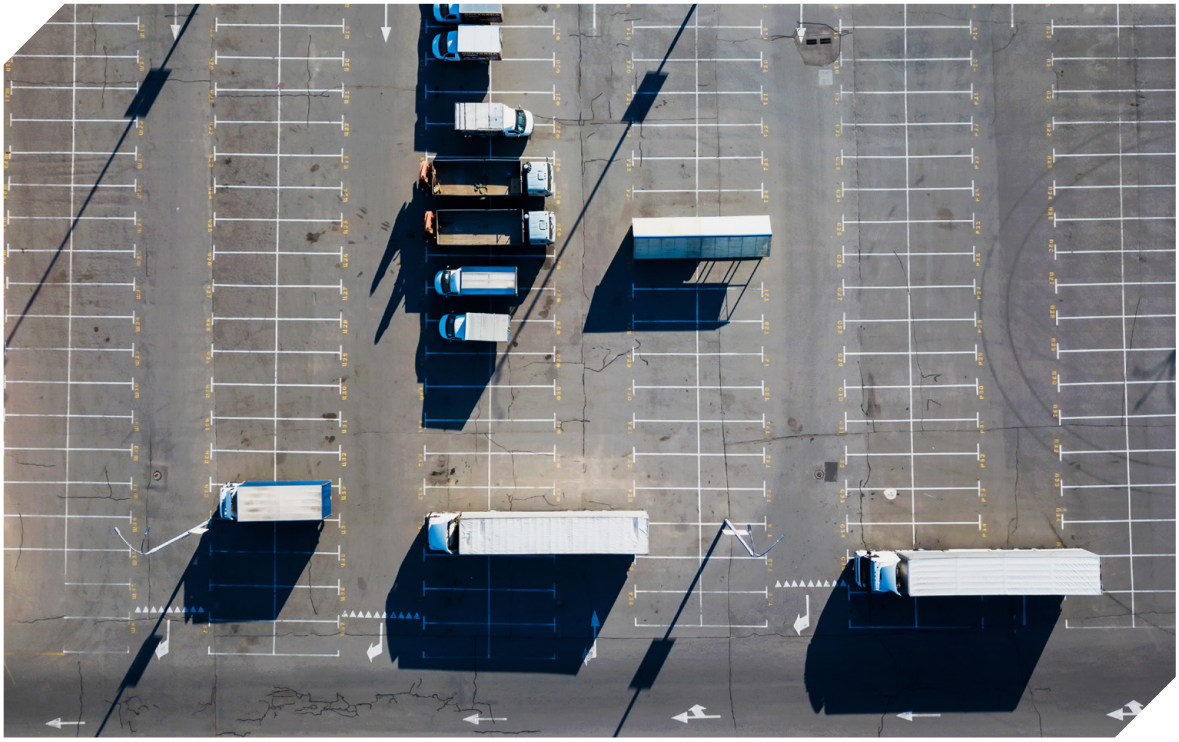
305 US DHS FEMA (2007 г.), *Проектирование территорий и городов для обеспечения безопасности: руководство по борьбе с потенциальными террористическими атаками.* Доступно по адресу: https://www.fema.gov/sites/default/files/2020-08/fema430.pdf [дата обращения: 21 июля 2025 г.].

Временные заграждения

В период повышенной угрозы на объекте КВИ временные заграждения могут обеспечить дополнительную защиту от транспортных средств злоумышленников. Их можно развернуть в короткие сроки и переориентировать для контроля или перенаправления движения по мере необходимости. Они не крепятся к земле, поэтому часто расчет делается на массу временных заграждений для постепенного замедления и остановки движущегося транспортного средства. Это зачастую наиболее эффективно, когда транспортное средство движется с относительно низкой скоростью. Это делает временные заграждения несколько менее практичными для долгосрочной защиты чувствительных участков или периметров объекта КВИ. Они могут служить визуальным сдерживающим фактором для потенциальных агрессоров, но также могут создать ложное чувство безопасности. Примерами временных заграждений являются бетонные или заполненные водой барьеры типа «Джерси» или крупные клумбы.[306]

Парковка транспортных средств

Транспортные средства злоумышленников не обязательно должны находиться в движении, чтобы представлять угрозу объекту КВИ. Например, они могут быть припаркованы и начинены взрывчаткой. В этой связи возникают сложные вопросы, связанные с парковкой транспортных средств снаружи объекта КВИ или рядом с ним. В качестве общей меры парковочные места за пределами объекта КВИ должны располагаться вдали от периметра объекта или критически важных элементов. Точное расстояние до объекта должно определяться компетентными органами и владельцами/операторами КВИ на основе оценочной взрывной силы взрывного устройства, размещенного внутри транспортного средства, припаркованного на объекте.



306 Карлос, В.; Ларчер, М. (2020 г.), *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак,* Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

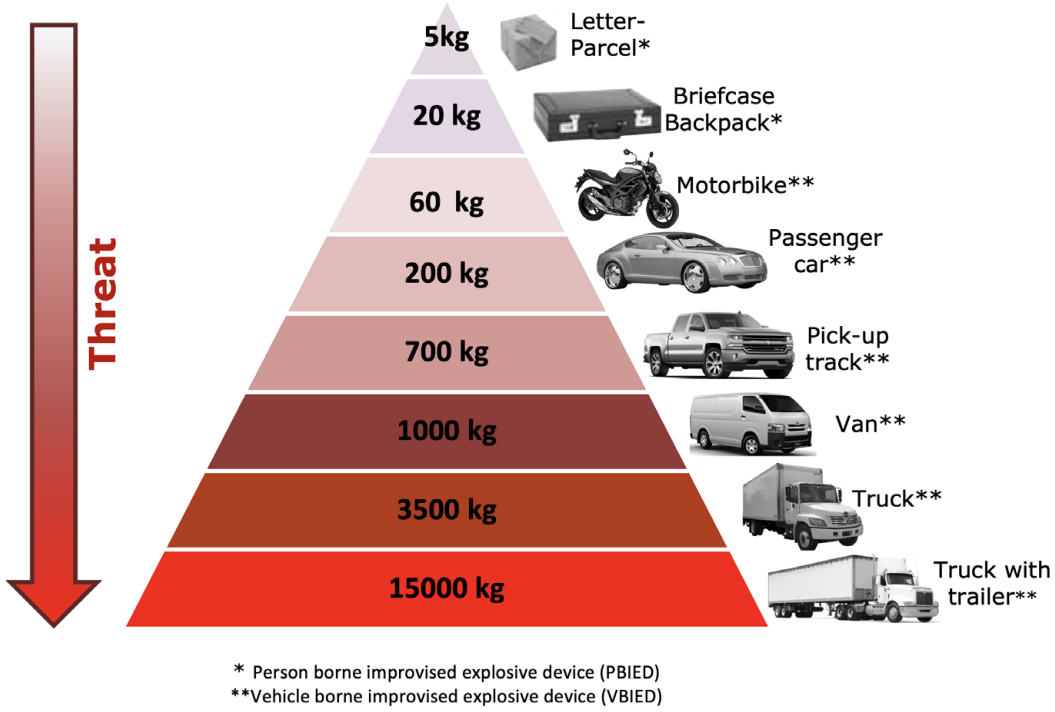
7.3 Планирование мер безопасности на случай нападения с использованием взрывных устройств

Террористы и другие насильственные субъекты могут стремиться совершить нападение на объект КВИ с использованием взрывного устройства. В данном разделе представлен ряд передовых подходов и рекомендаций для подготовки объектов КВИ к этим угрозам.[307] В некоторых случаях рекомендации в данном разделе скорее связаны с *реагированием* на инцидент с использованием взрывного устройства, а не с повышением физической безопасности объекта от этих угроз. Хотя это может выходить за рамки вопросов физической безопасности, это, тем не менее, часть эффективной системы безопасности любого объекта КВИ.

Шаги, которые можно предпринять для принятия решения о соответствующих мерах защиты от атак с использованием СВУ. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[308]

307 См. также: *Технические руководящие принципы по содействию осуществлению Резолюции 2370 (2017 г.) Совета Безопасности и связанных с ней международных стандартов и передовой практики по предотвращению приобретения оружия террористами,* опубликованные КТУ ООН, Исполнительным директоратом Контртеррористического комитета Совета Безопасности ООН, Институтом ООН по исследованию проблем разоружения и Глобальным договором ООН о координации контртеррористической деятельности.

308 Бюро публикаций Европейского Союза (2024 г.), *Безопасность по проектированию: защита общественных пространств от террористических атак.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC131172 [дата обращения: 21 июля 2025 г.].



Верхние пределы массы заряда по видам транспорта. Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[309]

Угрозы применения взрывных устройств

Угрозы применения взрывных устройств являются обычным методом действий для различных субъектов угроз, поскольку они могут вызывать существенные перебои, но при этом требуют минимальных усилий. В некоторых случаях террористические организации сообщали об угрозах взрыва сотрудникам правоохранительных органов или персоналу объектов КВИ, чтобы предупредить о реальной угрозе взрыва. В других случаях угрозы взрыва были лишь озвучены, но взрывчатые вещества не были обнаружены. Тем не менее, эти угрозы вызывали серьезные перебои в работе объекта. Угрозы взрыва могут также исходить от случайных граждан, недовольных действующих или бывших сотрудников объекта КВИ или других лиц, стремящихся проверить реакцию персонала объекта КВИ или правоохранительных органов. Независимо от обстоятельств, угрозы взрыва на объектах КВИ должны восприниматься серьезно, и должны быть предусмотрены процедуры, обеспечивающие быстрое принятие решений компетентными лицами на объекте и за его пределами (например, местными правоохранительными органами). Практические рекомендации по обеспечению надлежащей защиты объектов от угроз взрыва, например, путем укрепления зданий и периметральных конструкций, подробно изложены в главе 6 «Меры физической безопасности». В этом разделе приводятся примеры передовой практики реагирования на угрозы взрыва на объектах КВИ.

Персонал объекта КВИ, который может получать сообщения с угрозами взрыва, например, администраторы или сотрудники службы безопасности, должен быть обучен реагированию на такие угрозы. Чтобы оказать поддержку персоналу, объектам КВИ рекомендуется иметь письменные инструкции, к которым можно обратиться в случае получения звонка с угрозой.

309 Бюро публикаций Европейского Союза (2024 г.), *Безопасность по проектированию: защита общественных пространств от террористических атак.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC131172 [дата обращения: 21 июля 2025 г.].

Национальная практика: контрольный список, составленный Агентством по кибербезопасности и защите инфраструктуры США для реагирования на сообщение об угрозе взрыва (по телефону)[310]

Дата	
Время	
Время, когда звонящий повесил трубку	
Номер телефона, с которого был получен звонок	
Спросите звонящего: ▸ Где находится взрывное устройство? (здание, этаж, комната и т.д.) ▸ Как оно выглядит? ▸ Что это за взрывное устройство? ▸ Что вызовет срабатывание взрывного устройства? ▸ Это вы заложили взрывное устройство? ▸ Почему? ▸ Как вас зовут?	
Сообщение об угрозе дословно	
Информация о звонившем: ▸ Где находится звонящий? (фон/уровень шума) ▸ Предполагаемый возраст ▸ Знаком ли вам голос? Если да, то на чей голос он похож? ▸ Другие моменты	

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры

310 Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Контрольный список в случае угроз взрыва.* Доступно по адресу: https://www.cisa.gov/sites/default/files/2025-03/Bomb%20Threat%20Checklist%20v3.0%20508.pdf [дата обращения: 18 мая 2025 г.].

Практика: Руководство Ассоциации банков Сингапура по действиям при угрозах взрыва, полученных по телефону (2018 г.)[311]

При получении сообщения об угрозе взрыва:

1. Не паникуйте. Сохраняйте спокойствие.
2. Подайте сигнал кому-нибудь, чтобы он позвонил в полицию. Займите звонящего разговором как можно дольше, пока полиция отслеживает звонок.
3. Сотрудник, получивший такой звонок, должен [относиться] к ним серьезно и немедленно попытаться установить:
   - точное местонахождение взрывного устройства и его точный внешний вид;
   - время детонации и что ее вызовет;
   - количество и тип использованного взрывчатого вещества; и
   - причину такого действия.
4. Также важно принять во внимание следующее:
   - голос звонящего и голосовые характеристики (например, высота голоса, мужской/ женский, взрослый/ребенок);
   - используемый язык и акцент (например, местный или иностранный);
   - манера речи (например, быстрая, обдуманная, эмоциональная, гневная);
   - фоновые шумы (например, шум транспорта, музыка, публичные объявления, крики);
   - лицо или орган, которому должно быть передано это сообщение;
   - не провоцируйте и не дразните звонящего; и
   - будьте вежливы и сохраняйте спокойствие.
5. Не распространяйте слухи.
6. В зависимости от ситуации приступите к эвакуации.

Источник: Ассоциация банков Сингапура

311 Ассоциация банков Сингапура (2018 г.), *Руководство по физической безопасности для финансовых учреждений.* Доступно по адресу: https://abs.org.sg/docs/library/abs-scps-guidelines.pdf [дата обращения: 21 июля 2025 г.].

Национальная практика: Руководство Агентства по кибербезопасности и защите инфраструктуры США по реагированию на сообщение об угрозе взрыва (в социальных сетях, полученное по электронной почте или в письменной форме)[312]

Если вы получили угрозу в социальных сетях или по электронной почте:

- Не отключайтесь и не выходите из учетной записи.
- Оставьте сообщение открытым на устройстве.
- Сделайте снимок экрана или скопируйте сообщение и тему.
- Запишите дату и время.
- Уведомите [соответствующее] лицо(лица), принимающее (-их) решения.

Если вы получили письменную угрозу:

- Как можно меньше прикасайтесь к документу.
- Отметьте дату, время и место обнаружения документа.
- Обеспечьте сохранность документа и не изменяйте его каким-либо образом.
- Уведомите [соответствующее] лицо(лица), принимающее (-их) решения.

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры

В дополнение к определению немедленных шагов, которые должен предпринять получатель угрозы взрыва на объекте КВИ, например, какую информацию регистрировать и кому ее следует передавать, на объекте КВИ должна быть определена процедура экстренного реагирования. Она должна включать оперативное привлечение местных правоохранительных органов. Конкретные функции правоохранительных органов должны быть определены совместно с правоохранительными органами, чтобы обеспечить соблюдение этой процедуры в чрезвычайной ситуации.

312 Агентство по кибербезопасности и защите инфраструктуры США (без даты), Угрозы взрыва [веб-страница]. Доступно по адресу: https://www.cisa.gov/bomb-threats [дата обращения: 10 декабря 2024 г.].

Национальная практика: Руководство Канадского центра гигиены и безопасности труда по действиям при поступлении угрозы взрыва (2023 г.)[313]

Согласно канадскому законодательству, каждая юрисдикция несет ответственность за разработку процедур реагирования на чрезвычайные ситуации в консультации с комитетом по гигиене и безопасности труда (или представителем по гигиене и безопасности труда) для выявления и устранения всех прогнозируемых чрезвычайных ситуаций, включая угрозы взрыва. Работодатели должны гарантировать, что:

- Разработана комплексная процедура реагирования на чрезвычайные ситуации (совместно с местными органами полиции) для реагирования на угрозы взрыва.
- Процедуры доведены до сведения всех сотрудников и определены ключевые функции в случае возникновения чрезвычайной ситуации, связанной с угрозой взрыва.
- Проводятся учения по отработке действий в чрезвычайных ситуациях, связанных с угрозой взрыва.
- Практические учения документируются.
- При необходимости предусмотрены процедуры эвакуации.

Источник: Канадский центр гигиены и безопасности труда

Если компетентные органы и органы власти сочтут обыск на объекте целесообразным и соразмерным, процедура экстренного реагирования должна способствовать быстрому выполнению этой задачи. Важно, чтобы эта процедура отрабатывалась регулярно, чтобы гарантировать, что весь персонал объекта, а не только сотрудники службы безопасности, владеют информацией о надлежащем поведении в случае угрозы взрыва. Учения должны основываться на различных сценариях, включая получение угроз взрыва в письменной форме в виде письма, телефонного звонка или другими способами.[314]

313 Канадский центр гигиены и безопасности труда (2023 г.), Угроза взрыва [веб-страница]. Доступно по адресу: https://www.ccohs.ca/oshanswers/hsprograms/bomb-threat.html#section-3-hdr [дата обращения: 10 декабря 2024 г.].

314 Полное руководство по угрозам взрыва см.: Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Руководство по угрозам взрыва.* Доступно по адресу: https://www.cisa.gov/resources-tools/resources/bomb-threat-guide [дата обращения: 21 июля 2025 г.].

Национальная практика: Руководство Национального управления по борьбе с терроризмом Великобритании по проверке мест проведения мероприятий на предмет наличия подозрительных предметов[315]

- Обеспечьте наличие планов для проведения эффективного обыска в случае сообщения об угрозе взрыва.
- Определите, кто на вашем объекте будет осуществлять координацию и нести ответственность за проведение обыска.
- Начните обыск, отправив сообщение по системе оповещения (кодированные сообщения позволяют избежать ненужных помех и паники) в формате текстового сообщения, сообщения по рации или по телефонному каскаду.
- Разделите объект на зоны, подходящие по размеру для обыска 1–2 сотрудниками. В идеале сотрудники должны следовать плану обыска и осуществлять обыск парами, чтобы обеспечить эффективный охват всей зоны.
- Лица, проводящие обыск, должны быть знакомы со своими зонами ответственности; те, кто регулярно работает в данной части объекта, лучше всех способны обнаружить необычные или подозрительные предметы.
- Сосредоточьтесь на зонах, открытых для публики; замкнутых пространствах (например, гардеробах, лестницах, коридорах, лифтах и т.д.), путях эвакуации и пунктах сбора, автостоянках, других внешних зонах, таких как зоны погрузки-разгрузки.
- Разработайте соответствующие методы, позволяющие сотрудникам регулярно проводить осмотр мест общественного пользования, не вызывая беспокойства у посетителей или клиентов.
- Убедитесь, что все посетители знают, кому следует сообщать о подозрительном/оставленном без присмотра предмете, и могут сообщить о подозрительном поведении.
- Ни при каких обстоятельствах нельзя трогать или перемещать предметы, считающиеся подозрительными. Как только компетентное лицо признает предмет подозрительным, немедленно начинайте эвакуацию.

Источник: Национальное управление по борьбе с терроризмом Великобритании

315 Национальное управление по борьбе с терроризмом, ProtectUK (без даты), Угрозы взрыва [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/bomb-threats [дата обращения: 10 декабря 2024 г.].

Национальная практика: Руководство Управления по предотвращению взрывов и кибератак Агентства по кибербезопасности и защите инфраструктуры США по выявлению подозрительных или оставленных без присмотра предметов (2023 г.)[316]

Чтобы отличить подозрительные предметы от предметов, оставленных без присмотра, Агентство по кибербезопасности и защите инфраструктуры предлагает краткий справочный документ, основанный на принципе трех вопросов:

- Спрятан ли предмет?
- Является ли он явно подозрительным?
- Является ли он нетипичным?

Ответы на эти вопросы помогут определить, является ли рассматриваемый предмет подозрительным. Если есть основания полагать, что он является подозрительным, документ приводит людей к другому принципу из четырех пунктов:

- Распознайте признаки предполагаемого взрывного устройства.
- Избегайте этого места.
- Изолируйте подозрительный предмет.
- Сообщите в соответствующие экстренные службы.

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры

Угроза взрыва в отделе корреспонденции

Один из способов, которым террорист или другой злоумышленник может попытаться нарушить работу объекта КВИ, является доставка взрывного устройства в его отдел корреспонденции. У этого метода атаки есть несколько преимуществ: он ограничивает ущерб для самих злоумышленников, он позволяет обойти многие меры контроля и безопасности доступа к объекту КВИ, которые не сможет обойти злоумышленник или транспортное средство, и, если взрывное устройство не будет обнаружено сотрудниками отдела корреспонденции, его можно доставить в определенное место на объекте КВИ.

Любая зона, где досматриваются входящие отправления, должна быть спроектирована таким образом, чтобы смягчить последствия взрыва. Оптимальным вариантом в этом случае является размещение отдела корреспонденции полностью за пределами площадки КВИ, чтобы избежать перебоев в работе в случае обнаружения подозрительной посылки. Если это невозможно, владельцы/операторы КВИ могут разместить отдел корреспонденции рядом со входом в здание, которое само находится рядом со входом на площадку КВИ. Это означает, что в случае детонации взрывного устройства в отделе корреспонденции или по пути туда, оно не проникнет достаточно глубоко в здание/на площадку, чтобы серьезно нарушить критически

316 Агентство по кибербезопасности и защите инфраструктуры США (без даты), Подозрительный или оставленный без присмотра? [веб-страница]. Доступно по адресу: https://www.cisa.gov/sites/default/files/2023-04/Unattended%20vs%20Suspicious%20Card%20for%20Digital%20Final%20v2.1.pdf [дата обращения: 21 июля 2025 г.].

важную деятельность (в зависимости от места осуществления такой деятельности). При выборе места расположения отдела корреспонденции владельцы/операторы КВИ должны также учитывать его близость к лестницам и конструктивным элементам здания и обеспечивать достаточное расстояние от них. На некоторых объектах КВИ может не быть собственного отдела корреспонденции, и почта принимается, например, от сторонних поставщиков услуг или курьеров в помещении на входе на объект. Такие помещения могут подвергаться тем же угрозам взрыва от входящих посылок, что и отдел корреспонденции, поэтому следует принимать аналогичные меры физической безопасности (а именно меры по смягчению последствий взрыва).

В дополнение к мерам по смягчению последствий взрыва отделы корреспонденции также должны быть оборудованы системами видеонаблюдения и контроля, гарантирующими доступ к ним только уполномоченным лицам. Персонал отделов корреспонденции должен быть обучен соответствующим действиям в случае обнаружения подозрительного отправления.[317] Такие действия должны включать в себя своевременное оповещение сотрудников службы безопасности объекта КВИ.

Обнаружение подозрительных отправлений на объекте критически важной инфраструктуры

На объектах КВИ должны быть разработаны процедуры на случай обнаружения подозрительного пакета или предмета на объекте КВИ, поскольку это может представлять собой взрывоопасную угрозу. Подозрительными предметами могут быть чемодан, коробка, сумка или другой предмет в любом месте здания или объекта КВИ. Весь персонал КВИ должен быть ознакомлен с этой процедурой и знать, кому следует сообщать о любом подозрительном предмете, обнаруженном на объекте.

317 Пример краткого справочного плаката см. в документе Агентства по кибербезопасности и защите инфраструктуры (без даты), Подозрительные почтовые отправления или посылки [веб-страница]. Доступно по адресу: https://www.cisa.gov/sites/default/files/2023-11/Mail%20and%20Suspicious%20Package%20Guidance%20Poster.pdf [дата обращения: 21 июля 2025 г.].

Национальная практика: Рекомендуемый Национальным антитеррористическим комитетом Российской Федерации порядок действий при обнаружении подозрительного предмета, который может оказаться взрывным устройством[318]

1. Немедленно сообщите о находке администрации или охране учреждения.
2. Зафиксируйте время и место обнаружения неизвестного предмета.
3. Предпримите меры к тому, чтобы люди отошли как можно дальше от подозрительного предмета и опасной зоны.
4. Дождитесь прибытия представителей компетентных органов, укажите место расположения подозрительного предмета, время и обстоятельства его обнаружения.
5. Не паникуйте. О возможной угрозе взрыва сообщите только тем, кому необходимо знать о случившемся. Также необходимо помнить, что внешний вид предмета может скрывать его настоящее назначение. На наличие взрывного устройства, других опасных предметов могут указывать следующие признаки:
   - Присутствие проводов, небольших антенн, изоленты, шпагата, веревки, скотча в пакете, либо торчащие из пакета;
   - Шум из обнаруженных подозрительных предметов (пакетов, сумок и др.). Это может быть тиканье часов, щелчки и т. п.;
   - Наличие на найденном подозрительном предмете элементов питания (батареек);
   - Растяжки из проволоки, веревок, шпагата, лески;
   - Необычное размещение предмета;
   - Наличие предмета, несвойственного для данной местности;
   - Специфический запах, несвойственный для данной местности.

Источник: Национальный антитеррористический комитет Российской Федерации

Поскольку подозрительный предмет может оказаться взрывным устройством с системой дистанционного подрыва, мобильные телефоны и радиостанции не следует использовать расстоянии, превышающем установленное расстояние. Например, в Великобритании рекомендуется расстояние удаления в 15 метров для мобильных телефонов/радиостанций и 50 метров для радиоустройств, установленных на транспортных средствах.[319]

Угрозы подрыва взрывных устройств на транспортных средствах

Хотя террористы постоянно меняют способы совершения нападений, взрывные устройства, установленные на транспортных средствах, – как правило, самодельные взрывные устройства, заложенные в транспортные средства (СВУТС), – остаются эффективным и давно существующим методом действий. Этот метод предполагает использование транспортного средства для сокрытия взрывного устройства. Могут

318 Национальный антитеррористический комитет (без даты), Порядок действий при обнаружении подозрительного предмета, который может оказаться взрывным устройством [веб-страница, на русском языке]. Доступно по адресу: http://nac.gov.ru/rekomendacii-po-pravilam-lichnoy-bezopasnosti/poryadok-deystviy-pri-obnaruzhenii.html [дата обращения: 10 декабря 2024 г.] неофициальный перевод.

319 Полицейские силы Кембриджшира (без даты), Принцип трех вопросов [веб-страница]. Доступно по адресу: https://www.huntingdonshire.gov.uk/media/2750/hot-principle.pdf [дата обращения: 21 июля 2025 г.].

использоваться различные типы транспортных средств, включая автомобили, фургоны, автобусы, грузовики для доставки и т.д., а также более крупные транспортные средства, способные перевозить большее количество взрывчатых веществ. СВУТС могут быть приведены в действие различными способами, включая удар при таране объекта транспортным средством, таймер, дистанционное срабатывание или при помощи человека-оператора (террорист-смертник). СВУТС способны нанести значительный ущерб имуществу и, таким образом, представляют серьезную угрозу для периметров и внутренних конструкций объектов КВИ.[320]

В дополнение к основному взрывному воздействию от детонации СВУТС, разрушение транспортного средства взрывом может вызвать дополнительный разлет осколков и взрыв топлива. В зависимости от мощности заряда взрывчатого вещества и местоположения СВУТС, взрывная волна может выбить окна на расстоянии нескольких сотен метров. Осколки разбитых окон могут стать причиной смерти и травм, поскольку быстро летящие осколки стекла легко проникают в тело человека.[321]

При оценке угроз, исходящих от СВУТС для объекта КВИ, крайне важно определить расстояние удаления от транспортного средства, чтобы гарантировать отсутствие повреждений зданий КВИ, периметральных ограждений, ворот, других жизненно важных сооружений или транспортных средств на объекте или вблизи него. Это расстояние, также известное как безопасная дистанция, является важнейшим фактором при оценке степени ущерба, который может быть нанесен зданию в результате атаки с использованием СВУТС.

Увеличение безопасной дистанции значительно повлияет на способность снизить угрозы, связанные с использованием СВУТС. Ключевыми зонами защиты от таких угроз являются периметр объекта, прилегающие территории и пункты контроля доступа транспортных средств.

Угрозы подрыва взрывных устройств, носимых на теле

Распространенный метод действий террористов – доставка взрывного устройства к намеченной цели человеком. Такое устройство часто называют переносным самодельным взрывным устройством, носимым на теле человека (ПСВУ). Террористические организации зачастую делают выбор в пользу ПСВУ, поскольку оно позволяет доставить взрывное устройство к конкретной, потенциально хорошо укрепленной цели. Человек, носящий ПСВУ, может адаптироваться к меняющейся обстановке, добиваться проникновения на объект и принимать решения/менять стратегию в режиме реального времени. ПСВУ обычно скрытно размещается под одеждой, обувью или другими предметами либо внутри них. Людей, доставляющих ПСВУ, часто называют террористами-смертниками, поскольку они погибают в результате самоубийства при детонации устройства. Подрыв ПСВУ может осуществляться различными способами, включая, в числе

320 Для справки см.: Агентство по кибербезопасности и защите инфраструктуры США (без даты), Идентификация СВУ на транспортном средстве: припаркованные транспортные средства [веб-страница]. Доступно по адресу: https://www.cisa.gov/resources-tools/resources/vbied-identification-card [дата обращения: 21 июля 2025 г.].

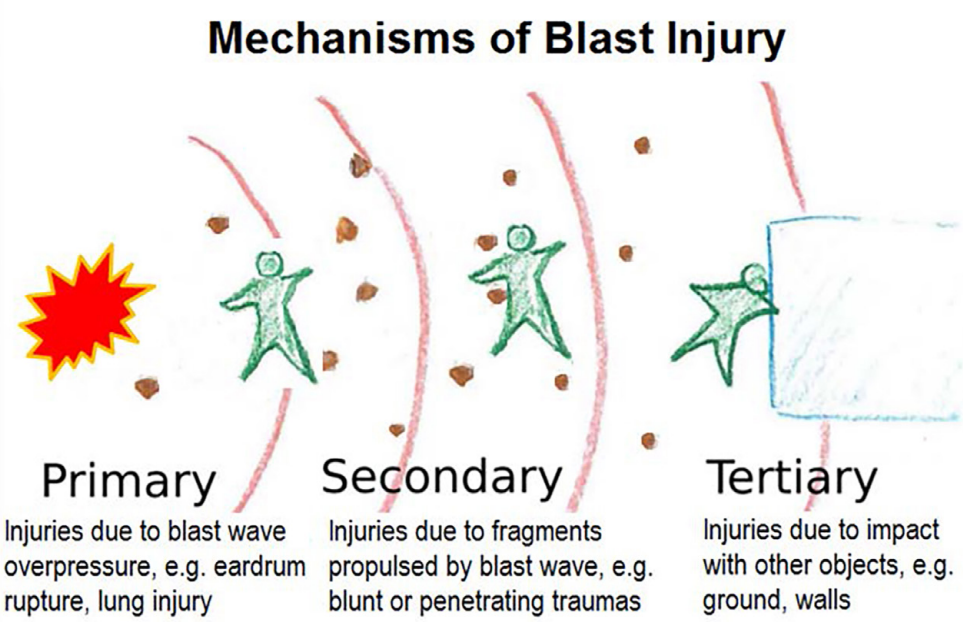
321 Карлос, В.; Ларчер, М. (2020 г.) *Руководство по защите периметра здания: Рекомендации по проектированию для повышения безопасности от террористических атак,* Бюро публикаций Европейского Союза. Доступно по адресу: https://op.europa.eu/en/publication-detail/-/publication/6d7e5311-f7c3-11ea-991b-01aa75ed71a1/language-en [дата обращения: 21 июля 2025 г.].

прочего, детонатор/инициатор, активируемый самим террористом-смертником, таймер или дистанционный подрыв третьим лицом. Последние два способа гарантируют детонацию ПСВУ, даже если человек, носящий его, передумает.

Существуют определенные ограниченные меры, которые могут снизить риск атаки с использованием ПСВУ на объекте КВИ, помимо тех, которые рассматриваются в других разделах настоящего *Технического руководства*, такие как безопасные дистанции, системы контроля доступа (включая металлодетекторы и средства досмотра, а также меры по смягчению воздействия взрывной волны). Они также рассматриваются в главе 6 «Меры физической безопасности».

Безопасная дистанция

Одной из мер по снижению угроз взрыва для объекта или здания КВИ является определение минимального расстояния, которое необходимо выдерживать между людьми и зданиями и взрывоопасной зоной, часто называемого безопасной дистанцией. *Безопасная дистанция* может меняться в зависимости от мощности заряда взрывчатого вещества, поскольку от мощности заряда зависит его разрушительный потенциал.



Использовано с разрешения Объединенного исследовательского центра Европейской комиссии.[322]

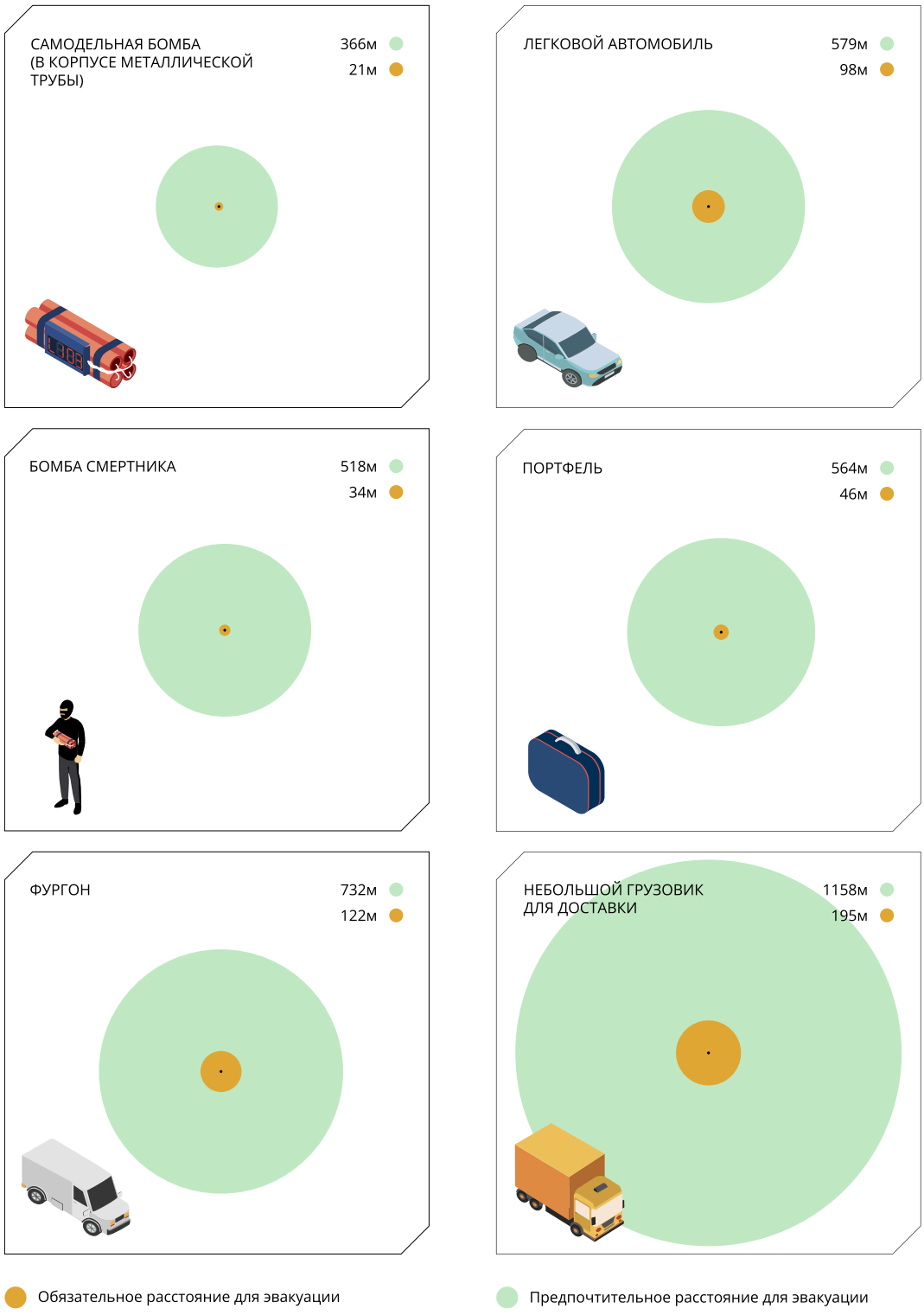
322 Бюро публикаций Европейского союза (2020 г.), *Обзор вычислительных моделей для человеческих травм, вызванных взрывами, для использования в сфере безопасности и обороны.* Доступно по адресу: https://publications.jrc.ec.europa.eu/repository/handle/JRC119310 [дата обращения: 26 июня 2025 г.].

Понимание взрывоопасного потенциала транспортных средств в зависимости от размера поможет владельцам и операторам оценить возможную взрывную силу и определить безопасную дистанцию для парковки.[323] Во многих странах приняты рекомендованные безопасные дистанции до парковки для взрывных устройств разных размеров, что позволяет владельцам/операторам КВИ придерживаться этого стандартизированного подхода. Например, британская инициатива ProtectUK рекомендует следующие минимальные расстояния безопасной дистанции, однако в особых обстоятельствах может потребоваться рассмотреть расстояние до одного километра[324]:

323 Полезная краткая справочная карта по этой теме: Агентство по кибербезопасности и защите инфраструктуры США (без даты), DHS-DOJ Bomb Threat Stand-Off Card [веб-страница]. Доступно по адресу: https://www.cisa.gov/sites/default/files/2025-03/Bomb%20Threat%20Stand-Off%20Card%20Digital%20Final%20v3.0_0.pdf [дата обращения: 21 июля 2025 г.].

324 Национальное управление по борьбе с терроризмом, ProtectUK (без даты, Раздел руководства Purple Guide о борьбе с терроризмом — Планирование атак [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/purple-guide-chapter-counter-terrorism-attack-planning [дата обращения: 10 декабря 2024 г.].

Совместная контртеррористическая группа экспертов по оценке США рекомендует следующие предпочтительные и обязательные расстояния безопасного расстояния, однако в особых обстоятельствах может потребоваться диапазон до одного километра[325]:



325 Совместная контртеррористическая группа экспертов по оценке (JCAT) (без даты), Руководство JCAT по противодействию терроризму для сотрудников служб безопасности. Доступно по адресу: https://www.dni.gov/nctc/jcat/references.html [дата обращения: 21 июля 2025 г.].

В случае угрозы взрыва, исходящего от транспортных средств, необходимо учитывать безопасную дистанцию при проектировании дорог, ворот и парковочных мест для транспортных средств на объекте КВИ и вокруг него, поскольку взрывоопасная угроза может перемещаться с места на место.

В случаях, когда установление разумной безопасной дистанции от объекта, представляющего собой угрозу взрыва, невозможно, может потребоваться укрепление конструкции здания объекта для предотвращения его обрушения в случае взрыва.

Безопасная дистанция также должна быть оперативно установлена компетентным персоналом на объекте КВИ в случае обнаружения подозрительного предмета. Это непосредственно связано с процедурами эвакуации с объекта КВИ, которые должны быть четко определены и отрабатываться на регулярной основе (для получения дополнительной информации см. главу 9 «Подготовка и учения»).

7.4 Планирование безопасности на случай химических, биологических, радиологических и ядерных атак

Хотя это и менее распространенный метод нападения, чем другие, рассматриваемые в этой главе, приобретение, превращение в оружие и использование химических, биологических, радиологических и ядерных (ХБРЯ) материалов террористическими организациями на протяжении десятилетий представляет постоянную угрозу для населения и объектов КВИ. В Консолидированной концептуальной базе для борьбы с терроризмом 2012 года государства-участники ОБСЕ определили незаконный оборот оружия и химических, биологических, радиологических и ядерных материалов в качестве приоритетного направления деятельности ОБСЕ. Это решение было

принято вслед за Решением Совета министров ОБСЕ 2005 года о противодействии угрозе, связанной с радиологическими источниками, в котором подчеркивалась «необходимость защитить человека, общество и окружающую среду от вредных последствий возможных случайных происшествий и злонамеренных актов, связанных с радиоактивными источниками».[326]

Угроза терроризма, связанного с применением ХБРЯ материалов, включает в себя использование в качестве оружия химических веществ, токсичных промышленных химикатов, биологических агентов, токсинов, ядерных и радиологических материалов. В 2021 году Организация Объединенных Наций расследовала использование химических и биологических материалов в террористических целях. Следственная группа ООН по привлечению к ответственности за преступления, совершенные ИГИЛ/Исламским государством Ирака и Леванта (ЮНИТАД) сообщила:

> «Уже имеющиеся доказательства свидетельствуют о том, что в рамках этой программы ИГИЛ испытывала биологические и химические отравляющие вещества и проводила эксперименты над заключенными, что приводило к летальным исходам. Предполагается, что в рамках этой программы исследовались боевые отравляющие вещества кожно-нарывного действия, отравляющие вещества нервно-паралитического действия и токсичные промышленные реагенты. [...] Благодаря этим материалам Группе [ЮНИТАД] удалось установить факт неоднократного применения химического оружия ИГИЛ против гражданского населения в период 2014–2016 годов. Расследования в отношении успешной разработки и использования ИГИЛ созданного собственными силами химического оружия может стать беспрецедентным моментом в плане привлечения к ответственности негосударственных субъектов в условиях современного конфликта».[327]

ХБРЯ материалы, используемые в качестве оружия, бывают разных форм и размеров, поэтому они представляют различные сложности для владельцев/операторов КВИ. Потенциальные инциденты включают в себя, помимо прочего, следующее:

- детонация самодельного радиологического распыляющего устройства;
- детонация самодельного ядерного устройства;
- выброс биологического агента в виде аэрозоля;
- выброс токсичного химического вещества в виде газа;
- загрязнение воды или продуктов питания опасными химическими, биологическими или радиологическими материалами;
- доставка опасного химического, биологического или радиологического материала в письме или посылке.

326 ОБСЕ (2005 г.), Решение Постоянного совета № 683 (PC.DEC/683), Противодействие угрозе радиоактивных источников. Доступно по адресу: https://www.osce.org/files/f/documents/f/c/15923.pdf [дата обращения: 21 июля 2025 г.].

327 СБ ООН (3 мая 2021 г.), Шестой доклад Специального советника и главы следственной группы ООН по содействию привлечению к ответственности за преступления, совершенные ИГ/Исламским государством в Ираке и Леванте (S/2021/419). Доступно по адресу: https://documents.un.org/doc/undoc/gen/n21/104/70/pdf/n2110470.pdf [дата обращения: 21 июля 2025 г.].

Учитывая разнообразие способов доставки, делающих возможным использование ХБРЯ материалов для совершения нападения, в отношении *преднамеренного* выброса таких материалов владельцы/операторы КВИ могут сосредоточить усилия на укреплении базовых мер физической безопасности и мер контроля доступа, обеспечивая при этом принятие мер, специфичных для ХБРЯ материалов, в зонах повышенного риска, таких как отделы корреспонденции отделения и зоны входа/выхода. Меры в отношении *непреднамеренного* выброса ХБРЯ материалов, например, разлива опасных химических веществ, также следует рассматривать в рамках плана действий на случай чрезвычайных ситуаций на объекте КВИ; однако такие меры выходят за рамки настоящего *Технического руководства.*

В конечном итоге, степень, в которой владелец/оператор КВИ уделяет внимание защите от атак с использованием ХБРЯ материалов, должна определяться по согласованию с правоохранительными и другими компетентными органами, которые могут иметь доступ к более актуальной информации и оперативным данным.

ХБРЯ материалы и риски для объектов

Поскольку доступ к ХБРЯ материалам представляет собой проблему для террористических организаций, в некоторых случаях назначение и профиль объекта КВИ могут повышать его привлекательность для террористических организаций. Например, если объект КВИ хранит токсичные химические вещества на своей территории, их использование в террористических целях может быть упрощено, и, следовательно, объект может стать целью как для получения материалов, так и для совершения нападения. Возросший риск террористических атак на химические объекты побудил что Соединенные Штаты разработать Стандарты по борьбе с терроризмом на химических объектах, которые вступили в силу в 2007 году и истекли в 2023 году.[328]

В некоторых случаях, вместо того чтобы совершать нападение на объект КВИ, террористические организации могут вербовать инсайдеров, чтобы они помогли им получить ХБРЯ материалы (подробнее см. главу 8 «Управление внутренними угрозами»).

328 Агентство по кибербезопасности и защите инфраструктуры США (без даты), Ресурсы стандартов по борьбе с терроризмом на химических объектах (CFATS). Доступно по адресу: https://www.cisa.gov/resources-tools/programs/chemical-facility-anti-terrorism-standards-cfats/cfats-resources [дата обращения: 12 декабря 2024 г.].

Владельцам/операторам КВИ следует учитывать привлекательность своего объекта для террористов в рамках оценки рисков, уделяя должное внимание потенциальному доступу к ХБРЯ материалам.

Национальная практика: Руководство по стандартам эффективности, основанным на оценке риска терроризма, для химических предприятий Министерства внутренней безопасности США (2009 г.)[329]

В 2007 году Министерству внутренней безопасности США были предоставлены полномочия по регулированию безопасности на высокорисковых химических объектах. В результате были разработаны правила, устанавливающие требования к химическим объектам, подпадающим под действие Раздела 550 Закона об ассигнованиях на внутреннюю безопасность 2007 года. В их число вошли 18 стандартов эффективности на основе оценки рисков, «которые определяют области, в которых будет проверяться состояние безопасности объекта, такие как безопасность периметра, контроль доступа, гарантии безопасности персонала и кибербезопасность. Чтобы соответствовать этим стандартам эффективности, [владельцы/операторы объектов, подпадающих под действие Закона] могут свободно выбирать любые программы или процессы безопасности, которые они считают целесообразными, при условии достижения требуемого уровня эффективности в каждой применимой области. Программы и процессы, которые в конечном итоге решит внедрить высокорисковый объект для соответствия этим стандартам, должны быть описаны в плане безопасности объекта, который должен разработать каждый высокорисковый химический объект в соответствии с правилами. Именно посредством анализа [плана безопасности объекта] в сочетании с выездной инспекцией [Министерство внутренней безопасности] определит, соответствует ли высокорисковый объект требуемым уровням эффективности, установленным стандартами, с учетом профиля риска объекта».

Источник: Министерство внутренней безопасности США

Физические меры

Для защиты объекта КВИ от террористических атак с использованием ХБРЯ материалов актуальны как минимум две категории физических мер: оборудование для обнаружения ХБРЯ материалов и системы вентиляции воздуха. Это основано на предположении, что на данном объекте реализованы меры на случай взрыва, поскольку ХБРЯ материалы могут быть использованы в качестве оружия в сочетании со взрывчатыми веществами.

Если владельцы/операторы КВИ или компетентные органы оценивают риск со стороны ХБРЯ материалов для объекта как достаточно существенный, они могут счесть необходимым установить оборудование для обнаружения в определенных местах внутри и за пределами периметра объекта (например, входы/выходы, отдела

329 Агентство по кибербезопасности и защите инфраструктуры США (май 2009 г.), *Руководство по стандартам эффективности на основе оценки рисков: стандарты по борьбе с терроризмом на химических объектах.* Доступно по адресу: https://www.cisa.gov/sites/default/files/publications/cfats-rbps-guidance_508.pdf [дата обращения: 21 июля 2025 г.].

корреспонденции, погрузочные платформы и т.д.). Определение места установки такого оборудования должно осуществляться совместно с компетентными органами. Поскольку уровень риска химического терроризма отличается, например, от уровня риска радиологического терроризма, подтверждение потребности объекта в оборудовании обнаружения (включая то, какие материалы оно должно обнаруживать) и выбор подходящего поставщика должны осуществляться по согласованию с компетентными органами. Оборудование должно регулярно проходить испытания в соответствии с рекомендациями органов власти и инструкциями производителя.

Национальная практика: Руководство Национального института охраны труда США по защите зданий от химических, биологических или радиологических атак с распылением веществ[330]

В 2002 году Национальным институтом охраны труда США было выпущено руководство, специально разработанное для борьбы с террористическими атаками с использованием химических, биологических или радиологических (ХБР) материалов на здания и их обитателей. Руководство, предназначенное для владельцев и управляющих зданий, содержит конкретные рекомендации по четырем различным направлениям: (1) что не следует делать; (2) физическая безопасность; (3) вентиляция и фильтрация; и (4) техническое обслуживание, администрирование и обучение. Примеры рекомендаций представлены ниже:

- Для предотвращения доступа террористов на объект необходимо обеспечить физическую защиту входа, складских помещений, крыши и технических помещений, а также обеспечить доступ к наружным воздухозаборникам системы отопления, вентиляции и кондиционирования воздуха (ОВиК) здания.
- Некоторые меры физической безопасности, такие как запирание дверей в технические помещения, не требуют больших затрат и не создадут неудобств пользователям здания. Такие меры могут быть реализованы в большинстве зданий. Другие меры физической безопасности, такие как увеличение численности персонала службы безопасности или рентгеновское оборудование для досмотра посылок, требуют больших затрат или могут создавать существенные неудобства пользователям. Эти меры следует применять, когда они являются оправданными с учетом анализа угрозы и последствий террористической атаки.
- Системы ОВиК и их компоненты следует оценивать с точки зрения их влияния на уязвимость к проникновению ХБР веществ. К соответствующим вопросам относятся управление системой ОВиК, способность системы ОВиК очищать воздух в здании, эффективность установленных фильтров, пропускная способность системы с учетом возможной установки дополнительных фильтров и последствия неконтролируемой утечки в здание.

Источник: Национальный институт охраны труда США

330 Национальный институт охраны труда (NIOSH) (без даты), Руководство по защите зданий от химических, биологических или радиологических атак [веб-страница]. Доступно по адресу: https://www.cdc.gov/niosh/engcontrols/ecd/detail147.html [дата обращения: 12 декабря 2024 г.].

Материалы ХБРЯ, используемые террористами в качестве оружия, могут распыляться в воздухе, поэтому необходимо уделить должное внимание соответствующим системам вентиляции воздуха, если владельцы/операторы КВИ или компетентные органы оценивают риск использования ХБРЯ материалов как достаточно существенный. При этом необходимо оценить как способность системы фильтровать опасные частицы, так и способность владельцев/операторов КВИ быстро уменьшать/отключать вентиляцию воздуха в определенных частях здания. Например, учитывая риск попадания материала ХБРЯ на объект КВИ через его отдел корреспонденции, возможность немедленного отключения вентиляции воздуха из этого помещения в остальную часть объекта может иметь важное значение для предотвращения распространения ХБРЯ материала. В некоторых случаях можно рассмотреть возможность установки отдельной системы вентиляции воздуха для этого помещения. Владельцам/операторам КВИ следует рассмотреть вопрос усиления мер безопасности вокруг мест забора воздуха, поскольку они могут быть потенциальными местами атак террористической организации.

ХБРЯ материалы, используемые террористами в качестве оружия, также могут переноситься через воду. Поэтому следует рассмотреть меры, направленные на контроль доступа к жизненно важным источникам воды на объекте КВИ, мониторинг качества воды и обеспечение надежной и быстрой идентификации патогенов или других токсичных веществ в источниках воды.[331]

Обеспечение готовности персонала

Учитывая разнообразие ХБРЯ материалов и их различное воздействие на человека, обобщение точных показателей воздействия является сложной задачей. Тем не менее, есть некоторые признаки, которые персоналу объектов КВИ следует знать, как указано Национальным управлением по защите и безопасности Великобритании:

> «Необъяснимые физические симптомы, такие как: раздражение глаз и кожи, подергивание мышц и судороги, дезориентация и потливость, раздражение дыхательных путей и затрудненное дыхание, тошнота и рвота.
>
> Другие признаки, такие как: недееспособность двух или более человек без объяснимой причины, наличие необычных/оставленных без присмотра материалов, устройств или оборудования, необъяснимые испарения, облака тумана, порошок, жидкости или маслянистые капли, необъяснимые запахи или привкусы, увядшие растения или растительность, необычное поведение птиц или животных.
>
> Некоторые симптомы могут проявляться быстро, указывая на то, что в настоящее время происходит атака. Однако в некоторых случаях признаки и симптомы могут

331 Теохариду, М.; Джаннопулос, Г. (ред.) (2019 г.), *Технические отчеты совместной исследовательской группы: Руководство по разработке плана обеспечения безопасности водоснабжения для питьевого водоснабжения* (Люксембург: Бюро публикаций Европейского союза). Доступно по адресу: https://erncip-project.jrc.ec.europa.eu/sites/default/files/2019.4805_EN_JRC116548.pdf [дата обращения 21 июля 2025 г.]; Коэльо, М.Р.; Батлье Рибас, М.Ф.; Коимбра, М.Ф. (2020 г.), *Технические отчеты совместной исследовательской группы: Обзор технологий быстрого обнаружения химических и биологических загрязнителей в питьевой воде* (Люксембург: Бюро публикаций Европейского союза). Доступно по адресу: https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC119994_2020.1117_en_jrc119994.pdf [дата обращения: 21 июля 2025 г.].

не проявляться в течение нескольких дней после инцидента, и ранние симптомы могут быть ошибочно приняты за симптомы обычной простуды или гриппа.

В таких случаях мониторинг характера заболеваемости персонала для выявления отклонений, например, большого количества больных сотрудников, может помочь в выявлении подобных инцидентов».[332]

Последнее предложение стоит особо подчеркнуть, поскольку для персонала объектов КВИ может быть неочевидно, почему их координаторы по безопасности должны знать о состоянии их здоровья. Без регулярного информирования координатора по безопасности объекта о состоянии здоровья персонала сложно выявить закономерности, которые могут указывать на продолжающуюся атаку с использованием ХБРЯ. Это требует более широкого обсуждения вопроса защиты личной информации персонала объектов КВИ и может потребовать консультаций с компетентными органами.

Отделы корреспонденции объектов КВИ могут быть первым местом доставки химических или биологических материалов, таких как споры сибирской язвы, поэтому персонал этих отделов должен знать, как реагировать на такие угрозы. Владельцы/операторы КВИ могут проводить регулярное обучение такого персонала и разрабатывать краткие справочные плакаты для отделов корреспонденции с четкими и краткими инструкциями по реагированию на инциденты, связанные с подозрительными предметами.

332 Национальное управление по защите и безопасности Великобритании (2024 г.), *Подготовка и реагирование на химически, биологически или радиологически опасные инциденты (CBR): руководство для менеджеров по безопасности по снижению воздействия ХБР инцидента.* Доступно по адресу: https://www.npsa.gov.uk/resources/official-cbr-security-managers-guide [дата обращения: 21 июля 2025 г.].

Национальная практика: Руководство Великобритании ProtectUK по обработке почты в общедоступных местах (2022 г.)[333]

Избегайте ненужных манипуляций и рентгеновского облучения:

Если вы держите предмет, положите его на чистую ровную поверхность и:

- пусть лежит отдельно, чтобы его было легко идентифицировать
- не перемещайте его, даже в рентгеновский аппарат
- если он находится в рентгеновском кабинете, оставьте его там

Немедленно покиньте помещение:

- удалите людей из прилегающей зоны и каждой смежной комнаты, включая комнаты выше и ниже
- в случае подозрения на наличие химических, биологических или радиологических материалов, переместите непосредственно контактировавших в безопасное место недалеко от места инцидента, держите этих людей отдельно от тех, кто не подвергался воздействию
- не допускайте приближения или доступа других лиц к освобожденным помещениям
- не пользуйтесь мобильными телефонами или рациями в освобожденных помещениях или в пределах пятнадцати метров от подозрительной посылки
- регулярно доводите информацию до персонала, посетителей и общественности

Уведомите полицию:

- если предмет был вскрыт или частично вскрыт до того, как его сочли подозрительным, крайне важно сообщить об этом в полицию
- и обеспечьте доступность информаторов и свидетелей для информирования полиции и достоверность их показаний. Призывайте свидетелей немедленно зафиксировать свои наблюдения в письменном виде и не позволяйте им обсуждать инцидент или свои наблюдения с другими до прибытия полиции

Дополнительные действия, специфичные для ХБР инцидента:

- если есть подозрение на инцидент с ХБР материалами, то как можно быстрее проведите импровизированную дезактивацию зараженных людей, в идеале в течение первых 15 минут
- в случае возникновения инцидента с ХБР материалами рекомендуется не использовать лифты для перемещения или эвакуации из здания
- если изменение функционирования системы [отопления, вентиляции и кондиционирования воздуха] предусмотрено вашим планом реагирования [...], это следует осуществить как можно быстрее

Источник: Национальное управление по борьбе с терроризмом Великобритании

333 Национальное управление по борьбе с терроризмом, ProtectUK (1 марта 2022 г.), Руководство по местам проведения мероприятий и общественным пространствам (VaPS). Обработка почты [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/mail-handling [дата обращения: 12 декабря 2024 г.].

Дополнительным и важным компонентом обеспечения готовности персонала на объекте КВИ является обеспечение достаточных и доступных запасов подходящих средств индивидуальной защиты.

Планирование мер по управлению кризисными ситуациями, связанными с ХБРЯ материалами

Владельцам/операторам объектов КВИ рекомендуется включать инциденты, связанные с ХБРЯ материалами, в свои планы действий по управлению кризисными ситуациями, поскольку террористическая атака с использованием ХБРЯ материалов принципиально отличается от террористической атаки с использованием огнестрельного оружия или взрывного устройства.

Поэтому планы действий по управлению кризисными ситуациями (включая планы эвакуации или укрытия на месте), разработанные для других форм террористических атак, могут быть неприменимы к инциденту с использованием ХБРЯ материалов. Например, в случае выброса токсичного химического газа на первом этаже объекта КВИ, использование лифта для эвакуации на верхние этажи может создать эффект, при котором опасный газ затягивается на верхние этажи.[334] Это контрастирует с использованием лифта во время инцидента со стрельбой, когда может быть целесообразно использовать лифт в качестве средства для спасения от угрозы на определенном этаже. Для принятия решений в этом отношении может быть полезным моделирование рассеивания в атмосфере для атак с использованием ХБРЯ материалов. Кроме того, если особые меры по эвакуации или укрытию на месте считаются необходимыми в случае нападения с использованием ХБРЯ материалов, средства индивидуальной защиты должны быть легкодоступны для персонала.

При оценке риска террористических атак с использованием ХБРЯ материалов на объектах следует учитывать тот факт, что ХБРЯ атака может привести к массовым жертвам (как немедленным, так и отсроченным). При успешном осуществлении атака с использованием отравляющего химического газа или биологического агента может за короткий период времени полностью подавить возможности медицинских служб объекта и местных служб экстренной помощи. Подготовка к такой угрозе, если владельцы/операторы КВИ и компетентные органы сочтут это необходимым, требует тесного и скоординированного участия служб экстренной помощи и быстрого реагирования в рамках плановых учений по реагированию на кризисные ситуации, связанные с ХБРЯ материалами.

334 Национальное управление по защите и безопасности Великобритании (2024 г.), *Подготовка и реагирование на химические, биологические или радиологически опасные инциденты (CBR): руководство для менеджеров по безопасности по снижению воздействия CBR-инцидента.* Доступно по адресу: https://www.npsa.gov.uk/resources/official-cbr-security-managers-guide [дата обращения: 21 июля 2025 г.].

Национальная практика: Руководство Великобритании ProtectUK по защите от химических, биологических и радиационных атак в общедоступных местах (2022 г.)[335]

Надлежащие общие меры физической безопасности и защиты персонала помогут сократить воздействие ХБР инцидентов. Применяйте соответствующие стандарты безопасности персонала к подрядчикам и посетителям, особенно к тем, кто часто посещает ваш объект.

Реализация полной защиты от ХБР материалов может быть чрезвычайно дорогостоящей, однако некоторые меры, которые помогут снизить последствия ХБР события, можно реализовать с относительно небольшими затратами.

Для повышения устойчивости к ХБР атакам рекомендуются следующие первые шаги:

- пересмотреть меры физической безопасности, относящиеся к тем участкам здания, которые в силу своего назначения, например, входы, выходы и окна, могут подвергаться повышенному риску нападения
- пересмотреть конструкцию и физическую безопасность систем обработки воздуха, например, доступ к воздухозаборникам и воздуховыпускным отверстиям, избегая использования воздухозаборников на уровне земли или вблизи нее
- включить меры реагирования на ХБР события в планы действий на случай крупных инцидентов на объекте
- включить меры реагирования на ЧМ-опасные ситуации в планы действий на случай крупных инцидентов.
- продумать пути эвакуации
- рассмотреть возможность использования заранее подготовленных сообщений
- при необходимости установить дополнительные воздушные фильтры или модернизировать системы ОВиК.
- ограничить доступ к резервуарам с водой и другим ключевым коммуникациям
- пересмотреть безопасность ваших цепочек поставок продуктов питания и напитков
- рассмотреть необходимость принятия специальных мер для обработки почты или посылок, например, выделить отдельное помещение для отдела корреспонденции, возможно, с выделенной вентиляционной системой, или даже организовать специализированное помещение за пределами объекта, учитывая, что отделы корреспонденции могут быть зоной повышенного риска

Источник: Национальное управление по борьбе с терроризмом Великобритании

335 Национальное управление по борьбе с терроризмом, ProtectUK (1 марта 2022 г.), Руководство по объектам и общественным пространствам (VaPS) Химические, биологические и радиологические (CBR) атаки [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/chemical-biological-and-radiological-cbr-attacks [дата обращения: 12 декабря 2024 г.].

7.5 Планирование мер безопасности на случай нападения с применением огнестрельного оружия

Террористические атаки с применением огнестрельного оружия происходят по всему миру и требуют схожих мер реагирования независимо от страны. Их часто называют мародерскими террористическими атаками или нападениями со стрельбой. Это стремительно развивающиеся инциденты, в которых нападающие, вооруженные огнестрельным оружием (а иногда и взрывными устройствами), перемещаются по объекту или территории с различными целями, включая убийство или ранение как можно большего числа людей или доступ к определенным местам.[336] Террористические атаки с применением огнестрельного оружия могут варьироваться от одиночных до групповых. Это создает широкий спектр проблем для объекта КВИ. Поскольку огнестрельное оружие часто легкодоступно, не требует сложных цепочек поставок или обширных технических знаний (в отличие от ХБРЯ оружия или СВУ) и требует ограниченной подготовки для обращения с ним, оно остается распространенным способом совершения нападений для террористических организаций и других субъектов угроз.

В некоторых случаях рекомендации в этом разделе больше связаны с *реагированием* на применение огнестрельного оружия, а не с повышением физической защищенности объекта от этой угрозы. Хотя это может выходить за рамки вопросов физической безопасности, планирование мер реагирования, тем не менее, является частью эффективной системы безопасности для любого объекта КВИ.[337]

336 Определение адаптировано из публикации Национального управления по защите и безопасности Великобритании (июнь 2023 г.), *Введение в стандарт мародерских террористических атак (MTAS)*. Доступно по адресу: https://www.npsa.gov.uk/resources/introduction-marauding-terrorist-attack-standard-mtas [дата обращения: 21 июля 2025 г.].

337 См. также: *Технические руководящие принципы по содействию осуществлению резолюции 2370 (2017 г.) Совета Безопасности и связанных с ней международных стандартов и передовой практики по предотвращению приобретения оружия террористами,* опубликованные КТУ ООН, Исполнительным директоратом Контртеррористического комитета Совета Безопасности ООН, Институтом ООН по исследованию проблем разоружения и Глобальным договором ООН о координации контртеррористической деятельности.

Предварительные меры, принимаемые до атаки

Владельцы/операторы КВИ могут принять меры для лучшей подготовки объекта КВИ к террористическим атакам с использованием огнестрельного оружия или даже для предотвращения подобных атак со стороны злоумышленников. К таким мерам относятся, помимо прочего:

- Установка системы видеонаблюдения на территории объекта, которая позволит выявлять подозрительных лиц, в том числе лиц, проводящих разведку перед атакой;
- Формирование культуры безопасности среди всего персонала, в том числе посредством обучения и регулярных инструктажей с участием местных экстренных служб и правоохранительных органов;
- Регулярное патрулирование территории (если это разрешено национальными и местными законами) и внутри объекта;
- Применение мер контроля доступа и досмотров;
- При необходимости усиление физической защиты окон, дверей, ставен и жалюзи для защиты от взлома и стрельбы;
- Рассмотрение мер, которые позволяют компетентному персоналу обеспечивать безопасность или блокировать критически важные части объекта или здания КВИ, мер, которые могут либо предотвратить доступ злоумышленников, либо сдержать их, позволяя персоналу отойти в укрытие;
- Определение путей эвакуации для каждого здания на территории КВИ; на каждом объекте должно быть не менее двух путей эвакуации;
- Внедрение двух различных типов тревожных сигналов и связанных с ними процедур на объекте КВИ: одного для общих вопросов безопасности (например, эвакуация из-за пожара) и одного на случай нападения (например, активный стрелок или внешняя атака);
- Проведение плановых учений для всего персонала с участием местных аварийно-спасательных служб и правоохранительных органов, имитирующих террористическую атаку с применением огнестрельного оружия, чтобы персонал объекта был осведомлен о процедурах эвакуации/укрытия/блокировки;
- Привлечение/поощрение местных экстренных служб и правоохранительных органов к проведению обучения по реагированию на террористические атаки с применением огнестрельного оружия на объекте КВИ;
- Разработка плана действий для объекта КВИ и его персонала на случай террористического акта с применением огнестрельного оружия.

Национальная практика: комплект материалов Агентства по кибербезопасности и защите инфраструктуры США по планированию экстренных действий на случай нападения активного стрелка[338]

В 2025 году Агентство по кибербезопасности и защите инфраструктуры США (CISA) разработало шаблон плана действий в чрезвычайных ситуациях, связанных с активным стрелком, и соответствующее учебное руководство «для помощи организациям и объектам критически важной инфраструктуры в разработке всеобъемлющего и реализуемого плана действий в чрезвычайных ситуациях. Это руководство содержит рекомендации, помогающие пользователям заполнять каждый раздел шаблона плана действий в чрезвычайных ситуациях, и включает примеры и дополнительные ресурсы для разработки эффективного плана». В учебном руководстве описаны шаги по подготовке к инцидентам со стрельбой, такие как, *в частности*, определение ключевых ролей и обязанностей группы планирования действий в чрезвычайных ситуациях на объекте КВИ, разработка и предоставление этажных планов персоналу и службам быстрого реагирования, принятие мер по обеспечению готовности к экстренному доступу на объект (например, приглашение местных правоохранительных органов и служб быстрого реагирования для участия в ежегодных посещениях объекта), определение процедур эвакуации, блокировки и укрытия на месте, разработка планов обеспечения непрерывности деятельности и планирование периода восстановления после инцидента.

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры

Обеспечение готовности персонала

Помимо принятия упреждающих мер по предотвращению и подготовке к террористической атаке с применением огнестрельного оружия, необходимо донести до персонала правила надлежащего поведения в случае атаки. В кризисной ситуации многие сотрудники объектов, особенно те, у кого ограниченный опыт действий в чрезвычайных ситуациях, могут быть неспособны ясно мыслить или действовать, что может подвергнуть опасности их самих и/или их коллег. В целях содействия эффективному принятию решений во время террористических атак многие государства-участники ОБСЕ разработали краткие кампании по повышению осведомленности для широкой общественности. Владельцы/операторы КВИ могут адаптировать эти кампании и использовать их для персонала своих объектов:

338 Агентство по кибербезопасности и защите инфраструктуры США (2023 г.), *Рабочая тетрадь по планированию безопасности*. Доступно по адресу: https://www.cisa.gov/resources-tools/resources/security-planning-workbook [дата обращения 21 июля 2025 г.]; Агентство по кибербезопасности и защите инфраструктуры США (2025 г.), Пакет продуктов для экстренных действий по активному нападающему-стрелку [веб-страница]. Доступно по адресу: https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite [дата обращения 21 июля 2025 г.].

- Кампания Министерства внутренней безопасности США: «Беги, прячься, борись»;[339]
- Французская кампания Vigipirate: «Беги, прячься, предупреждай, борись, облегчай доступ правоохранительным органам и экстренным службам»;[340]
- Кампания Национального управления по борьбе с терроризмом Великобритании: «Беги, прячься, расскажи».[341]

Меры, принимаемые после атаки

Планирование террористической атаки с использованием огнестрельного оружия должно быть в значительной степени сосредоточено на способах предотвращения таких атак и подготовки к ним. Тем не менее, следует также уделять внимание немедленным и долгосрочным последствиям атаки для персонала объекта КВИ и их семей. Управление этими последствиями должно быть частью любого плана действий в чрезвычайных ситуациях, разработанного для объекта КВИ. Особое внимание следует уделить следующим мерам:

Сразу после нападения	▸ Учет всего персонала в назначенном пункте сбора объекта КВИ для выявления без вести пропавших и потенциально пострадавших. ▸ Определение способа оповещения семей сотрудников, пострадавших в результате нападения, включая уведомление о смерти.
Через несколько дней, недель и месяцев нападения	▸ Проведение оценки психологического состояния сотрудников, присутствовавших при нападении (включая тех, кто не присутствовал, но может страдать от горя, утраты или чувства вины выжившего) и направление их к соответствующим медицинским и психологическим специалистам, если это необходимо. ▸ Выявление и заполнение критически важных кадровых позиций или оперативных пробелов, образовавшихся в результате нападения. ▸ Разработка коммуникационной стратегии, в которой открыто указываются пробелы в системе безопасности во время нападения и сообщается о конкретных действиях, которые предпринимаются для улучшения, при поддержке высшего руководства.

339 Агентство по кибербезопасности и защите инфраструктуры США (2022 г.), Карманная карта на случай стрельбы. Доступно по адресу: https://www.cisa.gov/resources-tools/resources/active-shooter-pocket-card [дата обращения: 21 июля 2025 г.].

340 Генеральный секретариат обороны и национальной безопасности (SGDSN), *Guide des Bonnes Pratiques pour la Sûreté des Espaces Publics.* Доступно по адресу: https://www.sgdsn.gouv.fr/files/files/Publications/guide-unique-de-sensibilation-vigipirate-pact-num-v7.pdf [дата обращения: 21 июля 2025 г.] неофициальный перевод.

341 Национальное управление по борьбе с терроризмом, ProtectUK (2 сентября 2021 г.), Run Hide Tell. Доступно по адресу: https://www.protectuk.police.uk/sites/default/files/2023-12/Marauding%20Attacker%20Action%20Card.pdf [дата обращения: 21 июля 2025 г.].

7.6 Планирование мер безопасности на случай захвата заложников

Террористические организации и другие субъекты угроз могут использовать захват заложников как часть атаки на КВИ, чтобы получить рычаги влияния и привлечь внимание к своим требованиям. Объекты КВИ часто имеют высокую стратегическое и символическое значение. Захватывая заложников в этих местах, субъекты угроз могут попытаться принудить правительства или владельцев/операторов КВИ вступить в переговоры, создавая ощущение безотлагательности по причине возможной гибели людей и/или нарушения работы критически важных служб. Захват заложников может привлечь внимание СМИ и вызвать целый спектр эмоций у широкой общественности. Давление со стороны общественности с целью обеспечения безопасности заложников и предотвращения дальнейшего ущерба может нарастать, что может подталкивать власти/заинтересованные стороны к выполнению требований или согласия на ту или иную форму переговоров. По этой причине на международном уровне проблеме захвата заложников уделяется значительное внимание.

Международная конвенция о борьбе с захватом заложников

Международная конвенция о борьбе с захватом заложников была принята Генеральной Ассамблеей Организации Объединенных Наций в 1979 году Резолюцией A/RES/34/146 и вступила в силу в 1983 году. В настоящее время ее подписали 39 государств и 176 участников.[342] В Конвенции приводятся определения преступлений захвата заложников, попытки захвата заложников и соучастия в захвате заложников. В соответствии с пунктом 1 статьи 1, преступление захвата заложников совершается: «любым лицом, которое захватывает или удерживает другое лицо и угрожает убить, нанести повреждение или продолжать удерживать другое лицо [...] для того чтобы заставить третью сторону, а именно: государство, международную межправительственную организацию, какое-либо физическое или юридическое лицо или группу лиц — совершить или воздержаться от совершения любого акта в качестве прямого или косвенного условия для освобождения заложника».[343]

Захват заложников является уникальной формой нападения, используемой террористами в отношении объектов КВИ. Хотя основное внимание в настоящем *Техническом руководстве* уделяется мерам физической безопасности, данный раздел выходит за рамки этих мер и содержит общие рекомендации по эффективным мерам и соображениям для подготовки к ситуациям с захватом заложников и реагирования на них.

342 Организация Объединенных Наций, Международная конвенция о борьбе с захватом заложников. Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/hostages.shtml [дата обращения: 21 июля 2025 г.].

343 Организация Объединенных Наций, Международная конвенция о борьбе с захватом заложников. Доступно по адресу: https://www.un.org/ru/documents/decl_conv/conventions/hostages.shtml [дата обращения: 21 июля 2025 г.].

Учитывая деликатный характер этой темы, количество общедоступных передовых практик ограничено. Действия, необходимые в любой конкретной ситуации захвата заложников, также зависят от контекста. Однако, поскольку захват заложников представляет собой реальную угрозу безопасности объектов КВИ и их персонала, в данном разделе представлены общие рекомендации и соображения, которые помогут лицам, принимающим решения, при планировании на случай подобных атак.

Практический пример: террористическая атака, связанная с «Аль-Каидой», и захват заложников на газодобывающем комплексе в Ин-Аменасе, Алжир (2013 г.)[344]

16 января 2013 года на газодобывающем предприятии Тигентурин в Ин-Аменасе (Алжир) произошел теракт с захватом заложников. Разработка газового месторождения Ин-Аменас осуществлялась совместным предприятием алжирской национальной нефтяной компании, Sonatrach, British Petroleum и Statoil. На момент нападения на объекте работали 800 человек, 130 из которых были приезжими из 30 стран. В нападении участвовали 32 хорошо вооруженных террориста, и оно продолжалось несколько дней. Оно началось с нападения на автобус и сопровождавшую его колонну в 300 метрах от жилой зоны объекта, после чего последовали одновременные атаки на жилую и газодобывающую зоны объекта. Объект перешел под контроль террористов в течение 15 минут.

В течение многодневного удерживания заложников террористы поддерживали связь с компаниями Statoil и British Petroleum и выдвинули несколько требований, включая освобождение известных заключенных в тюрьмах США и Алжира. В результате нескольких дней противостояния было убито 40 невинных людей, погибли 29 из 32 террористов. К 17 января алжирские военные восстановили контроль над объектом. Многим выжившим заложникам были нанесены не только физические травмы, но и психологический ущерб от пережитого.

После атаки были проведены официальные расследования, каждое из которых было направлено на разработку рекомендаций, которые бы улучшили понимание и повлияли на будущую готовность и реагирование на подобные атаки. Ниже приведены отдельные наблюдения из отчета о расследовании, подготовленного для Совета директоров Statoil:

- **Многоуровневая безопасность.** Эксперты-следователи подчеркнули важность применения комплексного подхода к обеспечению безопасности на объекте в Ин-Аменасе, призванного гарантировать, что каждый уровень защитной безопасности дает возможности (1) обнаружить начало нападения, (2) задержать нападающих и (3) обеспечить достаточно времени для реализации ответных мер, прежде чем нападающие успеют нанести еще больший вред. В частности, были даны следующие рекомендации:

344 Statoil (2013 г.), *Атака в Ин-Аменас. Отчет о расследовании террористического нападения на Ин-Аменас. Подготовлено для Совета директоров Statoil ASA.* Доступно по адресу: https://www.equinor.com/news/archive/2013/09/12/downloads/In%20Amenas%20report.pdf [дата обращения: 21 июля 2025 г.].

a. включить базовую подготовку по безопасности для всех сотрудников на объекте и специализированную подготовку по безопасности для менеджеров и международного персонала, а также
b. открыто и четко сообщать о потенциальных рисках безопасности сотрудникам объекта, определив взаимные ожидания между оператором и его персоналом в отношении друг друга.

- **Тестирование и учения.** Эксперты-следователи призвали лиц, ответственных за безопасность объекта, чаще проводить тестирование и учения, связанные с безопасностью, а также координировать/стандартизировать планирование реагирования на чрезвычайные ситуации во всех сферах деятельности.
- **Управление рисками и оценка рисков.** Эксперты-следователи рекомендовали разработать динамичную и целевую систему управления рисками безопасности. Кроме того, они призвали к поддержанию планов управления рисками безопасности, включающих определенные сценарии, связанные с безопасностью.

Источник: Statoil

Подготовка к ситуациям захвата заложников на объектах критически важной инфраструктуры

Владельцы/операторы КВИ должны быть готовы к ситуациям захвата заложников на своих объектах, чтобы обеспечить как безопасность персонала, так и защиту критически важных служб объекта. Ниже приведено несколько важных соображений, которые следует принимать во внимание в рамках этого процесса.

Обеспечение повышенной готовности. Одним из аспектов готовности в этом контексте является оценка вероятности возникновения подобного инцидента. Такая оценка может проводиться владельцами/операторами КВИ в рамках их процесса управления рисками. Например, в Великобритании ведется национальный реестр рисков, в котором упоминается «стратегический захват заложников», в том числе террористами.[345] Этот национальный реестр рисков оценивает как последствия, так и вероятность подобных событий, позволяя владельцам/операторам КВИ планировать и готовить меры безопасности, планы реагирования на кризисные ситуации и программы обучения персонала для управления такими событиями, оперативного реагирования на угрозы и минимизации ущерба. В случаях, когда такое национальное руководство отсутствует, владельцы/операторы КВИ могут оценить вероятность ситуации с захватом заложников на своем объекте совместно с правоохранительными органами.

Обеспечение мер безопасности в ситуациях захвата заложников. Для обеспечения быстрой и незаметной коммуникации между персоналом надлежащим подходом в подготовке к ситуациям захвата заложников является использование кодового слова и выделение специального безопасного места на объекте КВИ. Кодовые слова служат своеобразным сигналом тревоги для лиц, находящихся на объекте. Когда кто-то находится в опасности или подозревает, что имеет место захват заложников, кодовое слово можно незаметно передать, чтобы предупредить других, не нагнетая обстановку

345 Правительство Ее Величества (2023 г.), *Национальный реестр рисков: издание 2023 г.,* стр. 39–40. Доступно по адресу: https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf [дата обращения: 21 июля 2025 г.].

и не привлекая внимания к угрозе. Крайне важно, чтобы кодовое слово было легко запоминающимся и достаточно отличалось от повседневной речи, чтобы свести к минимуму двусмысленность. Весь персонал объекта должен быть проинформирован о кодовом слове, его значении и соответствующих процедурах, которым необходимо следовать при его использовании.

Наряду с кодовым словом, на территории объекта должно быть выделено специальное безопасное место, часто называемое «укрытием» или «цитаделью» в морском секторе.[346] Это место должно быть безопасным, легкодоступным и физически защищенным от потенциальных угроз. Убежище должно вмещать определенное количество людей и иметь средства связи с правоохранительными органами или аварийно-спасательными службами. Для повышения эффективности убежище может быть оснащено предметами первой необходимости, такими как аптечки первой помощи, резервные запасы питания и средства связи. В зависимости от рекомендаций компетентного персонала объекта КВИ, таким убежищем может быть то же помещение, что и пункт сбора при эвакуации, описанный далее в этой главе. Однако это не всегда так, поскольку они служат разным целям.

Формирование культуры безопасности среди персонала. Способность персонала объекта КВИ выявлять и распознавать потенциальные угрозы, включая развивающуюся атаку, которая может привести к захвату заложников, является ключевым фактором эффективной готовности. Необходимо поощрять персонал объекта КВИ сохранять бдительность и сообщать о любой подозрительной активности назначенным координаторам по вопросам безопасности.

Организация обучения персонала. Развитие навыков персонала объекта КВИ для эффективного реагирования на высоко стрессовые ситуации, такие как ситуация захвата заложников, повышает их осведомленность о ситуации и снижает панику. Регулярные тренировки и учения для всего персонала объекта КВИ имеют решающее значение для обеспечения понимания каждым сотрудником, среди прочего, кодового слова и маршрута к безопасному месту. Для более крупных объектов определение нескольких безопасных зон расширяет возможности для спасения персонала, пытающегося укрыться от опасности.

Реагирование на ситуации захвата заложников и управление ими

При реагировании на ситуацию захвата заложников приоритет должен быть отдан сохранению жизни. Другие цели включают в себя разрешение инцидента с минимальным применением силы и сбор информации о мотивах захватчиков, если они не были очевидны. В большинстве ситуаций захвата заложников на объекте КВИ будут задействованы государственные органы, и они будут руководить мерами реагирования. Однако могут быть ситуации, когда государственные органы недоступны или находятся в пути (например, в случае удаленных нефтегазовых объектов). Поэтому владельцы/операторы КВИ могут быть непосредственно вовлечены в процесс немедленного реагирования и управление ситуацией с захватом заложников и, следовательно, должны быть соответствующим образом

346 Балтийский и международный морской совет (BIMCO) и др. (2018 г.), Глобальное руководство по борьбе с пиратством для компаний, капитанов и моряков (Livingston: Witherbys Publishing Group). Доступно по адресу: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/global-counter-piracy-guidance-bmp_low_17-07-18.pdf [дата обращения: 21 июля 2025 г.].

подготовлены. При этом любое участие владельца/оператора КВИ в реагировании на ситуацию захвата заложников и ведении переговоров должно координироваться и согласовываться с местными органами власти. Ниже приведено несколько важных соображений, которые необходимо учитывать в рамках этого процесса.

Участие в переговорах в кризисных ситуациях. Переговоры в кризисных ситуациях являются важнейшим компонентом управления ситуациями захвата заложников. Они требуют взаимодействия опытных переговорщиков с захватчиками. С этим процессом связано множество нюансов, и он требует особых навыков общения, эмпатии и убеждения. Эффективные переговорщики устанавливают контакт с захватчиками, собирают ключевые сведения (включая информацию о требованиях, состоянии заложников или психологическом состоянии захватчиков – факторы, которые могут повлиять как на реакцию властей, так и на действия захватчиков), и стремятся снизить напряженность. К полезным методам относятся:

- *Активное слушание:* демонстрация понимания и участия может способствовать установлению доверия;
- *Создание диалога:* открытые вопросы побуждают захватчиков озвучивать свои мотивы;
- *Предложение вариантов:* вместо ультиматумов переговорщики могут предлагать возможные решения, которые удовлетворят потребности захватчика и одновременно обеспечат безопасность заложников.

Подготовка к тактическому взаимодействию. Хотя переговоры крайне важны, существуют ситуации, в которых может потребоваться тактическое вмешательство компетентных органов. Обычно это выходит за рамки полномочий владельцев/операторов КВИ и более актуально для местных властей и правоохранительных органов. Тактические группы компетентных органов, скорее всего, обучены проводить спасательные операции в случае провала переговоров или непосредственной угрозы заложникам. Тактические группы могут сотрудничать с владельцами/операторами КВИ для сбора информации в режиме реального времени о планировке объекта КВИ, местонахождении заложников, количестве захватчиков и состоянии заложников, а также для определения того, когда следует действовать. В таких случаях владельцам/операторам КВИ важно предоставлять запрашиваемую информацию в меру своих возможностей, обеспечивая тактическим группам и другим соответствующим субъектам надежную основу для их работы.

Обеспечение психологической поддержки. Как во время, так и после инцидента с захватом заложников, крайне важно осознавать психологическое воздействие на заложников и их семьи. После инцидента заложники могут испытывать травму. По этой причине психологическая поддержка может быть включена в меры по реагированию как компетентными органами, так и владельцем/оператором КВИ, включая оказание медицинской помощи и оценку психического здоровья заложников сразу после их освобождения, а также обеспечение эффективной коммуникации с семьями заложников на протяжении всего инцидента. Такая коммуникация способствует поддержанию эмоциональной стабильности всех участников инцидента. При необходимости эти услуги могут также могут быть предоставлены и другим сотрудникам.

Проведение анализа после инцидента. После разрешения ситуации захвата заложников важное значение для оценки эффективности реагирования имеет проведение тщательного анализа. Будет установлено четкое разделение между компетенцией владельца/оператора КВИ и задействованных компетентных органов. Этот анализ может включать в себя применяемые стратегии и тактику переговоров и тактические стратегии, оказанную психологическую поддержку и аспекты работы, требующие улучшения, которые следует учесть при принятии мер реагирования в будущем. Кроме того, проведение анализа после инцидента может помочь выявить непредвиденные проблемы и меняющиеся модели угроз, чтобы гарантировать, что эти знания будут учтены в будущих программах обучения, тем самым повышая готовность и снижая вероятность возникновения подобных инцидентов в будущем.

7.7 Планирование эвакуации, укрытия и изоляции

В случае активной угрозы объекту КВИ обеспечение безопасности персонала должно быть наивысшим приоритетом. В таких ситуациях для персонала существуют три варианта действий: эвакуация, следование в укрытие или изоляция (укрытие на месте).

Эвакуация

Укрытие

Изоляция

Эвакуация – это процесс перемещения персонала за пределы здания или объекта в сторону от активной угрозы. Следование в укрытие – это процесс перемещения персонала внутри здания или объекта в сторону от активной угрозы. В определенных обстоятельствах может быть целесообразнее переместить персонал в безопасное место внутри объекта, чем эвакуировать его наружу. Один из возможных сценариев, в котором этот вариант может применяться, – присутствие угрозы взрыва с возможностью использования вторичных устройств за пределами здания или объекта КВИ. В этом сценарии эвакуация персонала наружу и размещение его в зоне потенциального поражения (в том числе осколками стекла и другими обломками в результате взрыва) может быть опаснее, чем его укрытие внутри. Изоляция – это когда весь персонал должен оставаться внутри помещения или здания в течение определенного периода времени с целью защиты от активной угрозы. Этот вариант может быть наиболее эффективным способом действий, например, в случае террористического нападения с применением огнестрельного оружия, когда вооруженные лица перемещаются по территории здания или объекта КВИ.

Все эти варианты преследуют одну и ту же цель: отвести персонал от динамической угрозы. Для целей настоящего *Технического руководства* террористическая угроза имеет первостепенное значение и включает в себя вооруженных стрелков, а также транспортные взрывчатые или ХБРЯ угрозы. Меры эвакуации не ограничиваются исключительно террористическими угрозами; они также регулярно рассматриваются на случай пожаров, землетрясений, наводнений и непреднамеренных инцидентов (отключение электроэнергии и т.д.).

Планирование эвакуации

Чтобы подготовить персонал на объекте КВИ к ситуации, связанной с эвакуацией, необходимо разработать план эвакуации, провести учения со всеми сотрудниками и заранее скоординировать план с местными правоохранительными органами, местными аварийно-спасательными службами, местными органами власти и, при необходимости, с близлежащими объектами (например, школами или торговыми центрами). Для обеспечения быстрого принятия решений в зависимости от ситуации в плане эвакуации должны быть определены лица, принимающие решение об эвакуации на объекте КВИ. Во многих случаях решение об эвакуации принимается высшим руководством учреждения КВИ по согласованию с правоохранительными органами.

Одна из дилемм, с которой сталкиваются лица, ответственные за принятие решения об эвакуации в контексте террористической угрозы, заключается в определении безопасного места. Это сложная для планирования задача, поскольку террористические угрозы зачастую бывают динамичными. В некоторых случаях эвакуация может быть более рискованным решением, если, например, маршрут эвакуации персонала проходит мимо подозрительного предмета снаружи здания. В случае угроз взрыва важно помнить о безопасной дистанции, рассмотренной ранее в настоящем *Техническом руководстве*. Британская инициатива ProtectUK рекомендует следующие расстояния[347]:

Расстояние до кордона	Подозрительный предмет
100 метров	Сумка/чемодан
200 метров	Легковой автомобиль
400 метров	Крупное транспортное средство

347 Национальное управление по борьбе с терроризмом, ProtectUK (дата отсутствует), Раздел руководства Purple Guide о борьбе с терроризмом — Планирование атак [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/purple-guide-chapter-counter-terrorism-attack-planning [дата обращения: 10 декабря 2024 г.].

Совместная контртеррористическая группа экспертов по оценке США рекомендует[348]:

Обязательное расстояние для эвакуации	Предпочтительное расстояние для эвакуации	Подозрительный предмет
21 метр	366 метров	Самодельная бомба (в корпусе металлической трубы)
34 метра	518 метров	Бомба смертника
46 метров	564 метра	Портфель
98 метров	579 метров	Легковой автомобиль
122 метра	732 метра	Фургон
195 метров	1158 метров	Небольшой грузовик для доставки

В плане эвакуации должно быть заранее определено, какой персонал останется на объекте или на своих постах для поддержания критически важных служб.

В плане эвакуации должны быть определены маршруты эвакуации, направляющие персонал к выходу из объекта или в относительно безопасную зону. Все маршруты эвакуации и выходы должны быть четко обозначены. Эвакуационные пути всегда должны быть свободны от мебели, мусора или других предметов, а указатели аварийного выхода необходимо регулярно проверять на работоспособность. При проектировании маршрутов эвакуации следует консультироваться с людьми с ограниченными возможностями, в том числе отдавая предпочтение маршрутам с пандусами на лестницах, где это необходимо, и учитывая, каким образом персонал в инвалидных колясках, например, сможет спускаться по лестнице при неработающих лифтах. По возможности, в определенных пунктах сбора должен быть доступен список находящихся на объекте людей для облегчения поиска пропавших людей.

Пункты сбора на объектах КВИ обычно определяются на случай различных чрезвычайных ситуаций (таких как пожар или землетрясение) и, как правило, находятся вблизи зданий или на открытом/незащищенном пространстве. Однако террористические угрозы объектам КВИ требуют иного подхода. Например:

- При выборе пункта сбора для эвакуации в случае угрозы взрыва необходимо учитывать близость взрывного устройства и его размер, а также меры по защите цели.
- Террорист может использовать свои знания о существующих пунктах сбора на случай пожара, чтобы привести в действие взрывное устройство в толпе эвакуируемых людей.

348 Совместная контртеррористическая группа экспертов по оценке (JCAT) (без даты), Руководство JCAT по противодействию терроризму для сотрудников служб безопасности. Доступно по адресу: https://www.dni.gov/nctc/jcat/references.html [дата обращения: 21 июля 2025 г.].

Поскольку характер террористических угроз по своей сути динамичен и уникален, во время эвакуации следует провести оценку и принять решение о целесообразности использования определенных пунктов сбора на объекте.[349] Лицам, разрабатывающим план эвакуации, также следует заранее определить альтернативные маршруты и выходы. При возможности, а также в случае отсутствия заранее определенного маршрута эвакуации и необходимости поиска альтернативного варианта, следует провести проверку предлагаемого альтернативного маршрута эвакуации и пункта сбора на предмет отсутствия взрывных устройств. Примером потенциальной угрозы взрыва может служить транспортное средство, припаркованное в непосредственной близости от определенного пункта сбора.

После завершения эвакуации и устранения угрозы необходимо принять решение о том, когда персонал сможет вернуться в здание/на объект. После принятия решения персоналу может быть поручено проверить свои рабочие места, чтобы убедиться в отсутствии каких-либо подозрительных предметов. Персонал должен быть проинформирован о том, кого следует уведомить в случае обнаружения чего-либо подозрительного.

Чем отличается эвакуация в случае теракта?

Персонал объекта КВИ в большинстве случаев знаком с принципами и практикой эвакуации при пожаре или землетрясении. Однако в случае террористического акта эвакуация может быть нецелесообразной, и, следовательно, эвакуационные действия при террористическом акте будут отличаться от эвакуационных действий при пожаре. Например, персонал может быть направлен к определенным выходам или ему может быть предписано избегать определенного маршрута или зоны. Поэтому важно избегать активации одной и той же сигнализации при террористической угрозе и пожаре, чтобы снизить вероятность неправильной реакции. Если это невозможно, следует принять меры по информированию персонала о характере эвакуации. Это может быть достигнуто с помощью системы оповещения, автоматических текстовых сообщений или сообщений по электронной почте либо путем размещения компетентных сотрудников вдоль определенных путей выхода для информирования эвакуирующегося персонала.

Планирование маршрута следования в укрытие

Если террористическая угроза находится за пределами здания или объекта, персонал может быть подвергнут опасности, если маршрут эвакуации проходит в непосредственной близости от источника угрозы (будь то подозрительный предмет, среда, загрязненная ХБРЯ, или стрелок, ведущий огонь из огнестрельного оружия). Более безопасной альтернативой может быть укрытие персонала. Следование в укрытие – это процесс перемещения персонала внутрь здания или объекта, подальше от активной угрозы.

В любом плане эвакуации следует учитывать сценарий, при котором необходимо следовать в укрытие. Пункты сбора для этого варианта должны быть определены

349 БаМаунг, Д.; Бергин, Г.; Бирн, Дж.; Гарретт, Д.; Харрисон, А.; Мейплз, Л.; Куинн, Л. (2022 г.), *Терроризм и контрмеры*, версия 2. (Наас, графство Килдэр: Институт безопасности Ирландии).

заранее и выбраны с учетом спектра террористических угроз, рассматриваемых в настоящем *Техническом руководстве,* поскольку каждая из них может повлиять на выбор.

Учитывая, что укрытие происходит внутри здания или сооружения, в выбранных помещениях, скорее всего, потребуются вентиляция и доступ к воздуху, туалетам, питьевой воде, аварийному освещению, средствам оказания первой помощи и средствам связи.[350]

Национальная практика: Руководство Великобритании ProtectUK по организации укрытия, в том числе в защищенных пространствах (2022 г.)[351]

Защищенные пространства должны располагаться:

- в зонах, окруженных стенами из каменной кладки во всю высоту, например, во внутренних коридорах, туалетах или конференц-залах с дверями, открывающимися внутрь;
- вдали от окон и наружных стен;
- вдали от зоны между периметром здания и первым рядом опорных колонн (известной как «периметральная конструктивная ячейка»);
- вдали от лестничных клеток или зон с доступом к лифтовым шахтам, которые выходят на улицу на уровне земли. Это связано с тем, что в случае их повреждения взрывная волна может подняться по ним вверх. Однако, если лестничные клетки и лифтовые шахты полностью закрыты, они могут служить хорошими защищенными пространствами;
- по возможности избегайте первого или второго этажа;
- в зоне, достаточной для размещения необходимого числа людей.

Источник: Национальное управление по борьбе с терроризмом и безопасности Великобритании

Планирование укрытия на месте/изоляции

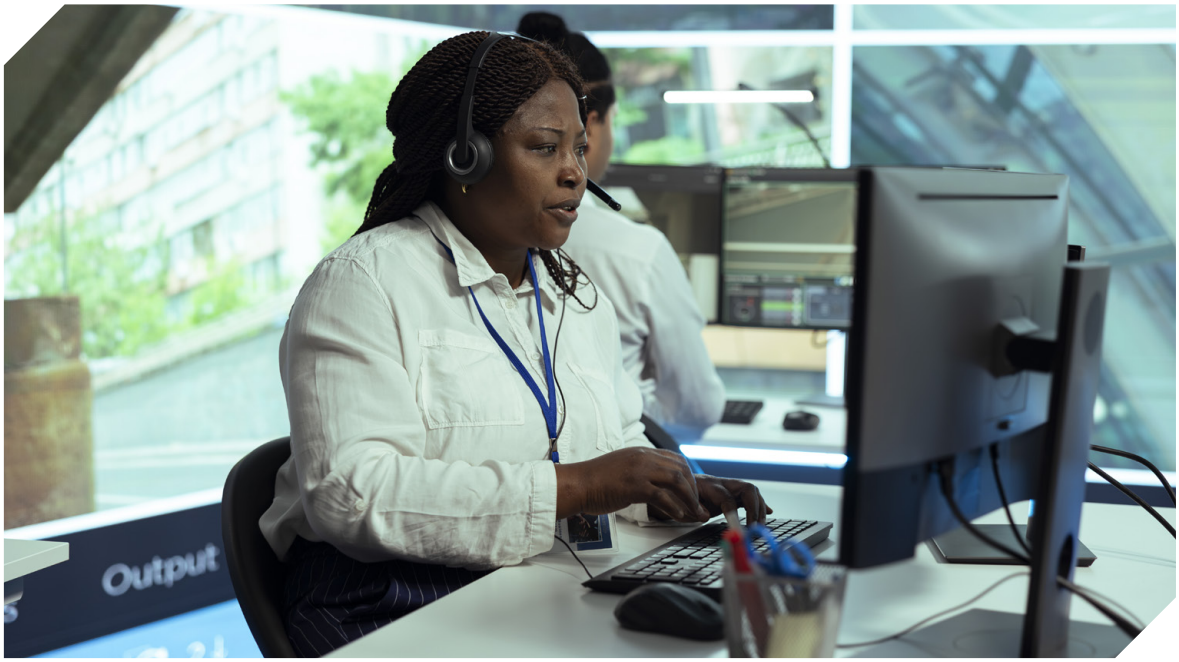
В случае террористической атаки с применением огнестрельного оружия, когда вооруженные лица перемещаются по зданию или территории КВИ, наиболее эффективным решением может быть требование ко всему персоналу изолироваться или укрыться на месте. Приказ компетентного персонала объекта КВИ об укрытии на месте может также быть отдан в случае, если активная угроза находится вблизи объекта КВИ. Такая возможность должна быть рассмотрена и описана в планах действий КВИ на случай чрезвычайной ситуации. В подобных случаях персонал должен иметь возможность быстро ограничить входы и выходы на весь объект или его части с помощью физических мер, таких как запирание дверей и опускание жалюзи на окнах.

350 Национальное управление по борьбе с терроризмом, ProtectUK (2022 г.), Руководство по местам проведения мероприятий и общественным пространствам (VaPS): эвакуация, укрытие, изоляция, защищенные пространства [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/evacuation-invacuation-lockdown-protected-spaces [дата обращения: 5 марта 2024 г.].

351 Национальное управление по борьбе с терроризмом, ProtectUK (2022 г.), Руководство по местам проведения мероприятий и общественным пространствам (VaPS): эвакуация, укрытие, изоляция, защищенные пространства [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/evacuation-invacuation-lockdown-protected-spaces [дата обращения: 5 марта 2024 г.].

7.8 Управление непрерывностью деятельности

Как показано в этой главе, владельцы/операторы КВИ должны планировать действия на случай разных инцидентов, вызывающих сбои, включая различные типы сценариев террористических атак. Как правило, многие из этих планов могут быть частью более широкой системы управления непрерывностью деятельности, которую можно увидеть во многих практических подходах, описанных в настоящем *Техническом руководстве.* Институт непрерывности бизнеса определяет непрерывность бизнеса как практику, которая «гарантирует, что организации могут поддерживать свои критически важные бизнес-процессы во время и после инцидентов».[352] Владельцам/операторам КВИ рекомендуется рассмотреть возможность внедрения и поддержания системы управления непрерывностью деятельности в рамках своих усилий по продолжению оказания критически важных услуг и восстановлению после разрушительных инцидентов, таких как террористическая атака.



Актуальность управления непрерывностью бизнеса подчеркивается в статье 13 Директивы ЕС об устойчивости критически важных объектов:

> «Государства-члены должны гарантировать, что критически важные субъекты принимают соответствующие и соразмерные технические, защитные и организационные меры для обеспечения своей устойчивости на основе соответствующей информации, предоставленной государствами-членами об оценке рисков государства-члена и о результатах оценки рисков критически важного субъекта, включая меры, необходимые для:
>
> a. предотвращения возникновения инцидентов, надлежащим образом учитывая меры по снижению риска бедствий и адаптации к изменению климата;

352 Институт непрерывности бизнеса (без даты), *Что такое непрерывность бизнеса?* [веб-страница]. Доступно по адресу: https://www.thebci.org/thought-leadership/what-is-business-continuity.html [дата обращения: 25 марта 2025 г.].

b. обеспечения надлежащей физической защиты своих помещений и критически важной инфраструктуры, должным образом учитывая, например, ограждения, барьеры, инструменты и процедуры контроля периметра, оборудование обнаружения и средства контроля доступа;
c. реагирования на инциденты, противостояния им и смягчения их последствий, должным образом учитывая внедрение процедур и протоколов управления рисками и кризисами, а также процедур оповещения;
d. восстановления после инцидентов, должным образом учитывая меры по обеспечению непрерывности деятельности и выявлению альтернативных цепочек поставок, с целью возобновления предоставления основных услуг;
e. обеспечения надлежащего управления безопасностью сотрудников, должным образом учитывая такие меры, как определение категорий персонала, выполняющего критически важные функции, установление прав доступа к помещениям, критически важной инфраструктуре и конфиденциальной информации, установление процедур проверки анкетных данных в соответствии со статьей 14 и обозначение категорий лиц, которые обязаны проходить такие проверки анкетных данных, а также установление соответствующих требований к обучению и квалификации;
f. повышения осведомленности о мерах, указанных в пунктах (a) - (e), среди соответствующего персонала, надлежащим образом рассматривая необходимость курсов подготовки, информационных материалов и учебных мероприятий».[353]

Системы управления непрерывностью деятельности рассматриваются в ISO 22301:2019. Согласно ISO, этот стандарт «предоставляет организациям основу для планирования, создания, внедрения, эксплуатации, мониторинга, анализа, поддержания и постоянного улучшения документированной системы управления для защиты от инцидентов, вызывающи сбои, снижения их вероятности и обеспечения восстановления после них».[354]

7.9 Кризисная коммуникация

Инциденты, рассмотренные выше в настоящем *Техническом руководстве,* представляют собой все формы кризисных ситуаций на объекте КВИ: террористические атаки с использованием транспортных средств, взрывчатых веществ, огнестрельного оружия, ХБРЯ материалов или ситуации захвата заложников. Различные аспекты подготовки к этим кризисным ситуациям были подробно рассмотрены в предыдущих главах. Однако важность коммуникации до сих пор не рассматривалась.

В 21-м веке информация, включая дезинформацию и недостоверную информацию, распространяется по всему миру мгновенно. В случае кризисной ситуации на объекте КВИ это может повлиять на безопасность персонала, реагирование на

353 ЕС (2022 г.), Директива 2022/2557 Европейского парламента и Совета от 14 декабря 2022 года об устойчивости критически важных субъектов и отмене Директивы Совета 2008/114/ЕС, *OJ* L 333. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [дата обращения: 21 июля 2025 г.].

354 ISO (2019 г.), *Безопасность и устойчивость. Системы управления непрерывностью бизнеса. Требования* (Стандарт ISO № 22301:2019). Доступно по адресу: https://www.iso.org/standard/75106.html [дата обращения: 21 июля 2025 г.].

кризис и/или его последствия. Если владелец/оператор КВИ не рассматривает кризисные коммуникации в рамках своего планирования, подготовки и реагирования на террористическую атаку и не использует эти коммуникации в достаточной степени, это может создать дополнительные проблемы, включая репутационный ущерб и нежелательное внимание со стороны СМИ. При инцидентах, связанных с терроризмом, репутационный ущерб является серьезной проблемой. Такой ущерб может быть нанесен, если владелец/оператор КВИ не отреагирует на инцидент надлежащим образом.

Механизм кризисных коммуникаций

Независимо от размера объекта КВИ, разработка механизмов кризисных коммуникаций имеет жизненно решающее значение для эффективного взаимодействия с персоналом объекта и общественностью в условиях развивающейся кризисной ситуации. По данным Контртеррористического управления ООН, цель механизма кризисных коммуникаций заключается в том, чтобы «занять лидирующую позицию в реагировании на последствия кризиса, повысить устойчивость сообщества, информировать и вовлекать население, стимулировать правильное поведение».[355]

355 Контртеррористический центр ООН (КТЦ ООН) (без даты), *Кризисная коммуникация.* Доступно по адресу: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/final_crisis_communication_toolkit_20042023.pdf [дата обращения: 21 июля 2025 г.].

Национальная практика: сеть устойчивости бизнеса Торговой палаты Канады: принципы эффективных коммуникаций в кризисных ситуациях[356]

- Начинайте коммуникацию незамедлительно – вам всегда есть что сказать.
- Установите временные рамки для коммуникации – сообщите СМИ/заинтересованным сторонам, когда им ожидать от вас следующего заявления; неопределенность может побудить их искать информацию в других источниках.
- Остановите всю прочую коммуникацию – в кризисной ситуации коммуникация должна касаться только кризиса и вашей реакции на него. Всю прочую коммуникацию следует приостановить.
- Используйте все свои каналы – аудитория получает информацию из разных источников, используйте все свои каналы для распространения последовательных сообщений.
- Краткость и по существу – аудитория ищет информацию, которую она может использовать для понимания ситуации и оценки ваших ответных действий. Быстро переходите к сути и сосредоточьтесь только на том, что актуально.

Источник: Сеть устойчивости бизнеса Торговой палаты Канады

Механизм кризисных коммуникаций должен требует создания междисциплинарной команды по кризисным коммуникациям, которая будет активироваться по мере необходимости для выполнения заранее определенных коммуникационных задач, актуальных для текущего кризиса. Этот механизм может предусматривать, среди прочего, разработку и распространение шаблонов сообщений в рамках кризисных коммуникаций, разработку плана кризисных коммуникаций, мониторинг освещения в СМИ, анализ общественного мнения, оценку воздействия кризиса на связи с общественностью, график реализации коммуникационного аспекта кризисных ситуаций и процесс посткризисной оценки.[357] Также следует подготовиться на случай публичного расследования действий владельца/оператора КВИ в кризисной ситуации.

356 Канадская торговая палата (без даты), *Руководство по планированию коммуникаций в кризисных ситуациях.* Доступно по адресу: https://chamber.ca/wp-content/uploads/2020/07/Guide_CrisisCommunicationsPlan.pdf [дата обращения: 21 июля 2025 г.].

357 PwC (без даты), Кризисная коммуникация [веб-страница]. Доступно по адресу: https://www.pwc.com/gx/en/issues/crisis-solutions/crisis-communication.html [дата обращения: 16 августа 2024 г.].

Практика: Инструментарий кризисных коммуникаций Контртеррористического управления ООН: механизм кризисных коммуникаций[358]

Этап	Цели	Стратегические действия
Этап I: активация	1. Сообщить факты и развеять страх 2. Установить ожидания относительно того, как может развиваться ситуация 3. Повлиять на национальное восприятие кризиса и посткризисных событий	▸ Активировать команду по управлению кризисными ситуациями и команду по коммуникациям в кризисных ситуациях ▸ Уделять приоритетное внимание здоровью и благополучию [...] людей ▸ Четко и последовательно распространяйте информацию, чтобы заполнить информационный вакуум ▸ Действовать последовательно, но гибко –адаптироваться к изменению ситуации ▸ Дать возможность лидерам распространять ключевые сообщения, поддерживать [...] людей и сообщество ▸ Быть готовым к эскалации к более масштабной кризисной ситуации.
Этап II: сдерживание	1. Демонстрировать заботу и активно действовать 2. Поддержать отдельных людей и сообщество, обеспечить непрерывность деятельности 3. Продолжать влиять на национальное восприятие кризиса и посткризисное видение	▸ Уделять приоритетное внимание здоровью и благополучию людей ▸ Сообщать факты через единый «источник истины» ▸ Следить за дезинформацией ▸ Действовать последовательно, но гибко –адаптироваться к изменению ситуации ▸ Дать возможность лидерам распространять ключевые сообщения, поддерживать людей ▸ Быть готовым к эскалации к более масштабной кризисной ситуации
Этап III: восстановление	1. Демонстрировать заботу и активно действовать 2. Поддержать отдельных людей, обеспечить непрерывность деятельности 3. Бороться с апатией, снижать уровень гнева, создавать видение будущего 4. Формировать будущее страны при ее восстановлении после кризиса	▸ Уделять приоритетное внимание здоровью и благополучию людей ▸ Сообщать факты через единый «источник истины» ▸ Продолжать отслеживать дезинформацию ▸ Действовать последовательно, но гибко –адаптироваться к изменению ситуации ▸ Дать возможность лидерам распространять ключевые сообщения посылы, поддерживать людей ▸ Быть готовым к неудачам, но смотреть в будущее

Источник: Контртеррористическое управление ООН

358 Контртеррористический центр ООН (UNCCT) (без даты), *Кризисная коммуникация*. Доступно по адресу: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/final_crisis_communication_toolkit_20042023.pdf [дата обращения: 21 июля 2025 г.].

Национальная практика: Аспекты Британского института по связям с общественностью и Центра защиты национальной инфраструктуры[359], рекомендуемые для включения в план кризисной коммуникации[360]

Национальное управление по защите и безопасности Великобритании (NPSA) рекомендует учитывать следующие элементы при составлении плана кризисной коммуникации:

- Политика в области коммуникаций: процесс коммуникаций при инциденте, внутренняя командная вертикаль, протоколы полиции, ожидания персонала и действия (включая соответствующие каналы).
- Озвучивание заявлений: выбор заявлений, подходящих для ряда инцидентов, готовых к публикации (с небольшими поправками) на начальном этапе кризиса.
- Роли и обязанности: внутри [владельца/оператора КВИ], включая назначенного сотрудника для планирования действий в чрезвычайных ситуациях и управления кризисными ситуациями. Определение спикеров и конкретных должностных ролей членов команды –также за пределами организации, с привлечением соответствующих партнеров.
- Благополучие: жизненный цикл кризиса может быть длительным и предполагать круглосуточную работу. Необходимо определить графики смен и время восстановления. Следует включить потенциальных партнеров (например, дополнительные ресурсы внешних агентств или других внутренних отделов, например, отдела маркетинга или отдела кадров).
- Список контактов: ключевые члены команды и внешние заинтересованные стороны, включая СМИ (по мере необходимости).
- Системы: сведения о входах в систему, процедурах работы корпоративных каналов (например, внесение изменений на веб-сайт или переход на теневой сайт), технические руководства, сведения о доступе в здание.
- Ресурсы: шаблоны, планы действий, корпоративные изображения и информационные материалы (например, информационные бюллетени), журнал коммуникаций, электронная почта и группы в WhatsApp, «экстренные рюкзаки» (например, зарядное устройство для телефона, вода, сменная одежда, основные туалетные принадлежности, информационные пакеты). Если полиция возьмет управление на себя, то организация все равно будет обязана предоставить вспомогательные ресурсы, но ваша коммуникация не будет главной в общении со СМИ.

Источник: Национальное управление по защите и безопасности Великобритании

359 Теперь – Национальное управление по защите и безопасности (NPSA).

360 Институт дипломированных специалистов по связям с общественностью, Центр защиты национальной инфраструктуры (без даты), *Управление кризисами в случае террористических событий.* Доступно по адресу: https://www.npsa.gov.uk/system/files/documents/de/eb/Crisis_Management_for_Terrorist_Related_Events.pdf [дата обращения: 21 июля 2025 г.].

Кризисная коммуникация в случае инсайдерских инцидентов

Инсайдерские инциденты могут создавать определенные проблемы для кризисной коммуникации внутри организации и между организациями (для получения дополнительной информации см. главу 8 «Управление внутренними угрозами»). По своей природе инсайдерский инцидент, скорее всего, будет вызван (по крайней мере частично) организационным или индивидуальным сбоем, что вызывает вопросы к уровню компетентности, культуры и доверия. Влияние инсайдерского инцидента как на персонал, так и на тех, кто находится за пределами объекта КВИ, может быть значительным и долгосрочным, приводя к подрыву доверия (как внутри организации, так и за ее пределами).

Чтобы смягчить негативные последствия инсайдерских инцидентов, некоторые государства-участники ОБСЕ призвали владельцев/операторов КВИ использовать методы коммуникации для успешного смягчения последствий инсайдерских инцидентов, управления ими и восстановления после них – либо с помощью программы кризисных коммуникаций, либо с помощью специальных мер, направленных на коммуникацию во время инцидентов такого типа.

Национальная практика: рекомендации Национального управления по защите и безопасности Великобритании по коммуникациям при инсайдерских инцидентах для предприятий (2023 г.)[361]

1. Коммуникацию следует эффективно интегрировать в процессы подготовки к инсайдерским инцидентам и ликвидации их последствий, а не только в процесс управления инсайдерскими инцидентами.
2. Чтобы обеспечить понимание и достижение желаемого результата, при коммуникации в случае инсайдерского инцидента необходимо отдать приоритет правильному сообщению, донесенному правильным тоном убедительным спикером и через правильные каналы.
3. Вместо того, чтобы использовать показатели, ориентированные на охват сообщением, успех коммуникационной стратегии должен определяться тем, насколько хорошо воспринято сообщение. Если оно не воспринимается хорошо, размер охваченной им аудитории не имеет значения.
4. Аспекты инсайдерских инцидентов должны быть интегрированы в существующие передовые практики реагирования на кризисы. Регулярные практические учения жизненно важны для формирования особой «мышечной памяти» и ответственного управления вопросами вины, субъективности и истины.

Источник: Национальное управление по защите и безопасности Великобритании (NPSA)

361 Национальное управление по защите и безопасности Великобритании (2023 г.), *Инсайдерские события: руководство по коммуникациям для снижения их воздействия.* Доступно по адресу: https://www.npsa.gov.uk/resources/insider-event-guidance [дата обращения: 21 июля 2025 г.].

Системы оповещения населения

В резолюции Совета Безопасности ООН 2341 (2017 г.) Совет Безопасности ООН «призна[ет], что усилия по защите должны осуществляться в многочисленных областях, таких как [...] общественная информация и предупреждение».[362] Таким образом, в качестве дополнительного инструмента коммуникации системы оповещения общественности могут помочь информировать членов общественности во время чрезвычайных ситуаций и могут быть полезны как часть более широкой структуры кризисной коммуникации на случай террористических атак на объекты и службы КВИ.

Согласно Европейской ассоциации номеров экстренных служб, система оповещения населения служит «ценным механизмом для минимизации ущерба и управления чрезвычайными ситуациями во время и после чрезвычайных событий».[363] По данным этой ассоциации, оповещения населения могут передаваться с использованием мобильных телефонов, стационарных телефонов, телевидения, радио, сирен и акустических устройств дальнего радиуса действия, табло с изменяемой информацией и систем оповещения, а также через Интернет.[364] Европейская комиссия в 2018 году приняла Европейский кодекс электронных коммуникаций, статья 110 которого прямо требует от государств-членов ЕС иметь системы оповещения населения, которые передают предупреждения через устройства на основе мобильных номеров или другие сервисы, «при условии, что эффективность системы оповещения населения эквивалентна в плане зрения охвата и способности достигать конечных пользователей, включая тех, кто временно находится в соответствующей зоне».[365]

362 СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

363 Европейская ассоциация номеров экстренных служб (30 сентября 2019 г.), *Системы оповещения населения – Обновление, версия 3.0*. Доступно по адресу: https://eena.org/wp-content/uploads/2021_02_18_PWS_Document_FINAL_Compressed.pdf [дата обращения: 21 июля 2025 г.].

364 Европейская ассоциация номеров экстренных служб (30 сентября 2019 г.), *Системы оповещения населения – Обновление, версия 3.0*. Доступно по адресу: https://eena.org/wp-content/uploads/2021_02_18_PWS_Document_FINAL_Compressed.pdf [дата обращения: 21 июля 2025 г.].

365 Директива (ЕС) 2018/1972 Европейского парламента и Совета от 11 декабря 2018 года, устанавливающая Европейский кодекс электронной коммуникации, *OJ* L 321. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2018/1972/oj/eng [дата обращения: 21 июля 2025 г.]. Список экстренных служб, доступных в ЕС, можно найти в разделе: Body of European Regulators for Electronic Communications (BEREC), Public Warning Systems [веб-страница]. Доступно по адресу: https://www.berec.europa.eu/en/pws [дата обращения: 21 июля 2025 г.].

Национальная практика: используемая в Швейцарии многоканальная стратегия по информированию, предупреждению и тревожной сигнализации (2024 г.)[366]

Основная система оповещения Швейцарии, называемая PolyAlert, позволяет использовать все каналы оповещения населения одновременно, при этом все уполномоченные органы гражданской обороны имеют доступ к основной системе. Она позволяет осуществлять удаленный контроль и управление сиренами, а также вводить сообщения соответствующими органами в случае чрезвычайной ситуации. Помимо использования более чем 7 000 стационарных и мобильных сирен, швейцарская система также обеспечивает оповещение населения через приложение и веб-сайт Alertswiss, а также радио и телевидение, которые по закону обязаны передавать определенные сообщения, связанные с общественной безопасностью. Другими каналами связи являются специальное аварийное радио, мобильная связь, партнерские каналы и пункты экстренного сбора. В своей *Многоканальной стратегии информирования, предупреждения и оповещения Ausblick 2035* Швейцария взяла на себя обязательство по дальнейшему развитию и актуализации этой многоканальной системы на основе новых технологий и требований безопасности.

Источник: Федеральное ведомство гражданской обороны Швейцарии

366 Федеральное ведомство гражданской обороны Швейцарии (BABS) (октябрь 2024 г.), *Многоканальной стратегии по информации, предупреждению и оповещению. Ausblick 2035.* Доступно по адресу: https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/11/27/bc33f6aa-911f-45fb-97fe-7978120b06b1.pdf [по состоянию на 21 июля 2025 г.] неофициальный перевод.

8 Управление внутренними угрозами

«Разнообразие угроз, которые инсайдеры могут представлять для объектов критически важной инфраструктуры, привело к появлению различных подходов со стороны владельцев/операторов, что позволяет им учитывать конкретные способы, которыми инсайдеры могут представлять риски для их организации.»

8 Управление внутренними угрозами

В предыдущих главах рассматривался ряд решений по обеспечению физической безопасности, ориентированных на *внешние* угрозы для объектов КВИ. За исключением, возможно, гражданской авиации и энергетического сектора, проблемам *внутренних* угроз традиционно уделялось меньше внимания.[367] Однако тенденция меняется из-за возросшего внимания и осведомленности владельцев/операторов КВИ и лиц, отвечающих за выработку национальной политики, об угрозе, которую внутренние лица (инсайдеры) могут представлять для эффективного функционирования КВИ.

В этой главе представлен ряд определений и подходов для концептуализации внутренних угроз, включая злонамеренных и незлонамеренных внутренних лиц. Далее в ней рассматриваются способы, которыми отдельные лица могут участвовать во враждебной внутренней деятельности, а затем предлагаются организационные меры в ответ на эту постоянно присутствующую проблему.

Практический пример террориста-инсайдера 1 – авиационный сектор

2 февраля 2015 года самолет авиакомпании Daallo Airlines вылетел из Могадишо, Сомали. Вскоре после взлета в самолете произошел взрыв, в результате которого в боку фюзеляжа образовалась дыра, через которую наружу утащило террориста Абдуллахи Абдисалама Борлеха. После расследования власти Сомали пришли к выводу, что произошло преждевременное срабатывание взрывного устройства, скрытого в ноутбуке. По данным представителей сомалийской разведки,[368] камеры видеонаблюдения зафиксировали, как двое работников аэропорта передали ноутбук Абдисаламу Борлеху перед его посадкой в самолет.[369]

Практический пример террориста-инсайдера 2 – энергетический сектор[370]

16 января 2013 года 32 террориста захватили контроль над газодобывающим заводом Тигентурин в Ин-Аменасе на юге Алжира, начав четырехдневное противостояние, в ходе которого были захвачены десятки иностранных

367 UNOCT и Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (2022 г.), *Защита критически важных объектов инфраструктуры от террористических атак: сборник передового опыта.* Доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf [дата обращения: 21 июля 2025 г.].

368 Маруф, Х. (2016 г.), «Сомалийские официальные лица: мужчине, погибшему при взрыве в самолете, перед вылетом дали ноутбук», Voice of America [веб-страница]. Доступно по адресу: https://www.voanews.com/a/airport-staff-airline-employees-detained-somali-plane-blast/3179920.html [дата обращения: 30 ноября 2024 г.].

369 Управление транспортной безопасности США (2020 г.), *Дорожная карта внутренних угроз.* Доступно по адресу: https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf [дата обращения: 21 июля 2025 г.].

370 Statoil (2013 г.), *Атака в Ин-Аменас: Отчет о расследовании террористической атаки на Ин-Аменас. Подготовлено для Совета директоров Statoil ASA.* Доступно по адресу: https://www.equinor.com/news/archive/2013/09/12/downloads/In%20Amenas%20report.pdf [дата обращения: 21 июля 2025 г.].

заложников, сорок из которых в конечном итоге были убиты. Разработка газового месторождения Ин-Аменас, одного из крупнейших газовых проектов Алжира, расположенного примерно в 1 300 километрах от столицы Алжира и в 50 километрах от границы с Ливией, осуществлялась совместным предприятием алжирской национальной нефтяной компании, Sonatrach, British Petroleum и Statoil.

В преддверии атаки был допущен ряд серьезных нарушений в системе безопасности, поскольку меры безопасности на объекте не были адаптированы к атаке такого масштаба. Выжившие после атаки впоследствии заявили, что нападавшие, по всей видимости, были хорошо осведомлены об объекте, включая местоположение офиса управления, где и когда на объекте будет находиться руководство, а также о том, как отключить электричество, что было сделано в течение первых нескольких минут после начала атаки. Представители Statoil и алжирские чиновники пришли к выводу, что террористы, вероятно, воспользовались определенной инсайдерской информацией при планировании атаки, однако никаких четких доказательств этого так и не было обнаружено.

В статье, опубликованной в 2016 году в журнале *«Исследования конфликтов и терроризма» (Studies in Conflict & Terrorism),* было установлено следующее:

> «Хотя угроза терроризма получила широкое признание за последнее десятилетие, проблема проникновения в организации инсайдеров-террористов остается непризнанной, а потенциальная опасность, которую представляют эти лица, до конца не изучена. Необходимо понимать более широкие аспекты инсайдерских угроз, включая мотивацию и методы атак, а также иметь возможность демонстрировать потенциальные разрушительные последствия, которые могут повлечь такие атаки».[371]

В 2023 году Национальное управление по защите и безопасности Великобритании (NPSA) провело исследование, которое подтверждает важность снижения уровня внутренних угроз для КВИ, указав, что:

- Количество инсайдерских инцидентов увеличилось почти на 50% всего за два года;
- 98% организаций чувствуют себя уязвимыми к инсайдерским атакам;
- В 25% случаев виновниками инцидентов были злонамеренные или преступные инсайдеры;
- Урегулирование инсайдерских инцидентов занимает больше времени (в среднем три месяца), и в результате расходы на устранение последствий инсайдерской деятельности на момент проведения исследования NPSA оценивалась более чем в 15.000.000 долларов США (что больше, чем в предыдущие годы).[372]

371 БаМаунг, Д., МакИльяттон, Д., МакДональд, М., Битти, Р. (2016 г.), «Враг внутри? Связь между внутренней угрозой и терроризмом». *Исследования конфликтов и терроризма* 41(2), стр. 133–150. Доступно по адресу: https://doi.org/10.1080/1057610X.2016.1249776 [дата обращения: 21 июля 2025 г.].

372 Национальное управление по защите и безопасности Великобритании (2023 г.), *Инсайдерские события: руководство по коммуникации для снижения их воздействия*. Доступно по адресу: https://www.npsa.gov.uk/insider-events-communications-guidance [дата обращения: 21 июля 2025 г.].

В 2020 году Управление транспортной безопасности США также подчеркнуло наличие внутренней угрозы в транспортном секторе:

> «Внутренняя угроза в [транспортном секторе], как правило, связана с промышленным саботажем, кражами и/или контрабандой, а не с терроризмом, однако еще в 2019 году террористы пытались использовать инсайдеров для проведения своих атак. Существуют обоснованные опасения, что террористы могут использовать тактику, методы и процедуры, используемые транснациональными преступными организациями, для выявления и вербовки или разработки и внедрения инсайдеров в [транспортный сектор]».[373]

8.1 Определение внутренних угроз

Прежде чем рассматривать вопросы и практику управления внутренними угрозами, важно рассмотреть, как разные государства-участники ОБСЕ и другие заинтересованные стороны определяют понятия *инсайдеры* и *внутренние угрозы*. Что касается термина *инсайдер*, во многих определениях (включая те, которые используются Соединенными Штатами[374] и Великобританией[375]) встречается одна ключевая повторяющаяся фраза *санкционированный доступ.* Практически в каждом определении *инсайдер* определяется как лицо, которое имеет или имело санкционированный доступ к ресурсам организации (или знание о них), включая персонал, объекты, информацию, процессы и данные.

373 Управление транспортной безопасности США (2020 г.), *Дорожная карта внутренних угроз 2020 г.* Доступно по адресу: https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf [дата обращения: 21 июля 2025 г.].

374 Агентство по кибербезопасности и защите инфраструктуры США (без даты), Определение внутренних угроз [веб-страница]. Доступно по адресу: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats#:~:text=Insider%20threat%20is%20the%20potential,organization%20to%20harm%20that%20organization [дата обращения: 21 июля 2025 г.].

375 Национальное управление по защите и безопасности Великобритании (22 мая 2023 г.), Изменения, внесенные Национальным управлением по защите и безопасности Великобритании, в определения инсайдерского риска [веб-страница]. Доступно по адресу: https://www.npsa.gov.uk/blog/npsa-changes-insider-risk-definitions [дата обращения: 21 июля 2025 г.].

Эту точку зрения разделяют некоторые владельцы/операторы КВИ: Венский международный аэропорт в Австрии считает инсайдером «лицо, которое имеет или имело санкционированный доступ к ресурсам, инструментам или процессам организации или знания о них. Это лицо обычно работает непосредственно на организацию или по контракту с ней. Инсайдер становится внутренней угрозой, как только эти знания намеренно используются против организации. Это лицо имеет преимущество перед посторонним лицом, поскольку он или она в целом знакомы с политикой и процедурами безопасности».[376]

В центре определения *внутренних угроз* обычно находится преднамеренное злоупотребление санкционированным доступом или знанием организации с целью причинения ей вреда. Однако важное значение имеют также непреднамеренные внутренние угрозы. В Руководстве по разработке программы по борьбе с внутренними угрозами Help2Protect[377] говорится: «внутренние угрозы, включая саботаж, кражу, шпионаж, мошенничество и конкурентное преимущество, часто реализуются посредством злоупотребления правами доступа, кражи материалов и ненадлежащего обращения с физическими устройствами. Инсайдеры не всегда действуют в одиночку и могут не осознавать, что они помогают субъекту угрозы (т.е. являются непреднамеренной внутренней угрозой)».[378] Определение, принятое в США, также включает в себя непреднамеренные или незлонамеренные действия инсайдеров, которые могут иметь схожие негативные последствия для организации.[379]

Практика: корпоративный регламент физической безопасности и антитеррористической защиты «КазМунайГаз»: внутренние источники угроз (2020 г.)[380]

В регламенте «КазМунайГаз» определены «основные цели, задачи, общие принципы и направления деятельности по обеспечению физической безопасности и антитеррористической защиты группы компаний [КазМунайГаз]». В рамках Регламента определены различные типы субъектов угроз с целью «установления необходимого уровня защиты объекта и его критических зон, разработки требований к системе физической безопасности и антитеррористической защиты объекта и оценки ее эффективности».

376 Аэропорт Вены (без даты), Типы угроз — от небрежности до намерения [веб-страница]. Доступно по адресу: https://www.viennaairport.com/en/business__partner/security_culture/types_of_threat_-_from_carelessness_to_intention [дата обращения: 21 июля 2025 г.].

377 Help2Protect (H2P) — это платформа электронного обучения, созданная в конце 2018 года в качестве основного результата финансируемого ЕС проекта AITRAP по внутренним угрозам. Проект координировался Конфедерацией европейских служб безопасности. Более подробную информацию можно найти здесь: https://www.help2protect.info/?doing_wp_cron=1744884209.4140460491180419921875 [дата обращения: 21 июля 2025 г.].

378 Help2Protect (2025 г.), *Руководство по разработке программы по борьбе с внутренними угрозами, издание 5*. Доступно по адресу: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [дата обращения: 21 июля 2025 г.].

379 Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Руководство по смягчению внутренних угроз.* Доступно по адресу: https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide [дата обращения: 21 июля 2025 г.].

380 Куликов, В. (2 декабря 2020 г.), Корпоративный регламент физической безопасности и антитеррористической защиты акционерного общества «Национальная компания «КазМунайГаз». Доступно по адресу: https://www.kmg.kz/upload/iblock/e94/g2t9u88ocpru7ls82dr7vrne28dmfzf4/Корпоративный регламент физической безопасности и антитеррористической защиты акционерного общества НК КМГ.docx [дата обращения: 21 июля 2025 г.].

Эти злоумышленники делятся на две категории: внутренние нарушители («лица из числа персонала объекта и другие лица, допущенные на его территорию установленным порядком») и внешние правонарушители («лица, не входящие в состав персонала (посетителей) объекта и не имеющие права доступа на него»). Затем в регламенте приводится подробное описание обоих типов нарушителей, их основных характеристик и вероятной тактики действий. Два типа внутренних правонарушителей из этого регламента кратко описаны ниже:

Вид нарушителя	Основные характеристики	Вероятная тактика действий
1. Внутренний нарушитель первого типа (Работник объекта (специалист), имеющий санкционированный доступ на его территорию. Основная цель - хищение ради собственной наживы, однако, не исключается возможность совершения акта терроризма.)	1. высокий уровень осведомленности о структуре и составе системы физической безопасности и антитеррористической защищенности объекта, а также о расположении постов охраны; 2. высокий уровень осведомленности о расположении объектов хищения или диверсии на территории объекта; 3. низкая вероятность наличия огнестрельного оружия, взрывчатых веществ и взрывных устройств; 4. возможность использования легкого и специального инструмента; 5. низкая вероятность использования автотранспорта; 6. достаточный уровень подготовленности к преодолению физических барьеров.	Легальный проход на территорию объекта в рабочее время, используя пропускные документы. Нарушитель может являться источником информации о потенциально опасном объекте для внешнего нарушителя первого и второго типа, вступать в сговор с внешними и внутренними нарушителями для участия в совместных актах терроризма.
2. Внутренний нарушитель второго типа (Работник [объектового подразделения охраны])	1. высокий уровень осведомленности о структуре и составе системы обеспечения физической безопасности и антитеррористической защиты объекта, расположении постов охраны; 2. низкий уровень знания технологического процесса; 3. высокий уровень осведомленности о расположении объектов охраны на территории объекта; 4. наличие вооружения и специальных средств (зависит от штатной экипировки сил охраны на конкретном объекте); 5. возможность беспрепятственного прохода в охраняемую зону; 6. низкий уровень подготовленности к преодолению физических барьеров.	Открытое проникновение к объектам хищения в рабочее время с использованием служебных полномочий. Нарушитель: осведомлен о режиме работы объекта, местонахождении возможных материальных и иных ценностей; может действовать в момент, наиболее подходящий для совершения акта терроризма; может вступать в сговор с внешними нарушителями.

Источник: КазМунайГаз

Разнообразие угроз, которые инсайдеры могут представлять для объектов КВИ, привело к появлению различных подходов у разных владельцев/операторов КВИ, позволяющих им учитывать конкретные способы, которыми инсайдеры могут представлять риски для их организации. Например, некоторые организации могут основывать свои определения на:

- типах субъектов угроз, считающихся инсайдерами (например, злонамеренные, непреднамеренные, сотрудники или подрядчики);
- типах объектов, к которым имеют доступ инсайдеры (например, информационные технологии [ИТ], объекты, сети или данные); или
- типах вреда, который может быть нанесен владельцу/оператору КВИ (например, мошенничество, кража, саботаж или насилие).

Эти различные подходы служат важным напоминанием о том, что определение *внутренней угрозы* должно соответствовать контексту конкретного сектора КВИ или заинтересованной стороны. Эта передовая практика включена в руководство Агентства по кибербезопасности и защите инфраструктуры США, в котором утверждается, что организация должна «определить внутреннюю угрозу с учетом уникального характера своей операционной среды, своих ценностей или ресурсов, которые, по ее мнению, подвергаются наибольшему риску».[381]

Национальная практика: пять типов инсайдерских инцидентов по версии Национального управления по защите и безопасности Великобритании (2023 г.)[382]

- Несанкционированное раскрытие конфиденциальной информации.
- Реорганизация процессов в свою пользу (вероятнее всего, мошенничество).
- Содействие доступу третьих лиц к объектам организации.
- Саботаж (физический, электронный или ИТ-саботаж).
- Физическая угроза (насилие).

Источник: Национальное управление по защите и безопасности Великобритании

381 Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Руководство по смягчению внутренних угроз.* Доступно по адресу: https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide [дата обращения: 21 июля 2025 г.].

382 Национальное управление по защите и безопасности Великобритании (10 ноября 2023 г.), Введение в тему внутренних рисков [веб-страница]. Доступно по адресу: https://www.npsa.gov.uk/introduction-insider-risk [дата обращения: 5 марта 2024 г.]

Хотя в регионе ОБСЕ не существует единого определения того, что на самом деле представляет собой внутренняя угроза, ниже приведены отдельные сценарии, при которых внутренний нарушитель может представлять угрозу владельцу/оператору КВИ:

Кража информации

Кража информации, такой как чертежи или конфиденциальные материалы, которая может скомпрометировать владельца/оператора КВИ или предприятие или поставить его в крайне невыгодное положение или подвергнуть риску.

Насилие на рабочем месте

Применение насилия или угроз насилия с целью оказания влияния или запугивания других лиц на объекте КВИ и воздействия на здоровье и безопасность сотрудников объекта.

Угроза безопасности

Получение информации о графиках и процедурах патрулирования сотрудниками службы безопасности с целью снижения уровня безопасности объекта и его персонала.

Шпионаж

Шпионаж в пользу другого лица с целью получения секретных, конфиденциальных или важных материалов или знаний, которые могут быть использованы против владельца/оператора КВИ.

Терроризм

Использование доступа к объекту КВИ с целью совершения или содействия совершению акта насилия в поддержку террористической или насильственной экстремистской идеологии.

Кража физического имущества

Кража материальных ценностей (товаров, оборудования, бейджей).

Саботаж

Преднамеренное уничтожение оборудования или ИТ, включая нанесениепрямого конкретного ущерба (например, внедрение вредоносного компьютерного кода в инфраструктуру информационных технологий организации).

Понимание угрозы инсайдера
Разнообразие определений внутренних угроз и подходов борьбе с ними, описанных выше, наглядно демонстрирует степень сложности, которую они могут представлять. Термин *«инсайдер»* может охватывать действующих или бывших сотрудников, сторонних подрядчиков или даже деловых партнеров, имеющих доступ к помещениям и системам в пределах объекта КВИ. Потенциально это огромное количество лиц. Каждый из них может иметь возможность наблюдать за процессами КВИ без помех в течение определенного периода времени и совершать несанкционированные действия.

Инсайдеры обладают явными преимуществами перед внешними источниками угрозы, которые обычно могут получить доступ к КВИ только посредством насильственных действий или уловок. Инсайдеры могут быть либо главными заговорщиками при нападении на КВИ, либо выступать в качестве сообщников (т.е. информаторов) внешних источников угрозы. Их знания (или легкость, с которой они могут получить определенную информацию) о целевом объекте могут быть легко использованы в преступных целях, включая террористические атаки.

Злонамеренные и незлонамеренные инсайдеры
Действия злонамеренных инсайдеров, имеющих доступ к критически важным объектам и системам, являются важным направлением стратегий снижения внутренних угроз на национальном уровне, уровне владельца/оператора КВИ и уровне объекта КВИ. Однако не все инсайдеры являются злонамеренными и имеют намерение причинить вред. Некоторые инсайдеры непреднамеренно причиняют вред, совершая ненадлежащие действия по причине стресса на работе, отвлекающих факторов, неосведомленности, нетерпения, лени, доверчивости или отсутствия бдительности. Примерами служат потеря конфиденциальных данных или оставление зон контролируемого доступа без должной защиты.

Другие инсайдеры могут быть вовлечены в манипуляцию, направленную на раскрытие информации о своем работодателе, со стороны внешних источников угрозы, таких как преступники, террористы, хакеры или другие. Кроме того, внешние источники угрозы могут использовать обман для манипулирования ничего не подозревающими инсайдерами, чтобы преодолеть разные уровни защиты целевых организаций. Такие манипуляции могут включать в себя применение методов социальной инженерии с целью получения информации, которая может быть использована для шантажа.

Эти разнообразные способы, посредством которых инсайдеры представляют угрозу владельцам/операторам КВИ, побудили некоторые стороны внести дополнительные нюансы в свои определения: в *Руководстве по разработке программы по борьбе с внутренними угрозами* Help2Protect определены три категории инсайдеров:

- **Непреднамеренный инсайдер:** сотрудник не осознает, что его/ее действия наносят вред. Сотрудник не имеет намерения причинить вред и признаки риска могут быть крайне незначительными.
- **Небрежный инсайдер:** сотрудник осознает, что его/ее действия являются нарушением правил безопасности, но «идет на риск», чтобы «облегчить себе жизнь». Сотрудник может демонстрировать некоторые признаки риска.

- **Злонамеренный инсайдер:** сотрудник действует сознательно с целью причинения вреда организации. Сотрудник может предпринять шаги, чтобы скрыть признаки риска.[383]

По данным Help2Protect, злонамеренные инсайдеры делятся как минимум на две категории:

- **Инсайдеры с собственной мотивацией:** это лица, действия которых совершаются по их собственной воле, а не по инициативе или указанию третьей стороны.
- **Завербованные инсайдеры:** это лица, привлеченные третьей стороной для целенаправленного использования в преступных целях их потенциального, текущего или бывшего привилегированного доступа. К ним относятся разработанные и завербованные агенты иностранной разведки или их структуры, действующие со злым умыслом.[384]

8.2 Факторы, влияющие на вероятность участия отдельных лиц во враждебной инсайдерской деятельности

Чтобы выбрать наиболее эффективные способы реагирования на внутренние угрозы, важно определить факторы, которые могут побудить сотрудника к совершению враждебных внутренних действий. В *Руководстве по разработке программы по внутренним угрозам* Help2Protect определены несколько потенциальных причин, побуждающих к становлению на путь у инсайдерской деятельности:

- Частный или связанный с работой кризис (финансовый или личный кризис, кризис в отношениях, здоровье, жизненные события и т.д.);
- Чувство фрустрации, разочарования или недовольства;
- Преувеличенное чувство собственных способностей и достижений;
- Сильное чувство собственной исключительности и эгоистическое представление о том, что организация делает или не делает для них;
- Необходимость продемонстрировать свою ценность другим, чтобы получить признание.[385]

Враждебные действия инсайдера могут также осуществляться в отместку организации или работодателю. Сочетание этих факторов может привести к триггерному событию, например, конфликту с коллегами или заболеванию (в том числе психическом), побуждающего человека к участию во враждебной инсайдерской деятельности.

383 Help2Protect (2025 г.), *Руководство по разработке программы по борьбе с внутренними угрозами, издание 5.* Доступно по адресу: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [дата обращения: 21 июля 2025 г.].

384 Help2Protect (2025 г.), *Руководство по разработке программы по борьбе с внутренними угрозами, издание 5.* Доступно по адресу: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [дата обращения: 21 июля 2025 г.].

385 Help2Protect (2025 г.), *Руководство по разработке программы по борьбе с внутренними угрозами, издание 5.* Доступно по адресу: https://www.help2protect.info/kickstarter/insider-threat-program-development/?doing_wp_cron=1744884664.1926438808441162109375 [дата обращения: 21 июля 2025 г.].

Даже если это не так, для совершения инсайдером враждебной деятельности у него должны существовать возможности. Такие возможности могут включать в себя доступ к ценным физическим предметам или информации, а также возможности, связанные с ненадлежащими мерами безопасности, такими как разрешенный обмен паролями или кодами доступа между коллегами.[386]

8.3 Признаки враждебной инсайдерской деятельности

Обнаружение признаков враждебной инсайдерской активности и подготовки к атаке имеет ключевое значение для эффективного противодействия внутренним угрозам со стороны владельца/оператора КВИ. Хотя не существует единого списка признаков (приведенные ниже признаки не являются исчерпывающими), существуют определенные действия, которые в сочетании с другими сведениями или оперативным данными, полученными от компетентных сотрудников служб безопасности КВИ или органов власти, могут указывать на наличие или, по крайней мере, возможность внутренней угрозы[387]:

- Сотрудники посещают зоны, где они обычно не работают или куда они не имеют доступа;
- Сотрудники задают вопросы об организации, помещениях, руководстве или владельце;
- Сотрудники задают чрезмерно личные вопросы о других сотрудниках;
- Сотрудники делают заметки о ключевых зонах объекта или фотографируют их;
- Сотрудники разгуливают по территории объекта в необычное время без четкой, определенной или разрешенной цели;
- Сотрудники ведут себя нервно или тревожно без видимых причин, когда к ним обращаются или вовлекают в разговор;
- Сотрудники присутствуют на объекте в нерабочее время/работают вне обычного рабочего времени (без запроса со стороны непосредственного руководства);
- Сотрудники ведут себя скрытно при расспросах об их перемещениях, биографии или семьях;
- Сотрудники пытаются обойти или протестировать средства безопасности;
- Сотрудники запрашивают разрешение или доступ к системам более высокого уровня без необходимости;
- Поведение сотрудников демонстрирует внезапное обогащение без очевидной причины;
- Сотрудники продолжают иметь доступ к конфиденциальным данным после уведомления об увольнении;
- Сотрудники используют несанкционированные внешние устройства хранения данных;
- Сотрудники проявляют явное недовольство работодателем или коллегами;
- Сотрудники, систематически нарушающие политику организации;

386 Мартин, П. (2024 г.), *Инсайдерский риск и безопасность персонала: Введение* (Абингдон, Нью-Йорк: Рутледж).

387 Эти признаки частично позаимствованы из публикации БаМаунг, Д.; Бергин, Г.; Бирн, Дж.; Гарретт, Д.; Харрисон, А.; Мейплз, Л.; Куинн, Л. (2022 г.), *Терроризм и контрмеры*, Версия 2. (Нейс, графство Килдэр: Институт безопасности Ирландии).

- Сотрудники демонстрируют заметное и необъяснимое снижение производительности труда;
- Сотрудники раскрывают информацию, не предназначенную для публичного раскрытия, в общественных местах, средствам массовой информации или другим источникам.

Помимо этих потенциальных признаков, сотрудник может проявлять другие тревожные признаки, указывающие на то, что он может быть вовлечен в процесс радикализации, ведущей к насилию. К ним относятся активная поддержка идеологий насильственного экстремизма, использование уничижительных и агрессивных высказываний в адрес отдельных лиц, организаций или органов власти, поддержка насилия как необходимого средства для достижения цели и/или попытки радикализировать других лиц, склоняя к насилию.

Хотя ни один из этих тревожных признаков не должен обязательно рассматриваться как демонстрация намерения сотрудника причинить вред, они могут потребовать инициирования процедуры анализа и уточнения. Эта процедура должна включать в себя идентификацию и сопоставление всех признаков. Вместо того чтобы оценивать каждый признак по отдельности, их следует анализировать в совокупности, чтобы выявить скрытые или неочевидные взаимосвязи между ними.

8.4 Организационные меры реагирования на внутренние угрозы

Хотя владелец/оператор КВИ может применять различные отдельные меры по снижению внутренних угроз, отсутствие взаимосвязи между ними, как правило, будет означать лишь ограниченный итоговый успех. В то же время, не существует универсального *решения* проблемы внутренних угроз, как и не существует конкретного подхода, который был бы *лучше* других. Многое зависит от размера, структуры и корпоративной культуры конкретного объекта КВИ, а также от поддержки со стороны высшего руководства и соответствующего сектора.

Практика: набор инструментов Международной организации гражданской авиации для борьбы с инсайдерской угрозой[388]

Для оказания помощи организациям, работающим в авиационной среде, Международная организация гражданской авиации (ИКАО) разработала набор инструментов в сотрудничестве с Рабочей группой по подготовке Группы экспертов по авиационной безопасности ИКАО. Этот набор инструментов включает в себя рекомендации по мерам снижения рисков, проверке анкетных данных и проверке, обучению и повышению осведомленности, мерам контроля доступа, патрулированию, наблюдению и мониторингу, механизмам отчетности, выявлению поведенческих характеристик, культуре безопасности, лидерству и стратегии, человеческому фактору и передовым технологиям.

Источник: Международная организация гражданской авиации

Практика: набор инструментов Международной морской организации для борьбы с инсайдерской угрозой (2024 г.)[389]

В 2024 году Международная морская организация (ИМО) выпустила набор инструментов для борьбы с инсайдерской угрозой для организаций, работающих в морской среде, включая «морские администрации, уполномоченные органы, судоходные компании, портовых операторов и другие заинтересованные стороны в морской сфере». Этот набор инструментов был разработан совместно с ИКАО, поэтому он соответствует вышеупомянутому набору инструментов ИКАО.

Источник: Международная морская организация

Разработка целостной и последовательной программы, ориентированной на внутренние угрозы на объектах КВИ (включая кризисную коммуникацию в случае инсайдерских инцидентов, как обсуждалось в главе 7 «Планирование безопасности и укрепление объекта»), имеет неоспоримое преимущество. В США Агентство по кибербезопасности и защите инфраструктуры выделяет пять преимуществ такого подхода. Программа снижения внутренних угроз предоставляет владельцам/операторам КВИ возможность:

1. Создать и поддерживать безопасную среду для предотвращения насилия и других враждебных действий.
2. Сдерживать потенциальные внутренние угрозы путем внедрения политики, мер безопасности, процедур и программ для защиты организации.
3. Выявлять угрожающее или вызывающее беспокойство поведение и лиц, которые могут стать источником внутренней угрозы.

388 ИКАО (2022 г.), *Набор инструментов ИКАО для борьбы с инсайдерской угрозой.* Доступно по адресу: https://www.icao.int/Security/Security-Culture/Documents2/Insider Threat Toolkit.RU.pdf [дата обращения: 21 июля 2025 г.].

389 ИМО (без даты), *Набор инструментов для борьбы с инсайдерской угрозой,* издание 1. Доступно по адресу: https://www.imo.org/ru/ourwork/security/pages/insider-threat%20training%20aid.aspx [дата обращения: 21 июля 2025 г.].

4. Оценивать информацию о фактических или потенциальных внутренних угрозах.
5. Управлять потенциальными внутренними угрозами до того, как они перерастут в насилие, шпионаж, саботаж или кражу.[390]

Для руководства этим процессом доступны несколько подходов к разработке программы по борьбе с внутренними угрозами, предлагаемых государственными органами и частным сектором. В любой программе по борьбе с внутренними угрозами особое внимание следует уделять разработке четких процедур и мер безопасности, касающихся использования персональных данных в конкретных разрешенных целях в соответствии с местными законами и регламентами защиты данных.

Национальная практика: рекомендуемый Министерством общественной безопасности Канады контрольный список мер безопасности для повышения устойчивости объектов критически важной инфраструктуры к инсайдерским угрозам (2019 г.)[391]

В 2019 году Министерство общественной безопасности Канады выпустило документ, призванный предоставить канадским организациям КВИ руководство по определению инсайдерских угроз и рекомендации по мониторингу инсайдерских угроз, их снижению и реагированию и на них. Руководство представлено в виде восьми рекомендуемых мер безопасности, каждая из которых подробно описана ниже. В этом общедоступном документе также подробно описаны соответствующие применимые национальные и международные стандарты.

Мера безопасности № 1: Формирование культуры безопасности

- Определить ответственного за управление инсайдерскими угрозами в организации с полной ответственностью;
- Определить старшего руководителя, ответственного за разработку общекорпоративной политики и программы безопасности;
- Разработать структуру управления, включая рабочую группу по инсайдерским угрозам, для разработки и внедрения программы по борьбе с инсайдерскими угрозами и управления ею;
- Принять организационное «обязательство» признавать важность безопасности для обеспечения прибыльного и устойчивого бизнеса;
- Разработать комплексные меры политики и процедуры физической безопасности и кибербезопасности сетей, охватывающие все отделы; и
- Способствовать формированию культуры безопасности на всех уровнях, связывая эффективность работы сотрудников и руководства с показателями безопасности.

390 Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Руководство по смягчению внутренних угроз.* Доступно по адресу: https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide [дата обращения: 21 июля 2025 г.].

391 Управление критической инфраструктуры Министерства общественной безопасности Канады (2019 г.), *Повышение устойчивости критически важной инфраструктуры Канады к инсайдерскому риску.* Доступно по адресу: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/nhncng-crtcl-nfrstrctr-en.pdf [дата обращения: 21 июля 2025 г.].

Мера безопасности № 2: Разработка четких мер политики и процедур безопасности

- Четко определить, назначить и обучить сотрудников корпоративным мерам политики безопасности;
- Проводить проверку сотрудников на соответствие должностным требованиям; и
- Присвоить сотрудникам соответствующие уровни риска в зависимости критичности и важности информации, систем и областей, к которым они получают доступ.

Мера безопасности № 3: Снижение рисков со стороны партнеров и сторонних поставщиков

- Провести оценку рисков в масштабах всей организации, определив все ключевые объекты и критически важные системы;
- Выявить все проблемы безопасности, связанные с доступом третьих лиц к сетям, данным и системам организации;
- Провести независимую проверку уровня безопасности сторонних поставщиков услуг, включая проверку анкетных данных сотрудников, имеющих доступ к критически важным объектам или сетям организации;
- Заключить комплексные соглашения о безопасности со сторонними организациями, включив в них положения о гарантиях, чтобы снизить риск в цепочке поставок; и
- Выстраивать долгосрочные доверительные отношения с ключевыми поставщиками услуг.

Мера безопасности № 4: Внедрение жизненного цикла проверки персонала

- Проводить тщательную предварительную и постоянную проверку всего персонала, используя все доступные ресурсы, включая социальные сети;
- Обновлять права доступа и допуски для сотрудников в соответствии с их функциями и обязанностями;
- Изменять права доступа для сотрудников, перешедших на новые должности в организации; и
- Продвигать прозрачную программу безопасности для всех сотрудников, чтобы обеспечить соответствие требованиям физической и сетевой безопасности.

Мера безопасности № 5: Осуществление мероприятий по обучению, повышению осведомленности и проведение учений

- Разработать программу обучения по вопросам безопасности для всех сотрудников;
- Повышать осведомленность о признаках потенциальных угроз безопасности;
- Предоставить доступ к программам помощи сотрудникам, чтобы предотвратить риск превращения сотрудников во внутренних нарушителей;
- Развивать и продвигать культуру бдительности в вопросах безопасности, побуждая сотрудников сообщать об обнаруженных ими нарушениях; и
- Проводить периодические учения для проверки состояния безопасности в организации.

Мера безопасности № 6: Определение критически важных объектов и их защита

- Провести оценку в масштабах всей организации для выявления и ранжирования критически важных объектов и систем, а также мер безопасности для их защиты;
- Контролировать использование системы авторизованными и неавторизованными пользователями, а также физический доступ в помещения;
- Определить, как и какие данные передаются третьим лицам, а также степень конфиденциальности данных, а также обеспечить надлежащую защиту данных;
- Учитывать принцип наименьших привилегий и разделения обязанностей в отношении критически важных систем и данных; и
- Использовать видимые сдерживающие факторы для снижения вероятности непреднамеренного доступа к объектам, сетям и системам.

Мера безопасности № 7: Мониторинг необычного поведения, реагирование на него и смягчение его последствий

- Установить средства мониторинга физического и сетевого доступа со всех конечных точек и удаленных устройств;
- Развивать культуру, повышающую осведомленность сотрудников в вопросах безопасности и предполагающую уведомление о подозрительной активности или необычном поведении;
- Повышать осведомленность о потенциальных рисках, связанных с сайтами социальных сетей;
- По возможности ограничивать удаленный доступ к объектам и системам, не являющимся критически важными;
- Разработать протоколы для уведомления о необычных инцидентах, их отслеживания и реагирования на них; и
- Рассмотреть возможность взаимодействия со службами безопасности и разведки, включая [местные органы власти].

Мера безопасности № 8: Защита собственных данных

- Регулярно создавать резервные копии и защищать все организационные данные и основные системы;
- Разработать политику загрузки больших объемов данных или конфиденциальных файлов;
- Консолидировать точки доступа к Интернету;
- Внедрить раздельные системы для предотвращения потери данных; и
- Ограничить или запретить использование портативных устройств хранения данных.

Источник: Министерство общественной безопасности Канады

Национальная практика: Руководство Агентства по кибербезопасности и защите инфраструктуры США по ключевым элементам создания программы по борьбе с инсайдерскими угрозами (2020 г.)[392]

- Принципы и стандарты, которые согласуют программу с культурой и бизнесом организации и описывают ее цель и задачи;
- Создание приоритетного списка критически важных объектов (как физических, так и интеллектуальных), которые имеют важное значение для организации, и компрометация, повреждение или потеря которых могут оказать неблагоприятное влияние на ее миссию;
- Определение наиболее значимых и распространенных угроз и того, как они могут повлиять на критически важные объекты организации;
- Средства обнаружения и идентификации признаков потенциальных рисков;
- План реагирования на инциденты в случае возникновения внутренней угрозы;
- Комитет заинтересованных сторон по управлению и руководству программой;
- Организационная культура, которая поощряет уведомления об угрозах и предоставляет средства для этого:
- От сотрудников разумно ожидается, что они будут сообщать о потенциальных угрозах, признаках угроз или проблемах ответственной стороне, при этом им гарантируется конфиденциальность;
- Центральный информационный узел для сбора, интеграции, анализа и хранения всех данных, касающихся внутренних угроз;
- Группа управления угрозами для оценки потенциальных внутренних угроз, реагирования на них и управления ими;
- Программа обучения и повышения осведомленности о внутренних угрозах, призванная важность выявления потенциальных угроз и сообщения о них, а также важность того, что каждый сотрудник является первой линией обороны в деле защиты организации.

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры

Проверка персонала

В рамках эффективной системы обеспечения безопасности персонала и управления внутренними угрозами многие государственные органы и владельцы/операторы КВИ проводят проверки благонадежности сотрудников объектов КВИ и проверки анкетных данных. Проверка анкетных данных и соответствующие меры проверки благонадежности должны разрабатываться в соответствии с местными законами и правилами защиты данных, а также более широкими обязательствами в области прав человека. Подробнее см. главу 3 «Соображения в области прав человека».

392 Агентство по кибербезопасности и защите инфраструктуры США (без даты), *Руководство по смягчению внутренних угроз.* Доступно по адресу: https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide [дата обращения: 21 июля 2025 г.].

Национальная практика: процедура проверки анкетных данных AusCheck в Австралии[393]

Министерство внутренних дел Австралии руководит центром AusCheck, который предоставляет услуги проверки анкетных данных «критически важных работников, которые, по мнению ответственного органа, нуждаются в проверке анкетных данных AusCheck для получения доступа к критическим компонентам их критически важных инфраструктурных объектов» в «критически важных секторах инфраструктуры Австралии, требующих защиты». Проверка анкетных данных состоит из следующих проверок:

- установление личности;
- проверка судимости, проводимая AusCheck с использованием информации, собранной Австралийским оперативно-аналитическим управлением;
- оценка национальной безопасности, проводимая Австралийской службой безопасности и разведки;
- проверка «права на работу в Австралии», если человек не является гражданином Австралии, проводимая через онлайн-систему проверки прав на получение визы VEVO.

Источник: AusCheck

В Руководстве ИКАО предусматривается первоначальная проверка анкетных данных[394] для определенных категорий сотрудников гражданской авиации (например, «всех сотрудников, которым необходим несопровождаемый доступ в контролируемую зону и зоны ограниченного доступа, и сотрудников, имеющих доступ к конфиденциальной информации, касающейся авиационной безопасности»). Первоначальные проверки анкетных данных, предусмотренные ИКАО, включают в себя следующие виды проверок:

- установление личности (например, предоставление паспорта, удостоверения личности, свидетельства о рождения и т.д.);
- сведения о судимости (в объеме, допустимом местными нормативными актами и законами);
- проверку послужного списка (для подтверждения трудовой этики и общей пригодности потенциального сотрудника);
- сведения о трудовой деятельности (например, предыдущие работодатели, информация об образовании и т.д.).[395]

393 Правительство Австралии, Министерство внутренних дел (2 декабря 2024 г.), Проверка биографических данных объектов критически важной инфраструктуры [веб-страница]. Доступно по адресу: https://www.auscheck.gov.au/critical-infrastructure/critical-infrastructure-background-checks [дата обращения: 7 апреля 2025 г.].

394 ИКАО (2022 г.), *Приложение 17 "Авиационная безопасность. Защита международной гражданской авиации от актов незаконного вмешательства", 12 -е издание*, Принцип 3.5.2.

395 ИКАО (2022 г.), *Набор инструментов ИКАО для борьбы с инсайдерской угрозой.* Доступно по адресу: https://www.icao.int/Security/Security-Culture/Documents2/Insider Threat Toolkit.RU.pdf [дата обращения: 21 июля 2025 г.].

ИКАО также предоставляет рекомендации по повторным проверкам анкетных данных, постоянным мерам проверки, а также расширенным проверкам анкетных данных при необходимости. ИМО предоставляет аналогичные рекомендации в своем *Наборе инструментов для борьбы с инсайдерскими угрозами.*[396]

Статья 14 Директивы ЕС об устойчивости критически важных объектов отдельно посвящена проверкам анкетных данных. Помимо определения рамок, в которых должны проводиться проверки анкетных данных, в Директиве определено, что проверка должна, как минимум: «подтвердить личность лица, являющегося объектом проверки анкетных данных» и «проверить судимость этого лица за правонарушения, которые имели бы значение для занятия конкретной должности».[397]

396 ИМО (без даты), *Набор инструментов для борьбы с инсайдерской угрозой,* издание 1. Доступно по адресу: https://www.imo.org/ru/ourwork/security/pages/insider-threat%20training%20aid.aspx [дата обращения: 21 июля 2025 г.].

397 ЕС (2022 г.), Директива 2022/2557 Европейского парламента и Совета от 14 декабря 2022 года об устойчивости критически важных субъектов и отмене Директивы Совета 2008/114/ЕС, *OJ* L 333, Статья 14. Доступно по адресу: https://eur-lex.europa.eu/eli/dir/2022/2557/oj [дата обращения: 21 июля 2025 г.].

9 Подготовка и учения

«Подготовка и учения играют центральную роль в формировании устойчивых и сознательных в вопросах безопасности кадров на объекте критически важной инфраструктуры.»

9 Подготовка и учения

Подготовка и учения играют центральную роль в формировании устойчивых и сознательных в вопросах безопасности кадров на объекте КВИ. Участвуя в подготовке и учениях, персонал КВИ не только приобретает новые навыки, но и становится все более уверенным в своей способности управлять множеством ситуаций, включая кризисные. В частности, подготовка и учения с участием персонала КВИ и местных органов власти, участвующих в реагировании на инциденты безопасности на объекте КВИ, могут помочь сократить время реагирования и способствовать бесперебойному сотрудничеству в кризисных ситуациях. Для владельцев/операторов КВИ и их сотрудников службы безопасности учения, в частности, предоставляют возможность пересмотреть существующие планы и определить аспекты, требующие улучшения. Планы на бумаге являются важной отправной точкой, но их необходимо воплощать в жизнь и регулярно отрабатывать, чтобы оценить их эффективность. В этой главе подробно описывается важность подготовки и учений как части планового планирования и мероприятий по обеспечению безопасности на объекте КВИ.

По мнению Совета Безопасности ООН, подготовка кадров рассматривается как основной компонент усилий по защите КВИ от террористических атак. В Резолюции СБ ООН 2341 (2017 г.) Совет Безопасности особо признает

> «жизненно важную роль, которую просвещенные, бдительные общины играют в повышении осведомленности и информированности о существовании террористических угроз и, в частности, в выявлении подозрительной деятельности и направлении информации о ней правоохранительным органам, и важность расширения осведомленности и участия общественности и государственного-частного партнерства, сообразно обстоятельствам, особенно в отношении потенциальных террористических угроз и факторов уязвимости,

путем регулярного проведения диалога, подготовки кадров и информационно-пропагандистских мероприятий на общенациональном и местном уровнях».[398]

Масштаб мер, описанных в настоящем *Техническом руководстве,* которые предусматривают ту или иную форму подготовки сотрудников, свидетельствует о важной роли мер физической безопасности и борьбы с терроризмом для всего персонала КВИ и их профессионального развития. Подготовка может проводиться несколькими способами для обеспечения максимально широкого охвата, например, в виде учебных курсов в классе под руководством инструктора, курсов обучения на рабочем месте, учебных курсов, предоставляемых местными аварийно-спасательными службами или правоохранительными органами, или дистанционного обучения посредством веб-семинаров и самостоятельно осваиваемых учебных веб-курсов.[399] В идеале, владельцем/оператором КВИ должна быть разработана специальная программа подготовки, включающая в себя сочетание методов обучения, при этом оптимальное сочетание должно быть адаптировано к возможностям и потребностям персонала, проходящего подготовку.

Практический пример: взрыв на «Манчестер-Арене» в Великобритании в 2017 году

Последствия недостаточной подготовки персонала при террористическом акте могут быть катастрофическими. 22 мая 2017 года террорист-смертник взорвал ПСВУ в конце концерта Арианы Гранде на «Манчестер-Арене». В результате атаки погибли 22 зрителя и ожидавшие их родители, также на выходе с концертной площадки были ранены сотни детей и взрослых. В ответ на это в 2019 году тогдашний министр внутренних дел Великобритании инициировал официальное публичное расследование гибели жертв теракта. Публичное расследование по делу «Манчествер-Арены» установило, среди прочего, что частный поставщик услуг безопасности, нанятый оператором площадки, провел онлайн-обучение по борьбе с терроризмом для своего персонала, однако [поставщик] «должен был организовать вслед за этим онлайн-обучением практическое очное обучение для проверки и закрепления знаний, полученных в ходе онлайн-обучения, и повышения доверия к системе уведомления о подозрениях».[400]

Управление индустрии безопасности (SIA), являющееся регулятором индустрии частных охранных услуг Великобритании,[401] впоследствии изменило содержание

398 СБ ООН (2017 г.), Резолюция 2341 (S/RES/2341). Доступно по адресу: https://docs.un.org/ru/S/RES/2341(2017) [дата обращения: 21 июля 2025 г.].

399 Агентство по кибербезопасности и защите инфраструктуры США (ноябрь 2019 г.), *Руководство по безопасности и устойчивости критически важной инфраструктуры.* Доступно по адресу: https://cncpic.mai.gov.ro/sites/default/files/2020-03/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf [дата обращения: 21 июля 2025 г.].

400 Сондерс, сэр Дж. (июнь 2021 г.), *Расследование по делу «Манчестер Арены». Том 1: Безопасность на Арене. Отчет о публичном расследовании нападения на «Манчестер-Арене» 22 мая 2017 г.* Доступно по адресу: https://www.gov.uk/government/publications/manchester-arena-inquiry-volume-1-security-for-the-arena [дата обращения: 21 июля 2025 г.].

401 В Великобритании частная охранная индустрия регулируется Управлением индустрии безопасности (SIA). SIA принимает решение о содержании учебных курсов, которые проходят сотрудники службы безопасности для получения соответствующей лицензии для своей деятельности. Сотрудники службы безопасности обязаны получить лицензию, прежде чем они смогут выполнять определенные функции по обеспечению безопасности. Обучение рассматривается как неотъемлемая часть требования лицензирования. Для получения дополнительной информации см.: https://www.gov.uk/guidance/check-what-training-you-need-to-get-an-sia-licence.

своего учебного курса для сотрудников частных охранных компаний, добавив больше антитеррористического содержания более высокого качества.[402]

В ответ на отчет о расследование полиция Большого Манчестера признала, что «плохая связь, ненадлежащее планирование, недостаточная подготовка и пробелы в стратегическом руководстве сыграли свою роль в нашем провале. Все эти недостатки могли и должны были быть выявлены и смягчены путем обучения на тщательно разработанных учебных курсах под эгидой нашего Форума по местной устойчивости. Увы, эти возможности не были в полной мере использованы».[403]

Проверка знаний обучаемых в ходе учений является одним из лучших способов оценки эффективности программ подготовки, поскольку позволяет участникам продемонстрировать полученные ими навыки в безопасной обстановке, а не в условиях реальной чрезвычайной ситуации. Учения также могут использоваться для выявления пробелов и уязвимостей в планах, процедурах, мерах и составе персонала. Они весьма полезны при подготовке к террористическим угрозам, поскольку при наступлении такого кризиса люди и персонал, скорее всего, будут испытывать сильный стресс и реагировать необдуманно, что может привести к ошибочным или нерациональным действиям.[404]

9.1 Подготовка

Подготовка играет важную роль в повышении физической безопасности объектов КВИ, особенно в связи с уникальной угрозой, которую представляют собой террористические атаки. Угрозы КВИ различаются по сложности и воздействию. Появление сложных технологических угроз, таких как кибератаки или использование БАС, добавило новое измерение риска. В связи с этим персонал объекта КВИ, отвечающий за безопасность объекта или работающий на объекте в рамках любой должностной категории, должен обладать достаточными навыками для понимания и реагирования на угрозы, с которыми сталкиваются объекты КВИ. Обучение может проводиться компетентными государственными органами, владельцами/операторами КВИ, частными компаниями и другими организациями.

Поскольку большинство объектов КВИ в регионе ОБСЕ принадлежит частным лицам или управляется ими, подготовку персонала объектов по вопросам предотвращения террористических атак и реагирования на них наиболее эффективно осуществлять в сотрудничестве с национальными органами власти, а также, при необходимости, с частными поставщиками услуг безопасности. Ранее ОБСЕ подчеркивала, что подготовка персонала объектов КВИ в сфере реагирования на инциденты, которая

402 Сондерс, сэр Дж. (июнь 2021 г.), *Расследование по делу «Манчестер Арены». Том 1: Безопасность на Арене. Отчет о публичном расследовании нападения на «Манчестер-Арене» 22 мая 2017 г.* Доступно по адресу: https://www.gov.uk/government/publications/manchester-arena-inquiry-volume-1-security-for-the-arena [дата обращения: 21 июля 2025 г.].

403 Полиция Большого Манчестера (3 ноября 2022 г.), Заявление в ответ на отчет о расследовании инцидента на Манчестер-Арене, том 2 [веб-страница]. Доступно по адресу: https://www.gmp.police.uk/news/greater-manchester/news/news/2022/november/statement-in-response-to-inquiry-report/ [дата обращения: 31 августа 2024 г.].

404 Федеральное управление информационной безопасности (2008 г.), *Стандарт 100-4. Управление в чрезвычайных ситуациях.* Доступно по адресу: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2. [дата обращения: 21 июля 2025 г.].

проводится с участием представителей местных органов власти, особенно полезна для разработки эффективного подхода к управлению кризисными ситуациями на основе ЧГП.[405]

Национальная практика: возможные темы подготовки, рекомендуемые Агентством по кибербезопасности и защите инфраструктуры США для персонала критически важной инфраструктуры (2019 г.)[406]

- Передовые методы практики обеспечения физической безопасности
- Активный стрелок
- Выявление подозрительной активности и сообщение о ней
- Внутренняя угроза
- Аттестация
- Проверка сумок
- Проверка посетителей
- Передовые методы практики секторах (например, химическая промышленность, энергетика, водоснабжение)
- Управление рисками в цепочке поставок и зависимость от третьих сторон
- Управление инцидентами и реагирование на угрозы взрыва
- Противодействие самодельным взрывным устройствам
- Угрозы, связанные с транспортными средствами
- Террористы-смертники
- Кибербезопасность
- Учения
- Угрозы терроризма, тактика и тенденции
- Промышленная система управления и операционные технологии
- Оценка рисков (угрозы, уязвимости и/или последствия) и снижение рисков

Источник: Министерство внутренней безопасности США, Агентство по кибербезопасности и защите инфраструктуры

405 ОБСЕ (2013 г.), *Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства.* Доступно по адресу: https://www.osce.org/files/f/documents/5/2/110472.pdf [дата обращения: 21 июля 2025 г.].

406 Агентство по кибербезопасности и защите инфраструктуры США (ноябрь 2019 г.), *Руководство по безопасности и устойчивости критически важной инфраструктуры.* Доступно по адресу: https://cncpic.mai.gov.ro/sites/default/files/2020-03/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf [дата обращения: 21 июля 2025 г.].

9.2 Учения

Учения представляют собой отработку определенных навыков или плана в безопасной обстановке и взаимодействие с другими лицами, которые могут быть затронуты на объекте КВИ или рядом с ним в результате потенциального инцидента. Учения могут использоваться для оценки актуальности учебных курсов, эффективности оборудования, межведомственных/многосторонних соглашений или ЧГП. Учения для защиты КВИ могут проводиться на разных уровнях:

- *На уровне объекта* могут быть организованы общеобъектовые учения по реагированию на террористическую атаку с применением огнестрельного оружия, или могут быть организованы менее масштабные учения с небольшой группой сотрудников (включая, при необходимости, частные охранные компании), ориентированные, например, на реагирование на террористическую атаку с использованием СВУ, заложенных в транспортные средства.
- *На уровне владельца/оператора КВИ* могут быть организованы общекорпоративные учения на случай отключения электроэнергии, которое может затронуть несколько объектов, находящихся в ведении владельца/оператора.
- *На уровне сектора* можно организовать общеотраслевые учения для проверки устойчивости сектора к перебоям в цепочке поставок, например.

Национальная практика: учения по действиям в чрезвычайных ситуациях для обеспечения безопасности поставок газа на Мальте (2020 г.)[407]

В рамках мальтийской программы по планированию действий в чрезвычайных ситуациях на случай крупных аварий с опасными веществами компания Enemalta, крупнейший поставщик энергетических услуг на Мальте, обязана проводить многосторонние учения по реагированию на чрезвычайные ситуации с участием всех соответствующих заинтересованных сторон на единственном в стране плавучем газохранилище. Помимо учений на случай пожара, утечек химикатов и других непреднамеренных инцидентов, ожидается, что учения по ликвидации последствий нарушений безопасности будут проводиться четыре раза в год, а по ликвидации последствий взрывов – два раза в год.

Источник: Министерство окружающей среды Мальты

Управление ООН по борьбе с терроризмом заявляет, что «на практике необходимо применять различные формы учений в зависимости от поставленных целей, числа участвующих субъектов и участников, наличия ресурсов и т. д.».

«В контексте ЗКВОИ межучережденческие учения / тренинги повсеместно признаны в качестве важного инструмента для проведения как минимум следующих целей:

- Достичь общего понимания применимых процессов и методологий;
- Выяснить роль и ответственность в циклах защиты КВОИ;
- Укрепить уверенность персонала в выполнении инструкций и политик по защите, связанных с КВОИ (важно во время стрессовых фаз реального кризиса);
- Выявить слабые стороны и внести любые изменения, необходимые для безопасного исхода реальной аварийной ситуации;
- Гарантировать, что эксплуатационная надежность и совместимость всего оборудования связи предназначены для использования во время инцидента».[408]

407 Министерство окружающей среды, энергетики и общественной чистоты Мальты (2022 г.), *План действий в чрезвычайных ситуациях на Мальте: безопасность поставок газа.* Доступно по адресу: https://sostenibilita.gov.mt/wp-content/uploads/2023/11/MT-Gas-SOS-Emergency-Plan.pdf [дата обращения: 21 июля 2025 г.].

408 UNOCT, Исполнительный директорат Контртеррористического комитета Совета Безопасности ООН (2022 г.), *Защита критически важных объектов инфраструктуры от террористических атак: Сборник передового опыта.* Доступно по адресу: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf [дата обращения: 21 июля 2025 г.].

Национальная практика: Руководство по проведению учений Министерства общественной безопасности Канады для критически важных секторов инфраструктуры (2022 г.)[409]

Министерство общественной безопасности Канады призывает секторы и владельцев/операторов КВИ разрабатывать и провести учения по «проверке и отработке действий, планов и систем по снижению рисков». Учения могут преследовать несколько целей, например:

- стимулирование налаживания отношений между отраслями и дисциплинами;
- уточнение ролей, обязанностей и возможностей;
- выявление и устранение зависимостей и взаимозависимостей критически важной инфраструктуры;
- повышение осведомленности о рисках для критически важной инфраструктуры;
- предоставление персоналу возможности отработать назначенные роли;
- определение степени готовности к конкретному инциденту; и
- выявление пробелов в протоколах связи, рабочих процедурах и процедурах реагирования на чрезвычайные ситуации.

Министерство общественной безопасности Канады призывает владельцев/операторов КВО и заинтересованные стороны рассмотреть возможность участия в учениях различного типа:

Командно-штабные учения: Метод отработки планов, при котором участники выполняют некоторые или все действия, которые они предприняли бы в случае активации плана в ответ на определенный сценарий. Конкретные действия не выполняются.

Функциональные учения: Метод отработки планов, при котором участники рассматривают и обсуждают действия, которые они предпримут в ответ на определенный сценарий, представленный организатором учений.

Полноценные оперативные учения: Метод отработки планов, при котором участники приостанавливают обычную работу и активируют планы, как если бы событие было реальным.

Источник: Министерство общественной безопасности Канады

В некоторых случаях государственные органы власти требуют от владельцев/операторов КВИ, предоставляющих критически важные услуги населению, подготовки планов учений как в целом по всему сектору, как и в качестве отдельных поставщиков. На практике в процессе разработки планов учений должны участвовать все заинтересованные стороны, включая владельцев/операторов КВИ, правоохранительные органы, представителей национальных и местных органов власти, органы реагирования на чрезвычайные ситуации, военных (при необходимости) и других субъектов.

409 Министерство общественной безопасности Канады (1 июля 2010 г.), *Руководство по управлению рисками для критически важных секторов инфраструктуры*. Версия 1. Доступно по адресу: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-mngmnt-gd/rsk-mngmnt-gd-eng.pdf [дата обращения: 21 июля 2025 г.].

Национальная практика: Закон Эстонии о чрезвычайных ситуациях (2017 г.)[410]

Закон Эстонии о чрезвычайных ситуациях (2017 г.) обеспечивает основу управления кризисами для разрешения чрезвычайных ситуаций и обеспечения непрерывности жизненно важных услуг, потенциально предоставляемых КВИ страны. Глава 5 закона определяет эти жизненно важные услуги, включая электроснабжение, поставку природного газа, услуги телефонной и мобильной связи, платежные услуги, централизованное отопление, водоснабжение и канализацию и другие. Поставщики жизненно важных услуг обязаны, *в частности,* «организовывать учения для проверки непрерывности предоставляемых ими жизненно важных услуг не реже одного раза в два года».

Источник: Правительство Эстонии

Оценка после учений

Учения всегда должны сопровождаться процессом оценки, при котором четко определяются и анализируются успехи и неудачи. Должны быть признаны и устранены недостатки, разработаны рекомендации и определены последующие действия. Например, если владельцы/операторы КВИ не получают объективных замечаний (в том числе об их неудачах) от соответствующих государственных органов, у них может сложиться неверное представление о своих возможностях противостоять такому инциденту, как террористическая атака. Это может иметь негативные последствия, если атака произойдет, а согласованные и запланированные процессы не сработают, что приведет к гибели людей или потере критически важных услуг.[411]

410 Правительство Эстонии, Закон о чрезвычайных ситуациях (3 марта 2017 г., Эстония). Доступно по адресу: https://www.riigiteataja.ee/EN/ELI/511122019004/CONSOLIDE [дата обращения: 31 августа 2024 г.].

411 ОБСЕ (2013 г.), *Руководство по передовой практике защиты критически важной неядерной энергетической инфраструктуры (NNCEIP) от террористических атак с упором на угрозы, исходящие из киберпространства.* Доступно по адресу: https://www.osce.org/files/f/documents/7/5/103954.pdf [дата обращения: 21 июля 2025 г.].

10 Возможности существенной эскалации угроз

«Существенная эскалация угроз очень важна для объектов критически важной инфраструктуры, поскольку они работают в условиях быстро меняющихся угроз, а атаки на них могут иметь местные, национальные, региональные или международные последствия.»

10 Возможности существенной эскалации угроз

Хотя многие меры физической безопасности, описанные в настоящем *Техническом руководстве,* являются статичными, угроза, которую они призваны снизить, является динамической. У каждого объекта КВИ есть свой собственный профиль угрозы. В случае террористических угроз этот профиль может зависеть от глобальных или региональных событий, идеологии террористических организаций, их возможностей в конкретной стране, их стратегических целей (которые также являются динамичными) и ряда других факторов. Важно учитывать эти факторы при оценке профиля угрозы объекта КВИ компетентным персоналом службы безопасности. Это шаг, который необходимо выполнять на регулярной основе. В некоторых случаях владелец/оператор КВИ получает общую или конкретную информацию об угрозе, требующую актуализации мер безопасности на объекте. Хотя возможные типы такой информации об угрозах сложно предсказать, они могут быть связаны со следующими факторами:

- террористическая организация публикует изображения объекта КВИ с явным намерением немедленно совершить на него нападение;
- правительственная разведка или правоохранительные органы выявили готовящийся террористический акт, целью которого является объект КВИ;
- террористическая организация обращается к своим «спящим» ячейкам или боевикам-одиночкам по всему миру с призывом атаковать КВИ конкретного типа.

В подобных случаях владелец/оператор КВИ может принять меры в ответ на это изменение уровня угрозы, также известные как варианты эскалации угрозы. В этой главе подробно описываются такие заранее запланированные меры, применяемые владельцами/операторами КВИ в ответ на повышение уровня угрозы.

10.1 Национальные оценки террористической угрозы

Государства-участники в регионе ОБСЕ и за его пределами используют национальные системы уровней террористической угрозы для представления общенациональной оценки террористических угроз, с которыми сталкивается страна. Эти системы сопоставляют угрозу с заранее определенными уровнями, давая общее представление о вероятности террористического акта. Национальные уровни террористической угрозы являются частью оценки владельцем/оператором КВИ своей среды угроз и общего риска (для получения дополнительной информации см. главу 5 «Угроза терроризма и оценка рисков»).

Государство-участник	Система национальной оценки террористической угрозы
Великобритания[412]	Низкий уровень: нападение крайне маловероятно. Средний уровень: нападение возможно, но маловероятно. Существенный уровень: нападение вероятно. Высокий уровень: нападение весьма вероятно. Критический уровень: нападение весьма вероятно в ближайшем будущем.
Латвия[413]	Низкий уровень: общая угроза терроризма. Повышенный уровень: растущая угроза терроризма. Высокий уровень: подтверждена террористическая угроза для конкретного объекта, сектора экономики или региона. Очень высокий уровень: террористический акт уже произошёл или неизбежен.
Российская Федерация[414]	Повышенный уровень: наличие требующей подтверждения информации о реальной возможности совершения террористического акта. Высокий уровень: наличие подтвержденной информации о реальной возможности совершения террористического акта. Критический уровень: наличие информации о совершенном террористическом акте либо о совершении действий, создающих непосредственную угрозу террористического акта.
Нидерланды[415]	Уровень 1: минимальный: террористический акт в Нидерландах маловероятен. Уровень 2: ограниченный: существует небольшая вероятность террористического акта в Нидерландах. Уровень 3: значительный: террористический акт в Нидерландах возможен. Уровень 4: существенный: существует реальная вероятность террористического акта в Нидерландах. Уровень 5: критический: террористический акт в Нидерландах неизбежен.

412 Национальное управление по борьбе с терроризмом, ProtectUK (12 марта 2022 г.), Уровни угроз [веб-страница]. Доступно по адресу: https://www.protectuk.police.uk/threat-levels [дата обращения: 16 декабря 2024 г.].

413 Служба государственной безопасности Латвии (2024 г.), Борьба с терроризмом. Доступно по адресу: https://vdd.gov.lv/en/areas-of-activity/counterterrorism [дата обращения: 16 декабря 2024 г.].

414 Национальный антитеррористический комитет (август 2023 г., Российская Федерация). Уровни террористической опасности. Доступно по адресу: http://nac.gov.ru/urovni-terroristicheskoy-opasnosti.html [дата обращения: 16 декабря 2024 г.].

415 Национальный координатор по борьбе с терроризмом и безопасности (2024 г.), Terrorist Threat Assessment Netherlands [веб-страница]. Доступно по адресу: https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands [дата обращения: 24 июля 2024 г.].

Канада[416]	Очень низкий уровень: вероятность насильственного теракта крайне мала (действуют меры по обеспечению безопасности канадцев). Низкий уровень: насильственный теракт возможен, но маловероятен (действуют меры по обеспечению безопасности канадцев). Средний уровень: насильственный теракт может произойти (принимаются дополнительные меры для обеспечения безопасности канадцев). Высокий уровень: насильственный теракт вероятен (принимаются усиленные меры для обеспечения безопасности канадцев. Канадцы проинформированы о том, какие действия следует предпринять). Критический уровень: вероятность насильственного теракта весьма высока, и он может произойти (приняты исключительные меры для обеспечения безопасности канадцев. Канадцы проинформированы о том, какие действия следует предпринять).

10.2 Возможности существенной эскалации угроз

Для каждого объекта КВИ изменения в оцененном уровне угрозы должны инициировать пересмотр действующих мер безопасности. Одним из факторов, способных повлиять на изменение оцененного уровня угрозы, является изменение уровня национальной угрозы терроризма. Однако это происходит не всегда, поскольку национальные уровни угрозы терроризма редко содержат конкретные, целевые оперативные данные или информацию (т.е. указывающие на угрозу безопасности конкретного объекта КВИ). Решение об изменении оцененного уровня угрозы на объекте КВИ должно приниматься владельцами/операторами КВИ совместно с местными органами власти и другими заинтересованными сторонами, при необходимости.

Необходимо разработать расширенные возможности существенной эскалации угроз для обеспечения структурированного и масштабируемого подхода, гарантирующий, чтоответ будет соразмерен потенциальному риску и сможет эффективно смягчить последствия. Варианты эскалации угроз жизненно важны для объектов КВИ, поскольку они работают в условиях быстро меняющихся угроз, а атаки на них могут иметь локальные, национальные, региональные или международные последствия.

416 Правительство Канады (2023 г.), Национальные уровни террористической угрозы в Канаде [веб-страница]. Доступно по адресу: https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html [дата обращения: 16 декабря 2024 г.].

Национальная практика: система оповещения об угрозах критически важной инфраструктуре в Испании[417]

Система оповещения об угрозах КВИ в Испании структурирована по уровням, каждый из которых связан с определенной степенью риска: уровень 1 – низкий риск, уровень 2 – умеренный риск, уровень 3 – средний риск, уровень 4 – высокий риск и уровень 5 – очень высокий риск. Активация уровня запускает реализацию набора заранее определенных мер, адаптированных к статусу и характеру угрозы.

Как правило, уровень риска совпадает с уровнем, установленным в рамках общего странового плана по предотвращению терроризма и защите от него. Однако эти два уровня не обязательно пересекаются. Расхождение может быть связано с разной оценкой угрозы, проводимой агентством, отвечающим за защиту КВИ. Особое внимание уделяется намерению, возможностям и вероятности совершения преднамеренной атаки на владельцев/операторов КВИ, предоставляющих критически важные услуги гражданам Испании.

Источник: Министерство внутренних дел Испании

В основе существенной эскалации угроз лежит способность динамически корректировать меры безопасности на основе новой информации/оперативных данных и оценки рисков. Этот процесс обычно включает в себя несколько уровней реагирования, каждый из которых соответствует определенному уровню угрозы. Например, объект КВИ может начать с усиления мониторинга и активизации взаимодействия между службами безопасности при более низком уровне угрозы. Дополнительные меры могут быть реализованы по мере эскалации угрозы, например, привлечение дополнительного персонала службы безопасности, активация протоколов экстренного реагирования или усиление физических барьеров.

В сценариях с наивысшим уровнем угрозы на объекте КВИ могут быть задействованы правоохранительные органы или специализированные группы реагирования и реализованы процедуры изоляции или эвакуации (подробнее см. в главе 7 «Планирование безопасности и укрепление объекта»). Ключевым фактором успешных планов эскалации угроз является заблаговременное определение каждого уровня реагирования, что гарантирует оперативность и скоординированность действий. Не менее важно распознавать, когда следует снижать эскалацию и сокращать масштабы мер реагирования по мере снижения уровня угрозы, учитывая, что они могут оказаться неустойчивыми в долгосрочной перспективе.

417 Национальный план защиты критически важной инфраструктуры (без даты), Уровень тревоги для критически важной инфраструктуры (NAIC) [веб-страница]. Доступно по адресу: https://cnpic.interior.gob.es/es/naic/ [по состоянию на 24 июля 2024 г.].

Национальная практика: перечень тактических вариантов действий, рекомендуемых заинтересованным сторонам Национальным управлением по борьбе с терроризмом и безопасности Великобритании (2023 г.)[418]

В Великобритании разработан «набор мер, которые могут быть использованы частным сектором и охранной индустрией для укрепления национальной безопасности в периоды повышенной угрозы или в ответ на террористический акт». Предлагаются следующие варианты:

- Закройте необязательные точки доступа и выхода.
- Найдите ближайшие парковочные места и проверьте доступ к ним.
- Убедитесь, что все посетители и подрядчики уведомили о своем визите не менее чем за 24 часа.
- Обеспечьте постоянное сопровождение посетителей и подрядчиков.
- Отмените или перенесите мероприятия.
- Обеспечьте, чтобы личность всех сотрудников была установлена и их удостоверения личности были проверены.
- Проверьте все транспортные средства и персонал на въезде, включая аварийно-спасательные службы.
- Осуществляйте регулярный и непредсказуемый обход и обыск территории, включая зоны, скрытые от наблюдения.
- Ограничьте поставки и принимайте только те, которые необходимы.
- Проверяйте всю почту и убедитесь в действии надежных сортировочных процедур.
- Просмотрите и доведите до сведения персонала и соседних предприятий планы реагирования на инциденты и обеспечения непрерывности деятельности.
- Обеспечьте полное соблюдение контрольного списка по реагированию на инциденты и планированию непрерывности деятельности.
- Убедитесь, что процедуры изоляции доведены до всех, опробованы и отработаны.
- Обеспечьте пригодность путей эвакуации и точек сбора.
- Обеспечьте, чтобы все сотрудники были проинформированы о ролях и обязанностях во время инцидента в соответствии с планами и процедурами реагирования.
- Обеспечьте актуальность, безопасность и легкий доступ к содержимому аптечек первой помощи при кризисных ситуациях и аптечек для оказания первой помощи при травмах.
- Подготовьте оповещения, сигналы тревоги и заранее подготовленные сообщения.
- Обеспечьте информирование персонала об уровнях угроз и реагирования.
- Обеспечьте, чтобы персонал был проинструктирован о том, как наблюдать, обнаруживать и реагировать на подозрительную активность.
- Обеспечьте своевременное сообщение о любом подозрительном поведении.

418 Национальное управление по борьбе с терроризмом, ProtectUK (14 декабря 2023 г.) Меню тактических вариантов действий для национальных заинтересованных сторон. Доступно по адресу: https://www.protectuk.police.uk/advice-and-guidance/security/national-stakeholder-menu-tactical-options-0 [дата обращения: 16 декабря 2024 г.].

- Внедрите каналы связи с окружающими объектами для передачи информации и сообщений о подозрительной деятельности.
- Постоянно осуществляйте активный мониторинг [систем видеонаблюдения] и просматривайте отснятый в нерабочее время материал.
- Убедитесь, что [системы видеонаблюдения] направлены на все общественные зоны и уязвимые точки.
- Обеспечьте надежный режим безопасности с помощью коммуникации с учетом вопросов безопасности.
- Проверьте режим патрулирования и расстановки сотрудников службы безопасности.
- Обеспечьте проверку периметрального ограждения и охранного освещения.
- Внедрите экстренное изменение графика смен и заранее согласуйте план с персоналом.
- Объедините ресурсы с соседними предприятиями и контактными лицами.
- Отмените все необязательные тренинги и встречи.
- Обеспечьте согласование стратегии коммуникации и документируйте все решения, включая обоснование.
- Убедитесь, что вспомогательные технологии, такие как системы контроля доступа, находятся в рабочем состоянии.
- Разработайте или пересмотрите план борьбы с беспилотными летательными аппаратами/беспилотными авиационными системами.

Источник: Национальное управление по борьбе с терроризмом и безопасности Великобритании

10.3 Стоимость вариантов существенной эскалации угроз

Варианты эскалации угроз можно классифицировать по уровню связанных с ними затрат. Классифицируя варианты эскалации угроз таким образом, владельцы/операторы КВИ могут лучше оценивать и выбирать подходящие меры реагирования, исходя из своих стратегических целей и доступности ресурсов.

Высокозатратные варианты

Значительные затраты ресурсов, такие как развертывание правительственных сил безопасности или внедрение обширных систем безопасности, которые могут ограничить возможности владельца/оператора КВИ при непропорциональном использовании.

Варианты с разделением затрат

Затраты распределяются между несколькими сторонами, например, посредством частного-государственного партнерства, что позволяет сократить индивидуальные расходы и одновременно использовать коллективный потенциал.

Малозатратные варианты

Минимальные ресурсы, часто с опорой на существующие возможности, которые позволяют достичь целей без существенных финансовых или логистических обязательств.

Беззатратные варианты

Используются легкодоступные или нематериальные активы, усиливая влияние и связи без прямых финансовых затрат.

ОБСЕ Организация по безопасности и сотрудничеству в Европе

PROTECT
ОБЗОР ПРОЕКТА

Проект по защите уязвимых целей от террористических атак или “Проект PROTECT” укрепляет национальные подходы по защите уязвимых объектов от террористических атак и других опасностей по всему региону ОБСЕ, посредством предоставления специализированных рекомендаций, технической помощи, а также возможностей для регионального сотрудничества и построения диалога об эффективных методах обеспечения безопасности.