УДК: 001.891.53

Особенности защиты объектов в местах проведения крупных общественно-политических и спортивно-массовых мероприятий

Features of protecting facilities at venues for large socio-political and sports events

И.В. Мороз © **I.V. Moroz ©**

Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации, г. Москва, Российская Федерация

E-mail: MorozIV@rosgvard.ru

Аннотация. В статье отражены особенности и рекомендации по защите ИТСО объектов в местах проведения крупных общественно-политических и спортивно-массовых мероприятий. Проведение крупномасштабных мероприятий требует комплексного подхода к вопросам безопасности, основанного на интеграции правовых механизмов, технологических инноваций и чётких процедур взаимодействия сил правопорядка и организаторов.

Abstract. The article reflects special features and provides recommendations on how to protect technical security equipment of facilities at venues for large socio-political and sports events. Major events require a comprehensive security approach, based on the integration of legal mechanisms, technology innovations and clear procedures for cooperation between law enforcement forces and event organizers.

Ключевые слова: инженерно-технические средства охраны; технические средства охраны; объект; антитеррористическая защищенность; защита; безопасность

Keywords: engineering and technical security equipment (ITSO); technical security equipment (TSO); facility; anti-terrorist security; protection; security

ДЛЯ ЦИТИРОВАНИЯ: Мороз И.В. Особенности защиты объектов в местах проведения крупных общественно-политических и спортивно-массовых мероприятий // Академический вестник войск национальной гвардии Российской Федерации. – 2026. – № 1. – С. 43–52.

Проведение крупных общественно-политических и спортивно-массовых мероприятий в Российской Федерации сопряжено с повышенными рисками террористических, криминальных и техногенных угроз. В условиях роста сложности и масштабов таких событий – от международных форумов до спортивных соревнований мирового уровня – обеспечение антитеррористической защищенности объектов становится задачей стратегического значения. Современная модель безопасности опирается на принцип комплексного, многоуровневого подхода, в котором ключевую роль играют нормативно-методические основы, инженерно-технические решения и интегрированные системы защиты.

Накопленный опыт проведения Олимпийских игр в Сочи (2014), Чемпионата мира по футболу FIFA (2018) и других мероприятий высокого уровня позволил сформировать отечественную систему обеспечения безопасности, основанную на дифференциации объектов по категориям угрозы, зонировании территорий, строгом контроле доступа и применении передовых технических средств охраны (далее – ТСО). Однако актуальность дальнейшей разработки и систематизации этих подходов сохраняется: с одной стороны, из-за динамично меняющейся обстановки, с другой – из-за необходимости балансировать между максимальной защитой и функциональной эффективностью объектов, особенно временных или многоцелевых.

Настоящая статья направлена на анализ и обобщение современных требований к обеспечению антитеррористической защищенности объектов массовых мероприятий, с акцентом на интеграцию инженерных, технических и организационных мер. Рассматриваются ключевые компоненты системы безопасности: контрольно-пропускной режим, периметральная защита, система контроля и управления доступом (далее – СКУД), система охранно-тревожной сигнализации (далее – СОТС), система охранная телевизионная (далее – СОТ), видеонаблюдение, охранное освещение, технические средства осуществления контроля (далее – ТСОК) и системы электропитания. Особое внимание уделяется устранению внутренних противоречий в нормативных требованиях и формированию гибкой, отказоустойчивой архитектуры, способной адаптироваться под специфику каждого мероприятия. Актуальность данного исследования обусловлена необходимостью повышения надежности, эффективности и научной обоснованности практик обеспечения безопасности в условиях растущих вызовов современности.

Согласно федеральному законодательству, антитеррористическая защищенность объекта определяется как состояние защищенности зданий, сооружений, территорий и мест массового пребывания людей, препятствующее совершению террористического акта (п. 6 ст. 3 Федерального закона № 35-ФЗ [2], п. 2 ст. 2 Федерального закона № 256-ФЗ [3]). Инженерно-техническая защита подобных объектов регламентируется Федеральным законом от 30 декабря 2009 г. № 384-ФЗ [4], в соответствии с которым меры безопасности должны реализовываться на всех этапах жизненного цикла объекта – от проектирования до эксплуатации, реконструкции и капитального ремонта.

Для обеспечения пропорциональности мер безопасности уровню угрозы применяется система категорирования объектов, основанная на оценке потенциальных последствий террористического акта. Так, для мест массового пребывания населения применяются критерии, установленные Постановлением Правительства РФ от 25 марта 2015 г. № 272 [4], а для спортивных сооружений – специализированные требования Постановления Правительства РФ от 6 марта 2015 г. № 202 [5]. В случае, если объект одновременно используется для спортивных и иных общественно значимых мероприятий, категория устанавливается по наиболее строгому из применимых нормативных актов, что исключает дублирование и обеспечивает единообразие подходов.

Одним из ключевых элементов современной модели безопасности является зонирование территории объекта. Для целей планирования и управления доступом объект с прилегающей территорией условно разделяется на четыре функциональные зоны:

Зона № 1 – непосредственное место проведения мероприятия (игровое поле, сцена, площадка);

Зона № 2 – зрительские сектора, фойе, точки общественного питания и сервисные помещения;

Зона № 3 – прилегающая инфраструктура: парковки, зоны СМИ, гостеприимства, выставочные павильоны;

Зона № 4 – внешняя зона, включающая подъездные пути, площадки для накопления зрителей и остановки общественного транспорта.

Зоны № 2 и № 3 дополнительно дифференцируются на общественные и служебные зоны, что позволяет строго регулировать доступ различных категорий персонала и посетителей: от VIP-персон и спортсменов до представителей СМИ, обслуживающего персонала и сотрудников экстренных служб. Каждая категория обеспечивается отдельными входами и досмотровыми маршрутами, что минимизирует риски конфликтов потоков и повышает эффективность контроля.

Предложенный подход – основанный на четкой нормативной базе, дифференциации объектов по категориям риска и функциональному зонированию территории – обладает рядом значимых преимуществ.

Во-первых, он обеспечивает пропорциональность мер безопасности уровню реальной угрозы, что позволяет избежать избыточного расходования ресурсов на объектах низкого риска и сосредоточить усилия там, где последствия теракта могут быть катастрофическими.

Во-вторых, единая система зонирования (четыре основные зоны с подразделением на общественные и служебные) создает прозрачную архитектуру управления доступом, минимизируя пересечение потоков VIP-персон, зрителей, персонала и спецслужб, что снижает как риски безопасности, так и логистические сложности.

В-третьих, четкая привязка требований к конкретным нормативным актам обеспечивает правовую определенность и упрощает проектирование и экспертизу объектов.

Вместе с тем, данный подход имеет и определенные ограничения. Основной недостаток – жесткость категоризации, которая не всегда учитывает динамику угроз: объект может быть отнесен к низкой категории за день до мероприятия, но стать мишенью из-за политической конъюнктуры. Кроме того, формальное зонирование не всегда реализуемо на практике, особенно на исторических объектах, реконструируемых площадках или в условиях плотной городской застройки, где физическое разделение зон № 3 и № 4 затруднено. Наконец, четкое разграничение доступа требует значительных людских и технических ресурсов, что может быть непосильно для региональных мероприятий с ограниченным бюджетом.

Таким образом, несмотря на отдельные ограничения, описанный подход остается наиболее сбалансированным и системным решением для обеспечения антитеррористической защищенности массовых мероприятий в современных условиях. Его дальнейшее совершенствование должно быть направлено на гибкость категорирования (с учетом оперативной разведывательной информации), адаптацию зонирования под архитектурные особенности объектов и развитие модульных, масштабируемых решений, доступных для широкого круга организаторов.

Особое внимание уделяется эвакуационной безопасности. Согласно современным требованиям, конструктивныепараметрыобъектадолжныобеспечивать вывод зрителей в безопасную зону в течение восьми минут. При этом пути эвакуации для зрителей проектируются независимо от маршрутов служебного персонала, а аварийные выходы оснащаются устройствами экстренного открывания (типа «Антипаника»). В то же время входные группы организуются таким образом, чтобы обеспечить прямой маршрут движения без необходимости изменения направления – это требование необходимо для снижения паники и ускорения массового прохода. Несмотря на кажу-

щееся противоречие, данные принципы совместимы при грамотном архитектурном решении, предусматривающем раздельные, но параллельные потоки.

Требование эвакуации зрителей в течение 8 минут, закрепленное в нормативной практике, базируется на расчетах, предполагающих упорядоченное движение при штатных условиях. Однако следует понимать, что в реальных чрезвычайных ситуациях – особенно при панике, давке или наличии значительного числа маломобильных групп населения (далее – МГН) – этот показатель может быть скорректирован. Для минимизации рисков реализуется комплекс компенсирующих мер: эвакуационные маршруты проектируются с избытком пропускной способности, пути зрителей и служебного персонала разделены, на выходах устанавливаются устройства «антипаника», а для МГН предусматриваются выделенные зоны ожидания и сопровождение сотрудниками. Дополнительно система оповещения обеспечивает дублирование информации через звуковые, речевые и визуальные каналы, что снижает уровень дезориентации и способствует сохранению контроля над толпой даже в условиях высокого стресса.

Таким образом, 8 минут – не абсолютный предел, а целевой ориентир, достижимый за счет системного подхода к эвакуационной устойчивости. Существенной проблемой остается согласование требований к времени досмотра и пропускной способности КПП. Расчет, основанный на нормативе 150 человек/час на один досмотровый проход (соответствующий 24 секундам на одного человека), выявляет необходимость в значительном количестве контрольных точек при пиковой нагрузке (до 70 % вместимости объекта за час до начала мероприятия). В реальных условиях это требует гибкого подхода: применения временных КПП, многоуровневого досмотра, предварительной аккредитации и использования технологий автоматической идентификации (турникеты с распознаванием лиц, QR-коды, биометрия), что позволяет оптимизировать поток без снижения уровня безопасности.

Важно также отметить, что требования к инженерному обустройству периметра различаются в зависимости от статуса объекта. Стационарные сооружения могут оборудоваться ограждениями на фундаменте высотой не менее 2,5 м, в то время как для временных мероприятий допускается применение мобильных ограждений быстрого развертывания, обеспечивающих достаточный уровень противотаранной и противопехотной защиты. Такой подход устраняет противоречие между требованием «непроницаемости» и необходимостью временного характера инфраструктуры.

Аналогично, требования к освещенности КПП приведены в соответствие с функциональной нагрузкой:

75 лк – в операторских и коридорах для персонала (требуется точная работа с оборудованием);

20 лк – в пешеходных проходах (обеспечение базовой видимости);

5 лк – на открытых досмотровых площадках (при условии использования специализированного досмотрового освещения, включаемого по необходимости).

Таким образом, общая освещенность зоны досмотра обеспечивается не только стационарным, но и дополнительным направленным освещением, что устраняет ранее выявленное несоответствие.

Современная модель обеспечения антитеррористической защищенности объектов проведения крупных общественно-политических и спортивно-массовых мероприятий базируется на принципе многоуровневой, интегрированной безопасности, в которой ключевую роль играют ТСО, которые, согласно действующим нормативным актам, предназначены для решения четырех фундаментальных задач:

– обнаружение несанкционированного проникновения на охраняемые территории, здания и зоны;

– выявление противоправных действий в режиме реального времени;

– контроль и управление доступом различных категорий лиц и транспортных средств;

– идентификация и локализация запрещенных предметов и веществ, включая взрывчатые материалы, оружие, радиоактивные и химические угрозы.

Эффективность ТСО напрямую зависит от их системной интеграции: отдельные подсистемы (видеонаблюдение, контроль доступа, тревожная сигнализация) должны функционировать не изолированно, а как единый комплекс, управляемый с централизованного поста (Координационного штаба). Такой подход соответствует международным практикам и позволяет минимизировать временные задержки в принятии решений, повысить точность идентификации и снизить количество ложных срабатываний.

СКУД занимает особое место в архитектуре антитеррористической защищенности объектов, предназначенных для проведения крупных общественно-политических и спортивно-массовых мероприятий. Ее роль выходит далеко за рамки простой фиксации факта прохода: СКУД выступает в качестве «нервной системы» всего комплекса безопасности, обеспечивая динамическое управление перемещением людей и транспорта в условиях строгого многоуровневого зонирования. Именно СКУД формирует первый и наиболее важный барьер на пути несанкционированного проникновения, одновременно обеспечивая бесперебойную логистику для аккредитованных участников.

На основе анализа опыта проведения крупнейших международных событий в Российской Федерации – Олимпийских игр в Сочи (2014), Чемпионата мира по футболу FIFA (2018), Всемирной зимней универсиады в Красноярске (2019) – сформирована трехуровневая структура доступа, ставшая стандартом для всех объектов высокой категории угрозы. Эта модель отражает не только функциональное назна-

чение зон, но и степень риска, связанного с каждой группой пользователей:

Общественная зона – предназначена для зрителей и посетителей, не имеющих специального допуска. Уровень проверки здесь ориентирован на предотвращение проноса запрещенных предметов и выявление лиц, находящихся в розыске.

Служебная зона – включает помещения для персонала, СМИ, организаторов, технических специалистов. Доступ регулируется с учетом зоны ответственности и временных рамок аккредитации.

Режимная зона – наиболее защищенная часть объекта, куда допускаются VIP-персоны, спортсмены, члены официальных делегаций и лица, находящиеся под государственной охраной. Здесь применяются усиленные меры идентификации и сопровождения.

Такая дифференциация соответствует принципу пропорциональности, закрепленному в Постановлениях Правительства РФ № 272[5] и № 202 [6], и позволяет избежать избыточного контроля на входах для зрителей, одновременно обеспечивая максимальную защиту критически важных зон.

Современная СКУД реализуется через три взаимосвязанные, но функционально независимые подсистемы, каждая из которых адаптирована под специфику соответствующей группы пользователей.

1. Подсистема контроля доступа посетителей основана на многофакторной идентификации: сканирование цифрового или бумажного билета (включая 2D/QR-коды с экрана смартфона) в сочетании с биометрической верификацией – распознаванием лица в режиме реального времени. Время верификации не превышает 5 секунд, что позволяет поддерживать пропускную способность на уровне 150 человек в час на один канал, соответствующую требованиям к пиковым потокам (до 70 % вместимости объекта за 1 час до начала мероприятия).

Система автоматически сверяет данные с централизованными базами, включая перечни лиц, ограниченных в доступе по решению суда или по оперативным данным органов безопасности. Это позволяет предотвратить использование поддельных билетов, выявить дубликаты и заблокировать доступ потенциально опасным лицам еще до их попадания в зону безопасности.

Турникеты оснащаются FullHD-камерами (разрешение 2048 1536) с ИК-подсветкой (не менее 40 диодов) и встроенным обогревателем, что обеспечивает надежную идентификацию даже в условиях полной темноты, контрового света или низких температур. Каждый проход фиксируется с привязкой к лицу, билету и времени, формируя цифровой след, который может быть использован в ходе уголовного расследования.

2. Подсистема контроля доступа обслуживающего персонала ориентирована на долгосрочную и гибкую аккредитацию. Персонал – от технических специалистов и сотрудников питания до журналистов и представителей маркетинговых партнеров – проходит верификацию по электронным пропускам с RFID-чипами, содержащими данные о зоне ответственности, времени действия и уровне допуска.

Система динамически управляет доступом: например, сотрудник получает право находиться только в зоне кухни и буфетов, но не может проникнуть в раздевалки спортсменов или зону гостеприимства. Такой подход реализуется через программируемые профили доступа, настраиваемые индивидуально для каждого сотрудника и обновляемые в реальном времени. Это минимизирует риски внутренних угроз и несанкционированного перемещения внутри объекта.

3. Подсистема контроля доступа транспортных средств обеспечивает автоматическую идентификацию автотранспорта по государственным регистрационным знакам (с использованием технологии ANPR – Automatic Number Plate Recognition) и/или дистанционно считываемым RFID-меткам. Ключевая задача – обеспечить беспрепятственный, но контролируемый пропуск категорий транспорта, имеющих право на упрощенный режим: официальные делегации, транспорт организаторов, медицинские и спасательные машины.

Особое значение имеет возможность мгновенного приоритетного проезда для специальных транспортных средств, участвующих в ликвидации чрезвычайных ситуаций (пожарные, скорая помощь, подразделения Росгвардии). Это достигается за счет автоматической сверки номера с базой предварительно аккредитованных ТС и дистанционного открытия шлагбаумов без остановки, что критически важно при реагировании на инциденты.

Все три подсистемы функционируют не изолированно, а в рамках единой информационной платформы, обеспечивающей аппаратную и программную интеграцию с другими компонентами комплекса безопасности:

– с системой видеонаблюдения – для визуального подтверждения личности и фиксации перемещений;

– с охранно-тревожной сигнализацией – для автоматической блокировки всех входов и въездов при срабатывании тревоги;

– с системой оповещения – для координации эвакуации и управления толпой;

– с Координационным штабом – для передачи данных о нарушителях в реальном времени.

Такая интеграция превращает СКУД из пассивного средства контроля в активный элемент превентивной безопасности: при обнаружении угрозы система может автоматически заблокировать проходы, вывести на мониторы изображения с камер, зафиксировать последние перемещения нарушителя и передать информацию в правоохранительные органы.

Важнейшей функцией СКУД является автоматическая разблокировка всех дверей, турникетов и шлагбаумов при пожаре или чрезвычайной ситуации.

Таким образом, СКУД на современных объектах массовых мероприятий представляет собой сложную, интеллектуальную модульную систему, сочетающую в себе функции контроля, управления, анализа и реагирования. Ее архитектура позволяет гибко адаптироваться под формат, масштаб и профиль угрозы каждого конкретного мероприятия – от региональных форумов до чемпионатов мирового уровня.

СКУД обеспечивает не только максимальную защиту от террористических и криминальных угроз, но и оперативную логистику, комфорт участников и эффективность постинцидентного анализа. Именно поэтому она справедливо рассматривается как центральный элемент современной модели антитеррористической защищенности, без которой невозможно обеспечить безопасность тысяч людей в условиях динамично меняющейся среды.

В условиях проведения крупных общественно-политических и спортивно-массовых мероприятий функции видеонаблюдения претерпели качественную трансформацию: от пассивного «наблюдения» система переходит к активному оперативному управлению толпой и прогнозированию инцидентов. Эта эволюция обусловлена ростом сложности угроз, увеличением плотности пребывания зрителей и необходимостью перехода от реактивной к превентивной безопасности.

Современная архитектура видеонаблюдения базируется на двух взаимодополняющих режимах.

Система телевизионного наблюдения (далее – СТН) предназначена для непрерывного визуального мониторинга критически важных зон: трибун, входных групп, периметра, подтрибунных помещений, парковок и КПП. Ее функционирование требует выделенного поста с круглосуточным дежурством операторов, что обеспечивает оперативное выявление аномалий в поведении толпы, подозрительных предметов или несанкционированного проникновения.

Система охранная телевизионная (СОТ) работает в автоматизированном режиме как компонент интегрированной системы безопасности. Видеоизображение выводится на монитор только по сигналу тревоги, поступающему от СОТС и логически связанного с конкретной камерой. Такой подход минимизирует когнитивную нагрузку на оператора и гарантирует фокус внимания исключительно на реальных инцидентах.

Обе системы обеспечивают многоуровневый контроль: от глобального обзора территории до детальной идентификации лиц и государственных регистрационных знаков. Для этого применяются камеры с разрешением FullHD и выше, оптическим увеличением до 30 раз, поворотными устройствами и инфракрасной подсветкой. Особое внимание уделяется устранению «слепых зон» – особенно на трибунах (не более 2°500 посадочных мест на одну камеру), в подтрибунных коридорах и у эвакуационных выходов.

Критически важны условия эксплуатации оборудования. Уличные камеры должны выдерживать температурный диапазон от –40 °С до +50 °С, быть защищены от вандализма и оснащены ИК-подсветкой для ночной съемки. Для предотвращения засветки от солнца или фар транспорта камеры устанавливаются под оптимальным углом и комплектуются датчиками автоматической компенсации контрового света.

Ключевым условием эффективности является глубокая интеграция с другими подсистемами безопасности: СОТС, СКУД и системой охранного освещения (далее – СОО). При срабатывании сигнала тревоги система автоматически:

наводит поворотную камеру на зону инцидента (время реакции – не более 10 секунд);

увеличивает частоту записи до 30 кадров/с;

активирует охранное освещение;

выводит изображение на главный монитор Координационного штаба.

Видеозапись ведется круглосуточно на цифровые видеосерверы с хранением архива не менее 30 суток. Для оптимизации объемов данных допускается событийная запись (по движению или тревоге) при наличии функции «отката» – сохранения нескольких секунд до момента срабатывания. Данное ПО обеспечивает:

разграничение прав доступа (оператор, администратор, инсталлятор);

поиск по времени, дате и идентификатору камеры;

экспорт кадров в качестве юридически значимых доказательств;

синхронизированное аудиопрослушивание.

Наиболее перспективным направлением развития является видеоаналитика на основе искусственного интеллекта. Современные алгоритмы в реальном времени распознают:

агрессивное или деструктивное поведение;

аномальное скопление людей;

брошенные предметы;

нарушение границ охраняемых зон.

Это позволяет перейти от фиксации уже произошедшего к прогнозированию и предотвращению инцидентов, кардинально повышая уровень безопасности.

Таким образом, СОТ и СТН трансформируются из пассивных инструментов наблюдения в интеллектуальную аналитическую платформу, способную не только фиксировать события, но и прогнозировать угрозы, координировать действия служб безопасности и формировать юридически значимую доказательную базу. Их эффективность напрямую определяет способность всего комплекса безопасности поддерживать контроль над ситуацией

в условиях высокой динамики и массового скопления людей.

СОТС представляет собой критически важный компонент интегрированного комплекса ТСО на объектах проведения крупных общественно-политических и спортивно-массовых мероприятий. Ее функциональное назначение выходит далеко за рамки простого обнаружения несанкционированного проникновения: СОТС обеспечивает оперативное информирование служб безопасности, автоматизированную координацию реагирования и сохранение целостности инфраструктуры даже в условиях частичного отказа оборудования или внештатных воздействий. Современная СОТС должна соответствовать строгому комплексу требований, направленных на обеспечение высокой надежности, устойчивости, скрытности и отказоустойчивости. В первую очередь, система обязана автоматически фиксировать несанкционированный доступ на территорию объекта, в охраняемые зоны и критически важные помещения – серверные, кассы, узлы жизнеобеспечения, инженерные коммуникации, внешние ворота, колодцы и шахты диаметром от 250 мм. Сигнал тревоги незамедлительно передается в пункт управления Координационного штаба и дежурные части федеральных органов исполнительной власти, обеспечивая соблюдение норматива: время реагирования не должно превышать двух минут.

Для повышения надежности СОТС дополняется ручными тревожными устройствами (скрытыми кнопками), размещаемыми в зонах повышенного риска: КПП, посты охраны, помещения с ценностями, рабочие кабинеты руководителей. Это критически важно в сценариях, где персонал не может открыто вызвать помощь (например, при захвате заложников), обеспечивая дублирующий канал оповещения.

Особое внимание уделяется отказоустойчивости. СОТС должна сохранять работоспособность при отключении основного источника электропитания за счет резервного питания (аккумуляторные батареи или независимый ввод), выдерживать воздействие агрессивных климатических факторов и автоматически восстанавливать функциональность после их устранения. Система также обязана фиксировать неисправности оборудования и вести архив всех событий не менее 30 суток, что обеспечивает возможность постфактум-анализа и формирует юридически значимую доказательную базу.

Ключевым принципом проектирования является недопустимость несанкционированного отключения или неавторизованного снятия/постановки под охрану. Для этого реализуются механизмы разграничения прав доступа (оператор, администратор, инсталлятор), исключающие бесконтрольные действия. Не менее важно, чтобы система не выдавала ложных тревог при штатных переключениях питания, вибрациях или перепадах температуры. Это достигается за счет многоуровневой логики принятия решений – например, совместного срабатывания датчика движения и видеодетектора.

Центральным элементом эффективности СОТС является ее глубокая интеграция на аппаратном и программном уровнях с СКУД и с СОТ. При срабатывании сигнала тревоги система автоматически:

выводит на монитор изображение с ближайшей камеры;

блокирует двери, ворота и шлюзы в зоне инцидента;

активирует дополнительное охранное освещение;

передает данные в правоохранительные органы.

Такая синергия превращает СОТС из пассивного «датчика тревоги» в активный элемент превентивного реагирования, способный минимизировать временные задержки и сохранить контроль над ситуацией даже в условиях высокой динамики и неопределенности.

Таким образом, СОТС на объектах массовых мероприятий выступает не просто как техническая подсистема, а как «нервный центр» безопасности, обеспечивающий раннее обнаружение угрозы и оперативную защиту жизни и здоровья тысяч участников. Ее эффективность напрямую определяет способность всего комплекса безопасности выполнять свою главную задачу – предотвращение террористических и криминальных актов на самых ранних этапах.

ТСОК представляют собой критически важный элемент первой линии физической защиты объектов проведения массовых мероприятий. Их основная задача – надежное обнаружение и предотвращение проноса (провоза) запрещенных предметов и веществ, включая огнестрельное оружие, взрывчатые материалы, радиоактивные, сильнодействующие и ядовитые вещества, а также контроль за выносом материальных ценностей.

Современный комплекс ТСОК строится по принципу многоуровневой верификации, где каждый тип оборудования компенсирует ограничения другого. Базовую конфигурацию составляют три ключевых компонента:

стационарный многозоновый металлодетектор;

рентгенотелевизионная установка (интроскоп);

стационарный радиационный монитор.

Металлодетекторы обеспечивают вероятность обнаружения типового огнестрельного оружия (например, пистолетов ПМ, ПСМ) не менее 0,98, при этом вероятность ложного срабатывания от бытовых предметов (ключи, часы, фурнитура) не превышает 0,02. Такая селективность достигается за счет многозонной архитектуры и автоматической калибровки. Устройства готовы к работе в течение 10 секунд после включения и функционируют в широком диапазоне температур (от –40 °С до +40 °С), что особенно важно для временных объектов.

Рентгенотелевизионные установки позволяют визуально контролировать содержимое ручной клади и мелких грузов. Минимальные требования включают габариты прохода 440×520×550 мм, грузоподъёмность до 30 кг и способность выявлять стальную проволоку диаметром 0,1 мм (без увеличения) и 0,02 мм (с 8-кратным увеличением). Важно, что мощность дозы на поверхности установки не превышает 1 мкЗв/ч, что соответствует международным стандартам радиационной безопасности.

Радиационный контроль осуществляется с помощью гамма-спектрометрических мониторов, работающих в двух режимах:

пороговом (сигнализация при превышении 0,5 мкЗв/ч),

спектрометрическом (идентификация изотопного состава).

Диапазон регистрируемых энергий – от 60 кэВ до 3 МэВ, что охватывает основные источники радиационной угрозы.

Для повышения точности локализации металлических предметов система дополняется ручными металлодетекторами. Для противодействия радиоуправляемым взрывным устройствам применяются передатчики помех, генерирующие широкополосный шумовой сигнал в ключевых частотных диапазонах, тем самым блокируя каналы управления. В зонах КПП и служебных помещений размещаются средства локализации взрыва – специальные контейнеры и щиты, подавляющие фугасное, осколочное и термическое воздействие при детонации.

Важно подчеркнуть, что полный перечень ТСОК применяется только на объектах высокой категории угрозы (Олимпийские игры, Чемпионаты мира). На региональных и муниципальных мероприятиях используется дифференцированный подход: базовый набор включает рамочные и ручные металлодетекторы, интроскопы и радиационные мониторы. Применение всех средств одновременно не предполагается. Вместо этого реализуется многоступенчатый досмотр:

предварительная фильтрация в зонах накопления;

целенаправленная проверка по сигналу от СКУД или видеонаблюдения;

углубленный контроль в специальной зоне отстоя.

Подобная стратификация позволяет избежать «узких мест» при пиковых потоках, предотвратить взаимные помехи между приборами и обеспечить пропорциональность затрат уровню реальной угрозы. Дополнительно используются мобильные досмотровые комплексы и модульная компоновка, позволяющая оперативно наращивать пропускную способность.

Таким образом, ТСОК функционируют не как набор изолированных приборов, а как интегрированный досмотровый комплекс, обеспечивающий высокую достоверность обнаружения, гибкость развертывания и готовность к экстренной нейтрализации угроз. Эффективное применение ТСОК – залог предотвращения террористических и криминальных актов до проникновения угрозы в зону безопасности.

В условиях проведения крупных общественно-политических и спортивно-массовых мероприятий система оповещения (СО) и система охранного освещения (СОО) выполняют синергетические функции, направленные на обеспечение как оперативного управления поведением толпы, так и эффективного визуального контроля в любое время суток. Их интеграция в единый комплекс безопасности является обязательным условием антитеррористической защищенности.

Система оповещения решает одну из самых критически важных задач – оперативное информирование тысяч людей о возникновении или угрозе чрезвычайной ситуации (пожара, техногенной аварии, террористического акта) и координация их действий. Даже незначительная задержка в передаче информации в условиях высокой плотности пребывания зрителей может спровоцировать панику, давку и тяжелые последствия.

Современная СО реализуется как двухканальная система:

звуковая и световая сигнализация (сирены, речевые сообщения, светодиодные табло) – для немедленного привлечения внимания;

речевая трансляция – для передачи точной информации о характере угрозы, необходимых действиях и маршрутах эвакуации.

Особое внимание уделяется инклюзивности: для лиц с нарушениями слуха или зрения предусматриваются тактильные и световые индикаторы, что соответствует принципам универсального дизайна. Сообщения дублируются во всех зонах пребывания людей – на трибунах, в подтрибунных помещениях, санузлах, торговых точках и на парковках. В шумных зонах (буфеты, фойе) применяется повышенная громкость и визуальное сопровождение.

Эффективность СО обеспечивается заранее разработанным планом оповещения, включающим: схему вызова ответственных сотрудников, регламентированные инструкции по действиям в ЧС, актуальные планы эвакуации и стандартизированную систему сигналов. Критически важно, что СО интегрирована с другими подсистемами: при срабатывании охранно-пожарной сигнализации автоматически активируется сценарий оповещения, разблокируются эвакуационные выходы, включается охранное освещение, а в Координационном штабе отображается схема угрозы. Время от регистрации инцидента до начала трансляции не должно превышать 10–15 секунд.

Система охранного освещения, в свою очередь, обеспечивает нормативно регламентированную видимость на критически важных участках: лестничных клетках, тамбурах, постах охраны и вдоль всего внешнего периметра. Минимальная освещенность со-

ставляет 0,5 лк – как горизонтальная (на уровне земли), так и вертикальная (на поверхности ограждения), что достаточно для работы и человеческого зрения, и камер ночного видения.

СОО функционирует в двух режимах:

основное освещение работает непрерывно в ночное время, формируя сплошную световую полосу шириной 3–4 м вдоль периметра и исключая «слепые зоны»;

дополнительное (сигнальное) освещение активируется автоматически по сигналу СОТС при попытке проникновения, усиливая визуальный контроль и оказывая психологическое сдерживающее воздействие на нарушителя.

Все светильники устанавливаются не выше уровня ограждения, защищены от вандализма и механических повреждений. Система поддерживает и ручное управление из помещения службы безопасности, что обеспечивает гибкость реагирования, в том числе днем при плохой видимости (туман, дым).

Обе системы – СО и СОО – глубоко интегрированы: при тревоге автоматически синхронизируется включение освещения, поворот камер и запуск речевых сообщений. Это создает единое информационно-визуальное поле, необходимое для организованной эвакуации и оперативного реагирования.

Таким образом, СО и СОО выступают не как вспомогательные элементы, а как многофункциональные инструменты, сочетающие задачи информирования, сдерживания, обнаружения и эвакуационной поддержки. Их грамотное проектирование и синхронная работа формируют отказоустойчивую среду, способную обеспечить безопасность тысяч людей в условиях динамично меняющейся обстановки.

КПП представляют собой первую линию физической защиты периметра объекта проведения крупного общественно-политического или спортивно-массового мероприятия. Их проектирование осуществляется с учетом интенсивности и состава потоков, а также требований к антитеррористической защищенности, что предполагает четкое разграничение на транспортные и пешеходные КПП.

Транспортные КПП проектируются, исходя из расчетной пропускной способности, определяемой временем досмотра: 2 минуты для легкового автомобиля, 5 минут – для микроавтобуса, 8 минут – для автобуса или грузового транспорта. Структура КПП включает в себя:

досмотровые площадки, количество которых рассчитывается по пиковому потоку;

контрольно-пропускные кабины для верификации водителей и сопровождающих лиц;

противотаранные устройства (подъемные барьеры, блокираторы колес, шлагбаумы);

систему видеонаблюдения с двойным выводом сигнала – на автоматизированное рабочее место (АРМ) Координационного штаба и локальный пост КПП;

технические средства организации дорожного движения, включая дорожный знак 3.17.3 «Контроль», исключающий проезд без остановки.

Досмотровая площадка комплектуется стандартизированным набором оборудования, обеспечивающим многоуровневую верификацию:

«шлюз» из основных и вспомогательных ворот (или шлагбаумов) для изоляции транспортного средства;

сканер днища и комплект досмотровых зеркал;

стационарный радиационный монитор, портативный дозиметр, детектор паров взрывчатых веществ (далее – ВВ) и экспресс-тесты для химического контроля;

детектор опасных жидкостей и обнаружитель акустических/ электромагнитных полей (для выявления радиоуправляемых взрывных устройств);

ручной металлодетектор, сканер скрытых полостей и локализатор взрывных устройств;

системы двусторонней связи и видеозаписи.

Хотя состав оборудования может показаться избыточным, он оправдан необходимостью перекрытия уязвимостей: каждое средство компенсирует ограничения другого, обеспечивая обнаружение как традиционных (оружие, ВВ), так и нетрадиционных угроз (радиологических, химических, электронных). Для повышения отказоустойчивости рекомендуется модульная компоновка – при выходе из строя одного прибора функционирование системы сохраняется за счет резервных средств (например, портативных детекторов).

Пешеходные КПП проектируются с учетом пиковых потоков, достигающих 70 % вместимости объекта за один час до начала мероприятия. На каждый досмотровый проход устанавливаются:

рамочный металлодетектор с вероятностью обнаружения пистолета не менее 0,98 и уровнем ложных срабатываний не более 0,02;

два ручных металлодетектора для локализации металлических предметов;

интроскоп (один на 2–4 прохода);

детекторы паров ВВ, опасных жидкостей и локализаторы взрывных устройств (по одному на КПП);

система видеонаблюдения с дублированием сигнала на АРМ Координационного штаба и локальный пост.

Центральным элементом пешеходного контроля является интегрированная СКУД, обеспечивающая:

контролируемый доступ в зависимости от категории аккредитации;

четкое разграничение зон (зрительской, служебной, режимной);

мониторинг перемещения лиц внутри объекта;

автоматическую разблокировку дверей и турникетов при пожаре;

интеграцию с федеральными и ведомственными

базами данных, включая перечни лиц, ограниченных в доступе по решению суда.

Таким образом, как транспортные, так и пешеходные КПП функционируют не как изолированные узлы, а как компоненты единой многоуровневой системы физической защиты, сочетающей автоматизированный досмотр, интеллектуальный контроль доступа и оперативное реагирование на угрозы.

Система электроснабжения ТСО является невидимым, но критически важным элементом общей архитектуры антитеррористической защищенности объектов проведения массовых мероприятий. Ее отказоустойчивость напрямую определяет способность всего комплекса безопасности сохранять контроль над ситуацией в условиях чрезвычайных обстоятельств – включая аварии, стихийные бедствия и, что особенно важно, целенаправленные диверсионные действия.

Отнесение ТСО к электроприемникам первой категории по надежности (в соответствии с Правилами устройства электроустановок) не является формальным требованием, а имеет глубокое функциональное обоснование. Современные ТСО – это не пассивные регистрирующие устройства, а активные компоненты превентивной безопасности: системы видеонаблюдения с ИИ-аналитикой распознают аномальное поведение до совершения преступления, СКУД блокирует доступ нарушителя в реальном времени, а СОТС инициирует каскадное реагирование – от включения охранного освещения до вызова группы задержания.

Даже кратковременный сбой питания одного элемента – например, камеры у входной группы или металлодетектора на КПП – создает «слепую зону», которой может воспользоваться злоумышленник. Таким образом, бесперебойное электроснабжение выступает не как техническая деталь, а как условие целостности всего защитного контура.

Для обеспечения этой целостности применяется дублирующая схема питания: либо от двух независимых источников переменного тока, либо от одного основного ввода с автоматическим резервированием от аккумуляторных батарей или источников бесперебойного питания. Такой подход гарантирует непрерывность функционирования систем даже при аварийном отключении внешней сети или саботаже энергоинфраструктуры. Дополнительно физическая защита кабельных линий (прокладка в бронированных каналах, стальных трубах, подземных коллекторах) препятствует попыткам вывода систем из строя путем механического повреждения линий питания.

Только при условии гарантированного энергоснабжения технические средства охраны способны выполнять свою основную задачу – надежное предотвращение угроз и обеспечение безопасности тысяч участников и зрителей крупных общественно значимых мероприятий. Особое внимание в рамках обеспечения антитеррористической защищенности объектов уделяется защите кабельных линий ТСО от несанкционированного доступа и умышленного повреждения, поскольку их целостность напрямую влияет на отказоустойчивость всей системы безопасности. Линии, прокладываемые через помещения, не охраняемые системой сигнализации, должны выполняться скрытым способом – в строительных конструкциях (стенах, перекрытиях) – либо механически защищаться посредством прокладки в стальных трубах, металлических коробах или бронированных металлорукавах. Такие меры исключают возможность быстрого перехвата, перерезания или демонтажа кабелей потенциальным нарушителем.

В пределах зоны безопасности допускается несколько вариантов прокладки, обеспечивающих как надежность, так и технологичность монтажа:

подземный способ – в траншеях или подземных коллекторах, обеспечивая максимальную защиту от внешних воздействий;

открытая прокладка по внутренней стороне периметрального ограждения или стены здания с использованием бронированных кабелей;

в обоснованных случаях – применение небронированных кабелей, проложенных в стальных трубах или металлических коробах;

подвеска на несущем тросе на высоте не менее 3-х м, при этом участки, расположенные ниже 2,5 м, обязательно защищаются металлическим кожухом, сетчатым ограждением или иными средствами, предотвращающими механические повреждения.

Такой дифференцированный подход к прокладке и защите кабельных линий обеспечивает не только физическую устойчивость инфраструктуры ТСО, но и ее соответствие требованиям нормативных документов по инженерной защите объектов с массовым пребыванием людей.

Проведенный анализ системы обеспечения антитеррористической защищенности объектов проведения крупных общественно-политических и спортивно-массовых мероприятий позволяет сформулировать следующие ключевые выводы.

Во-первых, эффективность безопасности на современных объектах достигается не за счет изолированных технических решений, а за счет глубокой интеграции нормативно-правовых, инженерных, организационных и технических компонентов в единый многоуровневый, адаптивный комплекс. Центральную роль в этой архитектуре играет принцип дифференциации: категорирование объектов по уровню угрозы, зонирование территорий, разграничение потоков посетителей и персонала, а также гибкая настройка технических средств в зависимости от категории мероприятия.

Во-вторых, контрольно-пропускной режим выступает первой линией обороны. Его рациональная организация – с учетом пиковых потоков, времени досмотра и пропускной способности – позволяет

не только предотвратить проникновение угроз, но и избежать формирования «бутылочных горлышек», провоцирующих панику. Применение биометрической верификации, распознавания госномеров и антидубликационного контроля билетов повышает не только безопасность, но и цифровую прослеживаемость каждого участника события.

В-третьих, ТСО функционируют наиболее эффективно в режиме автоматизированного взаимодействия. Интеграция СКУД, СОТС, систем видеонаблюдения и охранного освещения обеспечивает переход от пассивного наблюдения к оперативному реагированию: при срабатывании сигнализации автоматически активируются камеры, включается дополнительное освещение, блокируются проходы и передается тревога в Координационный штаб. Это сокращает время реакции до минимально возможного, что критично в условиях высокой динамики.

В-четвертых, надежность инфраструктуры является фундаментом всей системы. Отнесение ТСО к электроприемникам первой категории, дублирование источников питания, защита кабельных линий и применение оборудования, устойчивого к климатическим и механическим воздействиям, гарантируют отказоустойчивость даже при целенаправленных диверсиях или авариях.

В-пятых, человеческий фактор не устраняется, а минимизируется за счет автоматизации и четких регламентов. Система оповещения, основанная на двухканальной передаче информации (звук+речь+визуальные сигналы), позволяет управлять поведением толпы, предотвращая панику и обеспечивая организованную эвакуацию в течение регламентированных восьми минут.

Таким образом, современная модель безопасности объектов массовых мероприятий представляет собой сложную, самоадаптирующуюся систему, сочетающую превентивную защиту, оперативное реагирование и постинцидентный анализ. Ее успех определяется не столько количеством установленных приборов, сколько качеством их интеграции, научной обоснованностью требований и гибкостью в применении.

Дальнейшее совершенствование практик обеспечения антитеррористической защищенности должно быть направлено на:

развитие интеллектуальных систем на основе ИИ (видеоаналитика, прогнозирование аномального поведения);

унификацию нормативных требований с устранением внутренних противоречий;

обеспечение послемероприятийной рентабельности инфраструктуры (модульность, мобильность, повторное использование).

Только такой комплексный и научно обоснованный подход позволит обеспечить максимальную безопасность при сохранении функциональности, комфорта и устойчивости крупных общественных событий в современных условиях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Градостроительный кодекс Российской Федерации: Федеральный закон от 29 декабря 2004 г. № 190-ФЗ // Собр. законодательства Рос. Федерации. – 2005. – № 1 (ч. I). – Ст. 16.

2. Федеральный закон от 06 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // Собр. законодательства Рос. Федерации. – 2006. – № 11. – Ст. 1146.

3. Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» // Собр. законодательства Рос. Федерации. – 2011. – № 30 (ч. I). – Ст. 4604.

4. Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений» // Собр. законодательства Рос. Федерации. – 2009.

5. Постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)» // Собр. законодательства Рос. Федерации. – 2015. – № 14. – Ст. 2119.

6. Постановление Правительства Российской Федерации от 6 марта 2015 г. № 202 «Об утверждении требований к антитеррористической защищенности объектов спорта и формы паспорта безопасности объектов спорта» // Собр. законодательства Рос. Федерации. – 2015. – № 11. – Ст. 1608.

7. Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» [Текст]. – М.: НИЦ «Охрана», 2022. – 97 с. – URL: http://nicohrana.ru/engine/download.php?id=1456&area=static.

Статья проверена программой Антиплагиат. Оригинальность — 96 %.

Статья поступила в редакцию 29.12.2025; одобрена после рецензирования 16.01.2026; принята к публикации 25.02.2026.