

Министерство Российской Федерации по делам
гражданской обороны, чрезвычайным ситуациям
и ликвидации последствий стихийных бедствий

Министерство внутренних дел Российской Федерации

СБОРНИК ТРУДОВ



7-й МЕЖДУНАРОДНОЙ
СПЕЦИАЛИЗИРОВАННОЙ ВЫСТАВКИ
«ПОЖАРНАЯ БЕЗОПАСНОСТЬ XXI ВЕКА»



6-й МЕЖДУНАРОДНОЙ
СПЕЦИАЛИЗИРОВАННОЙ ВЫСТАВКИ
«ОХРАННАЯ И ПОЖАРНАЯ АВТОМАТИКА»
(Комплексные системы безопасности)

Москва
Эксподизайн-ПожКнига
2008

- С55** **Сборник трудов** 7-й международной специализированной выставки “Пожарная безопасность XXI века” и 6-й международной специализированной выставки “Охранная и пожарная автоматика” (Комплексные системы безопасности). — М.: Эксподизайн, ПожКнига, 2008. — 296 с., ил.

В Сборник трудов включены материалы участников 7-й международной специализированной выставки “Пожарная безопасность XXI века” и 6-й международной специализированной выставки “Охранная и пожарная автоматика” (Комплексные системы безопасности).

Сборник предназначен для инженерно-технических работников, занятых вопросами обеспечения безопасности от чрезвычайных ситуаций, преподавателей и слушателей учебных заведений системы МЧС России и МВД России, других министерств и ведомств, работников научных и проектных организаций.

Редакционный совет:

Председатель

Заслуженный юрист Российской Федерации, д.ю.н., профессор **Гуров А.И.**

Члены совета:

академик ВАН КБ **Аксютин В.П.**, академик ВАН КБ **Верзилин М.М.**,
академик ВАН КБ **Баранник Ю.А.**, к.э.н. **Будзинский Н.В.**,
академик ВАН КБ **Гордейчук А.П.**, член-корреспондент ВАН КБ **Зайцев А.Г.**,
д.т.н., профессор **Копылов В.П.**, д.т.н., профессор **Корольченко А.Я.**,
д.т.н., профессор **Любимов М.М.**, академик ВАН КБ **Микляев В.С.**,
к.т.н., с.т.н. **Пивоваров В.В.**, к.т.н., профессор **Собурь С.В.**,
к.т.н. **Стельмашенко В.Г.**, д.т.н. **Тагиев Р.М.**, к.с.н. **Тетерин И.М.**,
к.т.н. **Тодосейчук С.П.**, академик ВАН КБ **Черток В.Б.**



Интегрированные системы безопасности: современные решения и тенденции

Крахмалёв А., к.т.н., проф, акад. ВАНКБ, нач. отдела ФГУ НИЦ “Охрана” МВД России

Обеспечение безопасности объектов особой важности, повышенной опасности и жизнеобеспечения (критически важных объектов — КВО) на фоне роста террористических угроз является сегодня весьма актуальной проблемой. Захват, вывод из строя или нарушение функционирования таких объектов и перевозимых специальных грузов чреваты крайне негативными последствиями и могут нанести крупный или невосполнимый ущерб государству и обществу.

К таким объектам могут относиться:

- объекты высших органов власти, правительственные учреждения, крупные объекты кредитно-финансовой сферы;
- объекты особо важного административного, общественного и промышленного значения с высокими требованиями к системам жизнеобеспечения и безопасности,
- объекты топливно-энергетического комплекса, ядерно-опасные, радиационно-, химически- и биологически опасные объекты, электростанции, в том числе атомные, гидротехнические сооружения, тоннели, мосты, газо-нефтепроводы, склады горюче-смазочных материалов и т. п.;
- объекты микробиологической и фармацевтической промышленности, объекты по переработке и хранению наркотических веществ, сильнодействующих ядов и химикатов, психотропных веществ и препаратов;
- объекты, являющиеся архитектурными памятниками, музеи, здания для хранения архивов, художественных и других подобного рода культурных и материальных ценностей, объекты культа.
- объекты (территории) жизнеобеспечения;
- метрополитен, подземные сооружения особо важного значения;
- жилые многоэтажные дома;
- объекты массового пребывания людей: школы и больницы, кино-театры, стадионы, вокзалы, аэропорты и т.д.;
- специальные грузы, перевозимые автомобильным, железнодорожным транспортом, судами речного и морского флота.

Обеспечение безопасности подобных объектов требует комплекса мер направленных на предупреждение, пресечение и устранение угрозы или опасной ситуации. Комплекс мер должен основываться на принципах системного подхода к деятельности по обеспечению безопасности, как на этапах организации, подготовки, проектирования, так и в процессе эксплуатации и включать в себя совокупность организационных и технических мероприятий — систему комплексной безопасности.

Не умаляя значения организационно-правовых и профилактических методов борьбы с терроризмом, следует отметить, что их практическая

реализация невозможна без современных технических средств. Номенклатура таких средств достаточно широка и позволяет при грамотном проведении единой технической политики, умелом сочетании и применении технических средств обеспечить надежную защиту любого объекта, обнаружить и нейтрализовать террористические угрозы практически в любых условиях и при любых сценариях их развития. Поэтому во всем мире наблюдается устойчивая тенденция к расширению сферы задач безопасности, возлагаемых на технические средства.

На основании изучения перспектив развития как отечественных, так и зарубежных средств безопасности позволяет утверждать, что для обеспечения безопасности КВО наилучшим образом подходят интегрированные системы безопасности (ИСБ), которые представляют собой объединение на единой программно-аппаратной основе систем охранно-пожарной сигнализации, видеонаблюдения и контроля доступа. ИСБ предназначены для решения вопросов обеспечения безопасности крупных и средних объектов, объектов особой важности и повышенной опасности, объектов кредитно-финансовой сферы и позволяют решать на новом качественном уровне задачи по обеспечению безопасности объектов.

НИЦ “Охрана” совместно с ведущими отечественными предприятиями, работающими в этом направлении, были разработаны и внедрены в серийное производство интегрированные системы: “Рубеж”, “Аккорд-512”, “Орион”, “Кодос-А20”.

Эти современные ИСБ обеспечивают:

- модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты;
- контроль и управление доступом через точки входа (двери, турникеты, шлюзы, шлагбаумы);
- видеонаблюдение, видеоконтроль и видеорегистрацию тревожных ситуаций;
- управление установками пожарной автоматики;
- управление инженерными системами здания (кондиционирования, отопления, вентиляции, оповещения, аварийной сигнализации);
- защищенный протокол обмена по каналам связи, имитостойкие шлейфы сигнализации;
- возможность использования для взятия под охрану/снятия с охраны дистанционных радиокарт и электронных ключей;
- речевое предупреждение дежурного о тревожных событиях, возможность записи и воспроизведения речевых сообщений;
- отображение состояний зон, разделов, точек доступа, приемно-контрольных приборов, считывающих устройств, видеокамер на графических планах помещений с подробными текстовыми пояснениями;
- разграничение полномочий дежурных, операторов, администраторов за счет многоуровневой системы паролей и возможность подключения биометрических систем ограничения доступа к программам АРМ;
- протоколирование всех событий, происходящих в системе;

- развитую диагностику работоспособности всех блоков и устройств системы;

- удаленную передачу данных и защиту информации по различным каналам (выделенным проводным, телефонным через модемы, оптоволоконным, радиоканалам, каналам сотовой связи, цифровым сетям ISDN).

Кроме этого, ИСБ позволяют оптимальным образом сократить людские и материальные ресурсы, а также финансовые затраты (в т. ч. бюджетные) на оборудование объектов, эксплуатацию аппаратуры и содержание охранников.

Неотъемлемой частью ИСБ, в особенности, применительно к решению задачи защиты ОВВ должны служить СКУД и СОТ. Эти системы активно развиваются и в них появляются новые технологии.

В области СКУД — идентификация радиочастотная — дистанционная, биометрическая, идентификация транспорта. Сопряжение СКУД с ИСБ дает новые качества для обеспечения безопасности. Применение в СКУД новых преграждающих устройств повышенной степени защиты (полноростовые турникеты, шлюзы и т.д.).

СОТ — цифровые технологии и интеграция в ИСБ позволяет значительно повысить эффективность телевизионных систем наблюдения. Современные технологии в системах видеонаблюдения, которые особо важны для решения задачи борьбы с терроризмом и которые в настоящее время активно развиваются и внедряются, как за рубежом, так и в России. Это “интеллектуальные” детекторы движения, обнаружители пропаж/закладок, анализаторы баз видеоданных и т.д.

В целом перспективы развития СОТ следующие:

1. Применение цифровых технологий;
2. СОТ на базе цифровых видеорегистраторов (без компьютера);
3. СОТ на базе компьютера - видеосервера (в локальной сети верхнего

уровня ИСБ);

4. СОТ на базе сетевых видеокамер (IP-видеокамеры);

5. Автоматизация СОТ:

“интеллектуальные” видеодетекторы движения;

обнаружители пропаж/закладок предметов;

автоматическое слежение за объектом;

автоматическое распознавание объекта (человека по лицу, автомобилей, номерных знаков и др.)

автоматические анализаторы баз данных.

Особое значение в охране КВО объектов имеют средства охраны периметра. Периметр играет роль первого рубежа обороны объекта и должен быть оборудован соответствующим образом. Интеграция периметровых средств сигнализации в ИСБ также позволяет оптимально обеспечить защиту объекта, учитывая что на периметре должны быть сосредоточены инженерно-технические средства защиты, средства обнаружения, средства контроля доступа (КПП), средства телевизионного наблюдения.

На основании анализа развития ИСБ на современном этапе можно отметить следующие тенденции:

1 - стремительный прогресс развития СОР в системах безопасности требует значительного увеличения пропускной способности каналов передачи данных. Это дает возможность передавать по этим каналам и другую информацию в системах безопасности (объемы этой информации значительно меньше, чем СОР). Поэтому СОР становится в основе ИСБ. Поэтому в качестве каналов связи IP-сети.

2 - расширение возможностей ИСБ в удаленной передаче данных — создание на основе ИСБ мониторинговых систем безопасности территориально распределенных объектов (ИСБ+СПИ). В соответствии с этим — использование для удаленной передачи данных современных цифровых каналов (с учетом передачи видео) — ВОЛС, Интернет, GSM/GPRS, спутниковые каналы, проводные каналы ГТС в режимах использования технологий xDSL. С учетом использования нескольких каналов для обеспечения надежности и резервирования, а также с необходимой защитой информации.

3 - тенденция “разинтеграции” — предоставление заказчику возможности построения на основе, входящих в состав ИСБ компонентов, создания отдельных подсистем - СКУД, СОР, СПС, СОС, АСПТ и др. с характеристиками не хуже, чем у специальных аналогичных по назначению систем.

4 - использование беспроводных каналов передачи данных на нижних сетевых уровнях (беспроводные извещатели и др.).