

Комплексная безопасность: события, факты, комментарии

Пожарная безопасность

- С 20.06.2011 г. в России введены в действие изменения № 1 к своду правил СП5.13130.2009 «Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования».

Основные изменения внесены в п. 14.4 свода правил в части обязательной автоматической передачи сигнала «Пожар» в рамках СПИ (выделенный радиоканал или другие каналы) в подразделения пожарной охраны для объектов класса функциональной опасности Ф 1.1 и Ф 1.4. При этом должны обеспечиваться мероприятия по повышению достоверности извещения о пожаре, например передача извещений «Внимание», «Пожар» и др.

Комментарий: Применяемая в Беларуси система передачи извещений о ЧС «Молния» (ТУ ВУ 101114857.059-2007) осуществляет передачу извещений («Неисправность», «Пожар») по радиоканалу и проводным каналам электросвязи на ПЦН. УОО СПИ «МОЛНИЯ» обеспечивает передачу дежурных и информационных сообщений о своем состоянии по радиоканалу не реже одного раза за 5 минут или по запросу.

Следует отметить, что в России и Беларуси в настоящее время структурное построение СПИ (ПЦН) в связке с каналами связи / сопряжения фактически функционально не регламентировано по классам (категориям) охраняемых объектов. Алгоритм передачи сигнала, его помехозащищенность, защита пересылаемой информации (как правило, отсутствует вообще) одинаковы для всех категорий объектов, включая критически важные.

В США нормами NFPA 72 предусмотрено **7 типов СПИ**. Системы типа 1-3 — активные мультиплексные системы передачи (п. 3.3.2), при этом для систем 1-го типа предусматривается обратное дистанционное управление. Системы 4-5 типов — это мультиплексные двунаправленные радиосистемы, системы 6-7 типов — однонаправленные частотные радиосистемы тревоги. Факти-



Справка ТБ

Маликов Владимир Викторович. В 2000 г. закончил БГУИР, по специальности «Проектирование и технология ЭВС». В 2006 г. БГУИР (магистратура), специальность — «Техническое обеспечение безопасности». В 2010 г., закончил БГУИР (аспирантура), специальность — «Методы и системы защиты информации, информационная безопасность», ученая степень — «кандидат технических наук». Майор милиции, УО «Учебный центр Департамента охраны» МВД Республики Беларусь, начальник цикла технических и специальных дисциплин. Опыт работы в подразделениях средств и систем охраны Департамента охраны МВД Республики Беларусь с 2000 г.

чески СПИ (ПЦН) эксплуатируемые в России и Беларуси можно отнести к 4-7 типам по NFPA 72.

Учитывая то, что например термин «устойчивость при работе в условиях пожара» (BS 5839-1:2002 «Разработка, монтаж, ввод в эксплуатацию технического обслуживание систем пожарной сигнализации») в Европе введен в 2002, а «предел пожаростойкости кабелей (проводов)» (ТКП 45-2.02-190-2010 «Пожарная автоматика зданий и сооружений. Строительные нормы проектирования») в Беларуси в 2011 г. (с 01.01.2011 г.), можно предполагать, что около 10 лет нормативного и технологического отставания по отрасли пожарной и комплексной безопасности нам гарантировано.

Новая редакция BS 5839-1:2002 ужесточает критерии определения устойчивости функционирования автоматических пожарных детекторов (п. 32.2):

1. В системах, которые включают в себя более чем 40 автоматических пожарных детекторов, пользова-

тель должен инициировать всестороннее расследование соответствующими специалистами, если в течение года:

- величина ложной тревоги в среднем превысила одну ложную тревогу на 20 детекторов;
- три и более ложные тревоги возникали от какого-то одного ручного извещателя или пожарного детектора.

2. В системах, которые включают в себя 40 или менее автоматических пожарных детекторов, всестороннее расследование должно быть инициировано пользователем, если в течение года возникали три и более ложные тревоги.

Системы охранного телевидения / системы видеонаблюдения

- Активнабирает обороты рынок VSaaS (Video Surveillance as a Service / видео как сервис). Рост объема таких решений в 2011 г будет превышать 20% (IMSResearch).

Комментарий: Данная тенденция подтверждает общее движение всех сегментов отрасли безопасности (информационной и инженерно-технической) под общим трендом IT-технологий. Появление, развитие технологий и сервисов способствует доступности обеспечения услуг безопасности сегмента SOHO (Small Office / Home Office — малый/домашний офис) типовым потребителем, как правило, на уровне мониторинга, самостоятельно с приемлемым уровнем риска. Реагирование на инциденты безопасности и обеспечение защиты конфиденциальной информации (при ее наличии) в данном случае, естественно, являются уязвимыми звеньями системы защиты.

- 12 сентября 2011 г. HDcctvAlliance представила спецификацию новой версии стандарта V 2.0 HDcctv (V 1.0 HDcctv — 2009 г.). По заявлению разработчиков данная версия стандарта будет ратифицирована к концу 2011 г. Основные нововведения: передача HD-видеосигнала (формат XR) по кабелю RG-59 на расстояние более 300 м, по кабелю UTP — более чем

на 100 м, по устаревшему коаксиальному кабелю — на 40 м. Компания EverFocus одним из первых производителей приступила к выпуску оборудования под стандарт V 2.0 HDcctv.

- Агентство IMSResearch прогнозирует, что глобальный рынок сетевого видеонаблюдения обгонит рынок аналогового видео в 2014 г.

- Более 10 % продаваемых компаний Bosch Security Systems камер и кодеров оснащены встроенной видеоаналитикой для охраны периметра. При этом продажи видеоаналитики других типов (оставленных предметов и др.) остаются незначительными.

- Лаборатория i-LIDS (Imagery library for intelligent detection systems) в Департаменте научных разработок МВД Великобритании занимается тестированием технических средств обнаружения и сертифицирует оборудование для государственных проектов. Сертификат i-LIDS является общепризнанным стандартом качества видеоаналитики в отрасли. Лаборатория i-LIDS уже разработала методику и наборы данных для тестирования видеоаналитики видимого спектра по сценариям: стерильная зона, оставленные предметы, парковка транспортных средств, мониторинг дверей и проходов, многокамерное слежение в общественных местах.

Для каждого сценария были сделаны по три объемных комплекта тестовых видеоданных. Длина каждого тестового архива составляет около 24 часов, и в нем собрано видео при всех возможных условиях погоды и освещения. Комплект видеоданных для сценария с использованием нескольких камер насчитывает в сумме более 50 часов реального эксплуатационного видео. Технически каждый тестовый комплект данных состоит из двух или трех сцен, которые разбиты на ролики длиной от 30 до 60 минут. Для всех сценариев определены критерии оценки выделяемых событий: например, автомобиль должен присутствовать в указанной зоне на парковке в течение не менее чем 60 секунд. По результатам тестирования аналитический продукт может быть отнесен к одной из пяти категорий. Самая низшая категория не подтверждает наличия у продукта аналитических функций, а самая высшая предполагает способность системы работать в автономном режиме, используя видеоаналитику

Таблица			
Задача СВН	Отображение человеческого тела, %	Приблизительное линейное разрешение, пкс/м	Ширина лица, пкс
Идентификация	120	250	40
Различение	50	100	17
Обнаружение	10	20	3

как основное, а не вспомогательное средство детектирования.

Сертификация и категоризация производятся для каждого из пяти сценариев отдельно: продукт, например, может обладать сертификатом по детектированию автомобилей на парковке, но не соответствовать требованиям по ложным срабатываниям в «стерильной зоне». На логотипе указывается только тот тип теста, который продукт успешно прошел.

- Размер минимальной детали объекта контроля в зависимости от целевой задачи видеонаблюдения, рассчитанной для объекта «человек» специалистами компании AxisCommunications (с переводом ТВЛ в пиксели) приведен в таблице.

Антитеррористическая защита

- С 20.09.2011 г. в России вступил в силу свод правил СП 132.13330.2011 г. «Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования», который устанавливает минимально необходимые требования к проектным решениям, позволяющим обеспечить антитеррористическую защищенность объектов.

Комментарий: Основную информативную и функциональную нагрузку свода правил несут таблицы 1 и 2. Следует отметить, что документ не содержит ключевого термина «критически важный объект», хотя как минимум объекты класса 1 (ущерб федерального и межрегионального масштаба) уже относятся к критически важным. Предложенная классификация объектов и требования свода правил фактически представляют собой урезанный вариант проекта федерального закона «Технический регламент «О технических средствах обеспечения противокриминальной защиты объектов и имущества», разработанный ФГУ НИЦ «Охрана» МВД России еще в 2009 г.

- На всех крупных вокзалах России устанавливаются стационарные металлодетекторы (уже установленные

но 126 рамок). За 4 месяца 2011 г. ОВДТ России было зарегистрировано 22,6 тыс. преступлений (в т.ч. 2 террористических акта). Выявлено 4,5 тыс. преступлений связанных с незаконным оборотом наркотиков, 1,1 тыс. — с незаконным оборотом оружия. В течение 3-х лет (2011-2013 гг.) на оснащение ОВДТ России выделено RUB1,8 млрд., совершенствование кинологической службы ОВДТ — RUB 22,7 млн.

Комментарий: Как правило, применяются многозонные стационарные металлодетекторы предназначенные для обнаружения запрещенных металлических предметов проносимых в одежде или на теле человека. Несколько зон обнаружения и боковые панели индикации информируют не только о превышении тревожного порога, но и указывают на зоны, в которых находится запрещенное количество металла.

В Беларуси на критически важных объектах транспортной инфраструктуры (вокзалы, метро) стационарные металлодетекторы, несмотря на повышающиеся террористические угрозы, как правило, отсутствуют.

Информационная безопасность

- В Лондоне создан Международный альянс обеспечения кибербезопасности (ICSPA), объединяющий правительства, международный бизнес, и правоохранительные органы. Новая организация является некоммерческой, ее финансирование будет осуществляться ЕС и рядом правительств других стран (Австралия, Канада, США и др.). Возглавит ICSPA бывший министр внутренних дел Великобритании (2001-2004 гг.) Дэвид Бланкетт. Альянс уже поддержали компании McAfee и TrendMicro.

- По прогнозам IDC в 2011-2015 гг. российский рынок информационной безопасности будет ежегодно расти в среднем на 27,4 %, а рынок программных систем информационной безопасности на 18,3 %. ■