Ссылка на статью

http://www.securpress.ru/issue.php?m=66&art=1383

Полный текст статьи.

Интегрированные системы безопасности: современные решения и тенденции

А.К. Крахмалев,
зам. председателя ТК 234,
к.т.н., акад. ВАНКБ,

Обеспечение безопасности различных 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.

Особое значение в современных условиях имеет обеспечение безопасности объектов особой важности, повышенной опасности и жизнеобеспечения (критически важных объектов – КВО) на фоне роста криминальных и террористических угроз. 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, кинотеатры, стадионы, вокзалы, аэропорты и т.д.;
- специальные грузы, перевозимые автомобильным, железнодорожным транспортом, судами речного и морского флота.

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 (ОПС), видеонаблюдения - охранного телевидения (СОТ) и контроля доступа (СКУД). 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.

ФГУ НИЦ «Охрана» МВД России совместно с ведущими отечественными предприятиями, работающими в этом направлении, были разработаны и внедрены в серийное производство интегрированные системы: «Рубеж», «Аккорд-512», «Орион», «Кодос», «Ладога-А».

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

Технические возможности ИСБ позволяют определить дальнейшие перспективы их развития – интеграция с другими системами автоматизации и расширение видов и количества угроз, защита от которых обеспечивается с помощью ИСБ.

Тенденция дальнейшей интеграции – объединение ИСБ с системами автоматизации и управления инженерными системами здания или объекта. Это дает возможность построения комплексов, в которых автоматизация и управления инженерными системами объекта тесно связана с обеспечением безопасности, как собственно объекта, так и человека от различных видов угроз, которые могут возникнуть на объекте в результате его функционирования. Взаимосвязь с системами жизнеобеспечения, в этом случае позволяет эффективно и экономично выполнять функциональные задачи. Такие системы, по сути, представляют собой полноценные автоматизированные системы управления функционированием, жизнеобеспечением и безопасностью объекта (АСУ ФЖБ). Пример реализации подобной системы приведен на рис.1.

Рисунок 1 Автоматизированная система управления функционированием, жизнеобеспечением и безопасностью (АСУ ФЖБ) объектов транспортной городской инфраструктуры

ИСБ представляет собой сложную техническую систему и при ее создании приходится использовать различное оборудование, как по функциональному назначению, так и оборудование разных производителей. При этом всегда встает задача совместимости оборудования. Причем она включает в себя две составляющие. Первая это задача обеспечения взаимодействия оборудования различных подсистем, объединенных в ИСБ. Вторая – совместимость оборудования разных производителей. Эти задачи должны быть решены на этапе проектирования ИСБ и могут быть оптимизированы в рамках выбора способа (платформы) интеграции.

Принципы проектирования ИСБ во многом определяются способом интеграции, который можно разбить на четыре основных уровня (платформы интеграции):

1) интеграция на проектном уровне (проектная платформа) – объединение разнородного оборудования, специально не предназначенного для построения ИСБ, только на этапе проектирования системы;
2) интеграция на программном уровне (программная платформа) – объединение оборудования разных производителей, на базе специально разработанного для интеграции программного продукта и управления системой на базе ПЭВМ общего назначения или ЛВС ПЭВМ;
3) интеграция на аппаратно-программном уровне (аппаратно-программная платформа) – объединение оборудования и программного продукта единого производителя и управления системой на базе ПЭВМ общего назначения или ЛВС ПЭВМ;
4) интеграция на аппаратном уровне (аппаратная платформа) – объединение оборудования и программного продукта единого производителя и управления системой без использования ПЭВМ общего назначения, на основе специализированных высокопроизводительных контроллеров и ЛВС на их основе.

Особо следует отметить интеграцию в ИСБ подсистемы видеонаблюдения (системы охранного телевидения). Причем следует, прежде всего, рассматривать цифровые технологии в СОТ, как наиболее перспективные. Особенности интеграции СОТ связаны с тем, что для передачи и обработки видеоданных в цифровых СОТ требуются значительные вычислительные и информационные ресурсы, поэтому реализация цифровых СОТ в ИСБ возможна только на верхнем уровне управления на базе ПЭВМ или ЛВС ПЭВМ.

Общим недостатком первых трех платформ интеграции является использование на верхнем уровне управления ИСБ персональных компьютеров общего назначения. Известно, что ПЭВМ и базовое ПО

общего назначения (операционные системы, системы управления базами данных и др.) предназначены, в основном для офисного и бытового применения. Они обладают излишней функциональностью (мультимедийные, игровые и другие возможности бытовых и офисных ПЭВМ) и недостаточной надежностью для решения задач автоматизации управления системами, в особенности системами безопасности.

Для использования в ИСБ необходимо применять специализированные промышленные ПЭВМ и соответствующее специализированное базовое ПО. Однако стоимость такого решения существенно выше.

Аппаратная платформа интеграции – относительно новое направление развития принципов построения ИСБ. При разработке данного направления ставилась задача устранения общего недостатка других методов интеграции, то есть отказ от использования в ИСБ на всех уровнях ПЭВМ общего назначения.

Аппаратный способ интеграции – на основе оборудования без участия ПЭВМ, обеспечивает максимальную надежность и быстродействие системы.

Для замены ПЭВМ в составе ИСБ на верхнем уровне управления используется специально разработанный для этой цели универсальный контроллер с высокими вычислительными возможностями. Такой контроллер может служить основой для создания интегрированных систем комплексной безопасности и жизнеобеспечения.

Особенность аппаратной платформы заключается в том, что все элементы интегрированной системы безопасности, включая функционал верхнего уровня (АРМ оператора), реализованы в одном приборе по технологии System In Box.

Прибор должен обеспечивать непосредственное подключение и реализацию алгоритмов функционирования всех подсистем ИСБ: охранная и пожарная сигнализация, управление исполнительными устройствами, управление пожаротушением, контроль и управление доступом, видеонаблюдение, диспетчеризация и технологический мониторинг. И, главное, должна обеспечиваться возможность организации АРМ оператора системы без использования дополнительного компьютера: графический монитор, клавиатура, мышь должны подключаться непосредственно к прибору.

Общая структура контроллера для реализации ИСБ на основе аппаратной платформы и пример реализации контроллера приведены на рис.2.

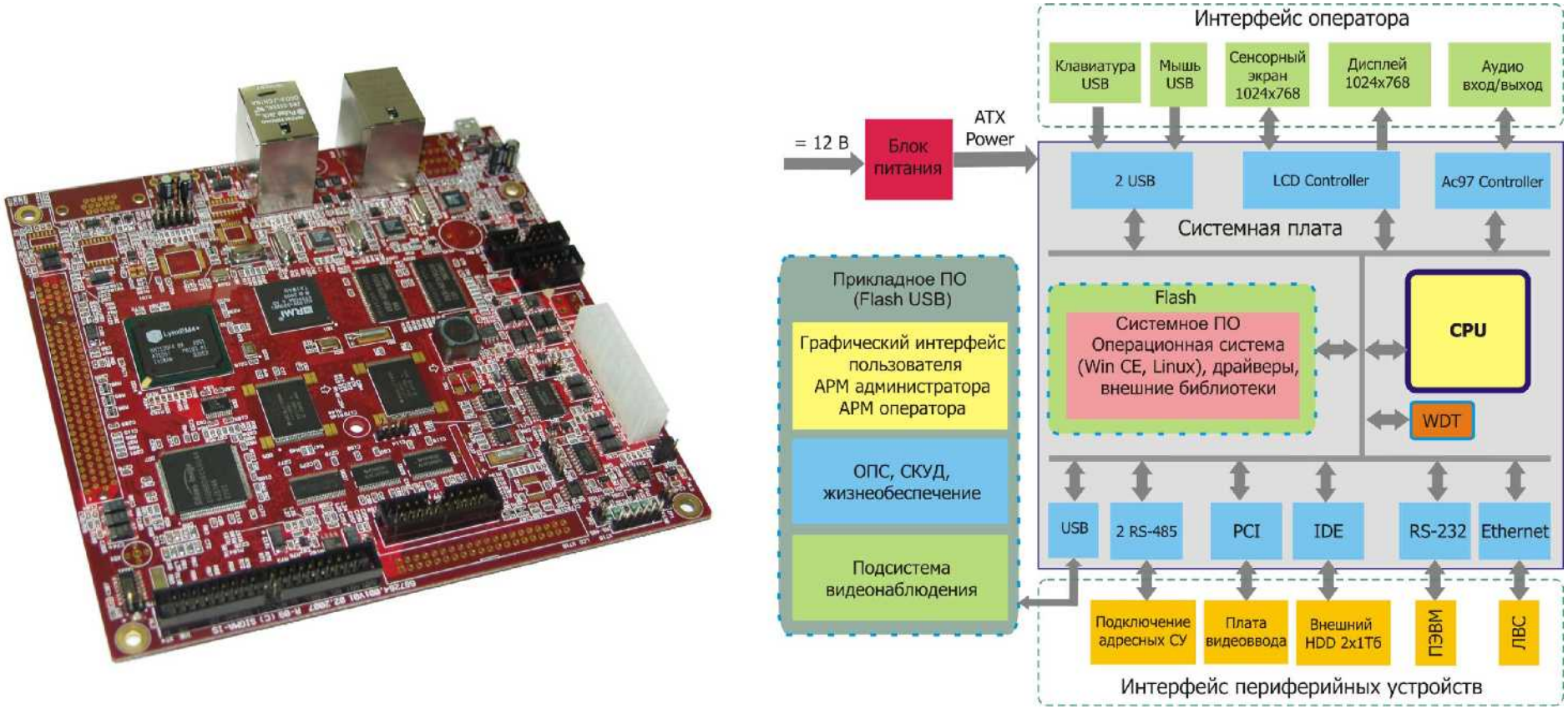

Рисунок 2 Внешний вид системной платы и общая структура контроллера аппаратной платформы

Основные требования для реализации универсальной аппаратной платформы ИСБ:

- мощный контроллер класса System On Chip;
- работа под управлением ОС Linux, Windows CE или других промышленных высоконадежных и защищенных ОС;
- размещение системного ПО и прикладного ПО АРМ во встроенной Flash-памяти;
- подключение внешнего жесткого диска в качестве устройства хранения архива, в том числе и видеоархива;
- полный набор интерфейсов: RS-232, RS-485, USB, Ethernet, IDE, VGA, Sound I/O;
- наличие широкого спектра коммуникационных интерфейсов для связи с удаленным центром;
- наличие программной и аппаратной функции WDT (автоматический сброс и восстановление работы системы при сбоях и «зависании» ПО);
- возможность организации полноценного графического АРМ оператора без использования компьютера;
- установка в контроллере платы видеоввода и соответствующая программная поддержка видео;
- интеграция функций ОПС, СКУД и СОТ в одном устройстве;
- поддержка контроллером большого количества разнообразного объектового оборудования ИСБ;
- реализация сложных автономно функционирующих алгоритмов работы ИСБ;
- низкое энергопотребление, пассивное охлаждение;
- работа в жестких климатических условиях.

Аппаратная платформа для ИСБ позволит также обеспечить:

- простоту инсталляции и эксплуатации системы;
- исключение нецелевого использования ПЭВМ верхнего уровня;
- исключение проблем, типичных для ПЭВМ общего назначения: вирусы, проблемы с драйверами, «зависание» ПО, проблемы механических HDD и т.д.;
- низкое энергопотребление контроллера позволит использовать стандартные источники бесперебойного питания для обеспечения резервного питания системы в течение 24 часов (по требованиям НПБ для систем противопожарной безопасности).

Аппаратная платформа – важный шаг в развитии комплексных систем безопасности. Сфера ее применения чрезвычайно обширна: от охраны квартиры до обеспечения безопасности важнейших государ-

ственных объектов особой важности и повышенной опасности, а также:

- применение в крупных комплексных системах безопасности в качестве интегрированного контроллера, на который сводятся все подсистемы логически выделенной части объекта охраны;
- применение в интегрированных распределенных системах в качестве аппаратной платформы отдельного объекта;
- построение компактных, но в то же время многофункциональных систем безопасности и жизнеобеспечения, где использование ПЭВМ экономически и функционально не оправдано;
- профессиональное решение для адресно-аналоговых пожарных панелей со встроенным графическим интерфейсом;
- профессиональное решение для высокопроизводительных сетевых контроллеров СКУД.

Сфера применения и классы объектов, которые оборудуются ИСБ чрезвычайно широки, поэтому перспективные ИСБ должны иметь набор программных и аппаратных средств для возможности реализации на их базе всех платформ интеграции, в том числе и аппаратной.

Пример структуры такой ИСБ приведен на рис.3.

Неотъемлемой частью ИСБ, в особенности, применительно к решению задачи защиты КВО объектов 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.).

В области 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.

Рисунок 3 Структура ИСБ с возможностью реализации всех платформ интеграции

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 основания анализа развития ИСБ на современном этапе можно отметить следующие тенденции:

1. Стремительный прогресс развития СОТ 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 СОТ). Поэтому СОТ 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, СОТ, 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.).

5. Еще одним из перспективных направлений в развитии ИСБ является переход в построении верхнего уровня управления в ИСБ от стандартных компьютеров к специализированным универсальным многофункциональным контроллерам – аппаратная платформа интеграции. Это позволяет значительно повысить надежность системы в целом.