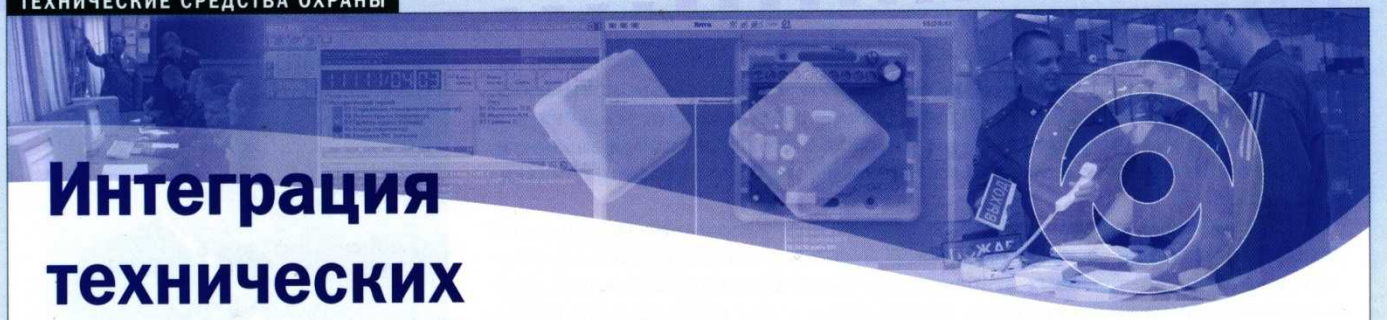

Интеграция технических систем безопасности

Александр Крахмалев

Рассматриваются вопросы создания, применения и классификации интегрированных систем безопасности для охраны объектов

В последние годы к комплексным и интегрированным системам безопасности (КСБ и ИСБ) проявляется повышенный интерес. Это связано с тем, что требования к уровню обеспечения безопасности объектов различных форм собственности постоянно растут, и для их наиболее полного удовлетворения необходимо широко использовать средства автоматизации, автоматизированные системы управления (АСУ), новые информационные технологии, которые позволяют интегрировать организационные и технические ресурсы для решения этих задач.

Такие интегрированные программно-технические комплексы, представляющие собой АСУ различным оборудованием технических средств безопасности, позволяют решительно поднять уровень обеспечения безопасности объектов, сократить требуемые для этого человеческие ресурсы и существенно улучшить работу служб безопасности.

Назначение и область применения

Для современного оснащения промышленных объектов, жилых зданий, учреждений, банков, офисов и др. характерна высокая насыщенность сложным инженерным оборудованием, в том числе и системами безопасности. Все более широкое применение в системах безопасности и инженерного обеспечения (системы охранно-пожарной, пожарной сигнализации, контроля доступа и охранные телевизионные, пожаротушения и АСУ жизнеобеспечением, инженерными системами зданий и технологическими процессами) сегодня находят новые автоматизированные и информационные технологии.

Проблема поддержания такой сложной инфраструктуры в рабочем состоянии, ее мониторинга и контроля является одной из важных задач. Наиболее оптимальный путь решения этой проблемы — создание единого комплекса, координирующего и управляющего работой систем. Логическим развитием такого подхода является создание КСБ и ИСБ. Основой для этого служит единая аппаратно-программная платформа, которая представляет собой АСУ с многоуровневой сетевой архитектурой, имеющую общий центр управления на базе локальной компьютерной сети и содержащую линии коммуникаций, контроллеры приема информации, управляющие контроллеры и другие периферийные устройства, предназначенные для сбора информации от различных датчиков (в том числе от извещателей пожарной и охранной сигнализации), а также для управления различными средствами автоматизации (оповещение, противопожарная автоматика и пожаротушение, инженерные системы и т. д.).

Интегрированная система безопасности (ИСБ) может рассматриваться как совокупность технических средств, предназначенных для построения систем охранной и пожарной сигнализации, контроля и управления доступом, систем охранных телевизионных и систем управления противопожарной автоматикой, которые обладают технической, информационной, программной и эксплуатационной совместимостью.

Еще одним компонентом ИСБ, обязательно присутствующим в составе любой из подсистем, является система оповещения, которая находится в каждой подсистеме в виде световых и звуковых оповещателей, световых табло, мониторов компьютеров и т. д. Однако в некоторых случаях система оповещения может представлять собой отдельную техническую систему (например, речевого оповещения), выполненную на основе радиотрансляционной сети и специализированной аппаратуры.

В соответствии с этим определением построено большое количество ИСБ, как отечественного, так и зарубежного производства. Основная область их применения — обеспечение комплексной безопасности больших, средних и особо важных объектов.

Наличие единых аппаратно-программных средств, которые обладают технической, информационной, программной и эксплуатационной совместимостью, позволяет не только снизить стоимость оборудования объекта, но и получить новые функции, связанные с возможностью обеспечения оперативного взаимодействия подсистем и компонентов ИСБ.

Рассматривая подобные системы с новыми функциями, необходимо оценивать их характеристики и возможности для правильного выбора технических средств при планировании и проектировании общей системы безопасности объекта. Следует отметить, что в этом случае недостаточно учитывать только технические средства. Необходимо рассматривать систему безопасности в целом, как совокупность организационно-технических мер, направленных на защиту от различных угроз. Такие системы обеспечения безопасности объекта предлагается именовать комплексными.

В этом случае комплексную систему безопасности (КСБ) можно представить как совокупность организационно-технических мер, направлен-

ных на защиту от различных угроз безопасности. То есть — совокупность технических средств в соответствии с предыдущим определением ИСБ и организационных решений.

Следующий этап интеграции — объединение территориально удаленных объектов в единую систему контроля и управления безопасностью. Принципиальная возможность удаленной передачи информации имеется во многих системах. Большинство из них построено на базе локальных компьютерных сетей. Следовательно, имеется возможность (используя стандартную аппаратуру передачи данных по телефонным каналам, радиоканалам и другим сетям передачи данных) организовать удаленный доступ.

Следует обратить внимание на системы централизованного наблюдения, которые используются вневедомственной охраной десятки лет. Технические средства этих систем представляют собой разветвленные системы передачи извещений (СПИ) и пульты централизованного наблюдения (ПЦН). Хотя основным назначением СПИ является охранная сигнализация, может обеспечиваться передача сигналов о пожаре. Есть также опыт расширения информативности указанных систем. В соответствии с этим СПИ можно отнести к особому классу КСБ. Перспектива развития систем передачи извещений видится в расширении их функциональных возможностей и превращении их (со временем) в региональные ИСБ — мониторинговые центры, обеспечивающие защиту от многих видов угроз.

Общие принципы построения ИСБ

Современные ИСБ строятся на основе локальных многоуровневых компьютерных сетей различного уровня сложности. Можно выделить **четыре** основных сетевых уровня.

Первый (высший) уровень представляет собой компьютерную сеть типа клиент/сервер на основе сети Ethernet, с протоколом обмена TCP/IP и с использованием сетевых операционных систем (ОС) Windows NT или подобных Unix. Этот уровень обеспечивает связь между сервером и рабочими станциями операторов.

Выбор ОС профессионального класса обусловлен тем, что здесь необходима высокая надежность и защита от несанкционированного доступа. На данном уровне обеспечивается управление ИСБ посредством программного обеспечения автоматизированных рабочих мест (АРМ).

Второй уровень — связь между контроллерами и компьютерами подсистем (вертикальный уровень связи) и связь между однородными контроллерами в каждой из подсистем (горизонтальный уровень связи). На вертикальном уровне наиболее часто используется интерфейс RS 232. На горизонтальном уровне — RS 485 или другие интерфейсы, предназначенные для построения сетей промышленного уровня с хорошей помехозащищенностью и достаточной скоростью обмена данными. В контроллерах некоторых ИСБ возможен прямой выход на первый уровень в протоколе TCP/IP. На этом уровне располагаются приборы приемно-контрольные, обеспечивающие управление средствами охранно-пожарной сигнализации (ОПС), контроллеры системы контроля управления доступом (КУД), а также универсальные контроллеры для обеспечения управления автоматикой.

Третий уровень — связь между контроллерами и считывателями систем доступа. Здесь, как правило, применяются интерфейсы RS 485, RS 232 или, ставшие уже стандартом, интерфейсы считывателей Wigand 26. На этом уровне располагаются также средства управления оповещением, пожаротушением и противопожарной автоматикой, адресные блоки управления с релейными и потенциальными выходами.

Четвертый уровень — извещатели ОПС и входные цепи управления (радиальные шлейфы, адресные шлейфы, входные цепи для контроля датчиков различных подсистем управления). Как правило, здесь применяются нестандартные специализированные интерфейсы и протоколы.

Среди общих принципов построения ИСБ необходимо отметить следующие:

- Расширяемая модульная архитектура аппаратных средств (возможность наращивания аппаратных средств)
- Для программного обеспечения — возможность добавления модулей и расширения функций
- Наличие в составе программного обеспечения упрощенного языка программирования для добавления пользователем собственных реализаций взаимодействия компонентов
- Масштабируемость — возможность первоначального развертывания системы в минимальном варианте с последующим наращиванием в процессе эксплуатации, как количественных характеристик, так и функциональных возможностей
- Интеграция подсистем не должна приводить к снижению общей надежности системы
- Высокая живучесть системы (сохранение работоспособности ИСБ при выходе из строя отдельных подсистем и блоков, а также сохранение работоспособности в пределах своих функций отдельных подсистем при потере связи с центром управления)
- Автономная работа контроллеров подсистем при нарушении связи с центром управления
- Удаленный доступ с использованием каналов связи для построения территориально распределенных систем
- Для распределенных систем со связью с удаленными компьютерами или модемной связью должна быть обеспечена криптографическая защита данных
- Защита программного обеспечения от несанкционированного доступа (разграничение доступа по уровням полномочий пользователей)
- Имитостойкость протоколов передачи данных в сетях
- Графическое отображение планов помещений объекта
- Отображение на плане тревожных точек (тревожная графика)
- Управление устройствами по графическому плану объекта (интерактивная графика)
- Поддержка фотографической базы данных на сотрудников
- Поддержка речевых сообщений.

Классификация

В настоящее время на российском рынке имеется большое количество КСБ и ИСБ, как импортного, так и отечественного производства, представляющих собой собственные разработки — аппаратные средства, аппаратно-программные или программные системы. Значительное количество фирм (проектно-монтажные организации, которые занимаются разработкой проектов, монтажом, пусконаладочными работами и обслуживанием систем индивидуально для конкретного объекта) предлагает услуги по интеграции систем на уровне проектных решений.

Поскольку в настоящее время отсутствует единая нормативная база для КСБ, перед заказчиком встает вопрос выбора ИСБ для оснащения своего объекта, что является довольно трудной задачей в связи с появившимся разнообразием систем. В оп-

ределенной мере выбору могла бы помочь классификация систем. Как правило, в стандартах классификация осуществляется по ряду основных критериев.

Приведенные выше определения систем могут служить в качестве классификации по критерию — «количество реализованных основных функций». Например, для ИСБ основными функциями являются: охранная сигнализация, пожарная сигнализация, контроль доступа, видеоконтроль. Для КСБ добавляются организационные меры, которые соответствующим образом должны быть оговорены в документации на систему. Дальнейшее наращивание функций управления в ИСБ, например, функций управления системами жизнеобеспечения здания (объекта) или автоматизации управления процессами функционирования объекта в соответствии с его спецификой (для промышленного предприятия — это автоматизация производственного процесса), приводит к расширению критерия «количество реализованных основных функций». Такие системы представляют собой автоматизированные системы управления функционированием, жизнеобеспечением и безопасностью (АСУ ФЖБ).

Таким образом, классификация по критерию «количество реализованных основных функций» может помочь выбирать системы в зависимости от необходимой степени автоматизации объекта, исходя из экономических соображений. Более подробное развитие классификации по указанному критерию могло бы получить в нормативных документах. До их разработки критерий «количество реализованных основных функций» должен быть отражен в технической и эксплуатационной документации на системы. Причем для разработчиков систем здесь есть широкое поле деятельности, связанное с расширением возможностей системы путем введения в нее новых функций.

Критериями, по которым можно классифицировать ИСБ, являются принципы интеграции. Здесь можно выделить следующие уровни интеграции подсистем.

1. Интеграция на проектном уровне. Объединение систем осуществляется на этапе проектирования системы для конкретного объекта. Такая работа проводится проектно-монтажными фирмами, которые именуют себя «системными интеграторами». Как правило, в этом случае применяются разнородные подсистемы различных производителей. Объединение (интеграция) указанных систем осуществляется посредством установки оборудования управления подсистемами в общем помещении — центральном пункте управления. Взаимодействие между подсистемами осуществляется на уровне операторов подсистем, то есть без автоматизации. Очевидно, что это минимальный уровень интеграции, ему присущи известные недостатки («человеческий фактор», разнородность аппаратуры, сложность обслуживания, параллельность прокладываемых коммуникаций, отсутствие автоматизации и т. д.) и в настоящее время его нельзя считать перспективным, хотя имеются фирмы, которые предлагают свои готовые и проверенные проектные решения. Оптимальным подходом в этом случае, наверное, следует считать разработанную фирмой собственную проектную методологию построения систем.

2. Интеграция на программном уровне (более точно — на программно-аппаратном уровне с приоритетом программной поддержки). В этом случае роль объединения подсистем играет программный пакет, разработанный и поставляемый как самостоятельный продукт, предназначенный для функционирования в аппаратной среде (как правило, в локальной сети стандартных ЭВМ, которая представляет собой верхний уровень ИСБ). Сопряжение с аппаратной частью подсистем нижнего уровня осуществляется с помощью программ-драйверов, разрабатываемых специально для поддержки конкретных средств других производителей. (Связь с аппаратными средствами осуществляется с помощью стандартных портов ЭВМ.)

Подобное построение ИСБ имеет ряд положительных сторон. Это — вероятность создания высококачественных многофункциональных программных систем на программном уровне, используя все возможности современных компьютерных технологий. Осуществимость интеграции с аппаратными средствами других производителей (при наличии соответствующих драйвера и интерфейсов обмена данными в самих применяемых средствах).

С другой стороны, это приводит к определенным недостаткам — необходимости разработки драйверов для каждого применяемого аппаратного средства. При этом разработчик аппаратного средства не всегда предоставляет протоколы обмена данными. Даже, если протоколы открыты и документированы, в них могут быть заложены ограниченные возможности, не позволяющие обеспечить сопряжение оптимальным образом. Кроме того, фирма-разработчик программной системы, поставляющая свой программный продукт, не может в полном объеме гарантировать работу системы в целом.

3. Интеграция на аппаратно-программном уровне — наиболее распространенный метод построения ИСБ. В этом случае аппаратные и программные средства разрабатываются в рамках единой системы, что позволяет достигнуть оптимальных характеристик (так как вся разработка сосредоточена, как правило, в одних руках и система, как законченный продукт, поставляется с полной гарантией производителя). При этом возможно также получить оптимальные экономические показатели.

Определенным недостатком здесь является то, что каждая фирма предлагает свою оригинальную систему, не совместимую, как правило, с системами других производителей. Данный недостаток обусловлен отсутствием стандартов на сопряжение подсистем ИСБ. Поэтому в перспективе, по мере разработки нормативной базы, здесь возможен определенный прогресс.

Разработка нормативной базы может создать предпосылки объединения всех трех способов интеграции. Это позволило бы разработчикам систем, опираясь на стандарты и используя их, как готовые решения, сосредоточить усилия на совершенствовании качественных характеристик систем и их отдельных составляющих, на разработке принципиально новых направлений.

Об авторе

КРАХМАЛЕВ Александр Кузьмич,
начальник отдела НИЦ «Охрана»
ГУВО МВД России,
кандидат технических наук, профессор.