УДК 654.924

РАЗРАБОТКА КЛАССИФИКАЦИИ И АРХИТЕКТУРЫ ПОСТРОЕНИЯ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ

В. А. Дурденко*, А. А. Рогожин**

* *Воронежский институт инновационных систем*
** *Воронежский институт МВД России*

Поступила в редакцию 26.10.2012 г.

Аннотация. В статье рассмотрены вопросы классификации интегрированных систем безопасности, а также способы построения их архитектуры.
Ключевые слова: интегрированная система безопасности, классификация, функциональная схема, структурная схема, архитектура.
Annotation. Matters of integrated safety systems classification as well as building of the systems are considered in the publication.
Keywords: integrated safety system, classification, functional diagram, block diagram, architecture.

ВВЕДЕНИЕ

Практическая реализация системного подхода к обеспечению комплексной безопасности объектов и имущества, неразрывно связана с идеей разработки и применения интегрированных систем безопасности (ИСБ), которым посвящен ряд научных исследований и нормативно-технических документов [6, 7, 10–17].

Подразделения вневедомственной охраны используют ИСБ, которые рекомендованы МВД России и входят в соответствующий «Список...» [17]. Данный «Список...» сформирован для реализации единой технической политики в обеспечении надёжной охраны объектов, квартир и других мест хранения личного имущества граждан на территории Российской Федерации.

При выборе и проектировании надежных ИСБ объектов необходимо руководствоваться действующей классификацией. Однако, в единственном стандарте [6] классификация ИСБ отсутствует. Отсюда вытекает актуальность и необходимость проведения классификации ИСБ.

1. АРХИТЕКТУРА ПОСТРОЕНИЯ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ

Интегрированная система безопасности объекта – это совокупность совместно действующих средств и систем охранной безопасности (СОБ), как правило, охранно-тревожной сигнализации (СОТС) [2, 3], пожарной сигнализации (СПС) [18], охранного телевидения (СОТ) [5], контроля и управления доступом (СКУД) [4], управления жизнеобеспечением (СУЖ) [6] и, возможно, других систем, обладающих технической, программной, информационной, электромагнитной и эксплуатационной совместимостью, работающих по единому алгоритму взаимодействия, имеющих общие каналы связи, программное обеспечение, базы данных, и предназначенная для обеспечения противокриминальной и антитеррористической защиты объекта, в том числе в безоператорном режиме [95].

Анализ современных ИСБ, входящих в «Список...» [17], а именно: «Кодос», «Орион», «Пахра», «Рубеж-08» позволил сформировать перечень основных эксплуатационных возможностей ИСБ. Итак, современные ИСБ обеспечивают:

– модульную структуру, позволяющую обеспечивать безопасность как малых, так и очень больших объектов, в том числе территориально распределенных;

– контроль и управление доступом на охраняемые объекты с учётом полномочий каждого сотрудника;

– контроль охранной и тревожной сигнализации на объекте;

– контроль пожарной сигнализации на объекте;

– видеонаблюдение, видеоконтроль и видеорегистрацию тревожных ситуаций с графических планов объектов;

– отображение событий на графических планах объектов;

– разработку сценариев действий (правил реакции) одной системы в ответ на события в другой;

– управление установками пожарной безопасности;

– управление инженерными системами здания;

– имитостойкость протокола передачи данных в сетях;

– возможность передачи информации по любым каналам связи;

– возможность взятия под охрану, снятия с охраны объектов с помощью электронных карт, ключей;

– речевое предупреждение дежурного о тревожных событиях, возможность записи и воспроизведение сообщений;

– отображение состояния зон, разделов, точек доступа, приемно-контрольных приборов, считывающих устройств, видеокамер на графических планах помещений с подробными текстовыми пояснениями;

– разграничение полномочий дежурных операторов, администраторов за счёт многоуровневой системы паролей и возможного подключения биометрических систем ограничения доступа к программам автоматизированных рабочих мест (АРМ);

– протоколирование всех событий, происходящих в системе;

– ведение единой базы данных пользователей;

– развитую диагностику работоспособности всех блоков и устройств системы;

– удаленное администрирование системы;

– сохранение общей надежности системы при интеграции подсистем;

– высокую живучесть системы, то есть сохранение ее работоспособности при выходе из строя отдельных подсистем и блоков, а также сохранение работоспособности отдельных подсистем (в рамках их функций) при выходе из строя сервера ИСБ или при потере связи с ним;

– автономную работу контроллеров подсистем при нарушении связи с сервером ИСБ.

В ИСБ входят традиционные СОБ с известным составом и структурами. Поэтому обобщенная функциональная схема ИСБ будет выглядеть, как показано на рис. 1.

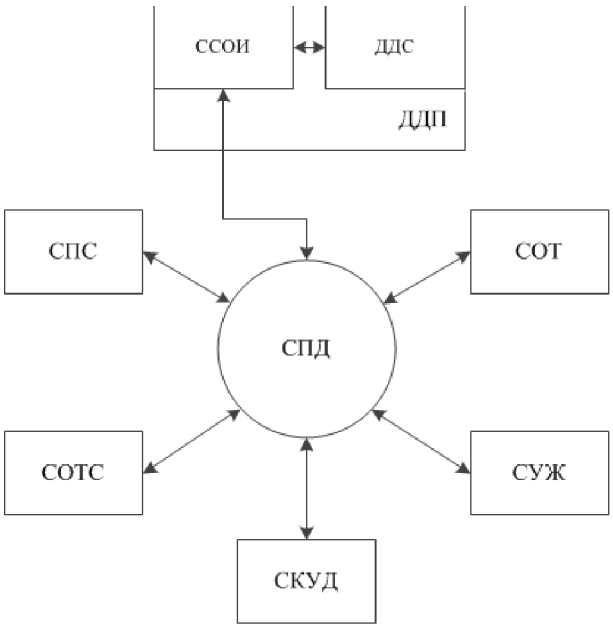

Рис. 1. Обобщенная функциональная схема ИСБ: *ДДП* – дежурно-диспетчерская подсистема; *ДДС* – дежурно-диспетчерская служба (служба охраны); *ССОИ* – система сбора и обработки информации

ИСБ обладает достаточно сложной многоуровневой (иерархической) структурой, обусловленной сложностью входящих в нее СОБ, программного обеспечения и коммуникационного оборудования сети передачи данных (СПД), поэтому для последующего анализа вопросов построения необходимо разработать иерархическую структурную схему ИСБ (см. рис. 2).

Первый (высший) уровень иерархии представляет собой компьютерную сеть типа клиент-сервер на основе сети Ethernet с протоколом обмена TCP/IP и с использованием сетевых операционных систем (ОС) Windows XP или

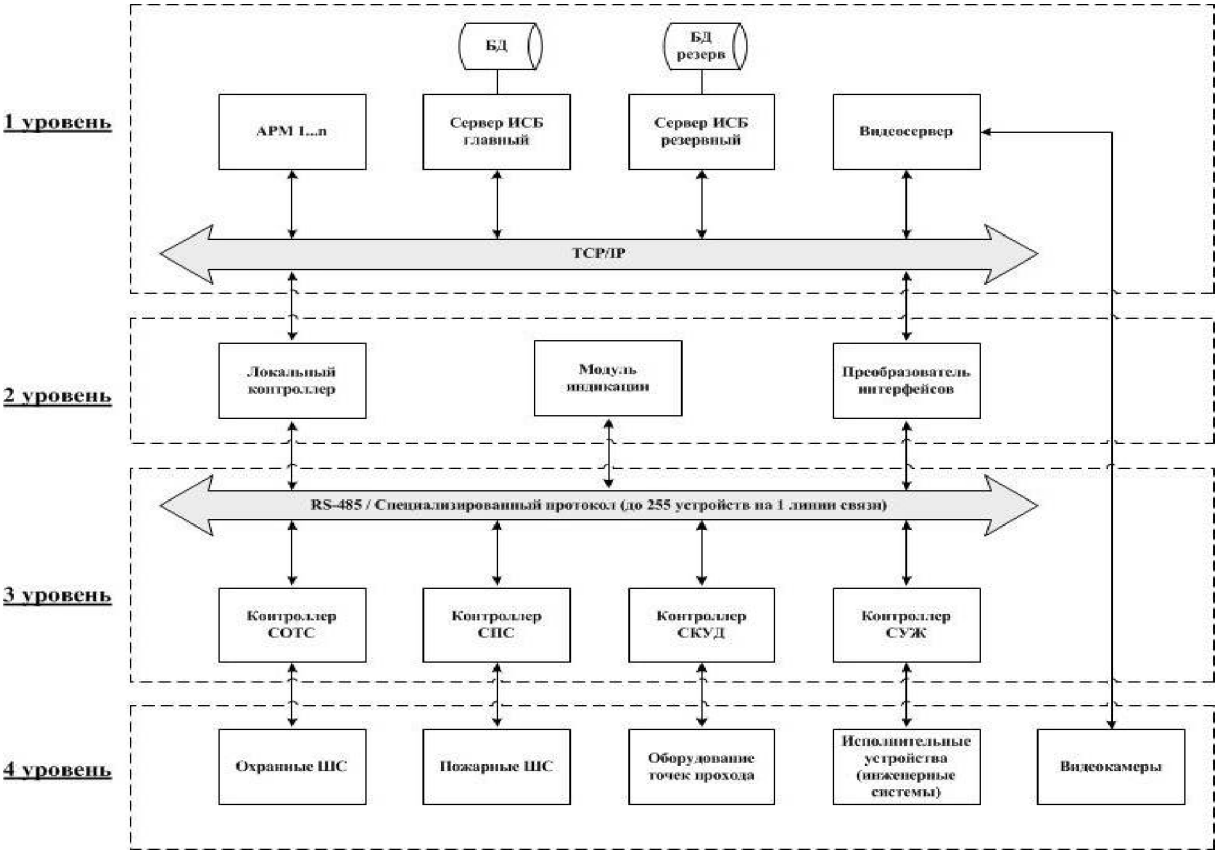

Рис. 2. Иерархическая структурная схема ИСБ: *БД* – база данных; *Сервер ИСБ* – персональный компьютер с установленным специализированным программным обеспечением ИСБ; *АРМ* – автоматизированное рабочее место оператора ИСБ (АРМ удаленного администрирования, АРМ бюро пропусков, АРМ оператора, АРМ начальника службы охраны и т.д.); *TCP/IP* – сеть передачи данных по протоколу TCP/IP; локальный контроллер – контроллер, с помощью которого можно автономно (без серверного ПЭВМ) управлять системой и вести протоколирование событий; *модуль индикации* – индикаторная панель, предназначенная для отображения состояния охранных/пожарных зон, разделов, каналов управления; *контроллеры СОТС, СПС, СКУД, СУЖ* – приборы контроля и управления периферийным оборудованием 4-го уровня иерархии

типа Unix. Этот уровень обеспечивает связь между сервером ИСБ и АРМ операторов. Выбор ОС профессионального класса обусловлен тем, что здесь необходим высокий уровень надежности и защита от несанкционированного доступа к информационных ресурсам ИСБ. На данном уровне обеспечивается управление всей ИСБ посредством специализированного программного обеспечения.

Второй уровень иерархии – связь между локальными контроллерами и компьютерами первого уровня (вертикальный уровень связи). На вертикальном уровне наиболее часто используется интерфейс TCP/IP или RS-232. Если в ИСБ не используются локальные контроллеры для локального управления (резервирования функций сервера ИСБ) объектовым оборудованием, то используются преобразователи интерфейсов типа RS-485/TCP/IP, которые предназначены лишь для обеспечения связи третьего уровня с первым.

Третий уровень иерархии – связь между однородными контроллерами каждой из подсистем третьего уровня с локальными контроллерами или с преобразователями интерфейсов второго уровня (горизонтальный уровень связи – протоколы RS-485 или специализированные); а также связь между локальными контроллерами или преобразователями интерфейсов с компьютерной сетью первого уровня (вертикальный уровень связи – протокол TCP/IP).

В контроллерах третьего уровня некоторых ИСБ реализован прямой выход на первый уровень в протоколе TCP/IP.

Четвертый уровень иерархии – связь между контроллерами подсистем ИСБ третьего уровня с периферийными устройствами четвертого уровня. Здесь располагаются: устройства считывания, электрозамки, различные исполнительные устройства, в том числе инженерных систем зданий, оповещатели, модули пожаротушения, радиальные ШС, адресные ШС, входные цепи для контроля датчиков различных подсистем управления, видеокамеры и т.п. Как правило, здесь применяются нестандартные специализированные интерфейсы и протоколы.

В связи со структурной и функциональной сложностью ИСБ, ограниченностью нормативно-правового поля и недостаточной квалифицированностью ИТР подразделения охраны испытывают определенные трудности в выборе, проектировании, внедрении и эксплуатации ИСБ на объектах.

Учитывая, что любой объект, на котором внедряется ИСБ, является уникальным, каждая проектируемая система представляет собой продукцию единичного производства, создаваемую вновь для каждого конкретного объекта. Следовательно, при создании ИСБ на объекте нужно учитывать положения [1]. Стандарт устанавливает порядок разработки, согласования и утверждения технического задания, технической документации, а также порядок изготовления, контроля, монтажа, приемки и сдачи в эксплуатацию изделий единичного производства и их составных частей, окончательная сборка, наладка, испытания и доводка которых могут быть проведены только на месте эксплуатации в составе конкретного производственного объекта.

Важнейшую роль при создании ИСБ на объекте играет процесс проектирования, так как именно на этапе проектирования закладываются все необходимые качественные и количественные характеристики, в том числе и надежностные. При проектировании важным вопросом является выбор подсистем и технических средств, из которых будет создаваться ИСБ. Под техническими средствами ИСБ понимаются технические изделия (продукция серийного производства, специально предназначенная для построения ИСБ), а также система в целом, как продукция единичного производства, создаваемая для каждого объекта путем проектирования, монтажа, пуско-наладки и сдачи в эксплуатацию, функциональным назначением которой является обеспечение безопасности от нормированных угроз. ИСБ представляет собой сложную техническую систему, и при ее создании приходится использовать различное оборудование, как по функциональному назначению, так и возможно оборудование разных производителей. Следовательно, на этапе проектирования ИСБ определяется способ (платформа) интеграции оборудования.

Учитывая тот факт, что основными системами, входящими в ИСБ и предназначенными для самого раннего обнаружения несанкционированного проникновения правонарушителя на объект или очага возгорания, являются СОТС и СПС, то основные требования к проектированию ИСБ можно сформулировать, полагаясь на [2, 3, 6]:

– Состав, структура построения и функции системы, комплекса должны быть технически и экономически обоснованы.

– Допускается разделение всей системы, комплекса в целом на функционально самостоятельные составные части (рубежи, участки, зоны, разделы, контуры и т.п.). При этом построение системы, комплекса должно обеспечивать возможность ее, его модификации (расширения функциональных возможностей) и устойчивую работоспособность (отказ какого-либо из функциональных участков не должен приводить к отказу всей системы, комплекса в целом).

– Проектируемые система или комплекс должны удовлетворять требованиям рациональности, целостности, комплексности, перспективности и динамичности:

– Рациональность выбираемого варианта системы или комплекса достигают его условной оптимизацией, означающей минимизацию затрат на реализацию при заданной эксплуатационной надежности.

– Целостность выбираемого варианта обеспечивают наилучшим сочетанием и взаимодействием его составных частей, имеющих ограниченные тактико-технические возможности и ресурс.

– Комплексность выбираемого варианта предполагает его сбалансированность с учетом общей целевой задачи при оснащении объекта, реальных (в т.ч. финансовых) возможностей пользователя.

– Перспективность выбираемого варианта означает, что он должен обеспечивать условия для своего развития с учетом возможных изменений в процессе эксплуатации.

– Динамичность выбираемого варианта заключается в гарантированном выполнении им целевых функций в течение заданного срока службы с учетом износа и восстанавливаемости ТСО.

2. КЛАССИФИКАЦИЯ ИНТЕГРИРОВАННЫХ СИСТЕМ БЕЗОПАСНОСТИ

Как правило, классификация технических систем осуществляется по ряду основных критериев, отличительных признаков.

Анализ предметной области помог разработать классификацию ИСБ по трем основным критериям, как показано на рис. 3.

Принципы построения и проектирования ИСБ во многом определяются способом интеграции оборудования подсистем, поэтому первым критерием, по которому можно классифицировать ИСБ является способ (платформа) интеграции подсистем.

Интеграция на проектном уровне (проектная платформа) – это агрегирование разнородного оборудования от разных фирм-производителей, специально не предназначенного для построения ИСБ, производится только на этапе проектирования (см. рис. 4). Интеграция проводится проектно-монтажными организациями, которые позиционируются как «системные интеграторы». Интеграция подсистем осуществляется путем организации ДДП в общем помещении – пункте автономной охраны (ПАО) или пункте централизованной охраны (ПЦО). Взаимодействие между подсистемами осуществляется на уровне операторов подсистем, то есть без автоматизации, и/или на «релейном» уровне отдельных технических средств охраны (ТСО). При этом разрабатываются инструкции по взаимодействию операторов СОБ, функционирующих на объекте (в первом случае), или схемы электрических соединений отдельных ТСО (во втором случае).

На рис. 4 показан пример интеграции подсистем СОТС, СПС и СКУД на релейном уровне. В этом случае используются нормально-замкнутые контакты реле прибора приемно-контрольного охранно-пожарного (ППКОП), которые включаются в разрыв цепи электромагнитного замка (ЭМЗ).

При срабатывании охранных, тревожных или пожарных ШС, логически «привязанных» к данному реле, разрывается цепь ЭМЗ и автоматически предоставляется доступ в/из охраняемую зону на заданный промежуток времени. Такой вариант интеграции можно использовать для организации, например, беспрепятственной эва-

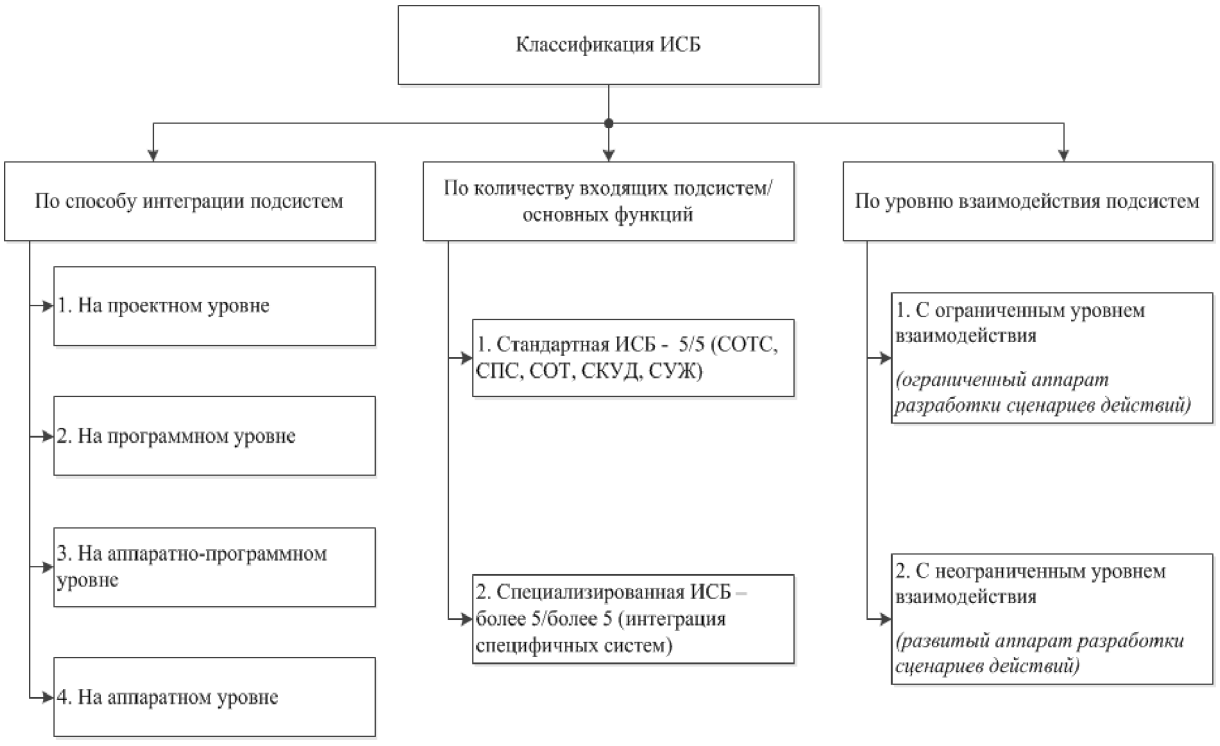

Рис. 3. Классификация ИСБ

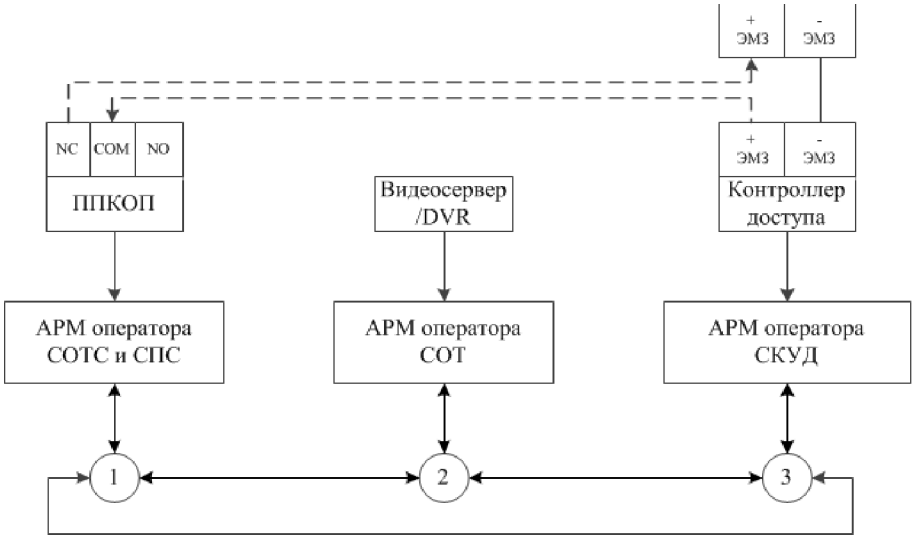

Рис. 4. Интеграция подсистем ИСБ на проектном уровне: 1, 2, 3 – операторы подсистем; NC, COM, NO – клеммы реле на переключение; +/- ЭМЗ – клеммы электромагнитного замка

куации людей с охраняемого объекта, на котором был обнаружен пожар или очаг возгорания.

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 его нельзя считать в настоящее время перспективным.

Интеграция на программном уровне (программная платформа) – в этом случае роль агрегирования разнородного оборудования от разных фирм-производителей играет специальное ПО – программный пакет, разработанный и поставляемый как самостоятельный продукт (программная продукция серийного производства, специально предназначенная для интеграции технических подсистем). Такое ПО предназначено для функционирования в аппаратной среде, как правило, в локальной сети ПЭВМ общего назначения, которая представляет собой первый (верхний) уровень ИСБ. Сопряжение с аппаратной частью подсистем нижнего уровня осуществляется с помощью программ-драйверов, разрабатываемых специально для поддержки конкретных ТСО других производителей. Связь с аппаратными средствами осуществляется с помощью стандартных портов ПЭВМ.

Пример интеграции подсистем на программном уровне представлен на рис. 5.

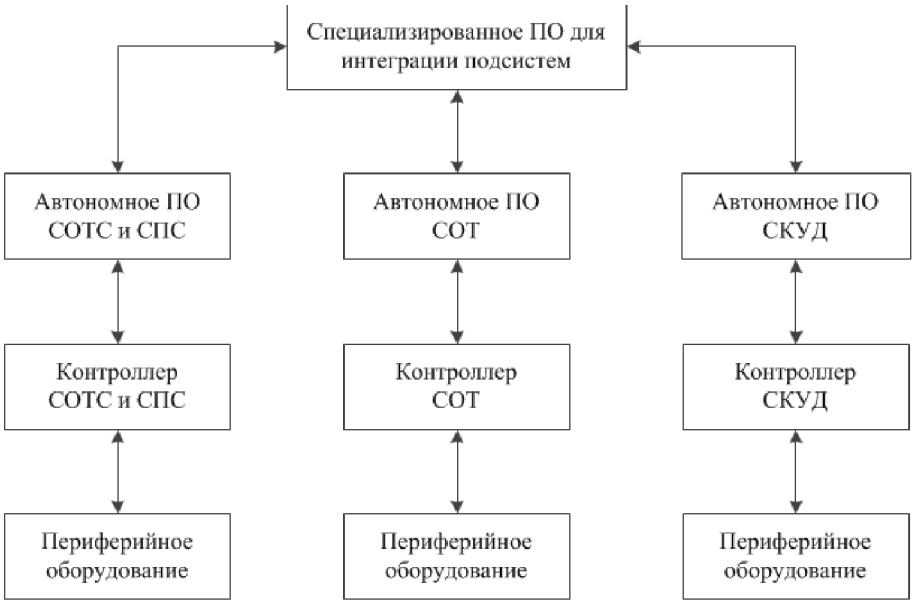

Рис. 5. Интеграция подсистем ИСБ на программном уровне

Подобное построение ИСБ имеет ряд положительных сторон. Это возможность на программном уровне, используя все возможности современных компьютерных технологий, создавать высококачественные многофункциональные программные системы. Появляется возможность интеграции с аппаратными средствами других производителей при наличии соответствующего драйвера и соответствующих интерфейсов обмена данными в самих применяемых средствах. С другой стороны, это порождает и определенные недостатки – необходимость разработки драйверов для каждого применяемого аппаратного средства. При этом не всегда разработчик аппаратного средства предоставляет протоколы обмена данными. Даже, если протоколы открыты и документированы, в них могут быть заложены ограниченные возможности, не позволяющие оптимальным образом обеспечить сопряжение. Кроме того, фирма-разработчик программной системы не может в этом случае в полном объеме гарантировать работу всей ИСБ в целом. Примерами таких систем являются ИСБ на базе ПО «Грифос», «Lyrix», «Apacs», «Интегра-С», «ParsecNET 3» и других.

Интеграция на аппаратно-программном уровне (аппаратно-программная платформа) – в этом случае аппаратные и программные средства разрабатываются унифицированными одним предприятием. Это позволяет достигнуть оптимальных эксплуатационных характеристик, так как ИСБ как законченный продукт поставляется с полной гарантией производителя.

В данном случае основой для построения ИСБ служит продукт серийного производства – комплекс (набор) аппаратно-программных средств, которые обладают технической, информационной, программной и эксплуатационной совместимостью. Примерами ИСБ с аппаратно-программной интеграцией являются ИСБ «Орион», «Кодос», «Рубеж-08», «Пахра» и другие.

Интеграция на аппаратном уровне (аппаратная платформа) – объединение оборудования и программного комплекса единого производителя и управление системой без использования ПЭВМ общего назначения, на основе специализированных высокопроизводительных контроллеров и ЛВС на их основе. Аппаратная платформа интеграции – относительно новое направление развития в построении ИСБ. При разработке данного направления происходит отказ от использования в ИСБ на всех уровнях ПЭВМ общего назначения. Аппаратный способ интеграции 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. Примером ИСБ с аппаратной платформой интеграции является ИСБ «Рубеж-09».

Классификация ИСБ также может осуществляться по критерию – «количество входящих подсистем/количество основных функций».

Стандартная ИСБ включает, как правило, 5 основных подсистем: СОТС, СПС, СОТ, СКУД, СУЖ, а следовательно, выполняет 5 основных функций: обнаружение проникновения/попытки проникновения в охраняемую зону; обнаружение пожара/очага возгорания в охраняемой зоне; видеоконтроль; ограничение и разграничение доступа в охраняемую зону; управление инженерными системами объекта.

Специализированная ИСБ включает тот же набор подсистем и реализуемых функций, что и стандартная, а также как минимум одну дополнительную подсистему безопасности из ряда [6] в зависимости от спектра угроз на конкретном объекте, например, систему оперативной связи или систему определения государственных регистрационных знаков автотранспортных средств и т.д.

Классификация ИСБ также может осуществляться по критерию – «уровень взаимодействия подсистем». Именно уровень взаимодействия подсистем определяет технический уровень ИСБ. Предложенный критерий объективно может быть выражен через общее количество информационных потоков между подсистемами ИСБ, например, как показано на рис. 6.

ИСБ с ограниченным уровнем взаимодействия обладает ограниченным аппаратом разработки сценариев действий (реакций) одной подсистемы в ответ на события в другой. Такой уровень взаимодействия характерен для ИСБ с проектной и чисто программной платформой интеграции.

ИСБ с неограниченным уровнем взаимодействия обладает развитым аппаратом разработки сценариев действий (реакций) одной подсистемы в ответ на события в другой. Такой уровень взаимодействия характерен для ИСБ с

№	Взаимодействующие системы			Передаваемая информация
1.	СОТС →	ДДП	-	Сигналы о снятии/постановке на охрану, тревожные сигналы от охранных и тревожных извещателей, подтверждение исправного состояния ШС
2.	СОТС →	ДДП →	СОТ	Вывод изображений видеокамер из тревожных зон, смена режима записи видеосервера
3.	СОТС →	ДДП →	СУЖ	Включение светового, звукового, речевого оповещения и т.п.
4.	СОТС →	ДДП →	СКУД	Блокировка точек доступа, примыкающих к тревожной зоне
5.	СПС →	ДДП	-	Сигналы о снятии/постановке на охрану, тревожные сигналы от пожарных извещателей, подтверждение исправного состояния ШС
6.	СПС →	ДДП →	СОТ	Вывод изображений видеокамер из пожарных зон, смена режима записи видеосервера
7.	СПС →	ДДП →	СУЖ	Включение светового, звукового, речевого оповещения; включение системы дымоудаления; включение системы пожаротушения и т.п.
8.	СОТС →	ДДП →	СКУД	Разблокировка точек доступа для эвакуации
9.	СОТ →	ДДП	-	Видеоконтроль за охраняемыми зонами объекта, подтверждение исправного состояния
10.	СОТ →	ДДП →	СОТ	Вывод изображений видеокамер из тревожных зон, контролируемых интеллектуальными датчиками движения, смена режима записи видеосервера
11.	СОТ →	ДДП →	СУЖ	Включение или выключение инженерных систем в зависимости от визуальной информации от видеокамер
12.	СОТ →	ДДП →	СКУД	Блокировка/разблокировка точек доступа в зависимости от визуальной информации от видеокамер
13.	СКУД →	ДДП	-	Текущие данные от предъявляемых идентификаторов, подтверждение исправного состояния
14.	СКУД →	ДДП →	СОТС	Управление снятием/постановкой на охрану через СКУД
15.	СКУД →	ДДП →	СОТ	Вывод изображений видеокамер из точек и зон доступа при поднесении идентификаторов к считывателям
16.	СКУД →	ДДП →	СУЖ	Включение речевого оповещения при поднесении идентификаторов к считывателям и т.п.
17.	ДДП →	СОТС	-	Управление снятием/постановкой на охрану оператором ИСБ, контроль параметров ШС
18.	ДДП →	СПС	-	Управление снятием/постановкой на охрану оператором ИСБ, контроль параметров ШС
19.	ДДП →	СКУД	-	Управление отдельными элементами доступа оператором ИСБ
20.	ДДП →	СОТ	-	Управление PTZ-видеокамерами оператором ИСБ, работа с архивами
21.	ДДП →	СУЖ	-	Управление оператором ИСБ инженерными системами объектами

Рис. 6. Основные информационные потоки в ИСБ

аппаратно-программной и аппаратной платформой интеграции.

ЗАКЛЮЧЕНИЕ

В работе предложены обобщенная функциональная и иерархическая структурная схемы ИСБ. Ввиду ограниченности нормативно-правового поля в области выбора и проектирования предложена классификация ИСБ.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 15.005-86. Система разработки и постановки продукции на производство. Создание изделий единичного и мелкосерийного производства, собираемых на месте эксплуатации.

2. ГОСТ Р 50775-95 (МЭК 60839-1-1:88). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения.

3. ГОСТ Р 50776-95 (МЭК 60839-1-4:89). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. ГОСТ Р 51558-2008. Системы охранные телевизионные. Общие технические требования и методы испытаний.

6. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования.

7. *Евдокимов Д.Е.* Классификация интегрированных систем безопасности / Д. Е. Евдокимов // Системы безопасности – № 6. – М., 2007. – С. 34–36.

8. *Кучумаров С.В.* Обзор интегрированных систем безопасности для решения широкого круга задач / С. В. Кучумаров, Р. А. Большаков // Системы безопасности. – 2010. – № 4. – С. 84–88.

9. О пожарной безопасности: Федеральный закон Российской Федерации от 21 декабря 1994 г. № 69-ФЗ (ред. 2006 г.).

10. *Рогожин А.А.* Инновационный подход к моделированию процесса обеспечения комплексной безопасности объектов на основе дорожного картирования / А. А. Рогожин, В. А. Дурденко // Общественная безопасность, законность и правопорядок в III тысячелетии: материалы международной научно-практической конференции. – Воронеж: Воронежский институт МВД России, 2012 г. – С. 75–80.

11. *Рогожин А.А.* Критериальное моделирование оценки качества функционирования и надежности интегрированных систем безопасности охраняемых объектов / В. А. Дурденко, А. А. Рогожин // Вестник Воронежского института МВД России. – Воронеж: 2012 г. – № 1. – С. 205–214.

12. *Рогожин А.А.* Логико-вероятностное моделирование оценки уровня защищенности охраняемых объектов путем анализа безопасности и надежности интегрированных систем безопасности / А. А. Рогожин, В. А. Дурденко // Математические методы и информационно-технические средства: Материалы VIII Всероссийской научно-практической конференции. – Краснодар: Краснодарский университет МВД России, 2012 г. – С. 188–193.

13. *Рогожин А.А.* Моделирование процесса совершения и пресечения правонарушения на объекте, охраняемом подразделением вневедомственной охраны при ОВД с помощью интегрированной системы безопасности / В. А. Дурденко, А. А. Рогожин // Информатика: проблемы, методология, технологии : материалы XII Международной научно-методической конференции. – Воронеж: Воронежский государственный университет, 2012 г. – С. 123–124.

14. *Рогожин А.А.* Обеспечение комплексной безопасности социально значимых объектов с помощью внедрения интегрированных комплексов безопасности на примере ИКБ «КОДОС» / П. М. Изразцов, А. А. Рогожин // Охрана, безопасность и связь : материалы международной научно-практической конференции, Ч. 1. – Воронеж: Воронежский институт МВД России, 2011 г. – С. 139–141.

15. *Рогожин А.А.* Разработка технического задания на проектирование интегрированной системы безопасности аэропорта / И. И. Шаяхметов, А. А. Рогожин, // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сборник материалов Всероссийской научно-практической конференции. – Воронеж: Воронежский институт МВД России, 2012 г. – С. 204–207.

16. *Рогожин А.А.* Разработка учебно-демонстрационных комплексов и применение технологии конфигурирования интегрированных систем безопасности в учебном процессе по специальности 210302.65 – «Радиотехника» / А. А. Рогожин // Математические методы и информационно-технические средства: Материалы VIII Всероссийской научно-практической конференции. – Краснодар: Краснодарский университет МВД России, 2012 г. – С. 179–183.

17. Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений и системам мониторинга подвижных объектов, предназначенным для применения в подразделениях вневедомственной охраны» и «Единым техническим требованиям к объектовым подсистемам охраны, предназначенным для применения в подразделениях вневедомственной охраны». – М.: ГУВО МВД России, 2012. – 50 с.

18. Технический регламент о требованиях пожарной безопасности : Федеральный закон Российской Федерации от 22.07.2008 г. № 123-ФЗ.

Дурденко Владимир Андреевич – д.т.н., профессор кафедры менеджмента, Воронежский институт инновационных систем. Тел.(473) 2-354-898. E-mail:dva_viis@mail.ru

Рогожин Александр Александрович – преподаватель кафедры технических систем безопасности Воронежского института МВД России. Тел. (473) 2-312-412. E-mail: raa_tsbs@list.ru

Дурденко Владимир Андреевич – д.т.н., профессор кафедры менеджмента, Воронежский институт инновационных систем. Тел.(473) 2-354-898. E-mail:dva_viis@mail.ru

Рогожин Александр Александрович – преподаватель кафедры технических систем безопасности Воронежского института МВД России. Тел. (473) 2-312-412. E-mail: raa_tsbs@list.ru