

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ И ПОДСИСТЕМЫ ОПС В ИХ СОСТАВЕ: ОПРЕДЕЛЕНИЯ, ПРЕИМУЩЕСТВА, ОСОБЕННОСТИ

И. Раков, И. Заботин, И. Подсекин

Большинство современных комплексов технических средств обеспечения безопасности средних и крупных объектов реализуется в виде интегрированных систем. При этом в состав комплекса входят, как правило, подсистемы:

- охранной, в том числе периметральной, сигнализации (ОС и ПОС соответственно),
- пожарной сигнализации (ПС),
- контроля и управления доступом (СКУД),
- телевизионного наблюдения и регистрации (СТН),
- автоматического оповещения о чрезвычайных ситуациях (СО),
- защиты речевой и компьютерной информации (ЗИ),
- охранного освещения (ОО) и др.

Стандарты на интегрированные системы безопасности (ИСБ), в том числе и касающиеся терминов и определений, находятся в стадии разработки. Поэтому для того, чтобы сделать последующее изложение предметным, уместным представляется привести наше определение понятия "ИСБ".

Необходимым и достаточным для отнесения комплекса средств безопасности к классу интегрированных систем является наличие следующих свойств:

- единые мониторинг, управление и протоколирование событий в подсистемах,
- автоматическое взаимодействие между подсистемами.

Заметим, что единое конфигурирование, являясь неоперативной функцией, желательно, но не обязательно в ИСБ, и потому не отнесено к необходимым и достаточным классификационным характеристикам.

Целесообразность построения комплекса технических средств безопасности как ИСБ обусловлена рядом преимуществ. Для конечного пользователя существенно следующее:

- встроенный в ИСБ механизм автоматических взаимодействий, в том числе и автоматической поддержки действий оператора, обеспечивает повышение оперативности и корректности принятия решений в тревожных ситуациях;
- этот же механизм наряду с объективным протоколированием событий обеспечивает постоянный контроль действий персонала охраны, повышая эффективность его работы, а также обеспечивая руководителей информацией, необходимой при расследовании нештатных ситуаций и разработке мероприятий по повышению квалификации персонала и совершенствованию системы обеспечения безопасности объекта;
- наличие единого интерфейса мониторинга и управления (Single-Seat Interface), позволяет оператору не переключаться между множеством окон отдельных программ при работе с ИСБ, что облегчает освоение и эксплуатацию системы, снижает утомляемость персонала, позволяет увеличить размеры контролируемого одним оператором фрагмента ИСБ;
- единство управляющего программного обеспечения исключает конфликты программных оболочек отдельных подсистем, разработанных разными производителями;
- единые мониторинг, управление и протоколирование событий в подсистемах обеспечивают гибкие возможности создания рабочих мест ИСБ с различными возможностями и полномочиями, быстрого и малозатратного переконфигурирования и развития ИСБ;
- единая база событий обеспечивает пользователя максимально полной информацией в форме, максимально удобной для проведения расследований нештатных ситуаций.

Тенденция интеграции подсистем безопасности объектов в настоящее время является фундаментальным направлением развития рынка. Однако подходы производителей к реализации интеграции различны. Аппаратная интеграция подразумевает объединение центральных процессоров подсистем безопасности (приемно-контрольных приборов (ПКП) ОС, ПОС и ПС, контроллеров СКУД и т.д.) общей специализированной информационной шиной, с помощью которой производится мониторинг, конфигурация, управление и взаимодействие систем между собой (рис. 1). Вырожденным вариантом такой интеграции является релейная. Отличаясь высокой надежностью, релейная интеграция находит

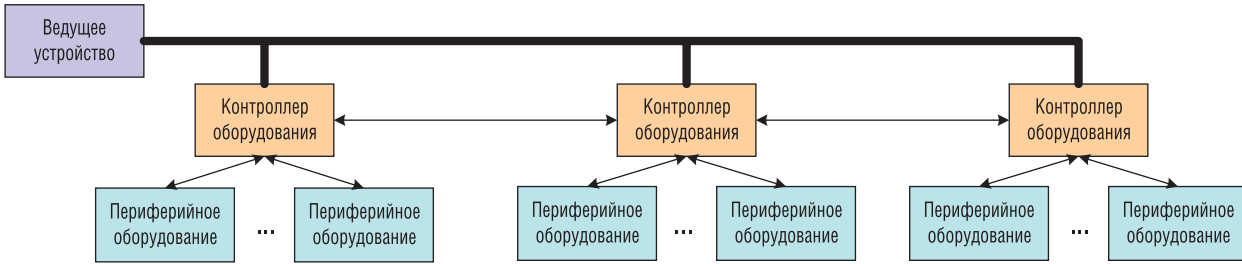


Рис. 1. Аппаратно-интегрированная система

применение, например, для автоматической разблокировки аварийных выходов при пожарной тревоге.

Однако вследствие малой информативности более сложные алгоритмы реализуются с применением специальных шинных протоколов. При корректном выборе алгоритмов взаимодействия и кодирования "шинная" аппаратная интеграция также высоконадежна, поскольку обслуживается "жесткими" вычислителями с неизменяемой оперативно программой. Большинство производителей таких систем применяют собственные уникальные закрытые протоколы, ограничивая, таким образом, возможности аппаратной интеграции оборудования других производителей. Негативной стороной этого подхода является последующая зависимость пользователя от первоначально выбранного производителя.

В аппаратно-интегрированных ИСБ применяются и компьютеры со специализированными программами, однако их функция при этом, как правило – одно из устройств управления (регистрации) с расширенными возможностями. Примерами аппаратно-интегрированных систем могут служить "Кодос", "Орион", Vista-250, "Рубеж-08" и др.

При программной интеграции оборудование каждой (или нескольких аппаратно-интегрированных) подсистем безопасности полностью контролируется собственной программой. Интегрирующим элементом в этом случае является программная надстройка (рис. 2), через которую осуществляется централизованный мониторинг, протоколирование и управление оборудованием, а также

межсистемное (в данном случае – межпрограммное) взаимодействие. Этот вид интеграции в общий комплекс ИСБ характерен в основном для компьютерных СТН.

Понимая возможность использования производимого оборудования в ИСБ не только собственной разработки, как мощного инструмента продвижения продукции на рынок, большинство производителей принимают меры для создания возможностей интеграции силами сторонних разработчиков. Последние при этом создают единую программу, реализующую все функции ИСБ и взаимодействующую (напрямую или через аппаратные и программные модули-преобразователи) с оборудованием подсистем. В отличие от предыдущей, в такой ИСБ, которую назовем аппаратно-программной (рис. 3), принятие решений и межсистемное взаимодействие происходит только в общей для всех подсистем программе, протоколирование – только в единой базе событий, контроль и управление – только через общий интерфейс. Работа с оборудованием (программная реализация протокола обмена) обеспечивается модулем, который называется драйвером.

Аппаратно-программная интеграция обеспечивает возможность оптимизации программного обеспечения с единых позиций, что позволяет создавать высокопроизводительные, устойчивые и надежные системы, упрощает оснащение их средствами защиты информации, уменьшает стоимость интегрирующей надстройки, особенно для ИСБ с большим числом рабочих мест операторов. С другой стороны, ИСБ по сравнению с аппаратно-интегрированной

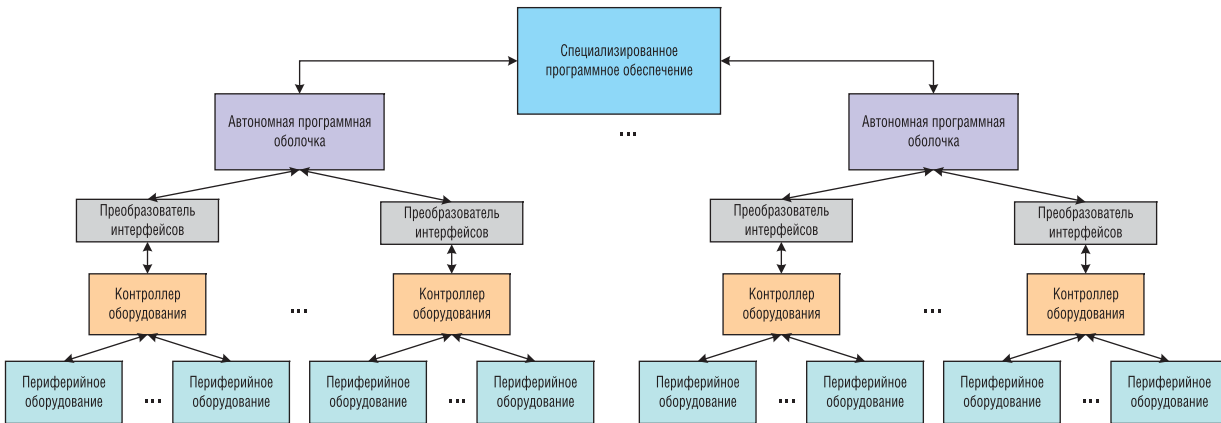


Рис. 2. Программно-интегрированная система

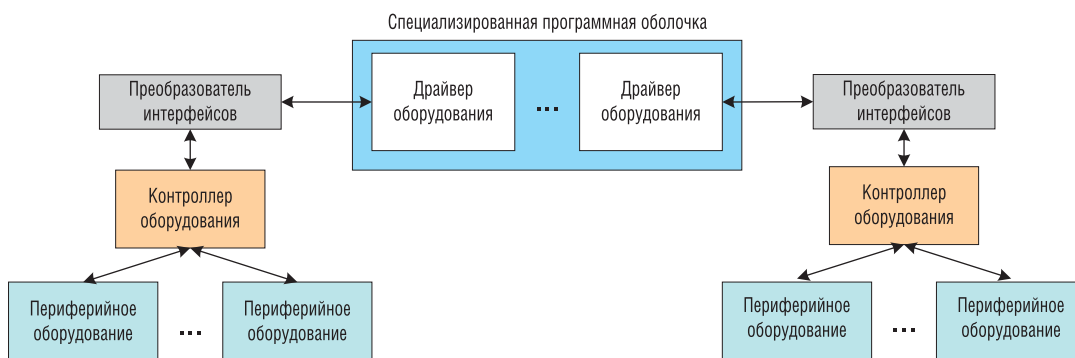


Рис. 3. Аппаратно-программная интегрированная система

системой приобретает необходимую гибкость. Появляется возможность оптимизации выбора аппаратуры для решения различных задач, развития действующих комплексов новейшими приборами без полной замены действующего оборудования. Существенным представляется сохранение автономной работоспособности подсистем при нарушениях в работе управляющей надстройки.

Учитывая привлекательную для пользователей открытость аппаратно-программных ИСБ, бурное развитие компьютерных и коммуникационных технологий и все возрастающую заинтересованность производителей оборудования в его продвижении в составе ИСБ, следует признать аппаратно-программную интеграцию наиболее перспективной технологией создания ИСБ. Необходимым условием реализации таких ИСБ является наличие у разработчика алгоритма управления оборудованием. Ряд производителей предоставляет низкоуровневый протокол взаимодействия подсистемы с управляющей компьютерной "надстройкой". При этом от разработчиков ИСБ требуется детальное владение алгоритмами и особенностями работы прибора.

Для облегчения работ производители оборудования передают на различных условиях так называемый Software Development Kit (SDK) разработчика – программный модуль, осуществляющий двухстороннее преобразование информации между уникальным аппаратным протоколом оборудования и формализованным и описанным внешним интерфейсом модуля. Система команд управления, доступная разработчику, упрощена, формализована и корректно описана. Обеспечивая полную реализацию функциональности прибора, SDK обычно ограничивает доступ к системным и служебным операциям, например, перепрограммированию внут-

реннего процессора прибора. В развитых зарубежных странах наличие SDK является важнейшим условием применимости оборудования, как средства защиты инвестиций от ущерба, связанного с быстрым моральным износом оборудования. По этому же пути идут передовые отечественные производители.

Авторы настоящей статьи представляют предприятие, почти десятилетие занятое разработкой и развитием аппаратно-программных ИСБ. Уместным представляется в качестве иллюстрации к сказанному рассмотреть некоторые особенности интеграции различного оборудования ОС и ПС.

Компания Notifier Italia на условиях конфиденциальности предоставила разработчикам с определенным статусом полный низкоуровневый протокол на свои ПКП АМ-2000/6000. Это позволило создать полностью адаптированный к российским условиям программный модуль, не только обеспечивший полнофункциональное включение ПКП в ИСБ, но и возможность одновременной совместной работы нескольких ПКП в составе комплекса крупного объекта.

Компания ESMI на тех же условиях предоставляет полнофункциональный низкоуровневый протокол, обеспечивающий мониторинг, управление и конфигурирование систем на основе ПКП серии ESA и MESA. Следует отметить наличие подробной документации, высокую надежность работы протокола: наличие механизмов гарантированной доставки сообщений, исключения случайного повтора команд, проверки наличия компьютера на линии связи и др. Контроллер MESA позволяет объединять в единую сеть несколько ПКП ESA, причем обмен данными между контроллерами внутри сети осуществляется по специальному закрытому протоколу. Протокол обеспечивает реализации функции

Аппаратно-программный комплекс

«БАСТИОН»

для создания открытых
интегрированных систем безопасности

Объединение в единый комплекс
подсистем безопасности

Охранно-пожарная сигнализация

Vista-50/50P/501/120/128BP/250BP (Honeywell Security)
«Сигнал-20» и система «Орион» («Болид»)
«Аккорд-512» («Аргус-Спектр»)
«Рубеж-08» («Сигма-ИС»)
ESA-1,2 (ESMI)
AM-2000/6000 (Notifier Italia)

Системы контроля и управления доступом

N-1000 (Nothern Computer)
Elsys («Электронные системы»)
Gate («Равелин ЛТД»)

Цифровые системы теленаблюдения

«ОТРА» («Электронные системы»)
CVS («Новые технологии»)
«Интеллект» (ИТУ)
PHOBOS (Vocord Telecom)
«Цербер» («СРС»)



Ассоциация
«ЭЛЕКТРОННЫЕ СИСТЕМЫ»
средства безопасности

Единые мониторинг, протоколирование и
управление, автоматические
взаимодействия подсистем

Более 500 инсталляций
от С.Петербурга до Владивостока



443011 г. Самара, ул. Советской Армии, 217
тел./факс (846) 927-99-00
E-mail: develop@elsystems.ru www.elsystems.ru

конфигурирования системы с использованием создаваемого интегратором приложения, но можно воспользоваться и бесплатно распространяемой производителем программой. Для ПС этот подход вполне допустим, поскольку переконфигурирование ПС осуществляется редко и, как правило, квалифицированным персоналом устанавливающей организации.

Интересен опыт интеграции оборудования ОС и ПС серии Vista, производимой компанией Honeywell Security (бывшая ADEMCO). Все ПКП линейки имеют два информационных порта – "принтерный" и "клавиатурный". При этом ни в один из портов, взятый отдельно, не поступает полная информация о работе системы, в штатных модулях обслуживания этих портов (4100SM и 4164E соответственно) отсутствует механизм гарантированной доставки команды, а их стоимость несоразмерно велика. По сути, на эти порты поступают не данные о состоянии системы и его изменениях, а лишь "верхушка" реализованного внутри ПКП протокола: нажатие управляющих клавиш и текстовые сообщения о событиях. Более того, нормальная работа ПКП обеспечивается лишь при определенных временных параметрах управляющего воздействия, что при использовании операционной системы Windows весьма затруднительно.

В этих условиях оказалась целесообразной разработка собственного контроллера, поддерживающего работу одновременно с обоими портами. Контроллер под управлением соответствующего драйвера играет роль всех восьми возможных в системе пультов управления и принтера, одновременно разгружая компьютер от выполнения задачи поддержки необходимого текущего обмена с системой. В результате удалось расширить возможности систем на основе ПКП Vista, в частности, подключить под единым управлением до 16 ПКП на один порт компьютера, реализовать выполнение макрокоманд, в частности, позововую постановку на охрану/снятие с охраны, фиксировать максимально полную информацию о событиях, в частности, фамилию оператора, производящего действия с системой.

При интеграции ПКП "Аккорд-512" помимо обслуживания предоставленного производителем протокола верхнего уровня пришлось принимать меры для компенсации известных недостатков внутрисистемного протокола ПКП. Программно задавая ряд "сверхплановых" команд установки и сброса, удалось существенно повысить устойчивость работы ПКП по сравнению с его автономной работой.

Без осложнений проведена интеграция ПКП "Рубеж-08" на основе переданного производителем SDK. Таким образом, приходится констатировать, что, несмотря на общую тенденцию к распространению аппаратно-программных ИСБ на основе открытой архитектуры, на рынке пока присутствует оборудование с принципиально разными возможностями и способами интеграции. Представляется целесообразным как с точки зрения мобилизации и концентрации ресурсов, так и с точки зрения получения максимальной прибыли разделение производителей на две группы – производителей оборудования и производителей систем. Мостом между ними мог бы стать стандарт на общие принципы построения SDK.

Доступность SDK позволила бы сосредоточить внимание и усилия разработчиков ИСБ на таких недостаточно проработанных направлениях, как оптимизация структур и информационных потоков в ИСБ, повышение защищенности, надежности и устойчивости работы, скорейшее внедрение новейших информационных и коммуникационных технологий в ИСБ, оптимизация взаимодействия "ИСБ-персонал", технико-экономической оптимизации структур ИСБ и др. Для производителей оборудования областью конкурентной борьбы стали бы надежность, функциональность оборудования, его технические характеристики, эффективность производства, а ИСБ стали бы мощным каналом продвижения лучших образцов на рынок. Вместе же эти тенденции привели бы к повышению уровня безопасности защищаемых объектов.

СЕМИНАР

2 февраля компания "ЛУИС+" провела очередной семинар "Тенденции развития комплексных систем безопасности". В работе форума приняли участие 280 представителей 206 компаний из 42 городов России и Белоруссии. По традиции, вниманию слушателей были представлены доклады о последних достижениях ведущих российских и зарубежных производителей:

- Системы телевизионного наблюдения производства PELCO - доклад представителя компании PELCO в России Федора Жидомирова
- Системы телевизионного наблюдения производства Geutebruck – доклад представителя компании Geutebruck в России Льва Даценко
- Цифровые технологии в системах телевизионного наблюдения – доклад ведущего технического эксперта компании "ЛУИС+" Максима Савельева
- Оборудование для систем противопожарной автоматики - доклад ведущего технического эксперта компании "ЛУИС+" Юрия Станкевича и директора компании "НПО Пожарная Автоматика Сервис" Евгения Чуйкова
- Построение систем оповещения на базе оборудования компании JEDIA – доклад технического эксперта компании "ЛУИС+" Дмитрия Атрошенко
- Электронные системы безопасности Honeywell

Security – доклад представителя компании Honeywell Security в России Михаила Николаева

- Системы защиты периметра SouthWest Microwave – доклад ведущего технического эксперта компании "ЛУИС+" Юрия Станкевича
 - Система контроля доступа Parsec – доклад генерального директора компании "РЕЛВЕСТ" Леонида Стасенко
 - Интегрированная система безопасности Бастион – доклад генерального директора компании "НИЦ ФОРС" Игоря Ракова
- Все выступления сопровождались презентациями и демонстрацией возможностей оборудования. По традиции, всем участникам форума была вручен полный комплект информационно-технических материалов компании.
- После напряженного рабочего дня слушатели семинара отставали честь компаний в турнире по боулингу.

Победителем турнира стал Александр Булатов, компания "ТСО", город Москва.
 Серебряным призером – Олег Голиков, компания "Мир безопасности", город Казань.
 Бронза – у Игоря Харюкова, директора компании "Диамант", город Москва.

