УДК 681.3.07

К.А. БОХАН[1], Н.С. КОВАЛЕНКО[2], Ю.В. КИЯЩЕНКО[1]

[1]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*
[2]*Бердянский государственный педагогический университет, Украина*

АНАЛИЗ И РАЗРАБОТКА АРХИТЕКТУРЫ ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЪЕКТОВ СО СЛОЖНОЙ ИНФРАСТРУКТУРОЙ

Рассмотрены принципы проектирования интегрированных систем объектовой безопасности. Проведен анализ существующих систем объектовой безопасности. Приводится архитектура ядра зонально-модульной интегрированной системы объектовой безопасности.

объектовая безопасность, масштабируемость, зонально-модульная архитектура, радиосети

Введение

Обеспечение безопасности крупных хозяйственных объектов – крайне сложная задача. Ее эффективная реализация требует учета большого количества аспектов. Руководители, призванные обеспечить устойчивое функционирование вверенных им предприятий, вынуждены нести новые расходы на увеличение штата службы безопасности, установку и эксплуатацию технических средств защиты, представляющих собой набор средств, обеспечивающих защиту от одной или нескольких угроз: охранная сигнализация, система видеонаблюдения, система пожарной сигнализации, система управления и контроля доступа и т.д.

Такой подход характеризуется высокими затратами и невысокой эффективностью, что, в первую очередь, связано с низкой управляемостью указанной системы объектовой безопасности (СОБ). Далее системы объектовой безопасности, построенные из отдельных технических средств защиты, будем называть комплексными системами объектовой безопасности (КСОБ).

Кроме низкой управляемости КСОБ характеризуется еще рядом недостатков, среди которых можно выделить следующее:

– требуется инсталляция и дальнейшая эксплуатация телекоммуникационной инфраструктуры для каждой из подсистем защиты, что приводит к значительным финансовым затратам и снижению надежности КСОБ в целом;

– отсутствуют единые системы визуализации информации о состоянии охраняемого объекта и управления техническими средствами защиты, что в значительной степени усложняет управление безопасностью охраняемого объекта;

– отсутствует единая система документирования информации о состоянии охраняемого объекта;

– интеграция сигналов от различных технических средств осуществляется в данном случае только оператором;

– обслуживающему персоналу необходимо изучать каждую подсистему в отдельности, что может значительно увеличить сложность эксплуатации системы в целом.

Решение указанных проблем заключается в построении интегрированных систем объектовой безопасности (ИСОБ), объединяющих различные подсистемы безопасности и представляющих собой автоматизированные системы управления объектовой безопасностью.

Под интегрированными системами объектовой безопасности будем понимать совокупность взаимосвязанных и обладающих технической, программной, информационной и эксплуатационной

совместимостью подсистем:

– тревожной, охранной и охранно-пожарной сигнализаций (ТС ОПС);

– контроля и управления доступом (КУД);

– обработки и визуализации информации об охраняемом объекте (ОВИ);

– управления составными частями ИСОБ (УСЧ).

Таким образом, основной отличительной чертой ИСОБ является наличие единой подсистемы визуализации информации об охраняемом объекте и подсистемы управления безопасностью объекта (рис. 1).

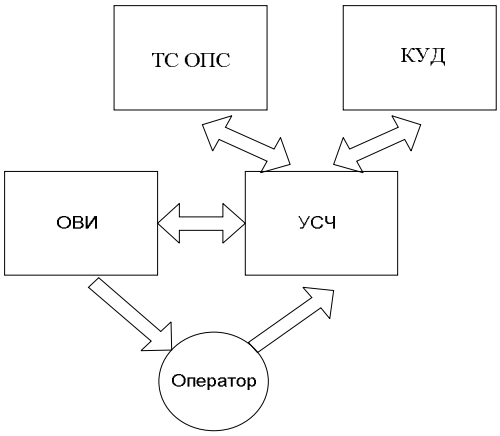

Рис. 1. Общая структурная схема ИСОБ

На сегодняшний день промышленностью предлагается множество различных ИСОБ. В качестве примера можно указать следующие:

– iSecure™Pro Simplex производства компании АРМО-Групп, которая построена на платформе Windows 2000 и MS-SQL [1]. Данная система позволяет интегрировать системы охранного телевидения, контроля доступа и охранно-пожарной сигнализации в единую и мощную сетевую систему управления безопасностью. Она имеет модульную расширяемую архитектуру, позволяет объединять сотни контроллеров iSecure, поддерживает тысячи считывателей карт (пропусков), точек доступа и других устройств;

– ДЕАН-ЭКСПРЕСС производства компании Деан [2], которая представляет интегрированную систему безопасности на основе аппаратной обработки видеосигнала;

– КОДОС производства компании НПК "СоюзСпецАвтоматика" [3], который обеспечивает: управление охранной сигнализацией, регистрацию видеоизображения на жесткий диск и оперативный просмотр архива, видеозапись и просмотр видеофрагментов происходящих в системе по тревожному сигналу системы охранной сигнализации, управление купольными поворотными камерами.

Анализ производимых промышленностью ИСОБ [1 – 3] показал, что они обладают либо ограниченной функциональностью, либо недостаточной масштабируемостью. Более того, в производимых системах не учитываются факторы, которые могут усложнить инсталляцию и эксплуатацию этих систем. К этим факторам можно отнести: сложную инфраструктуру, очень большие размеры охраняемых объектов и др. Так, сложная инфраструктура может привести к невозможности прокладки кабеля на определенных участках объекта.

Цель статьи – разработка архитектуры и принципов реализации ИСОБ.

Архитектура ядра модульно-зоновой системы объектовой безопасности

Как уже отмечалось выше, ИСОБ является сложной системой технических средств, требующей профессионального подхода при разработке, установке на объекте и эксплуатации. При этом у разработчика может быть два пути:

– разработка ИСОБ под требования определенного заказчика, что в последствии может вызвать необходимость заново выполнять все стадии проектирования для других заказчиков;

– разработка модульного ядра ИСОБ, с последующей его адаптацией под требования любого заказчика.

Под ядром ИСОБ будем понимать набор архитектурных решений, аппаратные и программные интерфейсы, протоколы обмена данными, аппаратные и программные средства, обеспечивающие базовую функциональность системы в целом.

Так как ядро системы не зависит или слабо зависит от требований заказчика, то оно должно соответствовать общим требования к ИСОБ, среди которых можно выделить:

– функциональность – возможность интеграции в единую систему произвольного количества функциональных модулей, что определяет функциональную масштабируемость системы;

– надежность – способность ИСОБ сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортирования;

– безопасность – защищенность ИСОБ от воздействия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способности ИСОБ выполнять предусмотренные функции без нанесения неприемлемого ущерба;

– масштабируемость – возможность ИСОБ обеспечить безопасность объектов произвольной площади от заданных видов угроз;

– оперативность – способность ИСОБ функционировать в реальном масштабе времени.

Соответствие указанным требованиям закладывается в проектируемую систему еще на этапе проработки архитектурных решений.

Рассмотрим вариант архитектуры ядра ИСОБ, удовлетворяющий выдвинутым общим требованиям.

Предлагаемая архитектура ИСОБ представляет собой масштабируемую модульную систему обеспечения объектовой безопасности, в которую интегрируются различные подсистемы – видеонаблюдения; аудиоконтроля; пожарной безопасности; контроля окружающей среды; контроля вторжений; другие подсистемы, необходимые заказчику.

При этом масштабируемость обеспечивается как по подсистемам (функциям), так и по площади покрытия. Такая масштабируемость обеспечивается модульно-зоновой архитектурой системы. Так, модули системы обеспечивают интеграцию в единую систему различных подсистем (см. выше), а зоновая архитектура обеспечивает масштабирование по площади покрытия.

На рис. 2 представлена общая структура предлагаемой системы.

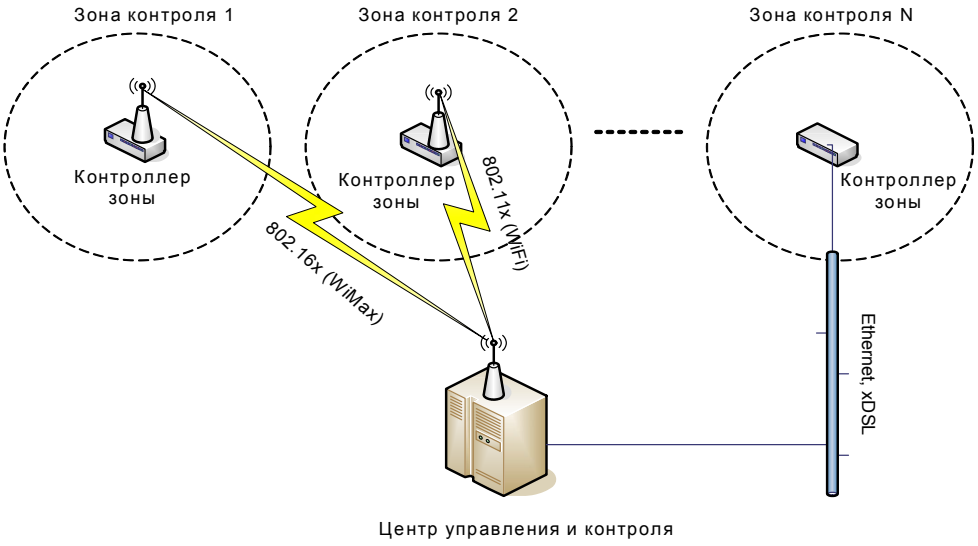

Рис. 2. Общая структура интегрированной системы объектовой безопасности

Вся площадь покрытия (охраняемый объект) разбивается на зоны контроля, в которых устанавливается необходимая номенклатура датчиков и контроллер зоны.

Такое разбиение позволит сформировать произвольное покрытие, как по площади, так и по геометрии. Архитектура зоны контроля представлена на рис. 3.

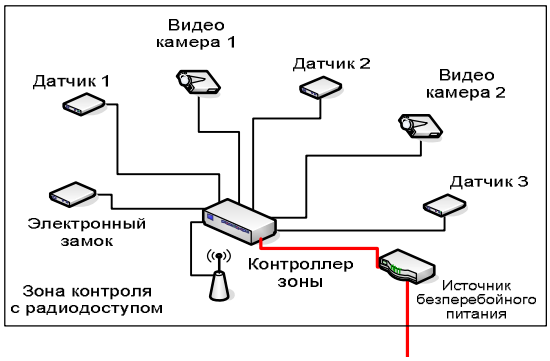

Рис. 3. Архитектура зоны контроля

Контроллер зоны предназначен для управления подконтрольными датчиками; контроля работоспособности аппаратуры своей зоны; ретрансляции данных с датчиков (видеокамер) или оповещение о срабатывании датчика; контроля доступа к аппаратуре своей зоны; других функций, определяемых из технического задания заказчика.

Техническая реализация контроллера зоны может быть выполнена на базе высокоинтегрированной платформы с низким энергопотреблением, которая не содержит механических частей (HDD, FDD и др.) и не требует активного охлаждения. Примером такой платформы может служить платформа EPIA производства фирмы VIA. Функционирование данной аппаратуры обеспечивается операционной системой Embedded Linux, которая загружается с Flash-drive. Удаленное управление данной подсистемой может быть реализовано посредством Web-интерфейса.

Указанная техническая реализация характеризуется высокой надежностью; наличием всех необходимых стандартных интерфейсов для подключения датчиков; низким энергопотреблением; высокой управляемостью; большой номенклатурой инструментальных средств по созданию управляющего программного обеспечения.

Информация, собранная контроллером зоны (КЗ), перенаправляется в центр управления и контроля (ЦУК) либо по радиосетям WLAN (WiMAX, WiFi), либо по кабельным сетям. При этом у WLAN есть много преимуществ:

– быстрое развертывание;

– возможность построения произвольной конфигурации;

– произвольная площадь покрытия;

– быстрая и легкая реконфигурация;

– слабая зависимость от наземной инфраструктуры (расположения зданий, коммуникаций и др.);

– высокая масштабируемость.

В случае использования радиосетей необходимо обеспечить должный уровень их безопасности. Для этого используются следующие подходы:

– ограничение количества абонентов WLAN в соответствии с количеством КЗ (обеспечивается оборудованием WLAN);

– запрет приема запросов на соединение с точкой доступа от абонентов, не входящих в список КЗ (обеспечивается оборудованием WLAN);

– авторизация абонентов WLAN на канальном уровне (обеспечивается оборудованием WLAN);

– использование VPN для доступа КЗ к ЦУК.

Центр управления и контроля предлагается реализовать на базе технологи HA-кластеров. Такой подход позволит:

– управлять производительностью вычислительной подсистемы в зависимости от

масштаба системы в целом;

– обеспечить высокий уровень готовности и надежности центра управления и контроля.

Серверное программное обеспечение следует реализовать на платформе J2EE, достоинство которой в следующем:

– прозрачное функционирование в кластерных системах;

– поддержка многоуровневых и многокомпонентных моделей программного обеспечения для данной платформы;

– легкая интеграция разрабатываемого ПО с практически любой СУБД;

– быстрое развертывание ПО;

– высокая безопасность ПО;

– легкость интеграции новых функциональных модулей в существующие приложения.

Важной особенностью данной платформы является возможность сборки программной среды из готовых модулей, хранящихся в репозитарии. Эта возможность позволяет создавать произвольные конфигурации серверного ПО с заданной функциональностью, которая определяет номенклатуру подсистем ИСОБ.

Реализация описанной архитектуры ядра ИСОБ обеспечит высокую масштабируемость и безопасность, а так же минимизирует время создания дополнительных функциональных модулей ИСОБ.

Определение требований к ИСОБ

Реализация готовой ИСОБ в соответствии с описанным выше подходом представляет собой сборку системы из готовых модулей в соответствии с требованиями заказчика и по результатам обследования объекта. При выборе эффективного, по соотношению затрат и качества, конфигурации объектовой ИСБ необходимо рассмотреть следующие основные вопросы:

– обследование объекта защиты;

– анализ угроз объекту;

– требования к решению по защите объекта и схема решения;

– применяемые технические средства;

– управление создаваемой системой и ее техническая эксплуатация;

– организационные вопросы создания и развертывания ИСБ.

При разработке системы ответы на данные вопросы образуют основу общей концепции безопасности объекта, защищаемого при помощи ИСОБ. Анализ общей концепции безопасности весьма полезен, так как позволяет оценить эффект от внедрения ИСОБ и достаточно точно для целей краткосрочного планирования (на 1 – 3 года) подсчитать затраты на ее развертывание.

Целью этапа обследования объекта защиты является получение актуальной и достоверной информации о текущем состоянии безопасности объекта: территории, капитальных сооружений (зданий), инженерной инфраструктуры (магистрали электро-, водо-, теплоснабжения и прочее) и др. Результатом этапа обследования обычно является характеристика (описание) объекта защиты – структурированная детальная информация, необходимая для проведения оценки состояния безопасности, разработки актуальной модели угроз для объекта, эскиза эталонного решения по защите объекта и рекомендаций по изменению или дополнению действующей политики безопасности и частных решений по защите объекта.

Типичный перечень возможных угроз представлен на рис. 4.

Целями и задачами проведения анализа уязвимости являются:

– определения важных для жизнедеятельности объекта предметов защиты (наиболее вероятных целей злоумышленных акций нарушителей);

– определение возможных угроз и моделей вероятных исполнителей угроз (нарушителей);

– оценка возможного ущерба от реализации прогнозируемых угроз безопасности;

– оценка уязвимости объекта и существующей системы безопасности;

– разработка общих рекомендаций по обеспечению безопасности объекта (выполняется в одном экземпляре для заказчика, причем доступ имеет узкий круг лиц).

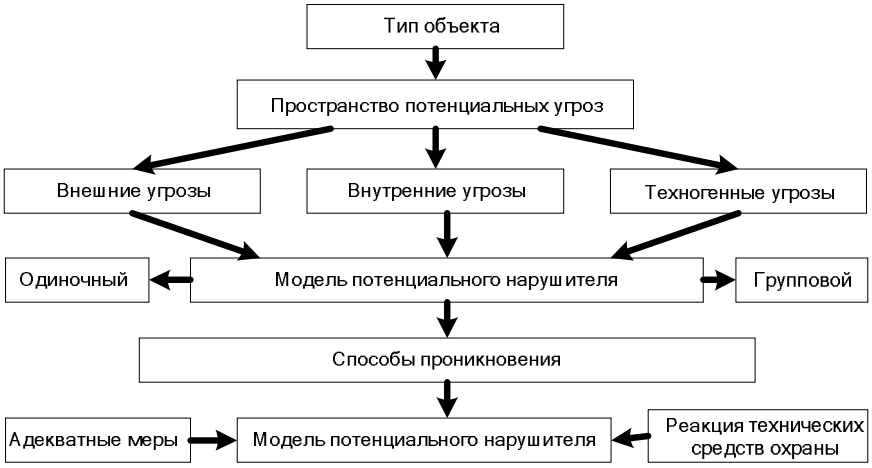

Рис. 4. Структурная схема анализа угроз

Требования к решению по защите объекта выдвигаются в результате сопоставления основных свойств защищаемого объекта с составленной на предыдущем этапе моделью угроз.

Заключение

Теоретическое рассмотрение вопроса проектирования конкретной ИСОБ в общем случае бесполезно, потому что ИСОБ, собираемая из унифицированных функциональных и аппаратных модулей, в готовом виде достаточно жестко индивидуально привязывается к объекту.

Следовательно, свойства объекта практически полностью определяют конечный вид оптимальной для него ИСОБ – как состав аппаратной части (количество зон контроля, номенклатура датчиков для каждой зоны и т.д.), так и состав модулей программной части (модули, обслуживающие ту или иную подсистему).

Проблема гибкости системы, возможности оперативного варьирования конфигурацией, поэтапное ее развитие при сохранении заданных показателей является актуальной и требует дальнейшего анализа. Создание надежной автоматизированной охранной системы, основанной на сочетании перспективных промышленных устройств и современных информационных технологий, позволит повысить безопасность охраняемых объектов.

Литература

1. Барсуков В. Радиомониторинг безопасности. Отечественная система радиосигнализации ОСПАС // Электроника: Наука, Технология, Бизнес. – М.: ЗАО “РИЦ “ТЕХНОСФЕРА”. – 2000. – № 1. – С. 32-36.

2. Беседин Д. О проектировании систем безопасности современного технического уровня // JetInfo. – М.: Джет Инфо Паблишер. – 2005. – № 6 (145). – С. 25-45.

3. Лысый В.М. Интегрированные системы физической защиты // Системы безопасности, связи и телекоммуникаций. – 1999. – № 29. – С. 16-32.

Поступила в редакцию 3.03.2006

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.