УДК 007.5

МЕТОДЫ ИНТЕГРАЦИИ И ВЗАИМОДЕЙСТВИЯ ПОДСИСТЕМ В КОМПЛЕКСНОЙ ИНТЕГРИРОВАННОЙ СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Асс. Перевощиков В.А.

Белорусский государственный университет информатики и радиоэлектроники

Комплексная система безопасности – это совокупность функциональных и информационных связанных друг с другом подсистем безопасности, работающих по одному алгоритму и имеющих общие каналы связи, программное обеспечение, базы данных.

При реализации систем безопасности крупных объектов обязательным требованием стала интеграция подсистем между собой с помощью программного обеспечения. Каждая конкретная КСБ может изменяться: некоторые подсистемы могут быть исключены или заменены новыми.

Основные признаки комплексной системы безопасности.

1. Единая система сбора, обработки и представления данных, мониторинга и управления всеми подсистемами.

2. Возможность задать требуемые сценарии действий любой сложности в ответ на различные события в системе. Под событием в системе понимается все, что происходит в системе: обнаружение движения подсистемой видеоконтроля, тревога датчиков охранно-пожарной сигнализации, факт прохода через двери, контролируемые подсистемой контроля доступа и т.п. Действием является все, что можно сделать в системе: включить камеру на запись, выдать предупреждение оператору, включить тревожную сигнализацию, поставить/снять датчики с охраны, запретить проход по всем дверям и т.д. В ответ на событие или некий набор событий можно определить любой набор действий системы – сценарий. Более того, применяя специальный язык сценариев, можно определить сколь угодно сложную реакцию системы на события.

3. Возможность интеграции любого оборудования и подсистемы, независимо от типа устройств и производителя. Интеграция осуществляется за счет протоколов обмена, программ-драйверов, контроллеров.

4. Модульность и открытые интерфейсы. Система может быть легко расширена как за счет включения новых модулей, так и за счет интеграции системы с уже существующими компьютеризированными системами предприятия. Дополнительные модули могут быть разработаны производителями системы безопасности.

5. Масштабируемость – отсутствие ограничений на масштаб охраняемого объекта и возможность подключения любого количества рабочих мест.

6. Многоуровневая (иерархическая) структура системы позволяет рационально распределить потоки информации между подразделениями предприятия и тем самым минимизировать объем передаваемых данных. Каждое подразделение получает только те сообщения, которые соответствуют служебным обязанностям и уровню ответственности. Тревожное сообщение может быть передано на следующий уровень системы только в том случае, если по истечении допустимого времени отсутствует реакция ответственного персонала.

Выделяют три основных типа интеграции подсистем в комплексной системе обеспечения безопасности.

1. Аппаратная интеграция. Представляет собой взаимодействие подсистем на уровне приборов, обычно без использования программного обеспечения. В простейшем случае, взаимодействие на аппаратном уровне осуществляется через релейные выходы: реле прибора одной подсистемы воздействует на входы датчиков прибора другой. Например, при срабатывании системы пожарной сигнализации, на приёмно-контрольном приборе срабатывает специально настроенное реле, замыкающее, либо размыкающее контакты на линии пожарной сигнализации контроллера доступа, который, в свою очередь, переходит в режим пожарной тревоги и открывает свободный проход.

2. Программная интеграция. Представляет собой взаимодействие программных обеспечений подсистем безопасности между собой. Способ программной интеграции применяется в случаях, когда интегрировать системы на аппаратном уровне либо неоправданно сложно, либо нецелесообразно. Как правило, таким путём интегрируются СКУД и системы видеонаблюдения. Взаимодействие подсистем между собой происходит по протоколу TCP/IP посредством локальной сети.

3. Аппаратно-программная интеграция. Представляет собой смешанный случай, когда аппаратное обеспечение одной подсистемы управляется из программного обеспечения другой. Так обычно интегрируются системы видеонаблюдения либо СКУД с системой ОПС. Взаимодействие осуществляется по линиям интерфейсов, используя стандартные протоколы (TCP/IP, Modbus и др.). В этом случае, требуются специальные устройства, объединяющие подсистемы – преобразователи интерфейсов, переходники и др. Пример: интеграция СКУД Сфинкс и ОПС Bolid (рисунок 1). Для интеграции применяется преобразователь интерфейсов Sphinx-Bolid, который позволяет управлять сетью приборов ОПС из интерфейса программного обеспечения СКУД Сфинкс.

Наиболее распространённый вариант интеграционных связей, объединяющих подсистемы обеспечения безопасности следующий.

Системы пожарной автоматики объединяются между собой только при помощи аппаратной интеграции как одной из самых простых и надёжных. Реализуется следующий сценарий: срабатывает система

пожарной сигнализации. От приёмо-контрольного прибора поступает сигнал на прибор системы оповещения и управления эвакуацией, где срабатывает программа эвакуационного оповещения. Включается звуковое сопровождение и объявление о пожаре через громкоговорители системы оповещения. Таким же образом поступает сигнал на пульт МЧС при помощи системы тревожных сообщений по GSM каналу или телефонии. Далее, происходит активация системы дымоудаления, также получившей сигнал от системы пожарной сигнализации. Спустя время, необходимое для эвакуации персонала и рассчитанное на стадии пусконаладочных работ системы, активируется система пожаротушения. В случае спринклерной системы пожаротушения, вода начинает поступать сразу же после разбития колбы с термочувствительным раствором на самом спринклере. После отработки всех систем и ликвидации возгорания, системы пожарной автоматики требуется выключать вручную.

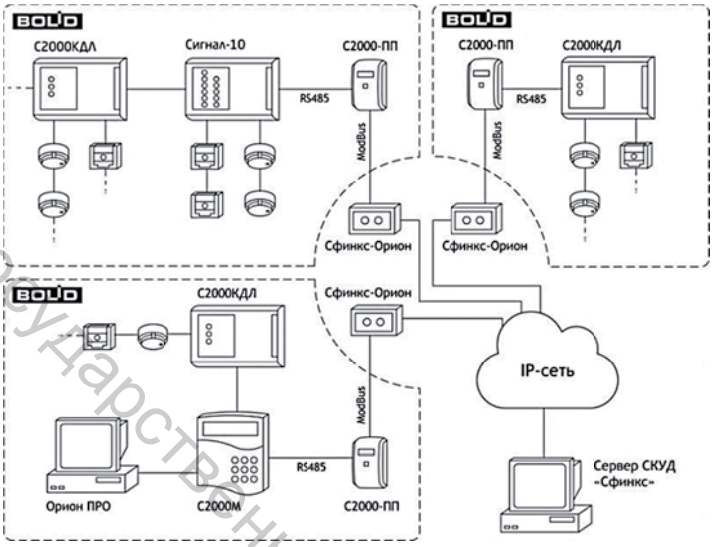

Рисунок 1 – Аппаратно-программная интеграция СКУД «Сфинкс» и ОПС «Bolid»

Помимо интеграции систем пожарной автоматики между собой, требуется обеспечить взаимодействие как минимум с системой контроля и управления доступом. Для этого сигнал от системы пожарной сигнализации поступает на контроллеры или сервер системы контроля и управления доступом, которая открывает точки доступа в свободный режим прохода для обеспечения быстрой эвакуации персонала. В данном случае также целесообразно использовать аппаратную интеграцию на уровне реле из-за высокой надёжности и простоты. При приходе сигнала пожарной тревоги на сервер системы контроля и управления доступом, создаётся событие и тревоге, передаваемое в систему видеонаблюдения при помощи связей программной интеграции, которая способна выполнить следующие действия:

1. Используя поступающее изображение с камер наблюдения, оценить его на наличие огня и дыма и вывести данные камеры на весь экран службе охраны, также при этом начать постоянную запись событий.
2. Вывести на экран видеоизображения эвакуационных путей и выходов для возможности управления СОУЭ при использовании СО-4 и СО-5 и начать постоянную запись сигнала с этих видеокамер.
3. Выводить изображение с ассоциированной видеокамеры при вызове с панели обратной связи СОУЭ.
4. Включить постоянную запись с видеокамер, установленных в особо охраняемых помещениях для регистрации возможных действий злоумышленников в сложившейся суматохе.

В другом сценарии, при срабатывании системы охранной сигнализации, может быть произведены следующие действия:

1. Сигнал о срабатывании охранной сигнализации передаётся на пульт централизованного наблюдения департамента охраны и происходит выезд оперативной группы.
2. Система контроля и управления доступом блокирует точки доступа, ведущие в помещение, где сработала сигнализация с возможностью открытия ответственным охранником.
3. Система видеонаблюдения переводит видеокамеры в режим постоянной записи на всех коридорах и самом помещении, где произошло срабатывание сигнализации и выводит изображение с этих видеокамер на монитор.

Выполнение подобных сценариев с использованием различных методов интеграции позволяет повысить эффективность совокупную эффективность систем обеспечения безопасности.

Список использованных источников

1. Системы безопасности и мониторинга – Интегрированные системы безопасности [Электронный ресурс]. – Режим доступа http: // rovalant.com/systems/integrated-systems.html
2. «Хранитель» – медиапортал о безопасности – Тенденции развития программного обеспечения интегрированных систем безопаности [Электронный ресурс]. – Режим доступа http://www.psj.ru/saver_magazins/detail.php?ID=67135
3. Интеграция СКУД «Сфинкс» с ИСО «Орион» [Электронный ресурс]. – Режим доступа http://spnx.ru/int_bolid.php