Доклад

Проводные и беспроводные  
 ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ.

Выполнил: Шишкин В. В

2014 г.

Интегрированные системы безопасности.

В последнее время получили развитие интегрированные системы безопасности (ИСБ), Сочетающие в себе частично или полностью систем предупреждения (информирования ) и активного противодействия, например: автоматическая охранно-пожарная сигнализация с системой пожаротушения, объединённая с системой видеонаблюдения.

**Интеграция** — качественно новый скачок в построении систем безопасности и управления объектом. Основное достоинство заключается в том, что все подсистемы взаимосвязаны, и в ответ на событие в одной подсистеме происходит соответствующее действие в другой. Можно задать требуемые сценарии реакции любой сложности на различные события. При этом нет никаких ограничений на описание логики взаимодействия - все, что может потребоваться на конкретном объекте, можно описать средствами интегрированной системы безопасности.

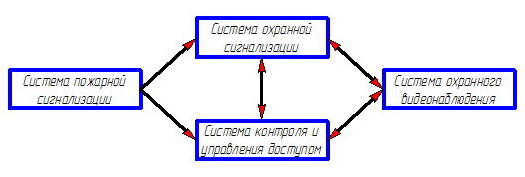
Система представляет собой управляющую среду, объединяющую все подсистемы безопасности в масштабе объекта (от загородного дома до крупного предприятия). Позволяет интегрировать работу следующих модулей:

* цифрового видеонаблюдения;
* охранно-пожарной сигнализации;
* контроля и управления доступом;
* жизнеобеспечения объекта;
* подсистемы безопасности производственных процессов

***Аппаратная интеграция***

Данный тип интеграции объединяет все системы безопасности исключительно с помощью аппаратного обеспечения каждой из систем без использования компьютеров управления и внешнего программного обеспечения.

Классическим примером данного типа интеграции является объединение систем посредством релейных контактов (рис. 1)



*Рис.1 - Аппаратная интеграция*

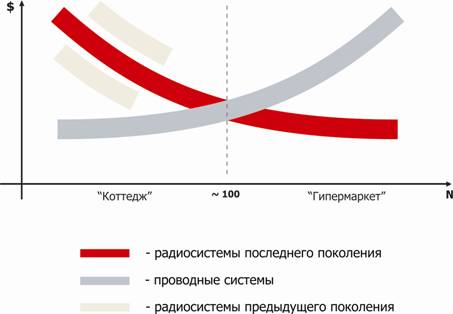
Этот способ интеграции реализуется за счет применения программируемых релейных контактов для передачи информационных сообщений между отдельными системами безопасности. Это старый добрый способ интеграции, через который 10–15 лет назад прошло большинство фирм, предлагавших своим заказчикам интегрированные системы безопасности.

Достоинством релейной интеграции является простота и надежность используемого для интеграции оборудования, невысокая стоимость и возможность объединения всех четырех систем безопасности, причем зачастую самых различных производителей.

Недостатков больше. Во-первых, данный способ интеграции не может обеспечить передачу большого количества сигналов о различных событиях между системами. Раньше было достаточно передать от одной системы к другой только тревожный сигнал – иными словами, внештатное событие. Как следствие, соседние системы реагировали только на тревоги друг друга. Сейчас в дополнение к этому необходимо передавать между системами целое множество штатных сообщений – например, сообщение о постановке области на охрану, считывание определенной карты доступа и т.п. Увеличение объема передаваемой между системами информации привело к появлению новых функций – например, к постановке области на охрану по считывателю системы контроля доступа и к автоматическому переводу соответствующего детектора движения в системе видеонаблюдения в рабочий режим. Если при этом еще и синхронизировать базы данных отдельных систем, то оператор ИСБ получает возможность автоматизировать процесс поиска интересующих его событий в одной системе по событию в другой. Например, получить в автоматическом режиме изображение человека, приложившего карту доступа к определенному считывателю.

Во-вторых, сегодня мы уже не представляем себе ИСБ без отображения информации о состоянии систем на графических планах объекта и без управления ресурсами систем по этим планам. А релейная интеграция не позволяет реализовать данную функцию.

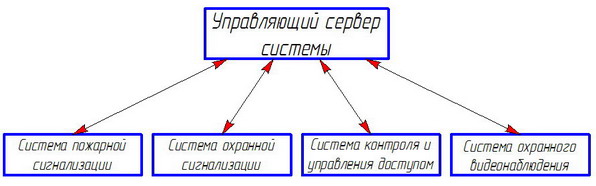
В-третьих, внесение изменений в релейную интеграцию на этапе эксплуатации – это достаточно трудоемкий и недешевый процесс. Ведь каждая логическая связь представляет собой релейный контакт и линию связи между системами. Поэтому любое изменение приводит к необходимости проведения монтажных работ и перепрограммирования.

В-четвертых, при использовании релейной интеграции на крупных объектах с большим количеством связей между системами (начиная с 200–300) утверждение о дешевизне и надежности данного способа интеграции перестает быть абсолютно верным. Проблема заключается в том, что по мере роста количества реле и линий связи суммарная стоимость релейной интеграции может превысить стоимость интеграции другого типа. Надежность релейной интеграции, в свою очередь, заметно падает с ростом количества связей из-за большого числа дополнительных соединений.

*Рис 2. Зависимость цены ИСБ от ее размера*

Для полноты описания аппаратной интеграции следует отметить, что большинство ИСБ последующих типов интеграции от разных производителей могут быть превращены в аппаратную интеграцию релейного типа, если убрать компьютеры управления и использовать имеющиеся в составе оборудования программируемые выходные и входные модули. Ближе всего к аппаратной интеграции стоят ИСБ с программно-аппаратной интеграцией, о которых будет рассказано ниже. В ИСБ этого типа достаточно обеспечить релейное управление системой видеонаблюдения (вместо имеющегося программного способа), чтобы получить полностью ап-паратно-реализованную ИСБ.

***Программная интеграция***

Программная интеграция систем безопасности обеспечивается за счет специализированного программного обеспечения (далее ПО), устанавливаемого на компьютере управления системами (рис. 2).

*Рис.3 - Программная интеграция*

ИСБ данного типа имеет два способа построения. Первый способ состоит в применении специально разработанного ПО, которое объединяет все системы безопасности. Второй способ предусматривает использование в качестве интегрирующего ПО программную оболочку одной из систем безопасности - чаще всего системы контроля доступа.

ИСБ со специализированным ПО

К данному классу интегрированных систем относятся комплексы, в которых взаимодействие между отдельными системами безопасности реализуется с помощью специально разработанного для этих целей внешнего программного обеспечения.

Взаимодействие между интегрирующим ПО и каждой из систем осуществляется за счет наличия программного интерфейса, который в каждом конкретном случае может быть реализован по-разному. Аппаратно взаимодействие реализовано между сервером ИСБ и центральным устройством или компьютером управления каждой из систем. В результате сервер с установленным на нем специализированным ПО является управляющим центром всего комплекса и все логические взаимосвязи между системами программно реализованы на сервере.

Достоинством данной ИСБ является возможность организации глубокого обмена информацией между отдельными системами, входящими в комплекс. То есть между системами передается не только тревожная информация, но и множество сообщений о штатных событиях в каждой из них. Это позволяет строить современные ИСБ с серьезной интеграцией между системами, с организацией автоматизированных алгоритмов реакции на события, с синхронизацией баз данных и автоматизацией поиска нужных событий в одной системе при известных входных событиях в другой.

Еще одно преимущество данного способа интеграции состоит в наличии удобного рабочего места оператора, на котором с привязкой к графическим планам объекта отображается состояние систем безопасности. Оператор также может управлять системами по графическим планам объекта, что сильно облегчает его работу и уменьшает время реакции и принятия решений. На дисплее автоматизированного рабочего места (далее АРМ) оператору могут выдаваться инструкции, соответствующие сложившейся на объекте ситуации.

Построение ИСБ данного типа требует меньшего количества линий связи между системами, по сравнению с ИСБ релейного типа, так как для интеграции каждой системы обычно нужен всего один кабель. Внесение изменений в логику работы ИСБ производится только перепрограммированием интеграционных настроек и не приводит к выполнению монтажных работ. В целом данный тип ИСБ представляет собой более удобный в эксплуатации комплекс по сравнению с аппаратной ИСБ.

В качестве примеров ИСБ со специализированным ПО можно назвать оборудование и Последующих фирм: Bosch (ПО BIS), Siemens (ПО ММ8000 и ТО-PSIS), Терна" (ПО "Комплекс 2000") и др.

Необходимо отметить, что существует отличие между приведенными примерами ИСБ со специализированным ПО, которое определенным образом влияет на характеристики комплекса. Это отличие отражает различные подходы фирм к созданию специализированного ПО. ПО фирм Bosch и Siemens разрабатывалось ими под свое собственное оборудование и не позволяет работать с оборудованием других производителей. ПО фирмы "Терна" разрабатывалось как открытая программная оболочка с возможностью подключения оборудования различных производителей, которые предоставляют программные драйверы для интеграции. Плюс создания открытого ПО состоит в возможности достаточно легкого включения в состав ИСБ оборудования новых производителей, что позволяет применять его на большем количестве объектов и легче подстраиваться под требования заказчиков по использованию различного оборудования. Минус открытого ПО заключается втом, что разработчики ПО и оборудования работают в разных фирмах и поэтому зачастую не могут получить более глубокую информацию, чем это необходимо с точки зрения производителей оборудования, а также не могут влиять на техническую политику производителей, что может сказаться на уровне и глубине интеграции. Принадлежность разработчиков ПО и оборудования к разным фирмам также будет негативно сказываться на скорости исправления ошибок и внесении новых функций в ИСБ.

Еще одной особенностью открытого ПО является то, что его разработчики очень часто в качестве основы для его создания используют уже готовые программные оболочки - в первую очередь, компьютерные базы данных. Однако большинство компьютерных баз данных не ориентировано для работы в системах безопасности. Поэтому то, что допустимо для обычных вычислительных целей (например, задержка в несколько секунд), совершенно неприемлемо для систем безопасности, так как после 3-5 секунд часто уже невозможно получить нужную информацию. Например, при получении тревоги от системы охранной сигнализации часто нужно немедленно получить изображение тревожной зоны на экране монитора. После 3 секунд в этой зоне можно ничего и не увидеть. Для преодоления данной проблемы в ИСБ, созданной на основе программной оболочки базы данных, применяют высокопроизводительные компьютеры, но это не всегда полностью решает проблему, а лишь приводит к заметному удорожанию ИСБ.

ИСБ с системным ПО

ИСБ с программной интеграцией, в которой роль интегрирующей программной оболочки выполняет ПО одной из входящих в комплекс систем, называется ИСБ с системным программным обеспечением.

В качестве интегрирующего ПО в таких ИСБ в настоящее время часто используется программная оболочка системы контроля и управления доступом (далее СКУД). Как правило, такая СКУД представляет собой мощную и высокопроизводительную систему, в которую уже интегрирована система охранной сигнализации Объединение системы охранной сигнализации и СКУД реализуется за счет подключения к обычному контроллеру доступа специализированных плат для подсоединения шлейфов охранной сигнализации. В качестве устройств постановки/снятия с охраны используются считыватели различных видов, а также ряд других устройств. В результате получается интеграция весьма приличного уровня между двумя системами ИСБ. Остальные системы безопасности объединяются в комплекс программным способом, как и в случае ИСБ со специализированным ПО.

Характеристики ИСБ данного типа очень похожи на характеристики ИСБ предыдущего. Существенным отличием является только то, что ИСБ с системным ПО уже имеет программную оболочку, реализованную на основе ПО системы контроля доступа. С одной стороны, это означает, что уже существует работоспособное ПО для создания ИСБ. С другой - ПО системы доступа при серьезной нагрузке дополнительными функциями и потоками данных может оказаться не в состоянии нормально функционировать, так как оно изначально не разрабатывалось для создания ИСБ.

Следует отметить, что системы охранной сигнализации, построенные на оборудовании систем контроля доступа большинства производителей, вынужденно используют компьютер управления для реализации логики своей работы Это ухудшает надежностные характеристики системы охранной сигнализации, а также ее быстродействие. Для преодоления этой проблемы приходится устанавливать дополнительное количество высокоскоростных компьютеров, что приводит к значительному удорожанию системы и не всегда позволяет полностью решить проблему.

Примерами ИСБ с системным ПО является оборудование Apollo (ПО Apacs), Siemens (СКУД Sipass) и др.

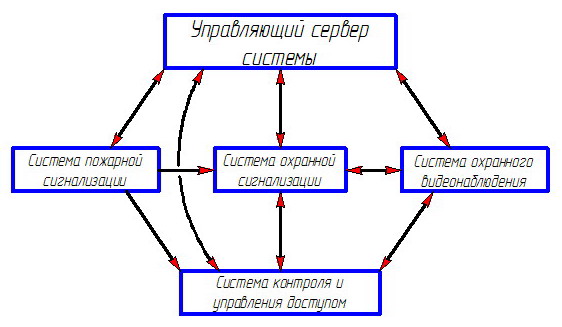
Надежность ИСБ программного типа определяется в первую очередь надежностью компьютеров управления и ПО. Выход из строя любого из этих компонентов полностью парализует работу ИСБ. Поэтому повышение их надежности для программной ИСБ представляет собой первоочередную задачу.

Обычный персональный компьютер нельзя рассматривать как высоконадежное устройство для создания систем безопасности, предназначенных для непрерывной круглосуточной работы. Поэтому строить крупные ИСБ на базе обычного компьютера не вполне разумное решение. При создании ИСБ следует использовать компьютеры, обладающие более высокой надежностью, собранные на качественных комплектующих промышленного типа. Более радикальный способ повышения надежности компьютерной части ИСБ - установка второго сервера ИСБ, работающего в "горячем резерве". В крупной ИСБ обычно работают несколько компьютеров, связанных между собой сетью Ethernet, поэтому необходимо повышать надежность не только самих компьютеров, но и компонентов и линий связи сети Ethernet. Необходимо также не забывать обеспечивать компьютеры и активные компоненты сети Ethernet бесперебойным электроснабжением.

Гораздо сложнее дело обстоит с надежностью ПО. К сожалению, в настоящее время в России не существует сертификации ПО, но имеется большое количество фирм, рекламирующих свое ПО для создания ИСБ. Сложившаяся ситуация приводит к тому, что при выборе ИСБ программного типа, основной частью которого является ПО, заказчик не может быть уверен в нормальной работоспособности всего комплекса в целом. В такой ситуации наиболее разумным решением представляется выбор ПО известных, долго существующих и хорошо зарекомендовавших себя фирм. Еще лучшим решением является посещение объектов, близких по размерам и характеристикам, где имеется ИСБ, которую заказчик планирует установить на своем объекте.

*Программно-аппаратная интеграция*

ИСБ с программно-аппаратной интеграцией называется комплекс, в котором не менее трех систем объединены аппаратно и существует компьютер с ПО, обеспечивающий дополнительный обмен информацией между системами, управление ими и сервисные функции.

Во всех наиболее известных ИСБ данного типа аппаратная интеграция осуществляется между системами пожарной, охранной сигнализации и контроля доступа (рис. 3).

*Рис.4 - Программно-аппаратная интеграция*

Аппаратное объединение систем реализуется не с помощью релейных контактов, а за счет интеграции систем, предусмотренной еще на этапе разработки оборудования каждой системы и/или за счет использования высокоинтеллектуального оборудования, которое может обмениваться информацией и принимать решения самостоятельно, без компьютера управления Система видеонаблюдения объединяется в комплекс на программном уровне через компьютер управления или с помощью релейных контактов.

ИСБ с программно-аппаратной интеграцией в целом имеют те же достоинства и функциональные характеристики, что и ИСБ с программной интеграцией. Но при этом надежность данной ИСБ выше, так как в случае выхода из строя компьютера управления или сбоя в работе ПО комплекс не распадется на отдельные системы, и интеграция сохранится как минимум между тремя системами безопасности. Благодаря наиболее высокой надежности среди всех типов интегрированных систем и наличию развитых функциональных характеристик ИСБ с программно-аппаратной интеграцией целесообразно применять на крупных объектах и на объектах с повышенными требованиями к безопасности.

Интегрированные системы бывают проводные и беспроводные. Проведем небольшое сравнение проводных, GSM и профессиональных радиоканальных систем передачи сообщений.   
Существует три основных технических решения организации системы охраны и мониторинга стационарных объектов, распределенных на большой площади:

*Беспроводные охранные системы*   
Наиболее критичной для беспроводных охранных систем является дальность действия и длительность автономной работы. Дальность может достигать 100 м., автономная работа – до трех лет. Обычные же батареи работают в среднем около 6 месяцев. На приборах, работающих от автономного питания устанавливаются индикаторы заряда батарей, сигнализирующие в случае разряда. Более продвинутые системы отправляют сообщения, какие батареи и когда необходимо заменить. (*ИСБ Стрелец-Интеграл.; Visonic - серия PowerG™ (PowerMaster);Беспроводные системы наблюдения – LightInTheBox;ELDES EPIR охранная беспроводная GSM сигнализация;Pyronix Enforcer WE;WisDom*)

1. Профессиональные радиоканальные системы (доставка сообщений по радиоканалу)   
*Достоинства:*

* независимость от наличия телефонных линий или GSM-связи;
* высокая информативность и криптостойкость (защитные свойства);
* большое количество предложений профессионального оборудования и программного обеспечения на рынке;
* Высокая надёжность доставки сообщения;

*Недостатки:*

* необходимость получения частот и регистрация передатчиков в Главном радиочастотном центре Министерства связи РФ;
* для обслуживания больших территорий необходима установка ретрансляторов;
* отсутствие единых стандартов передачи данных;

2. GSM-системы (доставка сообщений по GSM-связи)  
*Достоинства:*

* простота в тестировании и установке;
* большая зона охвата;

*Недостатки:*

* доступность аппаратуры подавления ( «глушилка» GSM 900-1800 МГц – от 100 $);
* платная эксплуатация (абонентская плата, оплата сеансов связи);
* наличие эффекта «праздника», когда сеть перегружена, и сигнал не проходит (Новый год);
* низкая частота тест-сигналов (максимум 2 раза в сутки);
* отсутствие единых стандартов передачи данных, низкая способность к интеграции и высокая стоимость объектового оборудования;
* охраняемые объекты должны находиться в зоне покрытия операторов сотовой связи;
* обычно высокая стоимость, значительно выше, чем проводных систем;
* они требуют постоянной оплаты трафика радиоканал;
* их надежность сильно зависит от состояния сети GSM операторов;
* беспроводные системы реагируют на воздействие радиопомех.

3. Проводные системы  (доставка сообщений по телефонным линиям)

Проводные охранные системы   
Проводная сигнализация стоит в два – три раза дешевле беспроводных систем охранной сигнализации. У проводных систем нет ограничений по отдаленности датчиков от блока приёмо-контрольного прибора (ППК). Особенно это важно для частных домов, у которых больше, чем один этаж. (*Интегрированная система охраны**"Орион" ; КОДОС; Paradox Digiplex /EVO ; ADEMCO; Интегрированные системы безопасности серии «Рубеж»; Интегрированная система охраны ИСО 777*)  
  
*Достоинства:*

* для «взлома» объекта необходим доступ к аппаратуре объекта, пульта или телефонной линии;
* высокая информативность;
* поддержка международных стандартов передачи данных, способность к глубокой интеграции, большой спектр объектового оборудования (пульт и объектовое оборудование могут быть разных производителей);
* более уверенный сигнал, чем сигнал по радиоканалу из-за отсутствия помех
* не надо менять батареи питания – системы работают от основного электроснабжения, дополнительное бесперебойное питание, которое может быть во включенном состоянии 7-10 суток, используется только в случае отсутствия напряжения в сети. Также предусмотрена рассылка тревожных сообщений в случае потери напряжения.

*Недостатки:*

* необходимо много входных телефонных линий на Центральной станции и наличие проводных телефонных линий на объектах;
* неустойчивость работы и ложные тревоги по телефонным линиям устаревших АТС;
* отсутствие контроля линий связи (если не установить специальное оборудование на АТС);
* возможные сбои в работе факса и internet;
* разработаны технологии подавления и взлома систем по телефонной линии.
* Сигнал передаётся по телефонному кабелю, плохое состояние которого уменьшает надёжность передачи;
* Провода можно найти и повредить;
* Длительное время восстановления работоспособности системы – до 2 суток. Если Вы решили установить охранную сигнализацию на постоянной основе, то для проводных систем лучше всего это сделать во время ремонта. Можно спрятать провода , чтобы они не привлекали внимание посторонних. Если же ремонт Вы уже сделали, стоит подумать о приобретении беспроводных систем охраны.

Таким образом, при выборе системы безопасности стоит обратить внимание на следующие моменты:   
Радио или GSM-каналы  — наилучший выбор при ограниченном количестве свободных телефонных номеров на объекте.  
Радио и GSM-каналы  — имеют наибольшую зону действия (а значит – и возможность применения), по сравнению с проводными.  
GSM-связь – легче всего заглушить и тем самым отключить с целью проникновения.  
Проводная и GSM-связь – наиболее проста в установке.  
Радиоканал – наиболее надежен для передачи сигнала.  
Проводная и радиоканальная передача – обладают наибольшей информативностью (способностью получать и передавать наибольшее количество сигналов от объекта на пульт). Они легче интегрируются к уже установленным системам;  
На основании вышесказанного можно сделать следующие выводы:  
Наибольший эффект безопасности на объекте достигается при использовании одновременно двух видов систем проводных и беспроводных.