СЕТИ ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ. ТЕОРИЯ. ИСТОРИЯ. ПРАКТИКА

Татарченко Николай Валентинович
технический директор, Группа «Октаграм»

КОМПЛЕКСНЫЕ СИСТЕМЫ

Часто в системах безопасности на основе оборудования отечественных и целого ряда зарубежных производителей используют для создания наиболее простые и неустойчивые к обрывам или коротким замыканиям топологии сетей. Это оправдано подходом заказчиков, когда цена решает все. Мне кажется, что профессионал должен использовать знания, чтобы не просто запустить в работу систему безопасности, но и минимизировать возможные потери в ее работе от внешних воздействий на оборудование и сети в процессе эксплуатации. Знание особенностей систем в сочетании с желанием объяснить заказчику и обосновать выбор поможет сделать системы инструментом обеспечения безопасности, а не набором оборудования, при первом же воздействии (по небрежности или злонамеренном) превращающемся в кучу металлолома.

Для создания надежной СБ желательно, а при наличии соответствующих нормативных документов необходимо, использовать топологию сети, обеспечивающую непрерывную работу в случае злонамеренного или случайного повреждения связей с компонентами системы. Рассмотрим топологии и особенностях сетей для безопасности.

На *рисунке 1* показаны типы топологий для централизованных систем. Варианты расположены слева направо – A, B, C, D в порядке убывания «живучести» сети. Подключение приборов по топологии A («звезда плюс кольцо») сохраняет связь с компонентом при двух коротких замыканиях или обрывах связи линий, подключенных к этому компоненту. Важно, что все используемые для создания такой топологии сети 4 входа прибора должны быть независимыми и иметь защиту от КЗ. Подключение приборов по топологии B («кольцо») позволяет сохранить работоспособность сети при одном коротком замыкании или обрыве в линии кольца. Оба входа (или вход/выход) центрального прибора должны быть независимыми и иметь защиту от КЗ. При использовании топологии C («звезда») связь будет потеряна только в поврежденной линии, если все входы центрального прибора независимы и имеют защиту от КЗ. Если приборы в системе подключены по топологии D («линия»), то короткое замыкание в любом месте линии приведет к прекращению связи со всеми компонентами цепи. Несмотря на столь очевидное несовершенство топологии D на практике она используется наиболее часто.

Для децентрализованных систем сети могут иметь топологию, показанную на *рисунке 2*. Опять же, топология «линия» используется на практике наиболее часто, несмотря на то, что короткое замыкание в линии может привести к прекращению связи со всеми компонентами сети. Другие варианты более устойчивы к короткому замыканию или обрыву линии. Подключение приборов по топологии «кольцо» позволяет сохранить работоспособность сети при одном коротком замыкании. Если приборы в системе подключены по топологии «линии плюс кольцо», то связь между компонентами сохраняется при двух коротких замыканиях. При использовании топологии «2 кольца» работоспособность сети сохраняется при трех коротких замыканиях. Во всех вариантах кроме «линии» все используемые для создания сети входы любого прибора должны быть независимыми и иметь защиту от КЗ.

Для того, чтобы лучше понять ситуацию на практике, начнем с ретроспективы создания сетей для СБ.

Исторически первыми типами подключения периферийного оборудования к управляющим приборам/контроллерам были прямые подключения. Один извещатель или исполнитель – одна линия связи. В такой схеме много

проводов, но выход из строя одной линии никак не влияет на работу остальных. Управляющие приборы/контроллеры соединялись с центром мониторинга по телефонным линиям. То была эпоха единичных локальных сетей, когда Интернета еще не существовало.

С улучшением технологий связи и ростом объемов присоединяемых компонент менялись схемы подключения. Развитие шло в двух направлениях.

1. Подключение к контроллерам периферийных устройств.
2. Соединение между собой контроллеров и подключение к серверам.

Рассмотрим эти два направления отдельно и сначала обратимся к подключению к контроллерам периферийных устройств.

Следующим шагом после прямого подключения стало присоединение к контроллерам периферийных устройств при помощи расширительных модулей/блоков, которые соединялись с выделенными группами клемм контроллеров. Периферийное оборудование по-прежнему подключалось к паре клемм такого модуля линией из двух проводов. Питание периферийных устройств поступало или от расширительного модуля или от контроллера.

Затем наступила очередь использования расширительных модулей, соединенных с контроллером по адресной шине *(рис. 3)*.

Логичным продолжением такого пути было увеличение количества адресов и использование каждого адресного модуля для подключения одного периферийного устройства. Так появились адресные шины и адресные приборы.

Примерно в 1991 году британская компания Advanced Design Electronics Ltd (ADE) создала небольшие адресные метки *(фото 1)*. Эти метки монтирова-

Рис. 1. Варианты топологии сети централизованной системы

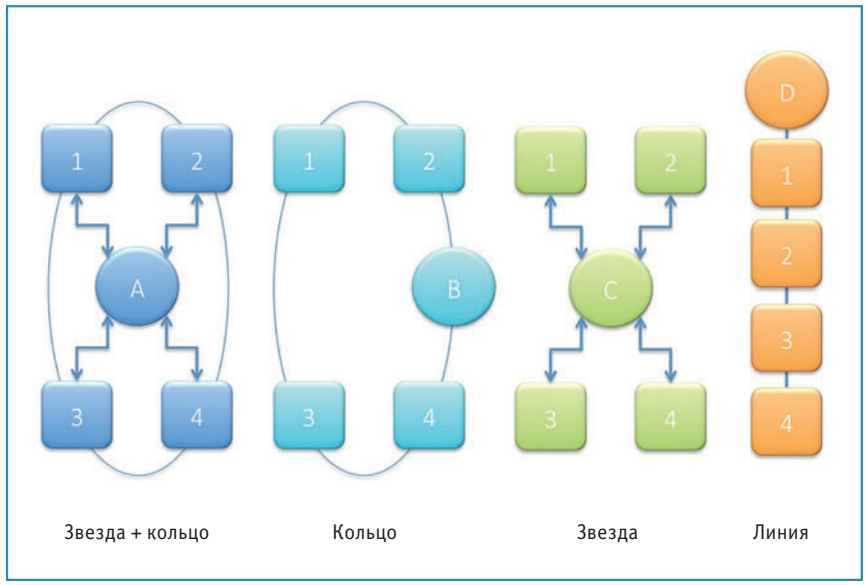


Рис. 2. Варианты топологии сети децентрализованной системы

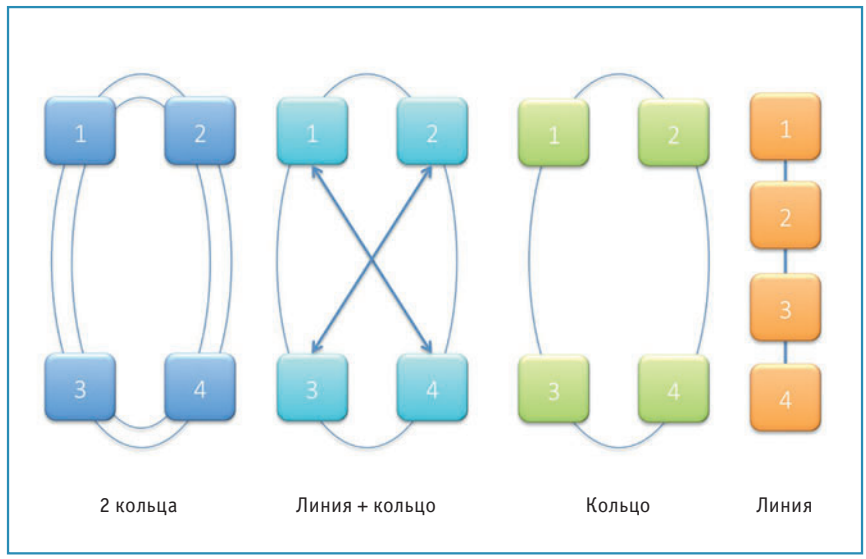


Фото 1. Адресные метки ADE

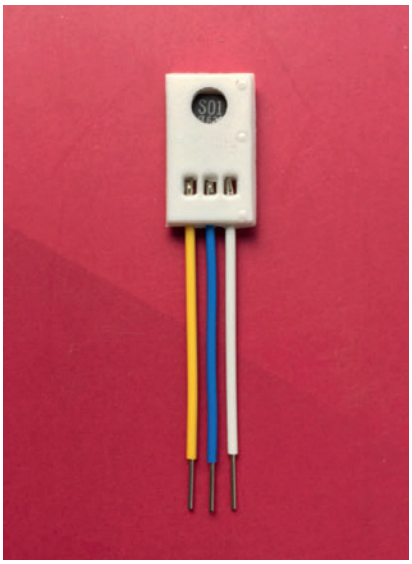


Рис. 3. Подключение расширительных модулей к контроллеру по адресной шине

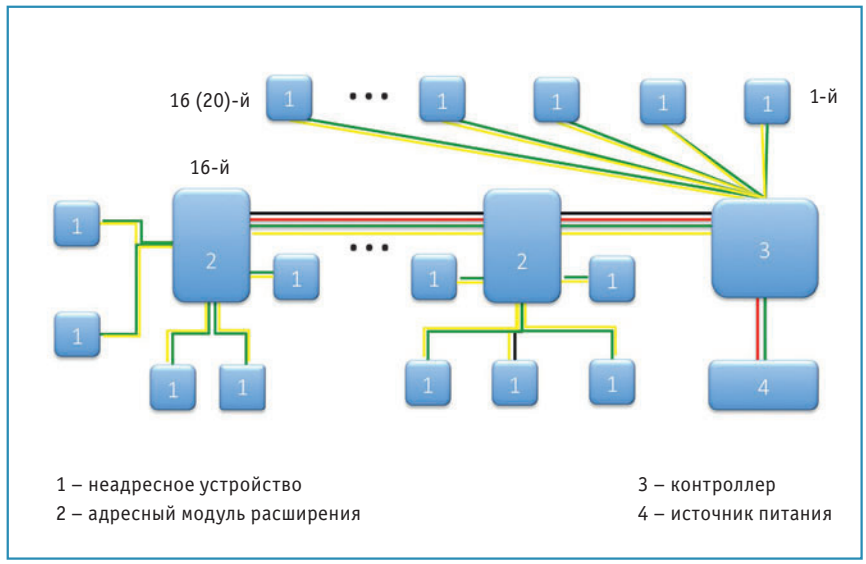
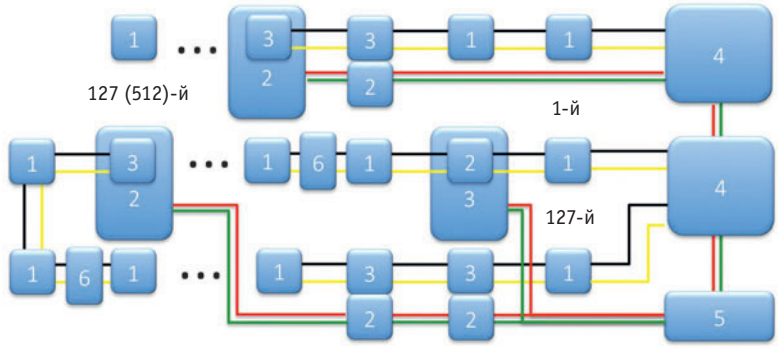
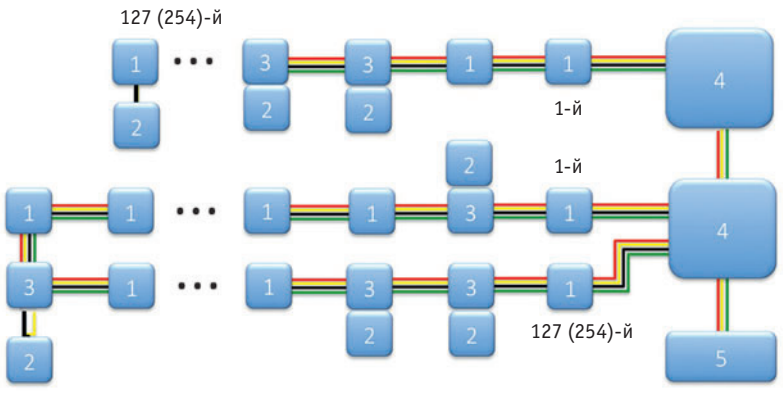


Рис. 4. Используем адресные устройства или подключаем другие через адресную метку



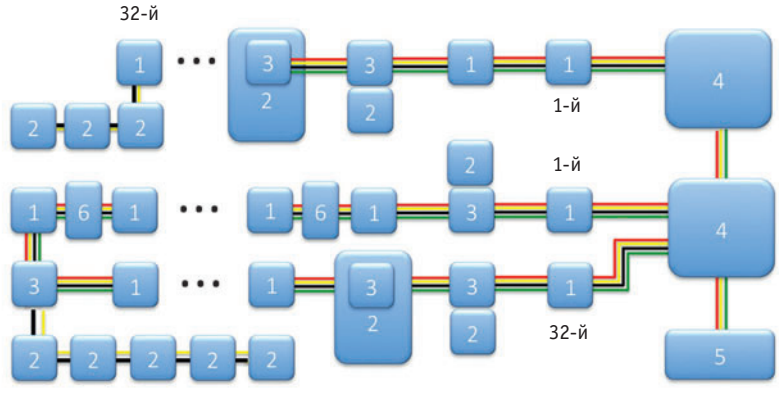
1 – адресное устройство
2 – неадресное устройство
3 – адресная метка
4 – контроллер
5 – источник питания
6 – локализатор КЗ

Рис. 5. Сеть с 2-мя изоляторами в каждом адресном модуле (технология LSN Bosch)



1 – адресное устройство
2 – неадресное устройство
3 – адресный модуль
4 – контроллер
5 – источник питания

Рис. 6. Ступенчатая схема: меньше адресов, микромодули вместо меток



1 – адресное устройство
2 – неадресное устройство
3 – адресная метка
4 – контроллер
5 – источник питания
6 – локализатор КЗ

лись в извещатель, подключались к его клеммам. Такой извещатель становился адресным. С метками работала адресная панель сигнализации Ultimate на 30 (60) зон. Годом или двумя позже британская Viper предложила извещатели, в которых адресную метку от ADE можно было вставить в специальный разъем, и извещатель становился адресным. Так появились системы, где каждое периферийное устройство имеет свой адрес и подключается к управляющему прибору по линии связи, в дальнейшем именуемой «шина».

Тут следует остановиться на количестве адресов в одной шине. В силу особенностей протокола и подхода к соотношению надежность/цена производители начали создавать приборы с количеством адресов в шине: 32 (50), 127, 254, 512.

Этот ряд можно продолжить, но очевидно, что чем больше адресов в одной шине тем меньше надежность такого соединения. Использование кольцевых шин *(рис. 4)* несколько улучшает ситуацию, но при этом защита от коротких замыканий значительно повышает стоимость такого решения.

Более того, целый ряд производителей предлагает использовать изоляторы короткого замыкания во входной и выходной цепях каждого адресного модуля (например, в технологии LSN Bosch, *рис. 5*).

Таким образом, вся экономия на стоимости проводов теряется и стоимость решения на основе такого подхода даже при современном уровне электроники будет выше, чем при прямом подключении каждого устройства к контроллеру.

Возможным выходом из подобного положения является многоступенчатая схема *(рис. 6)* присоединения к контроллерам периферийных устройств при помощи адресных микромодулей/микроконтроллеров и уменьшение количества адресов в одной шине контроллера.

Использование локализаторов короткого замыкания в этом случае не обязательно, но дает дополнительную гарантию работы наиболее важных участков сети. Каждый микромодуль имеет свою логику работы согласно выбранному для системы алгоритму и может сохранять автономную работоспособность, т. е. отключение от сети одного адреса/узла не меняет логику его работы. Это актуально, например, для СКУД, но не только.

Дополнительным бонусом при использовании микромодулей будет удобство монтажа:

1. Монтировать можно прямо в извещатель, исполнительное устройство, считыватель, монтажную коробку.
2. Часть соединений можно выпол-

нять при помощи скотчлока, что гораздо быстрее и надежнее винтовых соединений, не говоря уже о «скрутках».

Таково положение с подключением к контроллерам периферийных устройств сейчас.

Перейдем к соединению между собой контроллеров и подключению к серверам.

Вначале контроллеры соединялись между собой по проводным линиям с использованием протокола RS-422, топология «точка-точка». То была эпоха единичных локальных сетей, когда Интернета еще не существовало. Наверное, мало кто помнит те времена, когда ПК соединялись между собой и серверами при помощи коаксиального кабеля.

Хронологически схожей была история развития общих Ethernet-сетей для передачи данных и сетей для связи оборудования на основе протокола RS-485, который через какое-то время практически вытеснил RS-422.

Топологии соединения при этом использовались линейные многоточечные. Позже появляются кольцевые топологии, дублирование связей между точками.

Поскольку основная логика работы СБ лежит на контроллерах (как правило, это ПК у американцев и специальные вычислительные платформы у европейцев), то обеспечения максимальной надежности при построении средних и крупных систем можно достичь используя, как минимум, кольцевую топологию соединения контроллеров *(рис. 2)*. Вариант «линия» возможен в случае более простых объектов.

Очевидно, что создание сети, в которой каждое периферийное устройство (теперь оно уже не совсем периферийное) является одновременно и ретранслятором, и хранителем данных всей системы, выглядит наиболее отказоустойчивым. Однако, если в беспроводных системах такой подход относительно легко реализуем, то в проводных системах соединять все устройства друг с другом просто невообразимо трудно, так как мы утонем в паутине проводов (смотрите схему А *рис. 1*).

К счастью, в СБ в отличие от IT наиболее важной является текущая информация и мгновенная передача команд. Поэтому использование кластерно-централизованного типа систем выглядит весьма надежным и уместным для объектов любого масштаба.

Несколько примеров построения сетей для систем безопасности

А) Система пожарной сигнализации, управления вентиляцией, оповещения о пожаре и водяного пожаротушения в среднем торговом центре требует не просто линейного соединения приборов и шкафов при помощи RS-485 шины, а, как минимум, дублирующего подключения всех компонент через Ethernet или прямые подключения контроллеров через релейные входы/выходы с обязательным контролем неисправностей каждого соединения. Двухсторонний контроль должен быть за линией связи с центром мониторинга.

Б) Система контроля доступа с линейным подключением контроллеров в случае пожара должна иметь прямые подключения для разблокировки и иметь возможность передачи команды разблокировки через подсеть СКУД. В данном случае будет достаточно кластерно-централизованного типа систем. Аналогичная ситуация возникает в СКУД при Antipassback в отдельной части здания.

В) А вот согласованная работа охранной сигнализации в рамках корпорации принесет неудобства пользователям, если будет использовать Интернет без дублирования связи, например по GPRS-каналу. С другой стороны, при наличии персонала в офисах такой сбой не повлияет на безопасность, если информация в рамках офиса/кластера будет передаваться исправно.

Приведенные примеры показывают, что практически каждый объект требует индивидуального подхода к созданию сети для СБ, хотя зачастую не требует очень крутых мер для обеспечения живучести системы в целом.

Повторю: *«Знание в сочетании с желанием объяснить заказчику и обосновать выбор поможет сделать системы настоящим инструментом обеспечения безопасности»*.