МЗТА
mzta.ru

Сделано в России
Программно-технический комплекс «КОНТАР»

С 2010 г автоматизировано более 10 000 объектов в Москве и по России

Линейка **свободнопрограммируемых** контроллеров «Контар» (MC8/MC12, ML9);

Бесплатное ПО:

SOFTLOGIC,
- среда программирования контроллеров ПО «КОНГРАФ» ;
- средство отладки ПО «КОНСОЛЬ»

SCADA (сертифицирована в качестве АСКУЭ);
- WEB-SCADA для удаленного доступа
- АРМ диспетчера – для локальных решений

Бесплатная техническая поддержка

Защищенный протокол Kontar-Bus связи между SCADA и контроллерами при проектировании и инсталляции снижает:
- трудозатраты;
- потребности в компетенциях и специалистах;
- затраты денежных средств;

Особенности	Решения		
	Kontar-Bus	OPC- технология	Открытый протокол
Технические особенности			
Защита передаваемых данных	есть	нет	нет
Задержки на OPC-преобразования сигналов	нет	есть	нет
Дополнительная трудоемкость			
Разработка алгоритмов OPC-трансформации сигнала:			
• оборудование – OPC-сервер	нет	есть	нет
• OPC-сервер – SCADA	нет	есть	нет
Отладка алгоритмов OPC-трансформации сигнала:			
• оборудование – OPC-сервер	нет	есть	нет
• OPC-сервер – SCADA	нет	есть	нет
Формирование таблицы пересылки между SCADA и контроллером	нет	нет	есть
Настройка портов	нет	есть	есть
Дополнительные затраты			
Закупка платного OPC-сервера	нет	есть	нет

Независимость компонентов SOFTLOGIC и SCADA позволяют параллельно выполнять программирование контроллеров и разработку мнемосхемы системы диспетчеризации.

Полная совместимость SOFTLOGIC и SCADA минимизируют трудоемкость согласования алгоритмов управления контроллером и мнемосхемы SCADA-системы.

Некоторые удобные особенности линейки контроллеров:
- Поддержка стандартных протоколов взаимодействия с периферийными устройствами
- Универсальность назначения (Master/Slave/автономный)
- Универсальность аналоговых входов
- Мощные выходы (релейные - до 3А, ШИМ – до 10 А)
- Наличие блоков расширения входов/выходов

ПТК «Контар» поддерживает OPC-технологию для решения задач интеграции контроллеров и SCADA со сторонними системами.

Имеются обширные библиотеки алгоритмов для управления технологическими процессами в области:
- отопления,
- водоснабжения,
- кондиционирования,
- эксплуатации технологических печей.

Обучение, свободный доступ к обучающим материалам.

ОАО «МЗТА» Россия, 105318, Москва, ул. Мироновская, д.33. Тел.: **+7 495 720 54 44**, e-mail: **info@mzta.ru**

О киберугрозах для ЖКХ без иронии

МЗТА
mzta.ru

Жилищно-коммунальное хозяйство обеспечивает базовые потребности людей, и кибератака на системы диспетчеризации, обслуживающие объекты ЖКХ, способна нанести значительный экономический ущерб и привести к социальному обострению. Все это заставляет повышать безопасность АСУ ЖКХ, защищая их точки уязвимости. Такую возможность предоставляет ПТК «Контар».

«МЗТА Инжиниринг», г. Москва

Когда-то антиутопия «1984» Оруэлла воспринималась как нечто далекое, запредельное и гротескное, но сегодня Большой брат со своими методами слежки – просто малыш с совочком в детской песочнице по сравнению с возможностями «роторного экскаватора» по глобальному сбору и обработке данных, которыми располагают современные спецслужбы. Когда-то дикие мотобанды из «Бешеного Макса» казались безумной фантазией режиссера о жизни в мире после глобальной катастрофы, а сегодня куда лучше вооруженные и оснащенные мобильные отряды террористов сеют смерть и разрушения на Ближнем Востоке.

Сегодня вопрос о киберугрозах для ЖКХ у большинства специалистов и чиновников вызовет если не усмешку, то чувство недоумения – о чем это? Действительно, о чем?

ЖКХ – элемент стабильности государственной системы

ЖКХ обеспечивает людей в соответствии с их базовыми потребностями водой, теплом, электричеством. Географическое расположение России обуславливает низкие отрицательные температуры в зимний период, поэтому теплоснабжение – критическое условие физического выживания людей в большинстве российских городов. Длительное и массовое прекращение подачи тепла даже на некоторой части жилых объектов в городах способно привести к очень серьезным социально-экономическим последствиям – увеличению заболеваемости и смертности населения, возрастанию социально-политического напряжения в обществе, возникновению миграционных потоков и т.п.

Источник угрозы

Не будет преувеличением сказать, что сейчас весь мир переживает некий переломный момент, когда под словом «война» начинают понимать не только военные действия, но и информационные, политические, экономические и прочие методы воздействия. И такую вещь, как диверсия на объектах ЖКХ, нельзя списывать со счетов. Ведь, как мы говорили чуть выше, это очень серьезный инструмент для дестабилизации обстановки.

Нарушение работоспособности инфраструктуры ЖКХ в отопительный период представляет собой достаточно хорошую возможность нанести существенный социально-экономический урон:

- повысить социально-политическое напряжение среди населения;
- причинить значительный экономический ущерб, обусловленный необходимостью проведения ремонтов и замены вышедшего из строя оборудования.

Кибератака на ЖКХ и ее последствия

Под кибератакой понимается преднамеренное удаленное вмешательство в работу систем автоматического управления оборудованием с целью нанесения максимально возможного урона технико-экономической системе.

Массовый переход на высокоинтеллектуальные системы автоматики и системы диспетчеризации создает необходимые условия для подготовки и реализации кибератак на автоматизированное оборудование.

Кибератака, например, на управляющий отопительным котлом контроллер позволяет «раскачать» котел и привести к нежелательным последствиям: как минимум – к аварийному останову котла, как максимум – к его разрушению.

Последствия кибератаки на контроллер, управляющий работой насосной группой систем отопления (ХВС, ГВС), выглядят аналогично:

- минимум – ускоренная выработка ресурса как самих насосов, так и систем подключенного к ним трубопровода (например, отопительной системы), что повышает общий риск ее выхода из строя в отопительный период;
- максимум – разрушение насосов, прорывы трубопроводов.

По понятным соображениям, мы не будем подробно описывать технологию массовой кибератаки. К сожалению, она не так сложна и фантастична, как это может показаться на первый взгляд. А эффект от нее может быть очень впечатляющим: массовый

выход отопительного оборудования из строя в разгар зимнего периода, на который оперативные службы не смогут адекватно отреагировать, и соответствующие последствия.

Уязвимости АСУ ЖКХ

Однако перечислить уязвимости в системах автоматизированного управления (АСУ) объектами ЖКХ необходимо, потому что с ними можно и нужно бороться. Выделим следующие уровни уязвимости:

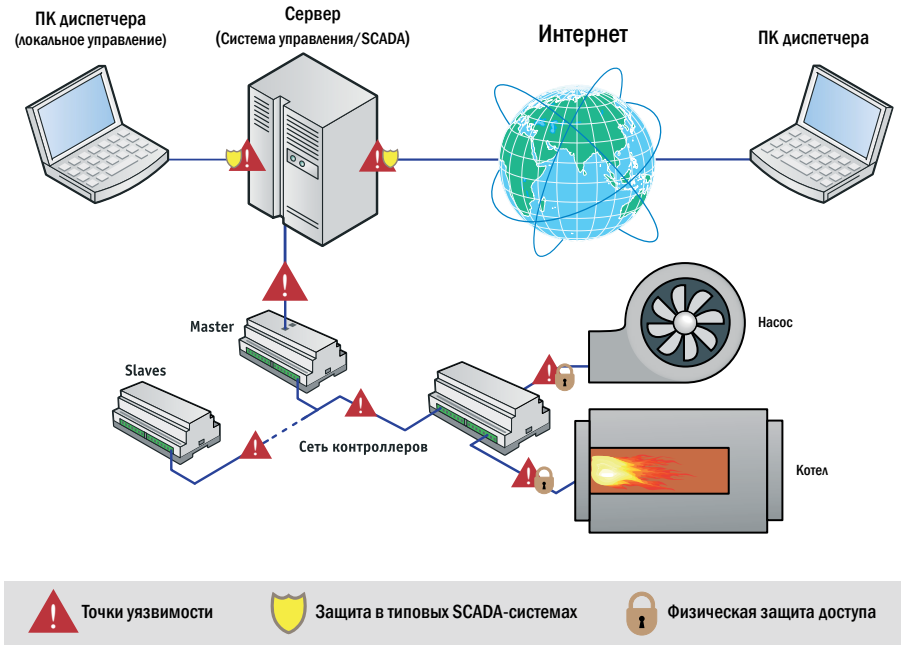
- система удаленного доступа к системе через Интернет;
- доступ к управлению оборудованием в системе диспетчеризации (управление в SCADA);
- система передачи данных и управляющих команд внутри SCADA-системы – между системой управления и контроллерами, осуществляющими непосредственное управление оборудованием;
- физические точки подключения к выводам управляющего контроллера и к выводам управления исполнительными механизмами.

Способы снижения уязвимости АСУ объектов ЖКХ

Какими же методами снижается уязвимость АСУ на каждом из перечисленных уровней?

- На уровне *удаленного доступа* эта задача обычно решается с помощью создания закрытой локальной сети, изолированной от сети Интернет, а также с помощью использования специализированных средств шифрования передаваемых данных.
- На уровне *управления оборудованием в системе диспетчеризации эта цель*, как правило, достигается с помощью дифференцированного предоставления прав доступа персоналу на определенные действия в системе, например, на просмотр, на подачу управляющих команд определенного оборудования, на внесение изменений в регулируемые параметры определенного оборудования и т.п.
- Что касается *управления оборудованием через физический доступ* к управляющим входам и портам контроллера и/или выводам управления исполнительными механизмами, то обычно организуется физическое ограничение доступа к местам расположения шкафов автоматики и к самому оборудованию.
- В области *передачи данных и управляющих команд между системой управления и контроллерами* эта задача обычно никак не решается.

Передача данных и управляющих команд между системой управления и контроллерами является не только самым уязвимым местом современных SCADA-систем, но и самым эффективным с точки зрения нанесения урона.



▲ Защищенность точек уязвимости в системах диспетчеризации, построенных на базе типовых SCADA

Шифрование передаваемых данных в SCADA как защита от кибератак

Особенностью большинства имеющихся на рынке SCADA-систем является использование в системе управления контроллерами открытых протоколов, в частности для передачи управляющих команд на контроллеры. Открытые протоколы, передаваемые в сетях, в том числе закрытых, достаточно просто считать и раскодировать, вследствие чего может быть получен прямой доступ к управлению контроллером.

Шифрование данных, передаваемых между SCADA-системой и контроллерами или между контроллерами, в настоящее время реализуется путем:

- использования специализированного зашифрованного протокола, который понимают и контроллер, и SCADA-система;
- применения дополнительных средств шифрования и дешифрования, встраиваемых в канал связи между устройствами, обменивающимися данными.

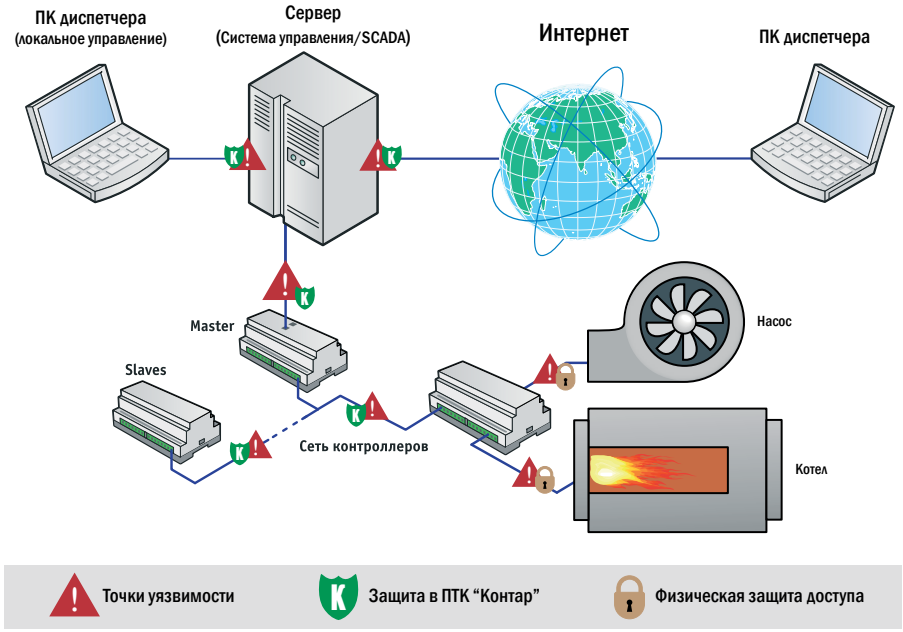
Применение шифрования передаваемых данных в SCADA-системе в наибольшей степени актуально для систем с удаленным управлением через Интернет. Однако, учитывая, что организация несанкционированного подключения с удаленным беспроводным доступом к закрытым локальным сетям задача технически несложная, шифрование передаваемых данных актуально и для локальных решений.

SCADA и контроллеры «Контар» с повышенной защитой от кибератак

Отечественный программно-технический комплекс (ПТК) «Контар» представляет собой набор следующих программно-технических средств:

- SOFTLOGIK – средства программирования и отладки контроллеров (ПО «КОНГРАФ» и ПО «КОНСОЛЬ» бесплатно);
- SCADA – система диспетчеризации (WEB-SCADA и АРМ диспетчера бесплатно);
- семейство контроллеров MC/ML с блоками расширения входов/выходов и приборов учета.

Единство разработки всех компонентов ПТК «Контар» обеспечивает возможность «сквозного проектирования», которое позволяет исклю-



▲ Защищенность точек уязвимости системы диспетчеризации в решениях на базе ПТК «Контар» (SCADA и контроллеры)

чить «ручное» определение соответствия тегов контроллера и SCADA, чем существенно сокращает трудоемкость создания проекта.

В ПТК обмен данными между SCADA и контроллерами, между контроллерами, между контроллерами и блоками расширения обеспечивается по протоколу с 64-битным шифрованием. Наличие мастер-ключа позволяет создавать для каждого проекта уникальный устойчивый шифр.

Также SCADA «Контар» предоставляет широкие возможности в области разграничения доступа пользователей к выполнению операций по диспетчерскому управлению объектами: просмотру данных, подаче управляющих команд, внесению изменения в настройки оборудования и многого другого.

А. Г. Краснов,
специалист по маркетингу,
«МЗТА Инжиниринг», г. Москва,
тел.: (499) 369-0600,
e-mail: eng@mzta.ru,
www.mzta.ru

МЗТА
mzta.ru

Готовятся к серийному производству новые модификации приборов, входящих в ПТК «Контар», производства МЗТА:

МА8.3М. Основное и главное отличие *МА8.3М* заключается в возможности конфигурирования аналоговых входов под различные типы сигналов датчиков.

МА8.3 на аналоговых входах воспринимала сигналы 0-2400 мВ и сопротивление. *МА8.3М* воспринимает сигналы со следующих типов датчиков:

1. Датчик с выходным сигналом постоянного напряжения от -100 до 2400 мВ (Вход АЦП).
2. Термометр сопротивления, реостатный датчик, термопара.
3. Датчик с выходным сигналом постоянного тока от 0(4) до 20 мА и от 0 до 5 мА.
4. Датчик с выходным сигналом постоянного напряжения от 0 до 10 В.

Новые исполнения контроллеров типа МС. *МС8.401* и *МС12.4*, контроллер с транзисторными и релейными выходами соответственно и упрощенной схемой питания, без гальванического разделения.

ОАО «МЗТА» Россия, 105318, Москва, ул. Мироновская, д.33. Тел.: +7 495 720 54 44, e-mail: info@mzta.ru