*Денис Зозуля*

# Защита промышленных сетей в системах автоматизации

**Современные системы автоматизации строятся с применением сетевых технологий, но информационной безопасности АСУ ТП не всегда уделяется должное внимание. Защита сетей Industrial Ethernet – это дополнительная мера обеспечения безопасности технологического процесса от современных информационных угроз.**

## Введение

Автоматизация опасных производств и объектов инфраструктуры требует соблюдения комплекса мер для обеспечения безопасности технологического процесса. Технологическая авария может привести как к серьёзным финансовым потерям, так и к экологической катастрофе. Для обеспечения безопасности технологического процесса на уровне АСУ ТП применяется комплекс мер, таких как резервирование и повышение надёжности компонентов.

Современные системы автоматизации строятся с применением сетевых технологий. Но даже промышленные сети Industrial Ethernet так же уязвимы, как и IT-сети. В отличие от офисных сетей, защите промышленных сетей не всегда уделяется должное внимание.

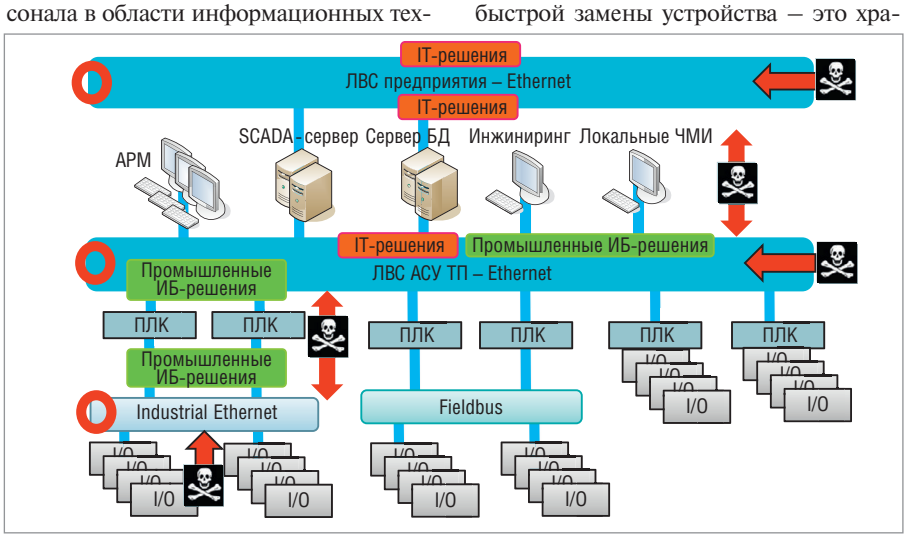
## Специфика промышленных решений в сфере информационной безопасности

Почему же защите промышленных сетей не всегда уделяется должное внимание? Ответ прост: специалисты в области АСУ ТП не имеют должной квалификации в сфере информационной безопасности (ИБ), а специалисты по ИБ не имеют полного представления о технологиях и специфике промышленных систем. Поэтому современные системы АСУ ТП имеют множество уязвимостей, которые необходимо принимать во внимание при реализации проектов.

В чем же специфика систем информационной безопасности в АСУ ТП? Во-первых, системы защиты должны соответствовать промышленным требованиям по механическим характеристикам и климатическому исполнению. Отличается и специфика работы систем. Промышленные решения должны быть необслуживаемыми, после установки обновление ПО, плановые перезагрузки и прочие сервисные действия не предусмотрены. Промышленные системы работают круглые сутки без перерыва и должны обеспечивать безотказную работу.

Квалификация обслуживающего персонала в области информационных технологий не всегда достаточна для правильной настройки и обслуживания сетевого оборудования, поэтому промышленные решения должны быть просты в настройке для любого инженера АСУ ТП. Исходное программное обеспечение не всегда доступно, а использование команд консоли (CLI) требует определённых знаний, поэтому необходимо иметь возможность настраивать каждый межсетевой экран через Web-интерфейс с любого компьютера.

Замена оборудования в случае неисправности должна производиться в считанные минуты. Лучший вариант для быстрой замены устройства – это хра-




**Условные обозначения:**

**АРМ** – автоматизированное рабочее место; **БД** – база данных; **ИБ** – информационная безопасность; **ЛВС** – локальные вычислительные сети; **ПЛК** – программируемый логический контроллер; **ЧМИ** – человеко-машинный интерфейс; **I/O** – устройства ввода-вывода; **IT** – информационные технологии.

**Рис. 1. Архитектура современных АСУ ТП и карта уязвимостей промышленных сетей**

нение конфигурации на карте памяти внутри устройства. Карта памяти извлекается из неисправного устройства и просто вставляется в новое. Система восстанавливается за несколько минут.

Немаловажной особенностью защиты сети АСУ ТП является возможность установки оборудования защиты в существующую сеть без изменения её архитектуры. Режим невидимости (Stealth Mode) позволяет настроить межсетевой экран и установить его между защищаемым оборудованием и внешней сетью как невидимый барьер для всех возможных угроз безопасности без перенастройки адресов в сети и настройки маршрутных таблиц.

## Фундаментальное отличие защиты сети АСУ ТП

Архитектура построения сетей IT и АСУ ТП также отличается (рис. 1). На территории объекта IT-сеть имеет одну или несколько серверных, и все точки подключения сопряжены всего лишь с несколькими коммутаторами. Промышленная сеть распределена по всему предприятию, и каждый шкаф АСУ ТП обычно имеет свой коммутатор, поэтому точек входа в промышленную сеть на порядок больше. В одной сети также могут находиться системы и оборудование различных производителей, и при обслуживании своей установки сервисный персонал может иметь неограниченный доступ к смежным системам.

## Угрозы в промышленных сетях

Рассмотрим угрозы в промышленных сетях, источники их возникновения и возможные последствия. Промышленные Ethernet-сети используются на всех уровнях АСУ ТП: на уровне связи систем управления между собой (средний уровень), на уровне коммуникации со SCADA-системами (верхний уровень) и на уровне распределённой автоматизации (нижний уровень). Сеть любого уровня может нести в себе угрозу безопасности технологического процесса, поэтому необходимо обеспечивать защиту на всех уровнях АСУ ТП. К основным угрозам сетевой безопасности относятся:

- сетевой шторм – лавинообразный рост широковещательного или многоадресного трафика;
- DDoS-атака – бомбардировка отдельных устройств сети большим количеством ICMP-пакетов (ICMP – межсетевой протокол контрольных сообщений, например ping) или очень частое подключение к устройству за малый промежуток времени;
- неавторизованный доступ к контроллеру и сети управления – возможность передачи команд управления и доступ к программированию или параметрированию контроллера;
- защита удалённого доступа к системе через сети с низким уровнем доверия, например через сеть Internet.

## Неавторизованный доступ

Главная уязвимость промышленных систем – это возможность неавторизованного доступа к системе управления. Очень часто сеть АСУ ТП опасного производства распределена по большой территории. И даже если доступ к центральному управляющему контроллеру закрыт физически, то сетевой доступ к нему, подчинённым системам, рабочим местам и серверам SCADA можно получить из любой точки сети. Многие современные контроллеры имеют возможность удалённого программирования через Ethernet и поддерживают связь со SCADA-системами по открытым протоколам. Если сеть АСУ ТП подключена к сети предприятия без межсетевого экрана, то к системам управления возможен неавторизованный доступ и контроллер можно перепрограммировать, остановить выполнение программы, изменить уставки или передать сигнал управления с помощью любого компьютера в сети всего предприятия.

Рассмотрим способы защиты системы автоматизации от неавторизованного доступа. Необходимо разделить сети верхнего, среднего и нижнего уровня межсетевыми экранами. Также для обеспечения максимальной информационной безопасности межсетевым экраном следует защитить Ethernet-интерфейсы управляющего контроллера. Таким образом мы ограничиваем доступ к локальным системам управления из внешних сетей и защищаем контроллер. Для получения доступа к данным системы, для передачи команд или для программирования системы в межсетевом экране настраиваются правила доступа. Межсетевой экран перед контроллером настраивается на блокировку портов для программирования, а коммуникация со SCADA-системой открывается только для IP-адресов основных и резервных серверов. Контроллер теперь полностью защищён от неавторизованного доступа. Перепрограммирование возможно только при прямом подключении, а команды управления могут передавать только SCADA-серверы.

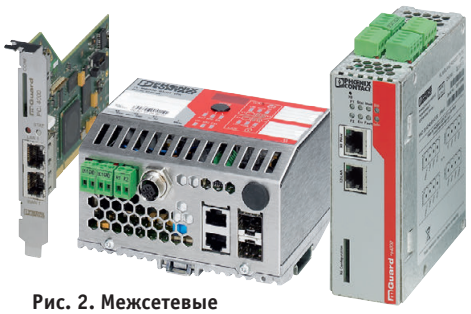


**Рис. 2. Межсетевые экраны FL MGUARD от Phoenix Contact**

Но что делать, если необходим временный сетевой доступ к контроллеру для перепрограммирования или отладки коммуникации? Для таких задач нет необходимости перенастраивать права доступа на межсетевом экране. Решения информационной безопасности MGUARD от Phoenix Contact поддерживают функцию пользовательского межсетевого экрана (рис. 2). Данная функция позволяет создать динамические права доступа к определённым частям системы АСУ ТП. Для доступа необходима аутентификация на межсетевом экране по заранее созданным учётным записям на самом устройстве или RADIUS-сервере. Пользователю необходимо просто зайти по IP-адресу межсетевого экрана на его Web-интерфейс, ввести логин и пароль. Межсетевой экран открывает заранее настроенные порты и даёт доступ к контроллеру.

Для оптимизации информационной защиты коммуникации по сбору данных и передаче сигналов управления в нормальном режиме должны быть открыты только для SCADA-серверов. На АРМ операторов используется клиент-серверная архитектура. Клиенты SCADA-системы могут находиться в любой сети предприятия, и защита доступа реализуется с помощью аутентификации, как в клиенте SCADA-системы, так и через пользовательский межсетевой экран.

## Заключение

Информационная безопасность АСУ ТП – это новая и перспективная составляющая современных систем автоматизации. Внедрение системы защиты – это инвестирование в безопасность людей, экологию и способ избежать финансовых потерь из-за сбоев в работе сетевой инфраструктуры или неавторизованного доступа к системам управления. ●

**ООО «Феникс Контакт РУС»**
**Телефон: +7 (495) 933-8548**
**E-mail: info@phoenixcontact.ru**
**www.phoenixcontact.ru**

На правах рекламы