

# Создание защищенного удаленного доступа к промышленному объекту

на основе оборудования Phoenix Contact



Промышленный маршрутизатор mGuard позволяет создать защищенный канал передачи данных в беспроводных сетях. Это единственный промышленный маршрутизатор, сертифицированный во ФСТЭК России. В статье описаны особенности функционирования и использования данного оборудования.

000 «Феникс Контакт РУС», г. Москва

В настоящее время практически все производственные процессы позволяют выполнять управление и мониторинг удаленно, без непосредственного присутствия человека на промышленном объекте. Но так как большинство удаленных подключений производится через Интернет, то при передаче данных в открытом виде существует огромная вероятность их подмены или кражи. На промышленном объекте подмена управляющих команд может повлечь за собой выход из строя высокотехнологического оборудования, экологические катастрофы или человеческие жертвы. Поэтому приходится задумываться о защищенности передаваемой информации. Чтобы обезопасить данные, не только создается защищенный канал, но и накладываются дополнительные ограничения на используемое оборудование, касающиеся окружающей среды объекта, специфического электрического питания, особенностей монтажа и т. д.

## Защищенный канал передачи данных

Создание защищенного канала для мониторинга или управления промышленного объекта происходит путем установки необходимого оборудования на объекте и в то же

время — программного или аппаратного оборудования для шифрования исходящего трафика и дешифрования входящего. Для усложнения задачи рассмотрим объект, который находится в труднодоступном месте и подвести к которому кабельную линию связи практически невозможно.

Для создания защищенного канала удаленного доступа к данному объекту используем промышлен-

ный маршрутизатор mGuard производства компании Phoenix Contact (рис. 1).

Данные маршрутизаторы крепятся на DIN-рейку и используют напряжение питания 24 V DC (с возможностью резервного питания). Также они поддерживают режим работы в расширенном диапазоне температур: от -40 до +70 °C.

Для реализации проекта на труднодоступных объектах возмож-



Рис. 1. Промышленные маршрутизаторы mGuard от Phoenix Contact

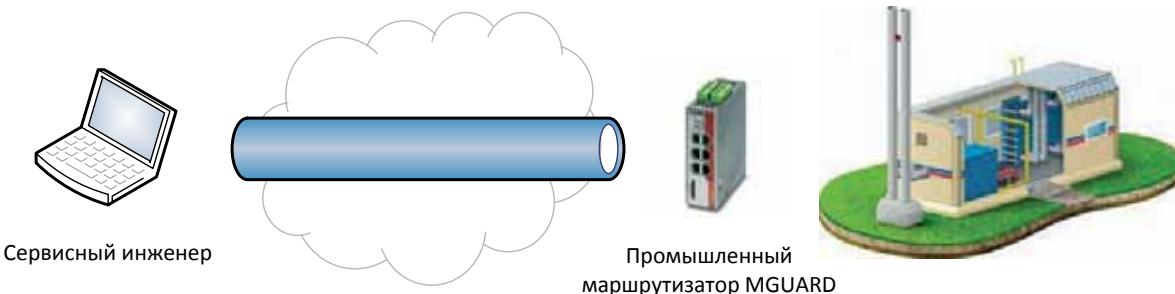


Рис. 2. Подключение сервисного инженера через VPN

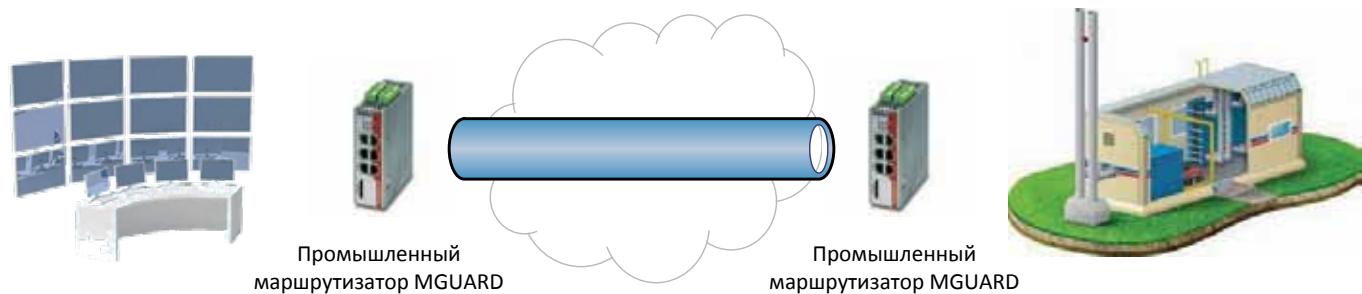


Рис. 3. Подключение диспетчерского пункта к промышленному объекту

но применение модельного ряда mGuard с поддержкой передачи информации посредством сетей GSM. Такие маршрутизаторы могут работать с двумя сим-картами одновременно (необходимо, чтобы это были сим-карты разных провайдеров). Создание защищенного канала передачи данных происходит с помощью технологии VPN (*от англ. Virtual Private Network – виртуальная частная сеть*), которая позволяет сервисному инженеру из центрального офиса подключаться к различным удаленным объектам с имитацией частного подключения (рис. 2).

Инженер идентифицируется, авторизуется на промышленном маршрутизаторе и только после этого получает доступ к необходимым сетевым ресурсам.

Аналогичным образом можно создать защищенный канал для мониторинга удаленного объекта. То есть система будет посыпать всю нужную информацию на диспетчерский пункт (рис. 3).

Важнейшими элементами при создании защищенного доступа являются шифрование, аутентификация и управление доступом.

Шифрование гарантирует защиту передаваемых данных от подмены

при передаче через открытую сеть. Для этого в mGuard используются различные алгоритмы шифрования: DES, 3DES, SHA 128, 192 и 256 бит. Для применения ключа в 256 бит дополнительная сертификация не требуется, так как mGuard обладает нотификацией ФСБ, разрешающей использовать данный ключ шифрования.

Аутентификация необходима для идентификации взаимодействующих систем на различных концах VPN. Для аутентификации существует возможность использовать PSK-ключи шифрования или сертификаты.

Управление доступом требуется для предоставления пользователю сетевых объектов, разрешенных только для него. Для этого можно применить стандартные правила фильтрации по IP, адресу источника, адресу назначения или портам. Кроме того, в маршрутизаторах Phoenix Contact реализован доступ к ресурсам с авторизацией пользователя – User Firewall. То есть после установления шифрованного соединения пользователь должен на защищенном веб-интерфейсе mGuard ввести свои данные (логин и пароль); при успешной авторизации ему будет предоставлен доступ к ресурсам

сети. Данные о пользователе могут храниться как на локальном промышленном маршрутизаторе, так и на RADIUS-сервере.

#### Вывод

Создание защищенного соединения необходимо для удаленного доступа к промышленному объекту. Это в высшей степени важная и необходимая составляющая сетевой безопасности, и пренебрегать ею крайне опасно. Также следует отметить, что компания Phoenix Contact сертифицирует промышленные маршрутизаторы mGuard во ФСТЭК России на соответствие 3-му классу защищенности межсетевых экранов (МЭ) и 4-му уровню контроля отсутствия недекларированных возможностей (НДВ). Данная сертификация будет получена ориентированно в начале 2016 года. В итоге это будет единственный сертифицированный промышленный маршрутизатор в России.

Д. Э. Тойвонен, менеджер по продукции I/O and Networks,  
ООО «Феникс Контакт РУС», г. Москва,  
тел.: (495) 933-8548,  
e-mail: info@phoenixcontact.ru,  
www.phoenixcontact.ru

Продажи осуществляются  
через сеть магазинов

**КИП-Сервис**

г. Астрахань  
ул. Ю. Селенского, 13  
тел.: (8512) 54-92-05, 54-93-65

г. Белгород  
ул. Студенческая, 19, офис 104  
тел.: (4722) 31-70-33, 31-70-34

г. Волгоград  
ул. Тимирязева, 9А  
тел.: (8442) 41-12-15, 41-14-48

г. Волжский  
ул. Горького, 4, офис 1  
тел.: (8443) 34-20-06, 41-54-02

г. Воронеж  
пр-кт. Труда, 16  
тел.: (473) 246-07-27, 246-07-89

г. Екатеринбург  
ул. Ферганская, 16, офис 109  
тел.: (343) 385-12-44

г. Краснодар  
ул. М. Седина, 145/т  
тел.: (861) 255-97-54

г. Липецк  
ул. С. Литаврина, 6А  
тел.: (4742) 23-39-56, 23-39-57

г. Москва  
Бумажный пр., 14, стр. 1  
тел.: (495) 760-33-62, 760-33-94

г. Нижний Новгород  
ул. Куйбышева, 57  
(831) 218-00-96, 218-00-97

г. Новороссийск  
ул. Южная, 1, пит. А,  
помещение 17  
тел.: (8617) 76-47-94, 76-45-66

г. Новосибирск  
ул. Серебренниковская, 9  
тел.: (383) 209-04-31, 209-13-25

г. Пермь  
ул. С. Данцига, 4А, офис 5  
тел.: (342) 237-16-16, 237-16-10

г. Пятигорск  
ул. Крайнего, 74  
тел.: (8793) 38-46-24, 33-70-98

г. Ростов-на-Дону  
пр. Ворошиловский, 6  
тел.: (863) 282-01-64, 282-01-65

г. Санкт-Петербург  
ул. 12-я Красноармейская, 12  
тел.: (812) 575-48-15, 575-48-17

г. Саратов  
Новоастраханское шоссе, 81  
тел.: (8452) 39-49-10, 39-49-11

г. Ставрополь  
ул. Мира, 323/А  
тел.: (8652) 35-74-16, 35-87-07

г. Чебоксары  
ул. Декабристов, 18А  
тел.: (8352) 28-06-28, 28-06-68

## Ультразвуковые датчики уровня для агрессивных сред



### Особенности:

hps+130	0,35 м	
hps+340	3,4 м	

Устойчивый к давлению  
до 6 бар

### LinkControl

возможность подключения  
для настройки с компьютера

### Аналоговый выход

4...20 мА (0...10 В) для измерения

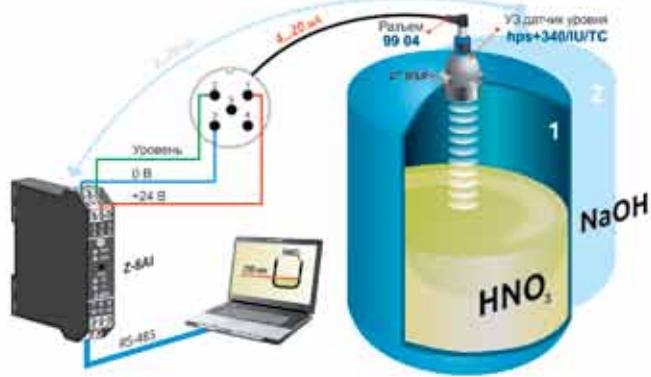
### Дискретный выход PNP

для сигнализации

### Питание

от 9 до 30 В пост. тока  
с защитой от переполюсовки

### Применение:



Одним из стандартных применений для датчика hps+ является измерение уровня агрессивных жидкостей в емкостях из пластика или нержавеющей стали. Выходной сигнал датчика 4...20 мА поступает на 8-ми канальный модуль ввода аналоговых сигналов Z-8AI (фирмы Seneca), после чего по интерфейсу RS485 передается на ПЛК или ПК (например, на SCADA систему).



**microsonic**

Сделано в Германии.

Официальный представитель Microsonic  
на территории России ООО "КИП-Сервис"

[www.kipservis.ru](http://www.kipservis.ru)