Концепция защиты промышленного IT-контура на основе брандмауэра Hirschmann серии Eagle 20

Франк Зойферт

В статье рассматриваются преимущества и особенности работы оборудования и ПО семейства EAGLE от компании Hirschmann. Приведены примеры типовых схем включения оборудования EAGLE в существующую сеть предприятия. Рассмотрены основные функции, режимы работы и нюансы настройки.

Введение

Собственные сотрудники – угроза безопасности?

В 2004 году 17-летний школьник обнаружил слабое место системы безопасности в ОС Windows XP и создал червя Sasser, который позволяет получать доступ к терминалам и выключать их. Данная уязвимость обусловлена тем, что разработчики компании Microsoft по неустановленным причинам не защитили порт 445.

Времени на создание червя потребовалось не более одной ночи, но полученные в результате его работы повреждения нанесли миллионные убытки. Специалисты Microsoft оперативно устранили технические недостатки, после чего появилась возможность перехватывать червей из внешних сетей центральным брандмауэром операционной системы.

Описанный случай повлиял на деятельность многих промышленных компаний и на административные ведомства, поскольку в настоящее время большинство систем управления промышленных предприятий построено на базе ОС Microsoft. Но в этом случае решение с помощью системного брандмауэра не помогло, так как вредоносное программное обеспечение было случайно принесено сотрудниками, использующими свои ноутбуки за пределами компании. Таким образом, инфицированные ноутбуки после повторного подключения к внутренней сети компании давали возможность червю снова и снова заражать всю сеть. Получается, что собственные сотрудники компании стали неумышленной угрозой её безопасности.

Угроза безопасности может включать как сотрудников компании, так и клиентов, которые получают тем или иным образом доступ к корпоративной сети. Источник опасности может таиться не только во вредоносном ПО. Зачастую при подключении к случайным сетям через стандартный браузер можно подвергнуть опасности локальный компьютер и далее компьютеры всей сети. Поэтому только технологии, основанные на механизме локальной безопасности, могут обеспечить эффективную защиту производственных мощностей или объектов, которые должны быть постоянно в работе.

Как брандмауэр Hirschmann EAGLE может решить эту проблему?

По умолчанию многопортовые брандмауэры EAGLE сконфигурированы для работы в прозрачном режиме (Transparent Mode) и для динамической проверки содержимого передаваемых пакетов (Stateful-Inspection). Таким образом, только данные, запрашиваемые изнутри, поступают в защищённую сеть.

В ранее упомянутом примере с Sasser при условии применения брандмауэра EAGLE червь не был бы передан через него, потому что порт 445 был бы недоступен. EAGLE может ограничить доступ к сети для конкретного IP-адреса или услуги, и при этом только авторизованные пользователи получают доступ к защищённой сети извне.

Программное обеспечение семейства брандмауэров EAGLE совместимо с различными службами безопасности: открытыми, промышленными или специального назначения, от глобального уровня управления до местного. С помощью разделения сети на зоны EAGLE обеспечивает комплексную защиту всех существующих и будущих приложений.

Обзор возможностей

Система безопасности промышленных сетей имеет свою специфику: уровень защиты должен быть выше, нежели используемый обычно в стандартной офисной среде. Такие решения предлагает компания Hirschmann, продукция которой в основном предназначена для промышленных применений. Кроме того, в результате вертикальной интеграции в перспективе всё больше и больше промышленных приложений будут разрабатываться для Ethernet.

Децентрализованная архитектура безопасности на базе семейства EAGLE вызывает особенный интерес при использовании в промышленных сетях, где требуется защита от случайных и неумышленных атак внутри сети:

- безопасный удалённый доступ к машинам (станки и печатающие устройства);

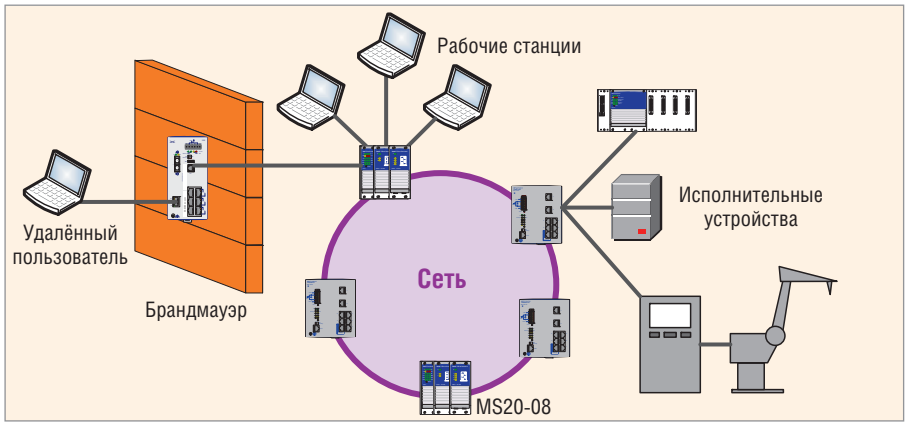

Рис. 1. Реализация защиты сервисного порта

- вход во внутреннюю сеть заводов (в том числе через незащищённый Интернет);
- работа в сети ветропарков (включая офшорные);
- разделение сети на сегменты в автомобильной промышленности и машиностроении. Фактически EAGLE, с одной стороны, дополняет существующие механизмы безопасности, включающие как брандмауэры, так и антивирусное ПО, а с другой стороны, представляет основу системы безопасности промышленного контура завода.

Система EAGLE – движущая сила безопасности компании

Решение на базе семейства EAGLE включает как линейку устройств для обеспечения безопасности приложений, так и средства операционной системы, систем управления и т.д. Преимуществами такого решения являются механизмы безопасности, которые могут быть разработаны с учётом требований конкретного проекта, тем самым обеспечивая более высокий общий уровень решения. При этом есть возможность реализовать защиту с точностью до сегмента или конечного устройства. Также стоит добавить, что EAGLE не имеет сложных списков доступа и правил брандмауэра, которые должны быть сохранены в магистральной сети, а удалённые входы в систему позволяют наблюдать и постоянно анализировать передачу данных.

Семейство брандмауэров EAGLE поддерживает механизмы резервирования Redundant Ring Coupling и Dual Homing – схемы дублированных соединений сегментов локальной сети, реализованных в управляемых коммутаторах Hirschmann.

Типовые режимы использования EAGLE

Рассмотрим типовые режимы использования семейства брандмауэров EAGLE:

- защищённый сервисный порт;
- защищённое разделение на подсети;
- безопасное соединение сетей;
- удалённый доступ через VPN-туннель.

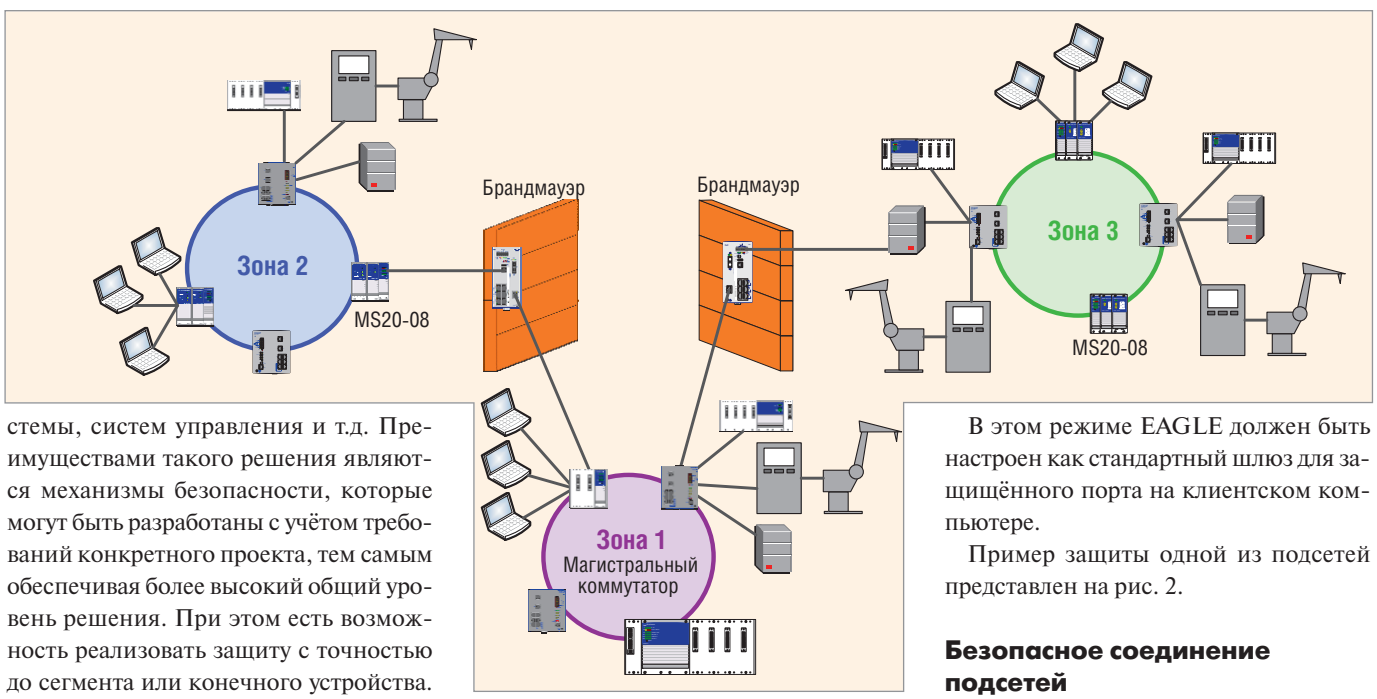

Рис. 2. Реализация защиты отдельной подсети

Далее приведём более подробное описание режимов и проиллюстрируем примеры применения каждого из них.

Защищённый сервисный порт

Безопасный доступ для первоначальной конфигурации или для внешних сотрудников осуществляется с помощью встроенного DHCP-сервера.

Перечислим сетевые режимы EAGLE: SCT (Single Client Transparency), MCT (Multi Client Transparency) или режим роутера.

- В режиме роутера EAGLE должен быть настроен как стандартный шлюз на защищённых портах клиентских компьютеров.
- Конфигурация EAGLE как DHCP-сервера: нужно ввести IP- и MAC-адреса на незащищённых портах.
- Необходимо определение правил брандмауэра для IP-адресов, предоставляемых DHCP-сервером.

Пример защиты сервисного порта представлен на рис. 1.

Защищённое разделение на подсети

Конфигурация 1: сетевой режим EAGLE – прозрачный многоклиентский режим (Multi Client Transparency mode).

- Использование в существующих сетях без изменения текущей IP-конфигурации.
- Создание правил брандмауэра для контроля доступа между магистральной сетью и зоной или между всеми зонами.

Конфигурация 2: сетевой режим EAGLE – режим роутера.

В этом режиме EAGLE должен быть настроен как стандартный шлюз для защищённого порта на клиентском компьютере.

Пример защиты одной из подсетей представлен на рис. 2.

Безопасное соединение подсетей

Конфигурация: сетевой режим EAGLE – режим роутера.

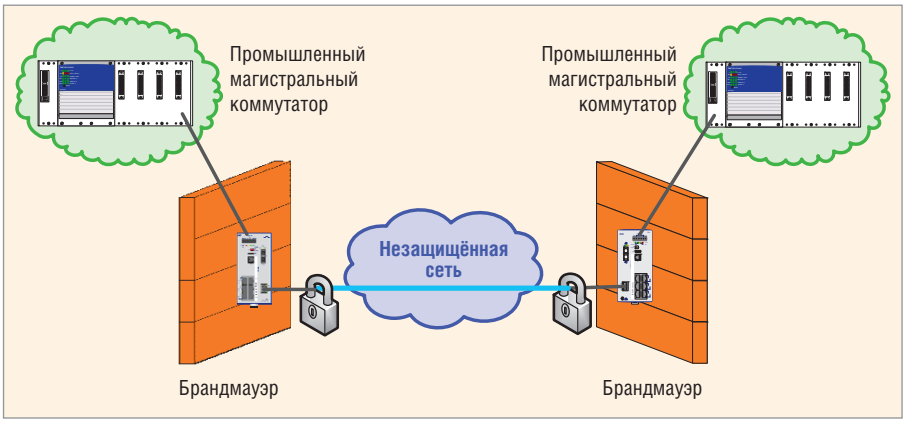

Рис. 3. Реализация защиты соединения между отдельными сетями

Конфигурация: сетевой режим EAGLE – прозрачный одноклиентский режим (single client transparency) или режим роутера.

- В режиме single client transparency для подключённого компьютера изменения настроек TCP/IP не требуется.
- В режиме роутера EAGLE должен быть настроен как стандартный шлюз для защищённого порта на клиентском компьютере.

Пример использования удалённого доступа через VPN-туннель представлен на рис. 5.

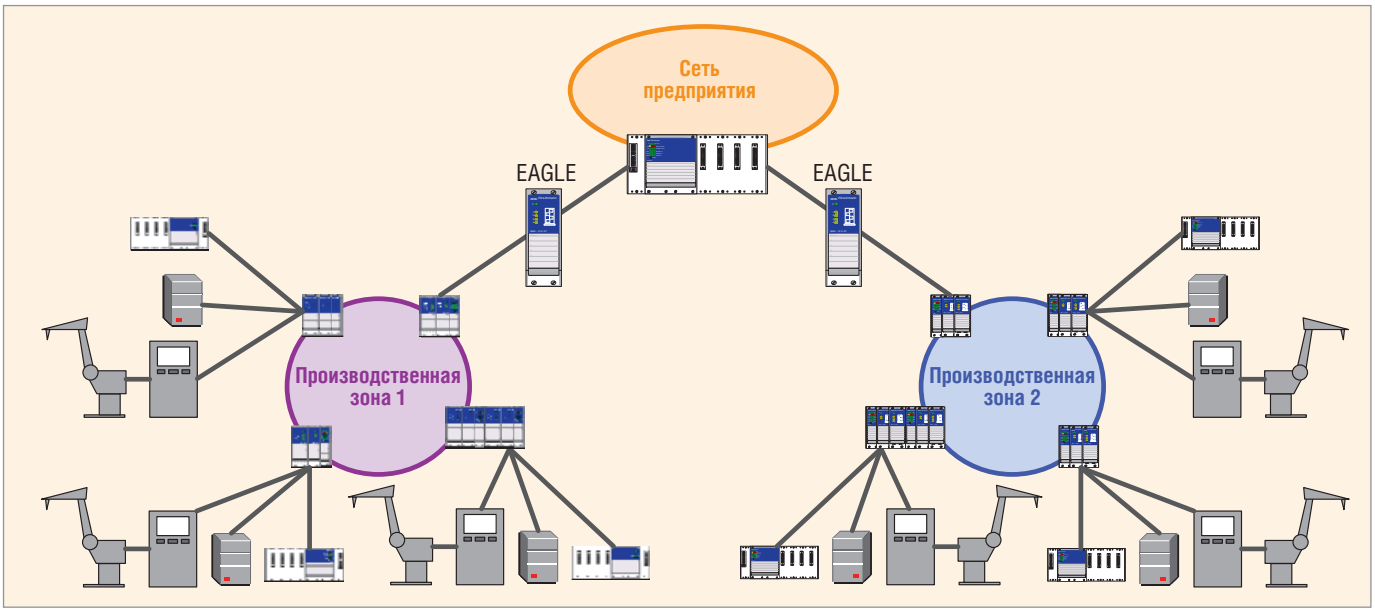

Рис. 4. Реализация защиты при использовании одинаковых сегментов сети

- В режиме роутера EAGLE должен быть настроен как стандартный шлюз для защищённого порта на клиентском компьютере.
- При использовании модема DSL необходимо настраивать параметры протокола Point-to-Point Protocol over Ethernet (PPPoE).

Пример защиты соединений между сетями представлен на рис. 3.

Обслуживание одинаковых сетевых сегментов с помощью 1:1 NAT

В некоторых специальных приложениях целесообразно настроить сетевые сегменты одинаково, даже использовать одни и те же IP-адреса. Для того чтобы это реализовать, необходима поддержка сетью механизма маскировки IP-адреса. EAGLE способен выполнять эти функции с помощью 1:1 NAT (Network Address Translation).

Одна из возможных конфигураций сети представлена на рис. 4.

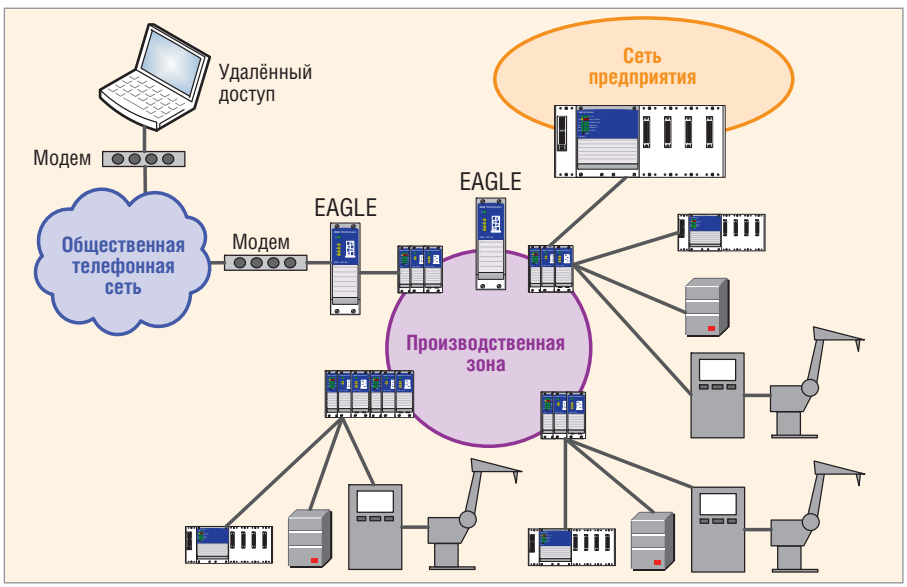

Рис. 5. Использование VPN-туннеля для получения удалённого доступа к сети

Удалённый доступ через интерфейс V.24 и внешний модем

На удалённом компьютере пользователя должна быть установлена ОС Windows 2000/XP, включающая в себя VPN-клиент.

Резервирование роутера с использованием VRRP

В крупных сетях, как правило, используются коммутаторы и маршрутизаторы третьего уровня OSI. Для добавления резервирования в маршрутизи-

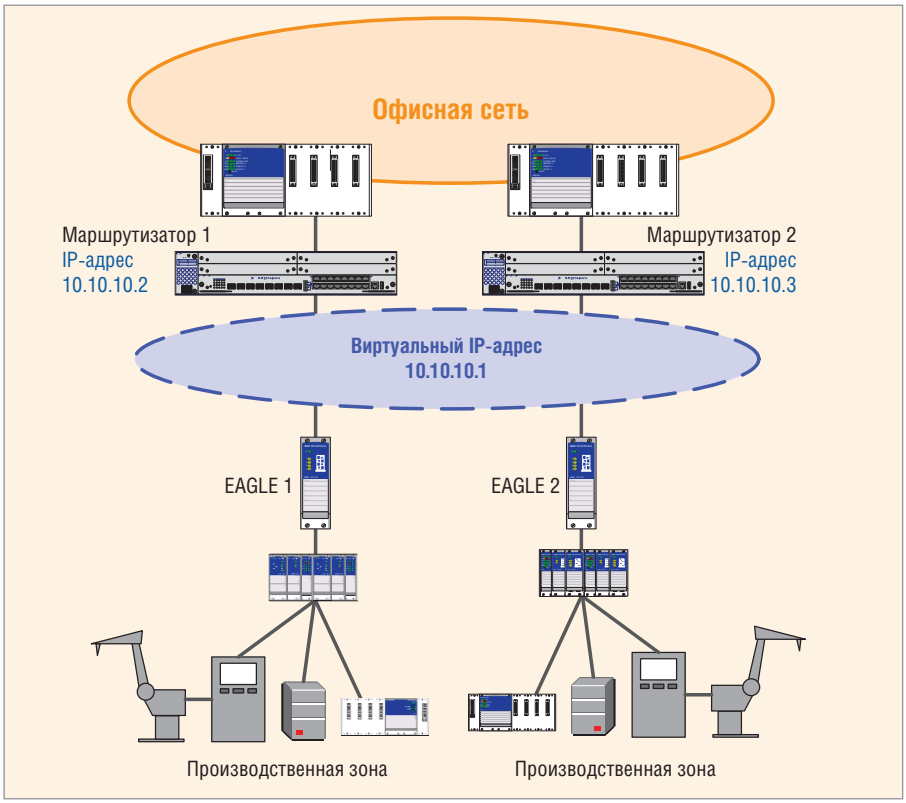

Рис. 6. Фрагмент сети третьего уровня OSI и реализация защиты в ней

руемых сетях принято использовать протокол Virtual Router Redundancy Protocol (VRRP). Повышение уровня безопасности в существующих сетях третьего уровня возможно средствами EAGLE, который также поддерживает VRRP.

Одна из возможных конфигураций сети уровня 3 представлена на рис. 6.

Центральное управление

В крупных сетях размеры подсетей и количество устройств EAGLE достаточно большое, и конфигурирование и особенно реконфигурирование параметров безопасности занимает много времени. Для того чтобы свести к минимуму такого рода усилия, есть возможность использования системы центрального управления ISCM (Innominate Security Configuration Management).

Пример использования системы ISCM представлен на рис. 7.

Обеспечение охраны с использованием световой сигнализации

Мигающая лампочка тревоги или предупреждающий маячок будет означать нарушение правил брандмауэра, то есть:

- попытку получения незаконного доступа (определяется по MAC- или IP-адресу);
- попытку использования запрещённого порта сети (например, использование протокола FTP, хотя брандмауэр запретил доступ).

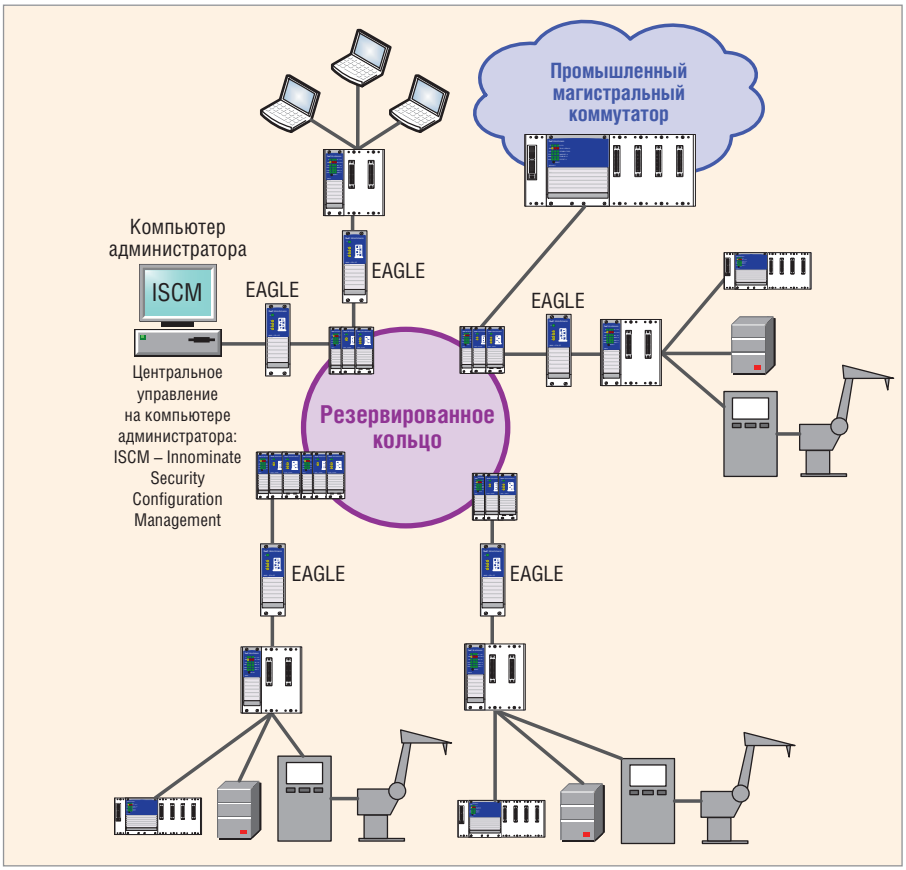

Рис. 7. Использование системы ISCM для конфигурирования параметров безопасности

одного из каналов ожидающий вторичный канал автоматически включается в работу, обеспечивая непрерывную связность в сети.

Конечный пользователь получает выгоду за счёт использования возможности резервирования топологии сети без необходимости перенастройки при добавлении оборудования сетевой безопасности. В случае если топология настроена как плоская L2-сеть, требовались бы огромные усилия, чтобы изменить архитектуру сети от L2 до L3.

Пример использования STP-резервирования представлен на рис. 9.

Заключение

Таким образом, серия Hirschmann EAGLE 20 несомненно повысит уровень безопасности компьютерной сети и поможет вывести информационную систему предприятия на качественно новый уровень. Она позволит облегчить масштабируемость смешанной сети за счёт применения модификаций моделей с самыми различными сочетаниями интерфейсов передачи данных по витой паре и оптическим каналам. А для интеграции на программном уровне не

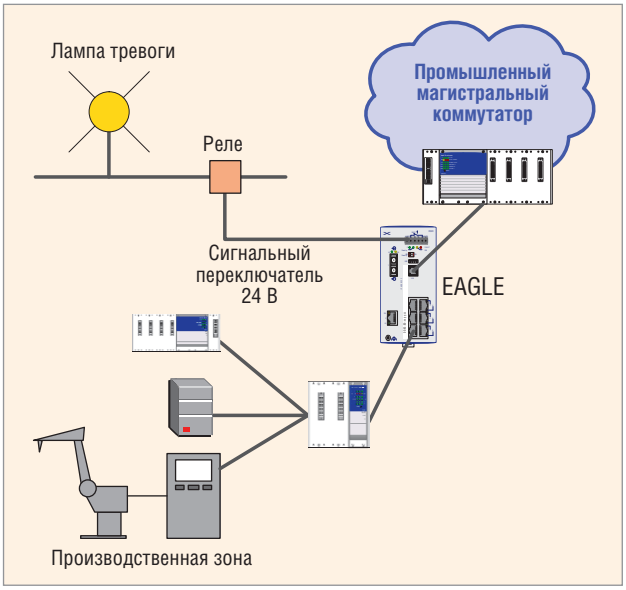

Рис. 8. Использование сигнального маячка для оповещения

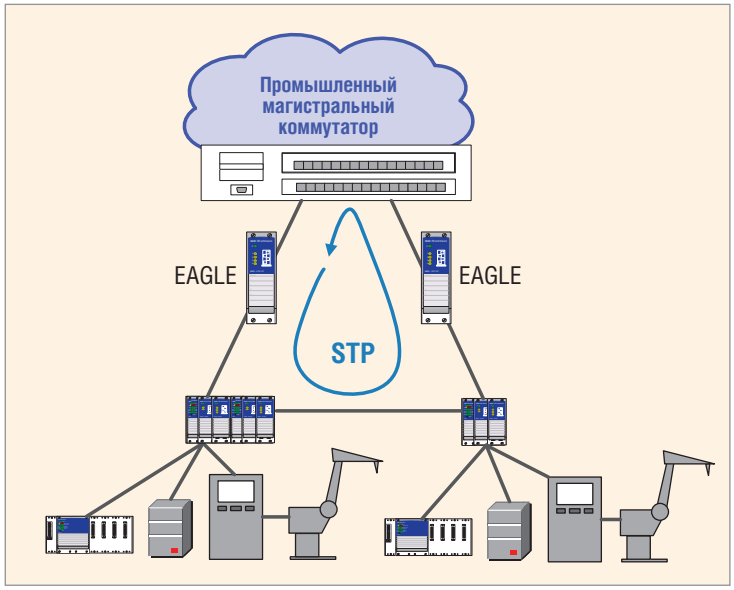

Рис. 9. Использование STP-резервирования

Реализация использования световой сигнализации в качестве оповещения о нарушении правил брандмауэра представлена на рис. 8.

Поддержка резервирования STP

Система EAGLE поддерживает STP-резервирование (Spanning Tree Protocol – протокол связующего дерева) благодаря BPDU (Bridge Protocol Data Unit, единица данных протокола управления сетевыми мостами). Таким образом исключается возможность возникновения петель в сетях передачи данных при наличии в них многосвязной топологии. Используя одну физическую либо логическую связь в качестве основной, BPDU удерживает одну из доступных вторичных связей в режиме бездействия (ожидания), поэтому полезный трафик передаётся только по одной из доступных связей. При нарушении функционирования придётся даже останавливать компьютерную сеть предприятия и менять сетевые адреса, интерфейсы удалённого управления и фирменное ПО сделают процесс администрировании более удобным. ●

Перевод Ивана Лопухова и Александра Цыганкова, сотрудников фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru