Безопасная беспроводная передача данных в системе МПЦ

В системе микропроцессорной централизации (МПЦ) EBI Lock 500, поставленной компании Duisburg Hafen (duisport), впервые внедрена система безопасной передачи данных по радиоканалам с использованием защитных шлюзов. Прежде в коммерческих проектах эта технология применялась только в европейской системе управления движением поездов ETCS.

Duisburg Hafen AG (duisport), в которую входит компания Duisburg Hafen Group, является оператором инфраструктуры и иных технических средств в порту Дуйсбурга. Кроме того, компания duisport — это системный поставщик рыночных логистических услуг. В настоящее время в портовой зоне располагаются более 200 компаний, которые занимаются логистикой и другой деятельностью, пользуясь услугами duisport. Для предоставления клиентам оптимальных транспортных путей компания Duisburg Hafen решила реорганизовать железнодорожную инфраструктуру на техническом и эксплуатационном уровнях, что повлекло за собой обновление устройств централизации.

Был объявлен тендер, который предусматривал обновление устройств централизации на пяти этапах строительных работ, а также устройство диспетчерского центра на территории нового центра логистики на левом берегу Рейна в Дуйсбург-Рейнхаузене.

Эта задача сравнительно легко решается при использовании системы МПЦ EBI Lock 500, если бы не исключительное географическое положение отдельных районов зоны действия централизации.

Соединение отдельных районов зоны действия МПЦ с новым диспетчерским центром требовало строительства удовлетворяющих требованиям безопасности линий дальней передачи данных, пересекающих акваторию Рейна и земельные участки, находящиеся в собственности третьих лиц. Использование существующих линий передачи не допускалось. В результате компания Bombardier приняла решение использовать для дальней передачи данных стандартную беспроводную локальную сеть, построенную на базе радиоканалов. Для защиты данных было решено использовать опыт реализации пилотного проекта внедрения европейской системы управления движением поездов ETCS, осуществленного в Швейцарии и предусматривавшего защиту данных при помощи криптографических алгоритмов.

Компания Bombardier получила право на заключение контрак-

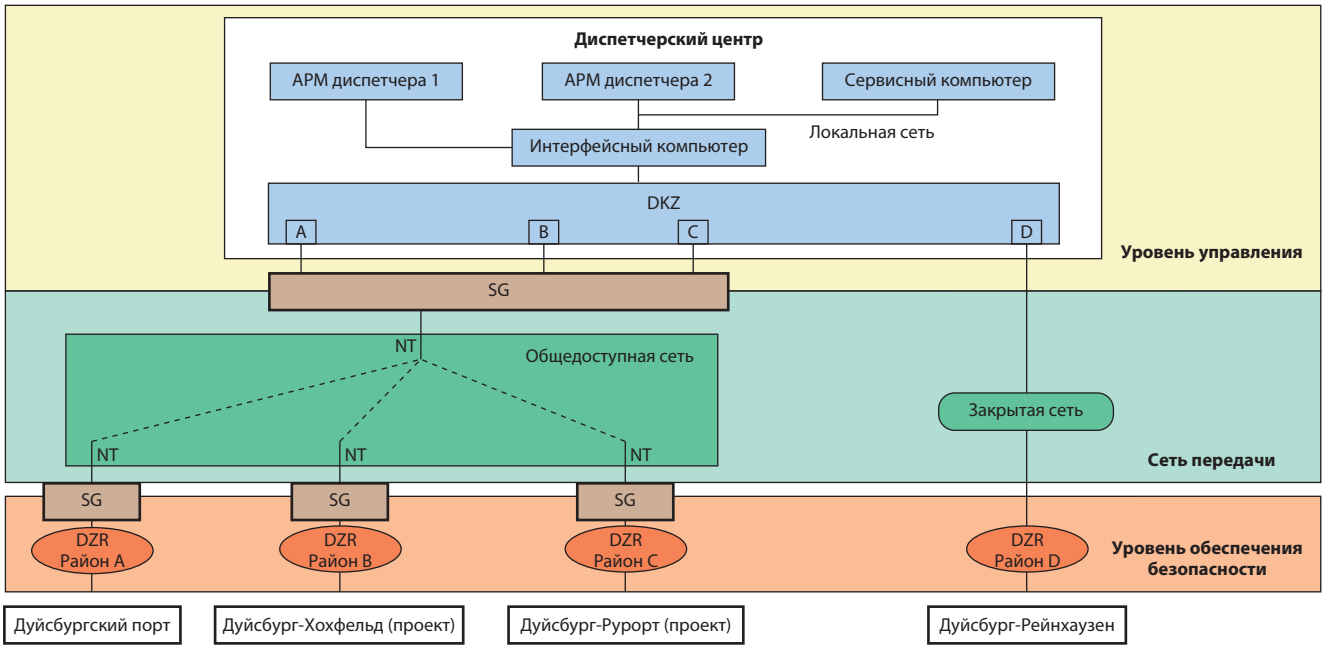

Рис. 1. Структура системы МПЦ железнодорожной сети компании duisport:
DKZ — концентратор данных; SG — защитный шлюз; DZR — децентрализованный компьютер; NT — сетевой терминал

та для реализации своего решения, и с 1 октября 2003 г. объект находится в промышленной эксплуатации. Ниже детально рассмотрена технология, выбранная для безопасной передачи данных по радиоканалам.

Описание системы

Система микропроцессорной централизации EBI Lock 500 (ее прежнее обозначение MCDS) компании Bombardier (рис. 1) базируется на модульной децентрализованной концепции, где каждый уровень безопасности включает в себя децентрализованный компьютер DZR. Совместно со специализированными объектными контроллерами ОС он берет на себя задачу безопасной обработки информации.

Соединение каждого уровня безопасности с распорядительным постом МПЦ осуществляется через концентратор данных DKZ. Для управления и наблюдения за районами зоны действия МПЦ используется одно (или в качестве опции — два) автоматизированное рабочее место оператора.

Соединение между уровнями безопасности EBI Lock 500 и диспетчерским центром обеспечивается посредством специализированных интерфейсных модулей в компьютерах DKZ и DZR. Эти интерфейсные модули рассчитаны на безопасную передачу данных через закрытые и общедоступные сети. Передача данных по общедоступным сетям должна сопровождаться шифрованием для гарантирования надлежащей защиты доступа к ответственным приложениям, поэтому между специализированными модулями и сетевыми терминалами NT общедоступной сети устанавливают защитные шлюзы SG.

В данном случае в качестве сетевого терминала используется система беспроводной локальной сети. В ней применен направленный радиорелейный мост компании Cisco, обеспечивающий прозрачную связь с сегментом сети Ethernet. Скорость передачи данных достигает 1 Мбит/с.

EBI Lock 500 с защитным шлюзом

Задача защитного шлюза состоит в том, чтобы обеспечивать только разрешенный доступ к безопасным компьютерам DKZ и DZR. Защита доступа основана на требованиях стандарта EN 50159. Ответственные данные перед передачей по общедоступной сети шифруются посредством криптографического алгоритма, а после передачи дешифруются.

В качестве алгоритма шифрования используется Triple-DES (TDES). Защитный шлюз работает с 192-разрядным ключом KTDES, состоящим из трех отдельных ключей длиной по 64 бита. Таким образом, длина собственно ключа составляет 168 бит, еще 24 бита (3×8 бит) являются контрольными.

Для шифрования и дешифрования применяется криптографическая платформа собственной разработки компании Bombardier —плата GCD (рис. 2), содержащая специальный крипточип. Аналогичный крипточип Bombardier использует в своих разработках в области ETCS, где в соответствии с требованиями системы Euroradio плата GCD выполняет MAC-вычисления.

Крипточип соответствует высоким требованиям, предъявляемым к криптографической защите. Считать с него криптографический ключ и информацию о пользовательских настойках нельзя механическими, химическими, оптическими или электрическими способами.

Защитный шлюз SG выполнен в виде стандартного 19-дюймового промышленного компьютера с 32-разрядной операционной системой. Он оборудован соответствующими последовательными интер-

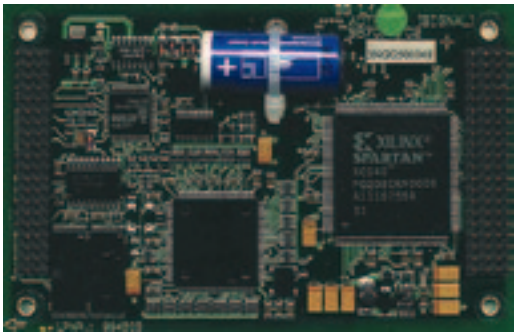

Рис. 2. Криптографическая платформа защитного шлюза

фейсами для связи с DKZ или DZR. Соединение с общедоступной сетью осуществляется через интерфейс Ethernet IEEE802.3 со скоростью 10/100 Мбит/с.

Программное обеспечение защитного шлюза подразделяется на коммуникационные модули COM и UDP, модули обеспечения безопасности SEC и диагностики DIA (рис. 3). Эти модули реализованы в качестве служб. Программное обеспечение не требует обслуживания. Для ввода в эксплуатацию предусмотрены диагностические инструменты. Настройка ПО осуществляется через файлы инициализации, а также непосредствен-

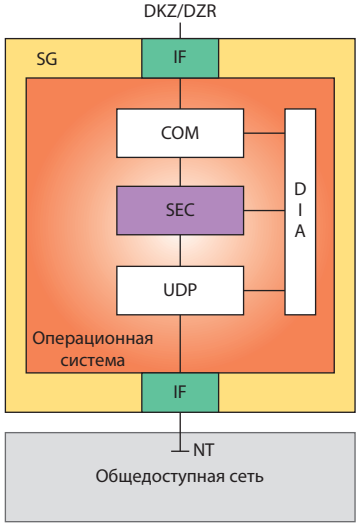

Рис. 3. Архитектура программного обеспечения защитного шлюза системы EBI Lock 500:
DKZ — концентратор данных; DZR — децентрализованный компьютер; SG — защитный шлюз; COM, UDP — коммуникационные модули; SEC — модуль обеспечения безопасности; DIA — модуль диагностики; NT — сетевой терминал

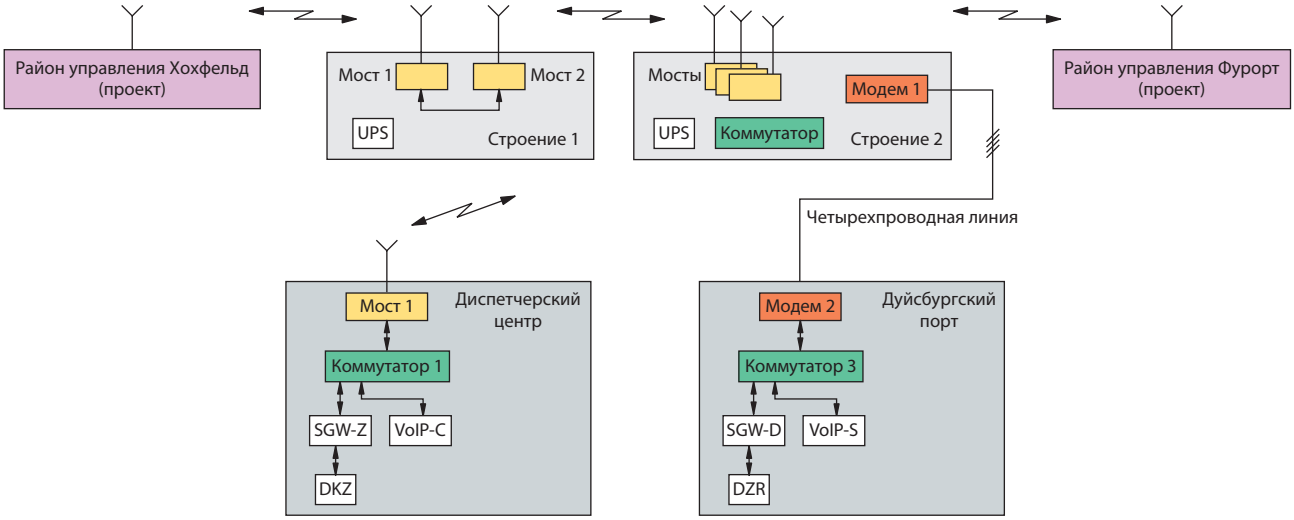

Рис. 4. Топология открытой сети EBI Lock 500:
DKZ — концентратор данных; DZR — децентрализованный компьютер; SGW-Z и SGW-D — защитные шлюзы; UPS — источник бесперебойного питания

Рис. 5. Устройство сети WLAN, рассчитанное на наружную установку

но в реестре операционной системы. В рабочем режиме никаких действий оператора не требуется. Администрирование осуществляется при входе под соответствующей учетной записью. Программное обеспечение защищено от изменений с помощью технических процедур.

Персонификация и управление ключами осуществляется через два транспортных протокола KTRANS1 и KTRANS2, учитывающих особенности ключей KTDES.

Для каждого соединения между компьютерами DKZ и DZR должен быть сгенерирован отдельный ключ KTDES.

Общедоступная сеть передачи

Защитный шлюз системы EBI Lock 500 может быть сконфигурирован для доступа к общедоступным сетям ISDN, GSM, WAN, WLAN (рис. 4). В настоящее время именно технология WLAN предоставляет новые эффективные возможности объединения в единую сеть исполнительного уровня МПЦ и уровня управления.

Хотя процедуры, применяемые в сети WLAN, могут быть использованы для ограничения доступа посторонних лиц к радиоканалу, адекватная защита может быть достигнута только применением стандартизованных криптографических методов с безопасным использованием шифровальных ключей. Эта технология реализуется при помощи защитного шлюза системы EBI Lock 500.

В дополнение к передаче ответственных данных между DKZ и DZR предусмотрено дистанционное управление средствами технологической радиосвязи (локомотивными радиостанциями) из диспетчерского центра. Для этого применяется технология передачи речи по протоколу IP (Voice over IP). Эта система объединена с существующей в диспетчерском центре инфраструктурой беспроводной передачи данных через WLAN (рис. 5).

Перспективы

Защитный шлюз реализует безопасную передачу данных через общедоступные сети (по так называемому серому каналу), открывая новые возможности для приложений в области систем СЦБ. Используемая при этом среда передачи данных не имеет значения.

Линия направленной радиосвязи хорошо зарекомендовала себя в эксплуатации. Безопасную передачу данных при помощи направленной радиосвязи и методов шифрования можно использовать в качестве недорогого технического решения на местности со сложными топографическими условиями или при наличии соответствующей инфраструктуры радиосвязи.

K. Busse, F. Felten. Signal und Draht, 2005, S. 10 – 12.