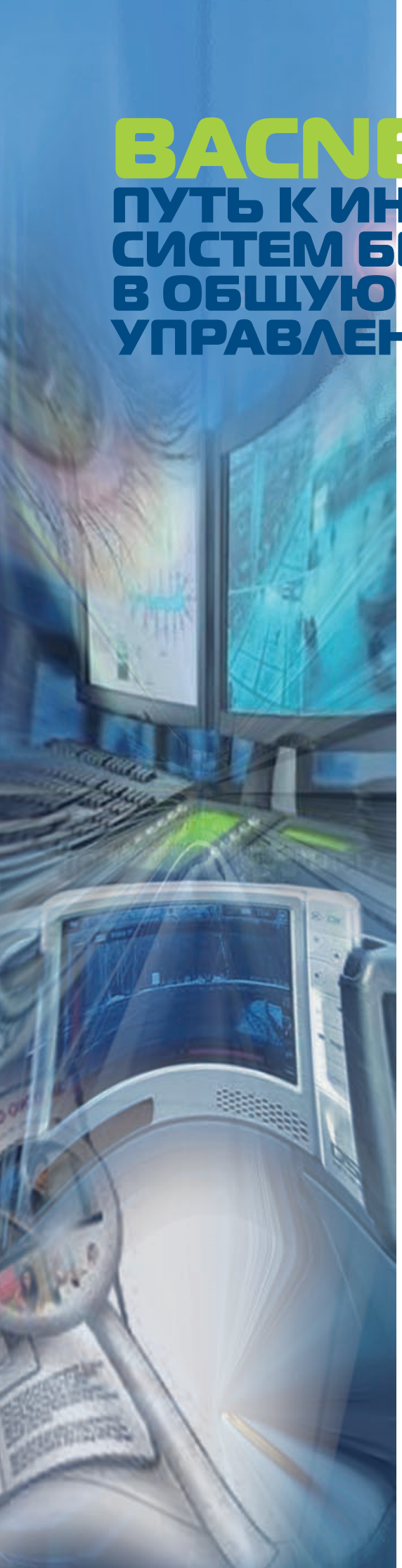


BACNET
ПУТЬ К ИНТЕГРАЦИИ СИСТЕМ БЕЗОПАСНОСТИ В ОБЩУЮ СИСТЕМУ УПРАВЛЕНИЯ ЗДАНИЕМ

С. Лёвин
главный конструктор НПФ «Сигма-ИС»

ВВЕДЕНИЕ

BACnet – это открытый протокол автоматизации и управления зданием, разработанный в ASHRAE (Американское общество инженеров систем отопления, вентиляции и кондиционирования). Протокол предназначен для обеспечения совместной работы таких инженерных систем здания, как отопление, вентиляция и кондиционирование, управление освещением, контроль и управление доступом, пожарная сигнализация. BACnet предоставляет механизмы, с помощью которых оборудование с любым функционалом может обмениваться информацией независимо от своей специфики. В результате протокол BACnet успешно может использоваться в компьютерах верхнего уровня, программируемых логических контроллерах общего назначения, а также специализированных прикладных контроллерах.

Предпосылками для создания подобного стандарта стало всеобщее желание владельцев зданий и системных интеграторов получить интероперабельные решения, то есть возможность интегрировать оборудование от различных производителей в согласованную систему автоматизации и управления. Для достижения этой цели комитет по стандартизации ASHRAE запросил и получил данные от десятков заинтересованных компаний и экспертов, рассмотрел схожие национальные и международные стандарты по обмену данных. Было затрачено огромное количество сил и времени на обсуждение каждого элемента протокола.

Из всего этого родилась модель сетевого протокола со следующими принципиальными характеристиками:

- Все сетевые устройства равноправны[1], то есть нет выделенного сервера, но некоторые имеют большие привилегии и ответственность, чем другие.
- Каждое сетевое устройство представлено как набор сетевых именованных сущностей, называемых объектами. Каждый объект характеризуется набором атрибутов или свойств. Стандарт описывает большинство широко применяемых типов объектов и их свойств, при этом, если необходимо, имеется возможность свободного создания дополнительных объектов. Так как объектная модель может легко расширяться, это дает возможность протоколу развиваться с сохранением обратной совместимости, что крайне важно, так как технология и оборудование постоянно совершенствуются и изменяются.
- Обмен данными производится путем чтения и записи свойств отдельных объектов через передачу сообщений и взаимного выполнения других служб (сервисов) протокола. BACnet предоставляет необходимый набор служб, кроме того, существуют механизмы для создания дополнительных сервисов непосредственно пользователями протокола, если это необходимо.
- Так как стандарт придерживается концепции уровневой коммуникационной архитектуры, одни и те же сообщения могут передаваться с использованием различных сетевых методов доступа и физических сред. Это означает, что BACnet сети могут быть сконфигурированы с различными требованиями к пропускной способности и соответственно к стоимости. Множество BACnet сетей могут быть объединены в одной большой системе с организацией межсетевой работы. Такая гибкость предоставляет возможность BACnet поддерживать новые сетевые технологии по мере их появления.

BACnet показал себя как изящная и развивающаяся компьютерная технология и изменил требования к системам автоматизации зданий. Впервые протокол был опубликован в 1995 году. Сейчас уже многое изменилось с момента первого обнародования стандарта – BACnet стал по-настоящему глобальным. BACnet устрой-

[1] За исключением ведомых устройств при использовании физического уровня MS/TP – будет рассмотрено позднее.

ства разрабатываются, производятся и внедряются на всех континентах. Предложения для расширений и улучшений постоянно принимаются, обрабатываются и проходят полный набор обсуждений и утверждений для включения в официальный стандарт.

В настоящее время в стандарт добавлено большое количество новых функций: возможность для объединения систем через глобальные сети с использованием Интернет-протоколов, добавлены новые объекты и сервисы для поддержки систем пожарной сигнализации и контроля доступа, что делает BACnet привлекательным для разработчиков и интеграторов в области систем безопасности.

ОБЪЕКТЫ BACNET

Как уже говорилось выше, сетевые устройства в BACnet представлены как наборы объектов. Каждый объект описывает тот или иной источник данных в системе или объект управления. Таким образом, можно считать, что объект – это основная сущность BACnet. В настоящее время протокол поддерживает всеобъемлющий набор объектов для описания общеинженерных систем, а также, что наиболее интересно для нас, ряд специальных объектов для систем безопасности, прежде всего для пожарной сигнализации и систем контроля и управления доступом.

В качестве примера объектов общего назначения можно привести следующий список:

- дискретный вход;
- дискретный выход;
- аналоговый вход;
- аналоговый выход;
- вход со многими состояниями;
- выход со многими состояниями;
- календарь;
- файл;
- программа;
- расписание;
- .....

Специальные объекты для систем безопасности, для исключения неправильной интерпретации привожу оригинальные названия:

- Life Safety Point Object Type – описывает извещатель (датчик) или исполнительное устройство системы безопасности;
- Life Safety Zone Object Type – описывает группу датчиков или зоны системы безопасности;
- Access Door Object Type – описывает оборудование двери в СКУД (замок, дверной контакт, кнопка запроса на выход);
- Access Point Object Type – описывает точку доступа в СКУД (дверь, калитка, турникет и т.п.);
- Access Zone Object Type – описывает зону доступа в СКУД;
- Access User Object Type – описывает пользователя СКУД;
- Access Right Object Type – описывает права пользователя СКУД;
- Access Credential Object Type – описывает идентификаторы пользователя СКУД (проксимити-карта, пинкод и т.п.);
- Credential Data Input Object Type – описывает устройство считывания, идентификаторы пользователя СКУД (считыватель карт, клавиатура, биометрический считыватель и т.п.).

С помощью этих объектов можно описать практически любой объект системы безопасности, будь то пожарная или охранная сигнализация, а также СКУД.

СЕТЕВАЯ АРХИТЕКТУРА ПРОТОКОЛА BACNET

Сетевая архитектура протокола базируется на хорошо известной модели OSI (Open System Interconnection – взаимодействие открытых систем). Эта модель описана в стандарте ISO 7498 и призвана решить задачу межкомпьютерного обмена данными и разбивает эту, вообще говоря, очень сложную задачу на 7 более простых, каждая из которых выполняет свою специфичную коммуникационную функцию. Каждая такая подзадача формирует уровень в архитектуре сетевого протокола.

BACnet базируется на сокращенной 4-уровневой архитектуре, что соответствует физическому, канальному, сетевому и прикладному уровням общей модели OSI. Прикладной и сетевой уровни определяются стандартом BACnet. Для канального и физического уровня BACnet предоставляет 7 вариантов реализации, что определяет возможность использования протокола поверх существующих коммуникационных технологий.

Сокращенная 4-уровневая архитектура была выбрана после тщательного рассмотрения конкретных функциональных возможностей и требований к сети, включая ограничения к накладным расходам, так как протокол должен быть как можно компактнее.

ТОПОЛОГИЯ СЕТИ BACNET

Для обеспечения гибкости при построении сети BACnet не предписывает жесткую топологию. BACnet устройства физически могут быть подключены к одному из четырех типов локальных сетей либо через выделенные или коммутируемые последовательные асинхронные каналы связи. Эти сети могут быть объединены вместе через BACnet маршрутизаторы.

В терминах топологии сетей каждое BACnet устройство подключено к среде передачи или физическому сегменту. BACnet сегмент содержит один или несколько физических сегментов, подключенных на физическом уровне через по-

Табл. 1. Сетевые уровни модели OSI

Уровень	Функции
Прикладной	Реализует интерфейс с пользовательским приложением
Представления	Кодирование/декодирование, конвертирование данных
Сеансовый	Управление сеансом связи, синхронизация передачи данных
Транспортный	Обеспечивает передачу данных между двумя узлами, сегментацию данных и коррекцию ошибок
Сетевой	Установление логической связи, адресация и маршрутизация между двумя узлами сети
Канальный	Управление доступом к физической среде передачи
Физический	Передача и прием двоичных данных в физической среде передачи

Табл. 2. Варианты реализации канального и физического уровней BACnet

Вариант	Канальный уровень	Физический уровень
1	ISO 8802-2 Type 1 (связь без установления соединения)	ISO 8802-3 MAC (Ethernet)
2	ISO 8802-2 Type 1 (связь без установления соединения)	ATA 878.1 (ARCNET)
3	Master-Slave/Token-Passing (MS/TP)	EIA-485 (RS-485)
4	Point-To-Point соединение	EIA-232 (RS-232)
5	LonTalk – протокол компании Echelon, используемый при построении сетей LonWorks	
6	BACnet Virtual Link Layer (BVLL)	UDP/IP (BACnet/IP)
7	BACnetZigBee Data Link Layer (BZLL)	ZigBee

вторители. BACnet сеть содержит один или несколько сегментов, объединенных через мосты (устройства, которые подключают сегменты на физическом и канальном уровнях и могут осуществлять фильтрацию сообщений на уровне MAC-адресов). Сеть образует простой домен MAC-адресов. Несколько сетей, возможно построенных на различных сетевых технологиях, могут быть объединены через BACnet маршрутизаторы, образуя при этом BACnet «межсеть» (internetwork).В BACnet межсети может существовать только один маршрут передачи сообщения между двумя узлами.

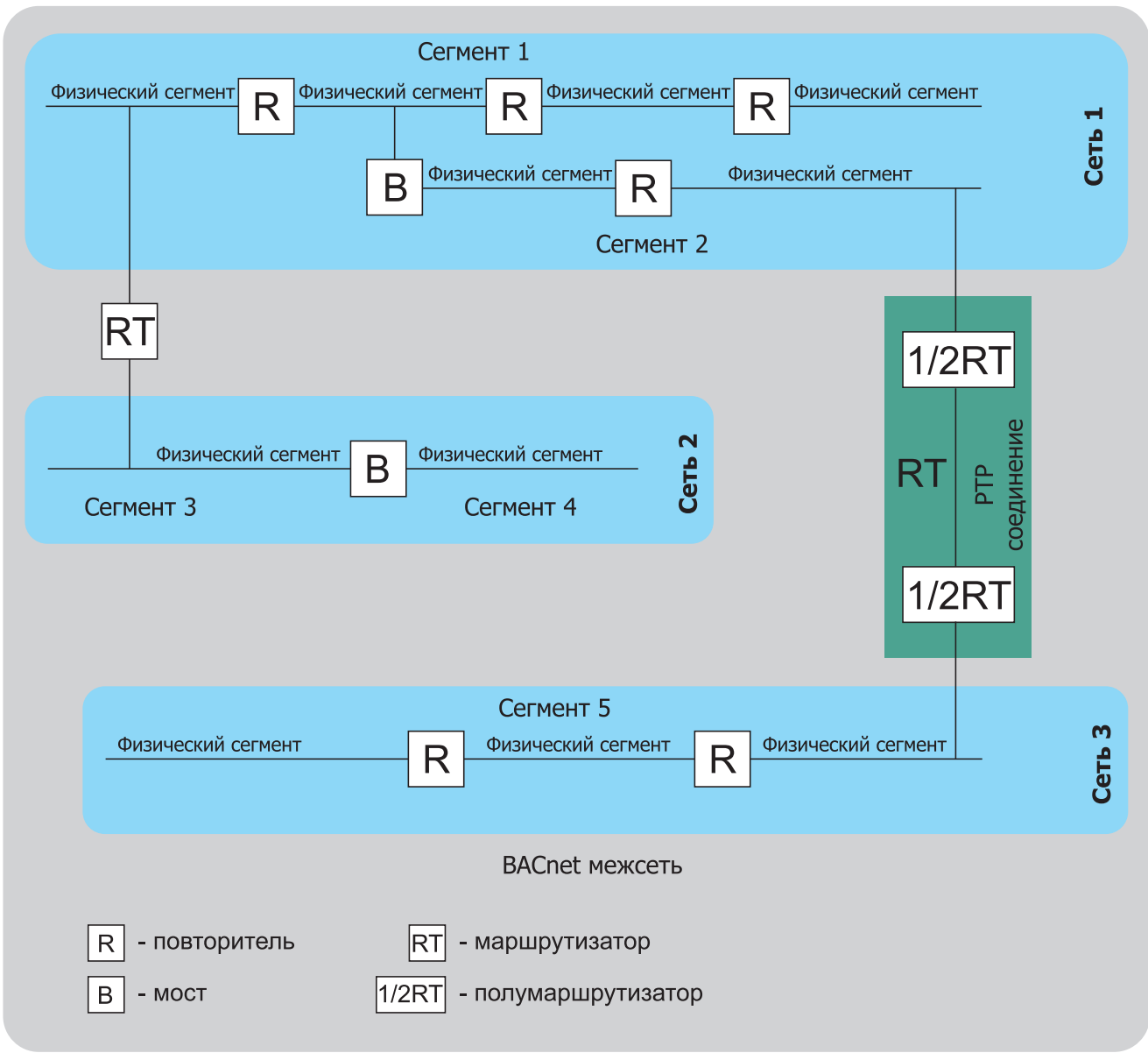
БЕЗОПАСНОСТЬ СЕТИ BACNET

Основные угрозы безопасности для сети – это случайное или преднамеренное изменение конфигурации устройств или управляющих параметров. Проблемы в основном исходят со стороны компьютеров верхнего уровня, которые находятся за рамками самого сетевого протокола. Одно из самых важных мест, определяющих безопасность, является человеко-машинный интерфейс (HMI – Human Machine Interface). Так как HMI не является частью коммуникационного протокола, задача защиты доступа со стороны человека с помощью паролей, протоколирование действий оператора и другие меры предосторожности отдаются на откуп производителям оборудования и разработчикам систем управления. В дополнение, доступ к записи любого свойства не ограничивается только требованием доступности свойства на запись. Стандарт может ограничивать изменения свойств только в виртуальном терминальном режиме или полностью. Это дает возможность производителям защищать ключевые свойства с помощью специального защитного механизма.

Сам протокол предоставляет возможности по аутентификации устройств, ограничению видимости данных и аутентификации пользователей. В целом требования к процедурам, обеспечивающим сетевую безопасность BACnet, могут быть сформулированы в следующем виде:

- применимость процедур для всех физических сред (Ethernet, MS/TP и т.д.);
- применимость процедур для всех типов BACnet устройств (конечные устройства, маршрутизаторы и т.д.);
- применимость процедур для всех типов сообщений (широковещательные, адресные, с подтверждением, без подтверждения);
- применимость процедур для всех сетевых уровней (физически-канальный, сетевой и прикладной);
- размещение незащищенных устройств позади защитного прокси-файрвол маршрутизатора;
- размещение защищенных устройств в незащищенных сетях.

Для достижения должного уровня сетевой безопасности стандарт BACnet имеет механизм защищенных сообщений на сетевом уровне. Специализированные стандарты по сетевой безопасности, такие как IPsec или Kerberos, были разработаны для



работы только в TCP/IP сетях и поэтому не отвечают всем изложенным выше требованиям. Тем не менее архитектура сетевой безопасности BACnet была разработана с учетом опыта применения и возможностей этих стандартов, что позволило выполнить все указанные требования.

ЗАЩИТНЫЙ УРОВЕНЬ

Функциональность сетевой безопасности добавлена в стек BACnet как набор сообщений сетевого уровня. В сущности, это не является явным уровнем безопасности, тем не менее при обсуждении работы механизмов безопасности для простоты понимания можно выделить это в самостоятельный уровень. Для этой цели механизмы безопасности и связанные с ними сообщения показываются как уровень безопасности или защитный уровень, тогда как фактически это часть сетевого уровня.

ОБЩИЕ КЛЮЧИ

Модель безопасности BACnet основана на использовании общих и секретных ключей. Аутентификация устройств и пользователей реализуется с помощью цифровой подписи сообщений и общих ключей подписи. Ограничение видимости данных достигается через шифрование защищаемой информации и общие ключи шифрования.

В BACnet ключи всегда распределяются как пары ключей, где одна половина – это ключ подписи, а вторая половина – это ключ шифрования. Существует 6 типов пар ключей: «Общий сетевой доступ», «Аутентификация пользователя», «Приложение», «Инсталляция», «Распределение» и «Мастер-устройство».

ЗАЩИЩЕННЫЕ СООБЩЕНИЯ

Особенность работы защитного уровня заключается в том, что информация передается через защищенные сообщения. Обычные BACnet сообщения помещаются внутри защищенного сообщения, которое является оберткой для пользовательских данных. Каждое защищенное сообщение имеет цифровую подпись, основанную на алгоритмах HMAC, MD5 или SHA-256. В базовом уровне безопасности защищаются адреса отправителя и получателя, идентификатор сообщения, а также метка времени. Эти меры позволяют защитить сообщения от подмены или перенаправления. Идентификатор сообщения (Message ID) выполняет несколько функций в защищенном BACnet сообщении. Он используется для детекции повтора сообщения, однозначного связывания защищенного ответа с защищенным запросом и вместе с меткой времени обеспечивает изменяемость сообщения. Метка времени (Timestamp) используется в основном для предотвращения повторов сообщений, но также еще и служит как источник изменяемости данных сообщения, поэтому, когда сообщения часто повторяются, новое значение метки времени не позволяет получить одинаковое значение цифровой подписи. Понятно, что часы защищенных устройств для этого должны быть синхронизированы. Если метка времени в сообщении выходит за границы защитного временного окна, будет выдана ошибка приема. Внутри защитного временного окна проверяется идентификатор сообщения для подтверждения того, что сообщение не было повторено. Самый высокий уровень безопасности предусматривает шифрование BACnet сообщения таким образом, что содержимое сообщения не может быть определено без наличия соответствующего ключа. Даже длина сообщения может быть скрыта путем использования дополняющего заполнения данных пакета.

В следующих номерах журнала мы продолжим обсуждение этой темы.

ЕЖЕГОДНЫЙ СЛЕТ «ПРОФИ КЛУБА»

Празднование дня рождения «Систем Сенсор» стало доброй традицией и самым любимым праздником в году не только для сотрудников компании, но и для приглашенных гостей.

Ощущение праздника витало в воздухе, коллектив фирмы старался поддерживать эту атмосферу: торжественность, улыбки, душевная теплота. На празднование были приглашены друзья, коллеги, партнеры, клиенты и конкуренты фирмы – все те, кто на протяжении этих лет были рядом.

По прибытии состоялся турнир по пейнтболу между двумя командами. Гости, которые остались вне зоны игры, активно болели и переживали как на чемпионате. Мероприятие прошло в спортивной и дружественной атмосфере, и победила, как всегда, дружба.

Чтобы восстановить потраченные на площадках игроками и болельщиками силы, по окончании мероприятия был организован банкет. Громкие и торжественные тосты смешивались с веселыми и музыкальными поздравлениями. В дружеской атмосфере под звон бокалов гости говорили самые теплые слова в адрес компании.

Ключ к успеху компании на рынке – внимание к нуждам заказчика, что позволяет разрабатывать и изготавливать продукцию, адаптированную к нуждам конкретного клиента.

В ближайших планах компании – дальнейшее развитие производственной базы и расширение модельного ряда выпускаемой продукции.

Уже есть новые интересные проекты и направления деятельности, которые, как и вся работа компании, нацелены на расширение ассортимента и повышение качества предлагаемой продукции.

Компания «Систем Сенсор Фаир Детекторс» – это всегда движение вперед.