ОСРВ QNX — выбор, проверенный временем

Александр Кузнецов, преподаватель учебного центра SWD Software

Название операционной системы QNX, как правило, хорошо знакомо разработчикам АСУТП, встраиваемых систем, интеллектуальных устройств и телекоммуникационного оборудования. В этом нет ничего удивительного, поскольку технологии канадской компании QNX Software Systems на протяжении почти 30-ти лет успешно внедряются по всему миру в самых разнообразных областях — от медицинских приборов до систем управления Международной космической станции.

Задача, которую ставили перед собой разработчики операционной системы реального времени (ОСРВ) QNX, формулируется следующим образом: «Основным назначением QNX Neutrino является реализация программного интерфейса POSIX в масштабируемой отказоустойчивой форме, подходящей для широкого круга открытых систем начиная от небольших встроенных систем с ограниченными ресурсами и заканчивая крупными распределенными вычислительными средами» [1].

Фундаментальным свойством ОСРВ QNX, отличающим ее от подавляющего большинства UNIX-систем, является микроядерная архитектура. В ней есть лишь два обязательных компонента — само микроядро и менеджер процессов. Менеджер процессов отвечает за управление процессами и защиту памяти, а микроядро — за диспетчеризацию, межпроцессное взаимодействие и прием прерываний от аппаратуры. Все остальные компоненты — это независимые друг от друга процессы, которые работают в защищенных адресных пространствах и взаимодействуют друг с другом через механизмы микроядра. Микроядро предоставляет всем процессам единый интерфейс, поэтому граница между системным и прикладным ПО условна: системные программы предоставляют определенные сервисы, а прикладные программы используют их (см. рис. 1).

Соответствие стандарту POSIX делает ОСРВ QNX внешне похожей на другие многочисленные POSIX-системы (согласно данным интернет-энциклопедий [2], существует около 20-ти полностью POSIX-совместимых ОС, еще более 10-ти имеют высокую степень совместимости). Это позволяет относительно легко переносить программы из других POSIX-систем в QNX, а также привлекать к разработке ПО специалистов, знакомых с этими системами. Первая сертификация ОСРВ QNX на соответствие стандарту POSIX прошла в 1993 г., а в начале 2008 г. QNX Neutrino получила сертификат POSIX PSE52, который гарантирует не только переносимость исходного кода, но и предсказуемость времени отклика, требуемую в строго ограниченных во времени приложениях.

Операционные системы QNX обеспечивают жесткое реальное время благодаря механизму диспетчеризации с вытеснением. Единицей диспетчеризации в ОСРВ QNX версии 4 является процесс, а в ОСРВ QNX Neutrino (версия 6) — поток. Фундаментальный принцип диспетчеризации в ОСРВ QNX состоит в том, что в каждый момент времени работает процесс/поток с наивысшим приоритетом; кроме того, обработчики прерываний имеют приоритет выше, чем у любого процесса/потока. Если при выполнении текущей задачи возникает задача с более высоким приоритетом, текущая задача вытесняется. Задержки диспетчеризации и прерывания ограничены, поэтому операционная система обеспечивает предсказуемое время запуска кода, ответственного за реакцию на событие.

Еще одной фундаментальной характеристикой ОСРВ QNX является надежность. Надежность системы тем выше, чем реже в ней происходят сбои и чем быстрее восстанавливается ее работоспособность. Для продления безостановочной работы системы ОСРВ QNX Neutrino обеспечивает механизм «горячей» замены программных компонентов. Сервис может предоставляться двумя или более компонентами (т.н. администраторами ресурсов), один из которых регистрируется как основной, а остальные — как резервные. В случае отказа основного администратора ресурса запрос клиента автоматически перенаправляется резервному, при этом ни клиент, ни администраторы ресурса не содержат какого-либо специального кода. Для сокращения времени восстановления применяются дополнительные технологии: комплект высокой готовности (High Availability Toolkit), адаптивное квотирование (Adaptive Partitioning) и мгновенная активация устройств (Instant Device Activation).

Комплект высокой готовности включает в себя сторожевой процесс и программный интерфейс для управления им. Сторожевой процесс наблюдает за заданными процессами и при соблюдении заданных условий (например, «процесс уничтожен» или «процесс перезапущен») выполняет заданные действия (например, «перезапустить», «зафиксировать в журнале», «передать уведомление»). Возможность автоматического перезапуска процессов при сбоях является мощным средством повышения коэффициента готовности системы.

Технология адаптивного квотирования применяется для защиты системы от монопольного захвата ее ресурсов каким-либо процессом. В настоящее время реализовано квотирование процессорного времени и оперативной памяти. Суть квотирования состоит в том, что процессы распределяются по нескольким разделам и каждому разделу назначается квота — доля защищаемого ресурса. Процессы делят квоту своего раздела между собой, а «излишки», если они возникают, динамически распределяются между другими разделами. Адаптивное квотирование предотвращает некоррект-

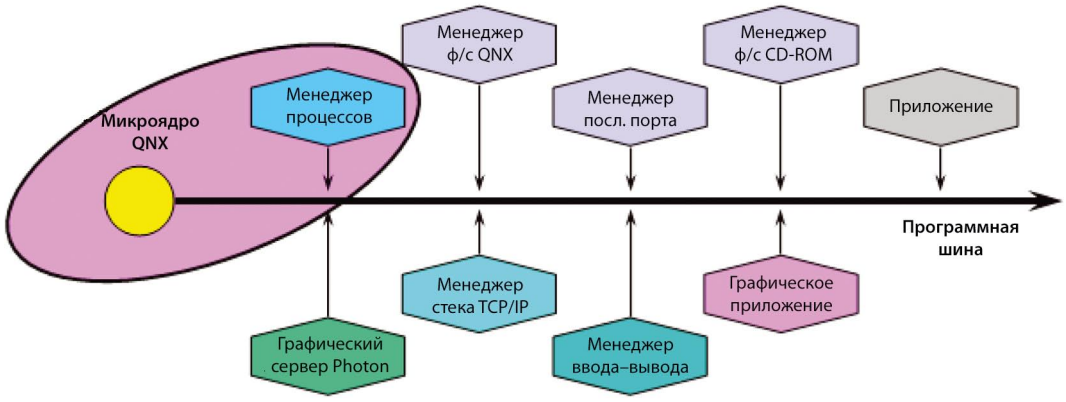

рис. 1. **Микроядро ОС QNX – это «программная шина», к которой подключаются компоненты системы**

ное потребление ресурсов системы, которое может происходить из-за недочетов при проектировании или реализации ПО и атак на отказ в обслуживании.

Технология мгновенной активации устройств позволяет значительно (до 1—2 порядков) сократить время запуска драйверов устройств при перезагрузке системы. Обычно драйверы можно запустить лишь после инициализации ядра ОС, что требует от нескольких сотен миллисекунд до нескольких секунд (в зависимости от оборудования и размера образа операционной системы). Технология мгновенной активации устройств основана на использовании минидрайверов, которые способны работать до инициализации микроядра. Минидрайвер принимает сигналы от оборудования, и когда ОС запускается и основной драйвер начинает работу, передает ему управление. В результате возобновление обслуживания устройств ускоряется до десятков миллисекунд; этого достаточно, чтобы избежать потери сообщений при использовании некоторых шинных протоколов (к примеру, MOST и CAN).

Операционные системы QNX включают в себя собственный сетевой протокол, который обеспечивает прозрачный доступ к ресурсам удаленных узлов и позволяет в полной мере реализовать принцип «сеть есть компьютер». В QNX 4 этот протокол называется FLEET, в QNX Neutrino — Qnet. Благодаря протоколам FLEET и Qnet методы межзадачного взаимодействия, которые работают в пределах одного узла, работают и в масштабе всей сети. Приложения, созданные для одного компьютера, можно распределять по сети, не внося принципиальных изменений в исходный код (см. рис. 2). Доступ к процессам, файлам и другим ресурсам удаленных узлов осуществляется так же, как и на локальном компьютере — достаточно лишь дополнить локальное имя ресурса именем узла. «Прозрачный» сетевой протокол позволяет применять ОСРВ QNX в сфере распределенных вычислений.

Пользователями ОСРВ QNX, как и других ОС жесткого реального времени, являются разработчики ПО. Создание программ для ОС QNX 4 осуществляется с помощью инструментария Watcom, который поставляется в составе ОС при покупке соответствующей лицензии. Гораздо большими возможностями обладает комплект разработчика QNX Momentics, который предназначен для ОСРВ QNX Neutrino. QNX Momentics основан на расширяемой платформе Eclipse и включает в себя инструментарий для всех стадий разработки ПО — редактор кода, символьный отладчик, анализатор памяти, профайлер приложений, анализатор покрытия кода, профайлер системы, построитель образов целевых систем и др. Существуют дистрибутивы QNX Momentics для различных операционных систем — QNX Neutrino, Windows и Linux. В QNX Momentics можно интегрировать инструменты третьих сторон, а также создавать собственные инструменты разработки.

В сентябре 2007 г. компания QNX Software Systems начала открывать свои исходные коды на основе гибридной лицензионной политики, сочетающей в себе принципы лицензирования систем с открытым кодом и коммерческого ПО. Разработчики могут скачивать исходные коды с официального сайта компании, модифицировать их и самостоятельно решать, открывать или не открывать результаты своих разработок. Коммерческие разработчики, для которых важно, чтобы ответственность за качество ОС несла компания QNX, по-прежнему имеют возможность приобретать компоненты среды исполнения и рабочие места комплекта QNX Momentics.

Наряду с открытием исходных кодов и введением гибридной лицензионной политики, компания QNX создала портал Foundry27, чтобы объединить разработчиков, использующих ее технологии. В настоящее время к сообществу присоединилось более 20-ти тыс. участников. На портале ведутся 14 проектов по развитию ОСРВ QNX и комплекта разработчика QNX Momentics: создание библиотеки классов для объектно-ориентированного программирования под QNX, перенос различных программных продуктов из других ОС (Solaris, NetBSD и др.), развитие микроядра, файловой, сетевой и других подсистем, а также инструментов разработки. Важный результат деятельности сообщества Foundry27 — выпуск нового продукта платформы разработки QNX Software Development Platform (SDP) 6.4.0 в октябре 2008 г. Этот продукт создан при непосредственном участии сообщества и объединяет в себе ОСРВ QNX Neutrino 6.4.0 и комплект разработчика QNX Momentics 6.4.0.

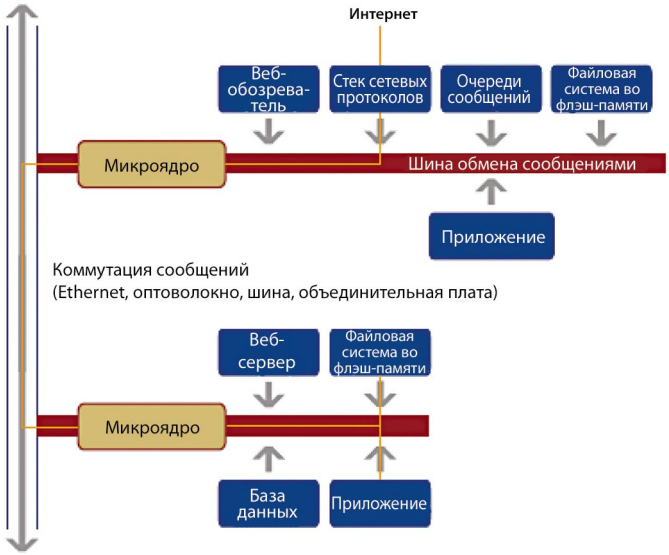

рис. 2. **Собственная сетевая технология ОСРВ QNX устраняет различия между локальным и межузловым взаимодействием программ**

В QNX SDP 6.4.0 входит новая файловая система с повышенной устойчивостью к сбоям при отключении питания, квотирование памяти, сетевой стек с поддержкой Jumbo-пакетов и улучшенной архитектурой драйверов, виртуальная память с изменяемым размером страницы, а также графический и сетевой TDK-комплекты. ОСРВ QNX Neutrino 6.4.0 получила сертификат POSIX PSE52 (упомянутый ранее) и оценку EAL4+ по стандарту безопасности информационных технологий «Общие критерии». Эта оценка подтверждает, что ОСРВ QNX Neutrino 6.4.0 может использоваться в приложениях, где к операционной системе предъявляются особые требования по защите информации от несанкционированного доступа.

Технологии QNX вызывают давний интерес со стороны российской оборонной промышленности. По этой причине на основе ОСРВ QNX 4.25 разработан программный комплекс «Защищенная операционная система реального времени QNX» (ЗОСРВ QNX) — изделие КПДА.00002-01, которое сертифицировано Гостехкомиссией России (ныне Федеральной службой по техническому и экспортному контролю — ФСТЭК) по 3-му классу защищенности от несанкционированного доступа и 2-му уровню контроля отсутствия недекларированных возможностей. Это позволяет использовать ЗОСРВ QNX в автоматизированных системах класса защищенности до 1Б включительно. Данный продукт оказался востребованным не только в ОПК, но и при создании ответственных систем коммерческого учета в добывающей промышленности, энергетике, а также в транспортной сфере [3].

Интенсивность развития технологий QNX говорит о мощном потенциале, заложенном в базовые архитектурные принципы семейства операционных систем QNX. ОСРВ QNX применяются в устройствах самого разного назначения — от бортовых информационных систем (QNX является доминирующей ОС в автомобильной электронике) и сетевых маршрутизаторов до распределенных систем управления предприятиями. В России технологиями QNX традиционно интересуются производители промышленных контроллеров, телекоммуникационных устройств, АСУТП и различных систем ВПК. Рост интереса к технологиям QNX в совокупности с амбициозными планами компании QNX Software Systems говорит о том, что в арсенале у QNX не только заслуженное прошлое и динамичное настоящее, но и перспективное будущее.

ЛИТЕРАТУРА

1. Операционная система реального времени QNX Neutrino 6.3. Системная архитектура.

2. Wikipedia, интернет-энциклопедия, http://wikipedia.org.

3. Зыль Сергей, Махилёв Владимир. Защищённая операционная система реального времени. СТА, 3/2007.