Защищенная ОС РВ нового поколения: особенности архитектуры и средства защиты информации

А.Н. Докучаев (ООО «СВД Встраиваемые Системы»)

Представлены архитектурные особенности современной защищенной ОС РВ «Нейтрино» (изделие ЗОСРВ КПДА.10964-01 компании ООО «СВД Встраиваемые Системы»). Производится сравнительный анализ изделия по отношению к предшественнику – ЗОСРВ КПДА.00002-01. Отдельно рассматриваются технологии и средства, обеспечивающие защиту информации для автоматизированных систем класса защищенности до 1Б включительно.

Ключевые слова: защищенная операционная система реального времени, жесткое РВ, автоматизированные системы, проектирование, средства защиты информации, встраиваемые системы.

На сегодняшний день уже ни у кого не вызывает сомнений тот факт, что ОС QNX прочно заняла лидирующее место в мире передовых информационных технологий РВ. Под управлением ОС РВ QNX успешно функционирует огромное число встраиваемых систем и систем РВ, относящихся к совершенно разным областям человеческой деятельности, будь то телекоммуникации, оборонная промышленность, авиация, медицина, энергетика, металлургия и др. Среди компаний активно применяющих ОС отметим VISA, Atomic Energy of Canada, General Motors, Cisco, Chrysler, Toyota, Ford, General Electric, Mitsubishi и др.

На протяжении более чем 20-летней эволюции ОС QNX степень ее популярности определяется в первую очередь следующими факторами: микроядерной архитектурой и сравнительно небольшими размерами программных компонент, высокой скоростью работы и реакции на события, высоким уровнем модульности и отказоустойчивости, а также поддержкой подавляющего большинства современных аппаратных платформ. Последние версии QNX способны выполняться на архитектурах x86, MIPS, ARM, PowerPC, SuperH, реализуют симметричное, асимметричное и ограниченное (bound multiprocessing) мультипроцессирование [1], поддерживают международный стандарт переносимых интерфейсов POSIX и имеют совместимость с GNU/Linux посредством GNU Compiler Collection. Среди наиболее востребованных технологий, поддержка которых имеется в ОС, отметим OpenGL ES, Qt, Adobe AIR/Flash и OpenVG. Тем не менее, при учете всего вышесказанного, использование коммерческой ОС РВ с закрытым исходным кодом в отечественном оборонно-промышленном комплексе (ОПК) не допустимо, ввиду жестких требований к информационной безопасности.

В 2004 г. компания ООО «СВД Встраиваемые Системы» успешно завершила разработку и сертификационные испытания программного комплекса «Защищенная операционная система реального времени QNX» (изделие КПДА.00002-01) [2]. Начиная с этого момента, ЗОСРВ имеет возможность применяться в автоматизированных системах (АС) класса защищенности до 1Б включительно благодаря соответствию третьему уровню защиты от несанкционированного доступа (НСД) и второму уровню контроля недекларированных возможностей (НДВ). Разработка защищенной ОС велась на основе полученных от QNX Software Systems исходных кодов, соответствующих версии ОС РВ QNX 4.25. Изделие могло успешно выполняться в однопроцессорных вычислительных системах с платформой x86, что соответствовало требованиям того времени. Отметим, что ЗОСРВ КПДА.00002-01 регулярно обновляется (последнее обновление было выполнено в 2011 г.), расширяется дополнительными технологиями и до сих пор успешно применяется в отечественном ОПК.

С момента сертификации в РФ ЗОСРВ требования к аппаратному обеспечению АС существенно изменились. К настоящему моменту широкое распространение получила мультпроцессорная техника и альтернативные по отношению к x86 архитектуры, востребованы высокоскоростные интерфейсы передачи данных (в том числе и беспроводные сетевые технологии), средства высокопроизводительного отображения различных видов графики и технологии распределенных вычислений. Современная QNX Neutrino в полной мере соответствует данным требованиям и обладает всем необходимым инструментарием.

К концу 2010 г. компания завершила разработку защищенной ОС нового поколения - ЗОСРВ «Нейтрино» (ЗОСРВ «Нейтрино» КПДА.10964-01) и представила изделие к сертификации. ЗОСРВ «Нейтрино» имеет бинарную совместимость с ОС РВ QNX Neutrino 6.5.0 и базируется на ее исходном коде, что позволяет при необходимости применять системы совместно, а также использовать одни и те же средства разработки и отладки. В частности, ПО, разработанное в интегрированной среде разработки QNX Momentics PE, в большинстве случаев может быть запущено в защищенной ОС без изменений исходного кода. Изменения могут потребоваться лишь в случае тесного взаимодействия со средствами защиты информации (СЗИ) либо при явном нарушении политик безопасности системы. Завершение сертификационных испытаний по 3 классу защиты от НСД и 2 уровню контроля отсутствия НДВ, а также на соответствие реальных возможностей декларированным запланировано на четвертый квартал 2011 г. Это позволит использовать изделие для соз-

дания АС с классом защищенности до 1Б включительно.

Особенности архитектуры изделия ЗОСРВ «Нейтрино»

Как уже упоминалось ЗОСРВ «Нейтрино» относится к классу микроядерных ОС РВ, что обуславливает сравнительно небольшой размер ядра ОС. Под микроядром в узком смысле понимается системный процесс, включающий менеджер памяти, менеджер процессов и планировщик, а также менеджер имен. В широком же смысле микроядро является особым компонентом ОС, обеспечивающим комплексную изоляцию остальных программных компонентов системы. Подразумевается изоляция адресного пространства процессов, реализация интегрированных в ядро механизмов межпроцессного взаимодействия (в том числе межпроцессорного и распределенного по сети) и организация эффективного распределения вычислительных ресурсов процессора. Все остальные системные сервисы реализованы в виде отдельных процессов (в терминологии QNX они называются менеджерами). Подобное разделение сфер ответственности позволяет «на лету», то есть без остановки или перезапуска ОС останавливать и перезапускать любую задачу, будь то прикладное ПО, драйвер файловой системы, менеджер видеоподсистемы или любой другой системный сервис. В обязанности ядра также входит первичная обработка прерываний и передача управления системному ПО.

В ОС, построенных на монолитном ядре, все системные компоненты составляют с ядром единый модуль, и в случае возникновения критических ошибок подчас может потребоваться пересборка всего ядра из исходного кода. Подобные ошибки также могут вызвать терминирование самого ядра, при недобросовестности разработчиков модуля, приведшего к сбою. В QNX и ЗОСРВ «Нейтрино» ошибка в отдельном процессе будет требовать модификации лишь конкретного модуля и приведет в худшем случае лишь к завершению с ошибкой активного процесса.

Применение микроядерной архитектуры в ЗОСРВ «Нейтрино» позволяет добиться высокой скорости реакции системы на события. Например, без потерь достижим прием прерываний от устройств ввода/вывода на шине PCI с интенсивностью несколько десятков тысяч в секунду при обработке запросов на прерывание в обычном потоке, а не в высокоприоритетном ISR. В данных условиях ОС Linux как яркий представитель технологии монолитной реализации ядра на аналогичном оборудовании показывает гораздо более скромные результаты при потоковой обработке прерываний. Отметим, что речь идет именно о гарантированной реакции системы на событие.

Единицей диспетчеризации в ЗОСРВ «Нейтрино» КПДА.10964-01 по сравнению с ЗОСРВ КПДА.00002-01 является поток, а не процесс. Иными словами поддерживается многопоточность приложений в соответствии с требованиями стандарта POSIX современной редакции. Изделие в полной мере реализует выполнение приложений в системах с мультипроцессорной архитектурой. Основные различия между рассматриваемыми защищенными ОС по части выполнения задач представлены в таблице.

Одной из ключевых технологий, поддержка которых отсутствовала в ЗОСРВ КПДА.00002-01, является адаптивное квотирование ресурсов процессора (Adaptive Partitioning). Суть технологии заключается в следующем: группе процессов задается квота процессорного времени (задачи объединяются в группы диспетчеризации или партиции), выраженная в процентном отношении ко всей вычислительной мощности процессора. До тех пор, пока нагрузка на процессор не велика, любой процесс может потреблять произвольное количество ресурсов процессора. Если же микроядром фиксируется высокая вычислительная нагрузка, потребление ресурсов процессора группами задач единой партиции не может превышать заданной квоты. Таким образом, достигается возможность задания минимального гарантированного числа системных ресурсов, предоставляемых процессором как отдельным задачам, так и логически объединенным группам задач.

Архитектура сетевой подсистемы ЗОСРВ «Нейтрино» унаследована от стека протоколов UNIX-подобной ОС NetBSD. Это позволяет успешно применять современные сетевые драйверы и драйверы предыдущих версий QNX, а также обеспечивает их легкое перенесение из ОС общего назначения NetBSD. За счет родственных связей сетевого стека его конфигурирование происходит аналогично большинству UNIX-подобных ОС, например: Linux, NetBSD, SunOS, Mac OS и FreeBSD. В ОСРВ QNX Neutrino 6.5.0 и ЗОСРВ «Нейтрино» реализована поддержка сетевого оборудования стандарта IEEE 802.11 (Wi-Fi) и Berkeley Packet Filter (BPF). До 2011 г. в состав ЗОСРВ КПДА.00002-01 не входил сертифицированный стек протоколов TCP/IP и в нем нет поддержки технологии Wi-Fi. Возможность организации распределенных вычислений, которая упоминалась ранее, достигается посредством протокола прозрачного взаимодействия QNET, который позволяет объединять сетевые узлы ЗОСРВ в единый вычислительный кластер. При этом программно-аппаратные ресурсы смежных узлов оказыва-

Таблица. Основные архитектурные различия ЗОСРВ «Нейтрино» КПДА.10964-01 и КПДА.00002-01

Критерий сравнения	ЗОСРВ «Нейтрино» КПДА.10964-01	ЗОСРВ КПДА.00002-01
Поддерживаемые архитектуры	x86, MIPS, ARM, PowerPC	x86
Максимальное число процессоров, ед	32	1
Единица диспетчеризации	поток	процесс (поддержка потоков отсутствует)
Максимальное число процессов, ед	4095	2000
Максимальное число потоков процесса, ед.	32767	1 (единственный поток команд процесса)
Число уровней приоритета, ед.	256	32

ются доступными на любой машине в виде обычных файлов и директорий, доступ к которым может быть осуществлен локально (сетевая составляющая взаимодействия для пользователя незаметна). Поддержка некоторых высокоскоростных интерфейсов (например, USB) в новых выпусках ЗОСРВ КПДА.00002-01 (2010 и 2011 годов) была реализована на основе исходных текстов ЗОСРВ «Нейтрино».

В ЗОСРВ «Нейтрино» имеется аудио подсистема, поддерживающая внушительное число современных контроллеров. Например, доступно использование аппаратуры стандартов AC'97 и Intel HDA, а также оборудования таких производителей, как Cirrus Logic, National Semiconductor и др. В ЗОСРВ КПДА.00002-01 поддержка некоторых аудио контроллеров обеспечивается с помощью дополнительного пакета Audio2. В число поддерживаемых устройств входят, например, C-Media, Intel AC'97, Creative Sound Blaster Live! и AMD Geode LX.

Графические возможности защищенной ОС развиваются в нескольких плоскостях. Одной из них является Photon Micro GUI – штатная графическая оболочка ЗОСРВ «Нейтрино». Ее внешний вид представлен на рис. 1. Особенностью графической оболочки является очень маленький размер, что с очевидностью следует из названия. При исключении ненужных компонентов, например, лишних графических драйверов, встроенной справочной системы, можно добиться размера загрузочного образа всего в несколько мегабайт. Подсистема поддерживает аппаратное 2D и 3D ускорение, встраиваемую версию кроссплатформенной библиотеки OpenGL ES и имеет возможность запуска приложений, разработанных для X Window System (распространенная графическая подсистема во многих UNIX-подобных ОС). ОС РВ QNX Neutrino 6.5.0 располагает средствами разработки графических приложений Photon Application Builder.

Другим немаловажным вектором развития графических возможностей ЗОСРВ является полноценная поддержка библиотеки Qt. В особых представлениях она не нуждается, поскольку ее реализации имеются, чуть ли не во всех распространенных ОС.

В последнее время получила большую популярность технология Flash. Один из ведущих мировых разработчиков мобильных устройств - компания Research In Motion (владеющая в настоящий момент QNX Software Systems) в 2011 г. успешно применила данный подход в своих решениях, что вылилось в появление на рынке планшетного компьютера BlackBerry PlayBook (а в скором времени и ряда смартфонов), выполненного на базе ОС РВ QNX. Большинство приложений для планшетного компьютера разработано на платформе Adobe AIR с поддержкой Flash.

Отметим, что на момент сертификации ЗОСРВ КПДА.00002-01 средства разработки имелись лишь в самой ОС. ЗОСРВ «Нейтрино» располагает инструментами разработки, профилирования и отладки (в том числе удаленной) как в самой ОС, так и для ОС Windows, Linux на основе Eclipse-ориентированной QNX Momentics IDE.

Для ЗОСРВ немаловажную роль играет поддержка

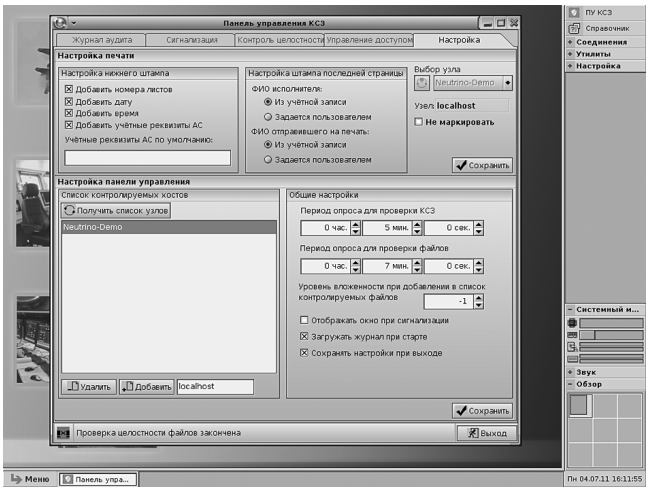

Рис. 1. Photon – графическая оболочка ЗОСРВ «Нейтрино» с запущенной панелью управления комплексом средств защиты (ПУ КСЗ)

современного аппаратного обеспечения, осуществляемая непосредственно разработчиком ОС. Для версии КПДА.00002-01 с каждым новым выпуском отмечается расширение списка устройств, применение которых доступно всем разработчикам АС. Что касается ЗОСРВ «Нейтрино», то здесь доступ к современному оборудованию осуществляется средствами пакетов поддержки плат (Board Support Package или BSP), а также отдельных менеджеров устройств и драйверов специфичных устройств. ЗОСРВ «Нейтрино» работает на микропроцессорах отечественных производителей, например, на платформе Мультикор от ГУП НПЦ «Элвис».

Обзор средств защиты информации

Кратко рассмотрим перечень основных средств защиты информации (СЗИ), представленных в ЗОСРВ «Нейтрино» КПДА.10964-01.

Подсистема контроля целостности обеспечивает периодическую проверку целостности компонентов системы защиты. Подсистема включает средства формирования и проверки контрольных хэш-сумм по алгоритму ГОСТ Р 34.11-94, а также механизмы комплексного анализа целостности компонент. Имеется возможность контроля целостности системы и СЗИ посредством панели управления комплексом средств защиты (ПУ КСЗ). Внешний вид ПУ КСЗ представлен на рис. 1.

Сетевая подсистема включает средства защиты стека протоколов TCP/IP и отдельно протокола прозрачной сети QNET. Для защищенных распределенных вычислений и сетевого взаимодействия через встроенную сеть QNX предусмотрен режим защиты узлов от несанкционированного доступа со стороны незащищенных систем. На все межузловые транзакции подобного рода распространены политики мандатного и дискреционного разграничения доступа. Пример диалога назначения мандатных и дискреционных прав администратором безопасности при помощи ПУ КСЗ представлен на рис. 2. Для стека протоколов TCP/IP предусмотрена собственная

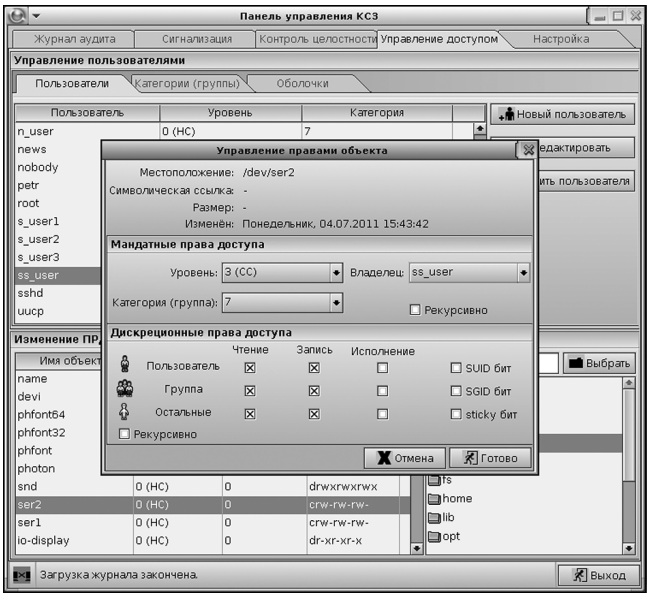

Рис. 2. Использование ПУ КСЗ для назначения мандатных и дискреционных прав защищаемым объектам файловой системы

независимая система мандатного контроля доступа. Необходимо также упомянуть наличие в составе ЗОСРВ средств интеграции с распространенными операционными системами общего назначения. В частности, представлены средства, позволяющие организовать сеанс удаленного взаимодействия с графической подсистемой. Реализация этой возможности в ОС Windows осуществляется посредством утилиты phindows, предоставляющей функционал сетевого взаимодействия с графическим сервером Photon и интерфейсами ввода/вывода. Для ОС семейства Linux также имеется возможность организации подобного удаленного пользовательского интерфейса средствами штатного приложения ЗОСРВ phinx в пределах возможностей сетевого протокола X Window System. Данный протокол является составной частью распространенной в UNIX-подобных ОС одноименной графической подсистемы.

Ввиду архитектурных особенностей ЗОСРВ «Нейтрино» КПДА.10964-01 средства защиты, включенные в *подсистему межпроцессного взаимодействия*, охватывают абсолютно все компоненты ОС и ПО любого вида. Данная подсистема распространяет политики мандатного и дискреционного контроля доступа на следующие механизмы взаимодействия процессов: передача сообщений и пульсов, передача сигналов, взаимодействие с очередями сообщений и объектами в разделяемой памяти. Для всех перечисленных методов взаимодействия применяется аудит безопасности, в случае, если он не противоречит концепциям ОС РВ. Поскольку межпроцессное взаимодействие является фундаментальным для ОСРВ QNX, средства защиты автоматически распространяются и на удаленное взаимодействие узлов по протоколу QNET.

Подсистема контроля доступа к объектам и контроль прав разграничения доступа тесно связаны между собой. По этой причине достаточно трудно отделить сферы их влияния друг от друга. В общем и целом, областью их ответственности являются практически все объекты файловых систем. Исключением не являются даже объекты микроядра ЗОСРВ, отображенные на пространство доступных имен. Подсистемы реализуют для защищаемых объектов политики контроля доступа и аудита безопасности.

В *защищенную подсистему печати* интегрированы механизмы маркирования документов, аудита и контроля доступа к ресурсам печати.

Контроль процессов осуществляется микроядром независимо от субъекта контроля доступа. Реализуется мандатная защита процессов, изоляция и очистка задействованной памяти, регистрация событий аудита и иерархическое сокрытие потоков в соответствии с политикой мандатного контроля доступа.

Все упомянутые подсистемы реализуют *аудит безопасности* подконтрольных объектов. В ЗОСРВ «Нейтрино» предусмотрен специализированный менеджер аудита, реализующий сбор, хранение и первичную обработку данных аудита, а также обеспечение оперативной сигнализации о нарушениях политик защиты информации на АРМ администратора безопасности и нарушителя. Без корректного запуска и выполнения менеджера аудита контроль целостности защищенной системы не может быть завершен успешно. Уровень подробности аудита регулируется микроядром ЗОСРВ и задается администратором безопасности в момент запуска системы. В число обязательных параметров каждого регистрируемого события аудита входят как минимум: дата и время возникновения события, субъект и объект защиты, ответственная подсистема, описатель класса события и результат его выполнения. В комплект изделия входят средства отображения логов аудита и событий оперативной сигнализации как с текстовым, так и с графическим пользовательским интерфейсом. Последние интегрированы в ПУ КСЗ.

В изделие включена исчерпывающая документация на русском языке, в том числе с описанием реализованных средств защиты и рекомендациями по удовлетворению требований РД АС (http://www.fstec.ru/_docs/doc_3_3_004.htm) для автоматизированных систем класса защищенности до 1Б включительно. Описанные в статье средства защиты соответствуют 3 уровню защиты от НСД и 2 уровню контроля НДВ в соответствии с РД СВТ (http://www.fstec.ru/_docs/doc_3_3_006.htm).

Список литературы

1. *Зыль С.* Проектирование, разработка и анализ программного обеспечения систем реального времени. С.-Петербург: БХВ-Петербург, 2010.
2. *Зыль С., Махилев В.* Защищённая операционная система реального времени // Современные технологии автоматизации. 2007. Вып. 3.

Докучаев Андрей Николаевич *- инженер-программист ООО «СВД Встраиваемые Системы».*
Контактный телефон (812) 373-41-17.
E-mail: A.Docuchaev@kpda.ru
http://www.kpda.ru