УДК 044.451.5

С.Г. СЕМЕНОВ, С.Ю. ГАВРИЛЕНКО, В.В. ДАВЫДОВ

Национальный технический университет «Харьковский политехнический институт», Украина

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Проведено сравнительное исследование операционных систем реального времени, выявлены их основные особенности, достоинства и недостатки, а также уровень безопасности. Построены сравнительные диаграммы быстродействия компьютерной системы и производительности сетевого оборудования для операционных систем реального времени VxWorks AE, Windows CE.NET/NT и QNX. Сделан вывод о целесообразности использования в автоматизированной системе технологическим процессом системы QNX. Проведено исследование микроядерной архитектуры операционной системы QNX, выявлены основные угрозы безопасности в этой системе.

Ключевые слова: *операционные системы реального времени, автоматизированные системы управления, QNX, безопасность.*

Постановка проблемы

В соответствии с законом Украины «О телекоммуникациях», государственными стандартами Украины (ДСТУ 2226-93, 3397-96, 3451-96, 3481-96) и другими руководящими документами, наиболее важными факторами эффективной работы автоматизированных систем управления технологическим процессом (АСУ ТП) являются готовность объекта к автоматизации, психологическая настроенность персонала, приспособленность технологии и оборудования и др.

Без указанных факторов будет происходить дискредитация автоматизации, а предприятия вместо ожидаемой прибыли получит убыток.

Существенное место в АСУ ТП занимают средства вычислительной техники, выполняющие трудоемкие операции по сбору и обработке информации, при этом общее администрирование техническими системами осуществляется с помощью общего и специального программного обеспечения.

Анализ современных средств автоматизации производством [2,6] показал, что в настоящее время в АСУ ТП находят применение различные программные пакеты, работающие под управлением операционных систем. При этом более 90% программ выполняют задачи, в которых важны не только правильность решения, но и сроки, в которые эти решения принимаются (оперативность принятия решений).

Поэтому для достижения оптимальных показателей оперативности и обеспечения качества принятия решений в АСУ целесообразно максимально использовать возможности операционных систем реального времени.

Исследования показали, что, несмотря на многообразие операционных систем реального времени (см рис. 1.) в настоящее время в АСУ ТП чаще всего используются три вида: VxWorks AE, Windows CE.NET/NT и QNX [1 – 3, 5, 6].

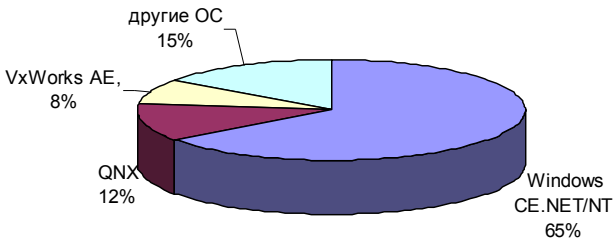

Рис. 1. Использование ОС реального времени в АСУ ТП

Их сравнительный анализ позволил выявить ряд достоинств (высокая надежность и масштабируемость системы QNX, интеграция операционных систем Windows CE.NET/NT с большим количеством уже готовых коммерческих программ, изоляция системы VxWorks AE от внешних воздействий) и недостатков (недостаток современных средств разработки программного обеспечения в системе VxWorks AE, слабая защищенность данных от хакерских атак и возможные негативные последствия от воздействия вирусов в системах Windows CE.NET/NT и QNX). Анализ литературы [1 – 3],

показал, что, в последнее время на крупных предприятиях в качестве операционной системы АСУ ТП все чаще стали использовать систему QNX. Связано это в первую очередь с рядом преимуществ указанной системы, таких как: предсказуемость, означающую ее применимость к задачам с высокими требованиями оперативности; расширяемость и надежность одновременно, поскольку реализованные драйвера не нужно компилировать в ядро, вызывая при этом нестабильность системы; быстрый сетевой протокол FLEET, обеспечивающий отказоустойчивость, распределение сетевой нагрузки и динамическую маршрутизацию; богатый выбор графических подсистем, включающий QNX Windows, X11R5 и Photon и др.

Основная часть

Анализируя структуру операционной системы QNX (рис. 2) можно заметить, что микроядерное построение архитектуры этой системы создает основу для ее надежной (отказоустойчивой), а в ряде случаев и безопасной работы. Из рис. 2 видно, что в перечень основных задач, решаемых операционной системой, составляет: управление адресным пространством, управление потоками и межзадачное взаимодействие. Все другие службы — которые, в случае обычного, монолитного ядра, как правило, выполняются внутри него — реализуются в пользовательском пространстве как самостоятельные процессы или программы.

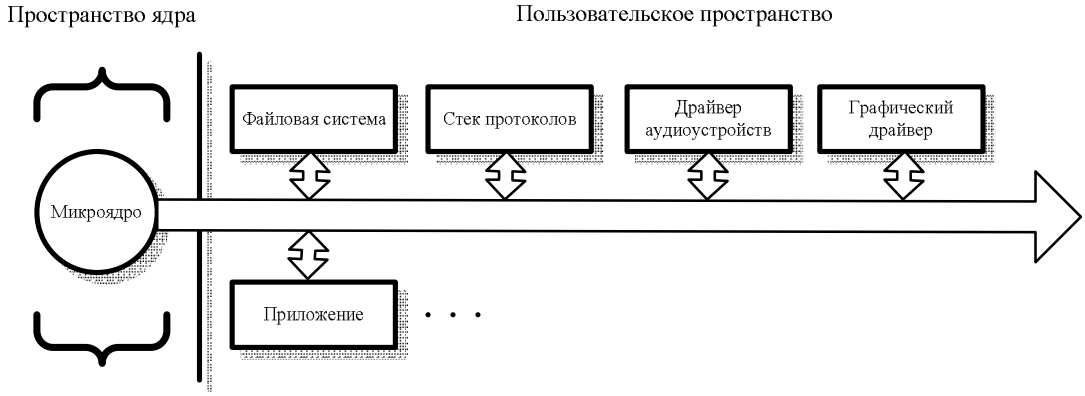

Рис. 2. Микроядерная архитектура QNX

Благодаря реализации системных служб (работа с сетью, драйверы устройств, файловые системы) вне ядра в виде отдельных процессов в пользовательском пространстве, сбои в работе любой службы не влияют на работу ядра или других выполняющихся процессов. Данный модульный подход обеспечивает гибкость и простоту расширяемости, а так же высокую эффективность механизма передачи сообщений внутри системы (рис. 3).

Кроме того, возможность передачи данных по 3 направлениям, с использованием различных технологий канального уровня позволяет существенно (до 40%) повысить производительность QNX сети, что наглядно иллюстрирует рис. 4.

В то же время в указанной системе существует ряд недостатков и ограничений. Часть их связанны с ориентацией системы на рынок встроенных систем реального времени:

− отсутствие поддержки SMP и своппинга виртуальной памяти на диск;

− неэффективная и нестандартная поддержка нитей (threads);

− отсутствие поддержки Java;

− ограниченный набор средств разграничения и контроля доступа пользователей;

− отсутствие средств безопасности (брандмауэра, антивирусных программ) в рамках собственного сетевого протокола;

− потребность в перезагрузке ОС после излечения от вирусов.

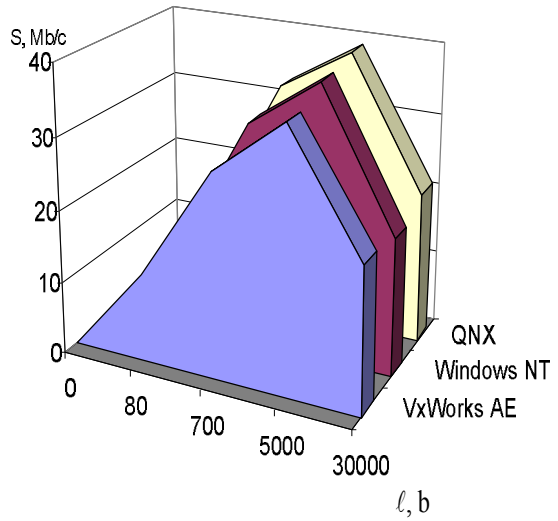

Рис. 3. Зависимость быстродействия S компьютерной системы от объема сообщений для различных операционных систем

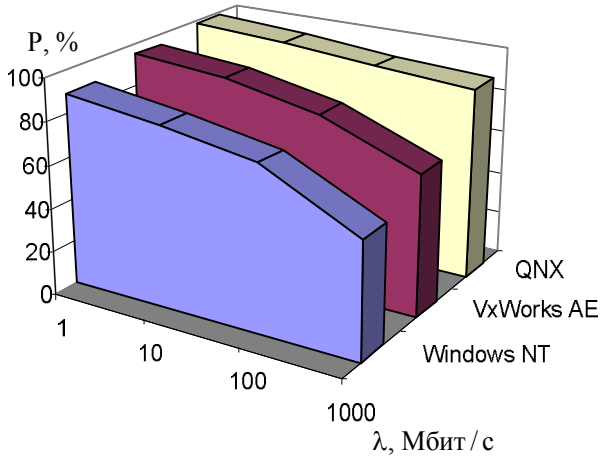

Рис. 4. Зависимость производительности P сетевого оборудования от интенсивности информационного потока λ для различных операционных систем реального времени

Некоторые из них связаны с недостатками в программном коде:

− возможность изменения переменных окружения внутренним программным обеспечением;

− возможности изменения системной области памяти (особенно при работе с компонентами графической подсистемы photon);

− использование необоснованно длинных (по количеству символов) параметров таких программ как SU, PASSWD;

− использование последовательностей команд для таких программ как GDB и др.

Проведенные исследования показали, что если недостатки, связанные с настройками сетевых приложений и внутренним управлением памятью отчасти компенсируются достоинствами (например, отсутствие поддержки SMP и своппинга виртуальной памяти на диск компенсируется быстротой (микросекунды) переключения контекста между процессами), то вопросы обеспечения безопасности информации в этой системе пока, еще не находят должного внимания у разработчиков.

Указанные уязвимости ухудшают в целом степень защиты операционной системы и способствуют проникновению в компьютерные системы (серверы) различных программных угроз.

Поэтому на этапе «внутреннего» функционирования АСУ ТП без выхода в региональные и глобальные сети данная проблема не выглядит актуальной, но в случае вынужденного подключения АСУ ТП к внешним телекоммуникационным сетям повышается опасность нарушения безопасности операционной системы и АСУ в целом.

Поэтому для повышения безопасности АСУ ТП и уменьшения возможных последствий реализации программных угроз в указанной операционной системе авторам представляется целесообразным использовать новые, комплексные подходы, позволяющие идентифицировать эти угрозы и максимально снизить их негативные последствия.

Проведенные исследования показали, что в настоящее время существует множество программных угроз. Их классификация представлена на рис. 5.

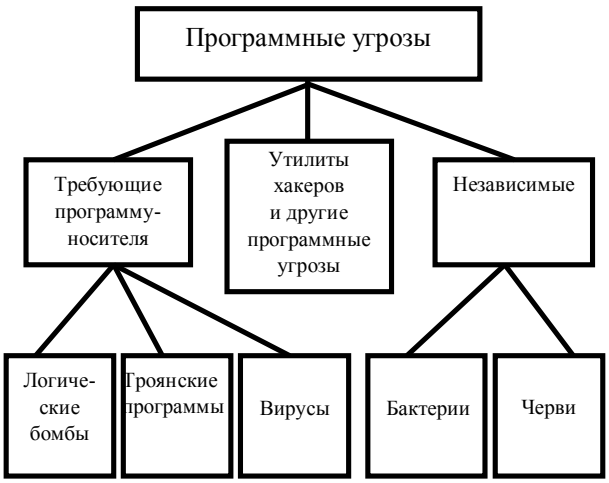

Рис. 5. Классификация программных угроз

Из [4] известно, что среди всего разнообразия приведенных программных угроз наиболее распространенными являются логические бомбы, троянские программы и компьютерные вирусы.

Их опасность для операционной системы QNX заключается в возможности переполнения существующих пользовательских подсистем (файловой подсистемы, графической подсистемы photon и др.), а так же изменении технических характеристик компьютерной системы с дальнейшим выходом из строя основных ее элементов (процессора, памяти, графического адаптера и др.).

Проведенный анализ показал, что особенно опасны данные программные угрозы в фазе распространения (выполнения деструктивных действий).

В этот промежуток времени вирусы могут изменять параметры (технические характеристики) как отдельных узлов, так и компьютерной системы в целом.

Поэтому именно на этой стадии распространения вируса целесообразно производить идентификацию компьютерной системы и уменьшать негативные последствия вирусной атаки.

Выводы

В результаты работы проведено сравнительное исследование операционных систем реального

времени, выявлены их основные особенности, достоинства и недостатки, построены сравнительные диаграммы быстродействия компьютерной системы и производительности сетевого оборудования для операционных систем VxWorks AE, Windows CE.NET/NT и QNX. В ходе исследования сделан вывод о целесообразности использования в АСУ ТП системы QNX. Анализ данной системы позволил выявить ее недостатки и определить пути их устранения. Одним из таких путей является разработка и внедрение системы идентификации для устранения угрозы вирусной атаки на компьютерную систему.

Литература

1. Горошко Е. QNX/UNIX: анатомия параллелизма / Е. Горошко, О. Цилюрик. – М.:"Символ-Плюс", 2006. – 288 с.

2. Денисенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием / В.В. Денисенко. – М.:Горячая линия–Телеком, 2009. – 608 с.

3. Кртен Р. Введение в QNX Neutrino. Руководство для разработчиков приложений реального времени (2-е издание) / Р. Кртен. – СПб.: БХВ-Петербург, 2011. – 368 с.

4. Кузнецов О.О. Протоколи захисту інформації у комп'ютерних системах та мережах: Навч. посібник. / О.О.Кузнецов, С.Г.Семенов. – Х.: ХНУРЕ, 2009. – 186 с.

5. Операционная система реального времени QNX Neutrino 6.3. Руководство пользователя / перев. Ю. Асотов. – СПб.: БХВ-Петербург, 2009. – 480 с.

6. Таненбаум Э. Современные операционные системы / Э. Таненбаум; 3-е изд. – СПб.: Питер, 2010. – 1120 с.

Поступила в редакцию 30.05.2011

Рецензент: д-р техн. наук, проф. С.Г. Удовенко, проф. кафедры электронных вычислительных машин Харьковского национального университета радиоэлектроники, Харьков, Украина.

БЕЗПЕКА ОПЕРАЦІЙНИХ СИСТЕМ РЕЛЬНОГО ЧАСУ В АВТОМАТИЗОВАНИХ СИСТЕМАХ КЕРУВАННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ

С.Г. Семенов, С.Ю. Гавриленко, В.В. Давидов

Проведено порівняльне дослідження операційних систем реального часу. Виявлені їх основні особливості, переваги та недоліки, рівень безпеки. Побудовані порівняльні діаграми швидкодії комп'ютерної системи та продуктивність мережевого обладнання для операційних систем VxWorks AE, Windows CE.NET/NT та QNX. Зроблено висновок о доцільності використання в автоматизованої системі технологічним процесом системи QNX. Проведено дослідження використання мікроядерної архітектури QNX, виявлені основні загрози безпеки в цій системі.

Ключові слова: операційні системи реального часу, автоматизовані системи керування, QNX, безпека.

REAL TIME OPERATION SYSTEM SECURITY IN INDUSTRY CONTROL SYSTEMS

S.G. Semenov, S.Yu. Gavrilenko, V.V. Davydov

Performed comparative research of real time operation systems. Identified their basic features, benefits and limitations, security level. Built comparative diagrams of computer systems and network equipment performance for VxWorks AE, Windows CE.NET/NT and QNX operation systems. Has been made a decision concerned to expediency of using QNX operation system in Industry Control Systems. Performed research of microkernel QNX architecture, identified basic security threats in this system.

Key words: real time operation system, industry control systems, QNX, security.

Семенов Сергей Геннадьевич – канд. техн. наук, доцент кафедры вычислительной техники и программирования, Национальный технический университет «ХПИ», Харьков, Украина, e-mail: s_semenov@ukr.net.

Гавриленко Светлана Юрьевна – канд. техн. наук, доцент, доцент кафедры вычислительной техники и программирования, Национальный технический университет «ХПИ», Харьков, Украина, e-mail: gavrilenko-sveta@rambler.ru.

Давыдов Вячеслав Вадимович – аспирант кафедры вычислительной техники и программирования, Национальный Технический Университет «ХПИ», Харьков, Украина, e-mail: davs87@inbox.ru.