12. Лабораторный практикум по изучению системы удостоверяющих центров и сертификатов открытых ключей №3619. – Таганрог: Изд-во ТРТУ, 2004. – 31с.

13. *Бабенко Л.К., Ищукова Е.А.* «Современные алгоритмы блочного шифрования и методы их анализа», – М.: Гелиос, 2006. – 375с.

14. *Бабенко Л.К., Ищукова Е.А.* Изучение метода линейного криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля.. – Таганрог, Изд-во ТРТУ, 2004. – 21 с.

15. *Бабенко Л.К., Ищукова Е.А*. Изучение метода дифференциального криптоанализа применительно к алгоритмам шифрования, построенным по схеме Фейстеля. – Таганрог, Изд-во ТРТУ, 2004. – 15 с.

16. *Бабенко Л.К., Ищукова Е.А*. Изучение метода слайдовой атаки на примере алгоритмов шифрования, построенных по схеме Фейстеля. – Таганрог, Изд-во ТРТУ, 2004. 24 с.

17. *Бабенко Л.К.,. Курилкина А.М*. Параллельный алгоритм «распределенных согласований» решения задачи дискретного логарифмирования в конечных полях. Журнал «Вопросы защиты информации». – М: «ФГУП «ВИМИ», 2005, №2 (69), – С.8-14.

18..*Курилкина. А.М.* Автореферат кандидатской диссертации «Оценка вычислительной стойкости защиты информации алгоритмами «распределенных согласований». – Таганрог, Изд-во ТРТУ, 2005. – 16 с.

А.И. Грюнталь
Россия, г. Москва,
Научно-исследовательский институт системных исследований РАН

ИНФОРМАЦИОННО – БЕЗОПАСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

1. Постановка задачи

В 1995 г. в НИИСИ РАН была поставлена задача создания отечественного комплекта средств общего программного обеспечения (ОПО) для вычислительных систем, функционирующих в реальном масштабе времени, удовлетворяющих требованиям информационной безопасности (ИБ) и технологической независимости (ТН). Информационная безопасность – это отсутствие в исполняемом коде программ недекларированных функций и/или закладных элементов. Технологическая независимость – это гарантированная возможность сопровождения программы на всех этапах жизненного цикла коллективами, работающими в РФ, без прямого или косвенного участия зарубежных специалистов. Разрабатываемый комплект средств ОПО также должен был быть лицензионно – чистым. Основное внимание уделялось разработке операционной системе реального времени, с учетом требований гарантированного быстродействия, и компилятора – основного технологического средства разработки прикладного ПО.

2. Информационная безопасность и технологическая независимость

Группы требований по ИБ и ТН формально различны. Соответствие требованиям ИБ подтверждается процедурами сертификации, основанной на анализе исходного текста программного средства. Обеспечение адекватности исходного и загрузочного текста программ требует применения сертифицированных инструментальных средств, в частности средств кодогенерации.

Эффективность формальных процедур выявления недекларированных возможностей и/или закладных элементов путем анализа исходного текста ограничена большим объемом и большой сложностью программ. Например, исходный текст Си-компилятора включает порядка 2-х миллионов строк. Содержательный и полный анализ программы такого объема требует квалификации разработчика этой программы. Неизбежно имеющиеся ошибки в программах такой сложности могут интерпретироваться при сертификации как закладные элементы. Поэтому

уверенность в ИБ обеспечивается не только (и не столько) формальным анализом исходного текста программного средства, но и доверием к коллективу разработчиков.

Необходимость анализа разработки для оценки уровня ИБ соответствует требованиям «Общих критериев» [1]: при оценке уровня доверия также принимаются во внимание действия, предпринятые на этапе разработки. Аналогичные требования содержатся в руководящем документе Гостехкомиссии [2].

Необходимость разработки программного средства отечественным коллективом - основополагающее требование технологической независимости. Сопровождение в течение жизненного цикла программного средства требует квалификации, сравнимой с квалификацией разработчика. В процессе сопровождения коллектив разработчиков должен самостоятельно принимать технологические, алгоритмические, реализационные решения.

При разработке программных средств, особенно средств общего программного обеспечения, встает проблема использования исходных текстов готовых программ, имеющих функциональность близкую к требуемой. Несмотря на разнообразие программ с открытым исходным текстом применение их в качестве основы для создания программных средств, удовлетворяющих требованиям ИБ, ограничено способностью разработчика к проведению полномасштабной инспекции исходного кода. Результатом такой инспекции должно быть «владение» исходным текстом и заложенными в нем алгоритмами на уровне разработчика. Другими словами, коллектив, применяющий готовые исходные тексты при создании программного средства, должен обладать квалификацией, достаточной для самостоятельной, без заимствований исходного текста разработки. В этом случае заимствованный исходный текст представляет собой источник апробированных программных решений. Инспекционный контроль не может быть сведен к тестированию заимствованного текста, поскольку тестирование представляет собой проверку на соответствие (или несоответствие) спецификациям, а функциональность недекларированных функций (при их наличии) априори неизвестна и не специфицирована.

Таким образом, выполнение требований ИБ и ТН обеспечивается разработкой программного средства отечественным доверенным коллективом, применением сертифицированных инструментальных средств, сертификацией разрабатываемых средств.

3. Технология разработки комплекта средств ОПО реального времени

Минимальный комплект, обеспечивающий разработку и исполнение приложений реального времени, включает операционную систему и компилятор. Во многих случаях такой минимальный комплект обеспечивает разработку приложений, функционирующих в автоматическом режиме.

При разработке операционной системы была выбрана наиболее радикальная технология обеспечения требований ИБ и ТН – разработка ядра ОС без заимствований готовых текстов. Дополнительное преимущество такого подхода, помимо обеспечений требований ИБ и ТН, - гарантированная лицензионная чистота.

Однако при этом возрастает риск принятия не апробированных и даже ошибочных реализационных и алгоритмических решений. Для того чтобы свести этот риск к минимуму, в рамках разработки комплекта средств ОПО реального времени было принято решение максимального использования международных формально утвержденных и фактических стандартов, поскольку стандарты представляют собой концентрированный опыт успешных программных разработок. Кроме того, строгое соответствие стандартам на уровне программных платформ обеспечивает мобильность прикладного программного обеспечения при модификации средств ОПО в продолжение жизненного цикла.

Разработка комплекта ОПО реального времени осуществлялась на базе следующих существовавших на момент разработки стандартов:

- POSIX 1003.1 – прикладной интерфейс операционной системы (ISO/IEC 9945-1);
- X-Window System – сетевая оконная графическая система;
- TCP/IP – семейство сетевых протоколов;
- Си - Programming languages – C, ISO/IEC 9899.

В качестве элемента разработки были подготовлены издания по трем из перечисленных стандартов, включая русский перевод POSIX 1003.1 [3], [4], [5].

В результате реализации такого подхода в 2001 г. была разработана, испытана и прошла сертификацию операционная система реального времени ос2000 [6]. Исходный текст операционной системы примерно на 80% является оригинальным. Заимствованными частями являются модули, обеспечивающие сетевое взаимодействие, и файловая система. В качестве источника заимствованных текстов был выбран BSD UNIX, поскольку эта ОС имеет «наиболее свободную» лицензию. Таким образом, ос2000 в максимальной степени соответствует требованиям ИБ и ТН.

Набор системных вызовов операционной системы ос2000 соответствует стандарту POSIX 1003.1. Однако, в отличие от требований этого стандарта, ос2000 реализована как однопроцессная система – многозадачность в ОС реализована как многопоточность. Это было связано с тем, что поддержка механизма многопроцессности и соответственно разделения ресурсов привела бы к существенной потере реактивности ОС, что противоречит требованиям реального времени.

При разработке компилятора использовался прототип gcc, разработанный в рамках проекта GNU.

4. Требования к комплекту средств ОПО реального времени

Помимо требований, обеспечивающих применение операционной системы в вычислительных комплексах, функционирующих в режиме реального времени, и требований к ИБ и ТН при разработке средств ОПО реального времени необходимо было принять технические решения по следующим вопросам:

- выбор технологии разработки (кросс- или одноплатформенной);
- выбор инструментальных средств;
- обеспечение мобильности программных средств при модификации СВТ;
- обеспечение мобильности прикладного ПО при модификации СВТ и модификации программных средств реального времени;
- выбор номенклатуры программных средств.

Основные программные решения, связанные с реализацией требований реального времени и архитектуры ос2000, изложены в [6].

Для систем реального времени характерной является технология кросс-разработки приложений. При кросс-разработке прикладная программа разрабатывается на инструментальном компьютере в среде инструментальной операционной системы. Готовый к исполнению программный модуль, называемый образом операционной системы, содержащий как модули прикладного ПО, так и модули ОС, обеспечивающие выполнение прикладного ПО, загружается на целевую ЭВМ и затем исполняется. Загрузка осуществляется по протоколу TCP/IP. При этом возможны два варианты процедуры загрузки-исполнения. При технологическом (или отладочном) режиме исполнение приложения начинается сразу после окончания загрузки. При эксплуатационном режиме образ операционной системы записывается в энергонезависимую память целевой ЭВМ. Приложение начинает исполняться при включении питания целевой ЭВМ. Технология кросс-разработки позволяет радикально уменьшить состав ПО целевой ЭВМ за счет исключения из памяти ЭВМ различных инструментальных средств. Кроме того, типичный аппа-

ратный комплекс реального времени представляет собой бездисковую ЭВМ, что делает разработку приложения непосредственно на целевой ЭВМ нереализуемой.

Кроме того, кросс-разработка обеспечивает высокую надежность приложения за счет того, что локальное, то есть средствами ПО, локализованными на целевой ЭВМ, случайное или преднамеренное изменение прикладного ПО невозможно.

Для ос2000 в качестве инструментальной ОС была выбрана ОС Linux, соответственно в качестве инструментальных применяются ЭВМ с микропроцессорной архитектурой Intel.

В качестве языка программирования для разработки приложений для ос2000 был выбран язык Си. Выбор языка Си был обусловлен универсальностью, апробированностью и высоким уровнем стандартизации.

Одной из целей при разработке комплекта средств ОПО реального времени было обеспечение мобильности. Программа мобильна, если ее возможно адаптировать к новому или модернизируемому оборудованию при минимальных изменениях исходного текста. В идеальном случае адаптация не требуется – одно и то же ПО может исполняться на различном оборудовании. Мобильность должна обеспечиваться как для самого общего программного обеспечения, так и для приложений, для которых средства ОПО являются платформой разработки-исполнения.

Мобильность операционной системы ос2000 обеспечивается разработкой программного компонента, формально не входящего в саму операционную систему, предоставляющего операционной системе инвариантный программный интерфейс для доступа к оборудованию. Этот программный компонент называется пакет поддержки модуля (ППМ). Он входит в состав процессорных модулей, на которых исполняется ос2000, и поставляется вместе с этими модулями. Сама операционная система непосредственно использует только ресурсы микропроцессора. Доступ ко всем остальным устройствам процессорного модуля, в том числе ко внешним интерфейсам, осуществляется через обращение к функциям ППМ. Поэтому при модификации оборудования (при неизменности микропроцессора) адаптация операционной системы не требуется. Помимо технологического удобства это повышает надежность ОС, поскольку минимизирует количество версий ОС и обеспечивает постоянство кода. Начиная с 2001 г., были выпущены три издания операционной системы, каждая из которых серийно поставляется.

Мобильность прикладного ПО обеспечивается неизменяемостью прикладного программного интерфейса ресурсов, предоставляемых ос2000 и другими целевыми программными средствами. Модификация прикладного программного интерфейса в течение жизненного цикла изделий (сейчас уже в течение 6 лет) осуществляется при сохранении ранее разработанного интерфейса, путем добавления новых функций. Обеспечению стабильности прикладного интерфейса в решающей степени способствует поддержка соответствия стандартам, поскольку стандарты исчерпывающе описывают не только синтаксис, но и семантику системных функций.

Выбор номенклатуры средств ОПО реального времени базировался на принципе минимальной функциональной достаточности.

Для создания автоматических систем, функционирующих в режиме реального времени, достаточно операционной системы и компилятора. Разработка автоматизированных систем, включающих диалоговые компоненты, требует графических систем разного уровня. Поэтому в начальный комплект средств ОПО реального времени были включены графическая библиотека для операционной системы реального времени (ГБРВ) и графический сервер для операционной системы реального времени (ГСРВ), реализующие соответственно функциональность X-клиента и X-сервера.

Для обеспечения хранения данных в задачах АСУ для ос2000 была разработана библиотека базы данных для ОС реального времени (ББДРВ), а для работы с

геоинформационными данными – библиотека географической информационной системы (БГИСРВ).

Наконец, для отладки приложений разработан отладчик ОРВ, обеспечивающий отладку приложений в терминах исходного текста.

Разработанный комплект программных средств ОПО реального времени ориентирован на отечественные процессорные модули с повышенными требованиями к защите от внешних воздействий (индустриальные ЭВМ). Типовой процессорный модуль представляет собой однопроцессорный компьютер с интерфейсом VME. На процессорный модуль могут устанавливаться мезонинные модули, один или два, реализующие внешние интерфейсы (SCSI, IDE, Arinc, мультиплексный канал, др.). Типовая ЭВМ включает несколько взаимодействующих по шине VME процессорных модулей. В процессорных модулях, на которых функционирует комплект средств ОПО реального времени, используется процессор с архитектурой MIPS. Также поддерживаются микропроцессоры с архитектурой Intel.

Для поддержки многопроцессорных конфигураций в состав ос2000 включены средства, обеспечивающие и стандартизующие это взаимодействие.

Таким образом, в 2001 г. был разработан и сертифицирован комплект отечественных средств общего программного обеспечения, предназначенный для поддержки разработки и исполнения приложений, функционирующих в составе автоматических и автоматизированных систем реального времени. Разработанный комплект удовлетворяет требованиям ИБ и ТН. В начальный комплект вошли операционная системы ос2000, Си-компилятор, отладчик, X-клиент (ГБРВ), X-сервер (ГСРВ), библиотека базы данных (ББДРВ), библиотека географической информационной системы (БГИСРВ).

Соответствие стандартам как операционной системы ос2000, так и других средств ОПО, предоставляет возможность эффективного использования этих средств в качестве универсальной программной платформы и при создании автоматизированных систем, к которым специальные требования реального времени не предъявляются.

5. Технические характеристики программных средств ОПО реального времени

Ниже приведены технические характеристики разработанных средств ОПО реального времени.

5.1. Операционная система ос2000

Операционная система ос2000 проектировалась так, чтобы минимизировать следующие временные характеристики:

- время ответа на прерывание (время между моментом, когда был выставлен запрос на прерывание, и моментом, когда начала выполняться первая команда функции обработки прерывания);

- время ответа потока управления (время между моментом, когда был выставлен запрос на прерывание, и моментом, когда начала выполняться первая команда потока, который должен отреагировать на это прерывание).

Также учитывались другие временные характеристики.

Операционная система реального времени ос2000 разработана в соответствии с требованиями стандарта POSIX 1003.1. Единственное отличие от этого стандарта следующее: многозадачность реализована как многопоточность. Процессы в ос2000 не поддерживаются. Такое решение было принято с целью минимизации временных затрат при переключении контекста при переходе к другой задаче. Для процессов, обеспечивающих защиту и изоляцию ресурсов, затраты ресурсов на переключение контекста значительно выше, чем при переключении в контексте одного процесса.

Согласно POSIX 1003.1 операционная система ос2000 включает: средства работы с потоками, средства работы с сигналами, средства синхронизации (семафо-

ры, мьютексы, условные переменные), очереди сообщений, часы и таймеры, средства синхронного и асинхронного ввода-вывода.

В ос2000 реализована поддержка файловых систем, прерываний, поддержка многопроцессорных систем, протокола TCP/IP.

В качестве языка программирования при разработке приложений для ос2000 используется язык Си.

В целом операционная система содержит примерно 480 системных вызовов.

5.2. Инструментальные средства

В начальный комплект средств ОПО реального времени вошли Си-компилятор и отладчик.

Компилятор предназначен для компиляции программ на языке Си с получением объектных файлов, которые могут быть загружены и выполнены на целевой ЭВМ. Компилятор обеспечивает следующие возможности:

- компиляцию с различными уровнями оптимизации;
- компиляцию с формированием отладочной информации в генерируемых объектных модулях.

Отладчик обеспечивает:

- установку/удаление точек прерывания (по чтению, по записи, по выполнению, условных, локальных, временных);
- чтение/модификацию памяти;
- чтение регистров;
- дизассемблирование отлаживаемого кода;
- отладку в терминах исходного языка (язык Си);
- предоставление листинга исходного текста отлаживаемой программы;
- пошаговую отладку (с заходом/без захода в вызываемые функции и длиной шага в одну строку исходного текста или в одну машинную команду);
- раскрутку стека вызовов функций отлаживаемого потока.

Компилятор и отладчик устанавливаются и работают на инструментальной ЭВМ, функционирующей под управлением ОС Linux. Отладчик взаимодействует с приложением на целевой ЭВМ посредством агента отладки.

5.3. Графические средства

Для ведения графического диалога и вывода графических данных разработаны графические пакеты ГБРВ и ГСРВ. В соответствии с технологией разработки комплекта средств ОПО реального времени, графические пакеты разрабатывались с учетом требований графического стандарта X Window [4]. ГБРВ и ГСРВ функционируют под управлением ос2000. Возможно исполнение этих графических пакетов как на одном процессорном модуле, так и на различных. Возможны неоднородные конфигурации, когда ГБВ исполняется на процессорном модуле под управлением ос2000, а в качестве графического сервера применяется ЭВМ с ОС UNIX и встроенным X-сервером.

5.4. Библиотека базы данных

ББДРВ - это клиент-серверная реляционная система управления базами данных, обеспечивающая поддержку реляционной модели данных автоматизированных систем различного назначения, особенно систем реального времени.

В соответствии с реляционной моделью данные базы логически представлены в виде двумерных таблиц, что обеспечивает высокую степень независимости пользовательских программ от физического представления данных. ББДРВ позволяет использовать полный набор возможностей стандартного языка SQL (ГОСТ Р ИСО/МЭК 9075-93 с расширениями). В ББДРВ реализованы возможности, относящие ее к СУБД реального времени:

- возможность подачи запросов в асинхронном режиме;

- возможность обработки запросов в соответствии с установленными для них приоритетами;

- наличие аппарата обработки событий;

- возможность отделения этапа трансляции запроса от этапа его выполнения,

- возможность слежения из приложения за состоянием использования ресурсов ядра СУБД, что позволяет написать задачу с супервизорскими функциями.

5.5. Библиотека геоинформационной системы

Библиотека геоинформационной системы обеспечивает отображение и редактирование электронной карты местности (матричной или растровой), решение расчетных задач. Над картой местности может отображаться произвольное число пользовательских карт. Расчеты по карте могут выполняться в плоской прямоугольной или геодезической системе координат.

Для ускорения вычислений, связанных с высотой рельефа местности, вместе с векторной картой может быть открыта одна или несколько матриц высот.

Изображение векторной карты может перемещаться в заданную точку и разворачиваться на указанный угол.

Поверх карты местности могут быть открыты тематические пользовательские карты различного назначения. Высота и ширина пользовательской карты изменяются динамически, соответственно с добавлением, удалением или перемещением объектов.

БГИСРВ обеспечивает отбор объектов, лежащих в указанной точке или заданной области. Объекты могут отбираться по номеру слоя, виду локализации (линия, полигон, точка, подпись), виду объекта, значению семантических характеристик, размерам и т.д. По карте могут рассчитываться расстояние, превышение, азимут, площадь, периметр, количество объектов, удовлетворяющих заданным условиям и т. п. При отсутствии векторной карты местности может использоваться отсканированный картографический материал (растр). Из отдельных растров может собираться единая растровая карта на большую территорию. После ввода паспортных данных каждый растр автоматически отображается на своем листе. Количество отображаемых растров программно не ограничено. Растровое изображение фотоснимка может отображаться совместно с пользовательскими картами.

5.6. Дальнейшие разработки

В 2001 – 2006 гг. разработаны три издания операционной системы ос2000 (включая начальное издание). В результате увеличилась функциональность операционной системы и увеличилась номенклатура поддерживаемых микропроцессоров. Вместе с операционной системой были доработаны с расширением функциональности другие программные средства.

Дополнительно разработаны следующие программные средства: программа просмотра и обработки протокола событий операционной системы и прикладной программы для операционной системы реального времени (Трассировщик ОС РВ), библиотека интерфейсных компонентов для операционной системы реального времени (БИКРВ), система визуального проектирования для операционной системы реального времени (СВПРВ), система коллективной разработки программ для операционной системы реального времени (СКРПРВ), построитель графических интерфейсов для операционной системы реального времени (ПГИРВ), файловый сервер для операционной системы реального времени (ФСРВ).

Работа [7] посвящена анализу информационной безопасности систем на платформе ос2000. В работе содержится вывод, что на базе ос2000 возможно получить решения, допускающие сквозную сертификацию по требованиям безопасности – от аппаратной платформы до прикладного уровня.

6. Заключение

В 2001 г. в НИИСИ РАН был разработан комплект средств общего программного обеспечения для вычислительных систем, функционирующих в реальном масштабе времени. Разработанный комплект ОПО удовлетворяет требованиям информационной безопасности и технологической независимости.

Разработанные средства соответствуют требованиям стандарта на интерфейс мобильной операционной системы POSIX 1003.1, сетевого стандарта TCP/IP, графического стандарта X Window, стандарта на язык SQL, стандарта на язык Си.

Функциональные характеристики операционной системы ос2000 позволяют создавать на ее основе автоматические системы управления жесткого реального времени. Наличие графических средств, а также библиотеки базы данных и геоинформационной системы предоставляют возможность создания на базе комплекта средств ОПО автоматизированных систем широкого назначения. Средства ОПО реального времени сертифицированы. В период с 2001 – 2007 гг. средства ОПО доработаны с целью расширения их функциональности, а также дополнительно разработаны новые целевые и инструментальные средства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 15408-1-2002, Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель, – М. Госстандарт России, 2002.

2. Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». -М. Гостехкомиссия, 1992.

3. ISO/IEC 9945-1 ANSI/IEEE Std 1003.1 Вторая редакция 1996-07-12. Информационная технология. Интерфейс мобильной операционной системы (POSIX). Часть 1: Интерфейс прикладных программ (API). – М., НИИСИ РАН, 1999.

4. Графический стандарт X Window, Функции библиотеки X lib, – М., НИИСИ РАН, 2000.

5. Сетевой стандарт TCP/IP, Спецификация протоколов обмена данными, – М., НИИСИ РАН, 2001.

6. *Безруков В.Л., Годунов А.Н., Назаров П.Е., Солдатов В.А., Хоменков И.И,* Введение в ос2000, Вопросы кибернетики. Информационная безопасность, Операционные системы реального времени, Базы данных/Под ред. чл.-корр. РАН В.Б.Бетелина. – Москва; НИИСИ РАН, 1999, – С. 76 – 106.

7. *Бетелин. В.Б, Галатенко В.А., Годунов А.Н., Грюнталь А.И.* Анализ информационной безопасности систем на платформе ОС РВ Багет // Безопасность информационных технологий. 2002, № 4.

В.В. Котенко
Россия, г. Таганрог, Технологический институт ЮФУ

СТРАТЕГИЯ ПРИМЕНЕНИЯ ТЕОРИИ ВИРТУАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ ПРИ РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современная стратегия информационной безопасности, ставящая основной целью обеспечение гарантированной стойкости защиты информации, порождает с позиций криптоанализа довольно парадоксальную ситуацию. С одной стороны, в рамках данной стратегии изначально постулируется возможность обеспечения гарантированной защиты информации только в пределах некоторого так называемого обозримого времени, что определяет правомочность применения теоретически дешифруемых алгоритмов защиты. С другой стороны, неопределённость само-