На правах рукописи

ВОВК Александр Михайлович

ПОСТРОЕНИЕ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ГИБРИДНЫХ ОС

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург - 2005

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования “Санкт-Петербургский государственный политехнический университет”.

Научный руководитель:

Доктор технических наук, профессор Дмитрий Петрович Зегжда

Официальные оппоненты:

Доктор технических наук, профессор Хомоненко Анатолий Дмитриевич

Кандидат технических наук, старший преподаватель Фокин Андрей Олегович

Ведущая организация:

ЗАО "Санкт-Петербургский Региональный Центр Защиты Информации"

Защита состоится «1» декабря 2005 г. в 16 часов на заседании диссертационного совета Д 212.229.27 при ГОУ ВПО “Санкт-Петербургский государственный политехнический университет” по адресу 195251, Санкт-Петербург, Политехническая 29, ауд. 175 главного здания.

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского государственного политехнического университета.

Автореферат разослан «31» октября 2005 г.

Ученый секретарь диссертационного совета Платонов В.В.

Общая характеристика работы

В настоящее время уделяется большое внимание вопросам построения защищенных информационных систем, что связано с растущей необходимостью применения современных информационных технологий в тех областях, для которых основным требованием к автоматизированным системам обработки информации является обеспечение безопасности. Широко распространенные операционные системы (ОС) типа Linux или Windows не могут удовлетворить этому критерию. В то же время эти ОС обладают огромным количеством приложений для обработки информации и имеют привычный для пользователя интерфейс.

Наиболее полные исследования проблем обеспечения безопасности информации, использования незащищенных компонентов для безопасной обработки информации, подходов к построению защищенных информационных систем и моделей безопасности выполнены в работах В.А. Герасименко, С.П. Расторгуева, Л.М. Ухлинова, А.И. Толстого, С.Н. Смирнова, А.А. Грушо, А.Ю. Щербакова, Зегжды П.Д., а также зарубежных К. Лендвера, Д. МакЛина, Р. Сандху, П. Самарати, М. Бишопа, К. Брайса, П. Ньюмена, Т. Джегера и многих других.

На основе этих результатов для удовлетворения высоких требований к безопасности создаются специальные защищенные ОС (ЗОС), нацеленные в основном на обеспечение безопасности и сохранение целостности защищаемых информационных ресурсов.

Такие ОС используются в узкоспециализированных областях и не имеют достаточно широкого набора пользовательских приложений, при помощи которых можно было бы работать с защищаемыми информационными ресурсами. Задача создания ЗОС, совместимой с распространенными приложениями, может быть решена при помощи портирования распространенных приложений в среду ЗОС. Однако этот путь требует значительных временных финансовых и интеллектуальных затрат.

Данная работа посвящена использованию другого подхода к обеспечению совместимости ЗОС с распространенными приложениями - выполнению в среде ЗОС приложений распространенной ОС без их модификации с использованием технологии гибридных ОС.

Суть технологии гибридных ОС в том, что на компьютере, работающем под управлением одной ОС (т.н. “базовой”), создается одна или несколько отдельных копий другой ОС (т.н. “встраиваемой”). Базовая ОС имеет эксклюзивный доступ к аппаратуре и контролирует все ресурсы вычислительной системы. Встраиваемые ОС не имеют непосредственного доступа к аппаратуре и взаимодействуют лишь с базовой ОС.

Гибридную ОС, в которой базовая ОС является защищенной, а встраиваемая ОС совместима с широким набором приложений, будем называть защищенной гибридной ОС (ЗГОС). Такое решение позволяет включать в состав защищенной информационной системы незащищенные компоненты – распространенную ОС и ее приложения, которые изначально не были рассчитаны на безопасную обработку конфиденциальной информации и работу со средствами защиты.

По сравнению с традиционными технологиями построения защищенных информационных систем, основанными либо на разработке специальных ЗОС, либо на интеграции средств защиты в распространенные ОС, применение технологии ЗГОС имеет следующие преимущества:

1. Полный контроль доступа распространенных приложений к информационным ресурсам со стороны доверенных средств защиты из состава базовой ЗОС.
2. Невозможность обхода или отключения защиты с помощью распространенных приложений, поскольку они находятся под контролем базовой ЗОС и не имеют доступа к аппаратуре.
3. Множество доступных приложений базовой ЗОС расширяется за счет приложений встраиваемой ОС, что позволяет использовать ЗГОС практически везде, где применяется встраиваемая ОС.
4. Накладные расходы на выполнение распространенных приложений в среде ЗГОС не велики — фактически единственным дополнительно исполняемым кодом, по сравнению с обычной встраиваемой ОС, является код средств защиты базовой ЗОС.

Следовательно, научные исследования проблемы безопасного использования распространенных приложений для обработки конфиденциальной информации и расширения множества приложений ЗОС можно признать **АКТУАЛЬНЫМИ.**

Данный вывод обусловил необходимость постановки и решения **НАУЧНОЙ ЗАДАЧИ** создания защищенной информационной системы, состоящей из защищенных и незащищенных компонентов с использованием технологии гибридных операционных систем.

ЦЕЛЬЮ диссертации является обеспечение безопасного применения приложений распространенных ОС для обработки конфиденциальной информации на основе использования технологии гибридных операционных систем. Для достижения этой цели в работе решались следующие основные задачи:

1. Анализ подходов к решению задачи построения гибридных ОС и выбор подхода для создания ЗГОС;
2. Разработка на базе выбранного подхода архитектуры ЗГОС, позволяющей безопасно использовать приложения встраиваемой ОС для обработки информации, находящейся под защитой базовой ЗОС;
3. Разработка общей модели безопасности ЗГОС, устанавливающей связь между безопасностью ЗГОС и безопасностью базовой ЗОС;
4. Реализация ЗГОС на базе предложенной архитектуры и общей модели безопасности ЗГОС;
5. Создание на базе разработанной ЗГОС макета защищенной информационной системы, позволяющего продемонстрировать преимущества данного подхода к построению защищенных информационных систем;
6. Исследование эффективности предлагаемого подхода к построению защищенных информационных систем при помощи построения модели нарушителя.

ОБЪЕКТОМ ИССЛЕДОВАНИЙ данной работы являются защищенные операционные системы, построенные с использованием незащищенных компонентов, а **ПРЕДМЕТОМ** – методы защиты, обеспечения безопасности и обработки информации в защищенных информационных системах.

ОСНОВНЫЕ НАУЧНЫЕ РЕЗУЛЬТАТЫ И ИХ НОВИЗНА.

1. Проведен анализ подходов к построению гибридных операционных систем, позволяющий выбрать архитектуру построения ЗГОС.
2. Сформулированы требования к архитектуре ЗГОС, позволяющие базовой ЗОС обеспечить контроль доступа к ресурсам со стороны встраиваемой ОС. Предложена архитектура ЗГОС, удовлетворяющая сформулированным

требованиям и позволяющая использовать приложения встраиваемой ОС для работы с ресурсами, находящимися под защитой базовой ЗОС.

3. Предложена общая модель безопасности ЗГОС, описывающая взаимодействие средств контроля доступа базовой и встраиваемой ОС, которая показывает, что при соблюдении сформулированных требований к архитектуре безопасность ЗГОС определяется безопасностью базовой ЗОС.
4. На базе предложенной архитектуры и общей модели безопасности ЗГОС на основе защищенной ОС “Феникс” и распространенной ОС “Линукс” разработана ЗГОС “Линукс-Феникс”.
5. На базе разработанной ЗГОС создан макет защищенной системы документооборота, обеспечивающий безопасное применение приложений для обработки конфиденциальной информации на основе использования технологии гибридных операционных систем.
6. Построена модель нарушителя, позволяющая продемонстрировать эффективность и практическую значимость предлагаемого решения для построения защищенных информационных систем с использованием незащищенных компонентов.

ПОЛОЖЕНИЯ, ВЫНОСИМЫЕ НА ЗАЩИТУ:

1. Анализ подходов к решению задачи построения гибридных ОС, позволяющий выбрать архитектуру ЗГОС.
2. Архитектура ЗГОС и требования к архитектуре ЗГОС, позволяющие использовать приложения встраиваемой ОС для обработки информации, находящейся под защитой базовой ЗОС.
3. Общая модель безопасности ЗГОС, показывающая, что безопасность ЗГОС определяется безопасностью базовой ЗОС.
4. ЗГОС, разработанная на основе защищенной ОС “Феникс” и распространенной ОС “Линукс” на базе предложенной архитектуры и общей модели безопасности ЗГОС “Линукс-Феникс”.
5. Макет защищенной системы документооборота, построенный на базе разработанной ЗГОС, предоставляющий пользователю изолированные среды для обработки информации разного уровня конфиденциальности.
6. Модель нарушителя, демонстрирующая эффективность и практическую значимость предложенного решения для построения защищенных информационных систем с использованием незащищенных компонентов.

ПРАКТИЧЕСКАЯ ЦЕННОСТЬ РАБОТЫ.

В основу диссертационной работы положены результаты, полученные автором в научно-исследовательских работах и практических разработках защищенных информационных систем, проводимых на кафедре информационной безопасности компьютерных систем СПбГПУ в период с 2001 по 2005 год:

1. Предложен подход к построению защищенных информационных систем с использованием технологии гибридных ОС, позволяющий расширить область применения защищенных информационных систем обработки конфиденциальной информации.

2. Разработана ЗГОС “Линукс-Феникс” на основе защищенной ОС “Феникс” и распространенной ОС “Линукс” на базе предложенного подхода.

3. Создан проект защищенной системы документооборота на базе разработанной ЗГОС, обеспечивающий безопасное применение приложений для обработки конфиденциальной информации.

ВНЕДРЕНИЕ РЕЗУЛЬТАТОВ.

Результаты проведенных исследований нашли практическое применение в разработках, в которых автор принимал личное участие в качестве ответственного исполнителя.

1. Созданная ЗГОС “Линукс-Феникс” использовалась в ЗАО “Инфосистемы Джет” для обеспечения защиты распределенных локальных сетей, обрабатывающих конфиденциальную информацию (акт об использовании результатов от 10 октября 2005 г.).

2. Созданный в процессе работы над диссертацией макет защищенной системы документооборота на базе ЗГОС “Линукс-Феникс” использовался в ЗАО "Санкт-Петербургский Региональный Центр Защиты Информации" (акт об использовании результатов от 17 октября 2005 г.).

АПРОБАЦИЯ И ПУБЛИКАЦИЯ РЕЗУЛЬТАТОВ РАБОТЫ. Научные результаты, полученные в диссертационной работе докладывались на межведомственных и международных научно-технических конференциях, опубликованы в 9 статьях.

В дальнейшем результаты диссертации целесообразно использовать в специализированных организациях Министерства Обороны Российской

Федерации, ФСБ, ФСТЭК, системе Банка России и промышленности при организации систем защиты и хранения конфиденциальной информации.

СТРУКТУРА И ОБЪЕМ ДИССЕРТАЦИИ. Диссертационная работа состоит из введения, пяти глав, заключения, приложения и списка литературы. Работа изложена на 102 листах машинописного текста (включая 29 рисунков, 6 таблиц и список литературы из 81 наименования).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В ПЕРВОЙ ГЛАВЕ для решения задачи выбора архитектуры ЗГОС был проведен анализ существующих подходов к решению задачи построения гибридных ОС. Подходы к решению задачи построения гибридных ОС отличаются способом создания среды для работы приложений встраиваемой ОС (Табл. 1).

Подходы к построению гибридных ОС	Встраиваемая ОС				
	Ядро				Прило-жения
	Компоненты для работы с аппаратурой	Драй-веры	Подсистемы планирования и распределения ресурсов	Прикладной программный интерфейс	
Эмуляция аппаратной платформы	Интер-претация	Интерп-ретация	Интерпре-тация	Интерпре-тация	Интер-претация
Создание в составе базовой ОС виртуальной машины	Интер-претация	Эму-ляция	Исполнение	Исполне-ние	Испол-нение
Эмуляция прикладного программного интерфейса	Отсутст-вие	Отсут-ствие	Отсутствие	Эмуляция	Испол-нение
Преобразование встраиваемой ОС в приложение базовой ОС	Эмуля-ция	Эму-ляция	Исполнение	Исполне-ние	Испол-нение

Табл. 1 Способы создания среды для работы приложений встраиваемой ОС

Используемый для построения ЗГОС подход должен удовлетворять следующим требованиям: обеспечивать достаточный уровень быстродействия, быть совместимым с максимальным числом приложений и обладать приемлемой трудоемкостью реализации (Табл. 2).

Требования	Эмуляция аппаратной платформы	Создание в составе базовой ОС виртуальной машины для запуска встраиваемой ОС	Эмуляция прикладного программного интерфейса	Преобразование встраиваемой ОС в приложение базовой ОС
Высокое быстродействие приложений встраиваемой ОС	-	+	+	+
Возможность запуска различных встраиваемых ОС	+	+	-	-
Совместимость с приложениями встраиваемой ОС	+	+	-	+
Низкая трудоемкость реализации гибридной ОС	-	-	-	+
Отсутствие исходных кодов встраиваемой ОС	+	+	+	-

Табл. 2 Подходы к решению задачи построения гибридных ОС

В качестве подхода к решению задачи построения ЗГОС предлагается подход “преобразование встраиваемой ОС в приложение базовой ОС”, т.к., по сравнению с другими подходами, он в наибольшей степени удовлетворяет выдвинутым требованиям.

ВО ВТОРОЙ ГЛАВЕ был проведен анализ защищенных ОС, на основании которого были сформулированы требования к архитектуре ЗГОС, позволяющие обеспечить безопасность информации при работе с ней распространенных приложений:

1. Все взаимодействия как между встраиваемыми ОС, так и между встраиваемой ОС и базовой ЗОС должны осуществляться под контролем базовой ЗОС.
2. Средства защиты базовой ЗОС должны осуществлять контроль доступа встраиваемой ОС к ресурсам базовой ЗОС.

Предложенный подход к решению задачи построения ЗГОС и сформулированные требования к архитектуре ЗГОС обусловили выбор архитектуры ЗГОС. Входящие в ЗГОС операционные системы, взятые по

отдельности, имеют недостатки, не позволяющие их использовать в качестве защищенной информационной системы – недостатки защиты и отсутствие приложений. Совместно они создают систему, способную обеспечить защиту информации и отвечающую потребностям пользователей в обработке такой информации.

В ЗГОС все функции защиты реализованы в базовой ЗОС, в среде которой на правах обычных пользовательских процессов работают копии встраиваемой распространенной ОС. Каждый пользователь имеет в своем распоряжении персональную копию среды встраиваемой ОС, полностью изолированную от всех остальных (Рис. 1).

Рис. 1. Архитектура ЗГОС

Встраиваемая ОС не имеет непосредственного доступа к ресурсам, находящимся под защитой базовой ЗОС. Единственный способ получить такой доступ – обратиться к средствам защиты базовой ЗОС, которые могут разрешить или запретить доступ к защищаемым ресурсам на основании действующей в базовой ЗОС политики безопасности. Обращение к средствам защиты базовой ЗОС не требует специальных действий со стороны приложений встраиваемой ОС, что позволяет работать с защищаемой информацией при помощи широкого набора существующих приложений встраиваемой ОС.

В ЗГОС ресурсы встраиваемой ОС могут быть интегрированы в пространство ресурсов базовой ЗОС, т.к. изолированная копия среды встраиваемой ОС также является ресурсом базовой ЗОС. Например, в ЗГОС нет необходимости создавать приложения, которые реализуют какую-либо защищенную службу (например, web-сервер). Служба, работающая в среде встраиваемой ОС, может выступать в базовой ЗОС в качестве защищаемого ресурса. С такой службой могут работать как клиенты базовой ЗОС, так и клиенты других копий встраиваемой ОС (Рис. 2).

Для обеспечения безопасности информации необходимо осуществлять контроль над сетевыми взаимодействиями. На Рис. 3 изображена схема сетевых

средств защиты ЗГОС: Внутренняя виртуальная сеть объединяет стеки сетевых протоколов копий среды встраиваемой ОС и стек сетевых протоколов приложений базовой ЗОС в единую сеть, которая может быть связана с внешней сетью. Все сетевые взаимодействия в ЗГОС контролируются средствами защиты базовой ЗОС.

Рис. 2. Доступ к ресурсам ЗГОС

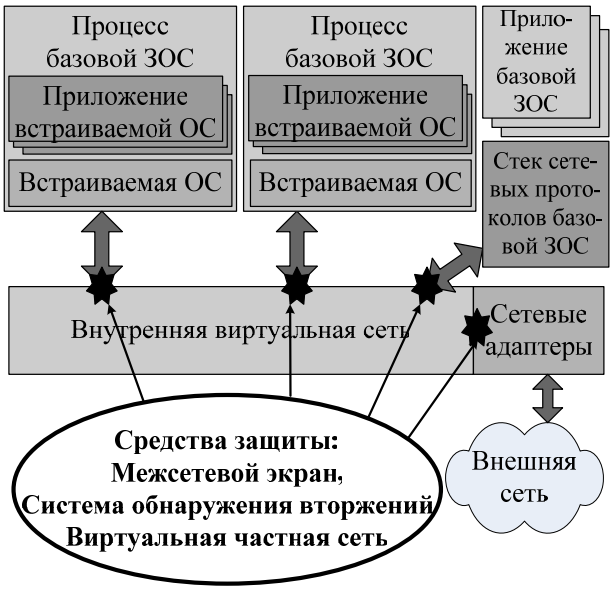


Рис. 3. Сетевые средства защиты ЗГОС

В ТРЕТЬЕЙ ГЛАВЕ предложена общая модель безопасности ЗГОС.

В ЗГОС, в отличие от систем с обычной ОС сосуществует две модели безопасности – модель безопасности базовой ЗОС и модель безопасности встраиваемой ОС, что обуславливает необходимость решения теоретической задачи построения общей модели безопасности ЗГОС.

Защищенная гибридная ОС G – это кортеж: $G = \{S^{SH}, R^{SH}, Op^{SH}, AC^{SH}, L^{SH}, A^{SH}\}$, где:

- S^{SH} – множество субъектов защищенной гибридной системы. $S^{SH} = S^{H} \cup S^{G}$, где S^{H} - множество субъектов базовой ЗОС, а S^{G} - множество субъектов встраиваемой ОС.

- R^{SH} – множество ресурсов системы. $R^{SH} = R^{H} \cup R^{G}$, где R^{H} - множество ресурсов базовой ЗОС, а R^{G} - множество ресурсов встраиваемой ОС, находящихся под защитой базовой ЗОС.

- Op^{SH} – множество операций ЗГОС, которые субъекты S^{SH} могут осуществлять над ресурсами R^{SH}.

- AC^{SH} – алгоритм контроля доступа ЗГОС субъектов S^{SH} к ресурсам R^{SH}. $AC^{SH} = \{AC^H, AC^G\}$, где AC^H – алгоритм контроля доступа базовой ЗОС, а AC^G – алгоритм контроля доступа встраиваемой ОС.

- L^{SH} - безопасность ЗГОС. $L^{SH} = \{L^H, L^G\}$, где L^H – безопасность базовой ЗОС, L^G – безопасность встраиваемой ОС.

- A^{SH} – архитектура ЗГОС. $A^{SH} = \{A^H, A^G\}$, где A^H – архитектура базовой ЗОС, A^G – архитектура встраиваемой ОС.

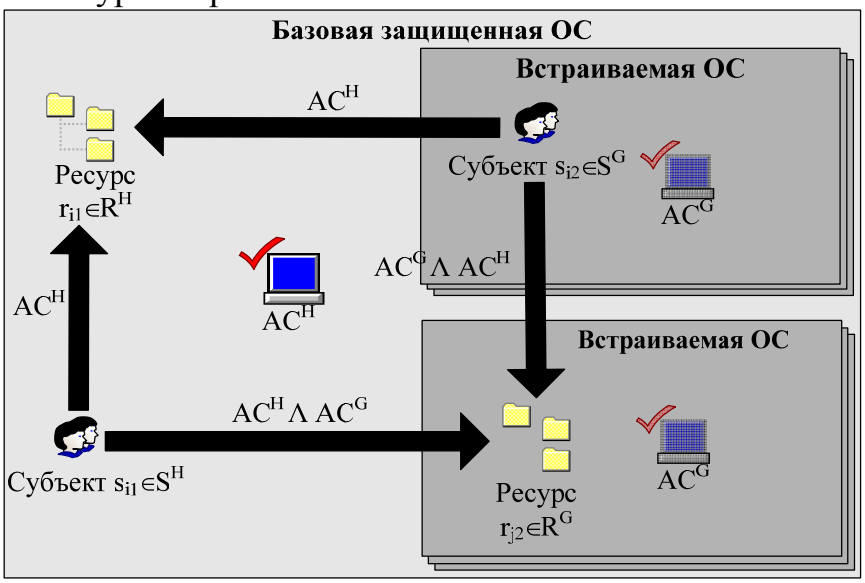


Рис. 4. Общая модель безопасности в ЗГОС

Архитектура ОС А может удовлетворять следующим требованиям:

- Все взаимодействия в системе должны осуществляться под контролем средств защиты ОС (обозначим это требование как требование контроля взаимодействий *CI(A)*). Требование выполняется тогда и только тогда, когда не существует такого взаимодействия $i_i \in I$ которое $i_i \notin IS$, где I – множество возможных взаимодействий в ОС, IS – множество взаимодействий, допускаемых средствами защиты ОС.

- Все обращения к ресурсам должны контролироваться средствами защиты ОС (обозначим это требование как требование контроля доступа *CA(A)*). Требование выполняется тогда и только тогда, когда для всех взаимодействий $i_i \in I$, соответствующих обращению субъекта $s_l \in S$ к ресурсу $r_k \in R$ с операцией $op_v \in Op$ функция безопасности $SF(s_l, r_k, op_v)$ истинна, где SF – функция безопасности ОС, S – множество субъектов ОС, R – множество ресурсов ОС, Op – множество операций ОС.

В работе сформулирована и доказана следующая теорема:
Безопасность ЗГОС (L^{SH}) определяется безопасностью базовой ЗОС (L^{H}) тогда и только тогда, когда архитектура базовой ЗОС (A^{H}) удовлетворяет требованию контроля взаимодействий $CI(A^{H})$ и требованию контроля доступа $CA(A^{H})$.

В ЧЕТВЕРТОЙ ГЛАВЕ для реализации предложенного подхода к построению защищенных информационных систем проведен анализ ОС, на основе которого для построения ЗГОС в качестве базовой ЗОС выбрана ЗОС “Феникс” (Табл. 3), в качестве встраиваемой ОС выбрана ОС “Линукс” (Табл. 4).

Защищенная ОС	Доступность исходных кодов	Наличие микро-Ядра	Возможность добавления новых типов ресурсов	Контроль взаимодействий	Контроль доступа	Унифицированный доступ к ресурсам
Trusted Mach	-	+	+	+	+	+
MCBC	-	-	+	-	+	-
Linux	+	-	-	-	-	-
Windows	-	-	+	-	+	-
Феникс	+	+	+	+	+	+

Табл. 3. Выбор базовой ЗОС

ОС	Доступность исходных кодов	Широкий набор приложений	Открытое распространение
Windows	-	+	-
Solaris	+	-	-
Linux	+	+	+

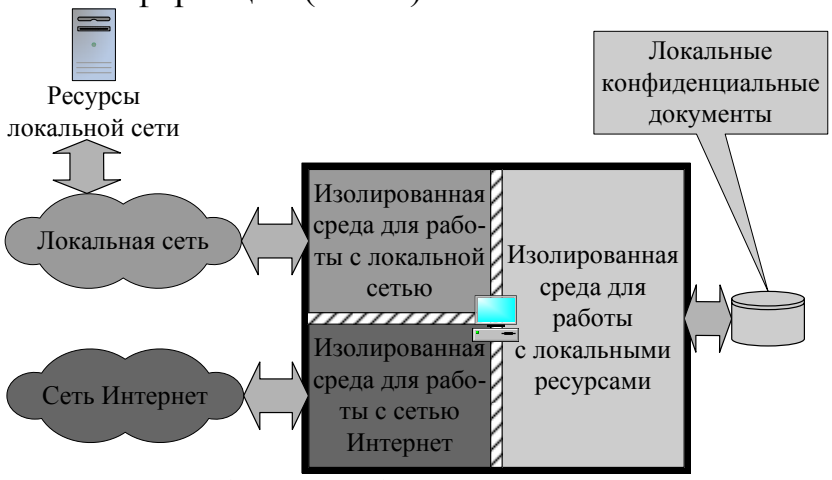
Табл. 4. Выбор встраиваемой ОС

Автором разработана ЗГОС “Линукс-Феникс”, обеспечившая пользователей ЗОС “Феникс” возможностью безопасного применения приложений ОС “Линукс” для обработки конфиденциальной информации, находящийся под защитой ЗОС “Феникс”. ”Линукс-Феникс” удовлетворяет сформулированным требованиям к архитектуре ЗГОС, построена на базе предложенной архитектуры и общей модели безопасности ЗГОС.

В ПЯТОЙ ГЛАВЕ предложен макет защищенной системы документооборота на базе ЗГОС “Линукс-Феникс”, демонстрирующий безопасное применение распространенных приложений для обработки конфиденциальной информации.

Работая с конфиденциальными документами пользователи сталкиваются с необходимостью одновременно обрабатывать информацию разных уровней конфиденциальности, при этом необходимо исключить риск для безопасности этой информации. Например, пользователю необходимо одновременно работать с локальными конфиденциальными документами, с Интернет и с ресурсами локальной сети. На текущем этапе развития защищенных информационных систем для этого пользователю необходимо работать с несколькими компьютерами: один для работы с конфиденциальной информацией, другой – для работы с Интернет, и третий для работы в локальной сети. Задача усложняется, если пользователю надо производить обмен информацией между этими компьютерами, например, отправить неконфиденциальный документ по конфиденциальному адресу.

На базе ЗГОС “Линукс-Феникс” разработана защищенная система документооборота, предоставляющая пользователю изолированные среды для обработки информации различных уровней конфиденциальности. В такой системе пользователь может одновременно работать с ресурсами Интернет, с ресурсами локальной сети и с локальной конфиденциальной информацией на одном компьютере, не нарушая безопасность обрабатываемой конфиденциальной информации (Рис. 5).



Рабочее место абонента защищенной распределенной автоматизированной системы документооборота, построенное на базе ЗГОС “Линукс-Феникс”

Рис. 5. Защищенная система документооборота

Каждая копия встраиваемой ОС “Линукс”, предоставляемая пользователю, представляет собой, изолированную среду, работающую под контролем базовой ЗОС “Феникс” и имеющую ограниченные права доступа к ресурсам. Например, копия встраиваемой ОС “Линукс”, предназначенная для обработки локальной конфиденциальной информации, вообще не имеет доступа к Интернет.

Для оценки эффективности и практической значимости предлагаемого решения составлены модели нарушителя для распространенной ОС, ЗОС и ЗГОС (Рис. 6).

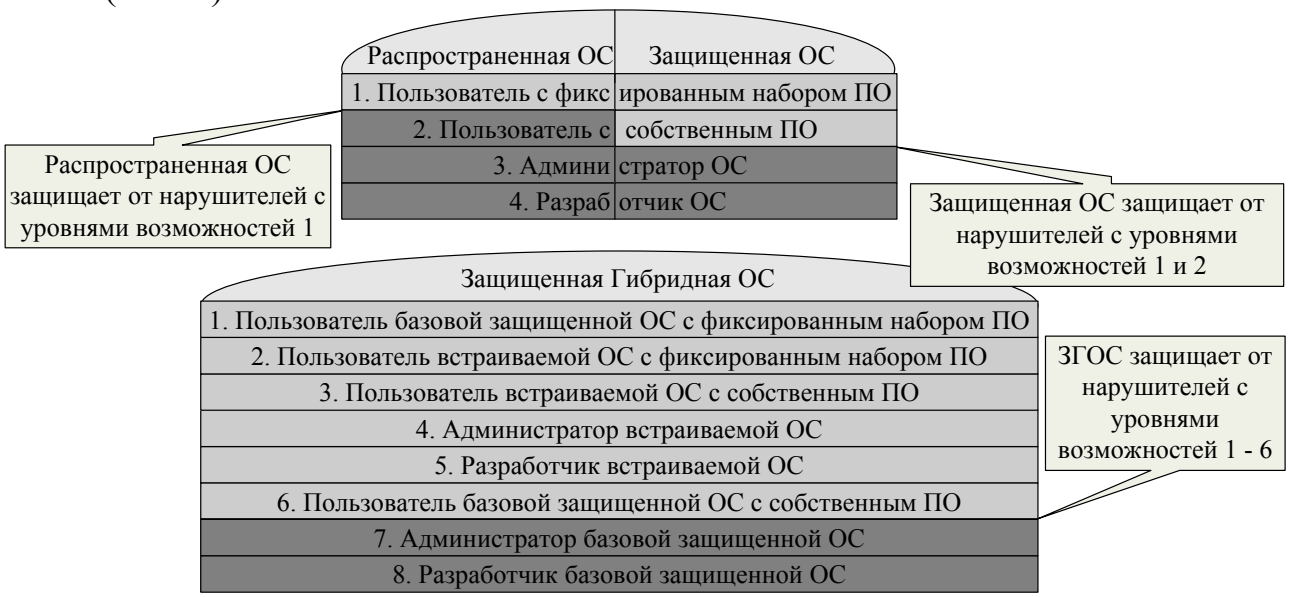


Рис. 6. Модель нарушителя для ЗГОС

В отличие от обычных ОС ЗГОС имеет 8 уровней возможностей нарушителя. Но ЗГОС защищает от 6 уровней, включая администратора и разработчика встраиваемой ОС.

Эффективность предложенного подхода с точки зрения возможностей получаемой защищенной информационной системы определяется следующим образом. Пусть $P = \{P^1 \dots P^i\}$ – множество операционных систем, каждая из которых обеспечивает безопасность обрабатываемой информации $S = \{ S^1 \dots S^i\}$ и набор средств обработки информации $N = \{ N^1 \dots N^i\}$. Таким образом защищенная информационная система есть кортеж $U = \{ P^m, S^m, N^m \}$.

Чем большую безопасность информации S^m обеспечивает ОС, тем меньшее количество средств обработки информации N^m она предоставляет пользователю. В случае применения технологии гибридных ОС защищенная информационная система представляет собой кортеж $U = \{ P^m, S^m, P^f, N^f \}$ (Рис.

7).. Для заданного уровня безопасности, определяемого базовой ЗОС, можно выбрать встраиваемую ОС, обладающую необходимым набором средств обработки информации.

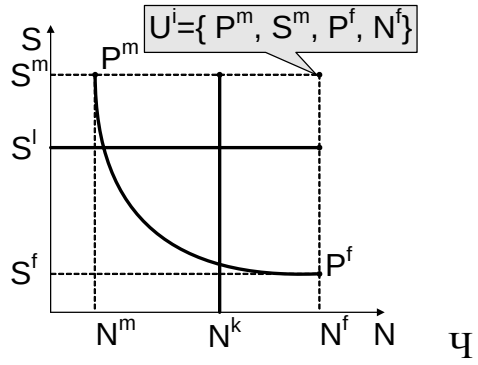


Рис. 7. Эффективность применения ЗГОС

Оценка эффективности предложенного подхода с точки зрения необходимых трудозатрат на реализацию ЗГОС проводилась при помощи сравнения трудозатрат, необходимых для безопасного использования распространенных приложений с помощью различных подходов, выраженных в строках кода (Табл. 5).

Подход	Количество строк кода	Количество приложений	Совместимость на уровне бинарных файлов
Портирование приложения под ЗОС	100000 (зависит от размера приложения)	1	Нет
Перенос библиотек распространенных ОС под ЗОС	10000	100	Нет
Построение ЗГОС	5000	Более 10000	Да

Табл. 5 Оценка эффективности предложенного решения

Предлагаемый автором подход требует меньше затрат и позволяет безопасно использовать большее количество распространенных приложений, чем другие подходы.

Основные научные результаты

Диссертационная работа является итогом научных и практических исследований, проведенных автором в период с 2001 по 2005 год. В работе получены следующие результаты:

1. Проведен анализ подходов к построению гибридных операционных систем, позволяющий выбрать архитектуру построения ЗГОС.
2. Сформулированы требования к архитектуре ЗГОС, позволяющие базовой ЗОС обеспечить контроль доступа к ресурсам со стороны встраиваемой ОС. Предложена архитектура ЗГОС, удовлетворяющая сформулированным требованиям и позволяющая использовать приложения встраиваемой ОС для работы с ресурсами, находящимися под защитой базовой ЗОС.
3. Предложена общая модель безопасности ЗГОС, описывающая взаимодействие средств контроля доступа базовой и встраиваемой ОС, которая показывает, что при соблюдении сформулированных требований к архитектуре безопасность ЗГОС определяется безопасностью базовой ЗОС.
4. На базе предложенной архитектуры и общей модели безопасности ЗГОС на основе защищенной ОС “Феникс” и распространенной ОС “Линукс” разработана ЗГОС “Линукс-Феникс”.
5. На базе разработанной ЗГОС создан макет защищенной системы документооборота, обеспечивающий безопасное применение приложений для обработки конфиденциальной информации на основе использования технологии гибридных операционных систем.
6. Построена модель нарушителя, позволяющая продемонстрировать эффективность и практическую значимость предлагаемого решения для построения защищенных информационных систем с использованием незащищенных компонентов.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Вовк А.М. Описание механизма удаленной отладки с использованием GDB // Журнал “Проблемы информационной безопасности, компьютерные системы” №2, Санкт-Петербург 2002, С. 18-22.
2. Вовк А.М., Зегжда Д.П. Построение гибридных систем на основе защищенной и популярной ОС // Конференция “Региональная информатика 2002”, Санкт-Петербург 2002, С. 27-29.
3. Вовк А.М. Зегжда Д.П. Построение гибридных систем на основе защищенной и популярной ОС // Сб. материалов конференции “Проблемы информационной безопасности в системе Высшей школы”, МИФИ, Санкт-Петербург 2003, С. 83-85.
4. Вовк А.М. Эмуляция операционных систем // Журнал «Проблемы информационной безопасности. Компьютерные системы», №3, Санкт-Петербург 2003, С. 10-13.
5. Вовк А.М., Зегжда Д.П. Применение гибридных операционных систем, // Сб. материалов конференции «ИБРР-2003», т.2, XI конференция «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург 2003, С. 86-88;
6. Зегжда Д.П., Вовк А.М. Гибридная операционная система Линукс-Феникс // XII Российская научно-техническая конференция “Методы и технические средства обеспечения безопасности информации ”, Санкт-Петербург 2004 г., С. 86-87.
7. Зегжда Д.П., Вовк А.М. Защищенная гибридная ОС Linux over Феникс // III общероссийская конференция “Математика и безопасность информационных технологий” (МаБИТ-04), Москва 2004, С. 43-45.
8. Dmitry P. Zegzhda, Alex M. Vovk. Secure Hybrid Operating System “Linux over Fenix” // Mathematical Methods, Models and Architectures for Computer Networks Security Workshop, St.Petarsburg, Russia, 2005, P. 32-33;
9. Вовк А.М. Подходы к решению задачи построения гибридных ОС // XIII Российская научно-техническая конференция “Методы и технические средства обеспечения безопасности информации ”, Санкт-Петербург 2005, С. 19-20.