

Операционная система РОСА БАРИЙ
Документация определения жизненного цикла

Листов 11

Аннотация

Данный документ содержит описание модели, применяемой при разработке и сопровождении Операционной системы, РОСА БАРИЙ (далее по тексту — ОС или изделие).

В документе предоставлена информация, удовлетворяющая требованиям компонентов доверия ALC_LCD.1 и ALC_LCD_EXT.3.1.

СОДЕРЖАНИЕ

1. Введение	4
1.1. Идентификация документа	4
2. Модель жизненного цикла	5
2.1. Общее описание	5
2.2. Жизненный цикл программного изделия	5
2.3. Жизненный цикл сертифицированного изделия	7

1. ВВЕДЕНИЕ

1.1. Идентификация документа

Название: ОС РОСА БАРИЙ Документация определения жизненного цикла.

Версия: 1.0.

Идентификация объекта оценки (ОО): Операционная система РОСА БАРИЙ.

2. Модель жизненного цикла

2.1. Общее описание

Модель жизненного цикла отражает различные состояния изделия, начиная с момента возникновения необходимости в данном программном изделии и заканчивая моментом его полного выхода из употребления. Модель жизненного цикла — структура, содержащая процессы, действия и задачи, которые осуществляются в ходе разработки, функционирования и сопровождения программного изделия в течение всей жизни изделия, от определения требований до завершения его использования.

Модель жизненного цикла изделия, определяемая на основе государственных стандартов, включает процессы и стадии, обеспечивающие выработку требований, разработку, производство и эксплуатацию изделия. Важной особенностью является то, что жизненный цикл программного изделия — непрерывный, и результаты, получаемые на предыдущих стадиях, служат основой для последующих стадий.

Модель жизненного цикла базируется на перечне работ (фаз жизненного цикла). Ниже приведены основные фазы жизненного цикла изделия:

- 1) Замысел/идея.
- 2) Разработка.
- 3) Изготовление/производство.
- 4) Использование.
- 5) Поддержка.
- 6) Прекращение использования.

2.2. Жизненный цикл программного изделия

Совокупность стадий и этапов, которые проходит изделие в своем развитии от момента принятия решения о создании изделия до момента прекращения функционирования изделия, называется жизненным циклом изделия.

Содержание жизненного цикла разработки изделия сводится к выполнению следующих стадий:

- 1) Планирование и анализ требований (предпроектная стадия) — системный анализ. Проводятся исследование и анализ, определяются требования к создаваемому изделию, формируются технико-экономическое обоснование (ТЭО) и техническое задание (ТЗ) на разработку изделия.
- 2) Проектирование (техническое и логическое проектирование). В соответствии с требованиями формируются состав функций (функциональная архитектура) и состав обеспечивающих подсистем (системная архитектура), проводится оформление технического проекта изделия.

- 3) Реализация (рабочее и физическое проектирование, кодирование). Разработка и настройка изделия, формулировка рабочих инструкций для персонала, оформление рабочего проекта.
- 4) Проведение испытаний изделия на выполнение требований технического задания.
- 5) Эксплуатация изделия (сопровождение, модернизация). Сбор рекламаций и статистики о функционировании изделия, исправление недоработок и ошибок, оформление требований к модернизации изделия и ее выполнение (повторение стадий 2–5).

Ниже рассматривается основное содержание стадий и этапов жизненного цикла изделия.

Системный анализ. Основными целями этапа являются:

формулировка потребности в новом изделии;
выбор направления и определение экономической обоснованности проектирования изделия.

Системный анализ изделия начинается с описания и анализа функционирования рассматриваемого объекта в соответствии с требованиями (целями), которые предъявляются к нему. В результате этого этапа выявляются недостатки существующего изделия, на основе которых формулируется потребность в совершенствовании изделия, и ставится задача определения экономически обоснованной необходимости (создается технико-экономическое обоснование проекта разработки изделия). После определения этой потребности возникает проблема выбора направлений совершенствования объекта на основе выбора программно-технических средств. Результаты оформляются в виде технического задания на проект, в котором отражаются технические условия и требования к изделию, а также ограничения на ресурсы проектирования.

Проектирование. Данный этап предполагает:

проектирование функциональной архитектуры изделия, отражающей структуру выполняемых функций;
проектирование системной архитектуры изделия (состава обеспечивающих подсистем);
реализацию проекта.

Формирование функциональной архитектуры, которая представляет собой совокупность функциональных подсистем и связей между ними, является наиболее ответственным и важным этапом с точки зрения качества всей последующей разработки изделия.

Построение системной архитектуры на основе функциональной предполагает определение элементов и модулей информационного, технического, программного обеспечения и других обеспечивающих подсистем, связей по информации и управлению между выделенными элементами.

Реализация включает разработку программ и инструкций для пользователей, Внедрение разработанного проекта разделяется на опытное и промышленное.

Этап опытного внедрения подразумевает проверку работоспособности изделия, устранение ошибок на уровне элементов и связей между ними. Этап сдачи в промышленную эксплуатацию заключается в организации проверки проекта на уровне функций, контроля соответствия его требованиям, сформулированным на стадии системного анализа.

Важной особенностью жизненного цикла изделия является его цикличность: системный анализ — разработка — сопровождение — системный анализ. При первом прохождении стадии «Разработка» создается проект изделия, а при последующих реализациях данной стадии осуществляется модификация проекта для поддержания его в актуальном состоянии.

2.3. Жизненный цикл сертифицированного изделия (ALC_LCD_EXT.3)

Разработчики защищенных сертифицированных программных изделий сталкиваются с двумя противоречивыми факторами:

- с одной стороны, требования защиты информации определяют необходимость сертификации программных средств, что предполагает их неизменность, подтверждаемую контрольными суммами;
- с другой стороны, изменяющиеся требования пользователей, высокая динамика развития современных технических средств и комплектующих, а также устранение ошибок и уязвимостей в программных средствах обуславливают необходимость их постоянной доработки и внесения изменений.

Эти противоречия нужно учитывать при обеспечении жизненного цикла сертифицированного изделия.

Самой ресурсоемкой стадией жизненного цикла изделия является разработка, которая ведется на основе свободного ПО. Ключевой процесс разработки — сертификация по требованиям защиты информации и предшествующая ей фиксация программного кода.

Включение в состав очередной версии дистрибутива изделия новых версий прототипов свободного ПО, исправление обнаруженных ошибок и устранение найденных уязвимостей возможны только до момента фиксации программного кода, после которой состав и содержание текстов программ уже не изменяются.

Таким образом, именно результаты разработки, достигнутые до начала сертификации, определяют последующие характеристики текущей версии сертифицированной ОС.

В целях ускорения обновления изделия жизненные циклы последующих версий могут начинаться параллельно с серийными поставками и эксплуатацией предыдущих

версий, что позволяет начать поставки новой версии сразу же после окончания срока эксплуатации предыдущей.

В отношении сертифицированных операционных систем этой схеме присущи существенные риски как заказчиков и потребителей, так и разработчиков программных изделий.

К рискам заказчиков и потребителей можно отнести:

- риск разработки ОС низкого качества из-за устаревших требований технического задания двух-трехлетней давности;
- риск несовместимости сертифицированной ОС с современными техническими средствами ввиду их постоянного развития и обновления;
- риск затруднений или невозможности применения сертифицированной ОС в других ведомствах или в межведомственных автоматизированных системах вследствие отсутствия соответствующей сертификации и техподдержки.

К рискам разработчиков программных изделий можно отнести:

- риск потери коллектива разработчиков вследствие неравномерности финансирования различных стадий жизненного цикла (финансирование НИР, серийных поставок и авторского надзора существенно ниже финансирования ОКР);
- риск невозможности поддержания жизненного цикла изделия в случае прекращения финансирования работ заказчиком или выбора другого исполнителя по результатам конкурса;
- риск невозможности использования полученного научно-технического задела вследствие того, что права на изделие принадлежат заказчику.

Последствия реализации этих рисков часто затрудняют или вовсе делают невозможным поддержание непрерывного жизненного цикла сертифицированных ОС.

Указанные особенности были учтены разработчиком при разработке модели жизненного цикла ОС, характеризующейся следующими ключевыми особенностями:

- все риски и затраты на определение требований к новым версиям дистрибутива, обеспечению разработки, производства и сопровождения эксплуатации взял на себя разработчик;
- жизненный цикл максимально уплотнен, некоторые процессы жизненного цикла поддерживаются непрерывно.

Кроме того, работы по сопровождению, эксплуатации и тестированию выполняются в одном подразделении, что позволяет организовать эффективную обратную связь между пользователями и разработчиками, направленную на повышение качества продукции и услуг.

Такая организация позволила максимально уплотнить жизненный цикл изделия и обеспечивать ежегодный выпуск сертифицированного релиза дистрибутива с

исправленными ошибками, устраненными уязвимостями и улучшенной функциональностью.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

НИР — научно-исследовательская работа.

ОКР — опытно-конструкторская работа.

ОО — объект оценки.

ОС — операционная система.

ОТК — отдел технического контроля.

ТЗ — техническое задание.

ТЭО — технико-экономическое обоснование.

