РЕДСОФТ

# Описание жизненного цикла

Мобильная операционная система РЕД ОС М


Листов 11

Москва
2023

# Оглавление

# 1 Введение

РЕД ОС М многозадачная и многопользовательская операционная система, обеспечивающая управляемый доступ субъектов к объектам доступа. Операционная система РЕД ОС М (далее - ОС) представляет собой удобно и гибко конфигурируемую ОС, основанную на модифицированном ядре Linux, которая была разработана для обеспечения приемлемого уровня безопасности, обычно требуемого в среде коммерческого применения.

В настоящем документе представлены описания системы управления жизненным циклом ОС, которая используется в ООО «РЕД СОФТ» при разработке ОС, список конфигурации и метод уникальной идентификации элементов конфигурации.

Управление конфигурацией (далее УК) помогает обеспечить сохранение целостности ОС, устанавливая и контролируя определенный порядок процессов уточнения и модификации ОС и предоставления связанной с ними информации. УК предотвращает несанкционированную модификацию, добавление или уничтожение составляющих ОС, обеспечивая тем самым доверие, что оценивается именно та ОС и документация, которые подготовлены к распространению.

Управление конфигурацией - один из методов или способов установить, что в созданной ОС реализованы функциональные требования и спецификации. УК отвечает этим целям, предъявляя требования дисциплины и контроля в процессе уточнения и модификации ОС и связанной с ним информации. Системы УК используют для обеспечения целостности частей ОС, которые они контролируют, предоставляя метод отслеживания любых изменений, и для того, чтобы все изменения были санкционированы.

# 2 Описание системы контроля версий

## 2.1 Общее описание

При разработке ОС для обеспечения контроля версий применяется программный продукт Git, который является свободно распространяемой по лицензиям GNU/GPL.

Подход Git к хранению данных похож на набор снимков миниатюрной файловой системы.

## 2.2 Возможности системы

- Git представляет свои данные как, поток снимков.
- При создании каждого коммита (сохранения состояния проекта в Git), система запоминает, как выглядит каждый файл в этот момент, и сохраняет ссылку на этот снимок.
- Для увеличения эффективности, если файлы не были изменены, Git не запоминает эти файлы вновь, а только создаёт ссылку на предыдущую версию идентичного файла, который уже сохранён.
- Хранение полной истории изменений отслеживаемых объектов (файлов, каталогов, символьных ссылок) в централизованном хранилище (репозитории), в
- Для работы большинства операций в Git достаточно локальных файлов и ресурсов — в основном, системе не нужна никакая информация с других компьютеров в вашей сети.
- В Git для всего вычисляется хеш-сумма, и только потом происходит сохранение. В дальнейшем обращение к сохранённым объектам происходит по этой хеш-сумме. Это значит, что невозможно изменить содержимое файла или каталога так, чтобы Git не узнал об этом. Данная функциональность встроена в Git на низком уровне и является неотъемлемой частью его философии.

## 2.3 Модель работы

Клиенты копируют файлы из хранилища, создавая локальные рабочие копии, затем вносят изменения в рабочие копии и фиксируют эти изменения в хранилище. Несколько клиентов могут одновременно обращаться к хранилищу. Для совместной работы над файлами в Git преимущественно используется модель копирование - изменение — слияние.

У Git есть три основных состояния, в которых могут находиться файлы: *изменён* (modified), *индексирован* (staged) и *зафиксирован* (committed):

- К изменённым относятся файлы, которые поменялись, но ещё не были зафиксированы.
- Индексированный — это изменённый файл в его текущей версии, отмеченный для включения в следующий коммит.
- Зафиксированный значит, что файл уже сохранён в вашей локальной базе.

Основные секции проекта Git: рабочая копия (working tree), область индексирования (staging area) и каталог Git (Git directory).

- Рабочая копия является снимком одной версии проекта. Эти файлы извлекаются из сжатой базы данных в каталоге Git и помещаются на диск, для того чтобы их можно было использовать или редактировать.
- Область индексирования — это файл, обычно находящийся в каталоге .git, в нём содержится информация о том, что попадёт в следующий коммит. Её техническое название на языке Git — «индекс», но фраза «область индексирования» также работает.
- Каталог Git — это то место, где Git хранит метаданные и базу объектов проекта. Это самая важная часть Git и это та часть, которая копируется при *клонировании* репозитория с другого компьютера.

Базовый подход в работе с Git выглядит так:

- Именение файлов рабочей копии.
- Выборочное добавление в индекс тех изменений, которые должны попасть в следующий коммит, добавление тем самым снимки *только* этих изменений в индекс.
- Когда делается коммит, используются файлы из индекса как есть, и этот снимок сохраняется в ваш каталог Git.

Если определённая версия файла есть в каталоге Git, эта версия считается зафиксированной (committed). Если файл был изменён и добавлен в индекс, значит, он индексирован (staged). И если файл был изменён с момента последнего распаковывания из репозитория, но не был добавлен в индекс, он считается изменённым (modified).

## 2.4 Доступ к репозиторию

В ООО «РЕД СОФТ» доступ к репозиториям Git обеспечивается из контролируемых зон объектов ООО «РЕД СОФТ» удаленно с использованием протоколов ssh и https. Доступ разработчиков обеспечивается внутри корпоративной сети.

## 2.5 Номера версии ОС

Версия ОС заносится в git в виде тега коммитов, используемых при сборке. Формируется по следующему шаблону:
*OSVER.VENDOR.HWPLATFORM.VER.BUILD*

- OSVER - Версия AOSP, на которой основана сборка
- VENDOR — Числовой код изготовителя оборудования, под которое собрано дерево.
- HWPLATFORM - Текстовое обозначение или числовой код устройства, например T2101
- VER - Номер версии. Четные - рабочие версии (production). Нечетные - тестовые (latest)
- BUILD - Номер сборки. Порядковый номер сборки, используемый для публичных сборок
- SUBBUILD - Внутренний номер сборки. Порядковый номер подсборки. Увеличивается при каждой попытке сборки дерева. Используется для отслеживания версий во время разработки.

## 2.6 Стадии разработки ОС

В разработке программного обеспечения, стадии разработки программного обеспечения используются для описания степени готовности программного продукта. Также стадия разработки может отражать количество реализованных функций, запланированных для определённой версии программы. Стадии либо могут быть официально объявлены и регламентируются разработчиками, либо иногда этот термин используется неофициально для описания состояния продукта. Следует отметить, что стадии Бета и Альфа (Пре-альфа) не являются показателями нестабильности релиза, так как присваиваются программе один раз или один раз за серию, в зависимости от системы разработки. Они могут присваиваться нескольким релизам подряд. Релизом в данном случае считается завершённая версия.

### 2.6.1 Пре-альфа

Начальная стадия разработки — Период времени со старта разработки до выхода стадии Альфа (или до любой другой, если стадии Альфа нет). Также так называются программы, не вышедшие еще в стадию альфа или бета, но прошедшие стадию разработки, для первичной оценки функциональных возможностей в действии. В отличие от альфа и бета версий пре-альфа может включать в себя не весь спектр функциональных возможностей программы. В этом случае подразумеваются все действия, выполняемые во время проектирования и разработки программы вплоть до тестирования. К таким действиям относятся - разработка дизайна, анализ требований, собственно разработка приложения, а также отладка отдельных модулей.

### 2.6.2 Альфа

Внутреннее тестирование — Стадия начала тестирования программы в целом специалистами тестерами, обычно не разработчиками программного продукта, но, как правило, внутри организации или сообществе разрабатывающих продукт. Также это может быть стадия добавления новых функциональных возможностей. Программы на данной стадии могут применяться только для ознакомления с будущими возможностями.

### 2.6.3 Бета

Публичное тестирование — Стадия активного бета-тестирования и отладки программы, прошедшей альфа-тестирование (если таковое было). Программы этого уровня могут быть использованы другими разработчиками программного обеспечения для испытания совместимости. Тем не менее, программы этого этапа могут содержать достаточно большое количество ошибок.

Поскольку бета-продукт не является финальной версией, и публичное тестирование производится на страх и риск пользователя, производитель не несёт никакой ответственности за ущерб, причинённый в результате использования бета-версии. Таким образом, многие производители уходят от ответственности, предоставляя пользователям только бета-версии

продукта.

### 2.6.4 Релиз-кандидат

Релиз-кандидат или RC (англ. Release candidate), Пре-релиз - кандидат на то, чтобы стать стабильной. Программы этой стадии прошли комплексное тестирование, благодаря чему были исправлены все найденные критические ошибки. Но в то же время существует вероятность выявления ещё некоторого числа ошибок, не замеченных при тестировании.

### 2.6.5 Релиз

Релиз или RTM (англ. release to manufacturing промышленное издание) — издание продукта, готового к тиражированию. Это стабильная версия программы, прошедшая все предыдущие стадии, в которых исправлены основные ошибки, но существует вероятность появления новых, ранее не замеченных, ошибок. RTM предшествует общей доступности (GA), когда продукт выпущен для общественности.

## 2.7 Сборка программного кода ОС

Сборка программного кода ОС производится на отдельной виртуальной ОС, размещенной на специальном выделенном серверев контролируемой зоне производственного объекта ООО «РЕД СОФТ». Доступ к виртуальной ОС имеют только определенные лица администраторов отделения разработки ОС, в круг обязанностей, которых входит работа со сборкой программного кода или иных задач по контролю за работой над разработкой кода ОС. Доступ осуществляется на основе логина и пароля пользователя.

Решение о необходимости сборки программного кода принимает руководитель отдела разработки после соответствующей проверки и тестирования всех компонентовОСи на основании решения аналитического отдела, который, в свою очередь, принимает решение на основание отчетов о проведении тестирования версии ОС отделом тестирования. Каждая сборка ОС имеет уникальный идентификатор ревизии, состоящий из номера ревизии ОС и номера версии сборки в ревизии.

## 2.8 Элементы конфигурации ОС

Элементами конфигурации ОС являются:

- исходный код ОС;
- проектная документация;
- тестовая документация;
- руководство пользователя;
- руководство администратора;
- документация УК.

## 2.9 Документация УК

### 2.9.1 Требования к составу и маркировке программной документации

Виды, комплектность и обозначение документации, создаваемойи сопровождаемойв рамках разработки ОС ,определяются ГОСТ34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем».

Состав программной документации на различных этапах создания и сопровождения ОС определяется ГОСТ19.101-77 «Виды программ и программных документов».

Маркировка программной документации на ОС соответствует ГОСТ 19.103-77 «Обозначения

программ и программных документов» и представляет из себя следующую структуру:
A.B.CCCCC-DD EE FF-G , где

- A – код страны разработчика (равен 46);
- B – код организации-разработчика (равен 98898398);
- CCCCC – регистрационный номер программного продукта по классификатору (равен 501110 –операционные системы общего назначения);
- DD – номер издания (для программы) или номер редакции (для документа);
- EE – код вида документа;
- FF – номер документа данного вида;
- G – номер части документа.

Например, документ «Руководство пользователя» маркируется следующим образом:
46.98898398.501110-01 34 1-1

### 2.9.2 Процедура формирования серийного номера продукта

Потребители и заказчики формируют заявки на поставку комплектов РЕД ОС М. Заявки направляются в адрес отдела маркетинга ООО «РЕД СОФТ».

Отдел маркетинга ООО «РЕД СОФТ» рассматривает поступающие заявки и после рассмотрения и согласования заявки предоставляет руководителю отдела материально-технического обеспечения информацию о поступлении заявки. Сведения предоставляются по служебной электронной почте в виде приложения к письму.

По информации в письме отдел материально-технического обеспечения, руководитель отдела материально-технического обеспечения формирует необходимое количество дистрибутивных комплектов программных продуктов, формирует необходимое количество серийных номеров программных продуктов, производит маркировку дистрибутивных комплектов программных продуктов, производит запись в журнале формирования и выдачи программных продуктов стенда тиражирования.

Далее отдел материально-технического обеспечения формирует письмо-уведомление для клиента о готовности дистрибутивных комплектов, после чего осуществляет доставку дистрибутивных комплектов оговоренными в заявке средствами.

### 2.9.3 Правила присвоения серийного номера программного продукта

Серийный номер состоят из набора атрибутов (таблица 1), отражающих информацию о продукте, его версии и дате выпуска дистрибутивного комплекта. В общей строке серийного номера атрибуты детерминируются разделительными символами – дефисами.
Серийный номер продукта имеет вид AA-BBB-CCC-12345678-123456-123 и состоит из:

*Таблица 1: Структура серийного номера*

| Тип серийного номера | - | Тип продукта | - | Редакция | - | Номер сборки | - | Дата формирования дистрибутивного комплекта | - | Порядковый номер комплекта за текущую дату |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 знака(2 буквы или буква и | - | 3 буквы латинского | - | 3 буквы латинского | - | 8 цифр | - | 6 цифр | - | 3 цифры |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| цифра) | | алфавита | | алфавита | | | | | | | |

ТИП СЕРИЙНОГО НОМЕРА
Может принимать следующие значения:

- PR — серийный номер для продукта. Данный тип серийных номеров присваивается при продаже продукта без продажи техподдержки.
- S0-S9 — серийный номер для технической поддержки. Данный тип серийных номеров присваивается при продаже техподдержки для продукта, то есть продажа техподдержки вместе с продуктом, или продажа техподдержки к ранее купленному продукту. Цифра, стоящая после буквы S определяет уровень технической поддержки клиента. Чем больше число, тем выше уровень поддержки. Стандартному уровню технической поддержки присваивается код S0, расширенному -S1. Чем больше опций приобретается клиентом, тем больше увеличивается число.

ТИП ПРОДУКТА
REDOSM - указывается: RSM

РЕДАКЦИЯ
Open - указывается: OPN
Standart - указывается: STN
Enterprise - указывается: ENT
Developer - указывается: DEV
Отсутствует - указывается: NED

НОМЕР СБОРКИ
Указывается 8 цифр номера сборки продукта см. пункт 2.5

ДАТА ФОРМИРОВАНИЯ СЕРИЙНОГО НОМЕРА
Указывается 6 цифр даты, без разделителей. Для чисел менее 10 указывается вместе с нулем. Год - указывается 2 последние цифры. Например: 6 февраля 2014 года —060214.

ПОРЯДКОВЫЙ НОМЕР
Указывает порядковый номер заказанного продукта за текущий день. Например: 001, 002 или 018

# 3 Система отслеживания ошибок и порядок обновления ОС

## 3.1 Общий алгоритм обновления ОС

Обновления изделия, если при поставке обновлений не обговорено иное, осуществляются согласно условиям договора о поставке изделия и технического сопровождения в следующих вариантах:

- Производится полнаядеинсталляция текущей версии ОС с последующей установкой обновленной сертифицированной версии ОС в полном соответствии с программной документацией;
- Производится обновление с использованием сервисов цифровой дистрибуции и обновления

репозитория сертифицированного изделия.

## 3.2 Обновление изделия с комплекта поставки на физических носителях

Производитель по результатам проведения оценок соответствия изделия в форме инспекционного контроля обеспечивает формирование комплектов поставки изделия.

Производитель направляет потребителям извещение об изменениях, содержащее развернутый перечень изменений в изделии, или публикует данное извещение на официальном общедоступном ресурсе.

По запросу потребителя, производитель направляет в адрес потребителя дистрибутив в комплекте поставки, извещения об изменениях эксплуатационной документации изделия в бумажном виде, а также заверенную копию сертификата соответствия СЗИ с внесенными изменениями.

Потребитель в соответствии с эксплуатационной документацией на изделие обязан выполнить обновление изделия с использованием, полученного от производителя дистрибутивного комплекта поставки.

Потребитель после выполнения обновления обязан делать соответствующую отметку в эксплуатационной документации изделия с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

При возникновении нештатных ситуаций, сбоев и отказов в процессе установки или обновления изделия, потребитель, выявивший сбой, должен немедленно сообщить о проблеме производителю изделия путем обращения по телефону или другими доступными потребителю средствами связи.

## 3.3 Обновление изделия с использованием репозитория

Производитель по результатам проведения оценок соответствия изделия в форме инспекционного контроля обеспечивает своевременное обновление репозитория изделия.

При обновлении и синхронизации уровней репозитория производитель использует только защищенные, т.е. доверенные каналы передачи данных.

Производитель публикует образы дистрибутивных дисков комплекта поставки изделия и бинарные установочные пакеты изделия в репозитории. Образы включают полный поставочный комплект документации на изделие и копию сертификата соответствия. При этом производитель обеспечивает усиленную квалифицированную электронную подпись образов дистрибутивных дисков и бинарных установочных пакетов комплекта поставки изделия квалифицированным сертификатом ключа проверки электронной подписи, выданным аккредитованным удостоверяющим центром.

После обновления изделия в репозиториях производитель направляет потребителям извещение об изменениях, содержащее развернутый перечень изменений в изделии. В случае необходимости, по запросу потребителя, производитель дополнительно направляет в адрес потребителя комплект извещений об изменениях эксплуатационной документации изделия в бумажном виде, а также заверенную копию сертификата соответствия СЗИ с внесенными изменениями.

Порядок действий по синхронизации репозиториев и обновлению СЗИ описан в эксплуатационной документации на изделие.

Потребитель после выполнения обновления обязан делать соответствующую отметку в эксплуатационной документации изделия с указанием типа, даты и времени обновления, а также с

указанием фамилии лица, применившего его.

При возникновении нештатных ситуаций, сбоев и отказов в процессе загрузки, установки или обновления изделия, потребитель, выявивший сбой, должен немедленно сообщить о проблеме производителю изделия путем обращения по телефону или другими доступными потребителю средствами связи.

## 3.4 Порядок установки критических обновлений

При возникновении необходимости установки критических обновлений производитель незамедлительно осуществляет доведение до потребителей информации о необходимости обновления и предоставляет возможность его получения по доверенному каналу.

Потребитель при получении указанной информации осуществляет получение обновления средства защиты информации и незамедлительно применяет его, о чем делает соответствующую отметку в эксплуатационной документации с указанием типа, даты и времени обновления, а также с указанием фамилии лица, применившего его.

При невозможности устранения уязвимостей средства защиты информации, в том числе путем применения обновления, производитель разрабатывает ограничения по применению средства защиты информации и согласовывает их с испытательной лабораторией. Если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, производитель незамедлительно доводит его до потребителей. Потребитель реализует указанное ограничение по применению средства защиты информации.

Если потребитель не может реализовать ограничение по применению средства защиты информации он прекращает его применение.

Производитель вносит необходимые изменения в эксплуатационную документацию и после завершения инспекционного контроля, получив во ФСТЭК России сертификат соответствия с внесенными изменениями, доводит его копию, а также изменения в эксплуатационную документацию до всех потребителей.

## 3.5 Характеристики репозитория изделия

Репозиторий изделия служит хранилищем дистрибутивных пакетов изделия, обеспечивает сервис онлайн-дистрибуции изделия для потребителей.

Физически репозиторий представляет собой набор сетевых ресурсов в сети передачи данных с идентифицированными для пользователей сетевыми именами. Идентификация доступного репозитория в сети передачи данных организуется на уровне сетевых протоколов.

Функционирование сервисов репозитория изделия в сети передачи данных осуществляется по следующим сетевым протоколам и портам:

- протокол HTTP, порт 80. На данном порту обеспечивается доступ потребителей к ресурсам репозитория и получение обновлений;
- протокол HTTPS, порт 443. Данный порт зарезервирован для обеспечения аутентификации и построения защищенного TLS-соединения на основании сертификата открытого ключа пользователя с использованием инфраструктуры PKI;
- протокол RSYNC, порт 873. Данный порт предназначен для обеспечения процессов синхронизации зеркалируемых репозиториев изделия.

Функции репозитория изделия заключаются в обеспечении следующих сервисов:

- сервис онлайн-дистрибуции изделия;

- сервис обновления изделия/обновление «по воздуху»;

Сервис обновления изделия круглосуточно обеспечивает обновление изделия для конечных потребителей изделия.

Сервисы онлайн-дистрибуции и обновления изделия обеспечивают для конечных потребителей однозначную идентификацию изделия по сборкам, версиям, релизам, точкам монтирования ресурса в репозитории.

Репозиторий обеспечивает предоставление потребителям сетевого доступа к бинарным исполняемым файлам сертифицированных средств защиты информации, а также репозиторий содержит образы установочных дисков СЗИ.

## 4 Способы распространения изделия

Изделие распространяется следующими способами:

- По договору (акту, соглашению) о поставке изделия между потребителем и производителем.
- Сервисом цифровой дистрибуции образа;
- При OEM-дистрибуции оборудования (от англ. original equipment manufacturer - производитель оригинального оборудования) в рамках договора о поставке изделия между потребителем и производителем. В данном случае распространение производится путем клонирования предустановленной сертифицированной копии изделия на однотипные мобильные устройства

## 5 Описание штатной архитектуры проекта

Проект «Операционные системы» в соответствии с приказом ООО «РЕД СОФТ» разрабатывается департаментом развития системных продуктов ООО «РЕД СОФТ» с января 2022 года.

Руководство проектом осуществляет начальник отдела мобильных операционных систем ООО «РЕД СОФТ», Петров Станислав Анатольевич