РЕДСОФТ

Операционная система РЕД ОС

Описание жизненного цикла и сопровождение продукта

46.98898398.501110-01 93 1-1

РЕДСОФТ

Перечень сокращений

ОО	Объект оценки
ОС	Операционная система
ПО	Программное обеспечение
УК	Управление конфигурацией

РЕДСОФТ

Оглавление

РЕДСОФТ

1. Введение

РЕД ОС многозадачная и многопользовательская операционная система, обеспечивающая управляемый доступ субъектов к объектам доступа. Операционная система РЕД ОС (далее - ОС) представляет собой удобно и гибко конфигурируемую ОС, основанную на 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 системы контроля версий

При разработке ОС для обеспечения контроля версий применяется программный продукт Subversion (также известный как SVN), который является свободно распространяемой по лицензиям GNU/GPL централизованной системой управления версиями, официально выпущенной в 2004 году компанией CollabNet Inc.

В ООО «РЕД СОФТ» при разработке ОС используется система Subversion версии 1.6.17 (r1128011, сборка от 3 июня 2011 г., 07:26:06).

2.2. Возможности системы контроля версий

Основными возможностями системы SVN являются:

– Хранение полной истории изменений отслеживаемых объектов (файлов, каталогов, символьных ссылок) в централизованном хранилище (репозитории), в том числе при изменении атрибутов («метаданных»), перемещении, переименовании и удалении.

– Копирование объектов с разветвлением истории - при копировании в хранилище появляются два отдельных объекта с общей историей.

– Поддержка переноса изменений между копиями объектов, в том числе полного слияния копий (в рабочей копии; без объединения истории).

– Поддержка ветвления:

- создания ветвей (копированием директорий) и работы с ними;
- слияние ветвей (переносом изменений).

– Поддержка меток (копированием директорий).

– История изменений и копии объектов (в том числе ветви и метки) хранятся в виде связанных разностных копий - «дешёвых» (не требующих больших временных и дисковых ресурсов) при создании и хранении.

– Поддержка конкурентной (в том числе одновременной, с изоляцией транзакций) многопользовательской работы с хранилищем и, в большинстве случаев, автоматическим слиянием изменений различных разработчиков (в рабочей копии).

– Фиксации изменений в хранилище (в том числе многообъектные) организуются в виде атомарных транзакций.

– Сетевой обмен между сервером и клиентом предусматривает передачу только различий между рабочей копией и хранилищем.

– Обеспечивается одинаково эффективная работа как с текстовыми, так и с двоичными файлами.

– Различные варианты доступа к хранилищу, в том числе:

- непосредственный доступ на локальной файловой системе;
- по собственному сетевому протоколу;
- через веб-сервер по протоколу WebDAV/DeltaV.

– Вывод клиента командной строки одинаково удобен и для чтения, и для разбора программами.

– Возможность зеркалирования хранилища.

– Два возможных внутренних формата хранилища (англ. repository): база данных или набор обычных файлов.

– Интернационализированные сообщения программы (используются настройки локали).

– Библиотеки для языков PHP, Python, Perl, Java позволяют встроить функциональность клиента Subversion в программы, написанные на этих языках.

– Многоуровневая архитектура библиотек, изначально рассчитанная на клиент-серверную модель.

2.3. Модель работы

Subversion - централизованная система (в отличие от распределённых систем, таких как Git или Mercurial), то есть данные хранятся в едином хранилище. Хранилище может располагаться на локальном диске или на сетевом сервере.

Работа в Subversion мало отличается от работы в других централизованных системах управления версиями. 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 Subversion преимущественно используется модель копирование - изменение - слияние. Кроме того, для файлов, не допускающих слияние (различные бинарные форматы файлов), можно использовать модель блокирование - изменение - разблокирование.

При сохранении новых версий используется дельта-компрессия: система находит отличия новой версии от предыдущей и записывает только их, избегая дублирования данных.

При использовании доступа с помощью WebDAV также поддерживается прозрачное управление версиями - если любой клиент WebDAV открывает для записи и затем сохраняет файл, хранящийся на сетевом ресурсе, то автоматически создаётся новая версия.

2.4. Типы поддерживаемых репозиториев

Subversion предлагает два варианта организации репозиториев. Репозитории первого типа используют для хранения базы данных на основе Berkeley DB, репозитории второго типа - обычные файлы специального формата (доступ к данным организуется с помощью собственных библиотек, без использования сторонних баз данных). Разработчики Subversion часто называют хранилище «файловой системой», поэтому второй тип получил название FSFS, то есть (версионированная) файловая система (англ. File System) поверх (обычной) файловой системы.

Оба типа репозиториев обеспечивают достаточную надёжность при правильной организации (Berkeley DB использует блокировки файлов, поэтому её нельзя использовать на некоторых сетевых файловых системах, не поддерживающих блокировок), каждая из них обладает своими преимуществами и недостатками. Считается, что FSFS легче правильно настроить, она требует меньшего внимания от администратора. Кроме того, до релиза 1.4 хранилища, использующие Berkeley DB, могли при определённых условиях оказаться в так называемом заклиненном (англ. wedged) состоянии; требовалось вмешательство администратора для восстановления его работоспособности. Начиная с релиза 1.2 для новых хранилищ по умолчанию используется FSFS.

В ООО «РЕД СОФТ» используется система Subversion на базе репозитория типа FSFS.

2.5. Доступ к репозиторию

Subversion предоставляет следующие способы доступа к репозиторию:

– прямой доступ к репозиторию на диске (на локальной или сетевой файловой системе);

– удалённый доступ по протоколу WebDAV/DeltaV поверх HTTP (или HTTPS) с использованием модуля mod_dav_svn для веб-сервера Apache;

– удалённый доступ с использованием собственного протокола SVN:

- на выделенном сетевом соединении (по умолчанию на TCP-порту 3690);
- через стандартный ввод-вывод (в том числе через средства удаленного CLI, например SSH).

Все эти способы могут быть использованы для работы с репозиториями обоих типов (FSFS и Berkeley DB). Для доступа к одному и тому же репозиторию могут одновременно использоваться разные способы.

В ООО «РЕД СОФТ» доступ к репозиториям системы Subversion обеспечивается из контролируемых зон объектов ООО «РЕД СОФТ» удаленно с использованием собственного протокола SVN. Доступ разработчиков обеспечивается внутри корпоративной виртуальной частной сети (VPN), организуемой сертифицированными средствами межсетевого экранирования и построения VPN каналов ПАК ViPNet Coordinator HW100 (модели А и С, сертификат соответствия ФСТЭК России № 2353 от 26.05.2011 г. по требованиям к устройствам типа межсетевые экраны по 3 классу и 3 уровню контроля отсутствия недекларированных возможностей, сертификат соответствия ФСБ России №СФ/124-1970 от 12.09.12 г. по требованиям к СКЗИ класса КС3).

2.6. Номера ревизий ОС

Номер ревизии в Subversion — это натуральное число (или 0 для самой первой ревизии), адресующее номер состояния хранилища в процессе изменения содержащихся в нём данных. Каждая успешная фиксация изменений порождает ровно одну новую ревизию в хранилище, то есть N-я ревизия — это состояние хранилища после N-й фиксации.

В Subversion ревизия характеризует состояние не отдельного файла, а всего хранилища в целом.

Номер ревизии является аналогом времени в том смысле, что меньшие номера ревизий соответствуют более ранним состояниям хранилища, а большие — поздним.

Минимальный номер ревизии 0 (ноль) соответствует изначальному состоянию хранилища, когда ещё не было зафиксировано ни одной правки. В нулевой ревизии хранилище содержит только пустую корневую директорию.

Максимальный номер ревизии соответствует самому последнему состоянию хранилища, то есть состоянию после фиксации последней правки. Вместо указания номера последней ревизии можно использовать ключевое слово HEAD (головная ревизия); это удобно, поскольку номер головной ревизии

увеличивается при каждой фиксации изменений.

Номер ревизии можно рассматривать как некую временную отметку в истории хранилища. Более того, с каждым номером ревизии связано абсолютное значение времени, когда эта ревизия была сделана (свойство svn:date). Однако указание номера ревизии удобнее, чем указание времени, так как нет путаницы с часовыми поясами, запись номера короче и номер ревизии не может быть изменён.

Номера ревизий ОС представляются в виде номера в формате X.Y, где X – номер ревизии, а Y – номер версии в ревизии.

За начальную ревизию ОС взята ревизия базового по отношению к ОС дистрибутива ОС GosLinux равная 6.6.

2.7. 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 Beta и Alpha (Pre-Alpha) не являются показателями нестабильности релиза, так как присваиваются программе один раз или один раз за серию (серией, в данном случае, считается число до первой точки), в зависимости от системы разработки. Они могут присваиваться нескольким релизам подряд. Релизом в данном случае считается завершённая версия.

2.7.1 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.

2.7.2 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.

2.7.3 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.

2.7.4 Релиз-кандидат

Релиз-кандидат или RC (англ. release candidate), Пре-релиз или Pre - стадия-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.

2.7.5 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.

2.8. Сборка программного кода ОС

Сборка программного кода ОС производится на отдельной виртуальной ОС, размещенной на специальном выделенном сервере в 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 компонентов ОС и 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.

2.9. Технология создания ОС

При создании ОС используются следующие средства технологического оснащения:

- персональный компьютер с архитектурой процессора x86_64;
- операционная система сервера сборки;
- koji-1.8.0 - система построения и отслеживания RPMS. Пакет содержит общие библиотеки и интерфейс командной строки;
- mock-1.1.38 - средство построения сборочного chroot;
- rpm-build-4.8.0 - пакет сценариев и исполняемых программ, которые используются для построения пакетов с помощью диспетчера пакетов RPM;
- rpmdevtools-7.5 - пакет сценариев и файлов поддержки для разработки RPM пакетов;
- anaconda-13.21.229 – программа установки операционной системы;
- комплект сборочных репозиториев.

Методы эксплуатации средств технологического оснащения при создании ОС:

– создаётся новый src.rpm пакет или модифицируется существующий с помощью пакетов rpm и rpmbuild;

– полученный src.rpm передается в koji с ключом --scratch, что обеспечивает сборку бинарного пакета без включения результата в базу данных koji;

– проверяется бинарный пакет на работоспособность и функциональность;

– повторяется сборка пакета в koji, но уже без ключа --scratch. Собранный пакет появляется в базе данных koji и его репозитории;

– после формирования необходимого списка пакетов, собирается установочный образ ОС с помощью anaconda.

Приемы эксплуатации средств технологического оснащения при создании ПО:

– mock используется как низкоуровневая сборочная среда, управляемая koji.

Правила эксплуатации средств технологического оснащения при создании ОС:

– необходимо соблюдение правил электро-технической безопасности при использовании сборочного персонального компьютера;

– появление сообщений об ошибках в работе mock свидетельствует о некорректной настойке средств технологического оснащения при создании ОС.

2.10. Элементы конфигурации ОС

Элементами конфигурации ОС являются:

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

2.11. Документация УК

2.11.1 Требования к составу и маркировке программной документации

Виды, комплектность и обозначение документации, создаваемой и сопровождаемой в рамках разработки ОС, определяются ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем».

Состав программной документации на различных этапах создания и сопровождения ОС определяется ГОСТ 19.101-77 «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

2.11.2 Процедура формирования серийного номера продукта

Потребители и заказчики формируют заявки на поставку комплектов РЕД ОС. 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. Правила присвоения серийных номеров приведены в разделе 2.10.3.

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

2.11.3 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:

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 цифра)	-	3 буквы латинского алфавита	-	3 буквы латинского алфавита	-	8 цифр	-	6 цифр	-	3 цифры

ТИП СЕРИЙНОГО НОМЕРА

Может принимать следующие значения:

PR — серийный номер для продукта. Данный тип серийных номер 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

RED OS - указывается: ROS

Database - указывается: RDB

Warehouse - указывается: RWH

Control - указывается: RCL

NCORE - указывается: NCR

РЕДАКЦИЯ

Open - указывается: OPN

Standart - указывается: STN

Enterprise - указывается: ENT

Developer - указывается: DEV

Отсутствует - указывается: NED

НОМЕР СБОРКИ

Указывается 8 цифр номера сборки продукта без разделителей. Недостающие позиции заполняются нулями. *Например: 00000052 или 2601234*

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*

ПРИМЕР СЕРИЙНОГО НОМЕРА:

S3-ROS-NED-00000073-100117-011

Серийный номер присвоен клиенту технической поддержки (расширенный

уровень с дополнительными опциями) на продукт РЕД ОС без указания редакции, версия 7.3, сформирован 10 января 2017 года, 11 заказ за день.

3. Система отслеживания ошибок и порядок обновления ОС

3.1. Общее описание и назначение

При разработке ОС использована система отслеживания ошибок «Ред Контроль» версии 2.0.45.1807 производства ООО «РЕД СОФТ». Система «Ред Контроль» предназначена для отслеживания одного или нескольких проектов, в которых циркулируют информационные элементы, которыми могут являться обращения клиентов, задачи департамента разработки, поручения руководителя, данные о сбоях, обнаруженных в продукте при контроле качества и т.д. Цикл обработки информационных элементов может проходить при участии различных программных комплексов в организации и персонала. «Ред Контроль» легко масштабируется и адаптируется для применения в любой отрасли.

Система «Ред Контроль» основана на СУБД «Ред База Данных», которая имеет сертификат соответствия ФСТЭК России по требованиям обеспечения информационной безопасности. Система «Ред Контроль» так же предназначена для оперативного управления бизнес-процессами и проектами, а также, для накопления фактов и их массивов, управления ими в организации.

Система «Ред Контроль» служит расширенным решением для хранения данных и обмена данными с пользователем бизнес-процессов и обеспечивает двунаправленные коммуникации, которые позволяют без усилий интегрироваться с другими решениями и источниками данных.

Ключевой сущностью в системе «Ред Контроль» являются информационные элементы, факты, которые определяют следующие группы:

– формализованные данные (поля, подструктуры, классификация) неформализованные данные (обсуждения, связи и т.п.);

– формальный жизненный цикл.

3.2. Техническая архитектура

Система «Ред Контроль» реализована с применением трехзвенной клиент-серверной архитектуры (Client GUI + AS + DB). Клиентская часть имеет собственную встроенную БД, синхронизируемую с сервером при наличии связи. Это позволяет работать с продуктом мобильным пользователям. Решение легко интегрируется в существующую IT-структуру ООО «РЕД СОФТ» благодаря серверу приложений системы «Ред Контроль», имеющему открытые интерфейсы на

основе CORBA, XML и других стандартов коммуникации и обмена информацией.

Система «Ред Контроль» может быть использована как:

– система управления проектами (Issue tracking system) – предоставляет расширенную функциональность в управлении и контроле над проектами и процессами в разных бизнес-потоках;

– CRM – Система управления взаимодействием с клиентами;

– система управления и контроля над разработкой SW решений (SW development tracking and supervising tool, buqtracking);

– система управления и контроля над проектами и т.д.

Система «Ред Контроль» обеспечивает в режиме реального времени отслеживание закрепленных за ответственными лицами задач, что делает ее незаменимой для руководителей при организации эффективного труда сотрудников, а также при организации взаимодействия сотрудников между собой.

Система «Ред Контроль» позволяет работать со справочниками данных. Справочники программы, используются для исключения заполнения полей вручную. Из справочника могут быть взяты следующие данные:

– статус заявки;

– автор записи;

– тип записи;

– название подсистемы;

– приоритет;

– дата обнаружения;

– тип обращения;

– срок исполнения заявки.

Использование справочников позволяет избежать ошибок при наборе реквизитов заявки (задачи), так как в справочниках хранится достоверная информация по заполнению полей в заявке. Если справочник был изменен, то при первом же запуске программы система сама автоматически обновит этот справочник.

Общая схема жизненного цикла задачи приведена на рисунке 1.

Задача регистрируется в рамках работы структурных подразделений разработчика ОС и линии технической поддержки пользователей ОС. Это может быть задача от аналитика ОС, связанная с доработкой по требованиям заказчика; ошибка, выявленная при тестировании ОС; проблема, возникшая у пользователя или сообщение об ошибке от системы, обнаруженное пользователем в процессе

эксплуатации ОС. Так же задача может возникнуть в рамках работы группы разработки ПО или анализа ПО при его согласовании с заказчиком продукта.

Далее, созданная задача поступает на рассмотрение руководителей отделов и ведущих аналитиков. Исходя из контекста, они принимают решение об отказе или назначении в работу поступившей задачи.

Принятая в работу задача поступает в группу тестирования для подтверждения факта обнаруженной ошибки или непосредственно в группу аналитики или разработки, если такое подтверждение не требуется. Если ошибка не будет подтверждена в результате тестирования, она отклоняется.

Подтвержденная тестировщиками ошибка поступает для согласования и утверждения в группу аналитики и далее непосредственным разработчикам программного продукта.

После доработки или разработки вновь задача возвращается на тестирование, и если будет подтверждено исправление обнаруженной ошибки или корректная работа созданного компонента, задача закрывается.

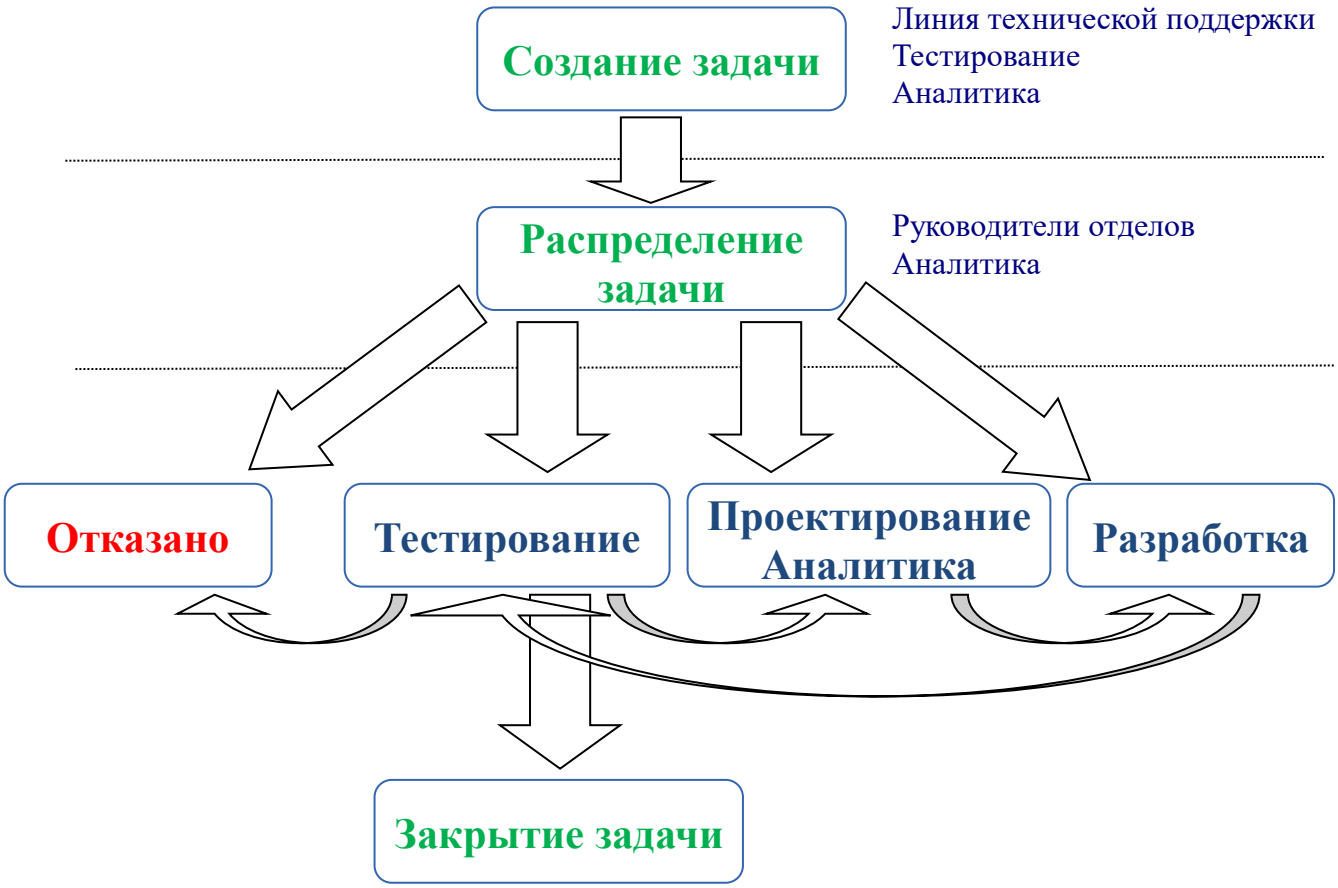

Рисунок 1 - Жизненный цикл задачи в системе отслеживания ошибок «Ред Контроль»

3.3. Общий алгоритм обновление ОС

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

– Производится полная деинсталляция 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.

Оба варианта обновления должны завершаться процедурой верификации изделия, описанной в разделе 3.8.

3.4. 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.

3.5. 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.

3.6. 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.

3.7. 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;

– сервис синхронизации зеркалируемых репозиториев;

– сервис верификации изделия.

Сервис онлайн-дистрибуции обеспечивает полную идентичность бинарных образов изделия, представленных на физических цифровых носителях информации (флеш-накопители, CD/DVD диски и т.д.), и бинарных образов изделия, размещаемых в ресурсах репозитория производителя и загружаемых потребителями по сети передачи данных.

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 и контрольным суммам.

Сервис верификации изделия обеспечивает для конечных потребителей средства для установления подлинности изделия как сертифицированного продукта, его бинарных файлов и цифровых установочных образов дистрибутивов изделия. Установление подлинности изделия проводится автоматизированно методом подсчета контрольных сумм бинарных файлов и установочных образов изделия.

Сервис верификации обеспечивает верификацию СЗИ на каждом рабочем месте пользователя. Более подробно процессы сервиса верификации описаны в пункте 3.8 «Верификация изделия» настоящего документа.

Для организации идентификации ресурсов репозитория в сети передачи данных и обеспечения потребителей сервисом онлайн-дистрибуции производитель обеспечивает регистрацию уникального домена.

Репозиторий обеспечивает предоставление потребителям сетевого доступа

к бинарным исполняемым файлам сертифицированных средств защиты информации, а также репозиторий содержит образы установочных дисков СЗИ.

3.8. Верификация изделия

При подключении и обновлении изделия из сторонних репозиториев, оно теряет статус сертифицированного продукта. Поэтому потребителю запрещается подключение и использование сторонних репозиториев.

Сервис верификации изделия в составе репозитория изделия обеспечивает верификацию для загружаемых образов дистрибутивных дисков комплекта поставки и проверку соответствия комплектов изделия, установленных на рабочих местах, пакетам, расположенным в репозитории изделия.

Для обеспечения верификации для загружаемых образов дистрибутивных дисков комплекта поставки производитель обеспечивает усиленную квалифицированную электронную подпись файлов образов дистрибутивных дисков.

Потребитель производит загрузку образов дистрибутивных дисков комплекта поставки изделия, размещенных в репозитории производителя. После загрузки потребитель производит верификацию загруженного дистрибутивного комплекта изделия методом проверки усиленной квалифицированной электронной подписи и проверки контрольных сумм комплекта поставки. Верификацию для загружаемых из репозитория образов дистрибутивных дисков комплекта поставки изделия потребитель проводит самостоятельно в соответствии с инструкцией, приведенной в эксплуатационной документации на изделие.

В случае неудовлетворительного результата верификации усиленной квалифицированной электронной подписи или контрольных сумм изделия, потребителю запрещается применение загруженного дистрибутивного комплекта.

Компонентой сервиса верификации изделия является утилита контроля целостности afick, входящая в состав операционной системы типового дистрибутива. Утилита контроля целостности afick обеспечивает верификацию бинарных исполняемых пакетов установленного изделия.

В состав репозитория изделия входит база данных утилиты контроля целостности afick, которая содержит перечень контролируемых бинарных исполняемых файлов изделия, согласно документации на изделие, и контрольные суммы данных файлов. Формирование контрольных сумм утилиты контроля

целостности выполнено согласно ГОСТ Р 34.11-94.

Производитель для обеспечения процессов верификации изделия размещает в репозитории изделия следующие пакеты:

– пакет обновления версии релиза изделия. Данный пакет обеспечивает настройку конфигурации менеджера пакетов yum путем указания ссылки на новую версию репозитория изделия. Тем самым обеспечивается версионная иерархия репозитория изделия;

– база данных утилиты afick. База данных поставляется в отдельном пакете и содержит контрольные суммы по ГОСТ Р 34.11-94 исполняемых и контролируемых файлов изделия;

– конфигурация утилиты afick. Конфигурация утилиты afick обеспечивает периодический запуск утилиты для проверки контрольных сумм изделия. Периодический запуск afick настраивается в системном сервисе cron изделия;

– база данных менеджера пакетов yum. Данная база данных содержит перечень изменений в составе пакетов изделия. Изменения перечня пакетов СЗИ могут иметь как характер добавления, так и исключения ранее содержавшихся в изделии пакетов.

При формировании или обновлении репозитория производитель обеспечивает размещение в репозитории изделия указанных файлов. При первоначальной установке изделия менеджер пакетов yum настроен на обновления со всех доступных на момент выпуска данной версии изделия репозиториев.

4. Способы распространения изделия

Изделие распространяется следующими способами:

– По договору (акту, соглашению) о поставке изделия между потребителем и производителем. В данном случае поставка может осуществляться в виде комплектов поставки;

– Сервисом цифровой дистрибуции репозитория;

– Средствами национального фонда алгоритмов и программ, действующего в соответствии с Постановлением Правительства Российской Федерации от 30 января 2013 г. № 62 г. Москва «О национальном фонде алгоритмов и программ для электронных вычислительных машин»;

– 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 идентичные носители информации: накопители на жестких магнитных дисках и твердотельные накопители. После клонирования производится верификация изделия способами, описанными в разделе 3.8.

5. Описание штатной структуры проекта

Проект «Операционные системы» в соответствии с приказом ООО «РЕД СОФТ» разрабатывается департаментом развития системных продуктов ООО «РЕД СОФТ» с сентября 2014 года.

Руководство проектом осуществляет директор департамента развития системных продуктов ООО «РЕД СОФТ», к.т.н., доцент кафедры ИС МИ (филиала) ВлГУ, научный сотрудник НИИ Системных исследований Симаков Роман Александрович.

Штатная структура проекта включает:

- Отдел маркетинга;
- Отдел аналитики;
- Отдел разработки;
- Отдел тестирования;
- Отдел технической поддержки;
- Отдел документирования.

Обеспечение процессов жизненного цикла РЕД ОС осуществляется командой разработчиков и технических специалистов в составе около 35 человек.