



SmartCard-Service

Акционерное общество «СмартКард-Сервис»

127106, г. Москва, Алтуфьевское шоссе, д. 1

Телефон: +7 (495) 981-12-10, 8 (800) 100-31-64, факс: +7 (495) 981-12-11

E-mail: reception@scserv.ru, site: www.scserv.ru

У Т В Е Р Ж Д Е Н О

Генеральный директор

АО «СмартКард-Сервис»

_____ В.А. Васильев

№ _____ «_____» _____ 20__ г.

Программа «Удостоверяющий центр CA.RUS»

ОРГАНИЗАЦИЯ И ПРОЦЕССЫ СОПРОВОЖДЕНИЯ ПО

Файл: организация и процессы сопровождения по.doc

Москва
2024

СОДЕРЖАНИЕ

1. СВЕДЕНИЯ О ДОКУМЕНТЕ.....	3
2. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ.....	3
3. ОПИСАНИЕ ПРОЦЕССА «СОПРОВОЖДЕНИЕ».....	3
3.1. Назначение процесса «Сопровождение».....	3
3.2. Состав работ процесса «Сопровождение»	4
3.3. Состав ролей процесса «Сопровождение».....	6
3.4. Связь процесса «Сопровождение» с другими процессами.....	6
3.5. Тестирование обновлений и изменений ПО сторонних производителей	9
3.6. Защищенная поставка пакета обновлений и исправлений	9
4. ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА.....	10

1. СВЕДЕНИЯ О ДОКУМЕНТЕ

Номер версии:	01.02
Дата выпуска:	22.12.2023 г.
Дата утверждения:	
Порядок обновления:	1 раз в год

2. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Расшифровка сокращений
PCI SSF	Семейство стандартов, направленных на обеспечение безопасности программного обеспечения (PCI Software Security Framework), на данный момент состоит из двух связанных между собой стандартов — Secure Software Standard (SSS) и Secure Software Lifecycle (Secure SLC) Standard.
PCI SSS	Стандарт безопасности данных программного обеспечения индустрии платежных карт (Payment Card Industry Security Software Standard)
PCI SLC	Стандарт, который определяет безопасные методы управления жизненным циклом платёжного ПО, позволяющие гарантировать вендору такого ПО, что оно спроектировано и разработано для защиты платежных транзакций и данных, минимизации уязвимостей и защиты от атак.
Программа «Удостоверяющий центр CA.RUS»	Программа реализует функционирование Удостоверяющего Центра для выполнения цифровой подписи публичных ключей EPP-клавиатур и Хоста.
УС	Устройство самообслуживания
ССК	Система Сопровождения Клиентов

3. ОПИСАНИЕ ПРОЦЕССА «СОПРОВОЖДЕНИЕ»

3.1. Назначение процесса «Сопровождение»

Назначение процесса «Сопровождение» — анализ и улучшение рабочих характеристик программного обеспечения (ПО) в процессе его эксплуатации, а также внесение соответствующих изменений по запросам заинтересованных лиц, вызванным возникающими проблемами или потребностями. Процесс охватывает также вопросы адаптации ПО к другим устройствам/средам эксплуатации и заканчивается выпуском новой версии и снятием предыдущей версии с эксплуатации.

Корректировки в коде ПО, осуществляемые в процессе сопровождения, проводятся под конфигурационным контролем в соответствии с документами «План конфигурационного управления» и «Положение о конфигурационном управлении при разработке ПО и документации». При этом назначение конфигурационного контроля в данном случае сводится к определению состава объектов конфигурационного управления, подлежащих корректировке, присвоению им новых названий версий/релизов/патчей и контролю за созданием новых объектов конфигурационного управления. В данном процессе могут

частично (на уровне работ и/или задач) использоваться и другие процессы, такие как «Разработка», «Тестирование», «Внедрение» и т.д.

В состав работ процесса «Сопровождение» входит:

- разработка и корректировка процедур и плана сопровождения ПО после сдачи его в эксплуатацию;
- анализ основных характеристик функционирования ПО в процессе его эксплуатации;
- обеспечение корректного и полного функционирования ПО;
- анализ рекламаций, замечаний и предложений от заинтересованных лиц клиентских организаций в процессе эксплуатации ПО и принятие мер по их реализации;
- анализ возможных уязвимостей ПО сторонних производителей, с которым происходит взаимодействие разрабатываемого ПО и принятие мер по обеспечению безопасности ПК, на котором установлено разрабатываемое ПО;
- оказание консультаций клиентским организациям по вопросам настройки и эксплуатации ПО.

3.2. Состав работ процесса «Сопровождение»

Все работы процесса «Сопровождение» по своему назначению разделены на две группы:

- группа работ подготовки процесса «Сопровождение»;
- группа работ непосредственно сопровождения в процессе эксплуатации ПО.

Назначение группы работ подготовки процесса «Сопровождение» — разработка концепции и модели сопровождения ПО, определение требований к ПО, разработка планов, процедур сопровождения и разработка правил конфигурационного управления при внесении изменений в ПО. В эту группу входят работы, выполняемые на основе регламентирующих документов «Положение об управлении требованиями при выполнении проектов разработки» и «План управления требованиями», определяющие организацию процесса управления требованиями. А также документы «Положение о конфигурационном управлении при разработке ПО и документации» и «План конфигурационного управления», определяющие работы по конфигурационному управлению. *Работы этой группы выполняются до начала эксплуатации версии ПО.*

Назначение группы работ сопровождения — консультирование клиентских организаций по вопросам настройки и эксплуатации ПО, анализ функционирования системы, прием и анализ предложений о модификации, отчетов о проблемах, поступающих от ответственных представителей заинтересованных лиц, принятие решений об их реализации, внесение необходимых изменений в ПО, корректировка кода; информирование заинтересованных лиц об изменениях, в процессе эксплуатации ПО, проведение верификации и тестирования изменений, разработка предложения о снятии с эксплуатации текущей версии и внедрении новой версии ПО. *Работы этой группы выполняются на протяжении эксплуатации ПО.*

На диаграмме (см. Рис. 1) показан состав основных работ процесса «Сопровождение».

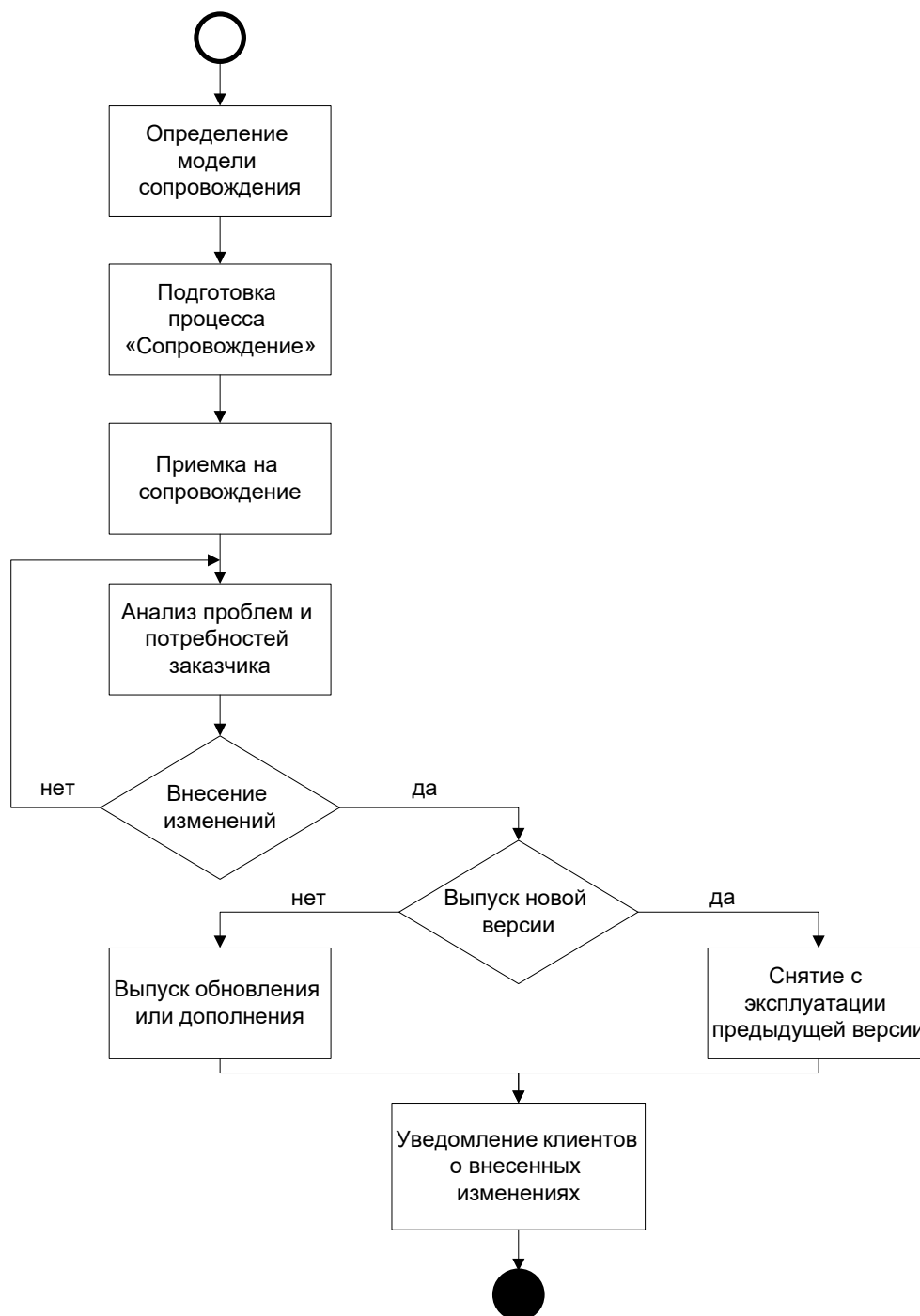


Рис. 1. Состав и логическая последовательность работ процесса «Сопровождение»

Поддержка программного обеспечения (Software Support) включает работы по консультированию пользователей, проводимые в ответ на их информационные запросы, поступающие по телефону, либо через специализированную Систему Сопровождения Клиентов (ССК). Процесс приема поступающих обращений происходит в соответствии с документом «Временный регламент приема обращений по вопросам сопровождения ПО».

Если полученные от клиентов журналы, содержат критичные данные платежных карт, то журналы безопасно удаляются сотрудниками отдела сопровождения после использования.

3.3. Состав ролей процесса «Сопровождение»

Роли, выполняющие задачи процесса «Сопровождение», объединены в «Группу сопровождения». Назначение группы сопровождения — обеспечение бесперебойного функционирования ПО на всех устройствах, анализ стабильности работы ПО в процессе ее функционирования, анализ рекламаций, требований и предложений по модификации ПО и обеспечение их реализации, а также оказание помощи в решении проблем, связанных с эксплуатацией ПО.

В состав группы входят: аналитик, инженеры сопровождения, разработчики, проектировщики, архитектор проекта, менеджер конфигурации, интегратор, тестировщики и менеджер по качеству.

3.4. Связь процесса «Сопровождение» с другими процессами

Процесс «Сопровождения» регламентирует состав функций, выполняемых персоналом сопровождения, состав процедур, определяющих правила взаимодействия всех сторон, имеющих отношение к эксплуатации и сопровождению ПО, требования и соответствующая реакция на них, особенности выполнения своих функций персоналом сопровождения и т.д.

Процесс «Сопровождение» использует в своих работах результаты, сформированные в процессах «Разработка» и «Тестирование».

После инициализации внесения Изменений в ПО, заявка на внесение изменений регистрируется в специализированном средстве управления запросами на изменение ПП «Rational ClearQuest». После этого заявка проходит обязательные процессы «Анализ», «Разработка», «Сборка» и «Тестирование».

1. На этапе «Анализ» все заявки на Изменение («Feature Request») могут, как приниматься и передаваться в работу соответствующими руководителями, так и отклоняться по различным обоснованным причинам — объему и/или сложности требуемых изменений, а также необходимых для этого усилий. В процессе создания заявке присваиваются значение заранее утвержденного набора атрибутов (ключевые слова, версия платежного приложения, приоритет выполнения, а также производится ранжирование важности/критичности по трем уровням — «Низкий», «Средний» или «Высокий»), которые могут быть изменены по усмотрению руководителя.

После процесса «Анализ» заявка подлежит дальнейшей разработке и внесению соответствующих изменений в код программного обеспечения.

2. Из процесса «Разработка» передаются измененные блоки ПО. Они используются в процессе «Сборка» и далее при сопровождении ПО. Заявка поступает менеджеру конфигурации в состоянии «AssignRelease». На этапе «Сборка» менеджер конфигурации проекта производит дополнительный просмотр (code review) и анализ изменений программного кода на предмет выявления потенциальных угроз и возможных уязвимостей. Взаимная инспекция кода при выполнении code review проводится средствами ClearCaseTools (утилита - ClearCase DiffMerge tool) и отображается графически. Результаты процедур дополнительного просмотра и анализа кода менеджер конфигурации фиксирует в заявке в разделе «Сборка». Если этап успешно пройден, то заявка поступает в релиз и переводится в состояние «OpenRelease». В жизненном цикле изменений, представленном на рисунке 2, наглядно отображена возможность возврата заявки на доработку в разные этапы жизненного цикла.

Важным этапом процесса «Сборка» является анализ необходимости выпуска новой версии, либо внесение изменений в уже существующие путем выпуска дополнения. Результатом процесса «Сборка» является новая версия ПО, либо обновление/исправление к предыдущей версии.

3. После сборки дистрибутива ПП проводится его тестирование. В ходе тестирования используются только тестовые карты. По окончании тестирования установленное на УС ПО удаляется и никаким образом не может быть использовано в промышленной эксплуатации. Для инсталляции ПО на УС в промышленной эксплуатации используются дистрибутивы ПО.

В процесс «Тестирование» попадает измененный проект ПО и возможные поясняющие документы со стороны разработчиков.

В процессе «Тестирования» ПО или его обновлений/исправлений осуществляется:

- проверка на переполнение буфера;
- проверка правильности обработки ошибок;
- проверка защиты хранимых криптографических материалов;
- проверка защиты телекоммуникаций;
- проверка на влияние сторонних уязвимостей высокого уровня (описание в документе «Управление уязвимостями»).

На диаграмме (см. Рис. 2) показан жизненный цикл изменений, которые необходимо внести в ПО в процессе «Сопровождение». Жизненный цикл изменений включает в себя процедуры управления изменениями при внесении любых изменений в конфигурацию программного обеспечения.

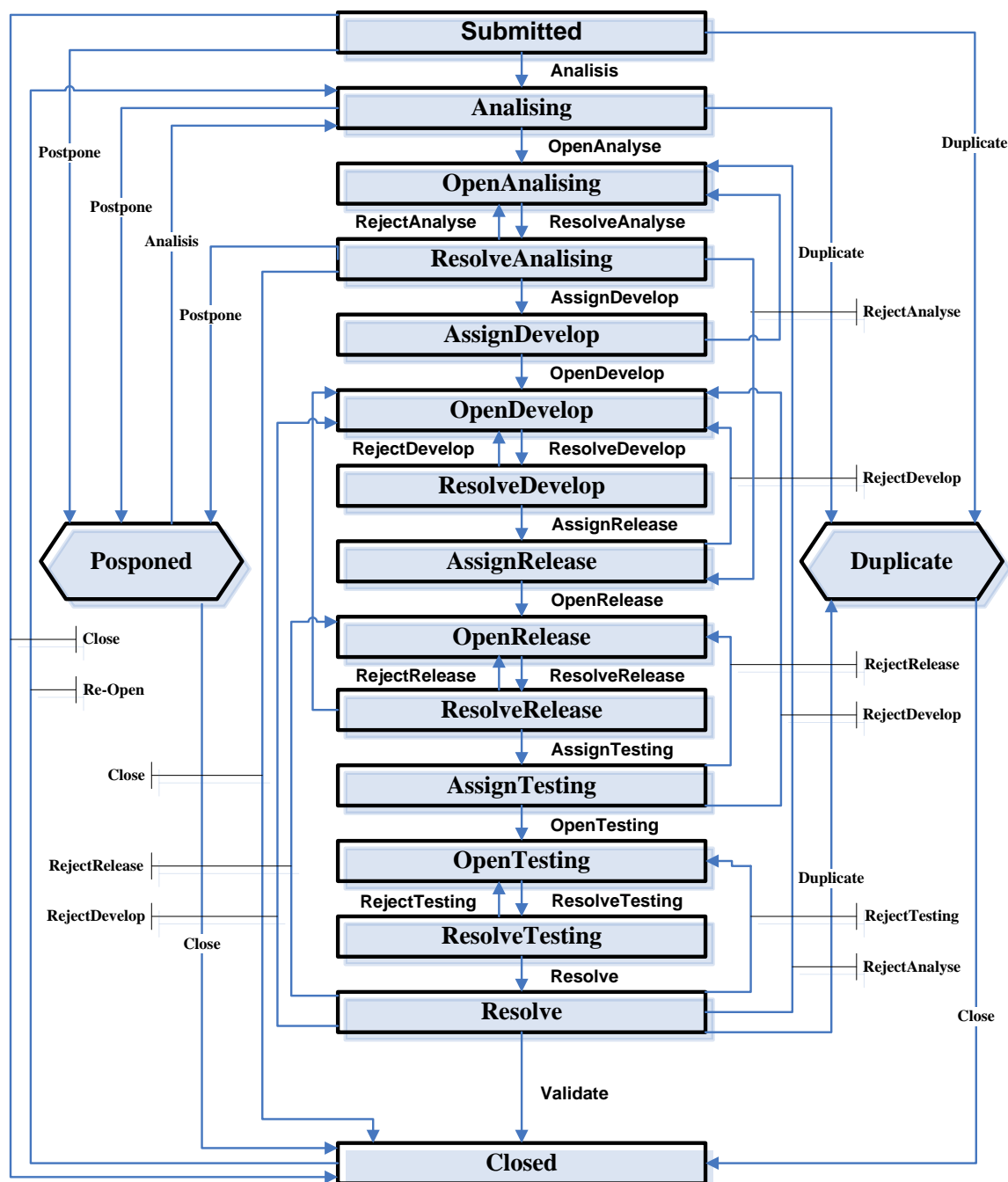


Рис. 2. Жизненный цикл изменений, которые необходимо внести в ПО в процессе «Сопровождение»

Персонал службы сопровождения проводит проверку внесенного изменения совместно с клиентской организацией, в целях подтверждения работоспособности измененной системы. Персонал службы сопровождения должен получить подтверждение того, что внесенное изменение удовлетворяет установленным требованиям.

По завершению тестирования все изменения проходят дополнительный анализ на необходимость внесения изменений в документацию. В ПП «ClearQuest» к каждой заявке на изменение может быть «привязана» заявка на изменение документации «DocQuest», на основании которой изменения отражаются в программной документации.

При приемке ПО клиентскими организациями, на сопровождение передается полный состав программной документации, разработанная версия ПО или обновление/исправление к основной версии.

3.5. Тестирование обновлений и изменений ПО сторонних производителей

До внедрения в среду эксплуатации сотрудниками компании АО «СмартКард-Сервис» выполняется тестирование всех обновлений безопасности. Также тестируются любые изменения в конфигурации систем и ПО сторонних производителей, которое используется в работе УС.

Тестирование обновлений безопасности, изменений конфигурации систем и ПО сторонних производителей происходит с обязательным выполнением следующих действий:

- проверка всех входных данных;
- проверка правильности обработки ошибок;
- проверка защиты хранимых криптографических материалов;
- проверка защиты коммуникаций;
- проверка правильности управления доступом на основе ролей.

Тестирование осуществляется в соответствии с документом «Положении о тестировании в проектах разработки программного обеспечения», входящем в состав документации по процессам производства Программного обеспечения в компании АО «СмартКард-Сервис».

3.6. Защищенная поставка пакета обновлений и исправлений

Для получения обновлений или исправлений Программного обеспечения клиенты или дилеры/интеграторы направляют запрос в Отдел сопровождения (по электронной почте или официальным письмом по факсу). После обработки запроса АО «СмартКард-Сервис» направляет ответное письмо (по электронной почте, либо официальным письмом по факсу) с указанием ссылки для скачивания обновлений или исправлений с WEB-портала АО «СмартКард-Сервис» в виде архива *.zip. Доступ на портал имеют только пользователи, зарегистрированные в Системе Сопровождения Клиентов (ССК). К письму также прикладываются ХЭШ-значения для проверки подлинности скачиваемых файлов. Хэш-значения вычисляется по алгоритму SHA-1.

В некоторых случаях Программное обеспечение передается на CD/DVD-дисках с сопроводительным актом приема-передачи.

Отдел сопровождения не предоставляет услуги по удаленной поддержке УС. Клиенты или дилеры/системные интеграторы осуществляют непосредственный доступ к УС, либо удаленный доступ самостоятельно.

Для организации удаленного доступа клиентам или дилерам/системным интеграторам необходимо руководствоваться документом «Руководство по применению стандарта PCI SSS ver_1_2_1 (PCI SSS Implementation Guide)» (см. раздел «15. Удаленный доступ»).

4. ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата изменений	Версия док-та	Описание изменений
09.07.2021	01.00	Исходная редакция документа, разработанная с учетом требований PCI DSF (версии 3.2.1) и PA-DSS (версия 3.2)
17.10.2022	01.01	Внесены корректировки, учитывающие требования PCI DSS (версия 4.0), PCI SLC v.1.1 и PCI SSS v.1.1
22.12.2023	01.02	Документ пересмотрен с учетом изменений в стандарте PCI SSS v.1.2.1