УТВЕРЖДЕН
ТАСП.62.01.12.000.005-ЛУ

КОМПЛЕКС ПРОГРАММ
«ЗАЩИЩЕННАЯ ОПЕРАЦИОННАЯ СИСТЕМА «СИНТЕЗМ»
(КП «ЗОС «СинтезМ»)
Процедуры устранения недостатков
ТАСП.62.01.12.000.005 И1

Листов 25

2021

АННОТАЦИЯ

Настоящий документ содержит описание процедуры устранения недостатков, процедуры приема и отработки сообщений пользователей о недостатках безопасности и запросов на их исправление, описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждой редакции изделия «Комплекс программ «Защищенная операционная система «СинтезМ» (далее – Изделие, опытный образец).

СОДЕРЖАНИЕ

1. ПРОЦЕДУРЫ УСТРАНЕНИЯ НЕДОСТАТКОВ

Разработчик Изделия АО «ФИНТЕХ» внедрил и применяет систему менеджмента качества при проектировании, разработке, построении, эксплуатации и сервисном обслуживании ИТ-систем и их компонентов в соответствии с нормами стандарта ISO 9001:2011 и ГОСТ Р ИСО 9001–2015.

АО «ФИНТЕХ» осуществляет сбор сведений о работе произведенных продуктов и устранение недостатков, выявленных в процессе эксплуатации. АО «ФИНТЕХ» имеет специализированное структурное подразделение – Служба технической и сервисной поддержки, которая обеспечивает послепродажное обслуживание. В случае появления каких-либо проблем потребитель обращается в Службу технической и сервисной поддержки по телефону или по электронной почте и оставляет заявку, заполненную по определенной форме. Каждая заявка проходит обязательную регистрацию в диспетчерской Службы технической и сервисной поддержки.

Инженер Службы технической и сервисной поддержки, получивший от диспетчера заявку на устранение недостатков, производит ее первичное рассмотрение. На этом этапе перед ним ставится задача выяснить, решается ли проблема с помощью изменения настроек той версии программного обеспечения, которая стоит у заказчика, или же она связана с наличием ошибки в самом программном обеспечении. В первом случае инженер подготавливает рекомендации по изменениям в конфигурации и направляет их потребителю. В наиболее сложных случаях осуществляется выезд на место. Если проблему решить удалось, то диспетчер Службы технической и сервисной поддержки присваивает заявке статус завершенной. Для наиболее типичных случаев подготавливается краткое заключение с изложением способа решения и размещается в корпоративной базе знаний.

Невозможность разрешить проблему с помощью конфигурирования означает, что пришлось столкнуться с недостатками безопасности в самом опытном образце

(ОО). В этом случае инженер подготавливает документ «Извещение об ошибке», и заявка в комплекте с этим документом направляется разработчику ОО. В «Извещении об ошибке» должны быть отражены: версия ОО, установленная у заказчика, условия эксплуатации, при которых возникла ошибка, частота повторяемости ошибки, степень критичности для функционирования ПО, данные о среде функционирования (информационном окружении) ОО. Извещение направляется в Отдел тестирования. Диспетчер Службы технической и сервисной поддержки делает в базе заявок отметку о направлении Извещения и посылает потребителю уведомление, что его проблема может быть решена только в новой версии.

Разработка компенсирующих мер по защите информации или ограничений по применению средства, а также доведение информации о таких мерах и ограничениях до потребителей должны осуществляться в срок не более 48 часов с момента выявления недостатка. Доработка средства, в том числе разработка обновлений программного обеспечения средства, или разработка мер по защите информации, нейтрализующих недостаток, должна осуществляться в срок не более 60 дней с момента выявления недостатка. Сроки устранения недостатков определяются в каждом конкретном случае индивидуально, но не могут превышать 6 месяцев с момента занесения проблемы в систему управления недостатками.

Отдел тестирования ведет свою собственную базу данных, где регистрируются поступающие извещения и, одновременно, свой раздел в корпоративной базе знаний. Получив извещение, инженер отдела тестирования анализирует ситуацию и производит сбор информации о таких же или похожих ситуациях. Все собранные сведения заносятся в специальную форму в базе данных отдела тестирования. Если в результате анализа не удалось найти решение сразу, то принимается решение о моделировании ситуации на стенде.

В процессе моделирования главной является задача воспроизводства аварийной ситуации. Когда такие условия определены, то приглашается разработчики и им предоставляется доступ к стенду и передается вся собранная информация.

Обязанностью разработчика в данном случае будет устранить неисправность в программном обеспечении и представить отделу тестирования новую версию.

Когда исправленная версия готова, отдел тестирования осуществляет комплексные приемо-сдаточные испытания. В ходе испытаний проверяется: во-первых, отсутствие аварийной ситуации после установки на стенд этой версии, а во-вторых, наличие у нее всех заявленных функциональных возможностей. Таким образом, отдел тестирования принимает решение о том, что исправленная версия свободна от неисправности и процесс ее устранения не затронул остальную часть кода. После появления исправленной версии (и обновления для версии, в которой обнаружен недостаток) может быть принято решение о внесении необходимых изменений в документацию, включающих и руководство по внесению исправлений.

По завершении всех работ производится сохранение исправленных исходных кодов в системе управления конфигурацией и формируется индексация новой версии. Формируется новый дистрибутивный носитель и передается инженеру Службы технической и сервисной поддержки. Потребителю направляется уведомление, что обновления готовы, и с ним согласуется способ их отправки и установки.

В случае обнаружения уязвимостей в программных модулях изделия устранение уязвимости осуществляется путем установки сертифицированного обновления либо путем принятия иных организационно-технических мер, направленных на затруднение возможности эксплуатации уязвимости. При этом сами меры носят временный характер, а их использование допустимо до момента выпуска соответствующего обновления.

Установка обновлений производится под контролем инженера Службы технической и сервисной поддержки, в особо сложных случаях инженер лично устанавливает обновление с выездом на место. После получения от потребителя подтверждения о ликвидации проблемы, диспетчер Службы технической и сервисной поддержки присваивает заявке статус завершенной.

Порядок обновления изделия определен в разделе 4 документа КП «ЗОС «СинтезМ». Руководство системного программиста ТАСП.62.01.12.000.005 32 01

2. РУКОВОДСТВО ПО УСТРАНЕНИЮ НЕДОСТАТКОВ

2.1. Действия при получении сообщения о недостатке

При получении сообщения о предполагаемом недостатке безопасности (уязвимости) выполняются следующие действия:

1. Занесение проблемы в систему управления недостатками, с подробным описанием.

2. Назначение исполнителя по данной проблеме.

3. Исполнитель проводит анализ воспроизводимости проблемы, анализ исходного кода для выявления модуля и/или функции реализующей функцию безопасности содержащую предполагаемый недостаток.

4. Проводится моделирование действий для воспроизведения предполагаемого недостатка безопасности.

5. В случае если проблема воспроизводится, проводится отладка для выявления места в исходном коде предполагаемого недостатка безопасности.

6. Вносится исправление в исходный код для исправления выявленного недостатка безопасности.

7. Осуществляется проверка разработчиком устранения недостатка безопасности.

8. Выполняется компиляция и сборка изделия для передачи на тестирование.

9. Изделие проходит проверку в системе тестирования.

10. В случае обнаружения дефектов исполнитель продолжает работу по устранению дефектов (пункты 3-8).

11. В случае успешного прохождения тестов исправление фиксируется в репозитории исполнителя, и отправляется запрос руководителю проекта на внесение изменений в главный репозиторий и сборку релизной версии.

12. Если недостатки выявлены в сертифицированном изделии, то изделие с внесенными изменениями представляется на инспекционный контроль в испытательную лабораторию, проводившую сертификационные испытания.

2.2. Способы, используемые для предоставления пользователям ОО необходимой информации о каждом недостатке безопасности

Разработчиком осуществляется постоянный (не реже одного раза в месяц) мониторинг сайтов, где публикуются общеизвестные уязвимости. Поиск общеизвестных уязвимостей проводится посредством анализа информации, представленной на сайтах www.bdu.fstec.ru, cve.mitre.org, securityfocus.com, nvd.nist.gov, securitylab.ru.

Разработчиком в рамках процессов жизненного цикла осуществляется непрерывный поиск недостатков в средстве, в том числе по выявлению уязвимостей и недекларированных возможностей средства. Поиск недостатков, уязвимостей и недекларированных возможностей осуществляется за счет проведения комплекса мероприятий, включающих: Тестирование на проникновение, Статический анализ исходного кода, Фаззинг-тестирование ПО.

На сайте www.fintech.ru предоставляется возможность получения информации о необходимых обновлениях с описанием устраненных недостатков. Пользователи изделия информируются по электронной почте о выпуске обновлений изделия и устраненных в новых версиях недостатках.

Информирование Пользователей изделия о обнаруженных недостатках средства осуществляется по электронной почте путем отправки сообщений на электронные адреса потребителей.

Доведение информации о недостатках средства, а также о компенсирующих мерах по защите информации или ограничений по применению средства до ФСТЭК России и банка данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России, осуществляется в соответствии с пунктом 2.2 «Регламента включения информации об уязвимостях программного обеспечения и

программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России» в течение 3 рабочих дней с даты ее выявления.

2.3. Порядок контроля целостности полученного обновления

При получении обновлений на оптическом носителе подсчет и проверка контрольной суммы, получаемой согласно ГОСТ 28147-89, осуществляется на ПЭВМ с КП «ЗОС «СинтезМ» в следующей последовательности:

1) установить оптический диск в устройство для чтения дисков;

2) в приложении «Magma» перейти во вкладку «Диски и ISO»

3) выбрать привод, в котором находится рассчитываемый диск (по умолчанию указан /dev/sr0);

4) выбрать директорию для сохранения текстового документа с результатом расчета директорий, для этого нажать кнопку «Выбрать» в строке «Выберите директорию для сохранения;

5) нажать на кнопку «Рассчитать КС диска»;

6) ожидать завершения работы программы подсчета контрольной суммы;

7) сравнить значение контрольной суммы, сохраненное в выбранной директории, со значением, поставляемым с обновлением.

Подсчет контрольной суммы с использованием программы «ФИКС-Unix 1.0» осуществляется на ПЭВМ, с КП «ЗОС «СинтезМ» и программой «ФИКС-Unix 1.0» (ufix), в следующей последовательности:

1) установить оптический диск в устройство для чтения дисков;

2) создать временную директорию для монтирования оптического диска командой:

```
# mkdir /tmp/template_d
```

3) примонтировать диск командой:

```
# mount –o loop /dev/sr0 /tmp/template_d;
```

4) создать директорию для временного хранения результатов:

```
# mkdir /root/$(date +%Y-%m-%d)-ks-iso
```

5) последовательно выполнить команды для подсчета контрольной суммы:

```
# ufix -jR /tmp/template_d/ > /root/$(date +%Y-%m-%d)-ks-iso/list.txt
# ufix -e /root/$(date +%Y-%m-%d)-ks-iso/list.txt
# ufix -h /root/$(date +%Y-%m-%d)-ks-iso/list.prj
# ufix -lv /root/$(date +%Y-%m-%d)-ks-iso/list.prj > /root/$(date +%Y-%m-%d)-ks-iso/list.ks
```

6) открыть в браузере полученный файл /root/$(date +%Y-%m-%d)/list.html

7) сравнить значение контрольной суммы (строка «ВСЕГО»), выданной на экран, со значением, поставляемым с обновлением;

8) отмонтировать диск командой:

```
# umount /tmp/template_d
```

2.4. Способ связи пользователей ОО с разработчиком

Связь пользователей с разработчиками осуществляется посредством электронной почты sintezm@fintech.ru Технического центра изделия, или через сайт компании www.fintech.ru.

3. ПРОЦЕДУРА АНАЛИЗА ВЛИЯНИЯ ОБНОВЛЕНИЙ НА БЕЗОПАСНОСТЬ ОС

3.1. Общие положения

Анализ влияния обновлений на безопасность ОС выполняется на стендах предприятия-производителя. Схемы стендов и их конфигурации представлены в тестовой документации «Комплекс программ «Операционная система «СинтезМ-К». Тестовая документация. ТАСП.62.01.12.000.005 Б10».

Выполняется анализ влияния обновлений на следующие функции безопасности ОС:

- идентификация и аутентификация;
- управление доступом;
- регистрация событий безопасности;
- ограничение программной среды;
- изоляция процессов;
- защита памяти;
- контроль целостности;
- обеспечение надежного функционирования;
- фильтрация сетевого потока;
- среда виртуализации.

3.2. Порядок проведения анализа влияния обновлений на безопасность ОС

Анализ влияния обновлений на безопасность выполняется в следующем порядке:

Установка обновленного дистрибутива. Обновленный дистрибутив ПО ОС устанавливается в соответствии с порядком, указанным в эксплуатационной документации на ОС.

Верификация версии ПО ОС. В ходе выполнения данного шага необходимо убедиться, что версия ПО ОС соответствует версии, указанной в сопроводительной

документации. Верификация версии ПО выполняется с использованием интерфейсов управления ОС.

Выполнение тестовых процедур, указанных в плане тестирования в тестовой документации «Комплекс программ «Операционная система «СинтезМ-К». Тестовая документация. ТАСП.62.01.12.000.005 Б10».

3.3. Предоставление обновлений для внешнего контроля

Процедура предоставления обновлений для внешнего контроля включает следующие действия:

– разработчик и уполномоченная организация, осуществляющая внешний контроль, договариваются о форме предоставления обновления;

– разработчик предоставляет доступ к обновлениям в соответствии с выбранной формой представления;

– разработчик предоставляет доступ к программной и эксплуатационной документации на ОО, а также документации к обновлению.

Порядок проведения контроля указан в подразделе 3.2 документа «КП «ОС «СинтезМ-К» Свидетельство анализа влияния обновлений на безопасность ТАСП.62.01.12.000.005 Б9». Порядок проведения тестирования при внешнем контроле соответствует порядку представленном в документе «КП «ОС «СинтезМ-К» Тестовая документация ТАСП.62.01.12.000.005 Б10».

Результаты тестирования обновлений оформляются организацией, осуществляющей внешний контроль, в виде отчета и предоставляются разработчику. Разработчиком, на сайте разработчика, осуществляется публикация отчета или выписки из него содержащей результаты тестирования обновлений.

Состав Отчета о проведении анализа влияния обновлений на функции безопасности Операционной системы «СинтезМ-К» представлен в пункте 3.4 настоящего документа

3.4. Обработка полученных результатов

По результатам выполнения действий, указанных в подразделе 3.2 настоящего документа, должен оформляться «Отчет о проведении анализа влияния обновлений на функции безопасности Операционной системы «СинтезМ-К», который представляется в испытательную лабораторию при проведении инспекционного контроля.

Документ должен содержать следующую информацию:

– номер обновления, в отношении которого выполнялась проверка;

– результаты выполнения проверок, выполненных в соответствии с тестовой документацией;

– вердикт и обоснование влияния/отсутствия влияния обновления на безопасность ОС;

– решение о публикации обновления на сервере обновлений предприятия-производителя.

Обновление признается не влияющим на безопасность ОС, если выполняются все условия, приведенные ниже:

– версия ПО ОС совпадает с версией, указанной в сопроводительной документации;

– в ходе выполнения функционального тестирования фактические результаты тестирования совпали с ожидаемыми для всех тестовых процедур.

Документ также должен содержать:

– краткое описание влияния обновления на задание по безопасности, представление функций безопасности ОС, реализацию функций безопасности ОС или содержать логическое обоснование отсутствия такого влияния;

– в случае если обновление влияет на задание по безопасности (в задание по безопасности вносятся уточнения в описания функций безопасности и сопоставленные с ними функциональные требования безопасности), представления, реализацию функций безопасности ОС, идентифицируются все функции

безопасности ОС, на которые воздействует данное обновление, и приводится краткое описание, каким образом обновление влияет на функции безопасности ОС;

– аргументацию для принятия испытательной лабораторией решения о возможности использования обновления потребителями ОС и необходимости или отсутствии необходимости проведения повторных испытаний ОС.

4. РЕГЛАМЕНТ ОБНОВЛЕНИЯ

4.1. Типы обновлений

В жизненном цикле КП «ЗОС «СинтезМ» предусмотрены следующие типы выпускаемых обновлений:

1) пакет обновления ОО – обновленная версия ОО с добавлением новых функциональных возможностей;

2) патч – исправление недостатков в ОО или пакете обновления ОО, выявленных на этапе эксплуатации изделия, выпускаемое по мере необходимости;

3) пакет модификаций – дистрибутив, содержащий все патчи, выпущенные за период после последней сертификации или инспекционного контроля. Выпускается в случае накопления большого количества патчей.

4.2. Оповещение потребителей о выпуске обновлений

Оповещение потребителей осуществляется инженерами Службы технической и сервисной поддержки разработчика. При формировании новой версии или обновления носитель передается инженеру Службы технической и сервисной поддержки разработчика. Потребителю направляется уведомление, что обновления готовы, и с ним согласуется способ их отправки и установки.

Разработчик ведет учет покупателей лицензии на дистрибутив ОО. Уведомление о выпуске обновлении программного обеспечения выполняется с использованием рассылки электронных почтовых сообщений с адреса электронной почты sintezm@fintech.ru.

Разработчик формирует документ с описанием обновления и отправляет его совместно с обновлением потребителю. Данный документ содержит описание обновления, процедур получения и контроля целостности обновления, процедур тестирования, установки, применения и верификации.

4.3. Предоставление обновлений потребителям

На сайте www.fintech.ru предоставляется возможность получения информации о необходимых обновлениях с описанием устраненных недостатков. Пользователи изделия информируются по электронной почте о выпуске обновлений изделия и устраненных в новых версиях недостатках.

Доставка обновлений программного обеспечения ОО до потребителей может осуществляться:

− с использованием сетевых протоколов передачи данных, за счет загрузки обновлений с сайта АО «ФИНТЕХ» (далее - разработчик).

− на DVD-дисках, промаркированных в соответствии с техническими условиями ТАСП.62.01.12.000.005 93 01.

Обновления, успешно прошедшие контроль влияния на безопасность ОО, публикуются в закрытой части сайта разработчика. Для получения обновлений с сайта разработчика, потребителю необходимо пройти по ссылке, указанной в письме, сформированном сотрудником Службы технической и сервисной поддержки разработчика по факту появления обновления.

Доступ потребителей к закрытой части сайта осуществляется с использованием учетной записи и пароля.

На сайте www.fintech.ru предоставляется возможность получения необходимых обновлений с описанием устраненных недостатков.

4.4. Проверка подлинности и целостности обновлений

Для проверки подлинности и целостности обновлений, до применения, необходимо осуществить процедуры контроля целостности и проверки подписи обновления.

4.4.1. Проведение контроля целостности обновления

При получении обновлений на оптическом носителе подсчет и проверка контрольной суммы, получаемой согласно ГОСТ 28147-89, осуществляется на ПЭВМ с КП «ЗОС «СинтезМ» в следующей последовательности:

8) установить оптический диск в устройство для чтения дисков;

9) в приложении «Magma» перейти во вкладку «Диски и ISO»

10) выбрать привод, в котором находится рассчитываемый диск (по умолчанию указан /dev/sr0);

11) выбрать директорию для сохранения текстового документа с результатом расчета директорий, для этого нажать кнопку «Выбрать» в строке «Выберите директорию для сохранения;

12) нажать на кнопку «Рассчитать КС диска»;

13) ожидать завершения работы программы подсчета контрольной суммы;

14) сравнить значение контрольной суммы, сохраненное в выбранной директории, со значением, поставляемым с обновлением.

Подсчет контрольной суммы с использованием программы «ФИКС-Unix 1.0» осуществляется на ПЭВМ, с КП «ЗОС «СинтезМ» и программой «ФИКС-Unix 1.0» (ufix), в следующей последовательности:

9) установить оптический диск в устройство для чтения дисков;

10) создать временную директорию для монтирования оптического диска командой:

```
# mkdir /tmp/template_d
```

11) примонтировать диск командой:

```
# mount –o loop /dev/sr0 /tmp/template_d;
```

12) создать директорию для временного хранения результатов:

```
# mkdir /root/$(date +%Y-%m-%d)-ks-iso
```

13) последовательно выполнить команды для подсчета контрольной суммы:

```
# ufix -jR /tmp/template_d/ > /root/$(date +%Y-%m-%d)-ks-
iso/list.txt
# ufix -e /root/$(date +%Y-%m-%d)-ks-iso/list.txt
# ufix -h /root/$(date +%Y-%m-%d)-ks-iso/list.prj
# ufix -lv /root/$(date +%Y-%m-%d)-ks-iso/list.prj > /root/$(date
+%Y-%m-%d)-ks-iso/list.ks
```

14) открыть в браузере полученный файл /root/$(date +%Y-%m-%d)/list.html

15) сравнить значение контрольной суммы (строка «ВСЕГО»), выданной на экран, со значением, поставляемым с обновлением;

16) отмонтировать диск командой:

```
# umount /tmp/template_d
```

Проверка осуществляется путем сравнения значения контрольной суммы, полученной в результате подсчета программным средством, указанным в формуляре на изделие ТАСП.62.01.12.000.005 30 01, с контрольными суммами дистрибутивов компонентов изделия, приведенными в формуляре ТАСП.62.01.12.000.005 30 01.

При поставке обновлений с использованием сетевых протоколов передачи данных процедура контроля целостности обновления обеспечивается путем сравнения значения контрольной суммы (КС) обновления, полученной в результате расчета программным средством, указанным в формуляре ТАСП.62.01.12.000.005 30 01, с КС обновления указанной в документе с описанием обновления.

В случае обнаружения несоответствий при проведении проверки обновления необходимо обратиться к производителю.

4.4.2. Формирование подписи

Формирование подписи осуществляется командой:

```
# /opt/cprocsp/bin/amd64/cryptcp -sign -askpin -detached
file_to_sign
```

, где: file_to_sign – путь до подписываемого файла обновления.

При выполнении подписи будет выполнен запрос на ввод пароля от хранилища сертификата, которым будет осуществляется подпись. В результате выполнения команды в директории будет создан отдельный файл подписи (Рисунок 4.1).

Например:

```
# /opt/cprocsp/bin/amd64/cryptcp -sign  -askpin -detached
UPDATE_31092020.7z
```

```
[root@crypt UPDATE]# ll
total 4
-rw-r--r--. 1 root root 4 Dec 18 07:24 UPDATE_31092020.7z
[root@crypt UPDATE]# /opt/cprocsp/bin/amd64/cryptcp -sign -askpin -detached ./UPDATE_31092020.7z
CryptCP 5.0 (c) "Crypto-Pro", 2002-2019.
Command prompt Utility for file signature and encryption.

The following certificate will be used:
RDN:Moscow, "AO ""test_ORG""", Fintech_test_code_sign, fintech@fintech.ru
Valid from 15.12.2020 08:07:30 to 15.03.2021 08:17:30

Certificate chains are checked.
Folder './':
./UPDATE_31092020.7z... Enter pin for container 73dd9c5a6-3e82-5fb0-4bec-6f9aa29aa1f:
Signing the data...
Signed message is created.
[ErrorCode: 0x00000000]
[root@crypt UPDATE]# ll
total 8
-rw-r--r--. 1 root root    4 Dec 18 07:24 UPDATE_31092020.7z
-rw-r--r--. 1 root root 2085 Dec 18 07:24 UPDATE_31092020.7z.sgn
[root@crypt UPDATE]#
```

Рисунок 4.1 – Формирование подписи

4.4.1. Проверка подписи

Проверка подписи осуществляется командой:

```
# /opt/cprocsp/bin/amd64/cryptcp -verify ./signed_file -detached ./sign
```

, где: signed_file – файл подпись которого проверяется;

sign – файл подписи.

Например:

```
# /opt/cprocsp/bin/amd64/cryptcp -verify ./UPDATE_31092020.7z -detached ./UPDATE_31092020.7z.sgn
```

В случае успешного завершения проверки подписи на экране отобразиться сообщение (Рисунок 4.2):

```
«Signature's verified.
[ErrorCode: 0x00000000]»
```

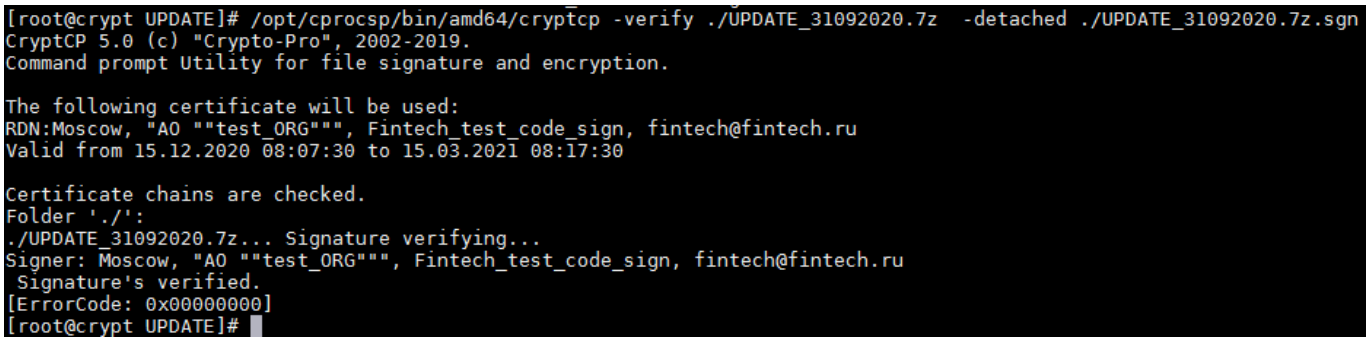

Рисунок 4.2 – Проверка подписи

В случае обнаружения внесения несанкционированных изменений в подписанный файл отобразиться сообщение (Рисунок 4.3):

```
«Error: Invalid Signature.
/dailybuildsbranches/CSP_5_0r0/CSPbuild/CSP/samples/CPCrypt/DSign.cpp:
748: 0x80090006
Error: Signature.
/dailybuildsbranches/CSP_5_0r0/CSPbuild/CSP/samples/CPCrypt/DSign.cpp:
863: 0x200001F9
[ErrorCode: 0x200001f9]»
```

```
[root@crypt UPDATE]# /opt/cprocsp/bin/amd64/cryptcp -verify ./UPDATE_31092020.7z  -detached ./UPDATE_31092020.7z.sgn
CryptCP 5.0 (c) "Crypto-Pro", 2002-2019.
Command prompt Utility for file signature and encryption.

The following certificate will be used:
RDN:Moscow, "АО ""test_ORG""", Fintech_test_code_sign, fintech@fintech.ru
Valid from 15.12.2020 08:07:30 to 15.03.2021 08:17:30

Certificate chains are checked.
Folder './':
./UPDATE_31092020.7z... Signature verifying...
Signer: Moscow, "АО ""test_ORG""", Fintech_test_code_sign, fintech@fintech.ru
Error: Invalid Signature.
/dailybuildsbranches/CSP_5_0r0/CSPbuild/CSP/samples/CPCrypt/DSign.cpp:748: 0x80090006
Error: Signature.
/dailybuildsbranches/CSP_5_0r0/CSPbuild/CSP/samples/CPCrypt/DSign.cpp:863: 0x200001F9
[ErrorCode: 0x200001f9]
[root@crypt UPDATE]#
```

Рисунок 4.3 – Подпись не верна

4.5. Тестирование и отладка обновления

Тестирование и отладка обновления осуществляется в соответствии с п 2.4. документа «КП «ЗОС «СинтезМ» Документация по определению жизненного цикла (ТАСП.62.01.12.000.005 П1).

Проведение тестирования является обязательным перед передачей версии КП «ЗОС «СинтезМ» потребителю. Тестирование проводится сотрудниками отдела тестирования разработчика. Для тестирования и отладки программной продукции сотрудники отдела собирают стенд, выдается задание на тестирование. По результатам тестирования осуществляется устранение ошибок и осуществляется (при необходимости) доработка программного обеспечения.

Порядок проведения тестирования описан в документе «КП «ЗОС «СинтезМ» Тестовая документация ТАСП.62.01.12.000.005 Б10»

4.6. Установки и применения обновления

В случае, если хост, на котором выполняется обновление программного обеспечения ОС является виртуальной машиной, до начала проведения обновления необходимо выполнить создание снимка (снапшота) виртуальной машины. Процедура создания снимков виртуальных машин описана в пункте 3.22.3. документа «КП «СинтезМ-ЗЭП» Руководство системного программиста (ТАСП.62.01.11.000.021 32 01)».

В случае, если хост, на котором выполняется обновление программного обеспечения ОС является физическим АРМ или сервером, до начала проведения обновления необходимо выполнить создание резервных копий системных директорий операционной системы в соответствии с порядком описанным в п. 3.9.1 документа «КП «СинтезМ-ЗЭП» Руководство системного программиста (ТАСП.62.01.11.000.021 32 01)».

Обновление ОО осуществляется в соответствии с порядком, описанным в документации, поставляемой на обновление. Установка/обновление пакетов обновлений осуществляется менеджером пакетов yum в соответствии с порядком, описанным в п. 3.10.3. документа «КП «СинтезМ-ЗЭП» Руководство системного программиста (ТАСП.62.01.11.000.021 32 01)».

Инструкция по установке и применению обновления содержит следующую информацию:

- описание обновления;
- описание процедуры получения обновления;
- описание контроля целостности обновления;
- описание установки обновления;
- описание применения;
- описание процедур тестирования и верификации.

4.7. Контроль установки обновления

Для контроля установки обновления необходимо убедиться, что после установки обновления установленная версия обновляемых пакетов соответствует версии, указанной в документации на обновление.

Верификация применения обновления выполняется за счет тестирования каждой функция безопасности. Порядок проведения тестирования описан в документе «КП «ЗОС «СинтезМ» Тестовая документация ТАСП.62.01.12.000.005 Б10».

Приложение А

Перечень сокращений и обозначений

(обязательное)

АСЗИ	–	автоматизированная система в защищенном исполнении
АО	–	акционерное общество
ОО	–	объект оценки
ОС	–	операционная система
ПО	–	программное обеспечение

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер документа	Входящий номер сопрово-дительного докум. и дата	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных					