УТВЕРЖДЕН

ТАСП.62.01.12.000.005 П1-ЛУ

КОМПЛЕКС ПРОГРАММ
«ЗАЩИЩЕННАЯ ОПЕРАЦИОННАЯ СИСТЕМА «СИНТЕЗМ»
(КП «ЗОС «СинтезМ»)

Документация по определению жизненного цикла

ТАСП.62.01.12.000.005 П1

Листов 24

2021

АННОТАЦИЯ

Настоящий документ является описанием процессов жизненного цикла комплекса программ «Защищенная операционная система «СинтезМ» (далее по тексту – изделие или КП «ЗОС «СинтезМ») и содержит сведения о жизненном цикле программного обеспечения, в том числе устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения, а также информацию о персонале, необходимом для обеспечения такой поддержки.

1. Назначение КП «ЗОС «СинтезМ»

КП «ЗОС «СинтезМ» представляет собой комплекс программ, соответствующий требования безопасности к ОС общего назначения (тип «А») четвертого класса защиты и может быть использован для создания АСЗИ в части обеспечения функционирования серверных группировок и автоматизированных рабочих мест пользователей, а также обеспечения выполнения требований по защите информации, обрабатываемой в АСЗИ, от НСД и реализации защищенного вычислительного процесса.

2. Жизненный цикл КП «ЗОС «СинтезМ»

Планирование и разработка требований к процессам жизненного цикла продукции регламентированы стандартом организации СТО ФТ 7.1-2016 «Планирование жизненного цикла продукции».

Жизненный цикл (ЖЦ) включает период создания и использования КП «ЗОС «СинтезМ», начиная с момента возникновения потребности в КП «ЗОС «СинтезМ», заканчивая её технической поддержкой.

Жизненный цикл определен с учетом положений следующих стандартов:

– ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»;

– ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

– ГОСТ РВ 0015-002-2012 «Системы менеджмента качества. Общие требования».

Для разработки КП «ЗОС «СинтезМ» выбрана итерационная модель жизненного цикла (рисунок 2.1).

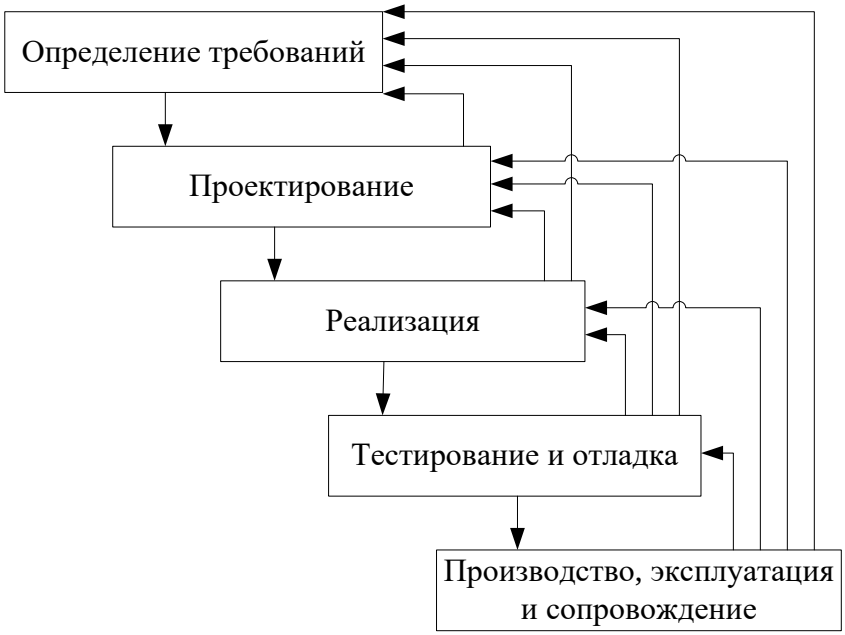

Рисунок 2.1 – Модель жизненного цикла

Стрелки, идущие вверх, обозначают возвраты к предыдущим этапам, для доработки по уточненным требованиям или для исправления обнаруженной ошибки.

Модель жизненного цикла обеспечивает необходимый контроль над разработкой и сопровождением КП «ЗОС «СинтезМ».

В АО «ФИНТЕХ» процессы управления конфигурацией КП «ЗОС «СинтезМ» осуществляются с использованием репозитория эталонных пакетов и дистрибутивов, стенда сборки и системы контроля версий.

Основными процессами жизненного цикла программной продукции являются:

- определение требований
- проектирование;
- реализация;
- тестирование и отладка;
- производство, эксплуатация и сопровождение.

2.1. Определение требований

Для каждой итерации разработки КП «ЗОС «СинтезМ» на этапе определения требований выявляются потребности в доработке

КП «ЗОС «СинтезМ». Определение и спецификация требований основываются на анализе выявленных бизнес-требований, функциональных требований, пользовательских требований, и внешних обязательств перед эксплуатирующими организациями.

По окончании выполнения данного этапа сотрудники информационно-аналитического отдела формируют перечень требований к КП «ЗОС «СинтезМ», включающий:

– функциональные требования по безопасности, описывающие действия, которые должно выполнять ПО с целью нейтрализации угроз безопасности информации;

– требования доверия, описывающих свойства и параметры ПО, имеющие отношение к нейтрализации угроз безопасности информации.

Сформированный перечень утверждается руководителем департамента разработки автоматизированных средств в защищенном исполнении.

2.2. Проектирование

Этап проектирования включает в себя:

– оценку входных и выходных данных;

– планирование проектирования и реализации;

– макетирование и уточнение требований;

– проведение анализа проекта;

– проведение верификации и валидации проекта;

– управление изменениями проекта;

– осуществление мониторинга процесса проектирования.

Работы по проектированию проводят сотрудники отдела сопровождения защищенной платформы АСЗИ. Мониторинг процесса проектирования осуществляется руководителем департамента разработки автоматизированных средств в защищенном исполнении, кроме того, он назначает сотрудников группы, ответственных за верификацию и валидацию проекта.

В процессе проектирования архитектуры ПО осуществляется:

– экспертная оценка и моделирование угроз с учетом сбора информации об области применения разрабатываемого ПО, типе обрабатываемой информации, среде эксплуатации ОО, снижение поверхности возможных атак;

– выявлен перечень заимствованных у сторонних разработчиков ПО компонентов, предполагаемых к использованию при разработке ПО и проведен анализ их защищенности, исключено использование вышедших из употребления и небезопасных компонент;

– формирование списка используемых инструментальных средств производства.

Также для архитектуры ОО предусматривается:

– уточнение проекта архитектуры, обеспечивается выбором проектных решений, направленных на нейтрализацию выявленных угроз безопасности информации;

– документирование и поддержание в актуальном состоянии, за счет периодического пересмотра компонентов ПО с учетом их версий, реализуется в том числе внутренними средствами GitLab при работе с репозиторием пакетов;

– идентификация, документирование, стратегия обработки выявляемых недостатков и угроз безопасности информации для компонентов ПО ОО (см. документ «Процедуры устранения недостатков ТАСП.62.01.12.000.005 И1»).

В процессе конструировании, создании ПО ОО, а также в процессе эксплуатации изделия также обязателен пересмотр документации на изделие при изменении любого элемента конфигурации ОО. Прослеживаемость исходного кода

программы и реализуемом на его основе пакета, логическая принадлежность к функциональной группе применения, также фиксируется в информации о пакете (см. документ «Руководство по разработке программного обеспечения АО «ФИНТЕХ»). Сведения о прослеживаемости исходного кода программы к проекту архитектуры программы представлены в документах «Комплекс программ «Защищенная операционная система «СинтезМ». Технический проект» (ТАСП.62.01.12.000.005 ТП) и «Комплекс программ «Защищенная операционная система «СинтезМ». Эскизный проект» (ТАСП.62.01.12.000.005 ЭП).

Подробная информация о видах средств, используемых при производстве, конструировании и разработке ОО, приведена в документе «Инструкция по сборке ТАСП.62.01.12.000.005 92 01», при добавлении нового или обновлении используемого инструментального средства указанный документ, должен быть обновлен:

- перечень инструментальных средств;
- используемая версия средства;
- применяемые опции и настройки.

Полученный на данном этапе план работ по реализации КП «ЗОС «СинтезМ» утверждается руководителем департамента разработки автоматизированных средств в защищенном исполнении.

2.3. Реализация

Реализация КП «ЗОС «СинтезМ» включает следующие процессы:

- разработка программной архитектуры, а также разработка решений по построению всех составных компонент;
- разработка исходных текстов, написание файлов спецификации для сборки пакетов прикладного программного обеспечения;
- сборка пакетов прикладного программного обеспечения и добавление их в репозиторий программного обеспечения;

– сборка дистрибутивов из репозитория программного обеспечения;

– контроль качества программного кода путем проведения проверки кода на предмет ошибок, использования статического анализа кода;

– поиск и устранение уязвимостей;

– анализ соответствия продукта предъявляемым требованиям безопасности и устранение найденных несоответствий;

– разработка программной документации в соответствии с ЕСПД и требованиями ФСТЭК России;

– контроль качества разработанной программной документации путем проведения проверки техническими экспертами, руководителем проекта и другими заинтересованными лицами.

Разработкой программной архитектуры и исходных текстов, сборкой пакетов и дистрибутивов, выполнением контроля качества, поиском и устранением уязвимостей, анализом соответствия продукта предъявляемым требованиям безопасности и устранением найденных несоответствий, разработкой программной документации и выполнением контроля качества программной документации занимаются сотрудники отдела сопровождения защищенной платформы АСЗИ.

В процессе реализации ПО и создания исходного текста программ, применяется перечень правил и рекомендаций, используемых разработчиками:

– о порядке оформления исходного кода;

– статический анализ исходного кода;

– экспертная оценка исходного кода программы.

Порядок правил и рекомендаций по оформлению исходного кода разрабатывается в зависимости от применяемых языков программирования (см. документ «Руководство по разработке программного обеспечения АО «ФИНТЕХ»).

До начала конструирования определяется порядок, методы и инструментальные средства проведения статического анализа исходного кода программы и параметры из запуска. Разработка процедуры проведения анализа,

анализ результатов статического анализа, ответственные за проведение определяются для каждого из проектов отдельно в процессе реализации ПО.

Важным подэтапом в процессе конструирования ПО является проведение экспертизы исходного кода, которая позволяет:

– подтвердить применение установленного порядка оформления, качество исходного кода;

– осуществить контроль соответствия правилам;

– инициировать процессы по пересмотру и изменению правил и рекомендаций по оформлению исходного кода, используемых в процессе разработки программы.

Качество исходного кода – совокупность параметров исходного кода, к которым относятся:

– читаемость кода;

– наличие комментариев к коду;

– легкость в поддержке, тестировании, отладке и устранении ошибок, модификации;

– экономное использование ресурсов: памяти, процессора, дискового пространства;

– отсутствие замечаний, выводимых компилятором;

– отсутствие неиспользуемых переменных, недостижимых блоков кода, ненужных устаревших комментариев и т. д.;

– адекватная обработка ошибок;

– возможность интернационализации интерфейса.

Для проведения экспертизы исходного кода должны применяться комбинации организационных и технических процедур:

– определяются способы проведения экспертизы;

– определяется необходимость привлечение инструментальных средств;

– определяются стратегии реагирования на недостатки и уязвимости, в зависимости от условий;

– привлечение работников и ответственных с определенными экспертными компетенциями.

Регламент экспертизы исходного кода, можно сформулировать в следующем виде:

1) руководитель при поступлении в подразделение задачи разработки программного продукта назначает ведущего программиста и определяет состав группы, работающей над разработкой ПО;

2) ведущий программист определяет периодичность процедуры рецензирования исходного кода, перечень событий, запускающих процесс рецензирования;

3) при наступлении события программист уведомляет рецензента о готовности исходного кода к рецензированию с указанием коммита;

4) рецензент получает из репозитория исходный код по указанному коммиту и просматривает его, оценивает параметры качества исходного кода;

5) в зависимости от качества исходного кода:

– рецензент вносит в исходный код комментарии, указывающие на ошибки и прочие недостатки исходного кода, создает коммит, в который включает свои комментарии. В комментарии к коммиту рецензент вносит оценку параметров качества исходного кода;

– рецензент подтверждает требуемый уровень качества исходного кода, создает коммит без изменений с соответствующим комментарием к коммиту. Конец процесса.

6) программист получает из репозитория изменения, внесенные в исходный код рецензентом, изучает комментарии рецензента, вносит исправления в исходный код, уведомляет рецензента о готовности к рецензированию с указанием нового коммита. Далее возврат на 4) шаг.

Исходный код – текст компьютерной программы на каком-либо языке программирования или языке разметки. Исходный код транслируется в исполняемый код целиком до запуска программы при помощи компилятора или может исполняться сразу при помощи интерпретатора.

Репозиторий исходного кода – хранилище исходного кода, доступное всем участникам процесса разработки программного продукта, обеспечивающее историческое хранение изменений в исходном коде, вносимых разработчиками в процессе разработки программного продукта.

Коммит – метка в репозитории исходного кода, идентифицирующее состояние исходного кода на заданный момент времени.

Рецензент – разработчик исходного кода, назначенный ведущим программистом, осуществляющий проверку исходного кода, разработанного программистами, на предмет выявления ошибок.

Рецензирование – процедура рассмотрения исходного кода рецензентом. Цель рецензирования – оценить качество исходного кода, в том числе: наличие ошибок в исходном коде, ясность исходного кода, возможность повторного использования исходного кода. Виды рецензирования кода:

– целевое рецензирование – разовая процедура проверки исходного кода отдельного модуля программного продукта;

– периодическое рецензирование – повторяющаяся выборочная проверка исходного кода отдельных модулей программного продукта.

Рецензия – отчет о качестве исходного кода, содержащий оценку параметров качества исходного кода, указание на ошибки и рекомендации по их устранению.

Результатами этапа разработки являются:

1. Пакеты программы с исходными кодами.
2. Программное обеспечение в виде собранных бинарных пакетов и дистрибутивов.
3. Комплект программной документации.

Описание мер безопасности, применяемых в АО «ФИНТЕХ» при разработке КП «ЗОС «СинтезМ» для защиты конфиденциальности и целостности проекта КП «ЗОС «СинтезМ» и её реализации в среде разработки, приведено в свидетельстве «Комплекс программ «Защищенная операционная система «СинтезМ». Документация безопасности разработки».

Сохранность КП «ЗОС «СинтезМ» реализуется путем резервного копирования и архивирования данных, находящихся на серверах и на файловых ресурсах.

2.4. Тестирование и отладка

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.

При тестировании и отладке программного обеспечения осуществляется:

- сборка дистрибутивов программного обеспечения;
- проведение тестирования программного обеспечения;
- устранение выявленных недостатков программного обеспечения;
- добавление в репозиторий эталонных версий дистрибутивов и исходных текстов программного обеспечения;
- корректировка программной документации.

Процесс тестирования ПО включает применение различных способов исследования и испытания ПО на этапе реализации, описанные в этом подпункте. Тестирования ПО осуществляется как на этапах производства, так и на этапах эксплуатации и сопровождения.

2.4.1. Функциональное тестирование

Функциональное тестирование – вид работ по исследованию программы, направленный на выявление отличий между ее реально существующими и требуемыми свойствами.

В процессе разработки Изделия отделом тестирования выполняется функциональное тестирование программы для того, чтобы определить, выполняются ли требования безопасности, идентифицированные в процессе анализа требований к ПО Функциональное тестирование осуществляется в соответствии с документом «Комплекс программ «Защищенная операционная система «СинтезМ» (КП «ЗОС «СинтезМ») Тестовая документация ТАСП.62.01.12.000.005 Б10». По результатам функционального тестирования программы проводится доработка программы.

2.4.2. Тестирование на проникновение

Тестирование на проникновение выполняется с целью выявления уязвимостей ПО путем имитации действий потенциального нарушителя. Тестирование на проникновение в отношении ПО выполняют работники разработчика ПО (Отдел тестирования) или сторонние специалисты, обладающие компетенцией в области проведения такого рода испытаний, для актуальной версии ПО.

Процесс тестирования на проникновение включает:

– определение компонентов ПО, для которых выполняется тестирование;

– разработка и документирование сценариев атак, с учетом архитектуры ПО, угроз безопасности информации, результатов статического анализа и экспертизы исходного кода ПО;

– выполнение тестирования и документирование результатов;

– анализ полученных результатов с точки зрения наличия уязвимостей ПО, принятие решений о стратегии их исправления;

– исправление уязвимостей ПО путем ее доработки в соответствии с выбранной стратегией при необходимости;

– в эксплуатационные документы включаются описание организационных или технических мер среды эксплуатации ПО, направленные на нейтрализацию уязвимостей ПО при необходимости.

Средства применяемые в процессе тестирования на проникновения и порядок применения данных средств представлен в документе «Комплекс программ «Защищенная операционная система «СинтезМ». Документация инструментальных средств разработки ТАСП.62.01.12.000.005 И2».

2.4.3. Статический анализ исходного кода

Статический анализ исходного кода ПО выполняется с использованием специализированных инструментальных средств (статических анализаторов) в режиме, не предусматривающем реального выполнения кода.

Статический анализ программных средств в КП «ЗОС «СинтезМ» выполняется с помощью анализатора Svace. При выполнении слиянии ветки dev, в которой ведется разработка, в master-ветку проекта в Gitlab, вызывается отправка исходных текстов на сервер сборки с помощью pipeline Jenkins. Один из этапов pipeline - сборка и анализ с помощью статического анализатора Svace. Результаты анализа Svace публикуются на сервере, к которому имеют доступ сотрудники отдела безопасности. Сотрудники отдела безопасности выполняют разметку выявленных проблем, комментируют проблемы, присваивают проблемам определенный статус:

Undecided – для предупреждений, для которых пока не производилась проверка. Это значение присваивается статусам новых предупреждений.

Confirmed – для предупреждений, которые пользователь, производивший разметку, посчитал истинными.

Won’t fix – для предупреждений, которые формально могут считаться истинными, но по тем или иным причинам исправление соответствующих дефектов не будет проводиться.

False Positive – для предупреждений, которые пользователь, производивший разметку, посчитал ошибочными.

Unclear – для предупреждений, для которых пользователь, производивший разметку, не смог определить истинность.

После выполнения разметки, разработчикам требуется подтвердить и устранить выявленные проблемы со статусом «Confirmed» в ветке dev, выполнить. слияние с веткой master.

Описанный выше процесс выполняется итерационно до тех пор, пока в Svace остаются проблемы с меткой «Confirmed».

2.4.4. Динамический анализ

Динамический анализ включает регрессионное тестирование с помощью санитайзеров и фаззинг.

Инструменты динамического анализа, применяемые при разработке дистрибутива КП «ЗОС «СинтезМ» АО ФИНТЕХ выполняют поиск ошибок работы с памятью: переполнение буфера, использование памяти после освобождения, утечки памяти, обращение к неинициализированным переменным. Они также позволяют обнаруживать состояние гонки для потоков, ситуации взаимной блокировки, обращения по нулевому указателю, деление на ноль, переполнения для типов данных и некорректные битовые сдвиги.

Средства для проведения регрессионного анализа:

1. Санитайзеры ASAN, MSAN, UBSAN;
2. LLVM, Clang, gcc, lcov, gcov.

2.4.4.1. Фаззинг-тестирование ПО

Фаззинг-тестирование программы выполняется с целью формирования перечня потенциальных уязвимостей программы. При выполнении фаззинг тестирования производится манипулирование входными данными программы или ее компонентов и фиксирование нарушений штатного поведения в результате обработки таких данных. Выявленные нарушения анализируются с целью формирования перечня потенциальных уязвимостей программы, который в дальнейшем используется при проведении тестирования проникновения.

Фаззинг-тестирование проводится сотрудниками отдела безопасности АО «ФИНТЕХ» после выпуска кандидата в релизы дистрибутива изделия в следующем порядке:

1) Анализ, какие векторы атаки есть в дистрибутиве.

2) Определение поверхности и глубины атаки.

3) Пакеты с описанием вектора атаки направляются на фаззинг-тестирование.

Дистрибутив кандидат в релизы не может стать стабильным до тех пор, пока не выполнен фаззинг для основных пакетов на выбранном векторе атаки.

После выпуска стабильной версии дистрибутива изделия фаззинг продолжается до выхода новой версии кандидата в релизы. В фаззинг-тестировании пакетов участвуют разработчики и специалисты по фаззингу (сотрудники отдела безопасности).

Список средств, применяющихся в фаззинге:

1. AFL++
2. Crusher
3. afl-cov (для покрытия)
4. syzkaller

2.4.5. Регламент проведения тестирования

В данном подпункте описаны общие принципы процедур проведения различных видов тестирования.

Руководитель отдела тестирования, отдела разработки программных средств защиты информации (ОРПСЗИ) и отдела сопровождения защищенной платформы АСЗИ (ОСЗП АСЗИ), с привлечением специалистов по информационной безопасности (Департамент информационной безопасности) выполняют анализ требований к ПО, определяют перечень работ по тестированию, используемые стратегии, средства и ресурсы, подходы, распределение обязанностей и

ответственности между работниками, сроки выполнения работ и условий завершения тестов, разрабатывают план тестирования.

Специалисты отдела тестирования (Ведущий тестировщик, тестировщик), с привлечением специалистов из отделов разработки программных средств защиты информации (ОРПСЗИ) и сопровождения защищенной платформы АСЗИ (ОСЗП АСЗИ):

– разрабатывает описание процедур тестирования и ожидаемых результатов для ПО, в отношении которой необходимо провести тестирование, версии ПО или отдельной ее части при необходимости;

– осуществляет тестирование в соответствии с разработанными процедурами тестирования;

– документирует результаты выполнения тестовых процедур;

– формирует отчет о недостатках, обнаруженных в процессе тестирования, фиксирует информацию и идентифицирует недостаток в системе учета запросов и ошибок.

Тестирование проводится в соответствии с порядком, описанным в документе «КП «ЗОС «СинтезМ» Тестовая документация ТАСП.62.01.12.000.005 Б10»

Анализ результатов выполненных работ по тестированию, оценку критериев завершения тестирования, анализ недостатков идентифицированных уязвимостей, изменение процесса тестирования при необходимости выполняется экспертной оценкой с привлечением руководителей отдела тестирования, отдела разработки программных средств защиты информации (ОРПСЗИ) и отдела сопровождения защищенной платформы АСЗИ (ОСЗП АСЗИ), специалистов по информационной безопасности.

2.5. Производство, эксплуатация и сопровождение

Предприятие-изготовитель гарантирует соответствие качества программного обеспечения при соблюдении потребителем (пользователем) условий и правил хранения, транспортирования, установленных эксплуатационными документами.

В период эксплуатации и сопровождения программного обеспечения АО «ФИНТЕХ» оказывает помощь в установке и настройке

КП «ЗОС «СинтезМ», устраняет недостатки, возникающие в работе программного обеспечения, выявляет и устраняет публикованные уязвимости, а также осуществляет обучение персонала, эксплуатирующего программное обеспечение.

2.5.1. Тиражирование

Тиражирование осуществляется сотрудниками Отдела сопровождения защищенной платформы АСЗИ (ОСЗП АСЗИ). Запись образца изделия осуществляется на стенде информационно-безопасного тиражирования. Описание процедуры тиражирования образца изделия представлено в документе «Комплекс программ «Защищенная операционная система «СинтезМ» (КП «ЗОС «СинтезМ») Инструкция по сборке ТАСП.62.01.12.000.005 92 01».

2.5.2. Порядок поставки

Порядок поставки описан в документе «Комплекс программ «Защищенная операционная система «СинтезМ». Технические условия» (ТАСП.62.01.12.0000.005 93 01).

2.5.3. Внедрение

АО «ФИНТЕХ» оказывает помощь в установке, настройке КП «ЗОС «СинтезМ», а также предприятие осуществляет обучение персонала, эксплуатирующего программное обеспечение.

2.5.4. Сопровождение

На этапе эксплуатации и сопровождения осуществляется техническая поддержка КП «ЗОС «СинтезМ».

Техническая поддержка программного обеспечения (ПО) – это процесс улучшения и оптимизации ПО, а также поддержка действующих специализированных программных систем.

Техническая поддержка позволяет обнаружить дефекты и недоработки, также добавлять новую функциональность, вносить изменения для повышения удобства использования программного обеспечения.

Услуги по поддержке программного обеспечения включают в себя работы по оптимизации функционирования программы при различных условиях эксплуатации.

Техническая поддержка осуществляется в формате консультирования пользователей и администраторов КП «ЗОС «СинтезМ» по вопросам установки, переустановки, администрирования и эксплуатации по каналам связи (телефону, электронной почте) или письменно по запросу.

Сотрудники АО «ФИНТЕХ» оказывают услуги по технической поддержке программного обеспечения, находясь в постоянном контакте с сотрудниками эксплуатирующей организации, что позволяет оперативно и динамично развивать ПО. Также сокращается время, необходимое на согласование плана работ, поскольку дополнения и исправления обычно несут менее глобальный характер, чем при разработке ядра операционной системы.

Описание оказываемых услуг по сопровождению КП «ЗОС «СинтезМ» приведено в «Соглашении о технической поддержке компании АО «ФИНТЕХ» (www.fintech.ru).

На этапе сопровождения осуществляется исправление ошибок и устранение неполадок, не выявленных ранее. Отделом сопровождения защищенной платформа АСЗИ осуществляется сбор информации о недостатках безопасности, обнаруженных в эксплуатирующих организациях, к полученным данным применяются процедуры по устранению недостатков.

Разработчиком осуществляется мониторинг сайтов, где публикуются общеизвестные уязвимости. Если в результате такого мониторинга обнаруживается уязвимость, применимая к поддерживаемому программному продукту, то группа осуществляет оповещение эксплуатирующих организаций, и применяются процедуры по устранению уязвимости.

Описание процедуры устранения недостатков (уязвимостей), как обнаруженных эксплуатирующей организацией, так и опубликованных, представлено в документе «Комплекс программ «Защищенная операционная система «СинтезМ». Процедуры устранения недостатков ТАСП.62.01.12.000.005 П2».

2.5.4.1. Анализ общеизвестных уязвимостей

Анализ общеизвестных уязвимостей в пакетах КП «ЗОС «СинтезМ» выполняется раз в месяц. Процесс должен повторяться до завершения срока поддержки. Анализ проводится:

- По базам данных;
- По сигнатурам.

Анализ общеизвестных требований выполняется сотрудниками отдела безопасности. Сотрудник отдела безопасности ведет мониторинг уязвимостей.

Автоматизация поиска общеизвестных уязвимостей осуществляется с помощью следующих средств, разработки АО «ФИНТЕХ»:

- VulnerabilityDownloader 2.6
- VulnerabilityUploader 2.1
- VulnerabilityWorker_Stage2-3 1.2

Так же используются СУБД MS SQL 2008 + Reporting Services.

VulnerabilityDownloader по данному списку наименований производит поиск по следующим базам общеизвестных уязвимостей: bdu.fstec.ru, cve.mitre.org, nvd.nist.gov. Найденные описания уязвимостей выгружаются в текстовый файл.

VulnerabilityUploader выполняет загрузку данных из текстового файла в БД.

VulnerabilityWorker_Stage2-3 предоставляет пользовательский интерфейс к данным БД, позволяющий разметить уязвимости по классам применимости в условиях конкретного программного продукта.

Формирование отчёта выполняется средствами Reporting Services.

2.5.5. Обновление

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.

По итогам тестирования и отладки сотрудник отдела сопровождения защищенной платформы АСЗИ, ответственный за выпуск версии

КП «ЗОС «СинтезМ», формирует заключение о качестве версии с оценкой уровня исправления ошибок и запускает процесс согласования разрешения на выпуск версии КП «ЗОС «СинтезМ» со следующими лицами:

- руководитель отдела сопровождения защищенной платформы АСЗИ;
- руководитель департамента разработки автоматизированных средств в защищенном исполнении.

Тестирование проводится в соответствии с порядком, описанным 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
ОС	–	операционная система
ЕСПД	–	единая система программной документации
ОКР	–	опытно-конструкторская работа
ПО	–	программное обеспечение
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю