ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА ЖЕЛЕЗНЫХ ДОРОГ (ОСЖД)

II издание

Разработано экспертами Комиссии ОСЖД
по инфраструктуре и подвижному составу
22-24 мая 2019 г., штаб-квартира МСЖД, г. Париж, Франция

Утверждено совещанием Комиссии ОСЖД
по инфраструктуре и подвижному составу
5-7 ноября 2019 г., Комитет ОСЖД, г. Варшава

Дата вступления в силу: 7 ноября 2019 г.

Примечание: Теряет силу I издание Памятки от 05.11.2004 г.

Р 843

ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ УСТРОЙСТВ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

СОДЕРЖАНИЕ

1. Область применения

1.1. Настоящая Памятка распространяется на программное обеспечение систем и устройств железнодорожной автоматики, выполненных на основе средств вычислительной техники, разрабатываемых и/или поставляемых для применения на железнодорожном транспорте стран – членов Организации сотрудничества железных дорог (ОСЖД), и к которым предъявляются требования по функциональной, информационной и кибербезопасности.

1.2. Настоящая Памятка может быть использована для разработки технических заданий на компоненты систем и устройств железнодорожной автоматики, выполненных на основе средств вычислительной техники. Может использоваться для целей сертификации.

1.3. Памятка определяет требования к перечню, содержанию, последовательности и документальному сопровождению работ по созданию безопасного программного обеспечения. Определяет состав участников работ и их взаимодействие. Конкретный состав участников работ определяется администрацией железных дорог стран-членов ОСЖД.

2. Термины, определения, сокращения

Программное обеспечение (ПО): Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Системное программное обеспечение: Программное обеспечение, которое обеспечивает функционирование и предоставляет сервисы для самого программируемого устройства, структура и состав которого не изменяются в зависимости от объекта внедрения микропроцессорной системы ЖАТ.

Примечание: Операционная система является системным программным обеспечением, которое не может быть модифицировано разработчиком ПО микропроцессорной системы ЖАТ, и в настоящей памятке не рассматривается.

Прикладное программное обеспечение: Часть программного обеспечения системы, которая не обеспечивает функционирование и не предоставляет сервисы для самого программируемого устройства.

Технологическое (прикладное) программное обеспечение: Программное обеспечение, структура и состав которого могут быть модифицированы в зависимости от объекта внедрения микропроцессорной системы ЖАТ.

Базовое (прикладное) программное обеспечение: Программное обеспечение, реализующее функции управления объектом автоматизации, структура и состав которого не изменяются в зависимости от объекта внедрения МПСУ.

Проектные файлы: совокупность исходных файлов прикладного программного обеспечения, адаптированного к проектируемому объекту, являющихся результатом работы инструментальных программных средств.

Безопасность ПО *(Safety of software)*: свойство с заданной вероятностью исключать переход системы в опасное состояние в результате ошибок ПО, искажения данных, отказов и сбоев аппаратных средств.

Экспертиза безопасности ПО *(Software safety verification)*: процесс, направленный на определение соответствия ПО требованиям безопасности.

Корректность ПО *(Software correctes)*: соответствие ПО, предъявляемой к нему системе требований, характеристик и правил.

Полнота ПО *(Software completeness)*: достаточность реализации ПО для обеспечения функциональных и системных требований.

Функциональные испытания ПО *(Operating test Software)*: испытания для проверки полноты и корректности решения функциональных задач при типовых условиях эксплуатации и исправных технических средствах.

Архитектура ПО *(Software architecture)*: концепция, определяющая структуру ПО, компоненты, отношения, в которых они находятся, и условия их реализации при заданных требованиях эффективности и безопасности.

Жизненный цикл ПО *(Software life-cycle)*: период существования ПО, исчисляемый от возникновения потребности в ПО до прекращения его эксплуатации.

Доказательство безопасности ПО (*Proof safety of the software)*: обоснование и подтверждение эффективности используемых организационных, программных и технических решений, направленных на достижение установленного в ТЗ уровня безопасности ПО.

Подтверждение корректности ПО *(Validation of software correct)*: процесс последовательной реализации комплекса проверок и испытаний ПО с целью получения гарантий его соответствия установленным в нормативной документации функциональным и системным требованиям.

Подтверждение безопасного функционирования *(Validation of safety operation)*: комплекс испытаний ПО, направленных на подтверждение безопасного функционирования ПО при возникновении заданного класса отказов технических средств и нормативных значениях внешних воздействий.

Информационная безопасность: Состояние защищенности информации, при котором обеспечиваются такие ее характеристики, как конфиденциальность, целостность и доступность.

Кибербезопасность: Действия, необходимые для предотвращения неавторизированного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов.

Киберзащищённость: Способность программно-управляемой системы (например, МПСУ) безопасно и эффективно осуществлять возложенные на нее функции в условиях несанкционированных, деструктивных воздействий различной физической природы.

Железнодорожная автоматика и телемеханика (ЖАТ): Технические средства автоматизации управления процессами железнодорожных перевозок,

обеспечивающие безопасность движения поездов и заданную пропускную способность, а также область науки и техники, связанная с их разработкой, производством и технической эксплуатацией.

Примечание: Основу железнодорожной автоматики и телемеханики составляют средства сигнализации, централизации и блокировки (СЦБ), обеспечивающие безопасное движение по железнодорожным путям при централизованном контроле и управлении путевыми объектами железнодорожных станций и перегонов.

Микропроцессорная система управления (МПСУ): Тип автоматизированных систем управления технологическими процессами и техническими средствами железнодорожного транспорта, функционирующими на основе принципов программно-управляемых устройств.

Контроль технического состояния: Процесс проверки соответствия значений параметров устройства установленным требованиям или нормам и определения на основе полученной информации текущего технического состояния объекта контроля.

Мониторинг технического состояния: Процесс непрерывного дистанционного контроля (телеконтроля) технического состояния объекта по определенному алгоритму с накоплением информации и оценкой полученной информации в течение времени с целью идентификации текущего состояния объекта.

3. Общие требования к ПО на этапах жизненного цикла

3.1. На стадии разработки требований к ПО должны быть определены функции, которые используют прикладные исходные данные.

3.2. На этапе разработки архитектуры ПО должны быть специфицированы интерфейсы между базовой и технологической частями прикладного ПО.

3.3. На этапе проектирования и разработки ПО должна быть обеспечена изолированность областей памяти, в которых хранятся базовая и технологическая части ПО, с целью независимой проверки и модификации.

3.4. На этапах проверки ПО должны быть рассмотрены все возможные комбинации исходных данных.

3.5. Документ «Доказательство безопасности системы» должен содержать раздел «Доказательство безопасности конфигурации (модификации) данных», в котором должны быть отражены результаты проверок, тестирования и подтверждения того, что подготовка данных выполнена корректно.

3.6. Каждое средство, используемое для проектирования, изготовления, исполнения и сопровождения ПО (операционная система, язык программирования, системы проектирования, трансляции, отладки и документирования) должно быть сертифицировано для применений, связанных с безопасностью.

В случае, когда на средство данного класса не требуется сертификат соответствия, все используемые для обеспечения безопасности возможности этого средства должны быть протестированы и документированы.

4. Требования к разработке ПО для обеспечения функциональной безопасности МПСУ ЖАТ

4.1. Требования к процессу разработки безопасного программного обеспечения

Процесс создания разработчиком безопасного ПО МПСУ ЖАТ, с целью обеспечения достижения требуемого уровня безопасности системы, включает следующие этапы работы:

- анализ и определение системных требований безопасности ПО МПСУ ЖАТ;

- выработка концепции обеспечения безопасности, разрабатываемого ПО МПСУ ЖАТ;

- проектирование архитектуры программно-аппаратных средств МПСУ ЖАТ;

- разработка требований безопасности к ПО;

- планирование мероприятий по обеспечению безопасности ПО, разработка программы обеспечения безопасности ПО (ПОБ ПО);

- проектирование, разработка и испытание ПО в соответствии с требованиями программы обеспечения безопасности и стадиями создания ПО;

- интеграция программных и аппаратных средств;

- испытания безопасности ПО в составе системы.

Указанные работы должны быть включены в выбранную разработчиком модель жизненного цикла ПО.

4.1.1. Анализ системных требований по безопасности программного обеспечения МПСУ ЖАТ

При анализе системных требований по безопасности ПО СЖАТ разработчик должен выполнить следующее:

- провести анализ основных эксплуатационных и системных характеристик, функций безопасности разрабатываемого ПО МПСУ ЖАТ

с учётом:

- возможности реализации требуемого уровня безопасности;

- возможности подтверждения заданного уровня безопасности;

- возможности обеспечения требуемого уровня безопасности при эксплуатации, обслуживании и сопровождении разрабатываемой системы ЖАТ;

- провести анализ требований руководящих и нормативно-технических документов по обеспечению безопасности функционирования ПО МПСУ ЖАТ на соответствие требованиям заказчика и нормативным требованиям безопасности (например, Памятки Р 807 «Количественные требования и средства обеспечения безопасности систем и устройств СЦБ»);

- определить качественные и количественные показатели безопасности разрабатываемого ПО МПСУ ЖАТ;

- определить перечень и описать критерии опасных отказов ПО МПСУ ЖАТ;

- создать модель угроз для ПО МПСУ ЖАТ в области информационной и кибербезопасности.

4.1.2. Определение концепции обеспечения безопасности разрабатываемого программного обеспечения МПСУ ЖАТ

Разработчик должен определить основные положения (стратегию), в соответствии с которыми будет осуществляться построение ПО МПСУ ЖАТ.

Опираясь на выбранную стратегию, должны быть сформулированы основные принципы обеспечения безопасности функционирования системы, а также её информационной безопасности и устойчивости к кибер-атакам.

4.1.3. Проектирование архитектуры программно-аппаратных средств МПСУ ЖАТ

В соответствии с идентификацией программных и аппаратных элементов системы должны быть определены функции безопасности, реализуемые программными и аппаратными средствами.

Должен быть проведен анализ интеграции функций безопасности программных и аппаратных средств. Должны быть определены уровень самопроверки ПО и уровень проверки программным обеспечением аппаратных средств в отношении заданного класса неисправностей и ошибочных входных воздействий.

4.1.4. Разработка требований безопасности к программному обеспечению

Разработчик должен разработать и документально оформить требования безопасности к ПО. Спецификации требований к ПО являются предметом верификации процесса разработки ПО.

Разработчиком должны быть предприняты все меры для возможности демонстрации их реализации на протяжении всех этапов жизненного цикла ПО.

В требованиях по безопасности ПО должны быть определены:

- организационное, методическое и программно-техническое обеспечение процесса проектирования и разработки ПО;

- функции ПО, связанные с безопасностью функционирования системы;

- требования к архитектуре ПО и ее элементам;

- средства ПО, которыми обеспечивается необходимый уровень безопасности;

- интерфейсы ПО с другими подсистемами, в том числе с человеком - оператором, критичные к вопросам безопасности;

- ограничения, связанные с методом конкретной реализации функций безопасности ПО.

Требования по безопасности должны быть взаимосвязаны и согласованы на протяжении всех этапов разработки и определять характеристики качества ПО в соответствии с ИСО/МЭК 9126.

Требования к системе должны быть сформулированы таким образом, чтобы обеспечивались:

- ясность и точность изложения, отсутствие двусмысленности;

- контролируемость;

- возможность реализации.

4.1.5. Планирование мероприятий по обеспечению безопасности ПО, разработка программы обеспечения безопасности ПО (ПОБ ПО) МПСУ ЖАТ

ПОБ ПО является частью общей ПОБ МПСУ ЖАТ.

В ПОБ ПО должны быть отражены:

- организационная структура выполнения проекта, полномочия и ответственность участвующих сторон;

- среда разработки (инструментальные средства разработки, оборудование, испытательные стенды, нормативные документы);

- работы по обеспечению и подтверждению безопасности разрабатываемого ПО;

- работы по экспертизе;

- форма отчетности результатов работы.

4.1.6. Проектирование, разработка и испытание ПО в соответствии с требованиями программы обеспечения безопасности и стадиями создания ПО

Проектирование архитектуры ПО производится на основе требований к структуре ПО и элементам ПО.

Разработчик должен выполнить проектирование и документирование внешних интерфейсов с программными компонентами и внутренних интерфейсов между модулями ПО. Если в состав МПСУ ЖАТ входит автоматизированное рабочее место, то разработчик должен представить заключение о соответствии экранных форм интерфейса человек-машина рекомендациям памятки Р-808 «Условные обозначения на устройствах отображения информации для компьютерных систем СЦБ».

Разработчик должен выполнить проектирование и документирование базы данных.

Компоновка структуры ПО, компонент ПО, интерфейсов и базы данных должна производиться на основе следующих критериев:

- соответствия системным требованиям;

- реализуемости;

- контролепригодности;

- сопровождаемости.

По результатам детального проектирования должны быть сформированы структурные единицы ПО, которые могут быть запрограммированы, откомпилированы и протестированы.

Разработчик должен составить и документально оформить требования по тестированию и программу испытаний для программных модулей и комплексному тестированию ПО.

Разработчик должен провести тестирование каждого программного модуля и базы данных. Результаты тестирования должны быть документально оформлены.

Интеграция программного ПО должна представлять собой процесс объединения предварительно протестированных программных модулей в единый комплекс. Разработчик должен подтвердить работоспособность и безопасность функционирования, интегрированного ПО на каждом шаге интеграции.

4.1.7. Интеграция программных и аппаратных средств

Программные компоненты и ПО в целом должны быть интегрированы с аппаратными средствами. Разработчиком должны быть протестированы интерфейсы программных и аппаратных средств.

Должна быть подтверждена эффективность программных и аппаратных средств контроля.

4.1.8. Испытания безопасности ПО в составе системы

Испытания системы на безопасность должны проводиться в соответствии с требованиями безопасности, разработчик должен подтвердить работоспособность и безопасность функционирования ПО в составе системы.

Испытания ПО в составе системы должны проводиться в соответствии с утвержденными для данной системы эксплуатационными и техническими требованиями.

5. Требования к разработке ПО для обеспечения информационной безопасности МПСУ ЖАТ

5.1. В состав требований к разработке ПО для управления доступом входят:

- требования по идентификации и аутентификации;

- требования по контролю доступа;

- требования по регистрации и учету;

- требования по обеспечению целостности.

5.1.1. Требования к функциям идентификации и аутентификации

5.1.1.1. Программное обеспечение должно осуществлять контроль за:

- идентификацией пользователей системы себя многоразовым паролем длиной не менее шести буквенно-цифровых символов, не содержащим персональные данные и иную информацию, позволяющую его определить;

- обновлением паролей с установленной периодичностью;

- для каждого пользователя должны быть установлены перечни объектов доступа и допустимых типов доступа, которые являются для него санкционированными. Изменение указанных прав разграничения доступа должен осуществлять администратор системы ЖАТ.

5.1.1.2. Объекты доступа (файлы, программы) должны иметь идентификационные метки.

5.1.1.3. В программном обеспечении системы ЖАТ должны быть предусмотрены настройки, осуществляющие блокирование доступа пользователя к несанкционированным для него объектам и типам доступа.

5.1.2. Требования к контролю доступа

5.1.2.1. Должны осуществляться идентификация и проверка подлинности пароля пользователя при входе в систему.

5.1.3. Требования по регистрации и учету

5.1.3.1. Должна осуществляться регистрация входа (выхода) пользователя в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.

5.1.3.2. В параметрах регистрации должны быть указаны: дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная). Регистрация выхода из системы не должна осуществляться в моменты отключения аппаратных средств ЖАТ.

5.1.4. Требования по обеспечению целостности

5.1.4.1. В базовом и технологическом программном обеспечении ЖАТ должны присутствовать настройки, исключающие возможность запуска нештатных компьютерных программ и блокирование подключения к системе нештатных носителей информации.

5.1.4.2. В базовом и технологическом программном обеспечении ЖАТ не должны присутствовать:

- средства разработки и отладки программ;

- средства модификации объектного кода программ в процессе обработки информации.

5.1.4.3. Должно быть обеспечено наличие средств восстановления программ,

предусматривающих ведение двух копий программных компонентов базового и технологического программного обеспечения, их периодическое обновление и контроль работоспособности.

5.1.4.4. Требования по обеспечению безопасного межсетевого взаимодействия предъявляются по назначению железнодорожной компании или соответствующего ее подразделения к системам ЖАТ, к которым по условиям их эксплуатации должен осуществляться удаленный доступ.

5.2. В состав требований к разработке ПО для обеспечения его киберзащищённости входят:

- Требования к электронным носителям информации;

- Требования по обнаружению вторжений;

- Требования к реагированию на инциденты нарушения информационной безопасности.

5.2.1. Требования к электронным носителям информации

5.2.1.1. Электронные носители, на которых записано базовое и технологическое программное обеспечение системы ЖАТ, должны быть защищены от возможности модификации информации.

5.2.1.2. Доступ к носителям информации должен предоставляться только уполномоченным на это лицам. Список лиц, имеющих доступ к носителям информации, должен быть минимальным. Доступ к носителям информации лиц, не включенных в этот список, должен быть исключен.

5.2.1.3. Должны быть определены процедуры защиты носителей информации от несанкционированного доступа.

5.2.1.4. Носители информации на объектах установки и эксплуатации систем ЖАТ должны быть зарегистрированы и учтены. Электронные носители должны иметь маркировку, обеспечивающую их однозначную идентификацию.

5.2.1.5. Должны быть идентифицированы места хранения носителей информации и их резервных копий. Места резервного хранения должны быть пространственно отделены от основных мест хранения. В местах резервного хранения должны быть обеспечены условия для своевременного восстановления носителей информации.

5.2.1.6. Должен осуществляться контроль за транспортировкой носителя информации, чтобы его могло получить только уполномоченное на это лицо.

5.2.1.7. При передаче электронного носителя информации для повторного использования за пределами объекта установки и эксплуатации системы ЖАТ должно быть выполнено его форматирование. Действия по форматированию должны контролироваться и документироваться.

5.2.1.8. Не используемые в дальнейшем носители информации подлежат уничтожению.

5.2.2. Требования по обнаружению вторжений

5.2.2.1. Данные требования предъявляются администрацией железных дорог или соответствующим ее подразделением к объектам установки и эксплуатации систем ЖАТ, к которым должен осуществляться удаленный доступ. При этом должны быть обеспечены возможности обнаружения информационных атак и оповещение об обнаруженной атаке.

5.2.2.2 Кроме этого, должны быть зафиксированы:

– информация о выявленных аномалиях сетевого трафика;

– тип обнаруженной атаки, дата и время обнаружения;

– сетевой адрес источника и объекта атаки;

– номер транспортного порта источника и объекта атаки;

– уровень приоритета выявленной атаки.

5.2.3. Требования к реагированию на инциденты нарушения информационной безопасности

5.2.3.1. Об инцидентах нарушения информационной безопасности необходимо немедленно информировать руководство железной дороги. На объекте установки и эксплуатации системы ЖАТ должны быть внедрены процедуры:

– информирования об инцидентах и реагирования на инциденты;

– обратной связи по результатам реагирования на инциденты;

– анализ ошибок – для уверенности в том, что они были устранены, и принятых корректирующих мер – для уверенности в том, что эти меры не были скомпрометированы и предпринятые действия надлежащим образом авторизованы.

5.2.3.2. Обработка инцидентов должна состоять из обнаружения, анализа, предотвращения развития, устранения инцидентов и восстановление работы системы ЖАТ после инцидентов. Инциденты нарушения информационной безопасности должны отслеживаться и документироваться на постоянной основе. Должны предоставляться отчеты об инцидентах в установленные адреса в соответствии с установленной формой, периодичностью и перечнем.

6. Требования к структуре программного обеспечения

В основе построения структурных компонент архитектуры ПО как на функциональном, так и на программном уровне должна быть заложена концепция модуля.

Концепция модуля на программном уровне разработки архитектуры ПО означает, что оно должно быть структурировано как в отношении исполняемых операторов, так и данных.

6.1. Модули взаимодействуют через строго определенный интерфейс и скрывают от других модулей детали реализации своих функций.

6.2. Модуль имеет один вход и один выход.

6.3. Текст каждого модуля должен быть понятным, а функция модуля должна быть ясна из его интерфейсной части.

6.4. Типы и диапазоны значений данных должны контролироваться как во время трансляции, так и во время исполнения программы.

6.5. Запрещается использование недокументированных возможностей, неочевидных свойств и побочных эффектов средств разработки и исполнения ПО.

7. Требования к надежности ПО

7.1. Спецификация требований к надежности программного обеспечения является основой для разработчика. Спецификация требований должна выражать требуемые свойства разрабатываемого программного обеспечения, но не процедуры его разработки. Она должна быть выражена и организована таким образом, чтобы быть полной, ясной, точной, недвусмысленной, поддающейся верификации, испытанию, пригодной для корректировки и выполнимой.

7.2. Спецификация требований к программному обеспечению должна включать в себя способы выражения и описания, которые являются понятными персоналу.

7.3. Требования к программному обеспечению должны устанавливать и документировать все интерфейсы с взаимодействующими системами. В спецификации требований должны быть описаны предусмотренные режимы работы программного обеспечения в системе ЖАТ, а также все режимы поведения программируемых электронных устройств, в частности, их поведение при отказах. Должны быть обозначены и документированы любые взаимные ограничения между программным и аппаратным обеспечением.

7.4. Спецификация требований должна показывать степень самопроверки программного обеспечения и заданную степень программной проверки аппаратных средств. Самопроверка программного обеспечения состоит в обнаружении и уведомлении программным обеспечением о его собственных отказах и ошибках.

7.5. Кроме качественных требований к надежности программного обеспечения должны быть предъявлены количественные требования. При этом следует исходить из того, что уровень надежности программного обеспечения не может быть равным или ниже уровня надежности системы ЖАТ.

7.6. Архитектура построения программного обеспечения системы ЖАТ должна удовлетворять заданным требованиям к надежности программного обеспечения. В ней необходимо идентифицировать и оценить значимость для надежности имеющиеся взаимодействия между программным и аппаратным обеспечением системы, а также проанализировать требования, возлагаемые архитектурой системы на ее программное обеспечение.

7.7. В программном обеспечении системы ЖАТ должна быть минимизирована его часть, наиболее влияющая на надежность системы. Когда имеется доказательство независимости между компонентами с разными уровнями надежности, то это доказательство должно быть записано в спецификации архитектуры программного обеспечения.

7.8. Спецификация архитектуры должна быть сформирована таким образом, чтобы выбранные технические приемы и меры удовлетворяли требованиям к программному обеспечению в соответствии с заданным уровнем его надежности.

8. Требования к вводу в эксплуатацию программного обеспечения МПСУ ЖАТ

8.1. К постоянной эксплуатации в составе МПСУ ЖАТ ПО допускается при наличии сертификата соответствия требованиям безопасности.

8.2. Разработчик должен выполнить установку ПО в том виде, в котором оно было представлено на сертификацию. Результаты установки должны быть документированы.

8.3. Разработчик должен показать, что установленное ПО функционирует в соответствии с требованиями на систему.

8.4. При вводе в постоянную эксплуатацию ПО, каждая установка которого должна отвечать специфическим требованиям, уникальным для объекта эксплуатации должны быть сертифицированы все изменения, влияющие на безопасность.

8.5. Все изменения, вносимые в ПО в результате корректировки, усовершенствования или адаптации к условиям эксплуатации, а также изменения условий функционирования ПО (в частности изменения операционной или аппаратной среды) должны быть согласованы с органом сертификации, издавшим сертификат безопасности на ПО.

8.6. В зависимости от влияния модификации ПО на безопасность функционирования системы орган сертификации, при необходимости, по согласованию с заказчиком ПО определяет объём повторных испытаний.

9. Требования к сопровождению программного обеспечения МПСУ ЖАТ

Виды сопровождения программного обеспечения МПСУ ЖАТ подразделяется на совершенствующее, профилактическое, адаптивное и корректирующее.

- Корректирующее сопровождение предназначено для исправления обнаруженных ошибок в базовом ПО МПСУ ЖАТ.

- Адаптивное сопровождение предусматривает изменение (модификацию) технологического ПО при изменении путевого развития, зависимостей, сигнальных показаний, технологии управления и т.п.

- Совершенствующее сопровождение применяется для улучшения эксплуатационных характеристик прикладного ПО, включения новых функций, дополнительной индикации, диагностики и т.п.

- Профилактическое сопровождение направлено на выявление в условиях эксплуатации скрытых дефектов, которые могут привести к нарушениям функционирования МПСУ ЖАТ.

Обязательными видами сопровождения ПО МПСУ ЖАТ являются корректирующее и адаптивное сопровождение.

9.1. Совершенствующее сопровождение программного обеспечения

В целях повышения эксплуатационных характеристик МПСУ ЖАТ, Организация, уполномоченная на сопровождение ПО системы, выполняет замену прикладного ПО по решению владельца инфраструктуры.

Организация проводит квалификационное тестирование модифицированного ПО с целью подтверждения правильности изменений и их согласованности с точки зрения полноты выполнения установленных требований, а также корректировку, при необходимости, программной документации.

До проведения квалификационного тестирования должны быть установлены и документально оформлены критерии проведения тестирования, оценки его результатов и измененных и неизмененных объектов (программных модулей, компонентов и элементов конфигурации) программного обеспечения. Если модификация ПО МПСУ ЖАТ проводится по требованию эксплуатирующей организации, указанные выше критерии должны быть согласованы с эксплуатирующей организацией.

Результаты тестирования оформляются актом, который утверждается руководителем Организации. Оригинал акта должен входить в комплект документов, который передается эксплуатирующей организации вместе с резервной копией модифицированного ПО.

Модифицированное ПО должно быть подвергнуто процедурам, которые подтверждают требования, предусмотренные п.4 данной Памятки, если оно предназначено для МПСУ ЖАТ, к которой в нормативных документах предъявляются требования по функциональной безопасности и область затронутой модификацией ПО относится к функциям безопасности системы.

Объем испытаний МПСУ ЖАТ, проводимых после установки модифицированной версии ПО, в каждом конкретном случае, определяется предприятием-разработчиком и согласовывается с эксплуатирующей организацией (если модификация ПО МПСУ ЖАТ проводится по требованию эксплуатирующей организации), исходя из характера и объема проведенной модификации.

Объём испытаний программного обеспечения по проверке зависимостей МПСУ ЖАТ, к которой предъявляются требования по функциональной безопасности и область затронутой модификацией ПО относится к функциям безопасности системы, определяется следующим образом:

- на предприятии-разработчике на аттестованном тестирующем комплексе проводится проверка зависимостей в полном объеме, а на станции в каждом конкретном случае, объём испытаний определяется предприятием-разработчиком и согласовывается с эксплуатирующей организацией владельца инфраструктуры;

- в случае отсутствия аттестованного тестирующего комплекса на предприятии-разработчике на объекте эксплуатации проводится проверка всех зависимостей;

- также может быть проведён на объекте эксплуатации минимально

необходимый объем проверок зависимостей, определенный предприятием-разработчиком, если он согласован с испытательным центром, аккредитованным на проверку функциональной безопасности МПСУ ЖАТ.

9.2. Профилактическое сопровождение ПО

Профилактическое сопровождение программного обеспечения МПСУ ЖАТ, если оно предусмотрено договором на сопровождение, выполняется по графику, который составляет Организация и согласовывает руководитель эксплуатирующей организации владельца инфраструктуры.

Работы по профилактическому сопровождению ПО МПСУ ЖАТ выполняются с разрешения оперативного персонала, пользующегося данной системой (ДНЦ, ДСП, инженер по мониторингу ЖАТ, маневровый диспетчер и т.п.) под контролем эксплуатационного персонала. Время, затрачиваемое эксплуатационным персоналом на контроль работ по профилактическому сопровождению ПО МПСУ ЖАТ, должно быть учтено в графиках технического обслуживания устройств СЦБ.

Если при проведении работ по профилактическому сопровождению выявлены дефекты ПО, Организация составляет план мероприятий по их устранению и согласовывает его с руководителем эксплуатирующей организации владельца инфраструктуры.

В том случае, когда для устранения выявленных дефектов необходимо модифицировать установленное в МПСУ ЖАТ программное обеспечение, должны быть выполнены требования пункта 9.3 настоящей Памятки.

9.3. Адаптивное сопровождение ПО

При планировании работ, связанных с изменением путевого развития, зависимостей, сигнальных показаний светофоров или технологии управления устройствами СЦБ эксплуатирующая организация владельца инфраструктуры направляет Организации запрос на модификацию программного обеспечения МПСУ ЖАТ с кратким описанием запланированных работ.

Организация на основании запроса на модификацию разрабатывает план мероприятий по модификации ПО МПСУ ЖАТ, запрашивает у эксплуатирующей организации – владельца инфраструктуры необходимую для разработки ПО информацию, согласовывает сроки подготовки модифицированного ПО.

При установке модифицированного ПО, разработанному в рамках адаптивного сопровождения на объекте эксплуатации, к нему предъявляются требования пункта 8 настоящей Памятки.

Установку модифицированного ПО на объекте эксплуатации осуществляют работники Организации или эксплуатирующей организации – владельца инфраструктуры железных дорог стран-членов ОСЖД.

9.4. Корректирующее сопровождение ПО

При обнаружении ошибки в программном обеспечении МПСУ ЖАТ, когда

процедуры, предусмотренные Инструкцией пользователя, не устраняют возникшую проблему, эксплуатирующая организация владельца инфраструктуры направляет Организации отчет о проблеме.

Отчет должен содержать описание ошибки, дату и время её обнаружения, действия оператора, в результате которых ошибка была выявлена, текст служебных сообщений системы или описание индикации (при их наличии), описание поездной ситуации. К отчету должен быть приложен архивный файл системного журнала.

Организация проводит работы по устранению ошибок в программном обеспечении. В том случае, когда для устранения выявленных ошибок необходимо модифицировать установленное в МПСУ ЖАТ программное обеспечение, должны быть выполнены требования пункта 8 настоящей Памятки.

10. Требования к документированию программного обеспечения

10.1. Общие требования к программной документации

Управление документированием должно осуществляться в соответствии с ИСО/МЭК ТО 9294.

Программная документация должна отражать структуру процесса разработки ПО по определенным этапам и действиям и регистрировать всю информацию, имеющую отношение к ПО, в течение его жизненного цикла.

Документация должна быть структурирована таким образом, чтобы обеспечивались развитие и пополнение документации в ходе процесса разработки ПО, а также простота поиска информации.

Программная документация должна иметь систему обозначения документов, т.е. каждый документ должен содержать:

- обозначение;

- данные;

- ссылки на документы, иерархически предшествующие данному.

10.2. Требования к качеству программных документов

Программные документы представляются на твердом или машинном носителях. Программы представляются на машинном носителе.

Информация, содержащаяся в документах, должна быть ясной, точной, полной и непротиворечивой.

Применяемые условные обозначения, сокращения, аббревиатуры, термины должны иметь общепринятое (однозначное) толкование либо поясняться и иметь одинаковое значение во всей документации.

10.3. Требования к перечню программных документов

В программную документацию должны входить:

- ведомость программных документов;

- документация разработки;

- эксплуатационная документация.

10.3.1. Документация разработки:

- техническое задание на разработку ПО;

- концепция обеспечения безопасности системы (включая информационную и кибербезопасность);

- описание архитектуры системы;

- спецификация ПО;

- описание программы;

- описание алгоритма;

- текст программы;

- документация по инструментальным и сервисным средствам разработки ПО;

- программа и методика испытаний на безопасность ПО, аппаратных средств и системы в целом;

- результаты испытаний (протоколы испытаний);

- доказательство безопасности ПО.

10.3.2. Эксплуатационная документация:

- руководство системного программиста;

- руководство программиста;

- руководство оператора;

- инструкция пользователя.

10.3.3. Требования к содержанию программных документов.

Ведомость программных документов содержит перечень, документов с указанием вида, формата (если документ содержится на машинном носителе) и объема каждого документа.

Техническое задание (ТЗ) должно содержать требования по безопасности. ТЗ на ПО может входить в состав общего ТЗ на систему.

Описание архитектуры системы должно отражать общую иерархическую структуру программно-аппаратных средств разрабатываемой системы с детализацией функций элементов структуры и связей между ними.

Спецификация описывает состав ПО, перечисляет реализуемые ПО функции, конкретизируя свойства этих функций в зависимости от требований, содержащихся в ТЗ.

Описание программы. В разделе "Описание логической структуры" должно быть приведено формальное описание архитектуры ПО, взаимодействие программных и аппаратных средств, соответствие программных процессов, объектов и параметров реальным.

Для этого может быть применено иерархическое дерево диаграмм потоков данных, детализированных до возможности описания внутренней логики процесса с использованием естественного языка и некоторых конструкций языка программирования высокого уровня (псевдо-кодов). В описании структуры нижних уровней иерархии процессы, не подлежащие дальнейшей детализации, должны соответствовать программным модулям разрабатываемого ПО.

Алгоритм программы должен быть представлен в формализованном структурном (при необходимости иерархическом) виде, например, в виде блок-схем алгоритмов (БСА), Р-схем алгоритмов, структурограмм, либо содержать иные сведения о логической структуре и функционировании ПО. В случае применения не стандартизованных систем записи алгоритмов должно быть приведено полное описание этих систем.

Текст программы содержит краткое описание функций программных модулей, структурированную запись программы на исходном языке, комментарии.

Текст программы должен быть понятным, что достигается, в частности, использованием осмысленных идентификаторов, минимизацией количества глобальных объектов, отказом от использования не именованных констант, подробными комментариями, описывающими смысловое назначение и диапазон значений глобальных (локальных) переменных и фактических (формальных) параметров подпрограмм, назначение и взаимосвязь подпрограмм, влияние подпрограмм на глобальные объекты.

Доказательство безопасности ПО (раздел документа «Доказательство безопасности системы») отражает принципы построения ПО, методы оценки и проверки, которым ПО подвергается для получения гарантии его соответствия требуемому уровню безопасности, а также результаты экспертизы, расчетов, испытаний и моделирования.

Последовательность создания программных документов приведена в таблице 10.1.

Таблица 10.1

Этап разработки	**Вид документа**
Анализ и определение системных требований безопасности МПСУ ЖАТ	Техническое задание
Определение концепции обеспечения безопасности, разрабатываемой МПСУ ЖАТ	Концепция обеспечения безопасности
Проектирование архитектуры МПСУ ЖАТ	Описание архитектуры системы
Определение функций безопасности, реализуемых программными и аппаратными средствами	Спецификация ПО
Анализ интеграции функций безопасности программных и аппаратных средств	Описание архитектуры системы
Разработка требований безопасности к ПО	Техническое задание
Планирование мероприятий по обеспечению безопасности ПО	Программа обеспечения ПО
Проектирование, разработка и испытание ПО в соответствии с требованиями программы обеспечения безопасности и стадиями создания ПО	ПО и протокол испытания
Проектирование архитектуры ПО, детальное проектирование ПО	Описание программы
Интеграция ПО	Текст программы
Интеграция программных и аппаратных средств	Протоколы испытаний ПО
Испытания безопасности ПО в составе системы	Протоколы испытаний ПО

11. Требования к проведению экспертизы и испытаниям ПО МПСУ ЖАТ

Экспертиза безопасности ПО должна проводиться параллельно с процессом разработки ПО, начиная с этапа ТЗ.

Экспертиза процесса разработки ПО должна выполняться организацией, независимой от разработчика и аттестованной на проведение данного вида деятельности.

Экспертиза процесса разработки ПО проводится на основе программы обеспечения безопасности ПО, которая включает в себя перечень видов деятельности и программной продукции, являющихся объектами экспертизы, а также формы отчетов, об испытаниях ПО, порядок взаимной ответственности сторон и график работ.

Основными целями экспертизы ПО на безопасность являются подтверждение полноты и корректности требований безопасности, предъявляемых к ПО, и сцепка соответствия их реализации на каждом этапе разработки ПО.

11.1. Экспертизе подлежат:

- Среда разработки ПО (инструментальные средства разработки, порядок разработки).

- Требования по безопасности:

полнота, корректность, реализуемость требований безопасности, согласованность системных (программных и аппаратных) требований безопасности.

- Программный проект:

соответствие проекта функциональным требованиям, соответствие проекта требованиям безопасности, соответствие проекта требованиям тестируемости, соответствие проекта требованиям интеграции с аппаратными средствами.

- Программы:

соответствие программ функциональным требованиям, используемые программные средства защиты, связанные с безопасностью функционирования.

- Документация:

соответствие, законченность и связность документации на ПО, полнота документации и её достаточность для сертификации, эксплуатации и сопровождения ПО.

11.2. Испытания ПО на безопасность направлены на экспериментальное подтверждение соответствия ПО требованиям безопасности.

11.2.1. Разработчиком ПО или испытательной лабораторией испытания на безопасность проводятся в соответствии с программой обеспечения безопасности. Программы и методики испытаний должны быть согласованы с заказчиком и организацией, осуществляющей экспертизу процесса разработки ПО.

11.2.2. Испытательная лаборатория проводит испытания ПО на

безопасность в объеме сертификационных испытаний.

11.2.3. Испытания на безопасность должны включать в себя:

- функциональные испытания;

- экспериментальное подтверждение полноты и корректности реализации функций безопасности системы программными средствами;

- подтверждение способности ПО обрабатывать искаженные данные вычислительного процесса в виде их обнаружения и соответствующей реакции, исключающей ошибку вычисления;

- подтверждение способности программ выполнять функции безопасности в условиях воздействия электромагнитных помех (Памятка Р 809 «Электромагнитная совместимость микроэлектронных устройств СЦБ») возникновения сбоев и отказов технических средств, искажения данных и ошибок оператора, ошибок программирования и при нормированных значениях внешних воздействий в соответствии с концепцией безопасности.

11.2.4. Инспекционный контроль программной продукции осуществляется органом сертификации с целью подтверждения, что:

- программная продукция соответствует проектной документации; изменения программ и среды функционирования (программной и аппаратной) согласованы с органом сертификации;

- диагностическое и техническое обслуживание ПО соответствуют требованиям безопасности и условиям эксплуатации.