ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70732— 2023

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Требования к функциональной и информационной безопасности программного обеспечения и методы контроля

Издание официальное

Москва
Российский институт стандартизации
2023

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Акционерным обществом «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2023 г. № 258-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 3
4 Общие положения 5
5 Требования к функциональной безопасности программного обеспечения 6
5.1 Общие требования 6
5.2 Уровни полноты безопасности программного обеспечения 6
6 Требования к информационной безопасности программного обеспечения 7
7 Порядок проведения и методы контроля 9
7.1 Порядок проведения и методы контроля соответствия требованиям функциональной безопасности 9
7.2 Порядок проведения и методы контроля соответствия требованиям информационной безопасности 9
Библиография 17

Введение

Настоящий стандарт разработан с целью повышения безопасности и бесперебойности функционирования автоматизированных систем управления технологическими процессами и техническими средствами железнодорожного транспорта за счет комплексного подхода к обеспечению и оценке функциональной и информационной безопасности их программного обеспечения. Такой подход способствует исключению или снижению вероятности возникновения различных видов ущерба от возможных транспортных происшествий, возникающих вследствие реализации угроз безопасности, связанных с функционированием программного обеспечения.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Требования к функциональной и информационной безопасности программного обеспечения и методы контроля

Automated control systems of technological processes and technical facilities for railway transport. Software functional and information safety requirements and control methods

Дата введения — 2023—11—01

1 Область применения

Настоящий стандарт распространяется на вновь разрабатываемое (модернизируемое) или приобретаемое у поставщика программное обеспечение (ПО) следующих автоматизированных систем управления технологическими процессами и техническими средствами железнодорожного транспорта (АСУ ЖТ) и их составных частей (устройств), которые выполняют функции контроля и управления технологическим оборудованием, техническими средствами (исполнительными устройствами) и технологическими процессами управления и обеспечения безопасности движения поездов:

- систем и устройств железнодорожной автоматики и телемеханики на железнодорожных станциях, сортировочных горках и железнодорожных переездах, перегонах железнодорожных линий, систем диспетчерской централизации и диспетчерского контроля движения поездов, в том числе автоматизированных систем оперативного управления технологическими процессами;
- систем и устройств железнодорожного электроснабжения;
- систем и устройств железнодорожной электросвязи.

Настоящий стандарт не распространяется на ПО систем, комплексов и устройств управления, контроля и безопасности, которыми оснащается железнодорожный подвижной состав. Соответствующие требования и методы контроля для ПО систем, комплексов и устройств управления, контроля и безопасности железнодорожного подвижного состава установлены в ГОСТ 33435, ГОСТ 34009 и ГОСТ 34673.3.

Настоящий стандарт устанавливает требования к функциональной и информационной безопасности ПО АСУ ЖТ, а также порядок и методы контроля соответствия этим требованиям.

Настоящий стандарт применяют:

- при формировании требований к функциональной и информационной безопасности ПО АСУ ЖТ, согласовании технических заданий, технических условий и заданий по безопасности на ПО АСУ ЖТ или на АСУ ЖТ в целом, проводимых на стадии разработки АСУ ЖТ и входящего в их состав ПО;
- организации оценки функциональной и информационной безопасности ПО АСУ ЖТ, выполняемой на всех стадиях жизненного цикла АСУ ЖТ и входящего в их состав ПО;
- заключении договоров на закупку (поставку) и при приемке ПО АСУ ЖТ и АСУ ЖТ в целом (с входящим в их состав ПО).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 33358 Безопасность функциональная. Системы управления и обеспечения безопасности движения поездов. Термины и определения

Издание официальное

ГОСТ 33433—2015 Безопасность функциональная. Управление рисками на железнодорожном транспорте

ГОСТ 33435 Устройства управления, контроля и безопасности железнодорожного подвижного состава. Требования безопасности и методы контроля

ГОСТ 33892—2016 Системы железнодорожной автоматики и телемеханики на сортировочных станциях. Требования безопасности и методы контроля

ГОСТ 33893—2016 Системы железнодорожной автоматики и телемеханики на железнодорожных переездах. Требования безопасности и методы контроля

ГОСТ 33894—2016 Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля

ГОСТ 33895—2016 Системы железнодорожной автоматики и телемеханики на перегонах железнодорожных линий. Требования безопасности и методы контроля

ГОСТ 33896—2016 Системы диспетчерской централизации и диспетчерского контроля движения поездов. Требования безопасности и методы контроля

ГОСТ 34009 Средства и системы управления железнодорожным тяговым подвижным составом. Требования к программному обеспечению

ГОСТ 34530 Транспорт железнодорожный. Основные понятия. Термины и определения

ГОСТ 34673.3 Тяговый подвижной состав железнодорожный. Часть 3. Методы контроля выполнения функций устройствами, обеспечивающими безопасность движения

ГОСТ IEC 61508-3—2018 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р 50739 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности

ГОСТ Р 58285—2018 Системы железнодорожной автоматики и телемеханики на высокоскоростных железнодорожных линиях. Системы интервального регулирования движения поездов. Требования безопасности и методы контроля

ГОСТ Р 58412 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения

ГОСТ Р 58489 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3-1. Требования к программному обеспечению. Повторное использование уже существующих элементов программного обеспечения для реализации всей или части функции безопасности

ГОСТ Р 58972 Оценка соответствия. Общие правила отбора образцов для испытаний продукции при подтверждении соответствия

ГОСТ Р ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности

ГОСТ Р МЭК 61508-5—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности

ГОСТ Р МЭК 62279—2016 Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения

(принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ 33358 и ГОСТ 34530, а также следующие термины с соответствующими определениями:

3.1 **автоматизированная система управления технологическими процессами и техническими средствами железнодорожного транспорта;** АСУ ЖТ: Система, состоящая из комплекса программных и технических средств и персонала, реализующая информационную технологию выполнения установленных функций контроля и управления технологическим оборудованием, техническими средствами (исполнительными устройствами) и технологическими процессами управления и обеспечения безопасности движения поездов.

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

3.3 **заказчик:** Организация, по заявке и договору с которой осуществляется разработка и/или поставка ПО как самостоятельного изделия или разработка и/или поставка автоматизированной системы управления, в состав которой входит ПО.

3.4 **защитный отказ:** Событие, при котором устройство, система переходит в защитное состояние.

3.5 **информационная безопасность ПО:** Состояние ПО, при котором оно не является источником угроз безопасности информации для взаимодействующих с ПО средств (систем) и обрабатываемых ими данных, и при котором обеспечивается целостность исполняемого кода ПО и целостность, доступность, конфиденциальность обрабатываемых (защищаемых) им данных.

3.6 **компьютерная атака:** Целенаправленное несанкционированное сетевое компьютерное воздействие (или их последовательность) на информационный ресурс, осуществляемое нарушителем с применением программных и/или программно-аппаратных средств и информационных технологий в целях реализации попыток нарушения и/или прекращения функционирования информационного ресурса или реализации угрозы безопасности информации, обрабатываемой таким ресурсом.

3.7 **мониторинг активности программы:** Получение сведений о взаимодействии программы со средой ее функционирования и другими программами, о взаимодействии между компонентами самой программы в процессе установки программы в среду функционирования, в процессе запуска, настройки и функционирования программы.

Примечание — Данный вид работ является методом испытаний ПО.

3.8

недекларированные возможности (программного обеспечения): Функциональные возможности программного обеспечения, не описанные в документации.

[ГОСТ Р 51275—2006, пункт 3.8]

3.9

несанкционированный доступ: Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа.

Примечания

1 Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.

2 Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

[ГОСТ Р 53114—2008, статья 3.3.6]

3.10

полнота безопасности (safety integrity): Вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного интервала времени.

[ГОСТ Р МЭК 61508-4—2012, статья 3.5.4]

3.11

программное обеспечение: Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

[ГОСТ 19781—90, статья 2]

Примечание — В общем случае ПО включает в себя микропрограммное, общесистемное и прикладное ПО.

3.12 **разработчик:** Организация, осуществляющая разработку программного обеспечения для реализации заказчику (потребителю).

3.13

статический анализ исходного кода программы: Вид работ по инструментальному исследованию программы, основанный на анализе исходного кода программы с использованием специализированных инструментальных средств (статических анализаторов) в режиме, не предусматривающем реального выполнения кода.

[ГОСТ Р 56939—2016, пункт 3.15]

Примечание — Данный вид работ является методом испытаний ПО.

3.14

тестирование на проникновение: Вид работ по выявлению (подтверждению) уязвимостей программы, основанный на моделировании (имитации) действий потенциального нарушителя.

[ГОСТ Р 56939—2016, пункт 3.16]

Примечание — Данный вид работ является методом испытаний ПО.

3.15

угроза (безопасности информации): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

[ГОСТ Р 50922—2006, статья 2.6.1]

3.16

уровень полноты безопасности; УПБ [safety integrity level (SIL)]: Дискретный уровень (принимающий одно из четырех возможных значений), соответствующий диапазону значений полноты безопасности, при котором уровень полноты безопасности, равный 4, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности.

[ГОСТ Р МЭК 61508-4—2012, статья 3.5.8]

Примечание — Уровень полноты безопасности АСУ ЖТ включает:

- значение (диапазон значений) количественного целевого показателя функциональной безопасности;
- комплекс мероприятий, осуществляемых для достижения полноты безопасности в отношении систематических отказов.

3.17

уровень полноты безопасности программного обеспечения (software safety integrity level): Стойкость к систематическим отказам элемента программного обеспечения, являющегося частью подсистемы или системы, связанной с безопасностью.

[ГОСТ Р МЭК 61508-4—2012, статья 3.5.10]

3.18

уязвимость: Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

[ГОСТ Р 56545—2015, пункт 3.3]

3.19

фаззинг-тестирование программы: Вид работ по исследованию программы, направленный на оценку ее свойств и основанный на передаче программе случайных или специально сформированных входных данных, отличных от данных, предусмотренных алгоритмом работы программы.

[ГОСТ Р 56939—2016, пункт 3.21]

Примечание — Данный вид работ является методом испытаний ПО.

3.20

функциональная безопасность: Свойство объекта железнодорожного транспорта, связанного с безопасностью, выполнять требуемые функции безопасности при всех предусмотренных условиях в течение заданного периода времени.

[ГОСТ 33432—2015, статья 3.1.29]

3.21

функциональное тестирование программы: Вид работ по исследованию программы, направленный на выявление отличий между ее реально существующими и требуемыми свойствами.

[ГОСТ Р 56939—2016, пункт 3.20]

Примечание — Данный вид работ является методом испытаний ПО.

3.22

экспертиза исходного кода программы: Вид работ по выявлению недостатков программы (потенциально уязвимых конструкций) в исходном коде программы, основанный на анализе исходного кода программы в режиме, не предусматривающем реального выполнения кода.

[ГОСТ Р 56939—2016, пункт 3.22]

Примечание — Данный вид работ является методом исследования ПО.

4 Общие положения

4.1 Высокая степень значимости безопасного и безотказного функционирования железнодорожного транспорта Российской Федерации и его зависимость от АСУ ЖТ требует отнесения АСУ ЖТ к объектам, подлежащим защите от угроз их функционированию (угроз выполнению функций безопасности по основному предназначению), в том числе от угроз безопасности информации как отдельного вида угроз для АСУ ЖТ, и комплексного подхода к обеспечению функциональной и информационной безопасности входящего в них ПО.

В соответствии с требованиями технических регламентов Таможенного союза [1], [2], ПО АСУ ЖТ должно обеспечивать безопасность функционирования АСУ ЖТ.

Функциональная безопасность ПО АСУ ЖТ должна обеспечиваться в соответствии с требованиями, установленными разделом 5 и ГОСТ Р МЭК 62279.

Информационная безопасность ПО АСУ ЖТ должна обеспечиваться в соответствии с требованиями нормативных правовых актов [3]—[8], разделом 6, уточняющим требования указанных нормативных правовых актов применительно к ПО АСУ ЖТ как части АСУ ЖТ, а также требованиями заказчика АСУ ЖТ в области обеспечения информационной безопасности.

4.2 Результаты оценки ПО АСУ ЖТ, полученные с использованием установленных в разделе 7 методов испытаний, предназначены для их предъявления:

- разработчиком заказчику в качестве подтверждения функциональной и информационной безопасности ПО АСУ ЖТ и АСУ ЖТ в целом для принятия заказчиком решения об их закупке (поставке) и приемке в эксплуатацию,

- заказчиком контролирующему уполномоченному федеральному органу исполнительной власти (далее — уполномоченный ФОИВ[1)]) для подтверждения выполнения требований нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации при эксплуатации АСУ ЖТ.

4.3 Необходимость проведения оценки соответствия требованиям по функциональной и информационной безопасности ПО конкретной АСУ ЖТ определяется ее заказчиком с учетом требований нормативных правовых актов [3]—[8], требований настоящего стандарта.

4.4 Требования к функциональной и информационной безопасности ПО конкретной АСУ ЖТ приводятся разработчиком в техническом задании (технических условиях, задании по безопасности) на ПО АСУ ЖТ или АСУ ЖТ в целом и согласовываются с заказчиком (при его наличии).

5 Требования к функциональной безопасности программного обеспечения

5.1 Общие требования

5.1.1 ПО АСУ ЖТ должно быть разработано, спроектировано и изготовлено таким образом, чтобы во всех предусмотренных проектной документацией на АСУ ЖТ условиях и режимах работы при соблюдении всех требований, установленных в эксплуатационной документации, обеспечивалась реализация всех функций безопасности в течение жизненного цикла ПО по ГОСТ Р МЭК 62279, ГОСТ Р 58489.

5.1.2 ПО АСУ ЖТ, как встраиваемое в аппаратные средства, так и поставляемое на носителях информации, должно:

- корректно выполнять все функции обеспечения безопасности движения поездов;
- быть тестируемым;
- сохранять работоспособность после перезагрузок, вызванных сбоями и отказами аппаратных средств и источников электропитания;
- контролировать целостность программ и данных;
- обеспечивать оперативный контроль возникновения отказов и ошибок ПО и аппаратных средств.

5.1.3 Программное обеспечение при обнаружении в нем отказа должно обеспечивать перевод АСУ ЖТ в защитное состояние, исключающее вероятность возникновения возможных транспортных происшествий, в том числе при использовании защитного отказа АСУ ЖТ.

5.1.4 ПО АСУ ЖТ должно обеспечивать восстановление работоспособного состояния АСУ ЖТ из состояния защитного отказа только с участием эксплуатационного персонала.

5.1.5 Требования по функциональной безопасности ПО АСУ ЖТ должны быть определены в соответствии с функциями АСУ ЖТ, для которой оно предназначено, и требованиями безопасности к выполнению данных функций. При этом требования безопасности должны учитывать возможность ошибочных или неквалифицированных действий оперативно-технического персонала в процессе эксплуатации и технического сопровождения АСУ ЖТ.

5.2 Уровни полноты безопасности программного обеспечения

5.2.1 Необходимый уровень полноты безопасности ПО должен быть определен для каждой функции безопасности, реализуемой в ПО АСУ ЖТ, на основе уровня риска, связанного с использованием ПО в АСУ ЖТ (см. ГОСТ Р МЭК 62279—2016, пункт 4.3), и уровнем полноты безопасности АСУ ЖТ в целом, исходя из критичности последствий, которые могут возникнуть вследствие отказа одной или нескольких функций безопасности и вероятности наступления данного события.

Определение уровня риска осуществляют в соответствии с ГОСТ Р МЭК 61508-5—2012 (пункты А.5—А.7 приложения А, приложения В—Е), ГОСТ 33433—2015 (разделы 5—8).

5.2.2 Требования к функциональной безопасности ПО АСУ ЖТ с функциями безопасности задают в его технической документации дифференцированно для каждой выполняемой им функции безопасности на основе анализа результатов соответствующих теоретических и/или экспериментальных исследований и использованных методов разработки и проектирования ПО.

[1)] Уполномоченный ФОИВ — федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации и технической защиты информации.

5.2.3 Значения показателей функциональной безопасности некоторых функций и качественные характеристики наступления опасных состояний для отдельных видов АСУ ЖТ приведены в ГОСТ 33892—2016 (подраздел 4.4), ГОСТ 33893—2016 (подразделы 4.3 и 4.4), ГОСТ 33894—2016 (подраздел 4.7), ГОСТ 33895—2016 (подразделы 4.4 и 4.5), ГОСТ 33896—2016 (подразделы 4.6 и 4.7), ГОСТ Р 58285—2018 (подраздел 4.2).

6 Требования к информационной безопасности программного обеспечения

6.1 Требования к информационной безопасности ПО АСУ ЖТ задают для обеспечения такого его состояния, при котором ПО АСУ ЖТ не содержит вредоносного кода вирусов, недекларированных возможностей и уязвимостей, создающих угрозу безопасному и безотказному функционированию АСУ ЖТ, и для обеспечения защищенности АСУ ЖТ (включая ПО АСУ ЖТ, обрабатываемые и хранимые данные) от несанкционированного доступа случайного и преднамеренного характера (в том числе от компьютерных атак), от последствий ошибок при хранении, вводе, выводе и обработке информации, от нарушений целостности ПО АСУ ЖТ при собственных сбоях и после перезагрузок, вызванных сбоями и отказами аппаратных средств АСУ ЖТ.

6.2 При задании требований по информационной безопасности в техническом задании (технических условиях, задании по безопасности по ГОСТ Р 57628) на ПО АСУ ЖТ или АСУ ЖТ в целом разработчик приводит согласованные с заказчиком (при его наличии) уровень доверия к информационной безопасности ПО АСУ ЖТ и функциональные требования по информационной безопасности ПО АСУ ЖТ.

6.3 Функциональные требования по информационной безопасности ПО АСУ ЖТ (состав и характеристики функций безопасности информации, подлежащих реализации в ПО АСУ ЖТ) задают на основе модели угроз безопасности информации на АСУ ЖТ с использованием ГОСТ Р ИСО/МЭК 15408-2, ГОСТ Р 50739, нормативных документов [5], [7], [9], [10] и нормативных документов заказчика (при их наличии).

Примечание — Под функциями безопасности информации понимают функции ПО АСУ ЖТ, реализующие меры по обеспечению безопасности (меры защиты информации) АСУ ЖТ, указанные в приложениях к нормативным документам [5], [7].

6.4 Уровень доверия к информационной безопасности ПО АСУ ЖТ задают в зависимости от установленной или предполагаемой категории значимости АСУ ЖТ как объекта (составной части объекта) критической информационной инфраструктуры (далее — категория значимости), определяемой в соответствии с Федеральным законом [3] и правилами [4], и/или в зависимости от установленного или предполагаемого класса защищенности АСУ ЖТ как автоматизированной системы управления (составной части автоматизированной системы управления) технологическими процессами критически важных, потенциально опасных, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды объектов (далее — класс защищенности), определяемого в соответствии с требованиями [5].

6.5 Для ПО АСУ ЖТ задают один из трех уровней доверия к информационной безопасности (по мере возрастания требований): низкий уровень — 6, средний уровень — 5, высокий уровень — 4. При этом:

- ПО АСУ ЖТ, соответствующее 6-му уровню доверия, может использоваться в АСУ ЖТ третьей категории значимости и/или третьего класса защищенности;
- ПО АСУ ЖТ, соответствующее 5-му уровню доверия, может использоваться в АСУ ЖТ второй и третьей категории значимости и/или второго и третьего класса защищенности;
- ПО АСУ ЖТ, соответствующее 4-му уровню доверия, может использоваться в АСУ ЖТ первой, второй и третьей категории значимости и/или первого, второго и третьего класса защищенности.

В случае если для АСУ ЖТ не были установлены категория значимости и класс защищенности, рекомендуется задавать уровень доверия к информационной безопасности ПО АСУ ЖТ не ниже 5.

6.6 Перечень требований, предъявляемых к ПО АСУ ЖТ в зависимости от заданного уровня доверия к информационной безопасности, приведен в таблице 1.

Примечание — Содержание требований приведено в [8]. Содержание требований, относящееся к аппаратным средствам, не применяется.

Таблица 1 — Перечень требований в зависимости от заданного уровня доверия к информационной безопасности ПО АСУ ЖТ

Наименование требования	Уровень доверия		
	4	5	6
1 Требования к разработке и производству			
1.1 Требования к разработке модели безопасности*	+	–	–
1.2 Требования к проектированию архитектуры безопасности	+	+	+
1.3 Требования к разработке функциональной спецификации	+	+	+
1.4 Требования к проектированию	+	+	+
1.5 Требования к разработке проектной (программной) документации	+	+	+
1.6 Требования к средствам разработки	+	+	+
1.7 Требования к управлению конфигурацией	+	+	+
1.8 Требования к разработке документации по безопасной разработке**	+	+	+
1.9 Требования к разработке эксплуатационной документации	+	+	+
2 Требования к проведению испытаний			
2.1 Требования к тестированию	+	+	+
2.2 Требования к испытаниям по выявлению уязвимостей и недекларированных возможностей	+	+	+
2.3 Требования к проведению анализа скрытых каналов***	+	–	–
3 Требования к поддержке безопасности			
3.1 Требования к устранению недостатков	+	+	+
3.2 Требования к обновлению	+	+	+
3.3 Требования к документированию процедур устранения недостатков и обновления	+	+	+
3.4 Требования к информированию об окончании производства и/или поддержки безопасности	+	+	+

* Требования предъявляют, если функция разграничения доступа и/или функция фильтрации информационных потоков является функцией по основному предназначению ПО.

** Разработку документации по безопасной разработке ПО осуществляют по ГОСТ Р 56939.

*** Требования предъявляют при обработке в ПО информации, требующей защиты ее конфиденциальности (например, паролей пользователей).

Примечание — Знак «+» указывает на предъявление требований при заданном уровне доверия, знак «–» означает, что требования при заданном уровне доверия не предъявляют.

6.7 Для достижения доверия заказчика к информационной безопасности ПО АСУ ЖТ и учета специфики железнодорожного транспорта заказчик вправе задать в техническом задании (технических условиях, задании по безопасности) требования, дополняющие (уточняющие) требования [8].

6.8 До проведения оценки информационной безопасности ПО АСУ ЖТ в соответствии с установленным в 7.2 порядком и методами испытаний разработчик должен применять меры по разработке безопасного ПО в соответствии с ГОСТ Р 56939 и ГОСТ Р 58412.

7 Порядок проведения и методы контроля

7.1 Порядок проведения и методы контроля соответствия требованиям функциональной безопасности

7.1.1 Контроль соответствия требованиям функциональной безопасности осуществляют на всех стадиях жизненного цикла ПО АСУ ЖТ в соответствии с ГОСТ Р МЭК 62279 и ГОСТ IEC 61508-3—2018 (раздел 8, приложения А и В).

7.1.2 Основными методами контроля являются:

- экспертиза проектной, технологической, программной, эксплуатационной документации;
- испытания ПО АСУ ЖТ для проверки реализации функций безопасности, выполняемых ПО;
- расчетные методы обоснования количественных показателей безопасности ПО АСУ ЖТ.

7.1.3 Реализацию функций безопасности проверяют путем моделирования отказов или другими методами в соответствии с ГОСТ IEC 61508-3, ГОСТ Р МЭК 62279—2016 (приложения А и D).

Проверяют условия возникновения опасных состояний и работоспособность функций безопасности, связанных с:

- обнаруженными программными ошибками и сбоями при периодическом тестировании;
- ошибками в получаемых данных вследствие сбоев и отказов интерфейсов;
- преднамеренным изменением или удалением данных в процессе их хранения или передачи;
- переполнением и потерей данных в памяти;
- недостаточной производительностью и временем отклика;
- ошибками диспетчеров.

7.1.4 Анализ реализации функций безопасности проводят при всех возможных условиях и режимах работы управляемых технических средств и выполнении технологических процессов, включая:

- подготовку к использованию АСУ ЖТ, а также установку и настройку ПО АСУ ЖТ;
- работу в режиме запуска ПО, в автоматическом, ручном, полуавтоматическом режиме (при наличии соответствующих режимов);
- повторный запуск, выключение;
- предполагаемые ненормальные условия функционирования.

7.1.5 На стадии жизненного цикла «Подтверждение соответствия ПО» (см. ГОСТ Р МЭК 62279) экспертизу предъявляемой документации на ПО и испытания ПО для подтверждения полноты и корректности реализации функций безопасности АСУ ЖТ, а также совместимости разрабатываемой АСУ ЖТ с другими взаимодействующими системами выполняет испытательная лаборатория (центр), аккредитованная(ый) на проведение работ по оценке соответствия ПО железнодорожного применения требованиям безопасности, при участии разработчика.

7.2 Порядок проведения и методы контроля соответствия требованиям информационной безопасности

7.2.1 Контроль соответствия ПО АСУ ЖТ требованиям информационной безопасности (оценка информационной безопасности) включает:

- проверку соответствия ПО АСУ ЖТ заданному уровню доверия к информационной безопасности;
- проверку соответствия ПО АСУ ЖТ функциональным требованиям по информационной безопасности, которую проводят при наличии в ПО АСУ ЖТ функций безопасности информации.

Примечание — В случае реализации в ПО АСУ ЖТ функций безопасности информации, которые отсутствуют в функциональных требованиях по информационной безопасности, установленных в техническом задании (технических условиях, задании по безопасности), эти функции должны быть описаны разработчиком в документации на ПО АСУ ЖТ (программной, эксплуатационной). Проверку таких функций проводят на соответствие документации ПО АСУ ЖТ, совместно с проверкой функций безопасности информации ПО АСУ ЖТ, заданных в функциональных требованиях по информационной безопасности;

- проверку производства (для ПО АСУ ЖТ, производимого серийно как программное изделие — ПО на носителях информации, предназначенное для поставки заказчику), с целью оценки достаточности условий производства для обеспечения у изготавливаемых образцов ПО АСУ ЖТ неизменности параметров и характеристик, подтвержденных при оценке информационной безопасности ПО АСУ ЖТ, и качества этих образцов.

Оценка информационной безопасности может быть проведена:

- для единичного образца ПО АСУ ЖТ. Оценка охватывает проведение испытаний и проверку организации технической поддержки образца ПО АСУ ЖТ;
- партии ПО АСУ ЖТ. Оценка охватывает проведение испытаний выборки образцов и проверку организации технической поддержки партии ПО АСУ ЖТ;
- серийного производства ПО АСУ ЖТ. Оценка охватывает проведение испытаний выборки образцов и проверку организации производства и технической поддержки ПО АСУ ЖТ;
- ПО АСУ ЖТ, поставляемого только в предустановленном виде (в аппаратных средствах АСУ ЖТ). Оценка охватывает проведение испытаний эталонного образца и проверку организации тиражирования и технической поддержки ПО АСУ ЖТ.

Примечание — Проверка организации тиражирования заключается в проверке наличия и оценке достаточности документированной процедуры, обеспечивающей неизменность подтвержденных по результатам испытаний параметров (характеристик) ПО АСУ ЖТ при его установке в аппаратные средства АСУ ЖТ. Для идентификации ПО АСУ ЖТ после его установки, в формуляре на ПО АСУ ЖТ должен указываться заводской (серийный) номер образца АСУ ЖТ, в аппаратные средства которого было установлено ПО АСУ ЖТ (обозначение и заводской (серийный) номер аппаратного средства из состава образца АСУ ЖТ).

7.2.2 Оценку информационной безопасности ПО АСУ ЖТ организуют на стадии жизненного цикла «Подтверждение соответствия ПО» (см. ГОСТ Р МЭК 62279), а также по истечении срока действия или при досрочном прекращении действия подтверждения о соответствии ПО АСУ ЖТ требованиям по информационной безопасности (см. 7.2.3, 7.2.7 настоящего стандарта) на стадии «сопровождение ПО» (см. ГОСТ Р МЭК 62279).

Оценку информационной безопасности ПО АСУ ЖТ проводят в форме испытаний, которые осуществляют компетентные[1)] испытательные лаборатории по программам и методикам, утвержденным (согласованным) компетентным органом по сертификации средств защиты информации на железнодорожном транспорте (ОС СЗИ)[2)].

Примечание — По требованию заказчика или в инициативном порядке информационная безопасность ПО АСУ ЖТ может подтверждаться в системе сертификации уполномоченного ФОИВ, действующей в соответствии с положением [11].

7.2.3 Результаты оценки информационной безопасности ПО АСУ ЖТ демонстрируют действующим сертификатом соответствия, оформленным ОС СЗИ, или заявлением о соответствии, зарегистрированным ОС СЗИ в ведущемся им реестре. Максимальный срок действия сертификата соответствия (заявления о соответствии) ПО АСУ ЖТ требованиям по информационной безопасности составляет пять лет.

Примечание — В случае подтверждения информационной безопасности ПО АСУ ЖТ в системе сертификации уполномоченного ФОИВ результаты проведенной оценки демонстрируют действующим сертификатом соответствия, оформленным ФОИВ.

7.2.4 Требования к проведению оценки информационной безопасности ПО АСУ ЖТ в форме испытаний установлены в 7.2.4.1—7.2.4.17.

7.2.4.1 Оценку информационной безопасности ПО АСУ ЖТ проводят в соответствии с программой и методикой испытаний, разрабатываемой компетентной испытательной лабораторией и утверждаемой (согласуемой) ОС СЗИ. Изменения в утвержденную (согласованную) программу и методику испытаний вносят по согласованию с ОС СЗИ.

Примечание — Программу и методику проверки производства (при серийном производстве ПО АСУ ЖТ) оформляют приложением к программе и методике испытаний.

7.2.4.2 Программа и методика испытаний ПО АСУ ЖТ должна отражать используемые методы испытаний (контроля).

[1)] Компетентность испытательных лабораторий и ОС СЗИ подтверждается уполномоченным ФОИВ.

[2)] ОС СЗИ обеспечивает учет отраслевой специфики при проведении оценки информационной безопасности ПО АСУ ЖТ.

Основными методами[1)] при оценке информационной безопасности ПО АСУ ЖТ являются:

- экспертный анализ (документации, информации из открытых источников, исходного кода, результатов исследований с применением других методов);
- статический анализ исходного кода программы;
- оценка соответствия исходного и исполняемого кода;
- фаззинг-тестирование программы;
- мониторинг активности программы;
- сканирование уязвимостей;
- тестирование на проникновение;
- антивирусный контроль;
- функциональное тестирование программы.

7.2.4.3 Экспертный анализ [документации, информации из открытых источников, исходного кода, результатов исследований с применением других (использованных) методов] представляет собой набор неинструментальных методов, используемых в том или ином сочетании при проведении всех исследований ПО АСУ ЖТ и объединенных по принципу их базирования (возможности использования) на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, проводящих испытания ПО АСУ ЖТ.

7.2.4.4 Статический анализ исходного кода программы предполагает исследование исходного кода ПО АСУ ЖТ с использованием специализированных инструментальных средств — статических анализаторов, а также последующий анализ результатов работы этих средств с использованием экспертизы исходного кода программы для определения истинности срабатываний статического анализатора и оценки степени опасности выявленных статическим анализатором ошибок и опасных конструкций кода.

Метод базируется на использовании статических анализаторов с современной базой выявляемых ошибок и опасных конструкций кода, максимально охватывающих языки программирования, на которых написаны исходные коды ПО АСУ ЖТ, а также на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.5 Оценка соответствия исходного и исполняемого кода предполагает проверку соответствия отобранных на испытания исходных кодов и дистрибутива ПО АСУ ЖТ и включает:

- фиксацию контрольных сумм исходных кодов и дистрибутива (в том числе объектных (загрузочных) модулей);
- проведение контрольных сборок объектных (загрузочных) модулей из зафиксированных исходных кодов;
- контроль соответствия собранных при контрольной сборке объектных (загрузочных) модулей зафиксированному дистрибутиву по контрольным суммам и/или методом экспертизы исходного кода программы;
- дополнительный контроль полноты и отсутствия избыточности исходных кодов ПО АСУ ЖТ с использованием методов экспертного анализа документации, исходного кода и инструментальных средств автоматизации анализа, используемых для выявления в ПО АСУ ЖТ недекларированных возможностей и уязвимостей.

Метод базируется на использовании доверенных средств расчета контрольных сумм, имеющих компетентное подтверждение корректности реализованных в них алгоритмов расчета, а также на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.6 Фаззинг-тестирование программы предполагает исследование исполняемого кода ПО АСУ ЖТ (модулей, осуществляющих обработку информации, поступающей через внешние интерфейсы ПО АСУ ЖТ, доступные не только администратору безопасности АСУ ЖТ) с применением специализированных инструментальных средств — фаззеров, подающих на соответствующие интерфейсы ПО АСУ ЖТ большое количество входных данных, формируемых путем мутаций специально подготовленных наборов образцов данных, и отслеживание возникновения при этом исключений и отклонений в работе ПО АСУ ЖТ (аварийных завершений, зависаний, нарушений поведения, не соответствующих документации), а также последующий анализ результатов, включая:

- определение охвата фаззингом кода программы;

[1)] При необходимости в дополнение к указанным основным методам могут быть использованы другие методы, предусмотренные в методике [12].

- фиксацию приводивших к исключениям (отклонениям) в работе программы наборов входных данных;

- определение уязвимого кода программы с использованием методов экспертного анализа [исходного кода и результатов исследований с применением других (использованных) методов].

Метод базируется на приоритетном использовании фаззеров, обеспечивающих обратную связь с исследуемым кодом, а также на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.7 Мониторинг активности программы предполагает отслеживание и фиксацию в процессе установки в среду функционирования, в процессе запуска, настройки и функционирования взаимодействий ПО АСУ ЖТ со средой его функционирования и с другим ПО АСУ ЖТ (при наличии другого ПО в составе АСУ ЖТ), с другими средствами и системами (при наличии в АСУ ЖТ возможности такого взаимодействия) с применением специализированных инструментальных средств (средств контроля обращений к файловой системе, средств контроля сетевого трафика и других средств), а также последующий анализ зафиксированных такими средствами взаимодействий для выявления недекларированных возможностей и уязвимостей ПО АСУ ЖТ с использованием методов экспертного анализа [документации, исходного кода, результатов исследований с применением других (использованных) методов].

Метод базируется на использовании инструментальных средств, обеспечивающих максимально возможное отслеживание и фиксацию взаимодействий ПО АСУ ЖТ, а также на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.8 Сканирование уязвимостей предполагает исследование ПО АСУ ЖТ и среды его функционирования на наличие известных уязвимостей с применением специализированных инструментальных средств — сканеров уязвимостей, а также последующий анализ результатов работы этих средств для выявления недекларированных возможностей и уязвимостей ПО АСУ ЖТ с использованием методов экспертного анализа [документации, информации из открытых источников, исходного кода, результатов исследований с применением других (использованных) методов].

Метод базируется на применении сканеров уязвимостей, использующих доступные зарубежные и национальные базы уязвимостей, а также на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.9 Тестирование на проникновение предполагает исследование ПО АСУ ЖТ в целевой среде функционирования, с учетом заданных в документации настроек и условий эксплуатации с использованием сценариев тестов, моделирующих (имитирующих) действия потенциального нарушителя, разработанных специалистами испытательной лаборатории и предназначенных для проверки актуальности (возможности эксплуатации) потенциальных уязвимостей ПО АСУ ЖТ (уязвимостей средств, подобных ПО АСУ ЖТ по архитектуре, в том числе уязвимостей других версий ПО АСУ ЖТ), идентифицированных по результатам проведенного анализа уязвимостей. При разработке сценариев тестов используют методы экспертного анализа [документации, информации из открытых источников, исходного кода, результатов исследований с применением других (использованных) методов]. В тестах на проникновение могут задействоваться инструментальные средства, в том числе специализированные тестовые платформы, применимые для реализации попыток эксплуатации исследуемых уязвимостей.

Метод базируется в основном на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.10 Антивирусный контроль предполагает исследование исполняемого кода ПО АСУ ЖТ и среды его функционирования для выявления в них вредоносного кода вирусов с использованием специализированных инструментальных средств — средств антивирусной защиты, а также анализ результатов работы этих средств (при невозможности их однозначной интерпретации) с использованием методов экспертного анализа [исходного кода, результатов исследований с применением других (использованных) методов].

Метод базируется на использовании средств антивирусной защиты с актуальными (предварительно обновленными) базами вирусных сигнатур, а также на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.11 Функциональное тестирование программы предполагает проведение тестирования функций безопасности информации ПО АСУ ЖТ в целевой среде функционирования, с учетом заданных в документации настроек и условий эксплуатации с применением разработанных специалистами испыта-

тельной лаборатории сценариев тестов, предусматривающих выполнение действий (в том числе с помощью имитаторов), которые должны приводить к срабатыванию механизма (алгоритма) проверяемой функции, а также последующий анализ и сопоставление полученных результатов тестирования с ожидаемыми результатами, которые должны свидетельствовать о реализации функции и ее соответствии заданным требованиям и описанию в документации.

Метод базируется на информации о ПО АСУ ЖТ, среде его функционирования и АСУ ЖТ в целом, полученной специалистами испытательной лаборатории при оценке соответствия ПО АСУ ЖТ заданному уровню доверия к информационной безопасности, а также на подтвержденной компетентности в области информационной безопасности испытательных лабораторий, использующих этот метод в ходе испытаний ПО АСУ ЖТ.

7.2.4.12 Соответствие требований по информационной безопасности ПО АСУ ЖТ и основных методов, применяемых для контроля соответствия ПО АСУ ЖТ этим требованиям, приведено в таблице 2.

Таблица 2 — Соответствие требований по информационной безопасности ПО АСУ ЖТ и основных методов, применяемых для контроля соответствия ПО АСУ ЖТ этим требованиям

Требование	Методы контроля (основные)
1 Функциональные требования по информационной безопасности ПО АСУ ЖТ	Экспертный анализ документации; экспертный анализ исходного кода; функциональное тестирование программы.
2 Требования доверия к информационной безопасности ПО АСУ ЖТ	
2.1 Требования к разработке и производству	
2.1.1 Требования к разработке модели безопасности	Экспертный анализ документации
2.1.2 Требования к проектированию архитектуры безопасности	Экспертный анализ документации
2.1.3 Требования к разработке функциональной спецификации	Экспертный анализ документации
2.1.4 Требования к проектированию	Экспертный анализ документации
2.1.5 Требования к разработке проектной (программной) документации	Экспертный анализ документации
2.1.6 Требования к средствам разработки	Экспертный анализ документации
2.1.7 Требования к управлению конфигурацией	Экспертный анализ документации
2.1.8 Требования к разработке документации по безопасной разработке	Экспертный анализ документации
2.1.9 Требования к разработке эксплуатационной документации	Экспертный анализ документации
2.2 Требования к проведению испытаний	
2.2.1 Требования к тестированию	Экспертный анализ документации
2.2.2 Требования к испытаниям по выявлению уязвимостей и недекларированных возможностей	Экспертный анализ документации; экспертный анализ информации из открытых источников; экспертный анализ исходного кода; экспертный анализ результатов исследований с применением других (использованных) методов; статический анализ исходного кода программы; оценка соответствия исходного и исполняемого кода; фаззинг-тестирование программы; мониторинг активности программы; сканирование уязвимостей; тестирование на проникновение; антивирусный контроль

Окончание таблицы 2

Требование	Методы контроля (основные)
2.2.3 Требования к проведению анализа скрытых каналов	Экспертный анализ документации; экспертный анализ исходного кода; экспертный анализ результатов исследований с применением других (использованных) методов; статический анализ исходного кода; сканирование уязвимостей; мониторинг активности программы; антивирусный контроль
2.3 Требования к поддержке безопасности	
2.3.1 Требования к устранению недостатков	Экспертный анализ документации
2.3.2 Требования к обновлению	Экспертный анализ документации
2.3.3 Требования к документированию процедур устранения недостатков и обновления	Экспертный анализ документации
2.3.4 Требования к информированию об окончании производства и/или поддержки безопасности	Экспертный анализ документации

7.2.4.13 Оценку информационной безопасности ПО АСУ ЖТ проводят на основании договоров, заключаемых с компетентной испытательной лабораторией и ОС СЗИ.

Примечания

1 В случае, если договоры заключаются не разработчиком ПО АСУ ЖТ, заключающая их организация должна иметь договорные отношения с разработчиком, обеспечивающие возможность проведения испытаний ПО АСУ ЖТ на материально-технической базе разработчика и обеспечивающие ПО АСУ ЖТ поддержкой безопасности со стороны разработчика в соответствии с предъявляемыми к этой поддержке требованиями в течение всего срока действия оформляемого ОС СЗИ сертификата соответствия (регистрируемого ОС СЗИ заявления о соответствии) ПО АСУ ЖТ требованиям по информационной безопасности.

2 В случае, если при серийном производстве договоры заключаются не производителем ПО АСУ ЖТ, заключающая договоры организация должна иметь договорные отношения с производителем, обеспечивающие возможность проведения проверки производства ПО АСУ ЖТ в течение всего срока действия оформляемого ОС СЗИ сертификата соответствия (регистрируемого ОС СЗИ заявления о соответствии) ПО АСУ ЖТ требованиям по информационной безопасности.

7.2.4.14 Для проведения оценки информационной безопасности ПО АСУ ЖТ должны быть представлены:

- образцы ПО АСУ ЖТ, отобранные для проведения испытаний;
- документация на ПО АСУ ЖТ (программная, эксплуатационная, технологическая), предусмотренная требованиями нормативных документов, программой и методикой испытаний и проверки производства (другие документы, необходимые для проведения оценки, представляются по запросу);
- эталонные исходные коды ПО АСУ ЖТ (на электронном носителе информации);
- программные и технические средства, необходимые для сборки объектных (загрузочных) модулей ПО АСУ ЖТ из исходных кодов и формирования дистрибутива ПО АСУ ЖТ, для установки ПО АСУ ЖТ в аппаратные средства АСУ ЖТ, а также документированные сведения о порядке выполнения этих операций.

Примечание — Документированные сведения о порядке (процедуре) установки ПО АСУ ЖТ в предназначенные для этого аппаратные средства АСУ ЖТ должны обеспечивать неизменность параметров и характеристик ПО АСУ ЖТ, подтвержденных по результатам оценки его информационной безопасности, после такой установки. Для идентификации ПО АСУ ЖТ после его установки, в формуляре на ПО АСУ ЖТ должен быть указан заводской (серийный) номер образца АСУ ЖТ, в аппаратные средства которого было установлено ПО АСУ ЖТ (обозначение и заводской (серийный) номер аппаратного средства из состава образца АСУ ЖТ);

- образец АСУ ЖТ или испытательный стенд, позволяющий проводить проверки ПО АСУ ЖТ в целевой среде функционирования в соответствии с программой и методикой испытаний.

В случае поставки ПО АСУ ЖТ в предустановленном виде должна быть обеспечена возможность доступа к файлам ПО АСУ ЖТ из аппаратных средств, в которые они были установлены.

7.2.4.15 Отбор образцов ПО АСУ ЖТ проводится представителями испытательной лаборатории в соответствии с ГОСТ Р 58972. Количество образцов ПО АСУ ЖТ, необходимых для проведения испытаний, устанавливается программой и методикой испытаний.

При оценке единичного экземпляра ПО АСУ ЖТ отбирается идентифицированный образец ПО АСУ ЖТ.

При оценке партии ПО АСУ ЖТ для отбора образцов должна быть представлена вся партия ПО АСУ ЖТ.

При оценке серийного производства ПО АСУ ЖТ для отбора образцов должна быть представлена партия ПО АСУ ЖТ, численность которой не менее чем в два раза превышает количество образцов, необходимых для проведения испытаний.

При оценке ПО АСУ ЖТ, поставляемого только в предустановленном виде (в аппаратных средствах АСУ ЖТ), отбирается тиражируемый эталонный образец ПО АСУ ЖТ, хранящийся в архиве разработчика (эталонное ПО на носителе информации, устанавливаемое в аппаратные средства АСУ ЖТ в соответствии с документированной процедурой, и поставляемая эталонная документация).

7.2.4.16 Испытания ПО АСУ ЖТ проводят на материально-технической базе испытательной лаборатории и материально-технической базе разработчика. При этом обеспечивается возможность присутствия при испытаниях представителя ОС СЗИ для контроля за проведением испытаний.

Примечание — При проведении оценки информационной безопасности ПО АСУ ЖТ на основании договоров, заключенных организацией, не являющейся разработчиком ПО АСУ ЖТ, отдельные проверки при испытаниях ПО АСУ ЖТ могут проводиться на материально-технической базе этой организации.

7.2.4.17 Материалы испытаний ПО АСУ ЖТ (отчетные документы испытательной лаборатории, документация на ПО АСУ ЖТ) представляют в ОС СЗИ для экспертизы. Состав материалов испытаний устанавливают в программах и методиках испытаний ПО АСУ ЖТ, в договоре с ОС СЗИ. По результатам экспертизы материалов испытаний ОС СЗИ оформляет экспертное заключение о соответствии или несоответствии ПО АСУ ЖТ требованиям по информационной безопасности и, в случае положительного заключения по результатам экспертизы, оформляет сертификат соответствия (регистрирует в реестре заявление о соответствии) ПО АСУ ЖТ требованиям по информационной безопасности.

7.2.5 При эксплуатации АСУ ЖТ периодически проводят контроль целостности ПО АСУ ЖТ (проверку соответствия версии, прошедшей оценку информационной безопасности, по составу и контрольным суммам модулей), контроль работоспособности реализованных в ПО АСУ ЖТ функций безопасности информации и контроль выполнения условий эксплуатации ПО АСУ ЖТ. Периодичность и порядок проведения контроля устанавливаются заказчиком, ответственным за эксплуатацию АСУ ЖТ, с учетом особенностей реализации и условий эксплуатации ПО АСУ ЖТ и АСУ ЖТ, указанных в эксплуатационной документации, и с учетом нормативных документов заказчика.

7.2.6 В случае внесения в ПО АСУ ЖТ изменений до истечения действия сертификата соответствия, оформленного ОС СЗИ (заявления о соответствии, зарегистрированного в реестре ОС СЗИ), организуют оценку информационной безопасности измененного ПО АСУ ЖТ. По согласованию с ОС СЗИ такая оценка может проводиться по ранее утвержденной (согласованной) программе и методике испытаний, в том числе по сокращенной программе.

7.2.7 Действие оформленного ОС СЗИ сертификата соответствия (зарегистрированного в реестре ОС СЗИ заявления о соответствии) ПО АСУ ЖТ требованиям по информационной безопасности приостанавливается или прекращается досрочно в следующих случаях:

- при изменении требований к информационной безопасности ПО АСУ ЖТ или АСУ ЖТ в целом, если несоответствие ПО АСУ ЖТ этим требованиям создает угрозу безопасной и/или безотказной эксплуатации АСУ ЖТ;
- при выявлении в ПО АСУ ЖТ недостатков, создающих угрозу безопасной и/или безотказной эксплуатации АСУ ЖТ, не устранимых в рамках поддержки безопасности ПО АСУ ЖТ разработчиком (о выявлении таких недостатков разработчик письменно извещает ОС СЗИ и заказчика, ответственного за эксплуатацию АСУ ЖТ);
- при невыполнении разработчиком требований по поддержке безопасности ПО АСУ ЖТ (по письменному обращению эксплуатирующей организации в ОС СЗИ);
- при досрочном прекращении разработчиком поддержки безопасности ПО АСУ ЖТ (по письменному извещению ОС СЗИ разработчиком);

- при выявлении нарушения производителем условий серийного производства ПО АСУ ЖТ, обеспечивающих неизменность параметров (характеристик) ПО АСУ ЖТ, подтвержденных при испытаниях (по результатам контрольной проверки, проведенной компетентной испытательной лабораторией или ОС СЗИ).

7.2.8 Информацию об оформленных ОС СЗИ сертификатах соответствия (о зарегистрированных в реестре ОС СЗИ заявлениях о соответствии) ПО АСУ ЖТ требованиям по информационной безопасности размещают на информационном ресурсе ОС СЗИ в сети Интернет. При истечении срока действия или досрочном прекращении действия сертификата соответствия (заявления о соответствии) информацию о нем удаляют с информационного ресурса ОС СЗИ.

Библиография

[1] Технический регламент Таможенного союза ТР ТС 002/2011 О безопасности высокоскоростного железнодорожного транспорта

[2] Технический регламент Таможенного союза ТР ТС 003/2011 О безопасности инфраструктуры железнодорожного транспорта

[3] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[4] Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

[5] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31)

[6] Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утверждены приказом ФСТЭК России от 21 декабря 2017 г. № 235)

[7] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239)

[8] Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76)

[9] Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

[10] Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.)

[11] Положение о системе сертификации средств защиты информации (утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55)

[12] Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении (утверждена приказом ФСТЭК России от 25 декабря 2020 г.)

УДК 656.25-52:656.2.08: 006.354 ОКС 45.020

Ключевые слова: автоматизированные системы управления, технологические процессы, технические средства железнодорожного транспорта, требования функциональной безопасности, требования информационной безопасности, программное обеспечение, методы контроля

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 24.04.2023. Подписано в печать 27.04.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru