

Пояснительная записка

к первой редакции проекта национального стандарта
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования»

1 Основание для разработки национального стандарта

Настоящий проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» разрабатывается в соответствии с Планом работы технического комитета по стандартизации «Защита информации» (ТК 362) на 2026 год.

2 Краткая характеристика объекта и аспекта стандартизации

Объектом стандартизации разрабатываемого проекта национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» являются технологии динамического анализа программного обеспечения, используемые в процессах разработки безопасного программного обеспечения согласно ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Аспектом стандартизации являются общие требования к содержанию работ по внедрению и регулярному выполнению процессов разработки безопасного программного обеспечения, в которых применяются технологии динамического анализа, требования к методам динамического анализа, инструментальным средствам и специалистам, задействованным в указанных процессах.

Основной целью внедрения технологий динамического анализа является повышение безопасности программного обеспечения путем его тестирования в режиме функционирования (исполнения кода), то есть в динамике.

Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» включает следующие разделы:

- область применения;
- нормативные ссылки;
- термины, определения и сокращения;
- общие положения;

- общие требования к внедрению технологий динамического анализа;
- общие требования к регулярному выполнению динамического анализа;
- описание и требования к технологиям динамического анализа;
- требования к инструментам динамического анализа;
- требования к специалистам;
- Приложение А (рекомендуемое) Применение технологий динамического анализа в процессах разработки безопасного программного обеспечения, определенных в ГОСТ Р 56939-2024, с учетом уровней тестирования;
- Приложение Б (справочное) Общая диаграмма процесса внедрения технологий динамического анализа
- Приложение В (справочное) Общая диаграмма процесса выполнения регулярного динамического анализа.

3 Обоснование целесообразности разработки стандарта на национальном уровне и ожидаемый эффект от его применения

Необходимость разработки проекта национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» обусловлена следующим.

Технологии динамического анализа позволяют выявлять недостатки программного обеспечения, которые могут привести к реализации угроз информационной безопасности, некорректному функционированию, ошибкам в поведении и отказам в обслуживании информационных систем, в составе которых функционирует программное обеспечение.

Технологии динамического анализа могут применяться при реализации таких процессов, предусмотренных ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», как динамический анализ и фаззинг-тестирование, функциональное тестирование, нефункциональное тестирование, поиск уязвимостей при эксплуатации.

Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» дополняет и уточняет требования к внедрению и регулярному выполнению процессов разработки безопасного программного обеспечения, в которых применяются технологии динамического анализа.

Применение национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического

анализа. Общие требования» позволит обеспечить соответствие программного обеспечения предъявляемым к нему требованиям, в том числе требованиям по безопасности, повысить надежность программного обеспечения, снизить риски реализации угроз безопасности и некорректного функционирования и, как следствие, повысить защищенность разрабатываемого программного обеспечения.

4 Сведения о соответствии проекта национального стандарта техническим регламентам Евразийского экономического союза, федеральным законам, техническим регламентам и иным нормативным правовым актам Российской Федерации

Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» разработан в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании», ГОСТ Р 1.2-2020 «Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления, внесения поправок и отмены», ГОСТ Р 1.5-2012 «Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения».

5 Сведения о соответствии проекта национального стандарта международному стандарту, региональному стандарту, региональному своду правил, стандарту иностранного государства и своду правил иностранного государства, иному документу по стандартизации иностранного государства и о форме применения данного стандарта (документа) как основы для разработки проекта национального стандарта Российской Федерации

При разработке проекта национального стандарта международные стандарты, региональные стандарты, региональные своды правил, стандарты иностранных государств и своды правил иностранных государств, иные документы по стандартизации иностранных государств в качестве основы не использовались.

6 Сведения о проведении научно-исследовательских работ, послуживших основой для разработки проекта национального стандарта

При разработке проекта национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического

анализа. Общие требования» научно-исследовательские и иные работы не выполнялись. Аналитическими работами, послужившими основой для разработки проекта национального стандарта, являются результаты деятельности в рамках сертификации процессов разработки безопасного программного обеспечения.

7 Сведения о наличии в Федеральном информационном фонде стандартов переводов международных, региональных стандартов, стандартов и сводов правил иностранных государств, на которые даны нормативные ссылки в стандарте, использованном в качестве основы для разработки проекта национального стандарта Российской Федерации

Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» не содержит нормативных ссылок на переводы международных, региональных стандартов, стандартов и сводов правил иностранных государств.

8 Сведения о взаимосвязи проекта национального стандарта с проектами или действующими в Российской Федерации другими национальными стандартами, сводами правил, а при необходимости также предложения по их пересмотру, изменению и составу

Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» дополняет и уточняет положения национального стандарта ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» в части требований к процессам разработки безопасного программного обеспечения, в рамках которых осуществляется тестирование программного обеспечения в режиме функционирования (исполнения кода).

Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Технологии динамического анализа. Общие требования» позиционируется как составная часть комплекса стандартов по разработке безопасного программного обеспечения.

Пересмотр, изменение или отмена действующих документов не требуется.

9 Перечень исходных документов и другие источники информации, использованные при разработке проекта стандарта, в том числе информацию об использовании документов, относящихся к объектам патентного или авторского права

При разработке проекта национального стандарта использовались следующие стандарты:

ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

ГОСТ 19781-90 «Обеспечение систем обработки информации программное. Термины и определения»;

ГОСТ Р 56920-2024 «Системная и программная инженерия. Тестирование программного обеспечения. Общие положения»;

ГОСТ Р 56921-2016/ISO/IEC/IEEE 29119-2:2013 «Системная и программная инженерия. Тестирование программного обеспечения. Часть 2. Процессы тестирования»;

ГОСТ Р 56922-2016/ISO/IEC/IEEE 29119-3:2013 «Системная и программная инженерия. Тестирование программного обеспечения. Часть 3. Документация тестирования»;

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

ГОСТ Р 71206-2024 «Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков C/C++. Общие требования»;

ГОСТ Р 58143-2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения»;

ГОСТ Р ИСО/МЭК 29119-4-2021 «Информационные технологии. Методы и средства обеспечения качества. Системы и программное обеспечение. Процессы тестирования. Часть 4. Проектирование тестов»;

ГОСТ Р 59453.1-2021 «Защита информации. Формальная модель управления доступом. Часть 1. Общие положения»;

ГОСТ Р 59453.3-2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке»;

ГОСТ Р 59453.4-2025 «Защита информации. Формальная модель управления

доступом. Часть 4. Рекомендации по верификации средства защиты информации, реализующего политики управления доступом, на основе формализованных описаний модели управления доступом».

При разработке проекта национального стандарта патенты не использовались.

10 Сведения о технических комитетах по стандартизации, в областях деятельности которых возможно пересечение с областью применения разрабатываемого проекта национального стандарта

Смежные технические комитеты отсутствуют.

11 Сведения о разработчике стандарта

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

Электронная почта: tk362@fstec.ru

Федеральное государственное бюджетное учреждение науки Институт системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН)

109004, г. Москва, ул. Александра Солженицына, дом 25.

Тел. 8-495-912-07-54

Электронная почта: petrenko@ispras.ru, esosnina@ispras.ru

Руководитель разработки:

Заведующий отделом
технологий программирования
ИСП РАН



Петренко А.К.

личная подпись