

Пояснительная записка

к первой редакции проекта национального стандарта
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения. Общие требования»

1 Основание для разработки национального стандарта

Настоящий проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения. Общие требования» разрабатывается в соответствии с Программой национальной стандартизации на 2025 год (шифр темы 1.11.362-1.012.21) и планом работы технического комитета по стандартизации «Защита информации» (ТК 362) на 2025 год.

2 Краткая характеристика объекта и аспекта стандартизации

Целями стандартизации является создание условий:

- для повышения безопасности государства;
- для внедрения передовых технологий в высокотехнологичных (инновационных) секторах экономики;
- для повышения уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества (за счет обеспечения безопасности обрабатываемой информации);
- для обеспечения конкурентоспособности, качества продукции и подтверждение соответствия продукции заявленным требованиям, в частности, по защите информации.

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

- область применения;

- нормативные ссылки;
 - термины и определения, обозначения и сокращения;
 - общие положения;
 - требования к порядку внедрения и применения композиционного анализа программного обеспечения (ПО);
 - требования к технологиям композиционного анализа ПО;
 - требования к инструменту композиционного анализа ПО;
 - требования к перечню программных компонентов;
- а также следующие приложения:
- приложение А (обязательное) Формат представления перечня программных компонентов;
 - приложение Б (обязательное) Состав данных описания модели машинного обучения.

Объектом стандартизации разрабатываемого проекта национального стандарта являются общие требования к содержанию и порядку выполнения работ, направленных на предотвращение появления либо нейтрализацию уязвимостей и недекларированных возможностей сторонних компонентов и выявление особенностей их использования в программном обеспечении, а также методология выполнения работ. Применение положений стандарта способствует решению задач улучшения оперативности выявления уязвимостей, и упростить внедрение специализированных процессов разработки безопасного ПО, позволит повысить эффективность мер по противодействию угрозам безопасности ПО, стандартизировать информационный обмен между участниками цепочки поставки ПО, в том числе за счет применения контролируемого репозитория и стандартизации формата перечня программных компонентов, содержащего в себе информацию о сторонних компонентах, а также моделях машинного обучения, используемых программным обеспечением. Решаемые задачи затрагивают все этапы жизненного цикла: анализ требований, проектирование, программирование и тестирование, эксплуатацию.

3 Технико-экономическое, социальное или иное обоснование целесообразности разработки стандарта на национальном уровне

Необходимость разработки проекта национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения. Общие требования» была вызвана следующим.

Безопасность информационных систем зависит от эффективности противодействия угрозам безопасности, в том числе обусловленным наличием уязвимостей программ, используемых в составе информационных систем. Для защиты от такого рода угроз, как правило, реализуют меры, направленные на предотвращение появления и устранение либо нейтрализацию уязвимостей программ в процессе жизненного цикла ПО.

Современные информационные системы, как правило, включают в себя широкий спектр типовых программ, которые в свою очередь в значительной степени состоят из программных компонентов с открытым исходным кодом, опубликованных под различными типами лицензий. Популярность компонентов стимулирует исследователей к выявлению в них различных уязвимостей, в том числе, с целью их дальнейшей эксплуатации. Централизованное автоматизированное оповещение пользователей и разработчиков информационных систем о наличии в составляющих их компонентах известных уязвимостей, а также, об особенностях использования этих компонентов, возможно с использованием инструментов композиционного анализа, взаимодействующих с банком данных угроз безопасности информации ФСТЭК России и иными публично доступными базами известных уязвимостей.

Настоящий стандарт устанавливает общие требования к содержанию и порядку выполнения работ, направленных на предотвращение появления, либо нейтрализацию уязвимостей сторонних компонентов и выявление особенностей их использования в ПО. Применение

настоящего национального стандарта позволит улучшить оперативность выявления уязвимостей, повысить эффективность принимаемых мер, стандартизировать отчетные материалы. Решаемые задачи затрагивают все этапы и процессы жизненного цикла ПО.

Настоящий стандарт предназначен:

- для организаций-разработчиков программного обеспечения, в том числе – разработчиков средств защиты информации, средств обеспечения безопасности информационных технологий;

- для организаций-разработчиков инструментальных средств, применяемых в процессах композиционного анализа ПО и обеспечения безопасности цепочки поставок;

- для организаций, выполняющих оценку соответствия процессов разработки безопасного ПО в части выполнения требований настоящего стандарта.

4 Сведения о соответствии проекта национального стандарта техническим регламентам Евразийского экономического союза, федеральным законам, техническим регламентам и иным нормативным правовым актам Российской Федерации, которые содержат требования к объекту и/или аспекту стандартизации

Проект национального стандарта разработан в соответствии с ГОСТ Р 1.2-2020 «Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления, внесения поправок, приостановки действия и отмены» и ГОСТ Р 1.5-2012 «Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила построения, изложения, оформления и обозначения».

Проект национального стандарта соответствует целям и принципам стандартизации, установленным Федеральным законом от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».

Проект национального стандарта соответствует законам Российской Федерации и не противоречит международным обязательствам.

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

Международные и региональные стандарты, а также иные документы по стандартизации иностранных государств использовались в качестве основы для разработки проекта национального стандарта, в частности:

- ISO/IEC 21778:2017 «Information technology – The JSON data interchange syntax» («Информационная технология. Синтаксис обмена данными в формате JSON»);

- RFC 4122 «A Universally Unique IDentifier (UUID) URN Namespace» («Пространство имен URN с Всемирным универсальным идентификатором (UUID)»);

- The Minimum Elements For a Software Bill of Materials (SBOM) Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity (Минимальные элементы для спецификации программного обеспечения (SBOM) в соответствии с исполнительным приказом 14028 об улучшении кибербезопасности страны).

6 Сведения о проведенных научно-исследовательских работах, технических предложениях, опытно-конструкторских, опытно-технологических и проектных работах, а также аналитических работах, послуживших основой для разработки первой редакции проекта национального стандарта

Для разработки проекта национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения. Общие требования» использовались результаты аналитических работ, проводимых в Федеральном государственном бюджетном учреждении науки «Институт системного программирования им. В.П. Иванникова Российской академии наук» (ФГБУН «ИСП РАН»), Обществе с ограниченной ответственностью

«Научно-технический центр «Фобос-НТ» (ООО «НТЦ «Фобос-НТ»), а также опыт Общества с ограниченной ответственностью «Профископ» (ООО «Профископ») в создании программных продуктов в области управления безопасностью программного обеспечения при использовании заимствованных и привлекаемых компонентов.

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 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 и межгосударственными стандартами, сводами правил, а при необходимости также предложения по их пересмотру, изменению или отмене

Проект национального стандарта применяется совместно с положениями ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Требования настоящего национального стандарта не противоречат требованиям других национальных стандартов Российской Федерации, а поэтому 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 национальные и международные документы по стандартизации:

- ГОСТ 19.101-77 «Единая система программной документации. Виды программ и программных документов»;
- ГОСТ Р 7.0.64-2018 (ИСО 8601:2004) «Система стандартов по информации, библиотечному и издательскому делу. Представление дат и времени. Общие требования»;
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»;
- ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие положения»;
- ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»;
- ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»;
- ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»;
- ISO/IEC 21778:2017 «Information technology – The JSON data interchange syntax» («Информационная технология. Синтаксис обмена данными в формате JSON»);
- RFC 4122 «A Universally Unique IDentifier (UUID) URN Namespace» («Пространство имен URN с Всемирным универсальным идентификатором (UUID)»);

- The Minimum Elements For a Software Bill of Materials (SBOM) Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity (Минимальные элементы для спецификации программного обеспечения (SBOM) в соответствии с исполнительным приказом 14028 об улучшении кибербезопасности страны).

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

Пересечение области применения разрабатываемого проекта национального стандарта с областями деятельности других технических комитетов по стандартизации не установлено.

11 Сведения о разработчике стандарта

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

Падарян Вартан Андроникович

Тел. 8-495-912-07-54

Электронная почта: tk362@ispras.ru

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

Общество с ограниченной ответственностью «Научно-технический центр «Фобос-НТ»

Пономарев Дмитрий Владимирович

Тел: 8-486-276-03-56

Электронная почта: info@fobos-nt.ru

302019, г. Орел, ул. Веселая, д. 1

Общество с ограниченной ответственностью «Профископ»

Смирнов Алексей Алексеевич

Тел. 8-800-301-93-54

Электронная почта: hello@codescoring.ru

196105, г. Санкт-Петербург, ул. Свеаборгская, д. 4, пом. № 9

Генеральный директор ООО «Профископ»



А. А. Смирнов