Нормативное правовое регулирование в области разработки безопасного программного обеспечения как фундамент качественной и эффективной разработки программного обеспечения

Заместитель начальника 2 управления ФСТЭК России

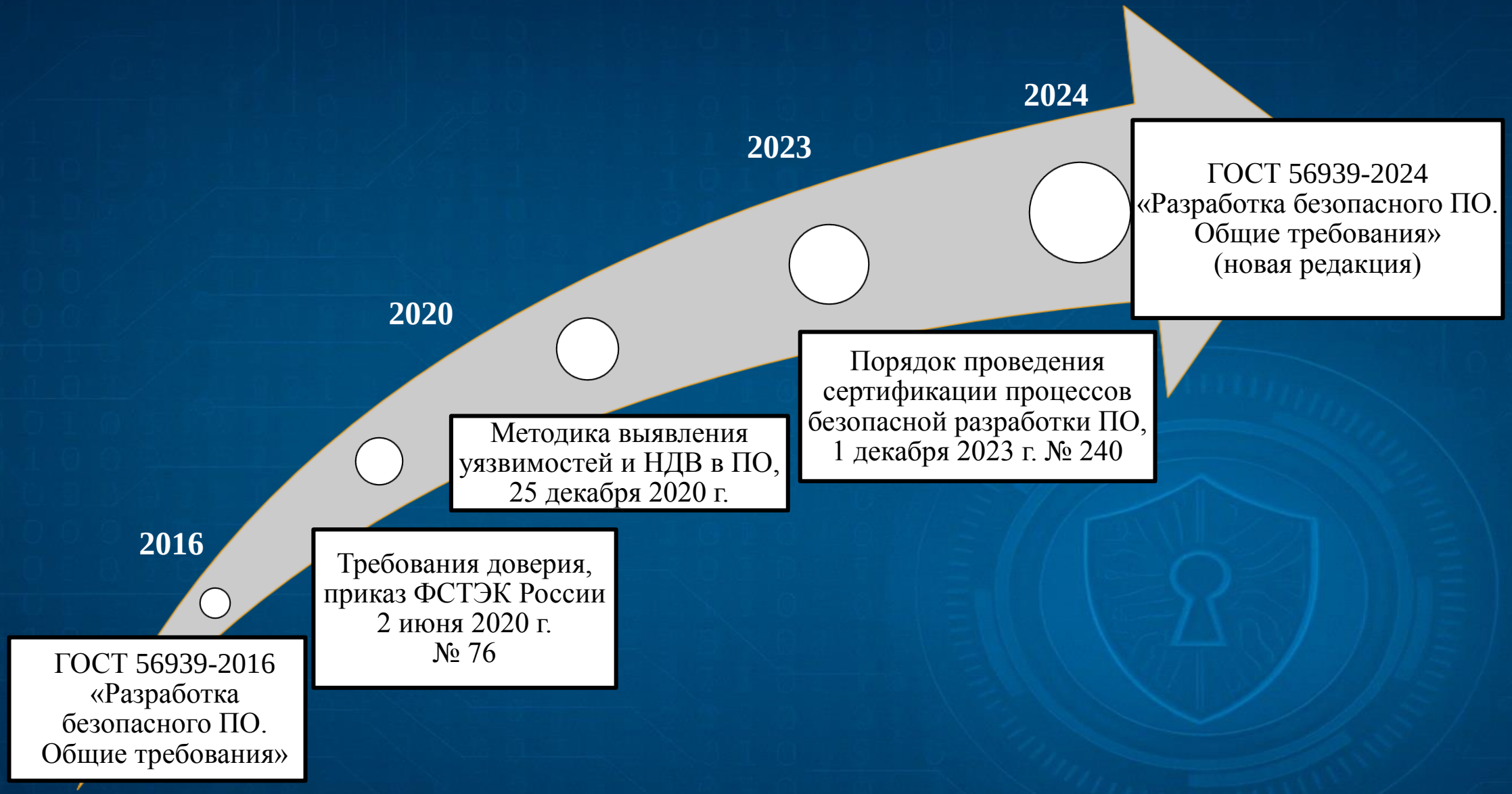
Гефнер Ирина Сергеевна

Направления совершенствования системы сертификации

РБПО

- Разработка требований по безопасности информации и стандартов
- Аттестация работников испытательных лабораторий и органов по сертификации
- Внедрение процессов разработки безопасного программного обеспечения
- Обеспечение функционирования Центра исследований безопасности системного программного обеспечения
- Сертификация процессов разработки безопасного программного обеспечения
- Создание унифицированной среды

Нормативное правовое регулирование в области РБПО



анализ архитектуры **статический анализ** **динамический анализ** **фаззинг-тестирование** **экспертиза кода**

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

Реализуемые меры по разработке безопасного программного обеспечения (ГОСТ Р 56939-2016)	Требования к процессам разработки безопасного программного обеспечения (ГОСТ Р 56939-2024)
было	**стало**
5.1 Меры по разработке безопасного программного обеспечения, реализуемые при выполнении анализа требований к программному обеспечению	5.2 Обучение сотрудников
5.2 Меры по разработке безопасного программного обеспечения, реализуемые при проектировании архитектуры	5.3 Формирование и предъявление требований безопасности к программному обеспечению
5.7 Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента документацией и конфигурацией программы	5.5 Управление недостатками и запросами на изменение программного обеспечения
• • •	• • •
5.9 Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента людскими ресурсами	5.25 Обеспечение безопасности при выводе программного обеспечения из эксплуатации

Подкомитет 2 «Разработка безопасного программного обеспечения» технического комитета 362 «Защита информации»

ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»
ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»
ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования»
ГОСТ Р 71206-2024 «Защита информации. Разработка безопасного программного обеспечения. Безопасный компилятор языков С/С++. Общие требования»
ГОСТ Р 72118-2025 «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Динамический анализ программного обеспечения»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения. Общие требования»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Методика оценки уровня внедрения процессов разработки безопасного программного обеспечения»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Термины и определения»

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

МЕТОДИКА ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

(новая редакция)

проект

при проведении исследований учитываются результаты реализации у разработчиков процессов разработки безопасного программного обеспечения в соответствии ГОСТ Р 56939

определен порядок использования результатов работы Центра исследований безопасности системного программного обеспечения для сертификации объекта оценки

введено требование о предоставлении исходного кода объекта оценки с 6 уровня контроля

уточнена методология определения поверхности атаки объекта оценки

введено требование о представлении информации о сторонних программных компонентах объекта оценки и проведении в их отношении композиционного анализа

уточнены требования к проведению анализа архитектуры, статического, динамического анализа и оформлению результатов

Сертификация процессов разработки безопасного ПО

Порядок сертификации процессов разработки безопасного программного обеспечения средств защиты информации

утвержден приказом ФСТЭК России от 1 декабря 2023 г. № 240

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

Цели:

Повышение безопасности программного обеспечения за счет:

- ❑ внедрения отечественными разработчиками процедур безопасной разработки;
- ❑ совершенствования качества разработки программного обеспечения;
- ❑ обеспечения качественной поддержки безопасности программного обеспечения.

Количество заявок на сертификацию: 12

Количество решений: 8

Количество сертификатов: 5

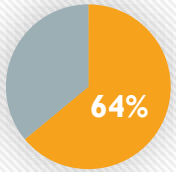
Средства защиты информации, в состав которых включены заимствованные программные компоненты с открытым исходным кодом

Порядок испытаний и поддержки безопасности средств защиты информации, в состав которых входят заимствованные программные компоненты с открытым исходным кодом

от 26 сентября 2024 г. № 240/24/4436

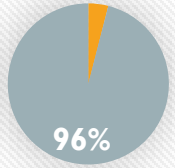
Выдано 23 плана испытаний на средства защиты информации

Сведения о SBOM



предоставили 133 организации

Направленные перечни



содержали недостатки

Аттестация работников органов по сертификации и испытательных лабораторий

Порядок аттестации работников органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа

утвержден приказом ФСТЭК России от 27 июля 2023 г. № 147

Аттестация экспертов проводится

В форме тестирования (100 вопросов по каждой области аккредитации)

В форме решения практических задач (2 задачи по каждой области аккредитации)

Время тестирования по каждой области – **90 минут**

Время решения практических задач по каждой области – **120 минут**

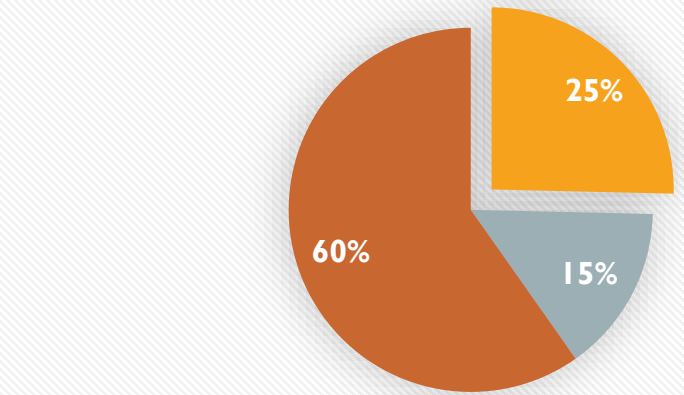
Статический анализ

Динамический анализ

Верификация результатов статического анализа

Анализ поверхности атаки программного обеспечения с открытым исходным кодом

Допущено 343 из 354 экспертов от 36 организаций



Аттестация экспертов осуществляется на материально-технической базе МГТУ им. Н.Э.Баумана

ЦЕНТР ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ
СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

599

патчей принято в основную ветку ядра Linux

ИСП РАН

Поддерживаемые Центром версии ядра Linux 5.10 и 6.1

24 поддерживаемых компонента

Размечено более 35 тысяч предупреждений, из которых 20 тысяч прошли независимую кросс-верификацию

Размечено более 20 тысяч предупреждений, из которых 3 тысяч прошли независимую кросс-верификацию

599 патчей разработано и принято

198 патчей разработано и принято

Создание унифицированной среды безопасной разработки отечественного ПО

Результаты (2022-2024 гг.)

Создана техническая инфраструктура Унифицированной среды

Разработан унифицированный набор инструментов для разработки безопасного отечественного ПО (среда интегрированной разработки, среда непрерывной интеграции и выпуска, безопасная компиляция, статический анализ исходного кода программ, фаззинг-тестирование программ, выявление утечек информации по памяти)

Разработана методология внедрения и обеспечения в организации-разработчике жизненного цикла безопасного ПО

Задачи (2025-2030 гг.)

Создание облачной платформы, предоставляющей средства разработки безопасного ПО как сервис

Расширение номенклатуры языков программирования, подлежащих анализу (C/C++, Java, Go, Python)

Развитие набора квалифицированных тестов для инструментов жизненного цикла безопасного ПО

Применение технологий ИИ в инструментах жизненного цикла безопасного ПО

Проведение испытаний средств статического анализа исходного кода

Пройдено	1 этап	Формирование перечня участников Формирование жюри Формирование критериев оценки Формирование площадки испытаний
Пройдено	2 этап	Согласование жюри комплектов тестов Запуск этапа «домашнее задание» Подведение предварительных итогов «домашнего задания»
01.08 – 01.11	3 этап	Подготовка площадки испытаний Запуск, проведение испытаний, разметка полученных результатов
01.11 – 01.12	4 этап	Оценка жюри результатов испытаний Опубликование результатов испытаний

ГОСТ Р 71207-2024

Полнота обнаружения критичных дефектов

Избыточность ложных обнаружений дефектов

Поддерживаемые методы анализа

Ресурсозатратность анализа

Отечественные разработчики ПО и экспертные организации, принявшие участие в испытании средств статического анализа

Ростелеком Солар, SBER TECH, АСТРА, positive technologies, PVS-Studio, Base ALT, ИСП РАН, KASPERSKY lab, Эшелон комплексная безопасность, SOLAR

Контактный телефон: +7 (499) 263 2775
Адрес эл. почты: znugis@fstec.ru

Нормативное правовое регулирование в области разработки безопасного программного обеспечения как фундамент качественной и эффективной разработки программного обеспечения

Заместитель начальника 2 управления ФСТЭК России

Гефнер Ирина Сергеевна