Опыт «Лаборатории Касперского» в стандартизации процессов разработки безопасного программного обеспечения

Certification Day 2024

Карина Нападовская

Руководитель центра сертификации и соответствия стандартам

kaspersky

Структурное подразделение в составе Лаборатории Касперского

Сертификация

- Сертификация в ФСТЭК России, ФСБ России, Минобороны России
- Подготовка к проведению аудитов в «Лаборатории Касперского» и их сопровождение
- Сертификация в Республике Казахстан, Республике Беларусь и др.
- Сертификация соответствия СМК «Лаборатории Касперского» ISO 9001
- Вендорские сертификации
- Сертификация соответствия международным стандартам ISO / EIC 15408, IEC 62443 ISO 26262 и др.

Центр сертификации и соответствия стандартам

Стандартизация

Участие в разработке методик, требований, проектов ГОСТ

Участие в работе технических комитетов и рабочих групп

Развитие бизнес-процессов

Опыт Лаборатории Касперского в процессах стандартизации

Лаборатория Касперского является постоянным членом ТК 362

Разработка проектов стандартов по разработке безопасного ПО

Разработка проектов стандартов по конструктивной безопасности

Участие в разработке стандартов по защите информации в рамках ТК 362 — разработка отзывов и предложений в проекты документов

Разработка безопасного ПО: предпосылки

Предпосылки

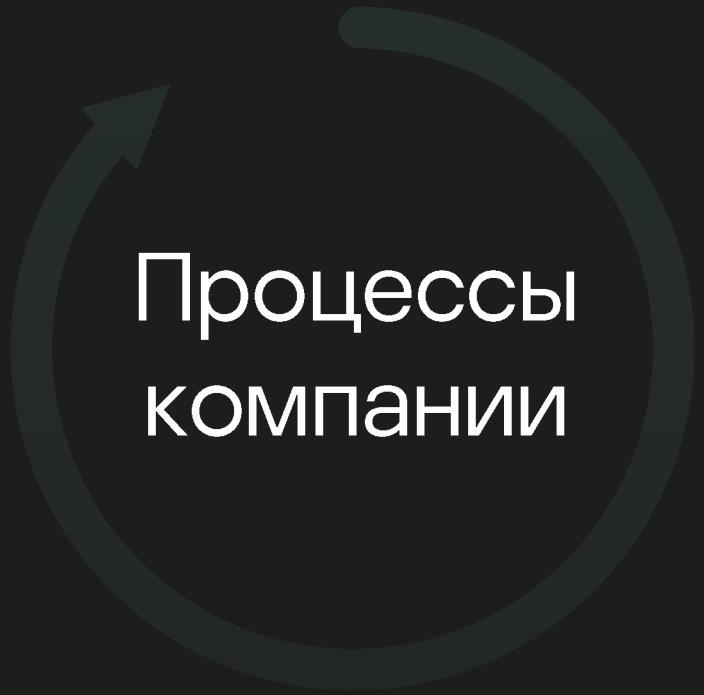
Необходимость для средств защиты была всегда, мы изначально думали о безопасности наших продуктов

Требования регулятора (ПЗ по ГОСТ Р ИСО / МЭК 15408, Требования доверия, Методика ВУ и НДВ)

Выявление и устранение уязвимостей в продуктах

Учет международных и зарубежных требований и практик

Появление стандарта ГОСТ Р 56939-2016


Процессы
компании

Проблемные вопросы

Что сделали?

1

Изучили международный опыт:

- Microsoft SDLC
- OWASP
- др...

2

Изучили ГОСТ Р 56939-2016

3

Разработали собственные методики:

- Реализации процессов / практик
- Применения инструментов для разработки безопасного ПО

4

Провели аудит с привлечением экспертных организаций

5

Решили проводить ежегодный Certification Day для обмена опытом с сообществом

Почему ГОСТ Р 56939-2016 нуждался в пересмотре

1

Действующая редакция стандарта на момент утверждения была своевременной, однако предполагала добросовестность организаций, внедряющих разработку безопасного ПО, и компетентность соответствующих экспертов

Почему ГОСТ Р 56939-2016 нуждался в пересмотре

2

Описание мер не имело достаточной конкретизации, позволяющей дать однозначный ответ при оценке о реализации конкретной меры, качестве ее реализации

3

Меры не содержали требований к составу и содержанию свидетельств разработчика

Почему ГОСТ Р 56939-2016 нуждался в пересмотре

4

С момента выхода стандарта существенно вырос запрос на безопасность ПО, требующий дальнейшей детализации мер по безопасной разработке ПО и расширения охватываемых аспектов безопасности

Что получили?

Набор требований, рекомендаций и методик для разных процессов собственной разработки

Опыт внедрения процессов в разных командах разработки

Понимание «слабых мест», нуждающихся в улучшении

Результаты аудитов внедрения процессов РБПО разных команд (как внутренними аудиторами, так и экспертными организациями, в т.ч. «Фобос-НТ»)

Материалы, готовые к оформлению в виде документа, регламентирующего процессы разработки безопасного ПО

Предложенный подход Лаборатории Касперского

Задание требований
не к мерам, а к процессам

Учет собственного опыта
разработки, практик
и инструментов

Учет положений:

- предыдущей редакции ГОСТ
- мер из Требований доверия
- мер из Методики ВУ и НДВ
- других ГОСТ по безопасной разработке (статика, динамика, композиционный анализ)

5.X Процесс разработки безопасного ПО

5.X.1 Цели

5.X.1.1 Повышение качества... при ...

5.X.2 Требования к реализации

5.X.2.1 Определить требования безопасности при...

5.X.3 Артефакты реализации требований

5.X.3.1 Требования безопасности должны содержать: ...

5.X Процесс разработки безопасного ПО

5.X.1 Цели

5.X.1.1 Повышение качества... при ...

5.X.2 Требования к реализации

5.X.2.1 Определить требования безопасности при...

5.X.3 Состав и содержание документированных свидетельств

5.X.3.1 Требования безопасности должны содержать: ...

5.X.4 Критерии принятия решения о реализации процесса

5.X.4.1 Определены требования безопасности...

Этапы разработки новой редакции ГОСТ Р 56939

Декабрь 2023 – январь 2024	Общественное обсуждение
Январь 2024 – апрель 2024	Доработка проекта по результатам общественного обсуждения
Апрель 2024	Представление в ПК 4 ТК 362, заседание ПК 4, представление на голосование
Январь 2023	Представление проекта документа в ФСТЭК России
Июль 2023	Представление первой редакции на обсуждение в составе ПК 4 ТК 362
Август 2023 – ноябрь 2023	Доработка проекта в составе рабочей группы (10 организаций)
Ноябрь 2023	Представление на обсуждение в ПК 4 ТК 362
Ноябрь 2022	Предложение разработать новую редакцию ГОСТ Р 56939

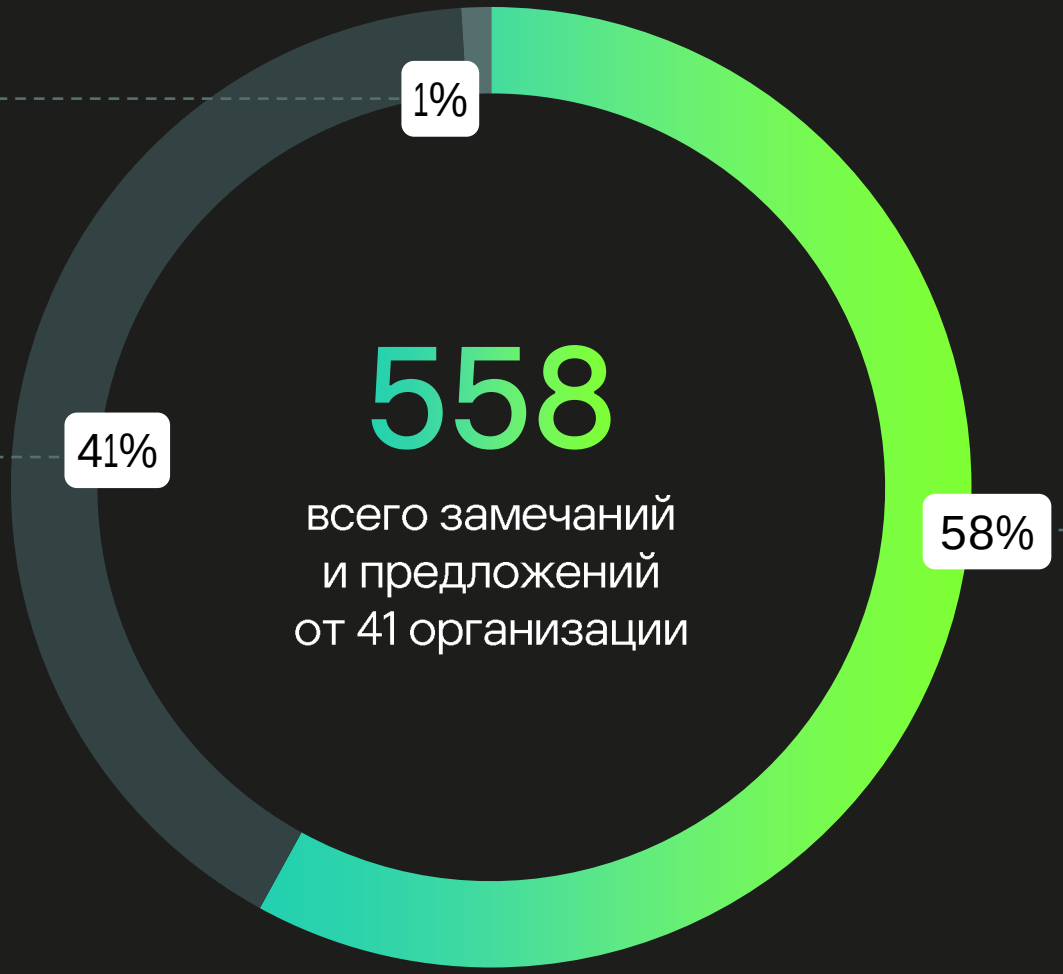
Состав рабочей группы

Обработка замечаний и предложений по результатам общественного обсуждения

7
Отсутствует замечание / предложение

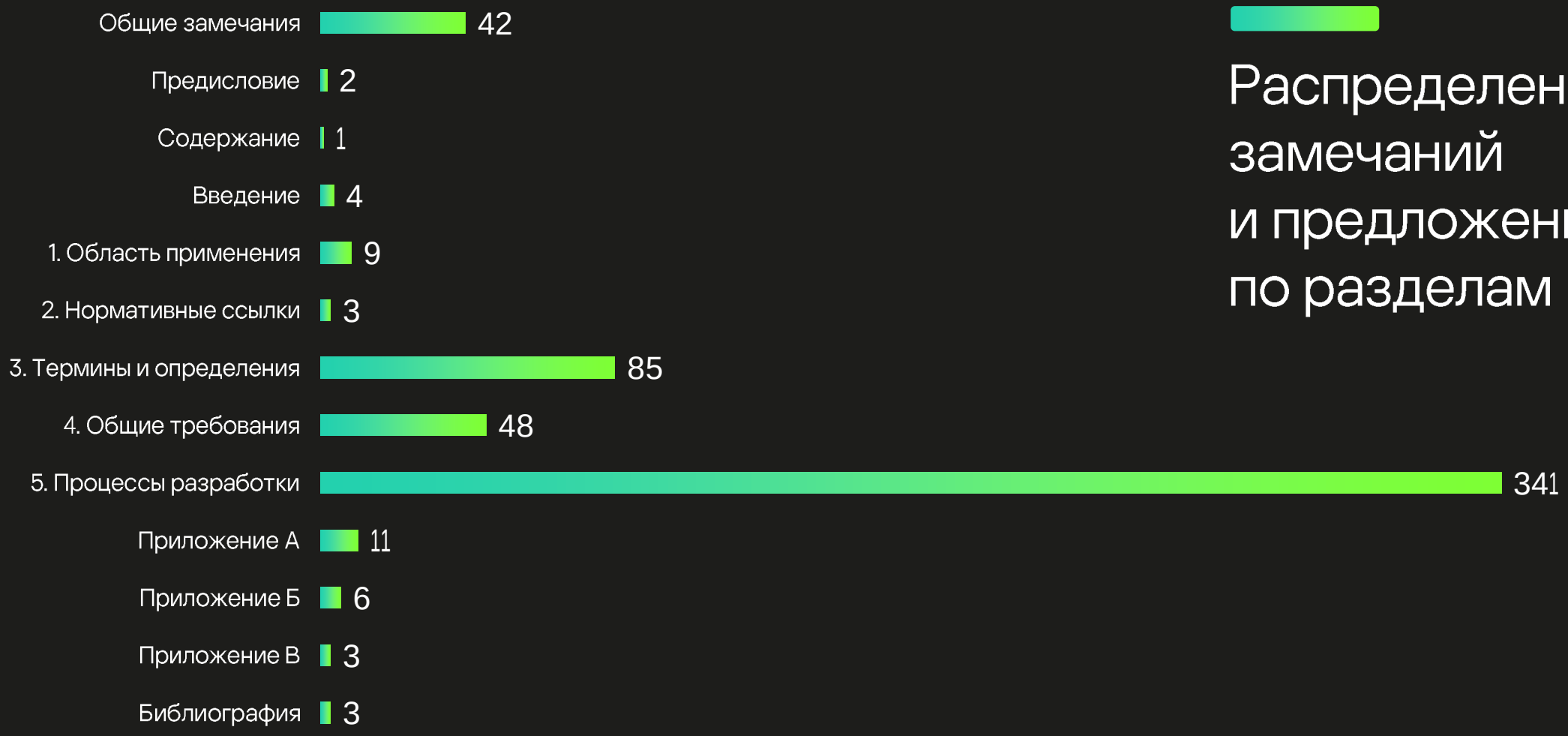
231
Не принято

10
организаций без замечаний и предложений



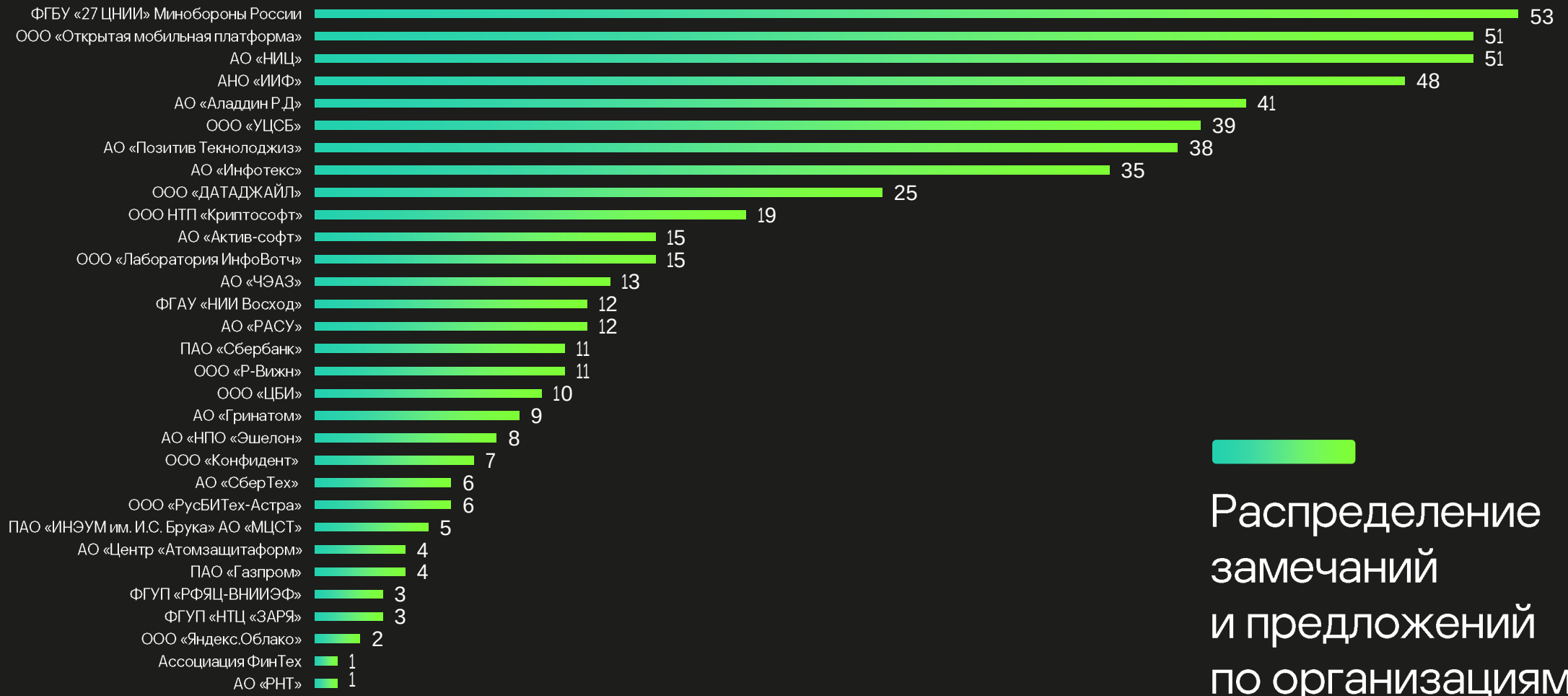
320
Принято

Распределение замечаний и предложений по разделам



Распределение замечаний и предложений по разделам

Распределение замечаний и предложений по организациям



Распределение замечаний и предложений по организациям

Наиболее часто встречающиеся замечания и предложения

Оформление (в соответствии с ГОСТ Р 1.5), опечатки	Термины и определения	Привязка к процессам жизненного цикла ПО
«Регламент», «свидетельство», «план», «документация» и др.	Учет стандартов (ГОСТ, ISO), других документов	РБПО / БРПО
«Может», «следует», «рекомендуется» (ГОСТ Р 1.5)		Учет НПА ФСТЭК России

Наиболее часто встречающиеся замечания и предложения

Принято	Принято частично	Не принято
Оформление (в соответствии с ГОСТ Р 1.5), опечатки	Термины и определения	Привязка к процессам жизненного цикла ПО
«Регламент», «свидетельство», «план», «документация» и др.	Учет стандартов (ГОСТ, ISO), других документов	РБПО / БРПО
«Может», «следует», «рекомендуется» (ГОСТ Р 1.5)		Учет НПА ФСТЭК России

Голосование по вопросу представления проекта стандарта на утверждение

35
«За»

0
«Против»

2
Воздержались

Голосование состоялось
10 июня 2024 г.

Пройден успешно

Аудит-2023

На основе первой версии проекта стандарта

Пройден успешно

Аудит-2024

На основе проекта стандарта, доработанного по результатам общественного обсуждения

Аудит-2024

Аудиту подвергались 4 продукта и их команды разработки

Проводился специалистами ИЛ «Фобос-НТ»

Проверялась реализация требований новой редакции ГОСТ Р 56939

Разработка всех оцененных продуктов соответствует требованиям новой редакции стандарта

Разработка первых редакций проектов ГОСТ Р «Защита информации. Разработка безопасного ПО», 2024

1

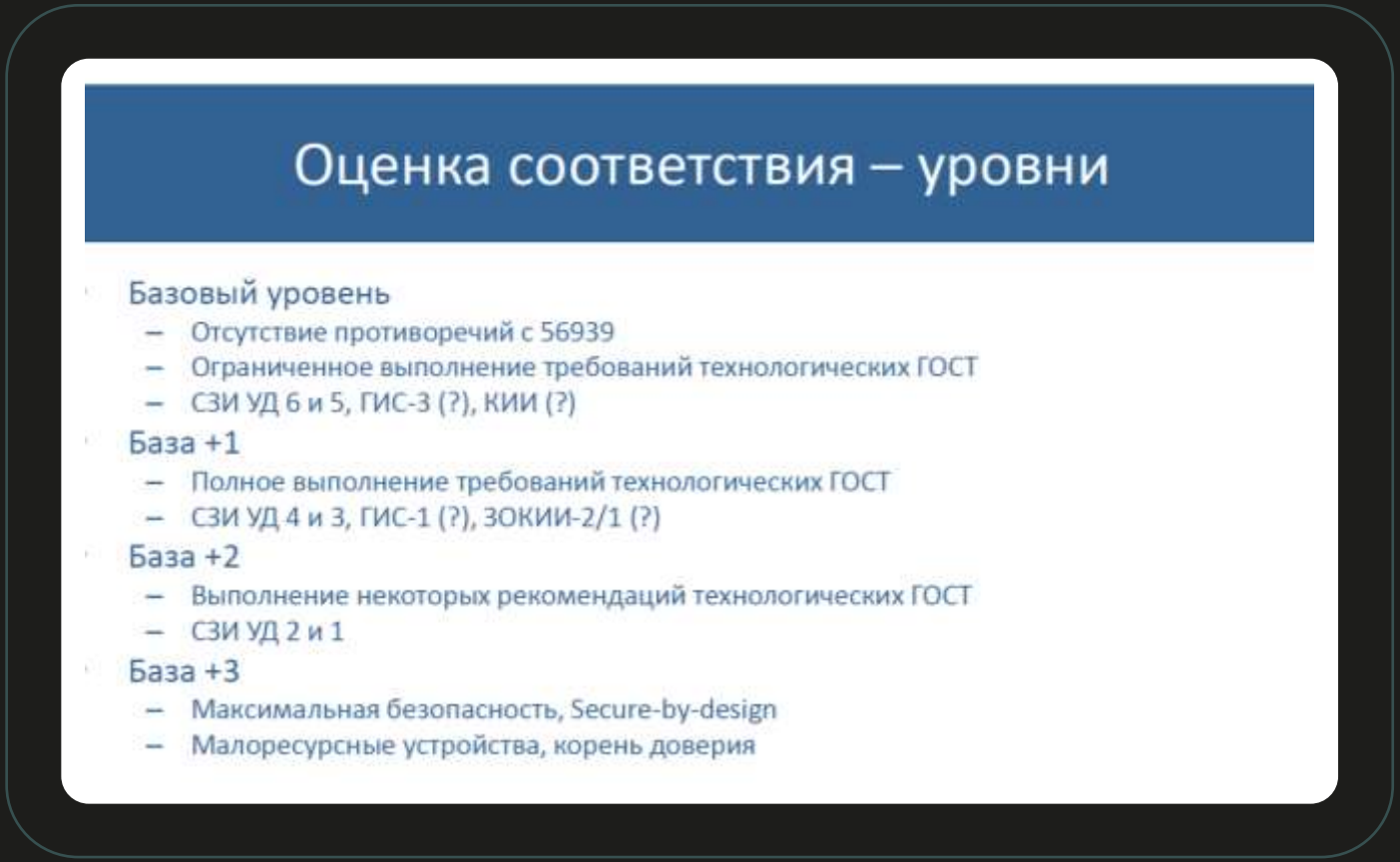
Методика оценки реализации процессов разработки безопасного ПО

2

Руководство по внедрению процессов разработки безопасного ПО

Уровни реализации процессов безопасной разработки (для стандарта «Методика оценки...»)

Из презентации Председателя ПК 4 ТК 362



Оценка соответствия – уровни

Базовый уровень
- Отсутствие противоречий с 56939
- Ограниченное выполнение требований технологических ГОСТ
- СЗИ УД 6 и 5, ГИС-3 (?), КИИ (?)

База +1
- Полное выполнение требований технологических ГОСТ
- СЗИ УД 4 и 3, ГИС-1 (?), ЗОКИИ-2/1 (?)

База +2
- Выполнение некоторых рекомендаций технологических ГОСТ
- СЗИ УД 2 и 1

База +3
- Максимальная безопасность, Secure-by-design
- Малоресурсные устройства, корень доверия

Уровни реализации процессов безопасной разработки (для стандарта «Методика оценки...»)

Видение Лаборатории Касперского:

Уровень 0

- процессы безопасной разработки отсутствуют или их реализованы в недостаточном объеме

Уровень 1

- процессы безопасной разработки есть и могут быть верифицированы, соответствуют требованиям ГОСТ Р 56939
- уровень реализации процессов безопасной разработки позволяет осуществлять сертификацию в Системе сертификации ФСТЭК России

- пр
и
- пр
ан
- по
пр
- ур
ра
се
из

Уровни реализации процессов безопасной разработки (для стандарта «Методика оценки...»)

Видение Лаборатории Касперского:

Уровень 2

- процессы безопасной разработки контролируются и улучшаются
- процессы обладают метриками, метрики анализируются, и отклонениями управляют
- Реализация данного уровня зрелости подтверждается историчностью выполнения процессов;
- уровень реализации процессов безопасной разработки позволяет разработчику **самостоятельно** осуществлять сертификационные испытания при внесении изменений

Уровень 3

- процессы безопасной разработки охватывают все продукты и команды разработки компании
- спец. тесты / инструменты используются на регулярной основе для большей части кода, включая заимствованный (привлекаемый)
- в данных практиках организация является «законодателем мод», визионером, контрибьютором, безусловным экспертом

Лаборатория Касперского подала заявку на сертификацию процессов безопасной разработки программного обеспечения

kaspersky

Исх. № 13628
от «10» июня 2024 г.

Начальнику 2 Управления
ФСТЭК России
Шешкову Д. Н.
105066, г. Москва, ул. Старая Басманная, 17

ЗАЯВКА

на сертификацию процессов безопасной разработки программного обеспечения

Полное и сокращенное (при наличии) наименование изготовителя, его организационно-правовая форма:	Акционерное общество «Лаборатория Касперского» (АО «Лаборатория Касперского)
Адрес юридического лица в пределах места нахождения юридического лица - изготовителя:	125212, РФ, г. Москва, Ленинградское шоссе, дом 39А, строение 2
Адрес для корреспонденции изготовителя:	125212, РФ, г. Москва, Ленинградское шоссе, дом 39А, строение 3
Фамилия, имя и отчество (при наличии) лица, ответственного за сертификацию процессов безопасной разработки программного обеспечения:	Нападовская Карина Олеговна
Номер телефона и адрес электронной почты (при наличии) изготовителя:	+7-916-888-85-89 Karina.Napadovskaya@kaspersky.com
Наименование органа по сертификации, в котором планируется проведение сертификации:	Институт системного программирования им. В.П. Иванникова Российской академии наук
Заявляемый срок действия сертификата соответствия:	5 лет
Должность руководителя изготовителя	Генеральный директор Е.В. Касперский «10» июня 2024 г.

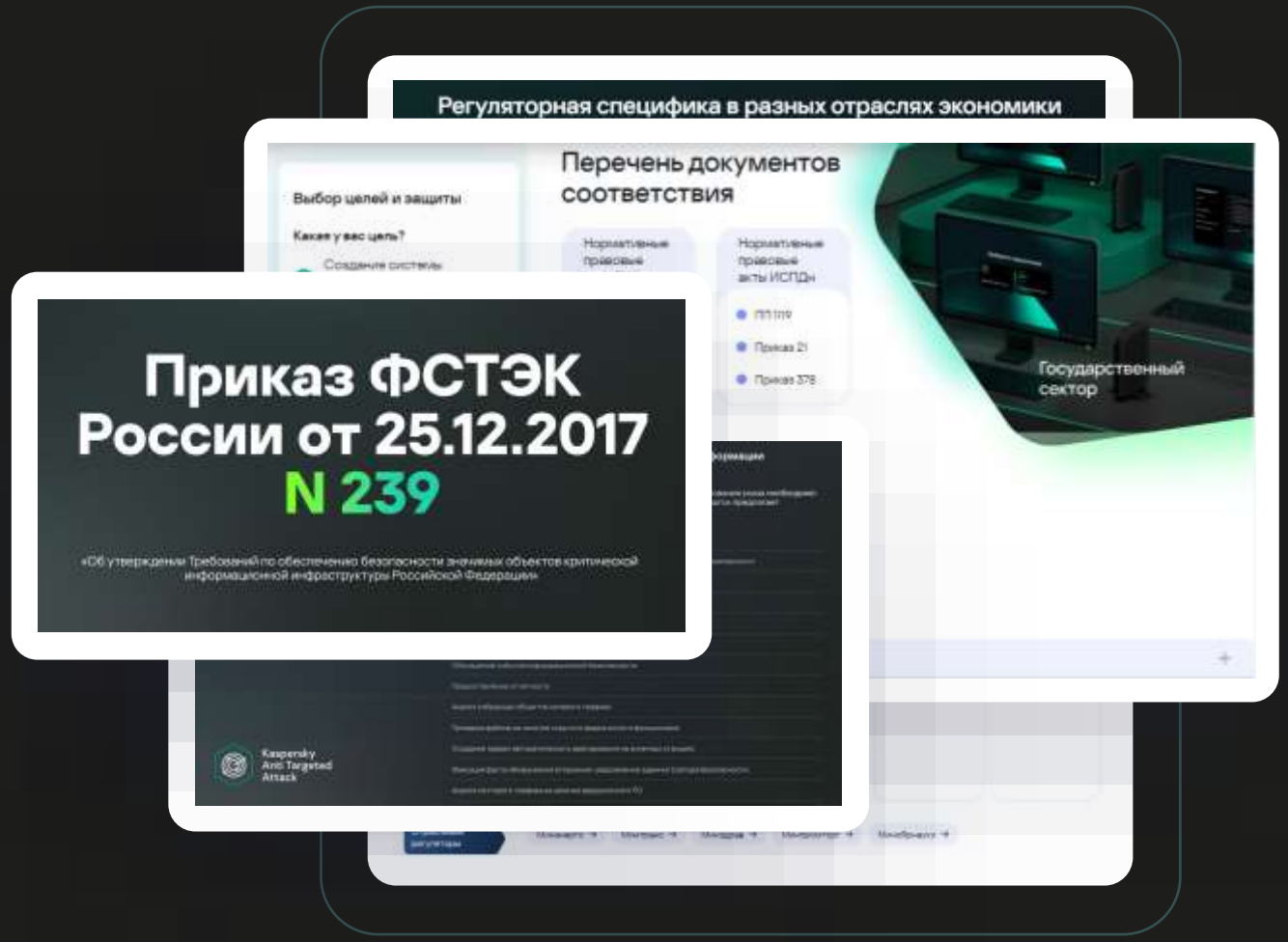
Планируем провести оценку на соответствие редакции ГОСТ Р 56939-2024

Сборные ведущих вузов Беларуси сразились за кубок Security challenge — первой олимпиады по кибериммунитету

28–29 мая в Минске при поддержке «Лаборатории Касперского» прошла республиканская олимпиада по защите информации среди студентов вузов «Security Challenge», в которой приняли участие 33 человека в составе 7 команд

Регуляторный хаб знаний

В области информационной безопасности



Регуляторный хаб знаний

В области информационной безопасности

Добавление информации и экспертизы:

- О национальных, отраслевых и международных стандартах
- О нормативных документах по сертификации по требованиям информационной безопасности
- О нормативных документах в области лицензирования деятельности по защите информации

Спасибо!