РБПО — не дополнительная активность ИБ, а обязательная часть создания и поставки ПО

Внедрение практик безопасной разработки и подготовка к сертификации

BASIS

Почему это обязательно?

РБПО — условие работы с госзаказчиками и объектами КИИ

ГОСТ Р 56939-2024

- Выявляем и закрываем уязвимости на ранних стадиях
- Безопасность встроена в CI/CD
- Нужны артефакты: отчёты и фиксация исправлений

Приказ ФСТЭК РФ №239 (КИИ)

- Безопасная разработка — обязательный процесс
- Нужно управление уязвимостями
- Подтверждение мер безопасности

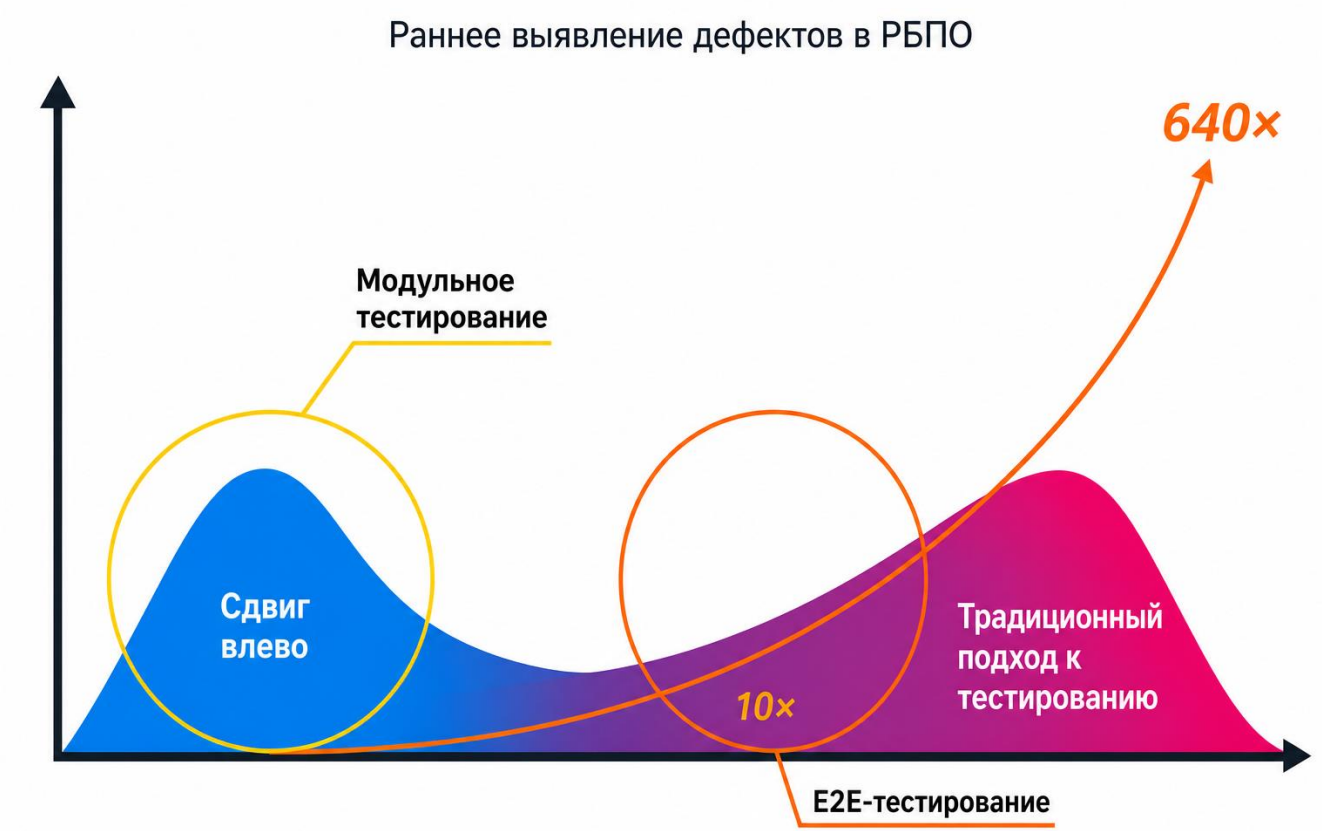
Приказ ФСТЭК РФ №117 (ГИС)

- Безопасность — на всём жизненном цикле
- Контроль изменений и компонентов
- Подтверждающие артефакты обязательны

BASIS

Раннее выявление = дешевле и быстрее

Практики РБПО снижают стоимость исправлений и ускоряют сертификацию



Что это дает?

- Ловим дефекты на ранних проверках, а не в конце
- Исправление дешевле в десятки и сотни раз
- Релизы и сертификация ФСТЭК РФ становятся более предсказуемыми
- Продукты «Базис» сертифицируются непрерывно

BASIS

С чего мы начинали

На старте безопасность подключалась поздно и несистемно

01

Вне жизненного цикла

Работы по ИБ начинались, в основном, перед сертификацией, а не были частью ежедневной разработки

02

Не было единого контура

Не было единой системы управления разработкой безопасного ПО и не было системы управления уязвимостями (VM)

03

Приоритет был низким

Команда фокусировалась на потребностях бизнеса, а исправления уязвимостей шли несистемно

Подробнее в блоге «Базиса» на Хабр

04

Культура РБПО была слабой

Было мало подсказок по фиксу; Security Champions ещё не было. Регламенты уже были, но команды их почти не читали

05

Не было доверенного репозитория

Компоненты брали из разных источников — без единого контроля версий и без воспроизводимости сборки

BASIS

Как устроен процесс сейчас

Чтобы закрыть разрывы, зафиксировали роли: отдел РБПО, УАПиКК и команды

Отдел обеспечения РБПО

- Центр компетенций по безопасной разработке
- Инструменты, методология и поддержка команд
- Подготовка производства к сертификации

Принцип разделения

- Отдел РБПО — методология, инструменты, триаж
- УАПиКК — финальная экспертиза и сертификация продуктов
- Команды — разработка и устранение дефектов

Отдел РБПО

Конвейеры, SAST/SCA, подготовка контура управления уязвимостями

УАПиКК

Качество релиза, регуляторные сканы, сертификация продуктов

Команды разработки

Модель угроз, регулярные проверки, фиксы, обновление компонентов

BASIS

Что изменилось

Год назад → сейчас: продукты, риски, команда, сборка, зрелость

01

Продукты

За квартал: 1 продукт с изменениями → до 4 (изменение/продление сертификата)

02

Уязвимости и зависимости

2024: 1 продукт, 3713 уязв. в 4195 завис. → 2025: 4 продукта, 351 уязв. в 4702 завис.

03

Команда РБПО

5 техспециалистов → 13 (сертификация, аналитики, фаззеры, DevSecOps, AppSec) и Security Champions в командах разработки

04

Сборка ППК и цепочка

ППК: вручную → DevSecOps + Code Scoring, время −1/3. Buildography — прозрачная и верифицируемая цепочка сборки

05

Зрелость и внешний контур

Поверхности атаки — с архитекторами на проектировании. Есть конвейер РБПО для новых продуктов. Вступили в 4 кластера ФСТЭК; с консорциумом — ~30 модулей

BASIS

Практики и инструменты

Упор на ИСП РАН и партнёров; остальное — вспомогательное

Типы проверок

SAST — Статический анализ
Код до запуска

SCA — Компоненты и зависимости
Сторонние библиотеки

Fuzzing — Динамический анализ
Поведение под нагрузкой входов

Secrets — Управление секретами
Ключи и пароли в коде

Threat Model — Моделирование угроз
Поверхность атаки

На чём делаем упор

ИСП РАН

Svace, Natch, Sydr, Crusher, Buildography

Партнеры

CodeScoring; ПО схематической визуализации поверхности атаки от НТЦ ФОБОС

Вспомогательные

SonarQube, CodeQL/PT AI, PVS Studio, Solar AppScreener, Dependency-Check/MaxPatrol SCA, Gitleaks, TruffleHog и др.

BASIS

Метрики и статус

Операционные метрики: покрытие проверок, SLA, статус процессов

100%
продуктов: SAST/SCA, Unit и фаззинг внедрены в CI/CD

≤ 48 ч.
норматив на компенсирующие меры (крит. — до 24 ч. у части заказчиков)

≤ 60 дн.
норматив на устранение уязвимости

сроки
горизонт — на дорожной карте

Статус процессов

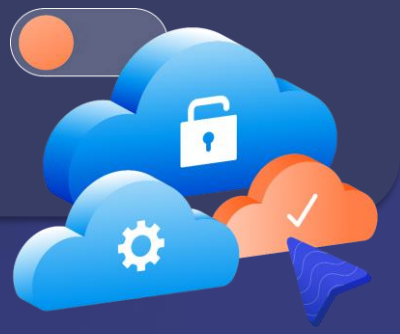
4/25
выполнено

3
из них передано в РБПО

4
в работе

17
в плане

Контролируем ход процессов по плану внедрения



BASIS

Дорожная карта

Что дальше: команды → пилот → масштабирование

Этап 1

3–4 месяца

Работа с командами

- Сбор по инфраструктуре и инструментам
- Проработка 25 процессов ГОСТ
- Обучение разработчиков и тестировщиков
- Довести контур BVP: закрыть оставшиеся процессы
- Срок с учётом объёма продукта, ролей и загрузки команд

Этап 2

6–7 месяцев

Пилот на BVP (+SDN)

- «Золотая» документация
- Практики в командах и CI/CD
- Подготовка к сертификации
- Выстроить контур управления уязвимостями (VM)
- Усилить автоматизацию вместе с DevOps
- Срок зависит от загрузки команды разработки

Этап 3

12–18+ месяцев

Масштабирование

- Адаптация под каждый продукт
- Security Champion в командах
- Сертификация по необходимости
- Ориентир — практики других компаний

BASIS

Цель: встроить РБПО в поставку и пройти сертификацию процессов по ГОСТ Р 56939-2024. Стремимся уложиться в 7–8 месяцев; по практикам рынка реалистичный горизонт часто от 1,5 лет; этап масштабирования — до 12 до 18 и более месяцев.

BASIS

Команда РБПО