Международный ТБ ФОРУМ Технологии и Безопасность

BASIS

От сертификации продуктов к культуре безопасной разработки на опыте внедрения процессов РБПО

Александр Каверин
руководитель Центра обеспечения автоматизации производства

Безопасная разработка — это про людей

Успех обусловлен не только инструментами, но и организационной трансформацией!

- От пилотного Python-продукта — к масштабированию на десятки проектов
- От инструментов — к процессам и партнёрству
- От контроля — к совместной ответственности

2024 год

1 продукт

3 713 уязвимостей в **4 195** зависимостей

2025 год

4 продукта

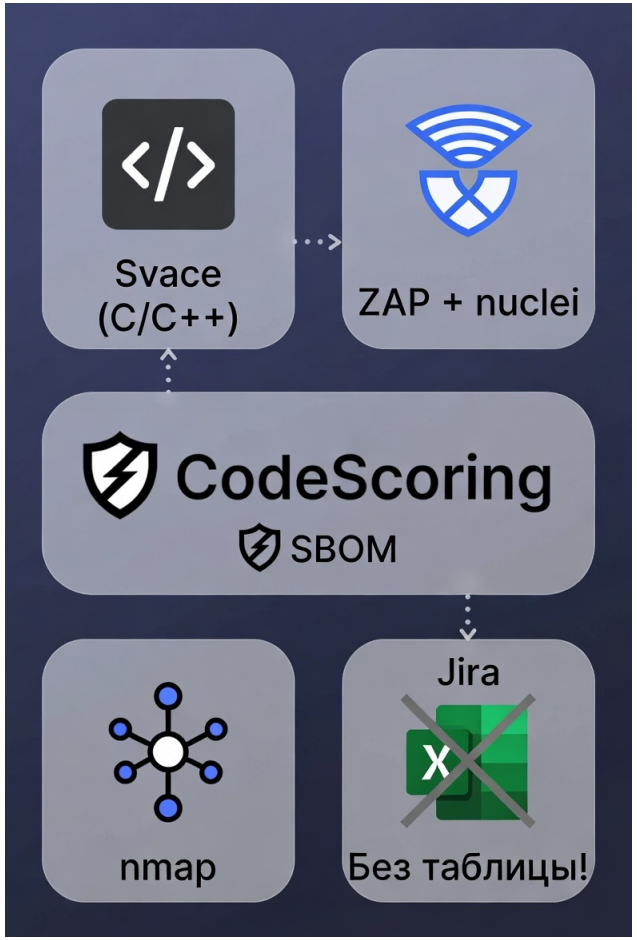
351 уязвимость в **4 702** зависимости

Сегодня — о том, как сделать безопасность частью культуры, а не пунктом чек-листа

Инструменты — единая платформа вместо фрагментов

Инструменты - это часть процесса, а не его цель

- CodeScoring — центральный хаб для SCA и SBOM
- Svace — глубокий SAST для C/C++ через стандартизированный Docker-образ
- ZAP + nuclei + nmap — DAST в рамках единого workflow
- Отказ от Excel, SonarQube, DefectDojo — всё в Jira + автоматизация

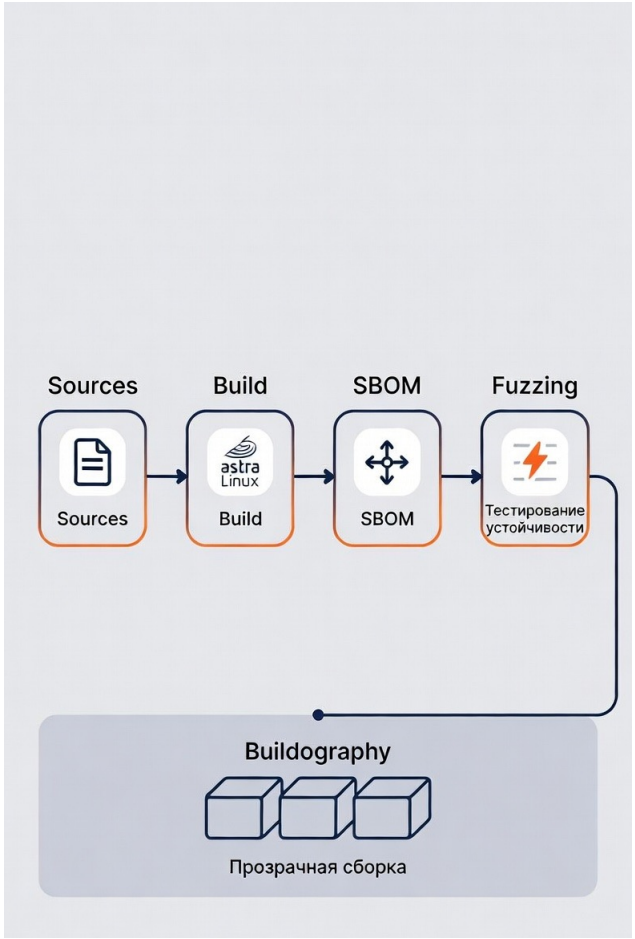


Сотрудничество с Консорциумом участников по поддержке Технологического центра исследований безопасности системного программного обеспечения

21 модуль
исследуется совместно

Процессы — безопасность как часть жизненного цикла

- Единый универсальный пайплайн для всех продуктов
- Автоматическое формирование ППК (SBOM) по требованиям сертификации
- Контрольные суммы — только через сертифицированные дистрибутивы Linux
- Buildography — прозрачная и верифицируемая цепочка сборки
- Фаззинг — регулярная практика, интеграция в CI/CD



Взаимодействие с командами разработки — от контроля к партнёрству

- Kick-off по чек-листу: архитектура, роли, точки интеграции
- Задачи в Jira + уведомления через Telegram-бота
- Security Champions в командах + централизованная методология
- Совместные контрольные точки на этапах сертификации
- Личный контакт = быстрое понимание без волокиты

Проблематика внедрения ГОСТ Р 56939 по РБПО

Без CISO/единого ИБ-подразделения — задача нерешаема

Уровень зрелости КБ/ИБ в компаниях:

от базового (антивирус + firewall) → до продвинутого (интеграция в ЖЦ продукта)

ГОСТ Р 56939:

целостная модель безопасной разработки (снижение рисков на этапе проектирования)

Разрыв:

декларируемые практики ≠ реальные процессы в разработке

Ключ:

CISO как архитектор ИБ + участие всех (от CISO до разработчиков)

Необходимость баланса между безопасностью и бизнес-реалиями

Цели сертификации РБПО

Основные цели

Для КИИ:

соблюдение требований по
Приказу ФСТЭК № 239

Для госструктур и регулируемых org:

внутренние требования
(Сбер, Газпром, ГринАтом)

Снижение затрат:

выявление уязвимостей
на ранних этапах дешевле

Конкурентное преимущество:

сертификат — аргумент в госзакупках
(инициатива по обязательности

- Самостоятельные испытания изменений (без labs) → ускорение time-to-market → повышение доверия заказчиков
- Сертификат РБПО — не маркетинговый инструмент
  Его использование в закупках как конкурентного преимущества без реального внедрения процессов может быть расценено как манипуляция

Проблема 1:
Ограниченное подразделение РБПО

- Подразделение только для сертификации продуктов
- Нет участия в требованиях, проектировании, управлении ЖЦ
- Нет dedicated-команды (методолог, аналитик, координатор)
- Перегруженность + отсутствие кадров (архитектура, требования)

Решение:

- Создать отдельное подразделение/штатную единицу
- Владелец процесса (25 процессов ГОСТ)
- Описание, актуализация, контроль, реестр требований

Проблема 2:
Ориентация на задачи, а не на процессы

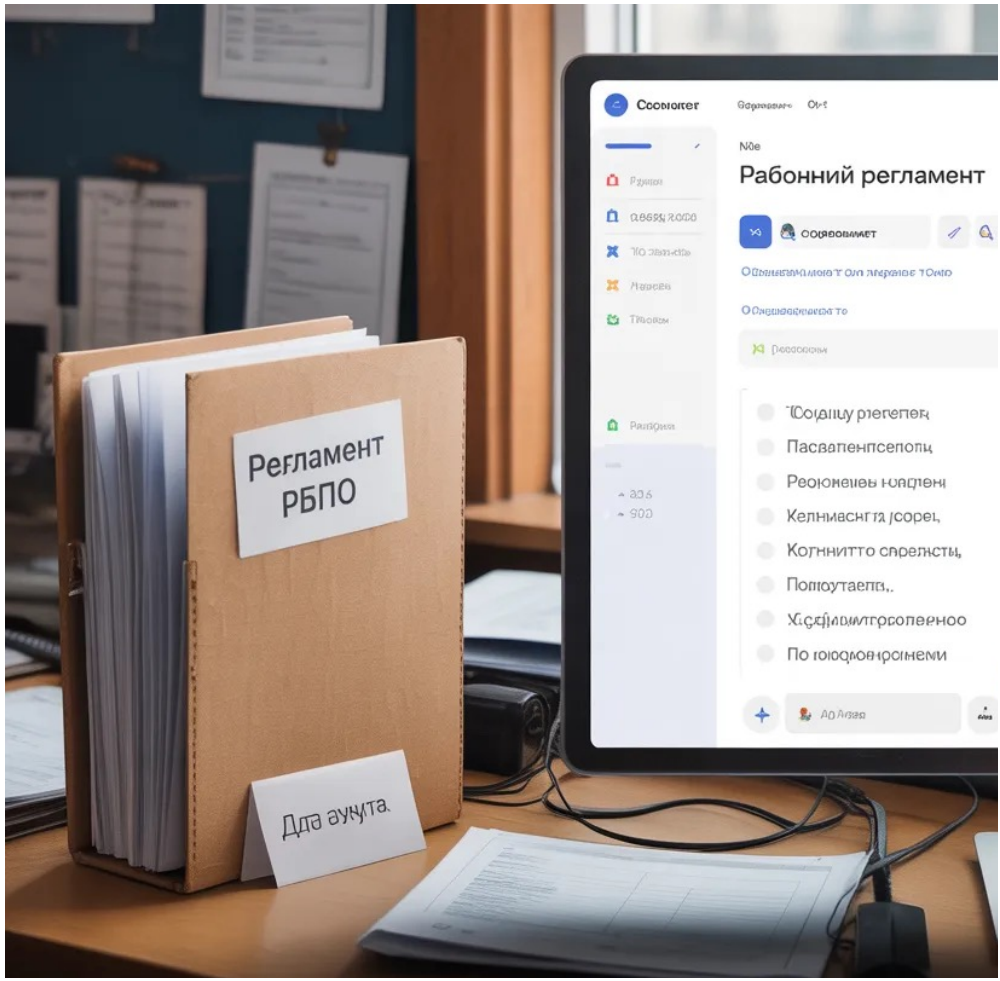
- Сотрудники: узкопрофильные действия для сертификации
- Нет системных архитекторов процессов (роли, триггеры, метрики)
- Потребность в Security Champions
  (один человек/распределение без ответственности)

Решение:

- Назначить Security Champion в каждой dev-команде
- Центральная команда: методология, артефакты, интеграция в CI/CD
- Security Champions — не дополнительная нагрузка, а встроенная роль
- Центральная команда РБПО — методологическая база, а не исполнитель

Проблема 3:
«Мёртвый» регламент

- Документ «для аудита»: зонтичный, декларативный
- Не ознакомлены, не используется в работе



Решение:

- Скорректировать конкретные шаги, артефакты, доступ в Confluence/tasks
- Обучение на примерах
- Консалтинг для рабочих инструкций

Проблема 4:
Отсутствие мотивации от руководства

- РБПО — «второстепенная» задача
- Жесткие сроки + коммерческие приоритеты
- Нет ресурсов на улучшение

Решение:

- Высшее руководство: объявить стратегическим приоритетом
- KPI, блокировки релизов, roadmap, напоминания
- Инициатива сверху (не от ИБ-подразделения)

Проблема 5:
Инициатива у «нескольких исполнителей»

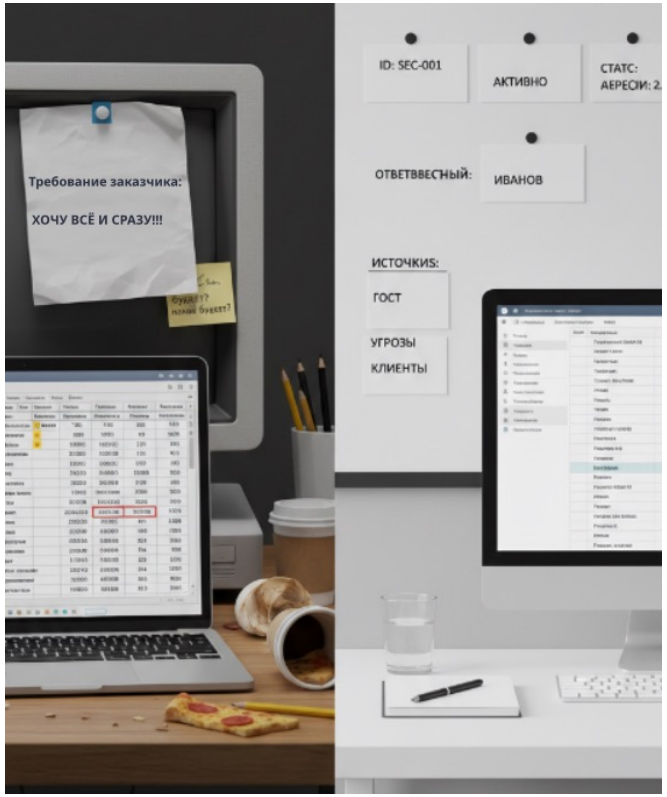
- Проблемы озвучивают только назначенные (консультанты/сертификация)
- Dev/тест/архитектура: «чужая» задача

Решение:

- Совместные сессии: «снизу вверх» (риски, автоматизация)
- Безопасность = защита продукта/репутации
- Проектирование с участием исполнителей

Проблема 6:
Стихийное управление требованиями

- «На коленке»: только очевидные/от заказчика
- Нет анализа угроз, стратегии, актуализации
- Фокус: «продать», а не устойчивость



Решение:

- Единый процесс: ID, статус, ответственный, привязка к версии
- Источники: нормативы, угрозы, ИБ, архитектура, заказчики/клиенты
- Автоматическая актуализация
- Ресурсы на поддержку

Как избежать провала

Внешний консалтинг на старте

- Фиксация зрелости
- Выявление разрывов
- Поэтапный план + обучение

+

Аудит

Проверка работоспособности (сборка, контроль, актуализация)

=

Результат

Дорожная карта + основа для ресурсов/команды

Аудит проверяет работоспособность процессов, а не наличие документов

Заключение

Зрелость безопасности

CISO + руководство

- Сотрудничество между CISO и руководством для стратегического руководства

Совместное проектирование

- Интеграция безопасности в процесс разработки с самого начала

Безопасность в каждом релизе

- Обеспечение безопасности на каждом этапе жизненного цикла разработки

Постоянные ресурсы

- Выделение достаточных ресурсов для поддержания и улучшения безопасности

BASIS

СПАСИБО ЗА ВНИМАНИЕ!

Александр Каверин
руководитель Центра обеспечения автоматизации производства