

**Опыт организации и проведения
сертификационных испытаний испытательной
лабораторией
ООО НТЦ «Фобос-НТ»**

ака радости и горести современной сертификации

Дмитрий Владимирович Пономарев

Москва 2025

Вместо предисловия. Принципы нашей работы

1. Служу Отечеству!
2. Сначала РБПО у заказчика - потом сертификационные испытания
3. Современная испытательная лаборатория - это ИТ/ИБ-компания
4. *«Не можешь остановить - возглавь»*. Развитие, апробация всех перспективных практик анализа и выстраивания процессов РБПО
5. Опора на создателей технологий, востребованных в коммерческом секторе
6. *«Если ты ходишь по грязной дороге, ты не сможешь не выпачкать ног»*. Отказ от работы с контрагентами, находящимися в зоне риска
7. *«Сильный не боится открытости»*. Делимся знаниями и опытом с сообществом и молодежью, на добровольных началах поддерживаем активности по популяризации РБПО
8. Лаборатория не может сделать за заявителя всё, но может научить, выборочно «щипнуть» в болевые точки, помочь *количественно*, дать свежий взгляд на состояние дел

Содержание доклада

1. Алгоритм работы с потенциальным заявителем
2. Связь внедрения и развития практик РБПО с сертификационными испытаниями
3. Технологические партнеры и стек инструментов РБПО
4. Опыт работы в Центре исследований безопасности системного ПО ФСТЭК России и ИСП РАН
5. Зоны потенциала совместной работы
6. События по теме РБПО

1. Алгоритм работы с потенциальным заявителем

Цель: отсеять заказчиков, принципиально не стремящихся внедрять и развивать процессы РБПО, до момента подписания каких-либо договорных обязательств.

Вопросы:

- вы понимаете, что инструменты и процессы РБПО должны появиться и развиваться на вашей стороне, поскольку никакая ИЛ за разумный срок не способна полноценно проанализировать весь код типового современного СЗИ
- вы понимаете, что на начальном этапе вложения в развитие Dev, QA, SDL и общий менеджмент могут составить до 10 процентов вашего бюджета, и что без поддержки «первого лица» люди могут взбунтоваться и вы получите отрицательный эффект
- вы понимаете, что РБПО - это про качество и эффективность бизнеса, а не «*за ради бумажки для ФСТЭК*»
- вы понимаете, что «весь код === ваш код»? Вы должны обеспечить контролируемый репозиторий, полную сборку из исходников (в т. ч. всего *зоопарка* в ваших контейнерах)

Типовые «ред-флаги» в ответах на наши вопросы:

- нам бы «*просто бумажку*»
- а сделайте весь анализ за нас, мы вам много заплатим!
- а мы с другой ИЛ делали 7 лет назад, там сказали что главное это ТУ и ФО
- нам бы через 3 месяца сертификат, нам очень надо
- у нас в компании всего 8 человек, (*но мы делаем СЗИ типа ОС...*) - мы же это не потянем

2. Связь внедрения и развития практик РБПО с сертификационными испытаниями

Формула из разряда «средняя температура по палате», но лучше мы не придумали:

- на команду 10-15 разработчиков + QA необходимо 1-2 специалиста РБПО (2-й может быть джуном-стажером у первого) с ролью Security Champion
- на две команды необходим как минимум один РБПО специалист в выделенный отдел РБПО

Тезисы:

- РБПО - для повышения эффективности вашего бизнеса в целом, а не для ФСТЭК России. Поэтому внедряем и автоматизируем все виды анализов и процессы порождения артефактов. Инженерные процессы «*ради ФСТЭКа*» - верный путь к плохому настроению и неэффективно потраченным финансам. Поэтому *сразу реализуйте процессы так, чтобы они жили без всякой сертификации*
- чтобы избежать «кота в мешке», необходимо провести большую часть испытаний до подачи Заявки, причем с привлечением и вовлечением специалистов разработчика. Поэтому *сначала контракт на внедрение и развитие практик РБПО, и только потом выход на сертификационные контракты*
- есть «коммерческое» и «полноценное» РБПО (ФСТЭК-РБПО). Оба полезны, но первое в первую очередь — про поиск известного, второе в первую очередь — про культуру разработки и поиск неизвестного. Поэтому *определение поверхности атаки на уровне кода, стат. анализ, генетический фаззинг и компиляторный харденинг, а не только «анализаторы уязвимостей»*

3. Технологические партнеры и стек инструментов РБПО

Принцип выбора инструментов:

- инструмент должен быть востребован у коммерческих заказчиков, в идеальном случае - в странах с развитым ИТ/ИБ. *Инструмент не должен целиться в «рынок сертификации» как в основной*
- инструмент должен создаваться коллективом с технологическим и научным бэкграундом, либо с востребованной у коммерческих заказчиков экспертизой (в идеале - оба пункта). *Перекрашенный опенсорс, как правило, не стоит своих денег, даже если обладает «сертификатами»*
- для спец. задач можно пробовать и интересные открытые инструменты. *Лучше попробовать +1 неизвестный инструмент и найти багу, чем не попробовать и не найти*

Наши технологические партнеры и стек инструментов РБПО:

- **ИСП РАН**: стат. анализ, генетический фаззинг, помеченные данные, харденинг и контроль сборочных процессов
- **КодСкоринг**: композиционный анализ, организация контролируемого репозитория
- **Лантри**: анализ безопасности kubernetes-based СЗИ
- **DPA Analytics**: анализ фронтенд-безопасности
- **Лукоморье**: трекер задач Яга

4. Бесценный опыт работы в Центре исследований безопасности системного ПО ФСТЭК России и ИСП РАН

Опыт 2024-2025 гг.:

- более 8 000 разметок статических анализаторов
- более 70 фаззинг-целей различного уровня
(рекорд фаззинг-обертки: 3 месяца разработки и ~2000 строк кода)
- участие в исследованиях 20+ открытых компонентов, в т. ч. в анализе ядра Линукс
- более 150 поданных заказчикам и в апстрим сведений об уязвимостях и дефектах кода, и исправляющих их патчах

Предложение - учитывать роль лабораторий в кроссверификации результатов анализа (и иных активностях) в Центре по отдельному от разработчиков принципу учета



Нельзя контролировать то и обучать тому, в чем не разбираешься сам

5. Зоны потенциала совместной работы

Существует широкий спектр задач, в совместном решении которых были бы заинтересованы все участники системы сертификации, в т. ч. ФСТЭК России. Ряд из них не являются потенциальными «зонами заработка», однако уже сейчас являются «зонами затрат» в силу отсутствия стандартизации:

- унифицированный формат представления материалов сертификационных испытаний
- унифицированные форматы нотирования, в т. ч. представления поверхности атаки, и инструменты их отрисовки
- репозитории верифицированных материалов по проведению различных видов исследований («хорошие» и «плохие» примеры). Частично закрывается телеграм-каналом @sdl_inform, а также рядом проектов, анонс которых состоится в среднесрочной перспективе
- развитие вспомогательных инструментов анализа (пример - инструмент автоматизации, генерации фаззинг-оберток FUTAG)

Решение данных задач представляется возможным и бесспорно полезным в режиме «сообщества» при организационной и методической поддержке ФСТЭК России, в формате рабочей группы или проектов с открытым исходным кодом

6. События по теме РБПО

Открытая конференция ИСП РАН 09-10 декабря



облачный партнер



официальный партнер



официальный партнер



официальный партнер



официальный партнер



официальный партнер



официальный партнер



партнер выставки



партнер выставки



партнер выставки



партнер выставки



партнеры выставки



партнер выставки



партнер конференции



партнер выставки



партнер выставки



партнер конференции



партнер конференции

Секция «Три кита РБПО» в журнале BIS: ib-bank.ru/rbpos



Три кита РБПО. 2. Динамический анализ

[ПОДРОБНЕЕ](#)



Три кита РБПО. 1. Статический анализ

[ПОДРОБНЕЕ](#)



Безопасная разработка. Эволюция по ГОСТУ

[ПОДРОБНЕЕ](#)

ТБФорум 2026 18-20 февраля. День РБПО-сообщества ФСТЭК России и ИСП РАН

