НПЦ КСБ

Построение процессов разработки безопасного ПО: от нормативной базы до лучших практик

Степан Харитонов
руководитель направления по безопасной разработке, НПЦ КСБ

Иван Федоров
первый заместитель генерального директора, НПЦ КСБ

Михаил Шипицын
заместитель генерального директора, КСБ-СОФТ

Всем участникам будет направлен чек-лист по проведению экспресс-аудита для оценки текущего уровня зрелости процессов РБПО

Запись вебинара направим Всем участникам на указанный при регистрации e-mail

Задавайте вопросы во вкладке «Вопросы»

ТЕМЫ ДЛЯ ОБСУЖДЕНИЯ

РБПО: что это и зачем?

- Почему есть смысл интегрировать практики безопасности в конвейер разработки?
- Драйверы внедрения РБПО

Нормативное регулирование в области РБПО

- Кому предстоит внедрить процессы РБПО?
- Как соблюсти требования НПА в области РБПО?

Основные этапы внедрения, примеры из жизни

- Какие первые шаги стоит выполнить?
- Типовые ошибки при внедрении процессов РБПО
- Реальные кейсы из опыта НПЦ КСБ
- Рекомендации разработчику по построению РБПО

Наградим авторов 3 лучших вопросов фирменным мерчем!

ЧТО ТАКОЕ БЕЗОПАСНАЯ РАЗРАБОТКА (SDL/РБПО)?

SDLC (Software Development Lifecycle)

Жизненный цикл разработки ПО.

Недостаток подхода – отсутствуют мероприятия, связанные с проверками безопасности ПО.

SDL (Security Development Lifecycle)

Жизненный цикл безопасной разработки ПО.

Набор процедур безопасной разработки ПО, позволяющий обнаруживать и устранять уязвимости на ранней стадии ЖЦ, до публикации релиза продукта.

РБПО (Разработка безопасного программного обеспечения)

Бизнес-процесс, предусматривающий внедрение практик и подходов обеспечения безопасности на всех этапах жизненного цикла разработки и эксплуатации программных продуктов.

ПОЧЕМУ СТОИТ ЗАДУМАТЬСЯ

35 000+

уязвимостей обнаружили по итогам 2024 года (число растёт с каждым годом)

до 78%

доля открытого исходного кода в ПО в некоторых отраслях

90%

инцидентов безопасности вызваны дефектами исходного кода

80%

веб-приложений имеют хотя бы 1 опасную уязвимость

21%

утечек данных вызван уязвимостями программного обеспечения

Высокая

стоимость устранения уязвимостей на поздней стадии

ПРЕДПОСЫЛКИ ДЛЯ РБПО

Рост киберугроз и атак на ПО

60% компаний
столкнулись с инцидентами из-за уязвимостей в ПО

«Стоимость» уязвимостей

$4,450,000
Средняя стоимость утечки данных

Финансовые и репутационные потери

Убытки от кибератак, утечки ПДн, потеря доверия клиентов

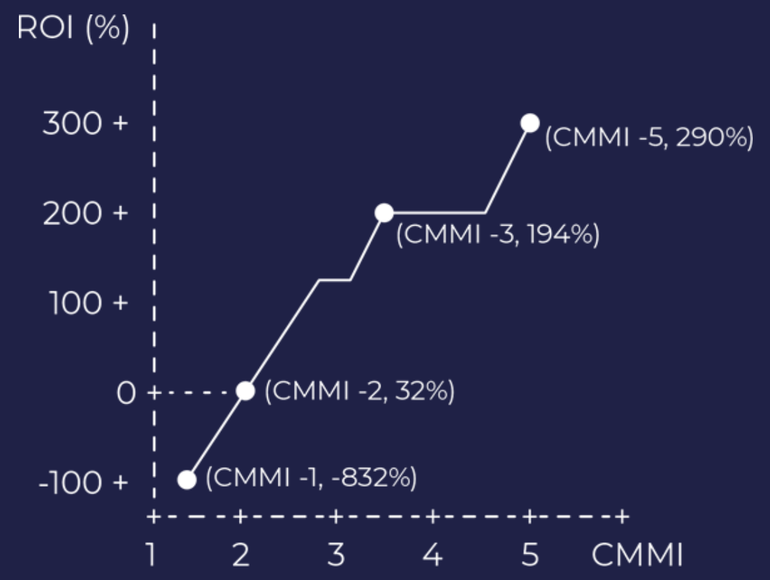
Усложнение архитектуры ПО и применяемых технологий

Рост числа уязвимостей, увеличение ПА

Законодательные и отраслевые требования

Внедрение процессов РБПО не просто «хорошая» практика, а обязательное условие для выхода на рынок

ЭКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ ВНЕДРЕНИЯ РБПО



для CMMI 1-2 – ROI отрицательный ввиду **высоких затрат на ручные процессы** и как следствие **сопротивления команд**

для CMMI 2.3-3 – происходит критический переход, при котором ROI растет экспоненциально благодаря **автоматизации и системному управлению качеством**

для CMMI 4-5 – происходит эффект насыщения – дальнейшее **повышение зрелости процессов разработки ПО** дает убывающую отдачу

Направление	Требования ГОСТ Р 56939-2024	Практики / коммуникации SAFe	Пояснения
Планирование и управление процессами	Регулярное планирование, анализ статуса	PI Planning, Iterations, ART Flow, Team Flow	Поддержка планирования и итеративной адаптации
Обучение и культура безопасности	Повышение осведомленности, учет обучения	CLC, ретроспективы	Упрощает внедрение и обучение по безопасности
Управление требованиями безопасности	Формализация и пересмотр требований	Backlog, PI Planning, System Demo	Учет требований в Backlog облегчает интеграцию
Контроль качества и анализ кода	Статический / динамический анализ, правила	Built-In Quality, DevOps, тестирование	Поддержка автоматизации контроля в review
Управление уязвимостями и инцидентами	Поиск, анализ, реагирование	DevOps, System Demo, итерации	Поддержка быстрой реакции и доставки исправлений
Прозрачность и коммуникации	Документирование, информирование	System Demo, открытые коммуникации	Поддержка открытости процессов и требований

ЦЕЛИ ПОСТРОЕНИЯ ПРОЦЕССОВ РБПО

Непрерывность и защищённость цифрового бизнеса

- Киберустойчивость программных продуктов
- Снижение количества уязвимостей в коде продуктов
- Проактивное выявление уязвимостей в ПО на этапе разработки
- Устранение технического долга дефектов ИБ

Зрелость технологий и процессов разработки защищенности ПО

- Продуктивность разработки при создании защищенного ПО
- Внедрение практик анализа защищенности в инженерный конвейер разработки ПО
- Экономия финансовых затрат на ИБ за счет роста экспертизы у команды разработки
- Снижение стоимости выявления и устранения уязвимостей

Time-to-market

- Снижение времени выхода на рынок защищенного ПО
- Рост объемов выпуска бизнес-функций с сохранением качества и защищенности ПО
- Прозрачный процесс оперативного и бесшовного внесения ИБ-изменений в ПО

Compliance

- Контроль уровня соответствия процессов индустриальным стандартам
- Соответствие ПО регуляторным требованиям
- Лицензионная чистота используемых компонентов с открытым исходным кодом
- Контроль рисков кибербезопасности ПО

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ РБПО

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 71206-2024

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Безопасный компилятор языков C/C++

Общие требования

ГОСТ Р 71207-2024

Защита информации

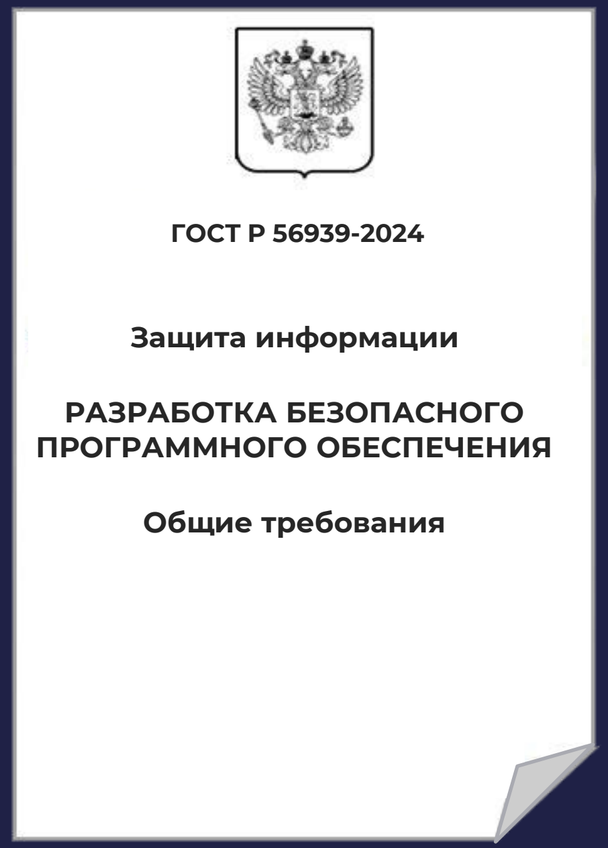
РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Статический анализ программного обеспечения

Общие требования

СТРУКТУРА ГОСТ Р 56939-2024

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. ОБЩИЕ ТРЕБОВАНИЯ



Разработан на смену ГОСТ Р 56939-2016

25 процессов, из них 8 – новые, относительно ГОСТ Р 56939-2016:

- Планирование процессов РБПО
- Формирование и поддержание в актуальном состоянии правил кодирования
- Управление доступом и контроль целостности кода при разработке ПО
- Обеспечение безопасности используемых секретов
- Использование инструментов композиционного анализа
- Проверка собранного бинарного кода на предмет наличия признаков внедрения вредоносного кода через цепочки поставок
- Безопасная поставка ПО пользователям
- Обеспечение безопасности при выводе ПО из эксплуатации
- Требования по обязательному наличию IT-инфраструктуры *(Управление версиями, Bug tracking / управление задачами, CI/CD)*

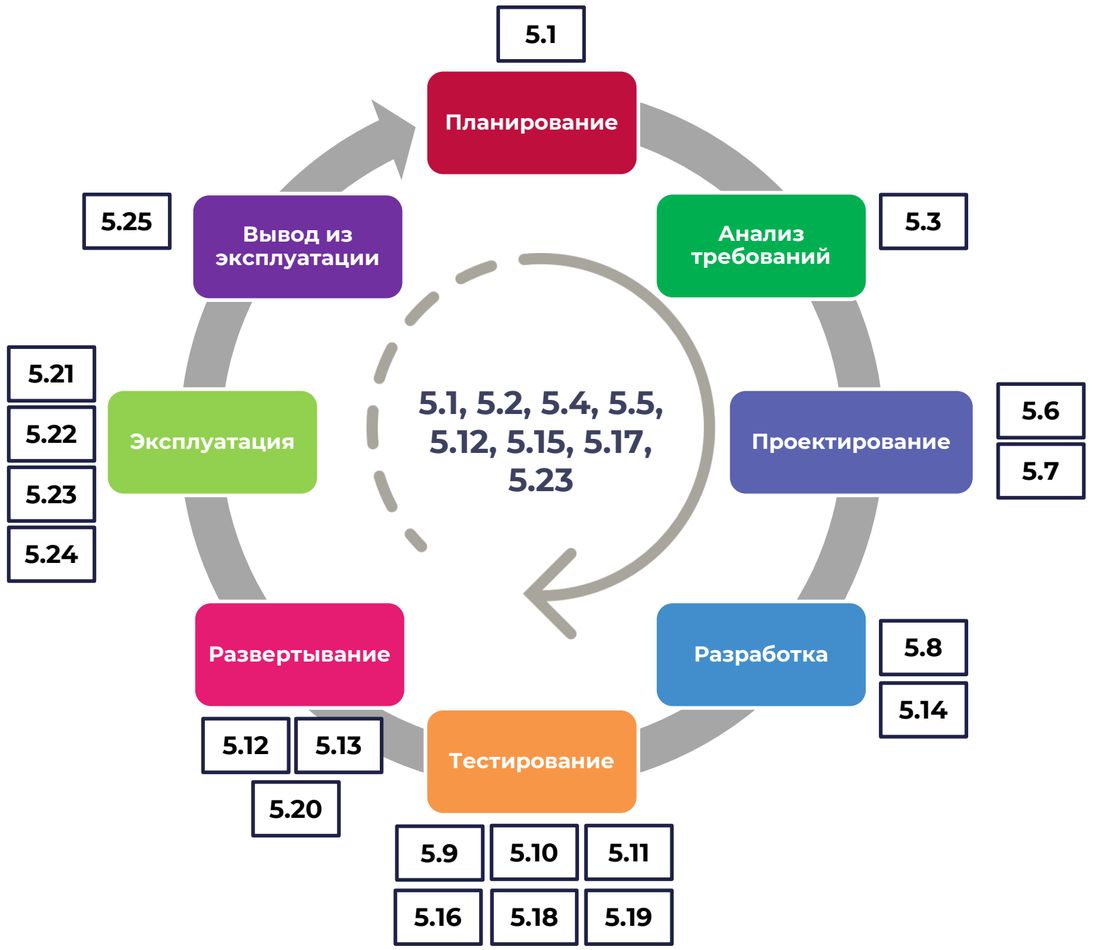
Стандарт направлен

на достижение целей, связанных с **предотвращением появления, выявлением и устранением недостатков**, в том числе **уязвимостей, в ПО**, и содержит общие требования, предъявляемые при реализации процессов РБПО.

Стандарт предназначен

для разработчиков и производителей ПО, а также для организаций, выполняющих оценку соответствия процессов разработки ПО.

Процессы разработки безопасного ПО согласно ГОСТ Р 56939-2024



5.1 Планирование процессов разработки безопасного ПО
5.2 Обучение сотрудников
5.3 Формирование и предъявление требований безопасности к ПО
5.4 Управление конфигурацией ПО
5.5 Управление недостатками и запросами на изменение ПО
5.6 Разработка, уточнение и анализ архитектуры ПО
5.7 Моделирование угроз и разработка описания поверхности атаки
5.8 Формирование и поддержание в актуальном состоянии правил кодирования
5.9 Экспертиза исходного кода
5.10 Статический анализ исходного кода
5.11 Динамический анализ кода программы
5.12 Использование безопасной системы сборки ПО
5.13 Обеспечение безопасности сборочной среды ПО
5.14 Управление доступом и контроль целостности кода при разработке ПО
5.15 Обеспечение безопасности используемых секретов
5.16 Использование инструментов композиционного анализ
5.17 Проверка кода на предмет внедрения вредоносного ПО через цепочки поставок
5.18 Функциональное тестирование
5.19 Нефункциональное тестирование
5.20 Обеспечение безопасности при выпуске готовой к эксплуатации версии ПО
5.21 Безопасная поставка ПО пользователям
5.22 Обеспечение поддержки ПО при эксплуатации пользователями
5.23 Реагирование на информацию об уязвимостях
5.24 Поиск уязвимостей в ПО при эксплуатации
5.25 Обеспечение безопасности при выводе ПО из эксплуатации

НОРМАТИВНЫЕ ТРЕБОВАНИЯ В ОБЛАСТИ РБПО

ПО ДЛЯ ГИС

Приказ ФСТЭК России № 117

50. В случае **самостоятельной разработки оператором** (обладателем информации) ПО, предназначенного для использования в ИС, **должны быть реализованы меры, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024**

В случае привлечения **подрядной организации** по решению руководителя в ТЗ могут быть включены **требования по РБПО в соответствии с ГОСТ Р 56939-2024**

ЦИФРОВОЙ ПРОДУКТ НА ПЛАТФОРМЕ ГОСТЕХ

Концепция РБПО на ЕЦП РФ «ГосТех»

Нормативная база в области РБПО:

- Методические рекомендации «Базовые сервисы Единой цифровой платформы Российской Федерации «ГосТех». Основные требования к составу и функциями
- Методические рекомендации по включению сервисов в Единую цифровую платформу Российской Федерации «ГосТех»
- Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы «ГосТех»

ПРИКЛАДНОЕ ПО ДЛЯ КИИ

Приказ ФСТЭК России № 239

29.3 Прикладное ПО, планируемое **к внедрению** в рамках создания (модернизации или реконструкции, ремонта) **ЗОКИИ** и обеспечивающее выполнение его функций по назначению, должно соответствовать требованиям **по безопасной разработке программного обеспечения.**

Определены требования:

- по безопасной разработке ПО;
- к испытаниям по выявлению уязвимостей в ПО;
- к поддержке безопасности ПО.

ПРИКАЗ ФСТЭК РОССИИ № 117 (п.50)

Привлечение подрядной организации для разработки ПО

ФСТЭК России

Направляет результаты оценки показателей защищенности и уровня зрелости *(не позднее 5 рабочих дней после их расчета)*

Оператор (обладатель информации)

Предъявляет требования

Проверяет выполнение требований

Подрядная организация (разработчик ПО)

Выполняет требования

ГОСТ Р 56939-2024

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Самостоятельная разработка ПО оператором (обладателем информации)

ФСТЭК России

Направляет результаты оценки показателей защищенности и уровня зрелости *(не позднее 5 рабочих дней после их расчета)*

Оператор (обладатель информации)

Выполняет требования

Производит оценку показателей защищенности *(не реже 1 раза в год)* и уровня зрелости *(не реже 1 раза в 2 года)*

ГОСТ Р 56939-2024

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

ПРИКАЗ ФСТЭК РОССИИ № 239 (п. 29.3-29.4)

Прикладное ПО, планируемое к внедрению в ЗОКИИ

- SCADA
- ГИС/МИС
- ИАС
- Системы диспетчеризации
- EPR-системы
- АБС

Субъект КИИ

Предъявляет требования

Разработчики (производители) прикладного ПО

Выполняет требования

Проверяет выполнение требований

Лицо, выполняющее работы по:
- созданию ЗОКИИ
- модернизации ЗОКИИ
- реконструкции ЗОКИИ
- ремонту ЗОКИИ
- обеспечению безопасности ЗОКИИ

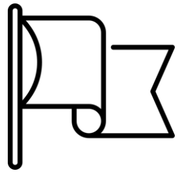
Требования

Требования по РБПО:
- Наличие руководства по РБПО
- Анализ угроз безопасности информации ПО
- Описание структуры ПО на уровне подсистем и результат сопоставления функций ПО и интерфейсов *(для 1 КЗ)*

Требования к испытаниям по выявлению уязвимостей в ПО:
- Статический анализ
- Фаззинг-тестирование
- Динамический анализ *(для 1 КЗ)*

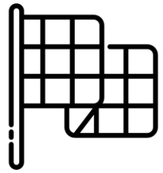
Требования к поддержке безопасности ПО:
- Отслеживания и исправления обнаруженных ошибок и уязвимостей ПО
- Информирование пользователей об уязвимостях ПО, о компенсирующих мерах, о способах обновления ПО
- Оповещение об окончание поддержки ПО *(для 1 КЗ)*

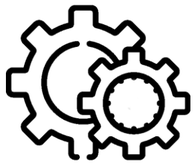
ИЗ КАКИХ ЭТАПОВ СОСТОИТ ВНЕДРЕНИЕ ПРОЦЕССОВ РБПО?



1 марта 2026

Вступает в силу Приказ ФСТЭК России № 117





3-6 месяцев

Организационный этап
(постановка задач, выбор пилотных команд разработки)

3-5 месяцев

Аудит текущих процессов РБПО

Формирование стратегии построения процессов РБПО

12-24 месяцев

Пилотирование и внедрение инструментов РБПО

Формирование Центра компетенций

Документирование практик РБПО

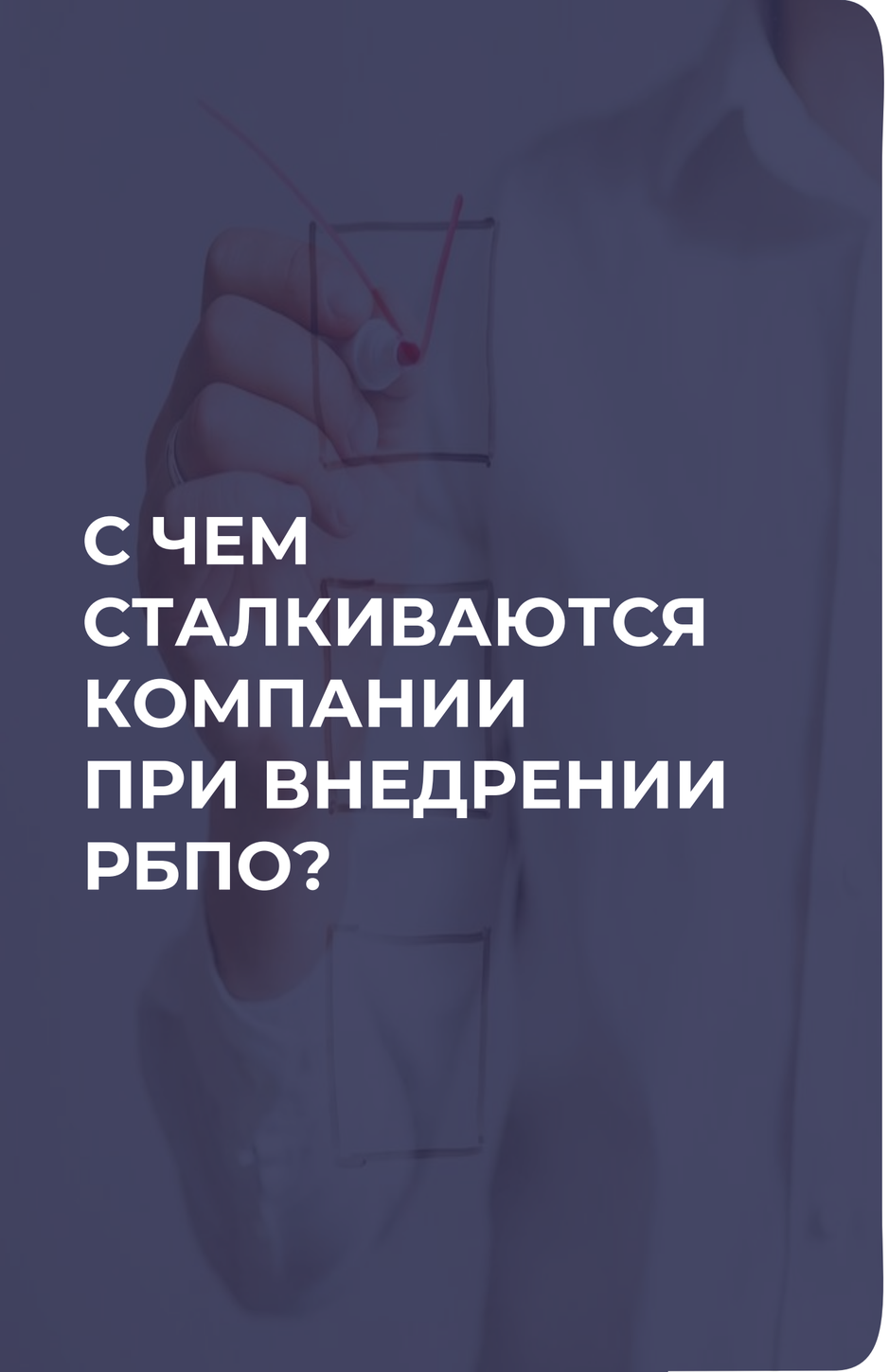
Циклично

Масштабирование
(внедрение практик РБПО во все команды разработки)

Развитие практик РБПО
(интеграция инструментов в CI/CD, расширение применяемых практик)

Регулярные проверки

Периодические аудиты РБПО



С ЧЕМ СТАЛКИВАЮТСЯ КОМПАНИИ ПРИ ВНЕДРЕНИИ РБПО?

- **Руководство** компаний-разработчиков **не видит необходимости** во вложении финансовых и людских ресурсов при формировании и построение РБПО
- **Незрелость команд разработки** в области обеспечения безопасности разрабатываемых приложений
- **Отсутствует понимание** техник и технологий в разработке со стороны специалистов ИБ
- **Отсутствие навыков** управления как организационными, так и техническими аспектами *(либо только «бумажная» безопасность, либо только «практическая»)*
- **Отсутствует понимание** как должны быть модернизированы уже существующие процессы разработки
- У специалистов **не хватает навыков** работы с инструментами безопасной разработки

ПУТИ ВНЕДРЕНИЯ И РАЗВИТИЯ ПРОЦЕССОВ РБПО

Самостоятельная работа	• Постепенное встраивание в уже сформированные процессы компании • Подготовка собственной команды по внедрению и обеспечению безопасной разработки	• Неразборчивость в последовательности встраивания различных практик • Долгое погружение сотрудников в «новый» уклад работы
Привлечение сторонних ресурсов	• На порядок быстрее, чем при самостоятельной процедуре • Внедрение гарантировано работающих практик и методологий • Отсутствие необходимости отвлечения специалистов от профильной деятельности • Обучение специалистов навыкам использования необходимого инструментария	• Медленное развитие внутренних компетенций в области РБПО • Отсутствие собственного опыта борьбы с «проблемными ситуациями»

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Аудит процессов РБПО

РБПО | СЗИ

Сроки выполнения

4 месяца

Результат

Проведен анализ текущего состояния процессов РБПО с оценкой их соответствия требованиям национальных стандартов.

Сформированы качественные рекомендации по совершенствованию процессов РБПО.

Разработчик СЗИ обратился с запросом проведения оценки соответствия выстроенных процессов РБПО

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Выполнение требований безопасности
к прикладному ПО

РБПО КИИ

Сроки выполнения

6 месяцев

Результат

Подготовлена документация, описывающая цикл РБПО. Проведены инструментальные исследования безопасности ПО.

Подготовлено заключение о соответствии реализованных мер в части выполнения требований Приказа ФСТЭК России № 239.

Субъект КИИ, самостоятельно разрабатывающий ПО для значимого объекта КИИ, обратился с запросом выстраивания процессов РБПО

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Аудит безопасности кода

AppSec

Сроки выполнения

5 месяцев

Результат

Проведены исследования ПО методом «белого ящика»:

- Композиционный анализ;
- Динамический анализ, включая фаззинг-тестирование;
- Статический анализ исходного кода.

Выявленные проблемы безопасности приняты во внимание и устранены Заказчиком по переданному детальному отчету.

Компания-разработчик транспортной системы обратился за экспертизой по проверке безопасности ключевого продукта

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Внедрение практик РБПО для разработчиков ПО для его включения на платформу «ГосТех»

РБПО ГИС

Сроки выполнения

7 месяцев

Результат

Реализован проект по внедрению процессов РБПО. Разработан комплект документации.

Проведены инструментальные исследования и подготовлены рекомендации по устранению ошибок, НДВ и уязвимостей.

Подготовлено заключение о соответствии реализованных мер по РБПО.

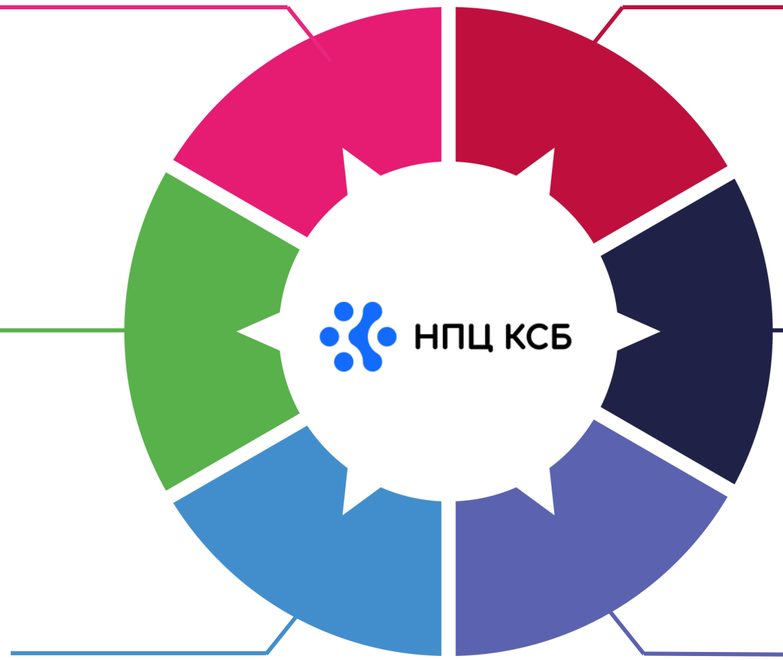
Разработчик ПО обратился с запросом по включению программного продукта к включению в ЕЦП РФ «ГосТех»

ПОСТРОЕНИЕ РБПО СОВМЕСТНО С ЦЕНТРОМ ЭКСПЕРТИЗЫ «НПЦ «КСБ»

Проведение аудита процессов безопасной разработки

Внедрение и развитие процессов безопасной разработки

Проверка соответствия требованиям стандартов

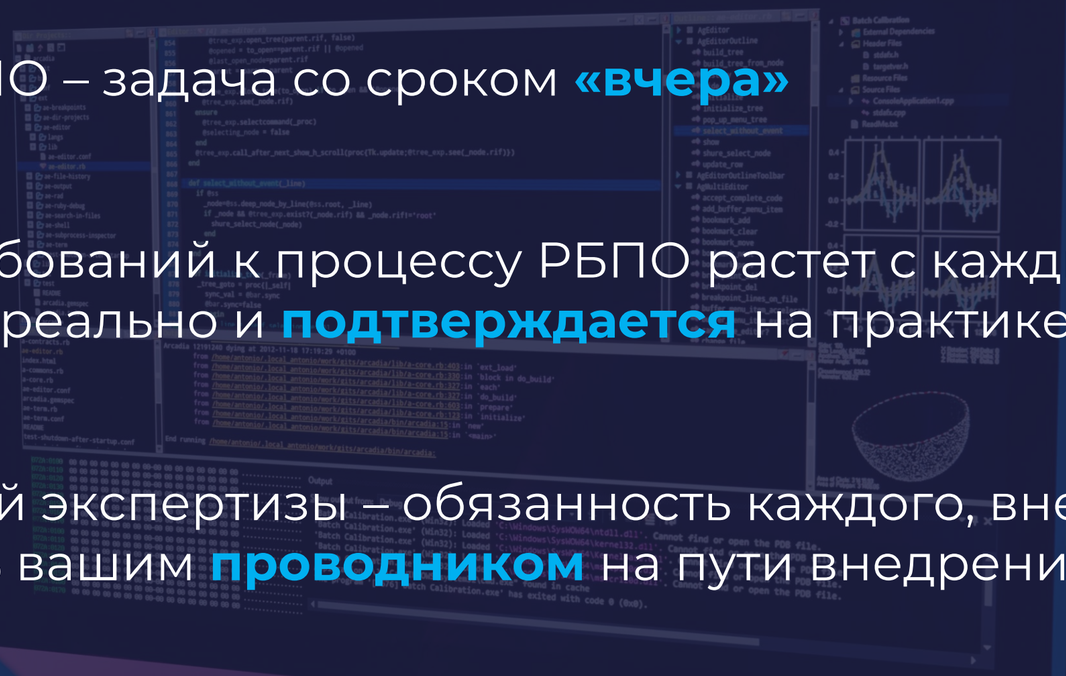


Подготовка документации, описывающей разработку безопасного ПО

Проведение композиционного, статического и динамического анализа, включая фаззинг-тестирование

Сопровождение процесса сертификации «под ключ»

ПОДВОДЯ ИТОГИ



1. Внедрение РБПО – задача со сроком **«вчера»**

2. Количество требований к процессу РБПО растет с каждым днем – их выполнение реально и **подтверждается** на практике

3. Рост внутренней экспертизы – обязанность каждого, внешняя компания – выступает лишь вашим **проводником** на пути внедрения

4. Нет предела совершенству – постоянное развитие процессов безопасной разработки позволит соответствовать **«новым» вызовам**

5. Сторонняя оценка ваших процессов РБПО позволит получить **независимое мнение** о реальном «положении дел»

Что сделать сейчас?

1. Формирование целостной картины по текущему **уровню реализации процессов РБПО** с учетом отраслевых требований

2. Налаживание **производственных практик** (модернизация тулчейна, DevOps, гибкие методологии разработки)

3. Повышение безопасности ПО путем **внедрения инструментов РБПО** с учетом специфики кодовой базы

4. Проведение **анализа безопасности** приложений и сервисов с последующим построением процесса устранения дефектов

НПЦ КСБ

Помогаем вам построить и интегрировать процессы, позволяющие обеспечить безопасность на всех этапах жизненного цикла разработки и эксплуатации ПО

Решение:

- ✓ Аудит процессов РБПО;
- ✓ Подготовка комплекта документации по РБПО;
- ✓ Исследования безопасности приложений и сервисов;
- ✓ Проектирование платформы РБПО;
- ✓ Внедрение инструментальных средств безопасной разработки.

СПАСИБО ЗА ВНИМАНИЕ!

Сделайте первый шаг к новому видению информационной безопасности вместе с нами!

https://npc-ksb.ru/

428000, Чувашская Республика – Чувашия, г. Чебоксары, пр-т Максима Горького, 18 Б, пом. 6

8 800 500 52 33

info@npc-ksb.ru

Раздел по внедрению РБПО НПЦ КСБ

Сайт КСБ-СОФТ