AKTIV.
CONSULTING

Внедрение процесса безопасной разработки программного обеспечения

Безопасная разработка программного обеспечения (БРПО)

Безопасная разработка программного обеспечения (БРПО) — это бизнес-процесс, предусматривающий внедрение практик и подходов обеспечения безопасности в ходе жизненного цикла разработки ПО (SSDLC), состоящий из комплекса организационных и техническим мер.

Что дает бизнесу внедренный процесс БРПО:

Сокращение стоимости разработки за счет стандартизации процессов и инструментов разработки, снижения требований к квалификации разработчиков и быстрой адаптации новых сотрудников.

Повышение стабильности релизов программного продукта за счет улучшения транспарентности (прозрачности) разработки и выявления уязвимостей на самых ранних стадиях разработки.

Снижение затрат и сроков внедрения и повышение управляемости процесса внедрения автоматизированных информационных систем.

Сокращение расходов на обеспечение ИБ, благодаря использованию нативных (встроенных) механизмов безопасности.

Обеспечение непрерывности бизнеса за счет снижения рисков ИБ, связанных с эксплуатацией автоматизированных информационных систем.

Минимизация комплаенс-рисков и соответствие требованиям регуляторов, международным и отраслевым стандартам.

Драйверы внедрения процесса БРПО

	Конечные пользователи			Разработчики ПО и ПАК			
	Финансовые организации	Субъекты КИИ	Корпоративный сектор	Разработчики прикладного ПО	Разработчики СЗИ	Экспортеры ПО и СЗИ	Импортеры ПО и СЗИ
Бизнес-цели	**При собственной разработке:** • снижение совокупной стоимости владения (ТСО) АС/ИС • сокращение стоимости и сроков внедрения АС/ИС **При собственной разработке и/или использовании вендорских решений:** • обеспечение непрерывности бизнеса • минимизация рисков информационной безопасности			**Увеличение объемов продаж за счет:** • возможности выхода на новые клиентские сегменты • дополнительного конкурентного преимущества **Сокращение стоимости разработки и владения продуктом за счет:** • стандартизации процессов и инструментов разработки • повышения стабильности релизов • управляемости процесса внедрения			
Комплаенс	• ГОСТ Р ИСО/МЭК 27034 • ГОСТ Р ИСО/МЭК 15408 • ГОСТ Р 57580.1-2017	Приказ ФСТЭК РФ №239	ГОСТ Р ИСО/МЭК 27034	**ПО для ФО** • ГОСТ Р ИСО/МЭК 15408 • ГОСТ Р ИСО/МЭК 27034 **ПО для КИИ** Приказ ФСТЭК РФ №239	Приказы ФСТЭК РФ №55, №76	• Международные и отраслевые стандарты • ИСО/МЭК 15408 • ИСО/МЭК 27034	Приказы ФСТЭК РФ №76, №55 **ПО для КИИ** Приказ ФСТЭК РФ №239

Консалтинг при внедрении БРПО

Препятствия для внедрения БРПО:

- сложность обоснования для принятия решения по внедрению БРПО
- потребность в специалистах узкого профиля
- страх вмешательства в выстроенные процессы разработки
- отсутствие готовых кейсов и универсальных инструментов для внедрения
- наличие внутреннего «сопротивления» необходимым изменениям
- сложность в трактовке требований регуляторики

Привлечение консультантов позволяет развернуть процесс БРПО за счет:

- гибкого проектного подхода, гарантирующего достижение результата в планируемые сроки и с учетом ресурсных ограничений
- сконфигурированного на старте проекта целевого состояния процесса БРПО, учитывающего индивидуальные особенности и потребности организации

Наши услуги

Мы предлагаем консалтинговые услуги по внедрению процессов безопасной разработки, в том числе:

Проектирование и внедрение процесса БРПО в соответствии с ИБ-требованиями и существующим жизненным циклом разработки

Наши специалисты спроектируют процесс безопасной разработки и подготовят проект по его внедрению, включая разработку ТЭО, составление рекомендаций по внедрению БРПО и создание дорожной карты. Консультанты также помогут обеспечить реализацию организационных и технических мер и проведут контрольные мероприятия для проверки соответствия целевому состоянию процесса БРПО.

Проведение независимой оценки процессов разработки ПО и подготовка рекомендаций по их оптимизации

Внешняя независимая оценка процессов создания ПО позволит найти точки оптимизации за счет внедрения передовых практик и технологий безопасной разработки, а также позволит выстроить сквозные процессы и качественный диалог между бизнесом, разработчиками, ИТ- и ИБ-подразделениями.

Разработка требований по ИБ к информационным системам

Наши специалисты разработают техническое задание по ИБ к автоматизированным информационным системам, ориентируясь на производственные процессы, актуальную модель угроз и требования регуляторов. Консультанты также могут обеспечить сопровождение при создании и внедрении информационной системы, участвовать в приемочном тестировании для оценки соответствия требованиям ИБ.

Проведение статического и динамического анализа уязвимостей, а также тестов на проникновение

Наш практический опыт использования технических средств позволит подобрать оптимальные способы проверки программного кода и проведения тестов на проникновение, регулярность и своевременность которых обеспечит значительное снижение рисков информационной безопасности и операционных рисков в целом.

Приведение к соответствию требованиям регуляторов по безопасной разработке прикладного ПО и средств защиты информации

Собственная уникальная методология позволит сконфигурировать проект по внедрению БРПО, а также целевое состояние процесса безопасной разработки с учетом взаимосвязи различных нормативно-правовых актов, международных и отраслевых стандартов. При этом учитываются не только цели комплаенса, но и бизнес-потребности организации.

Пример схемы внедрения БРПО

Заказчик:
разработчик автоматизированных информационных систем для субъектов КИИ

Цели проекта:
выполнение требований Приказа ФСТЭК РФ №239

Сроки реализации:
от 3-х месяцев

1 этап Обоснование

- Определение целей и задач проекта
- Подготовка ТЭО

Результат: готовое ТЭО

10 рабочих дней

2 этап Аудит

- Обследование текущих бизнес-процессов разработки
- Формирование целевого состояния процесса БРПО в соответствии с требованием регулятора
- Проведение GAP-анализа

Результат: рекомендации по внедрению БРПО

20 рабочих дней

3 этап Разработка дорожной карты

- Ранжирование организационных и технических мер на основе рекомендаций
- Разработка плана перехода и пояснительной записки

Результат: утвержденная дорожная карта

10 рабочих дней

4 этап Внедрение процессов

Внедрение организационных мер (ОРД, ЛНА, обучение) и технических мер (SAST, DAST, Fuzzing)

Результат: функционирующие процессы БРПО

от 10 рабочих дней

5 этап Контроль

Проверка полноты и достаточности внедренных мероприятий для достижения целевого состояния организации

Результат: свидетельства, подтверждающие функционирование БРПО

5 рабочих дней

Итог:
подтверждение соответствия требованию Приказа ФСТЭК РФ №239, относящегося к использованию программного обеспечения на объектах ЗО КИИ.

Почему выбирают нас?

Сокращаем время и затраты на внедрение бизнес-процесса БРПО за счет уникальной методологии и компетенций.

Практикуем гибкий подход при внедрении БРПО, учитываем разные бизнес-цели компаний, этапы зрелости их бизнес-процессов, имеющиеся бюджетные и ресурсные ограничения.

Обладаем знаниями в области организации процессов анализа требований, моделирования угроз, безопасного написания кода, навыками применения статического и динамического анализа, фаззеров, сканеров, имеем опыт проведения пентестов, что позволяет нам внедрять БРПО в компаниях как с водопадной моделью разработки, так и с Agile-подходом.

Помогаем разработать технико-экономическое обоснование для принятия управленческих решений по реализации программы внедрения требований.

Подбираем технические решения, исходя из реальных потребностей заказчика, так как вендоронезависимы.

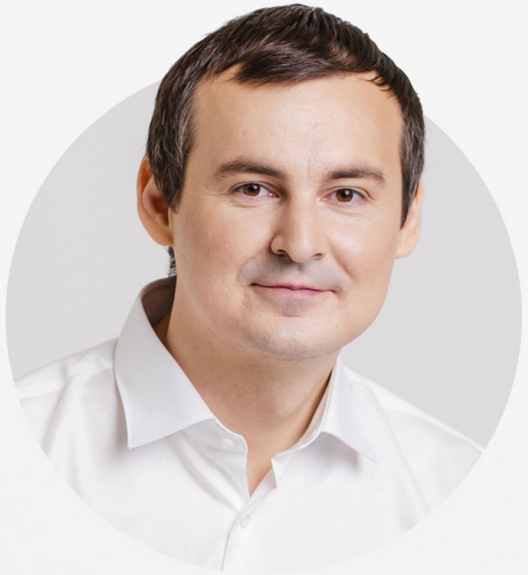
Проводим поэтапное внедрение БРПО, включая обоснование проекта по внедрению БРПО, аудит процессов разработки, формирование целевого состояния, разработку дорожной карты.

Предлагаем услуги, обладающие оптимальным соотношением цены/качества для современного рынка.

Опираемся в своей работе на лучшие мировые и отраслевые практики, являемся профессионалами ИБ рынка, участвуем в разработке нормативных документов.

Контактная информация

AKTIV. CONSULTING



Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting

Олег Симаков

Руководитель направления
по работе с клиентами

simakov@aktiv.consultin