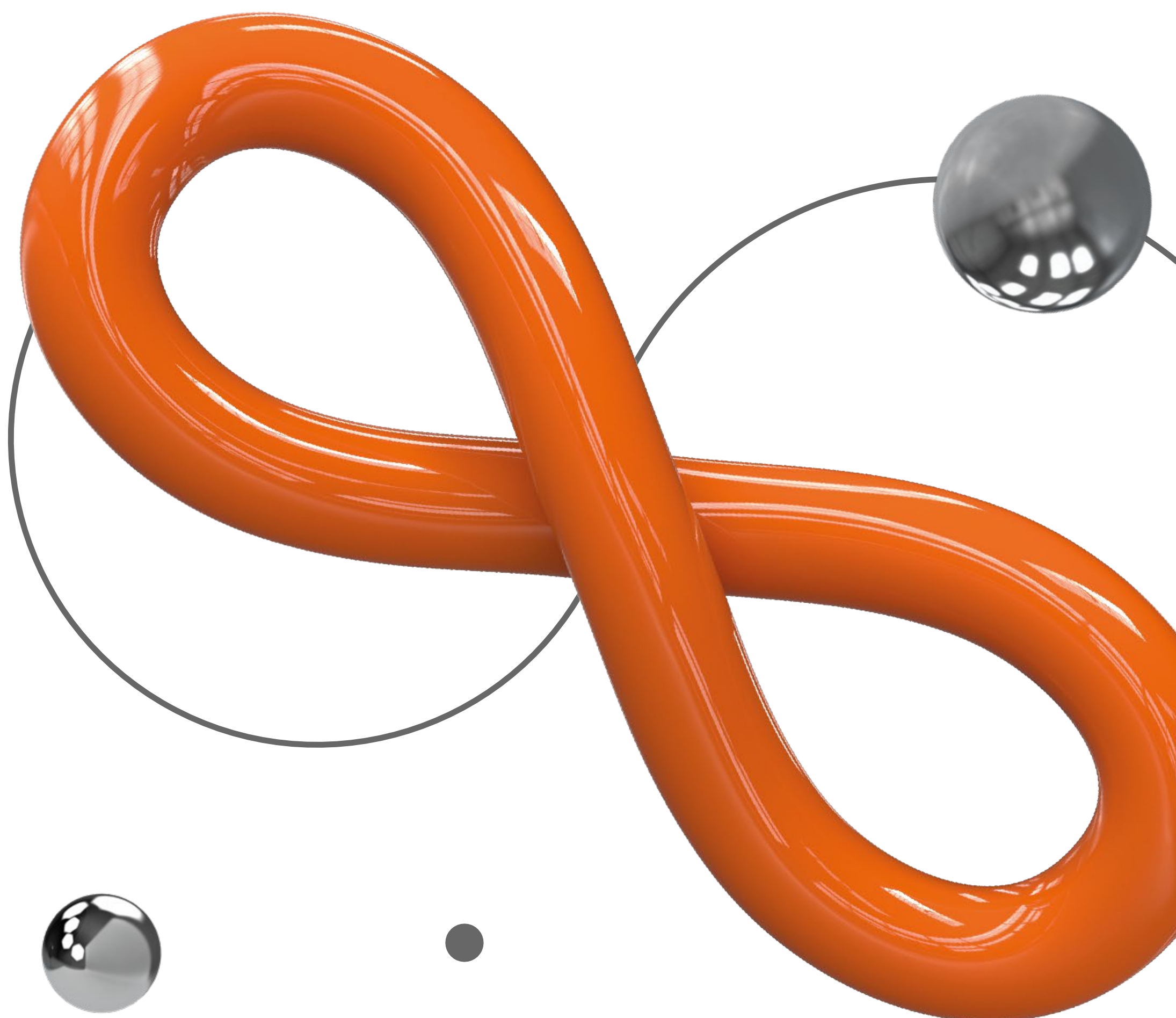
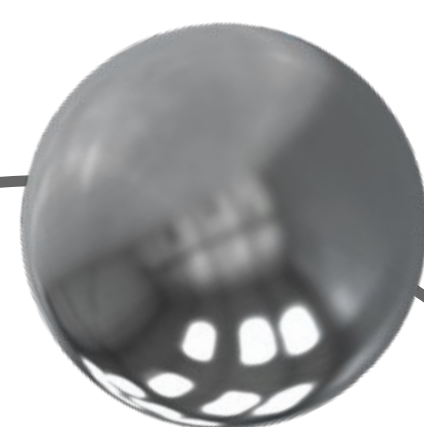
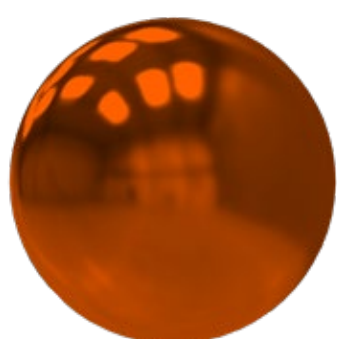
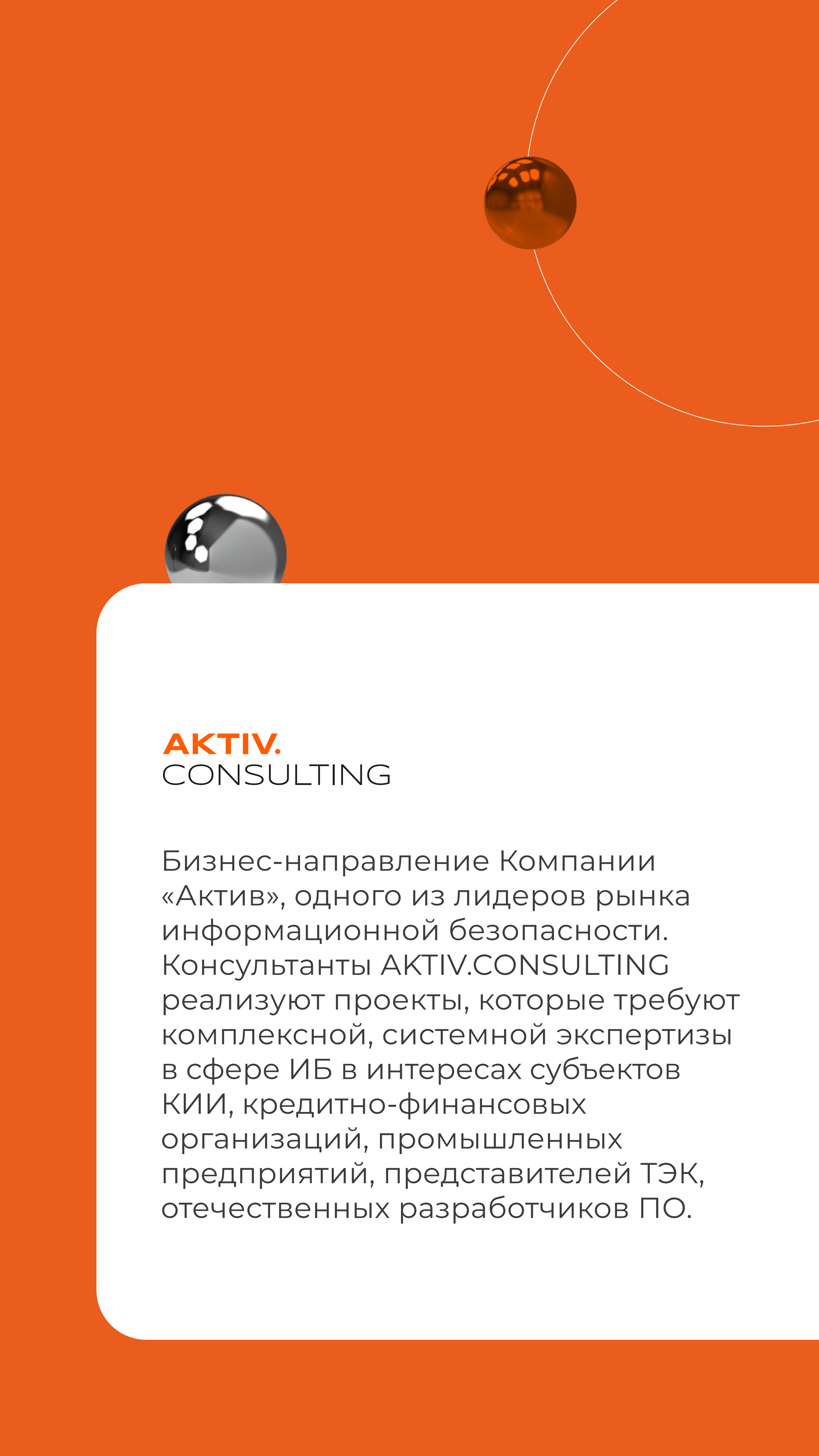


Внедрение процесса **безопасной разработки**





AKTIV. CONSULTING

Бизнес-направление Компании «Актив», одного из лидеров рынка информационной безопасности. Консультанты АКТИВ.CONSULTING реализуют проекты, которые требуют комплексной, системной экспертизы в сфере ИБ в интересах субъектов КИИ, кредитно-финансовых организаций, промышленных предприятий, представителей ТЭК, отечественных разработчиков ПО.

Безопасная разработка программного обеспечения (БРПО)

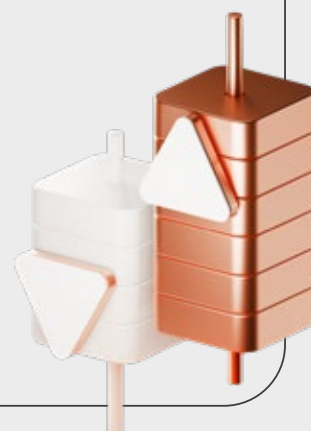
Безопасная разработка программного обеспечения (БРПО) — это бизнес-процесс, предусматривающий внедрение практик и подходов обеспечения безопасности в ходе жизненного цикла разработки ПО (SSDLC). Процесс состоит из комплекса организационных и технических мер.

Внедрение БРПО предоставляет компании следующие ключевые выгоды:

Минимизацию рисков и повышение стабильности релизов за счет улучшения прозрачности (прозрачности) разработки и раннего обнаружения уязвимостей



Сокращение time to market за счет быстрого прохождения проверок безопасности ПО, так как требования в части ИБ учитываются на каждом этапе разработки ПО



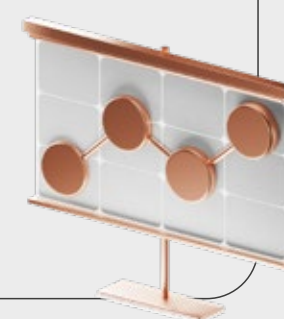
Минимизацию комплаенс-рисков за счет соответствия требованиям регуляторов, а также соблюдение норм международных и отраслевых стандартов



Повышение эффективности онбординга благодаря прозрачному и описанному процессу разработки



Сокращение операционных затрат благодаря стандартизации процессов разработки



Для кого актуально внедрение БРПО?

Ключевые бизнес-цели

Комплаенс

Разработчики ПО в том числе СЗУ

- Сокращение стоимости разработки и владения продуктом
- Сокращение time to market за счет быстрого прохождения проверок безопасности ПО
- Увеличение продаж за счет выполнения требований регуляторов к безопасности ПО

ГОСТ Р 56939-2024

Международные и отраслевые стандарты (ИСО/МЭК 15408, 27034)

Финансовые организации

- Сокращение стоимости разработки и владения продуктом, а также сроков внедрения
- Минимизация рисков ИБ и обеспечения непрерывности бизнеса
- Выполнение требований регулятора

Приказ ФСТЭК России № 239

ГОСТ Р 56939-2024

ГОСТ Р ИСО/МЭК 27034

ГОСТ Р ИСО/МЭК 15408

ГОСТ Р 57580.1-2017

Субъекты КИУ

- Выполнение требований регулятора
- Сокращение стоимости разработки и владения продуктом, а также сроков внедрения
- Минимизация рисков ИБ

Приказы ФСТЭК России № 239

ГОСТ Р 56939-2024

ГОСТ Р ИСО/МЭК 27034

ГОСТ Р ИСО/МЭК 15408

С какими трудностями сталкиваются команды разработки при внедрении БРПО:



Нехватка экспертизы

Потребность в узкопрофильных специалистах



Дефицит практики

Отсутствие универсальных кейсов, а также готовых методик и инструментов, адаптированных к специфике бизнеса



Тяжесть аргументации

Сложность обоснования для принятия решения о необходимости инвестиций во внедрение БРПО



Неготовность к изменениям

Наличие внутреннего сопротивления внутри команды необходимым изменениям



Риск нарушений

Опасения вмешательства в уже выстроенные процессы разработки и релизов



Сложность трактовки требований регуляторов и их практического применения

Привлечение консультантов позволяет развернуть процесс БРПО за счет:



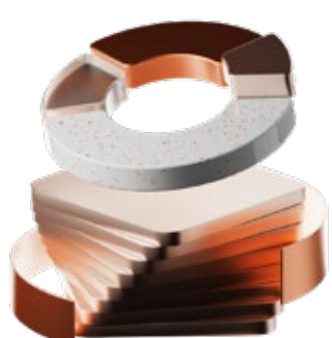
Практического опыта внедрения требований по безопасной разработке в компаниях с разной отраслевой спецификой и бизнес-процессами



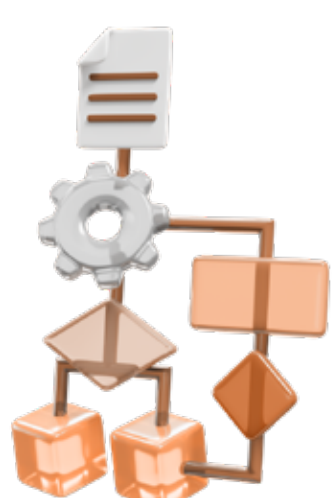
Комплексного подхода к внедрению процесса безопасной разработки, включающего внедрение как организационных, так и технических мер



Применения лучших отечественных и мировых практик построения процесса безопасной разработки



Использования **гибкого проектного подхода**, гарантирующего результат в установленные сроки и с учетом ресурсных ограничений



Центра технической экспертизы, включающего специалистов, обладающих собственной уникальной технической базой, позволяющей проводить качественные проверки безопасности ПО и ОУД4

Наши услуги

Мы предлагаем полный спектр консалтинговых услуг по внедрению процессов безопасной разработки, в том числе:

Интеграция процесса БРПО в жизненный цикл разработки с учетом требований ИБ

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 организационно-технических мер и проведут контрольные мероприятия для проверки соответствия целевому состоянию процесса БРПО и органичной интеграции в существующий жизненный цикл разработки.



Независимая экспертиза процессов разработки и рекомендации по их улучшению

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.



Проведение анализа уязвимости ПО и ОУД4

Собственная уникальная техническая база и методология в сфере использования технических средств позволит подобрать оптимальные способы проверки программного кода. Систематическое и грамотно спланированное проведение этих процедур позволяет выявить существующие уязвимости и существенно минимизирует угрозы информационной безопасности.

Разработка технических требований к разработке ПО

Наши специалисты помогут разработать техническое задание для вашей команды разработки или подрядчика, разрабатывающего программное обеспечение по вашим требованиям. Задание будет включать актуальные для вашей компании модели угроз, а также требования со стороны ИБ и ИТ-служб и регуляторные требования. Кроме того, консультанты могут обеспечить сопровождение при приемочном тестировании для оценки соответствия требованиям ИБ разработанного ПО.

Комплаенс в области безопасной разработки 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

Сроки реализации: выполнение рассчитывается индивидуально для каждого проекта



1 этап | Разработка ТЭО

- ☑ Определим цели и задачи проекта внедрения
- ☑ Проанализируем влияние процессов безопасной разработки на бизнес-цели организации
- ☑ Подготовим технико-экономического обоснования (ТЭО) проекта

Результат:

разработанное ТЭО для обоснования старта проекта

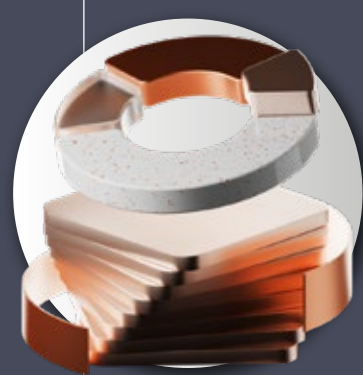


2 этап | Разработка целевого состояния

- ☑ Сформируем цели и задачи проекта внедрения (если не было этапа 1)
- ☑ Подберем методологии и инструменты построения процессов безопасной разработки
- ☑ Опишем и картируем процессы безопасной разработки

Результат:

карта целевого состояния процесса безопасной разработки ПО



3 этап | Оценка соответствия требованиям регулятора

- ☑ Обследуем текущие бизнес-процессы разработки
- ☑ Сформируем целевое состояние в соответствии с требованиями регуляторов
- ☑ Проведем GAP-анализ
- ☑ Разработаем рекомендации, включая организационные и технические меры

Результат:

для тех, кому актуален комплаенс

рекомендации по приведению процессов безопасной разработки ПО к соответствию требованиям регулятора



4 этап |

Разработка дорожной карты по внедрению процесса безопасной разработки

- ✓ Проведем приоритезацию организационных и технических мер на основе рекомендаций
- ✓ Проанализируем взаимные связи и влияние данных мер
- ✓ Разработаем календарный план перехода к целевому состоянию

Результат:

дорожная карта перехода к целевому состоянию процесса безопасной разработки ПО



5 этап |

Внедрение процессов безопасной разработки ПО в соответствии с дорожной картой

- ✓ Внедрим организационные меры, включая разработку руководства по безопасной разработке ПО
- ✓ Внедрим технические средства (SAST, DAST, Fuzzing и т.п.)
- ✓ Проведем консультации по работе с инструментальными средствами
- ✓ Проведем консультации выполнения проверок безопасности ПО

Результат:

функционирующие процессы безопасной разработки ПО



6 этап |

Проверка полноты и достаточности внедренных мероприятий для достижения целевого состояния организации

- ✓ Проведем контрольные мероприятия по проверке соответствия целевому процессу
- ✓ Организуем сбор свидетельств действующего процесса безопасной разработки ПО

Результат:

свидетельства, подтверждающие функционирование БРПО

Почему выбирают нас?



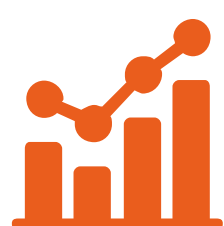
Сокращаем время и затраты на внедрение бизнес-процесса БРПО за счет уникальных методик и экспертизы во внедрении БРПО



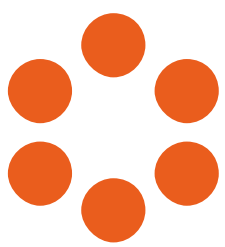
Обладаем экспертизой от анализа угроз, внедрения **security by design** (SAST, DAST, fuzzing) до пентестинга. Это позволяет нам работать как с водопадной моделью разработки, так и с Agile-методологиями



Вендоронезависимый подбор решений помогает выбрать технические решения, которые наилучшим образом соответствуют реальным потребностям заказчика



Реализуем комплекс услуг, где цена и качество находятся в идеальной пропорции, отвечающей актуальным требованиям рынка



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



Помогаем обосновать инвестиции, подготавливая технико-экономическое обоснование для принятия взвешенных управленческих решений по реализации программы внедрения требований



Реализуем комплексную интеграцию БРПО с полным циклом работ, включая обоснование проекта, аудит процессов разработки, формирование целевого состояния, разработку дорожной карты



В основе нашей работы лежат **лучшие мировые и отраслевые практики.** **Наша команда** состоит из **профессионалов** рынка информационной безопасности, которые непосредственно участвуют в разработке нормативных документов

Контакты

info@aktiv.consulting

115088, Москва,
ул. Шарикоподшипниковская 1,
Бизнес-центр «Прогресс-Плаза»

