Безопасная разработка в жизненном цикле ПО

Балансируем характеристики

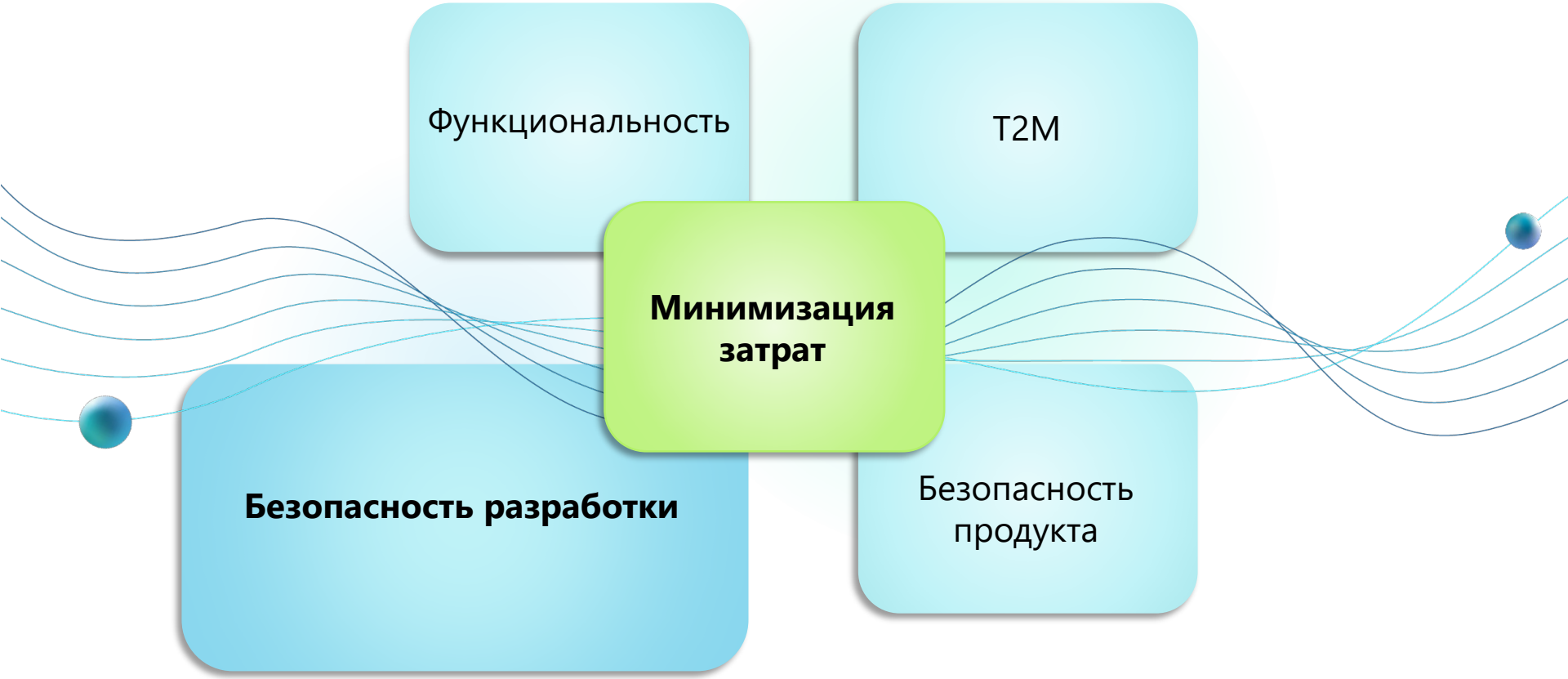
Калугина Анастасия

Руководитель направления безопасной разработки и инфраструктуры

infotecs

Проблематика
(что хотим достичь)

Бизнес потребности



Ключевые проблемы

Цели и задачи зачастую противоречат друг другу

Нет готовых методологий для разрешения конфликтов

Необходимо совместить несовместимое

Совместить несовместимое

Миф или реальность?

Введение
(как разрабатываем)

Жизненный цикл продукта

РБПО на жизненном цикле

Как будем оценивать?

Отталкиваясь от целей:

- Реализация функциональных характеристик
- Обеспечение безопасности продуктов
- Оптимизация трудозатрат

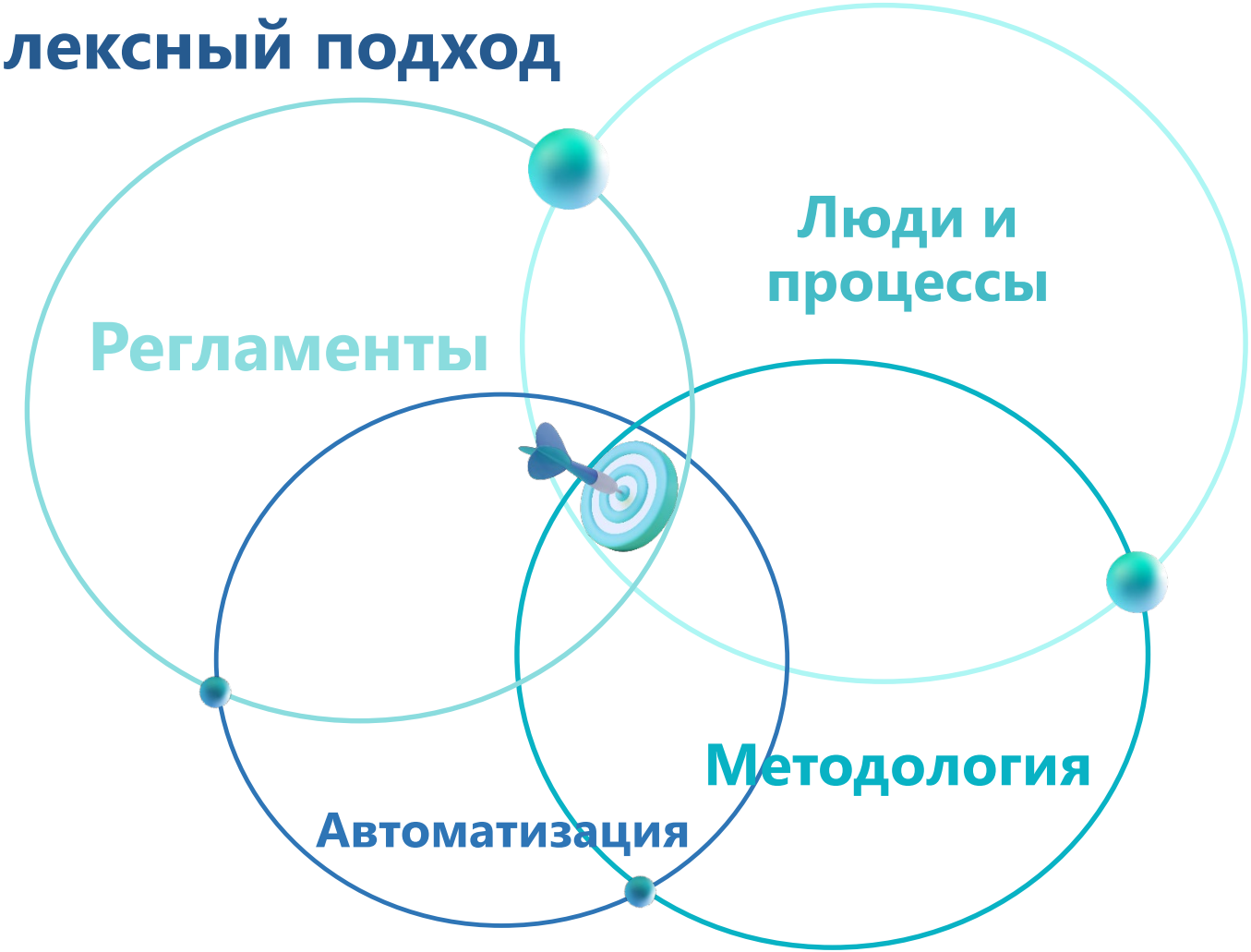
Подход

(как разрабатываем продукты)

Из чего состоит разработка

1. Регламенты
   - Политики
   - Положения
   - Регламенты
2. Люди и процессы
   - Процессы управления
   - Процедуры
   - Должностные инструкции
   - Ресурсы (сотрудники, техника и т.д.)
3. Методология
   - Инструкции
   - Рекомендации
   - Шаблоны
   - Чек-листы
4. Автоматизация
   - Сервисы анализа уязвимостей
   - Механизмы встраивания в процесс сборки
   - Механизмы управления уязвимостями
   - Мониторинг уязвимостей

Комплексный подход



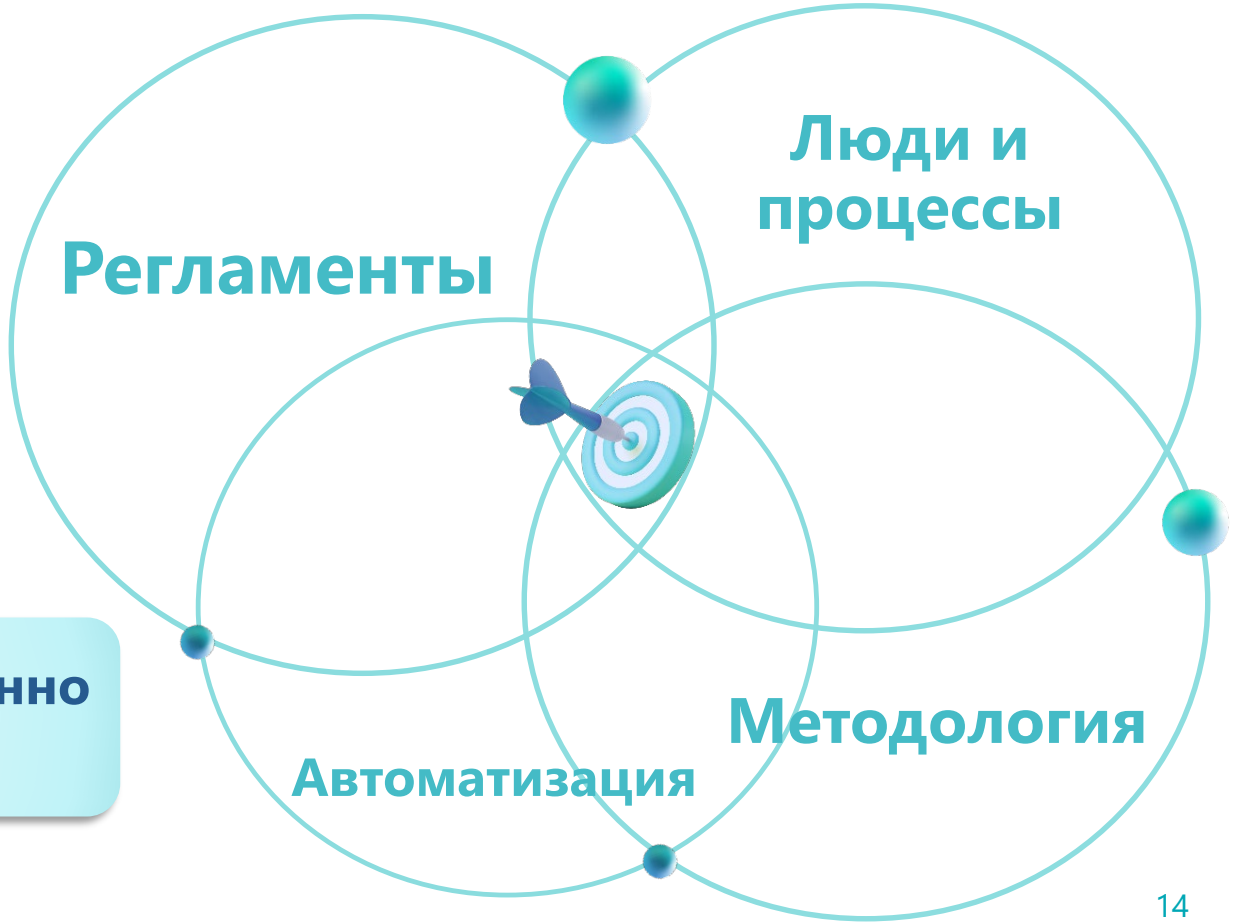
Вернемся к нашим целям

- Реализация функциональных характеристик
- Обеспечение безопасности продуктов
- Оптимизация трудозатрат

Методология оптимизации трудозатрат

infotecs

Готовый механизм не существует



Развиваем одновременно все механизмы

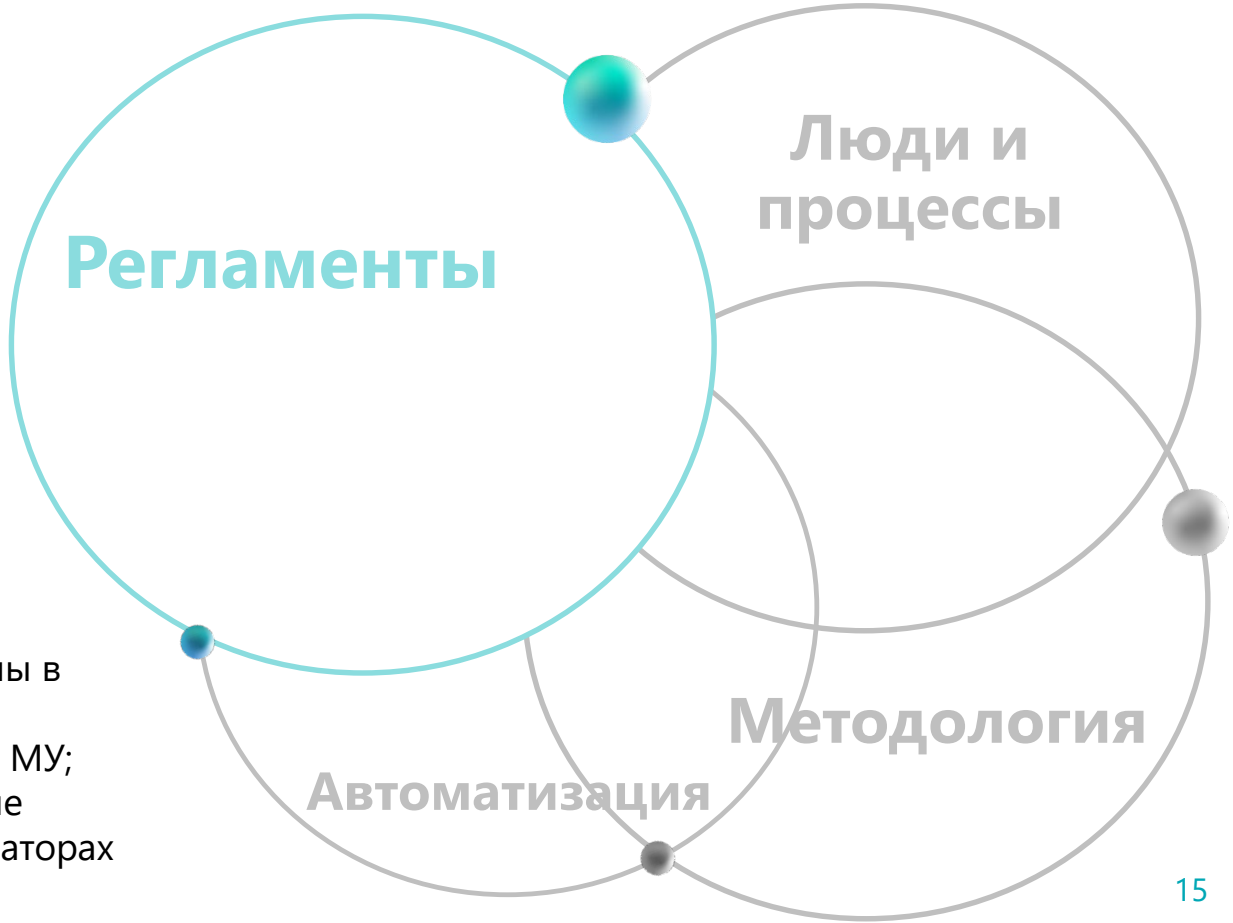
Оптимизация затрат. Регламенты

Регламентация:

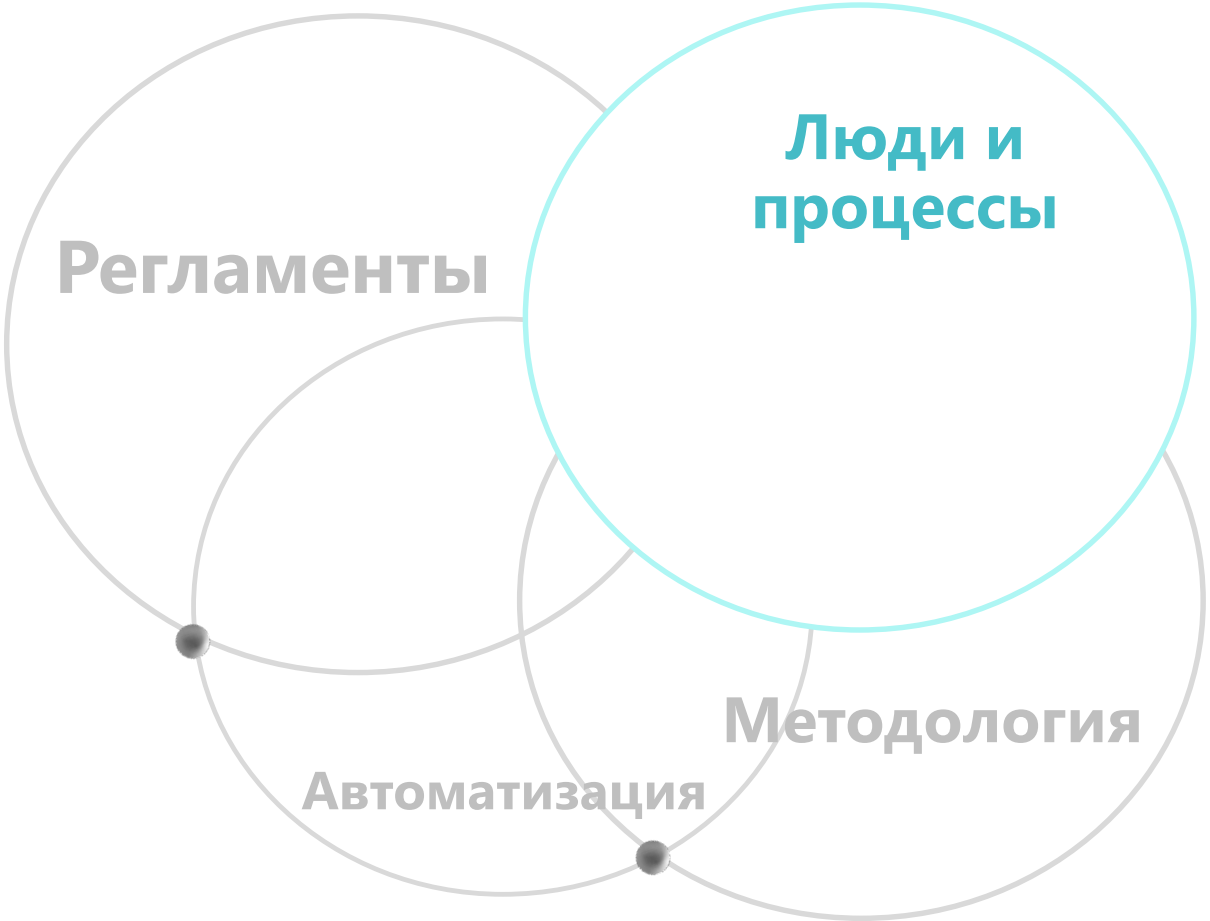
- ✓ Регламентация всех этапов ЖЦ ПО
- ✓ Регламентация всех процессов разработки
- ✓ Переиспользование лучших практик

Оптимизация практик:

- ✓ Базовый набор требований ИБ для продуктов;
- ✓ Принципы и паттерны в проектировании;
- ✓ Поверхность атаки в МУ;
- ✓ Критичные и высокие уязвимости в анализаторах



Оптимизация затрат. Люди и процессы



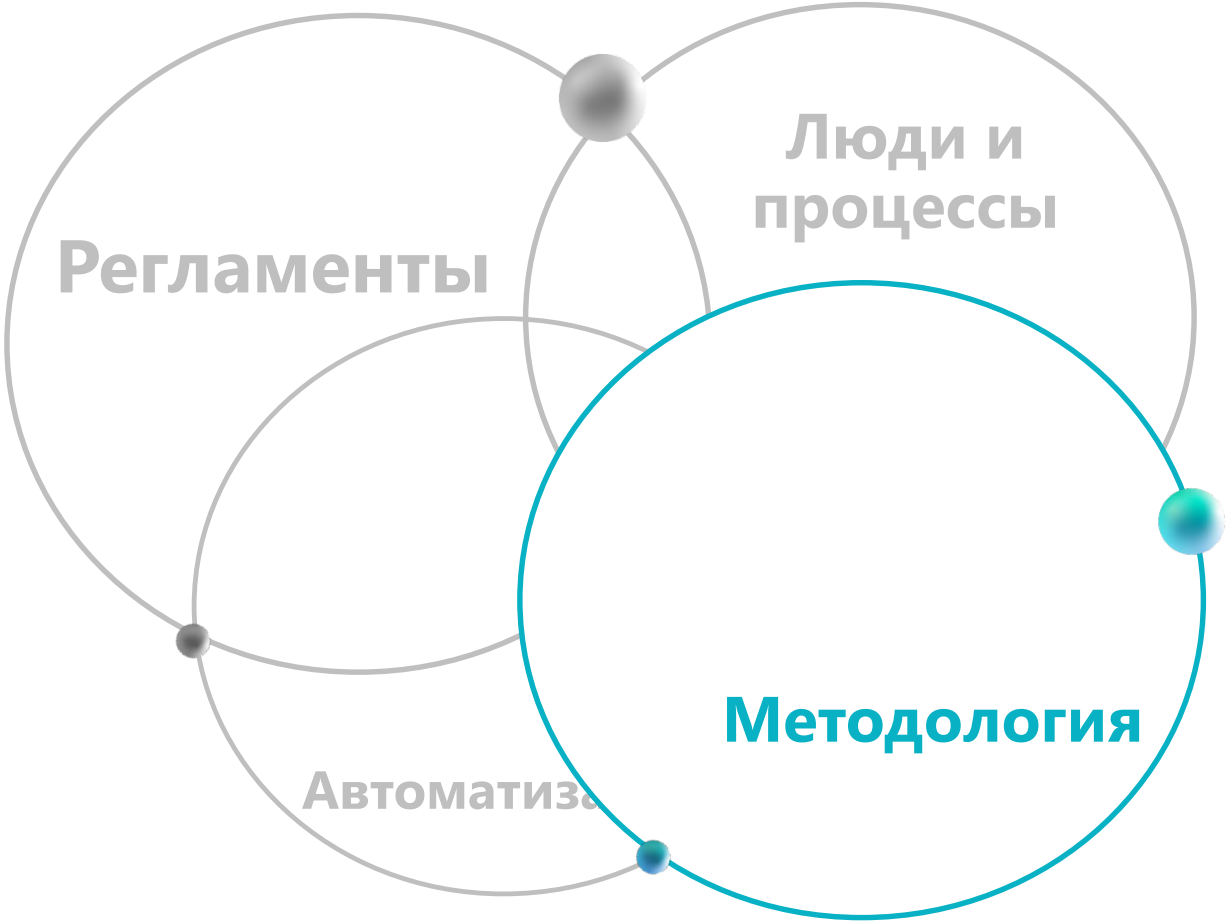
Процессы:

- ✓ Планирование трудозатрат;
- ✓ Контроль выполнения;
- ✓ Контроль корректности выполнения;
- ✓ Мониторинг прогресса

Люди:

- ✓ Эксперт – как точка входа
- ✓ Закрепление экспертов за проектами
- ✓ Активное участие экспертов на всех этапах разработки
- ✓ Обучение

Оптимизация затрат. Методология



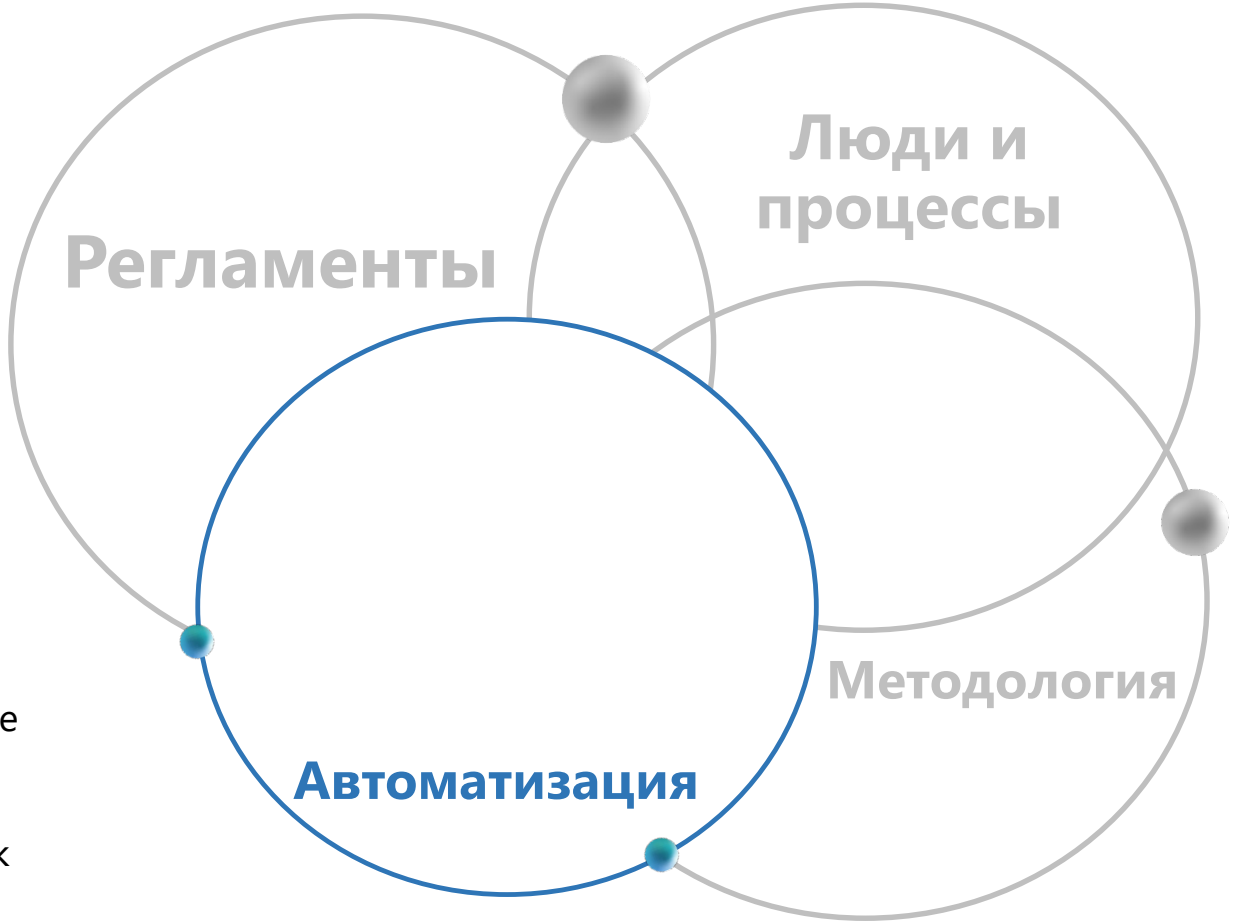
Рекомендации:

- ✓ Детальные низкоуровневые инструкции
- ✓ Рекомендации и описание лучших практик
- ✓ Шаблоны для практик и отчетов
- ✓ Чек-листы для самопроверки

Оптимизация затрат. Автоматизация

Максимальная автоматизация:

- ✓ Автоматизация практик в сборочном конвейере;
- ✓ Автоматизация сохранения уязвимостей;
- ✓ Автоматизированное отслеживание;
- ✓ Авто-проверки выполнения практик



Краткий чек-лист

Балансируем отталкиваясь от целей

Задачи для достижения целей:

- Доработка регламентации
- Доработка процессов
- Обеспечение механизмами
- Обучение участников процессов
- Максимальная автоматизация
- Поэтапное развитие

Результат

Оцениваем результат

Отталкиваясь от целей:

- Функциональные характеристики реализованы
- Трудозатраты на выполнение практик уменьшаются
- Уязвимости в продукте уменьшаются со временем

Что получаем?

Комплексную безопасность продукта

Минимизация трудозатрат на обеспечение безопасной разработки

Дополнительные выгоды

Минимизируем сопротивление команд
при внедрении практик безопасной разработки

Б**о**льший интерес в части профессионального развития

И пара цифр для примера

Наши достижения за год

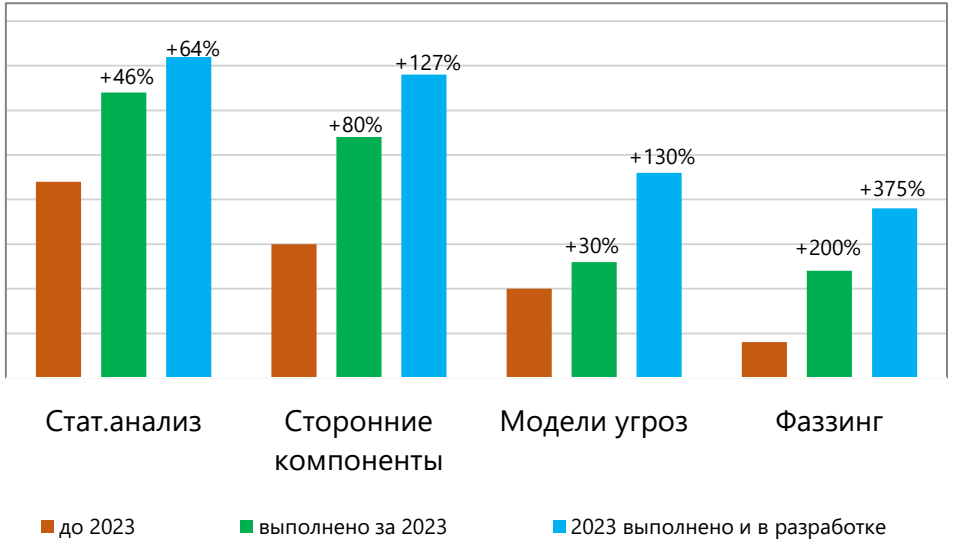
Снижение трудозатрат по практикам безопасной разработки:

- Статический анализ – **на 20%**
- Анализ сторонних компонентов – **на 43%**

Несколько цифр для примера

Наши достижения за год

Повышение % и глубины выполнения
практик безопасной разработки:



Спасибо за внимание!

Калугина Анастасия

Руководитель безопасной разработки и инфраструктуры

e-mail: akalugina@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363

infotecs

Ответы на вопросы

https://vk.com/infotecs_news

https://t.me/infotecs_news