

Подводные камни внедрения принципов разработки безопасного программного обеспечения

Шаньгин Дмитрий

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА
ЦЗИ ООО «КОНФИДЕНТ»
(ТЕХНИЧЕСКИЙ ДИРЕКТОР)

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU





Многие думают, что внедрение практик безопасной разработки в IT – это как круиз на океанском лайнере, роскошный и безопасный

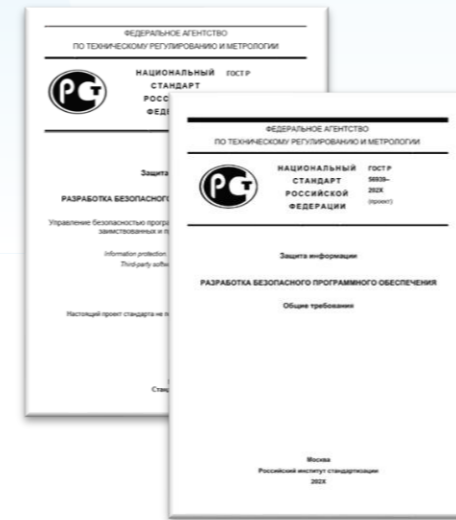


Однако на самом деле это больше похоже на рафтинг по бурной реке с порогами – опасно, но возможно



Сложности выбора инструментов

Разнообразие инструментов



Практически невозможно найти идеальный по соотношению:

- цена
- выполнение функций РБПО
- удовлетворение требований регулятора

Совместимость и интеграция



Важно учитывать совместимость выбранных инструментов между собой и с уже используемыми системами разработки

Обучение и адаптация



Переход на новые инструменты требует времени и усилий для обучения сотрудников и адаптации к новым рабочим процессам

Практические сложности внедрения



Сопротивление сотрудников

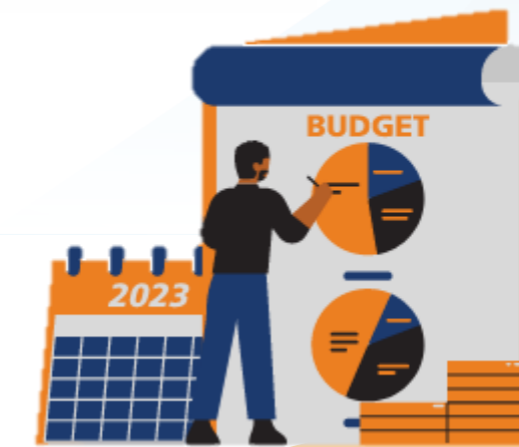
сотрудники могут быть против внедрения новых инструментов из-за страха изменений или дополнительной нагрузки на рабочий процесс



Непредвиденные проблемы

при внедрении новых инструментов может возникнуть:

- несовместимость с текущей инфраструктурой;
- сложность в настройке и использовании;
- уход вендоров из России.



Финансовые ограничения

инструменты могут быть дорогими в поддержке и лицензировании, что создает финансовые сложности для компании. Особенно подписочные модели дистрибуции

А как в ЦЗИ «Конфидент»?

Выбор инструментов в соответствии с требованиями регулятора

Обучение сотрудников на базе ИСП РАН



Внутреннее обучение сотрудников компании

Создание общей базы знаний для сохранения и усовершенствования практик

Дефицит специалистов

Рынок труда

- сфера IT становится все более конкурентной
- дефицит специалистов в области разработки ПО и ИБ
- зарплатные ожидания не соответствуют уровню компетенций

1

Быстрое развитие технологий

Постоянное развитие технологий требует постоянного обновления знаний и навыков у специалистов. Наблюдается нехватка качественных образовательных программ

2

Отток специалистов

Кадровый голод специалистов по специальности DevSecOps составляет 75-90%

3



Сложности формирования команд

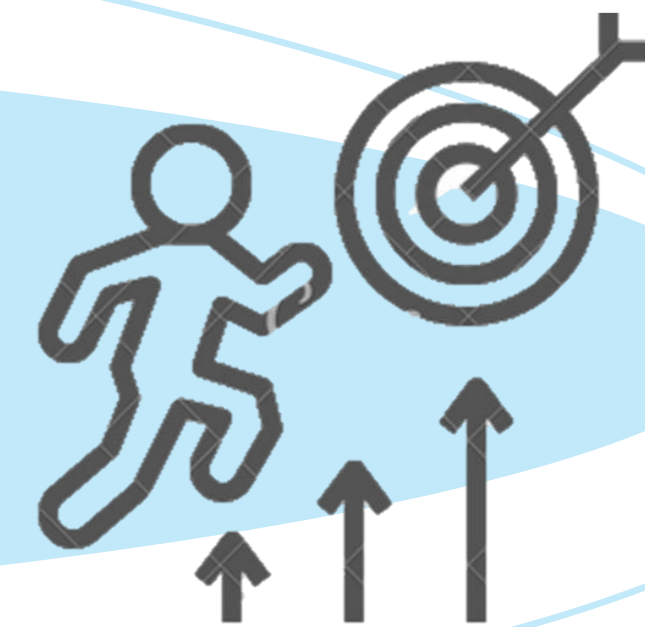
1. Несоответствие компетенций

соискатели часто склонны преувеличивать свои компетенции. Это касается как студентов, так и возрастных специалистов



2. Управление и мотивация

необходимо эффективно управлять командой, учитывая индивидуальные особенности каждого специалиста, а также мотивировать их на достижение общих целей



3. Проблема кадрового резерва

- сотрудники не взаимозаменяемы
- обладают уникальными навыками и компетенциями
- потеря сотрудника означает приостановку процессов в компании



Выбор ЦЗИ «Конфидент»

1

Ставка на студентов ведущих вузов страны
ИТМО, ГУАП и пр.

2

Стажировки по всем направлениям деятельности

- разработка
- тестирование
- информационная безопасность

3

Комфортная процедура онбординга

как первый глоток горячего кофе утром — бодрящая и мгновенно вовлекающая в рабочий процесс

4

Гибридный режим работы

сотрудники видят друг друга в офисе, а не только онлайн

5

Культивация участия сотрудников в городских и международных спортивных мероприятиях



Участие в Центре верификации ядра Linux

Вносим вклад в совместный анализ ядра Linux
(статический и динамический)

Отправляем «патчи» ядра Linux

Участвуем в совершенствовании статических и
динамических анализаторов



LINUX



Спасибо за внимание!



Шаньгин Дмитрий

**ЗАМЕСТИТЕЛЬ ДИРЕКТОРА
ЦЗИ ООО «КОНФИДЕНТ»
(ТЕХНИЧЕСКИЙ ДИРЕКТОР)**

EMAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

