ОДИН В ПОЛЕ НЕ ВОИН
ИЛИ
КАК НЕ ЗАПЛУТАТЬ НА ПУТИ ВНЕДРЕНИЯ SDL

Степан Харитонов

Начальник сектора безопасной разработки и сертификации ООО «КСБ-СОФТ»

КСБ-СОФТ

Системный интегратор
в сфере информационной
безопасности и импортозамещения
информационных технологий

Входим в ГК «Кейсистемс»

Лицензиат ФСТЭК России

Лицензиат ФСБ России

Проекты компании курируют опытные
ИБ-специалисты, аккредитованные
по международным сертификациям
OSCP, CISM, CGEIT и CISA.

80+

регионов
внедрения

4000+

реализованных
проектов

С ЧЕГО МЫ НАЧИНАЛИ И КУДА ДВИЖЕМСЯ

НПЦ КСБ

Внедрили процессы SDL для разработчика

Сопровождали разработчика при сертификации СЗИ

информационные технологии КЕЙСИСТЕМС

Масштабировали процессы SDL во всей ГК

Уже помогаем нашим клиентам с выстраиванием процессов SDL

ПОЧЕМУ СТОИТ ЗАДУМАТЬСЯ

28 000+

уязвимостей обнаружили
по итогам 2023 года
(число растёт с каждым годом)

до 78%

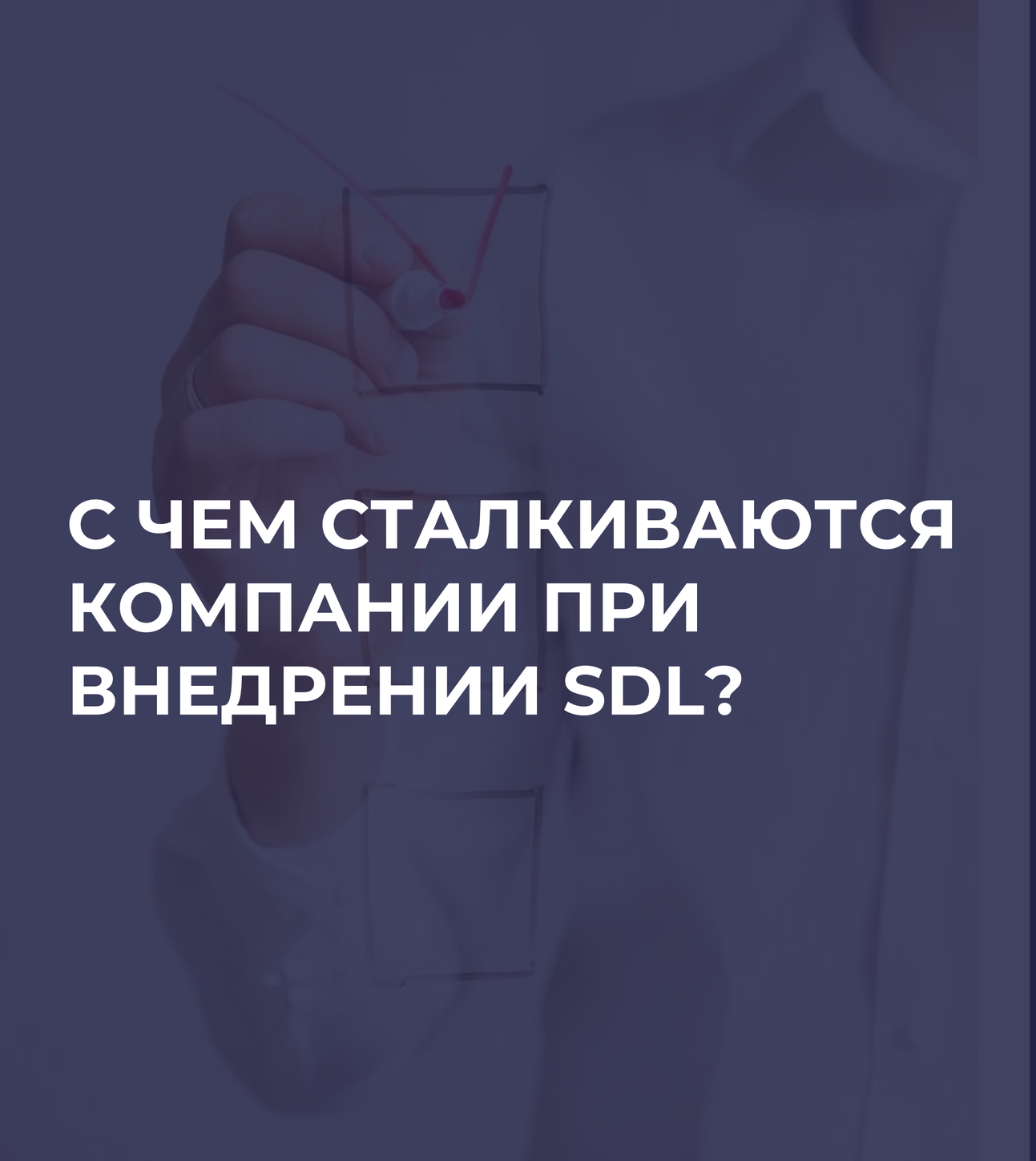
доля открытого исходного
кода в ПО в некоторых
отраслях

80%

веб-приложений
имеют хотя бы 1
опасную уязвимость

Высокая

стоимость устранения
уязвимостей
на поздней стадии



С ЧЕМ СТАЛКИВАЮТСЯ КОМПАНИИ ПРИ ВНЕДРЕНИИ SDL?

- **Нет специалистов**, которые будут заниматься внедрением и обеспечением SDL
- **Отсутствует понимание** как должны быть модернизированы уже существующие процессы разработки
- У специалистов **не хватает навыков** работы с инструментами SDL

Три столпа безопасной разработки – процессы, технологии и люди!

ПУТИ ВНЕДРЕНИЯ И РАЗВИТИЯ SDL

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

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Внедрение процессов
безопасной разработки

SDL

Сроки выполнения

9 месяцев

Результат

Выстроен процесс безопасной разработки в соответствии с действующими стандартами и нормативными документами ФСТЭК России. Подготовлена документация, описывающая цикл разработки безопасного программного обеспечения.

Российский разработчик ИТ-решений для бизнеса обратился с запросом выстраивания SDL-процессов

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Аудит цикла разработки ПО

AppSec

Сроки выполнения

4 месяца

Результат

Выполнены работы по обследованию процессов разработки, сформированы рекомендации по приведению цикла разработки в защищенное исполнение. Разработана дорожная карта по выстраиванию SDL-процессов.

Компания, занимающаяся заказной разработкой программных продуктов, обратилась с вопросом проверки качества цикла разработки

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Аудит процессов SDL

SDL

Оценка соответствия

Сроки выполнения

5 месяцев

Результат

Реализован проект по обследованию процессов разработки безопасного программного обеспечения, проведена оценка соответствия требованиям национальных стандартов.
Сформированы качественные рекомендации по совершенствованию SDL-процессов.

Разработчик АСУ ТП обратился с запросом в проведении оценки эффективности существующих процессов SDL

ПРАКТИЧЕСКИЕ ПРИМЕРЫ

Задача

Анализ защищенности транспортной системы

AppSec

Сроки выполнения

3 месяца

Результат

Проведен экспертный анализ программного обеспечения методом «white-box».
Выявленные проблемы безопасности приняты во внимание и устранены Заказчиком по переданному детальному отчету.

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

ПОСТРОЕНИЕ БЕЗОПАСНОЙ РАЗРАБОТКИ СОВМЕСТНО С ЦЕНТРОМ ЭКСПЕРТИЗЫ КСБ-СОФТ

01 Внедрение и развитие процессов безопасной разработки

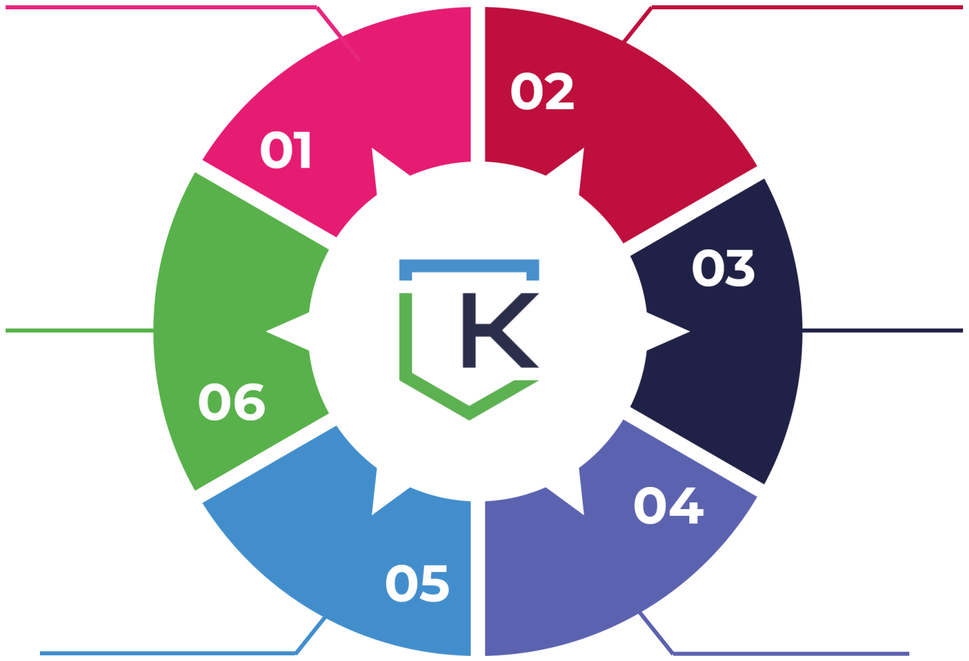
02 Разработка документации, описывающую разработку безопасного программного обеспечения

03 Проверка соответствия требованиям стандартов

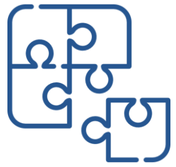
04 Проведение аудита процессов (безопасной) разработки

05 Обеспечение безопасности приложений во время их выполнения

06 Проведение композиционного, статического и динамического анализа, функционального и фаззинг-тестирования



ПОЧЕМУ МЫ?



Обладаем глубоким пониманием в организации процессов, и готовы предложить наилучшие подходы и технологии в области SDL

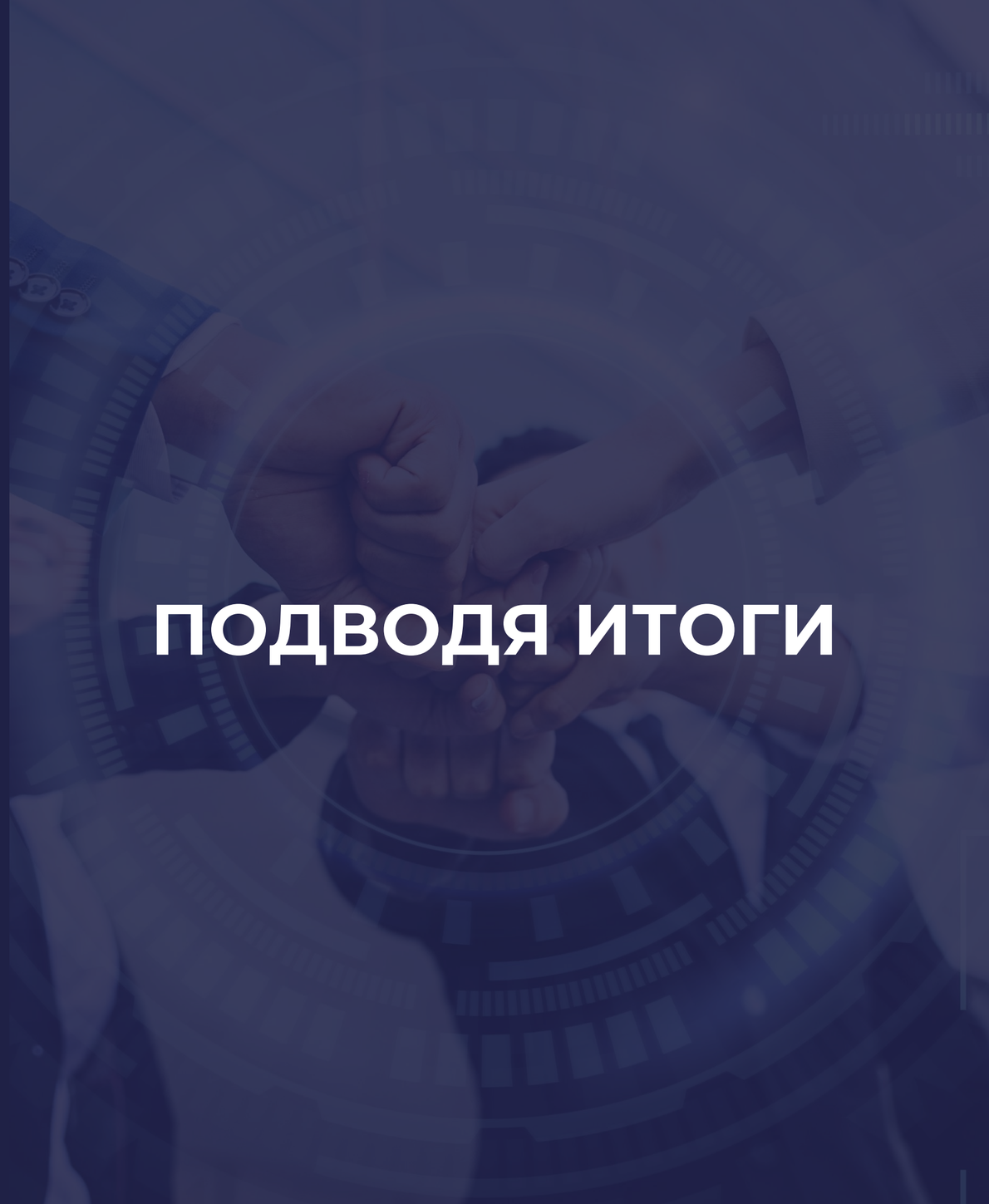
Являемся активными участниками сообщества Центра компетенций в области разработки безопасного программного обеспечения, созданного под эгидой ФСТЭК России и ИСП РАН

Проводим работу в рамках Центра исследований безопасности системного программного обеспечения

Обучаем и развиваем будущее поколение специалистов по безопасности приложений в рамках деятельности Лаборатории системного программирования и безопасной разработки ЧГУ им. И.Н. Ульянова

ПОДВОДЯ ИТОГИ

1. Внедрение SDL – задача со сроком **«вчера»**
2. Количество требований к процессу SDL 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 SDL-процессов позволит получить **независимое мнение** о реальном «положении дел»



СПАСИБО ЗА ВНИМАНИЕ!

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

ПРИГЛАШАЕМ ВАС ПОСЕТИТЬ НАШ СТЕНД №E50!

ОСТАЛИСЬ ВОПРОСЫ?

ksb-soft.ru

+7 (8352) 322-322

info@ksb-soft.ru