Сервисный подход в построении процессов РБПО: миф или реальность?

Степан Харитонов

Руководитель направления безопасной разработки ООО «КСБ-СОФТ»

КСБ-СОФТ

Системный интегратор
в сфере информационной
безопасности и импортозамещения
информационных технологий

Входим в ГК «Кейсистемс»

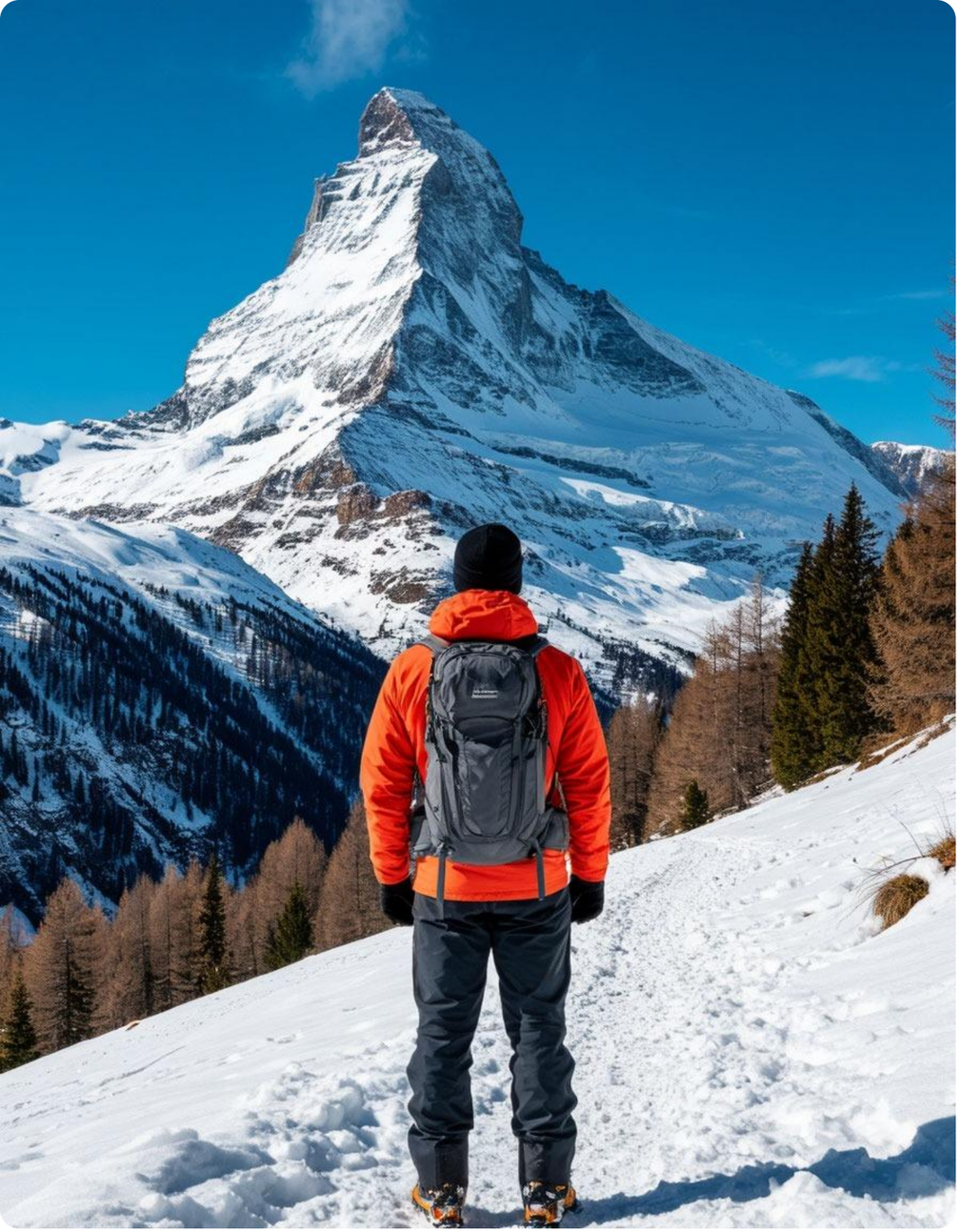
Лицензиат ФСТЭК России

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?

- Более 75 разрабатываемых программных продуктов
- Многообразие подходов и практик к процессам разработки в ГК «Кейсистемс»
- Отсутствие единых стандартов безопасной разработки
- Дефицит кадров в сфере РБПО в регионе
- Отсутствие компетенций у разработчиков в части создания безопасного ПО
- Разрозненные проверки качества и безопасности кода

Наш путь к безопасной разработке

Отсутствуют четкие зоны ответственности между командами разработки

Процессы зависят от отдельных сотрудников: после увольнения знания потеряны

«Хаос при реализации»: централизовано не задокументированы реализуемые процессы

Нет системного подхода к обработке результатов тестирования безопасности

Частые исправления багов отвлекают разработчиков от реализации новых идей

Разработчики воспринимают безопасность как дополнительную нагрузку

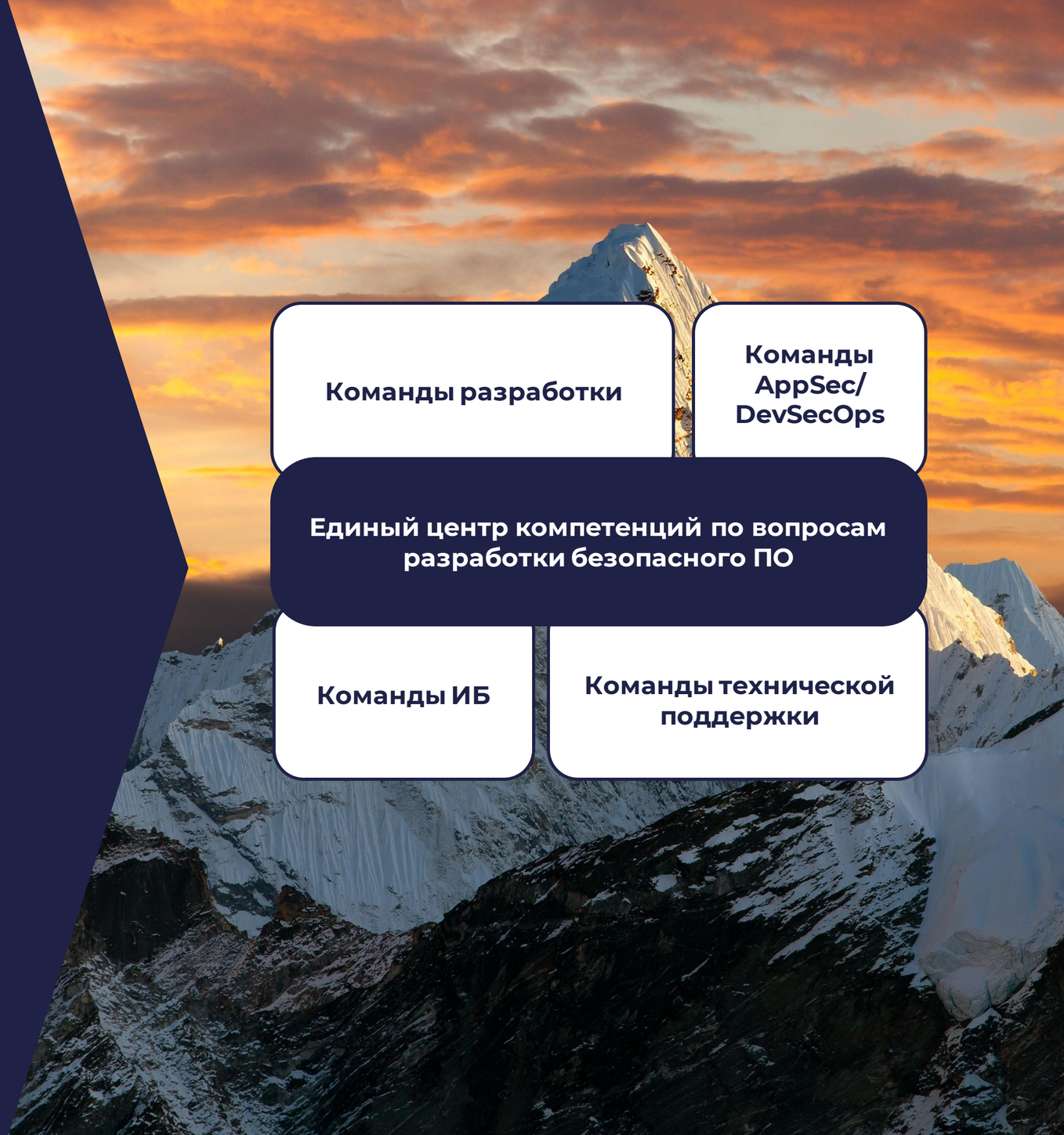
Отсутствует «системность»: хаотичное внедрение практик на уровне отдельных команд

Команды разработки

Команды AppSec/ DevSecOps

Команды ИБ

Команды технической поддержки



Команды разработки

Команды AppSec/ DevSecOps

Единый центр компетенций по вопросам разработки безопасного ПО

Команды ИБ

Команды технической поддержки

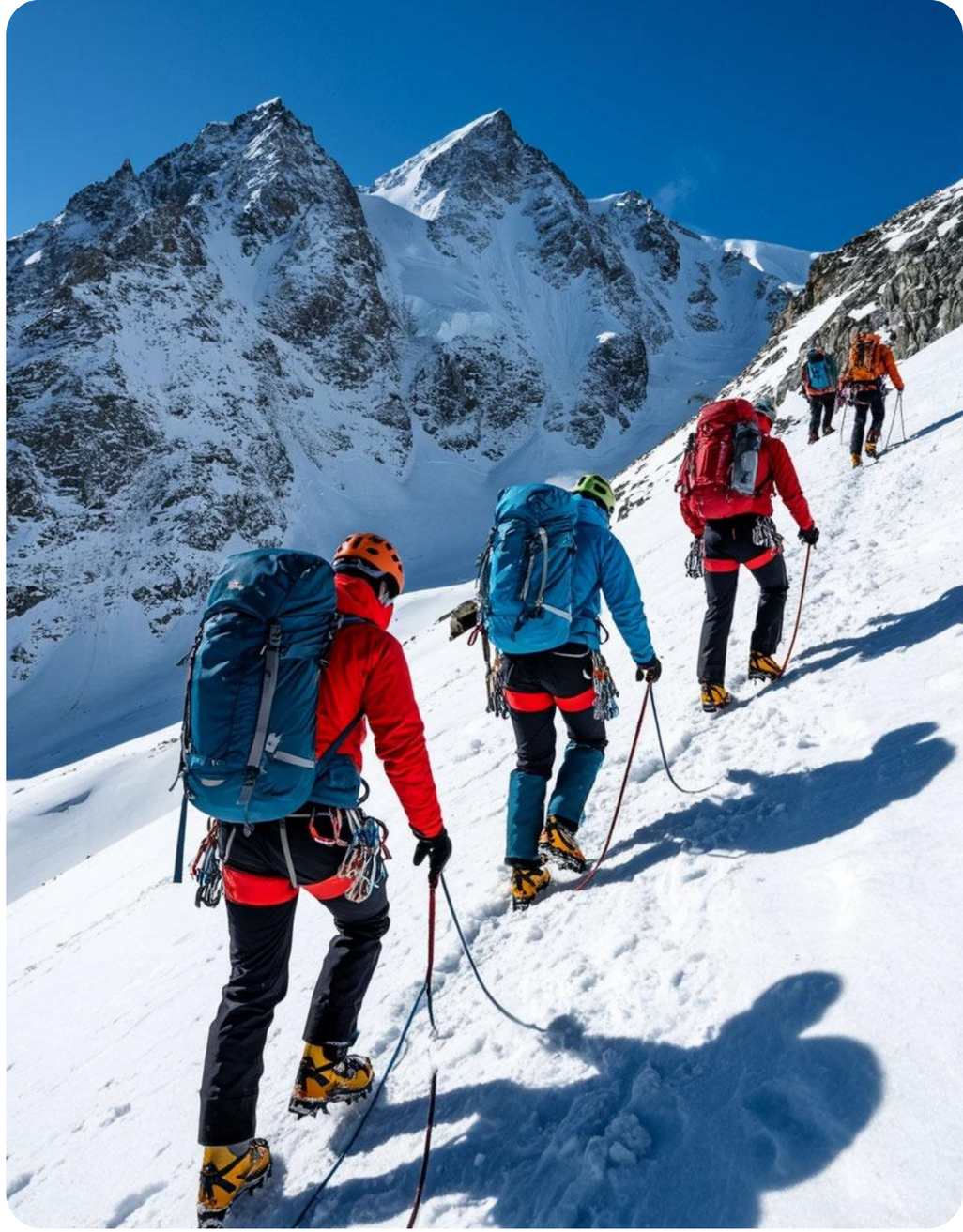
Центр компетенций по РБПО: помогаем создавать качественное и безопасное ПО

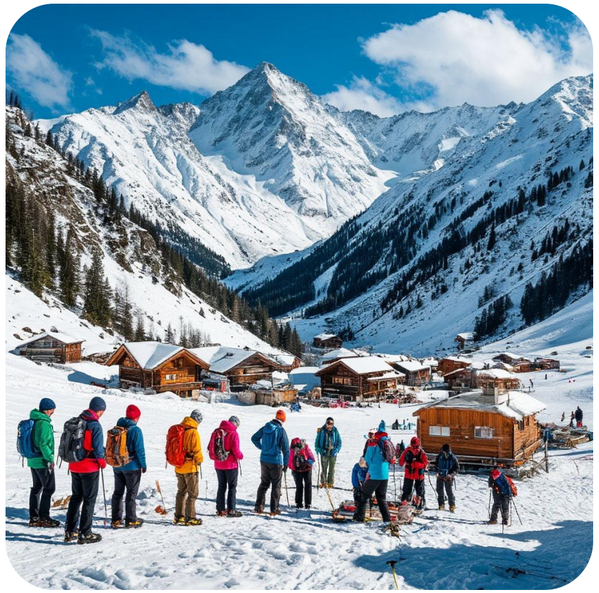
Обеспечение безопасности продуктов ГК «Кейсистемс»

Центр компетенций по РБПО

- **Домен «Построение процессов РБПО»**
- **Домен «Сертификация СЗИ»**
- **Домен «Исследования качества и безопасности программных продуктов»**
- **Домен «Образование и наука»**

Консультации по обеспечению безопасности для внешнего рынка

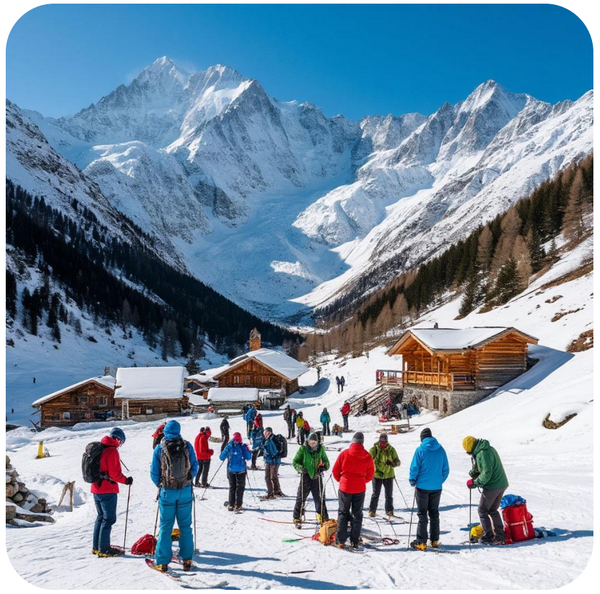




Домен «Построение процессов РБПО»

Ключевые задачи

- Оценка текущего состояния процессов разработки с точки зрения качества и безопасности
- Проектирование и адаптация процессов РБПО с учетом особенностей принципов разработки и применяемых технологий
- Консультирование разработчиков по вопросам безопасного кодирования
- Участие в процессе управления требованиями ИБ к ПО, контроль за их выполнением
- Помощь в проектировании безопасной архитектуры, построение МУ и определение ПА
- Регламентирование деятельности команд разработки с учетом предъявляемых требований по РБПО



Методическое сопровождение при реализации механизмов безопасности в составе ПО

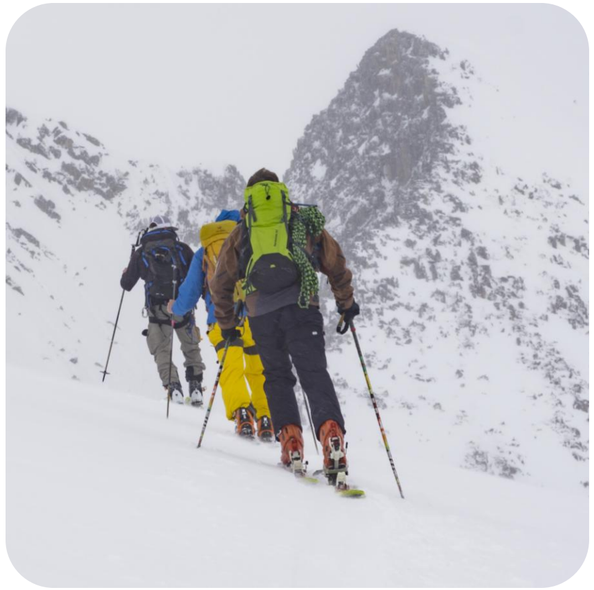
Разработка комплекта сертификационной документации на ПО

Практическая помощь при проведении испытаний ПО по ВУ и НДВ с учетом требований ФСТЭК России

Организация взаимодействия с участниками сертификации (ФСТЭК России, орган по сертификации, испытательная лаборатория)

Консультационная поддержка по вопросам организации прохождения сертификации по линии ФСТЭК России

Домен «Сертификация СЗИ»



Ключевые задачи

Подбор и внедрение инструментальных решений для исследования безопасности ПО

Анализ исходного кода ПО (статический анализ, композиционный анализ, поиск секретов, ревью кода, фаззинг-тестирование)

Обеспечение проверок ПО в режиме эксплуатации (динамический анализ, функциональное тестирование ИБ, пентест и пр.)

Управление уязвимостями: разметка, оценка рисков и приоритизация, сопровождение при их устранении

Контроль безопасности компонентов с открытым исходным кодом, входящих в состав ПО

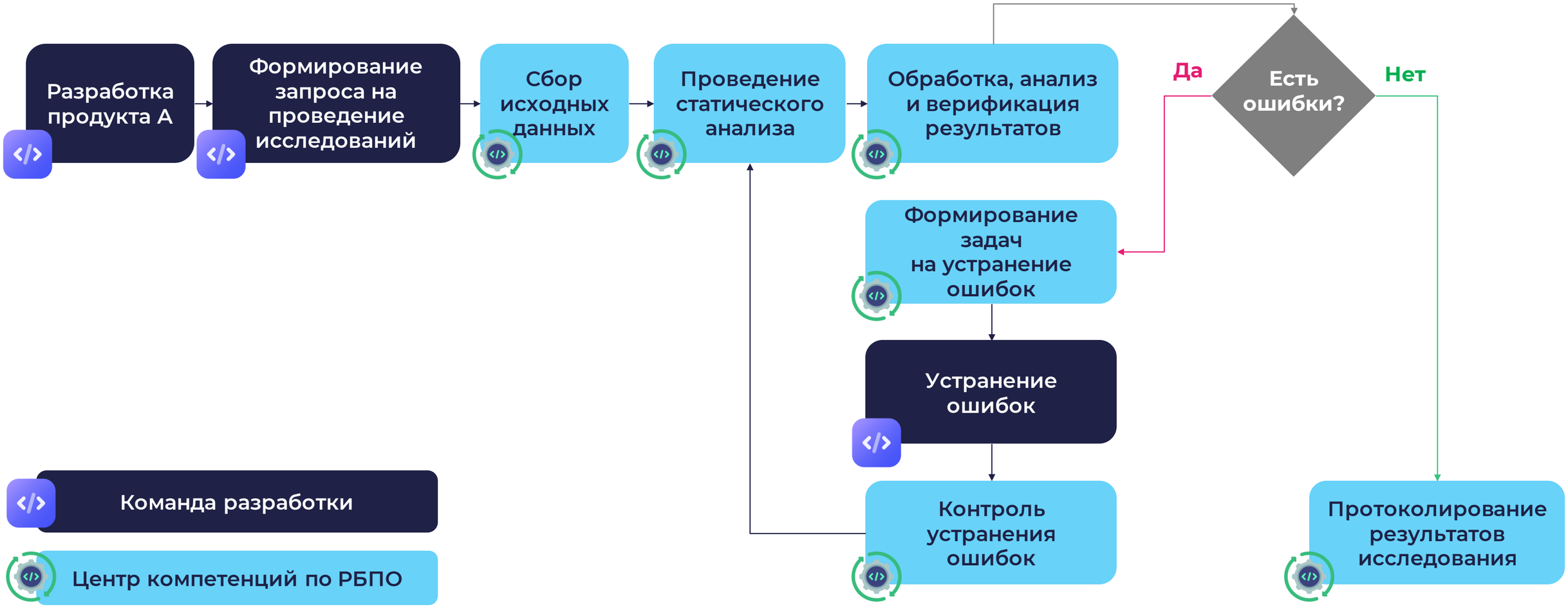
Приемочные испытания очередных версий ПО до момента их выпуска и передачи пользователям

Домен «Исследования качества и безопасности программных продуктов»

Ключевые задачи

Практический кейс

Задача: Проведение инструментальных исследований безопасности в части статического анализа исходного кода продукта А для прохождения сертификации СЗИ по линии ФСТЭК России



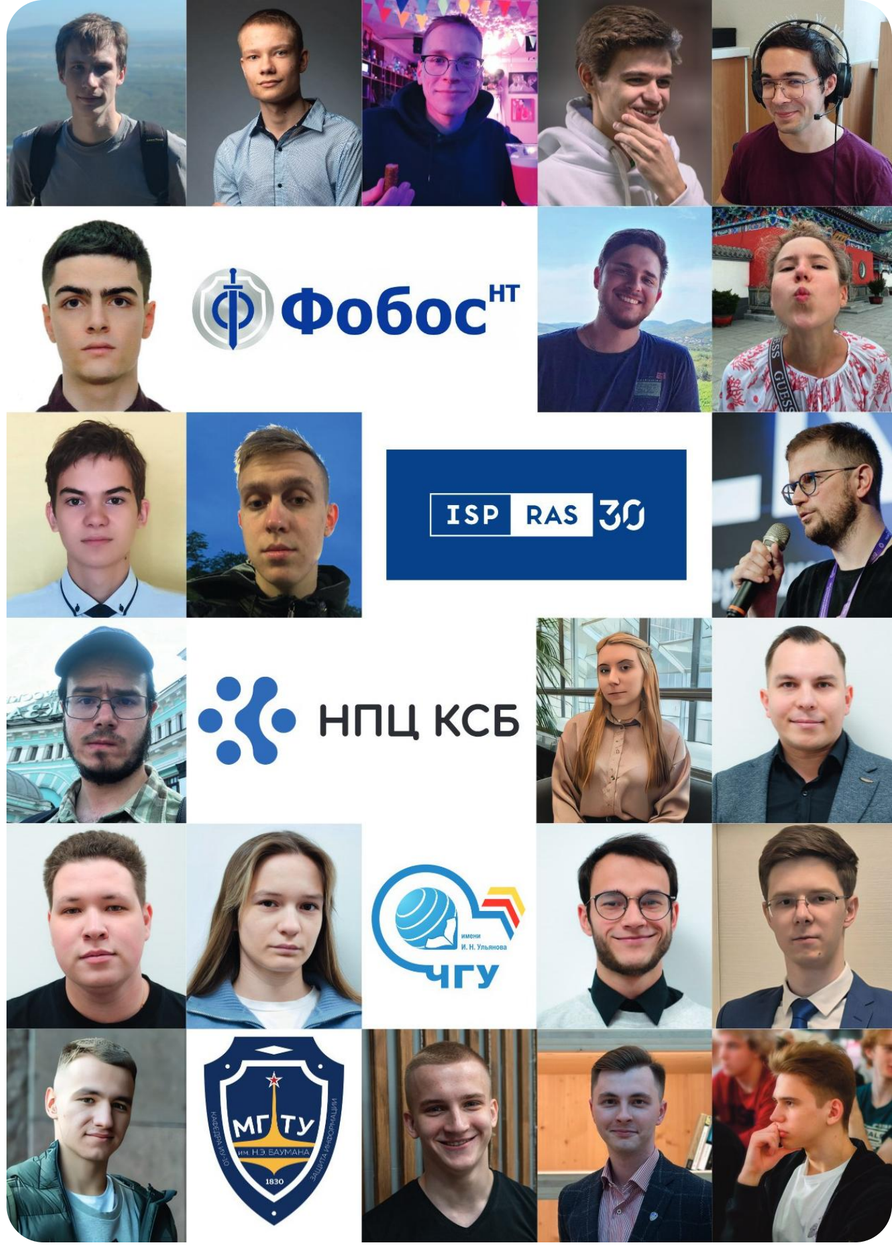
Исследование безопасности системного ПО

>4000
разметок статического анализа

60+
исправлений принято в upstream

>45
фаззинг-целей разработано

30+
исправлений на рассмотрении



В фокусе исследования

keycloak, openjdk, activemq, apacheds, dotnet (aspnetcore, runtime), libvirt, libvirt-exporter, qemu, gnutls, openssh, snmpd, postgresql, nginx, angie и пр.

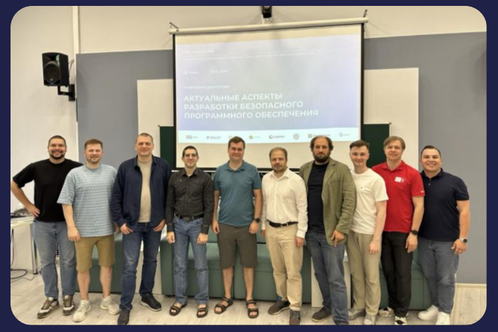
Домен «Образование и наука»

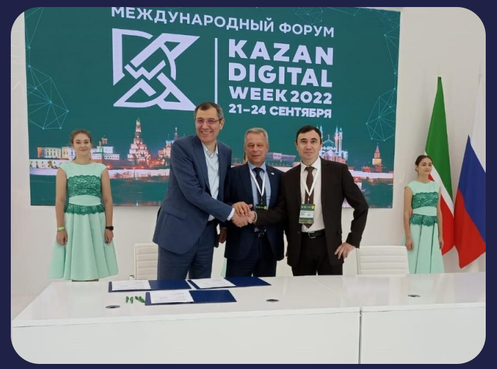
ВНЕШНЕЕ ОБУЧЕНИЕ

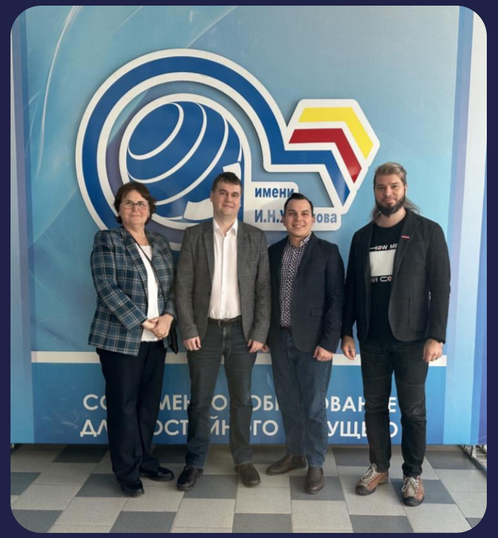
- Лаборатория безопасной разработки и системного программирования ЧГУ им. И.Н. Ульянова
- Сетевая магистерская программа совместно с ИСП РАН и ЧГУ им. И.Н. Ульянова
- Организация и проведение дополнительных образовательных программ по РБПО
- Выполнение НИР по тематикам РБПО

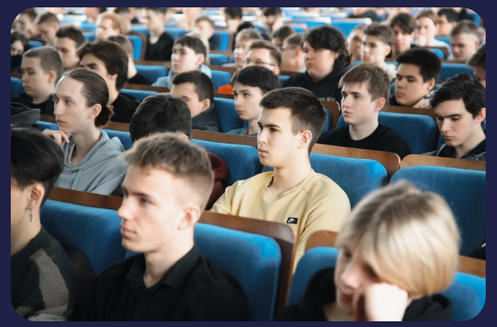
ВНУТРЕННЕЕ ОБУЧЕНИЕ

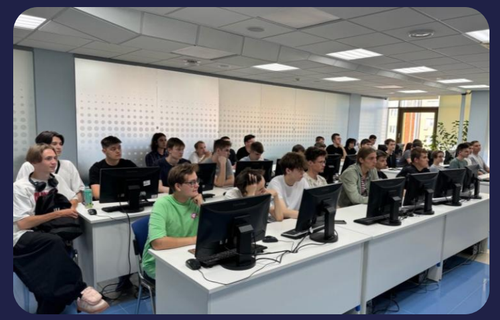
- Практико-ориентированные курсы по РБПО для команд разработки
- Воркшопы по вопросам применения инструментария в цикле РБПО
- Развитие института «Чемпионов безопасности» (SecChamp)











Записки альпинистов
или Истории из жизни

Внутренний департамент обратился с запросом на проведения мероприятий необходимых для прохождения сертификации СЗИ

Задача

Сертификация программного продукта по линии ФСТЭК России

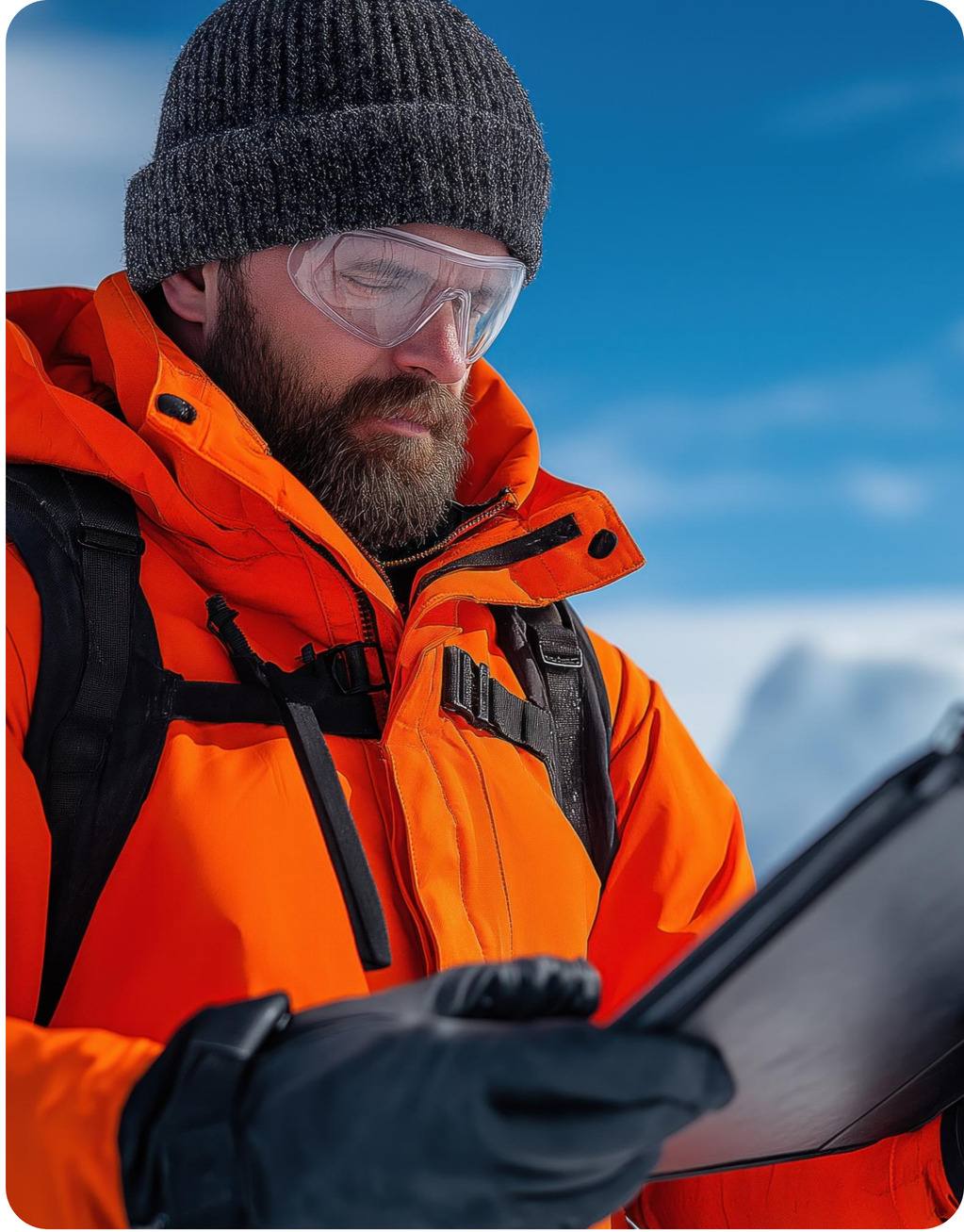
Домен «Сертификация СЗИ»

Сроки выполнения

9 месяцев

Результат:

- Организованы консультации по подготовке к сертификации СЗИ.
- Проведены испытания программного обеспечения по ВУ и НДВ.
- Предоставлена методическая поддержка на протяжении сертификации СЗИ.



Записки альпинистов или Истории из жизни

Внутренний департамент обратился с запросом подтверждения выполнения требований безопасной разработки ПО

Задача

Интеграция практик безопасности в процесс разработки ПО

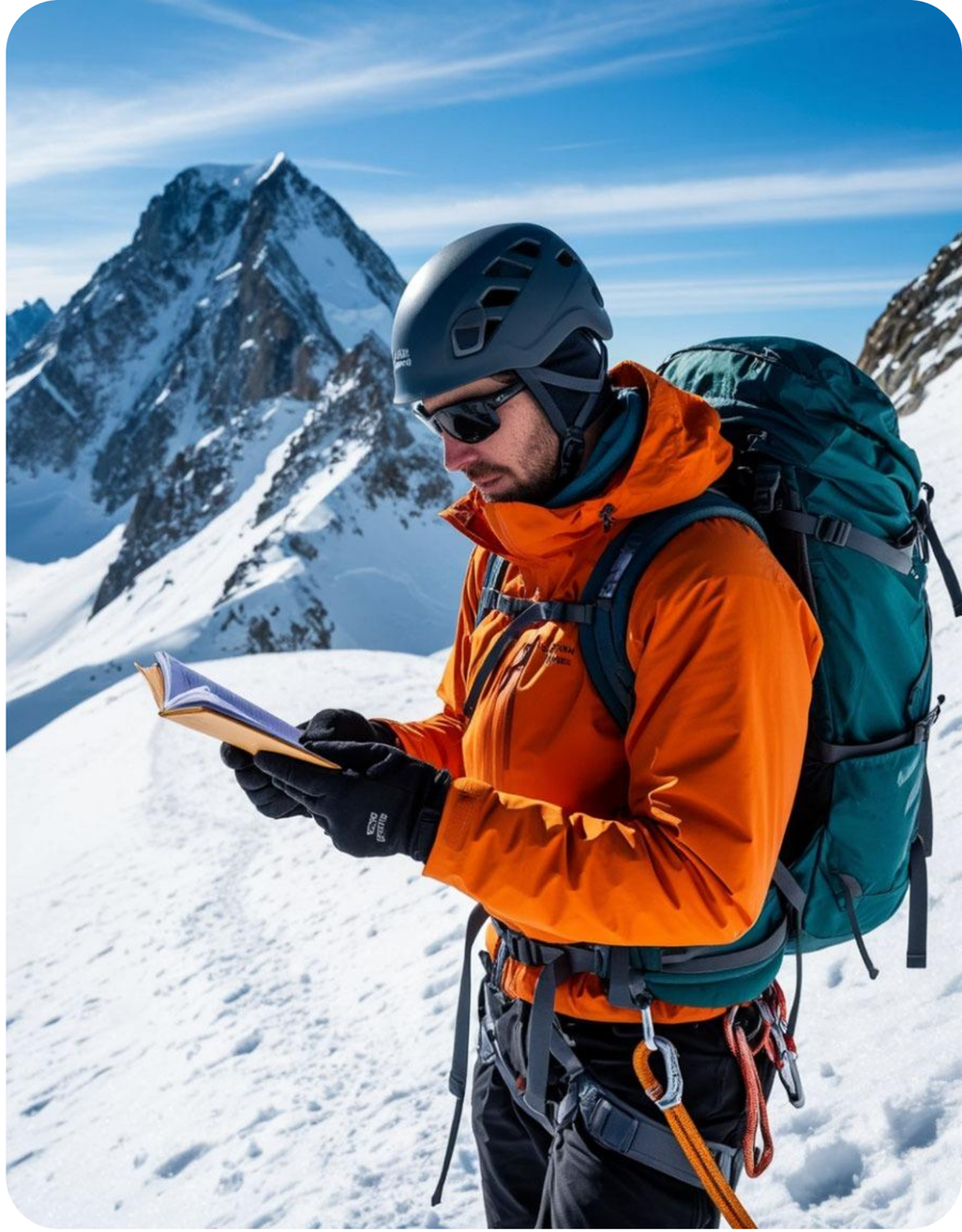
Домен «Построение процессов РБПО»

Сроки выполнения

8 месяцев

Результат

- Проведен **анализ текущего состояния процессов РБПО** с оценкой их соответствия требованиям национальных стандартов и Приказу ФСТЭК России № 117.
- Обеспечена методическая и практическая помощь в процессе трансформации практик безопасной разработки ПО.



Записки альпинистов или Истории из жизни

Компания-разработчик обратилась за экспертизой по проверке безопасности ключевого продукта

Задача

Исследования компонентов с открытым исходным кодом

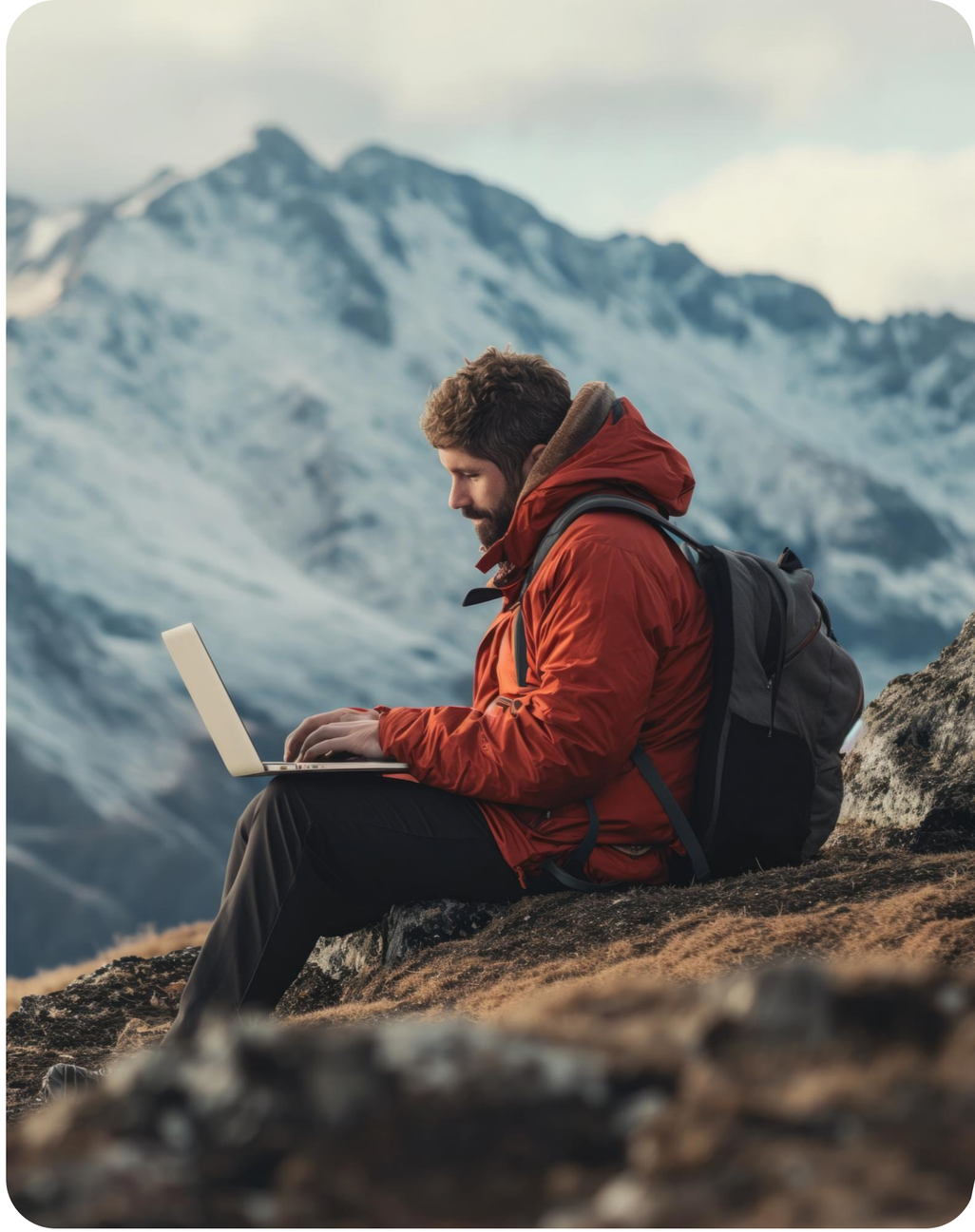
Домен «Исследования качества и безопасности программных продуктов»

Сроки выполнения

4 месяца

Результат

- Проведены исследования применяемых сторонних компонентов посредством **статического анализа исходного кода ПО.**
- Выявленные проблемы безопасности приняты во внимание и устранены Заказчиком по переданному **детальному отчету** и **рекомендациям** по устранению ошибок и уязвимостей.



Записки альпинистов или Истории из жизни

Компания, разрабатывающая ПО для ЗОКИИ, обратилась с запросом выстраивания процессов РБПО

Задача

Выполнение требований безопасности к прикладному ПО

Домен «Построение процессов РБПО»

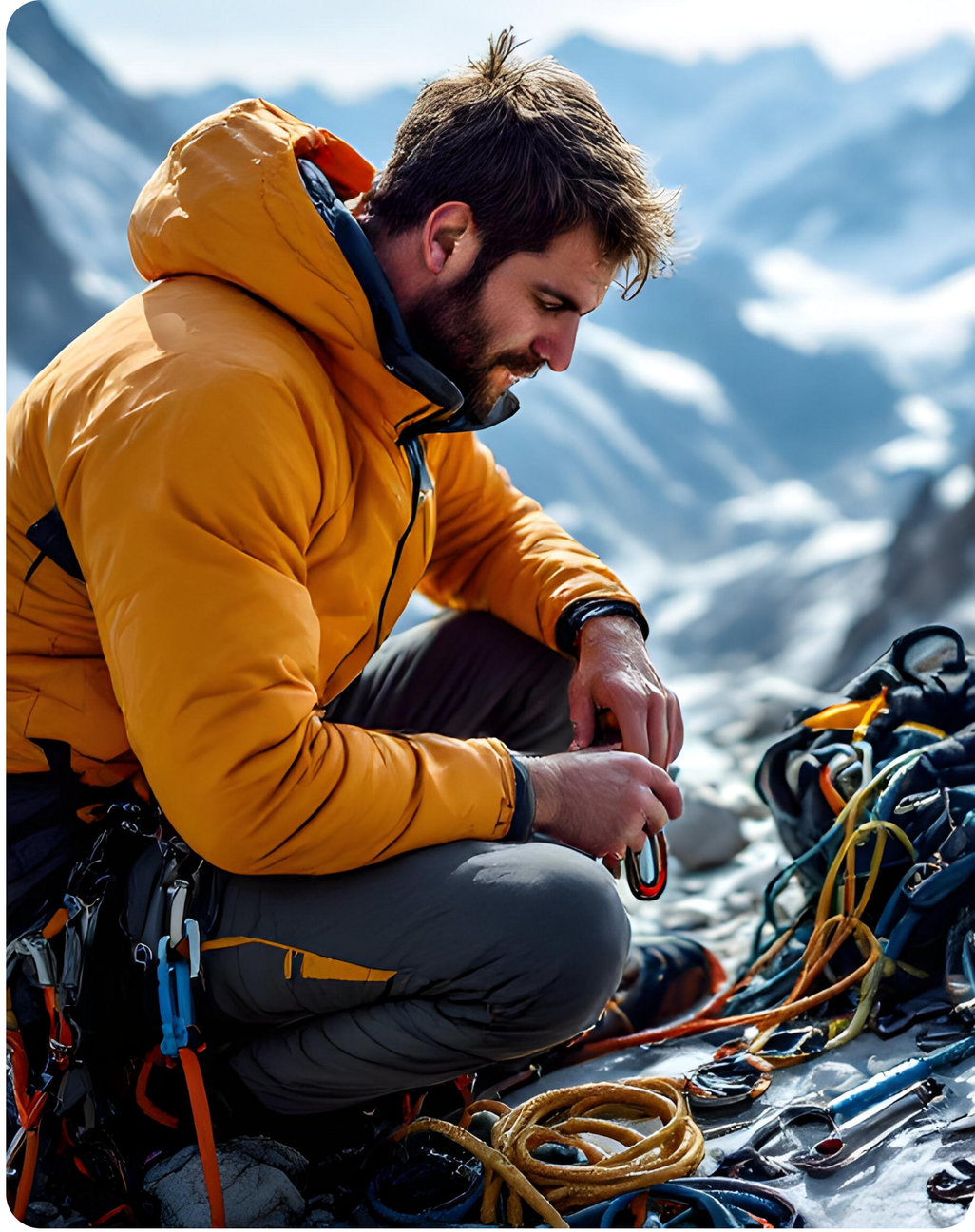
Домен «Исследования качества и безопасности программных продуктов»

Сроки выполнения

6 месяцев

Результат

- Подготовлена **документация**, описывающая цикл РБПО.
- Проведены инструментальные исследования безопасности ПО с применением различных технологий.
- Подготовлено **заключение о соответствии реализованных мер** в части выполнения требований Приказа ФСТЭК России № 239.



Стоит ли игра свеч?

Встраивание принципов безопасности в корпоративную культуру – от руководства до команд разработки

Централизованное управление ресурсами и инструментами

Единый канал коммуникаций для быстрого решения вопросов в части РБПО

Унификация подходов и практик разработки безопасного ПО

Трансляция и масштабирование практик в разных проектах и командах

Построение РБПО совместно с центром компетенций КСБ-СОФТ

Проведение аудита процессов безопасной разработки

Внедрение и развитие процессов безопасной разработки

Проверка соответствия требованиям стандартов

Подготовка документации, описывающей разработку безопасного ПО

Проведение композиционного, статического и динамического анализа, включая фаззинг-тестирование

Сопровождение процесса сертификации «под ключ»

Что сделать сейчас?

1. Формирование целостной картины по текущему **уровню реализации процессов РБПО** с учетом отраслевых требований

2. Формирование инициативной группы, заинтересованной в безопасности приложений и сервисов

3. Налаживание **производственных практик** (модернизация тулчейна, DevOps, гибкие методологии разработки)

4. Определение пилотной зоны и решений с целью **внедрения инструментов РБПО** с учетом специфики кодовой базы

5. Проведение **анализа безопасности** приложений и сервисов с последующим построением процесса устранения дефектов

КСБ-СОФТ

Помогаем вам построить и интегрировать процессы, позволяющие обеспечить безопасность на всех этапах жизненного цикла разработки и эксплуатации ПО

Решение:

- ✓ Аудит процессов РБПО;
- ✓ Подготовка комплекта документации по РБПО;
- ✓ Исследования безопасности приложений и сервисов;
- ✓ Проектирование платформы РБПО;
- ✓ Внедрение инструментальных средств безопасной разработки.

Полезные ресурсы

Обзор ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

Безопасное применение Open Source: о процессах и инструментах

Фаззинг-тестирование
От простого к сложному
(стр. 17)

Построение процессов разработки безопасного ПО: от нормативной базы до лучших практик

Внедрение статического анализа: на что обратить внимание или 5 «правил хорошего тона»

DevSecOps, AppSec, РБПО: путь тернист, но все возможно

Начните внедрять процессы РБПО!

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

ПРИГЛАШАЕМ ВАС ПОСЕТИТЬ НАШ СТЕНД № G01!

ОСТАЛИСЬ ВОПРОСЫ?

ksb-soft.ru

+7 (8352) 322-322

info@ksb-soft.ru