

ИТТСУ. Расследуй быстро!

Ожидаемые сроки исполнения:

Два семестра (Сентябрь 2024 - Июнь 2025)

Заказчик

-

2024



Контекст

В какой области решаем проблему?



Форензика, расследование инцидентов в области
информационной безопасности



Проблема

Что за проблема: кто пытается достичь какую цель и что мешает?

Кто?

Специалист службы информационной безопасности

Что хочет?

хочет уменьшить время на расследование инцидентов информационной безопасности

Что мешает?

но не может, при расследовании инцидентов ИБ используется в том числе экспертный анализ, что может привести к некорректному расследованию из-за человеческого фактора.

Какие есть способы решения и почему они не подходят?

Существующие средства для расследования разрозненны и не позволяют в короткие сроки получить однозначный ответ.

