

**Проект:** КП-06-Н57/4  
„Изследване и приложение на алгоритми за машинно обучение при анализ и разработка на високо сигурен софтуер“

**Финансиране:**

Фонд „Научни изследвания“

**Участващи организации:**

- Технически университет – София
- Софийски университет „Св. Климент Охридски“



**Свържете се с нас**

**Аделина Алексиева-Петрова**

Ръководител проект  
aaleksieva@tu-sofia.bg

# Изследване и приложение на алгоритми за машинно обучение при анализ и разработка на високо сигурен софтуер

ФИНАНСИРАН ОТ ФОНД „НАУЧНИ ИЗСЛЕДВАНИЯ“

## ОСНОВНА ЦЕЛ

Автоматизация на процесите от жизнения цикъл на софтуер и откриване, анализиране и предотвратяване на зловредните атаки към софтуерните продукти за постигане на висока сигурност на системите.

## ОСНОВНИ НАПРАВЛЕНИЯ И РЕШЕНИЯ

1. Откриване на аномалии и защита на данни
  - Машинно обучение + генетични алгоритми + анализ на главни компоненти (PCA)
  - Тестване с KDD Cup 1999
  - Висока точност при разпознаване на известни и нови заплахи
2. Защита на веб и IoT среди
  - Браузърен плъгин NotPwned за откриване на фишинг сайтове
  - Анализ на форми за вход и лога чрез изображения
  - Симулиране на уязвими IoT среди с отворени езикови модели (LLMs)
3. Мрежова защита
  - Архитектура за анализ на устройства в мрежа
  - Графова база данни за визуализация и зависимости
  - Правила за автоматично ограничаване на опасно поведение

## КЛЮЧОВИ РЕЗУЛТАТИ

- Три експериментални прототипа
- Намаляване на риска от кибератаки
- Повишена устойчивост на дигитални и IoT системи
- Приложимост в научни и практически среди

---

**Уебсайт:** <https://devops.tu-sofia.bg>

---