



# Модуль Анализа Поведения Пользователей в Сети “Katya v.1.0”

AC-VO & PPR Hackathon

# A DREAM TEAM



Андрей Илюхин



Дмитрий Дудунов



Светлана Бормотова

“ Потенциальный ущерб от киберпреступлений сравним с потерями от самого разрушительного урагана в истории США «Катрина»: порядка \$120 млрд. ”

*Финансист и мультимиллиардер Уоррен Баффет*



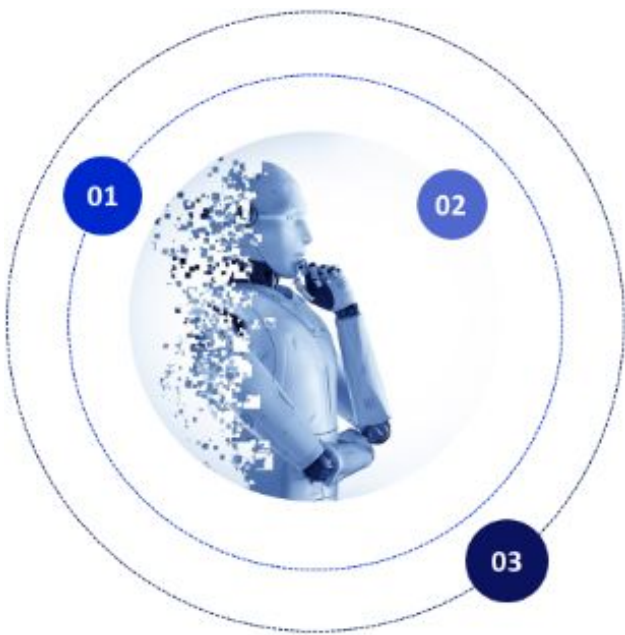
# Katya v.1.0

---

Модуль анализа трафика,  
позволяющий выявлять  
вредоносные соединения и  
прогнозировать их появление с  
помощью алгоритмов  
машинного обучения



# МЕТОДОЛОГИЯ РАЗРАБОТКИ Katya v.1.0



Предварительный  
анализ данных  
Чистка данных



Шаг 1

Feature  
Engineering  
Feature  
Importance  
(Корреляция  
Пирсона, MI  
classifier)



Шаг 2

Генерация  
целевой  
переменной  
Классификация  
атак



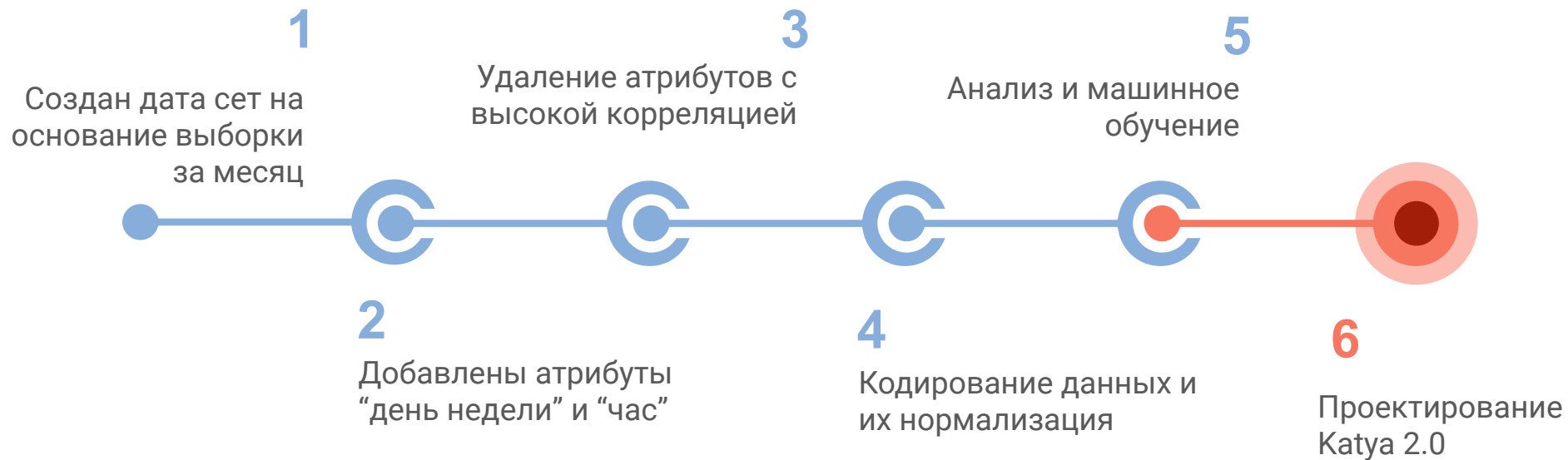
Шаг 3

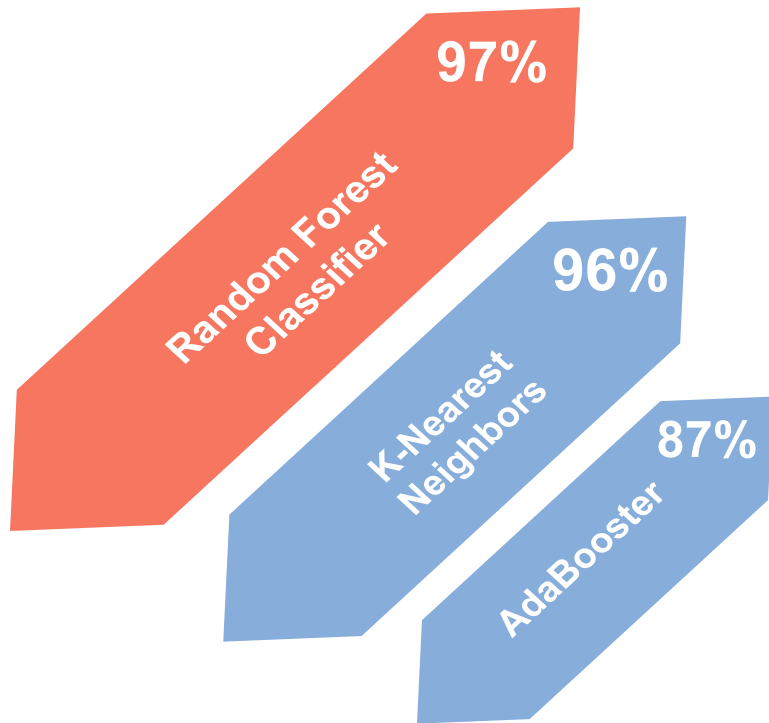


Шаг 4

Машинное обучение и  
интерпретация  
результатов

# А ЭТАПЫ РЕАЛИЗАЦИИ

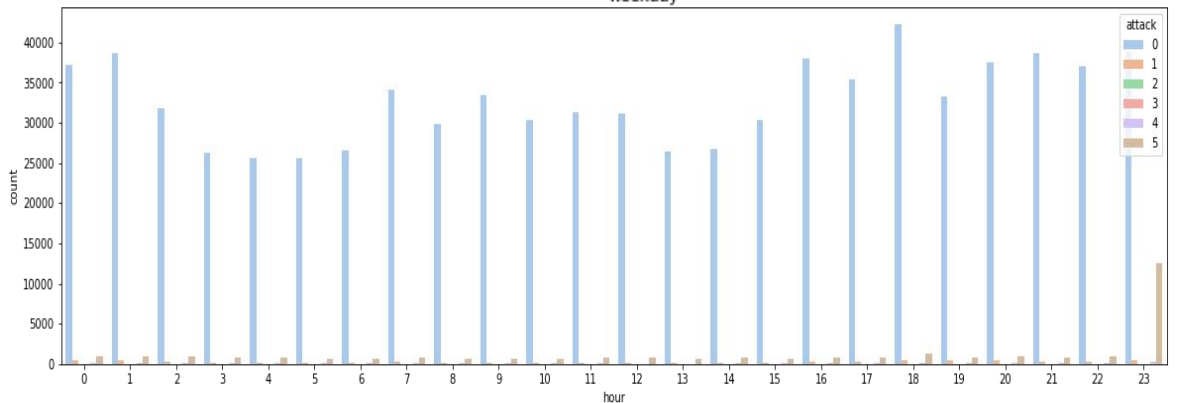
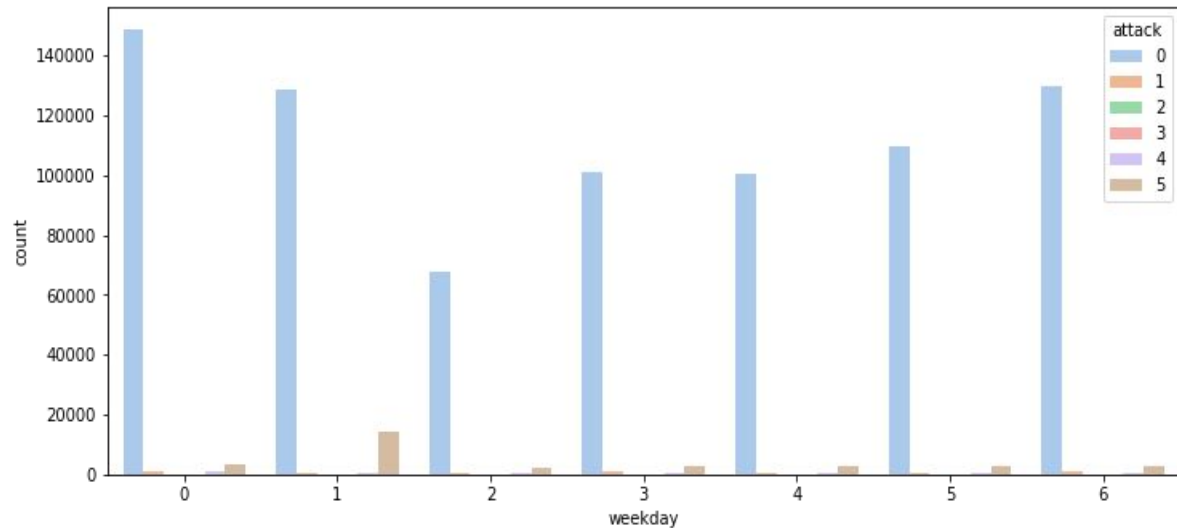




Матрица ошибок

True label	0	1	2	3	4	5
	156203	275	0	2	82	686
	566	477	0	0	65	76
	6	0	17	0	0	0
	5	0	0	47	0	0
	339	161	0	0	39	47
Predicted label	0	1	2	3	4	5
	1026	82	2	0	24	4969

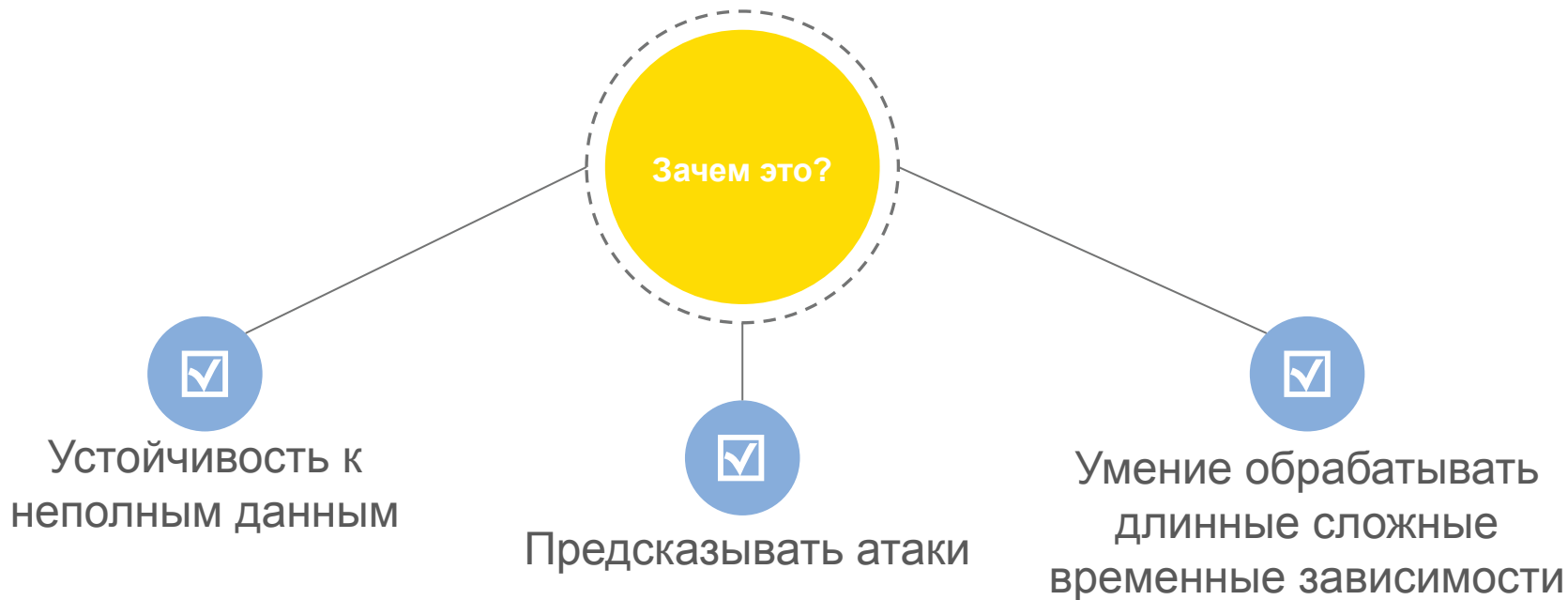
# РАСПРЕДЕЛЕНИЕ АТАК В РАЗРЕЗЕ ВРЕМЕННЫХ ДАННЫХ



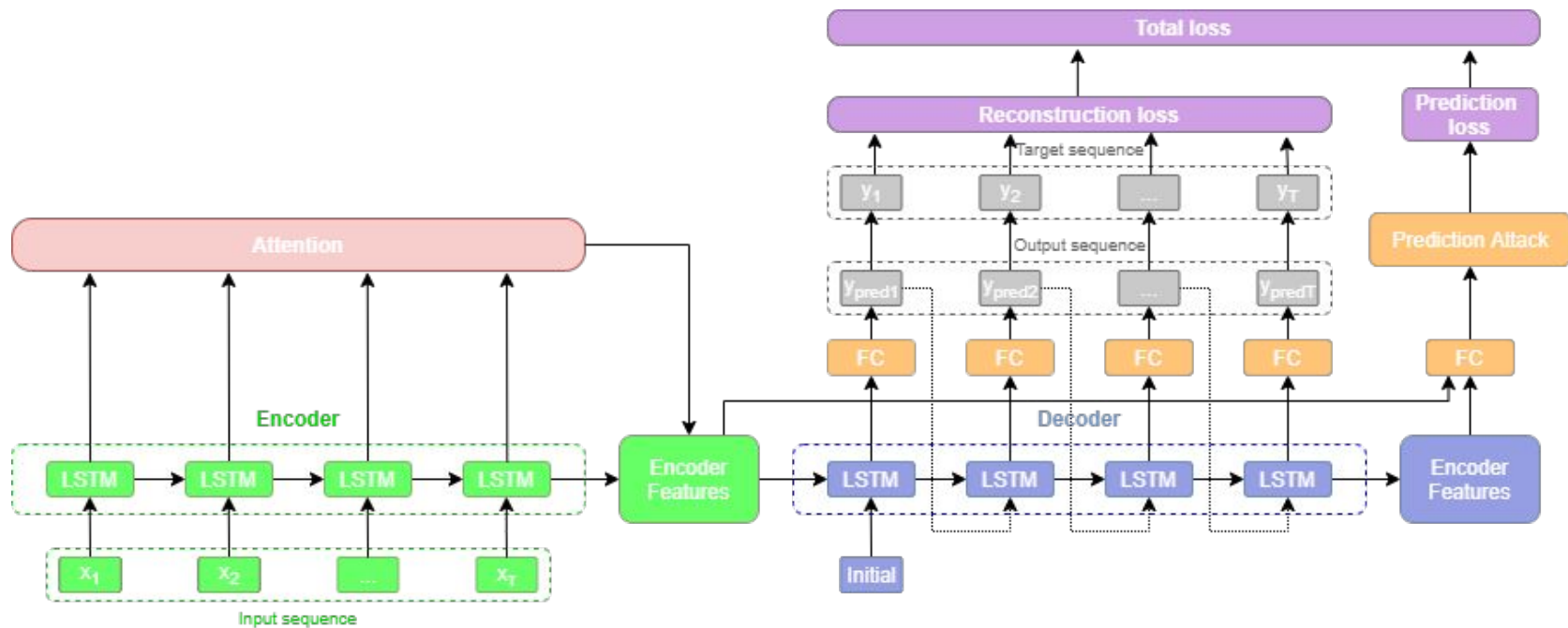


# Katya v.2.0

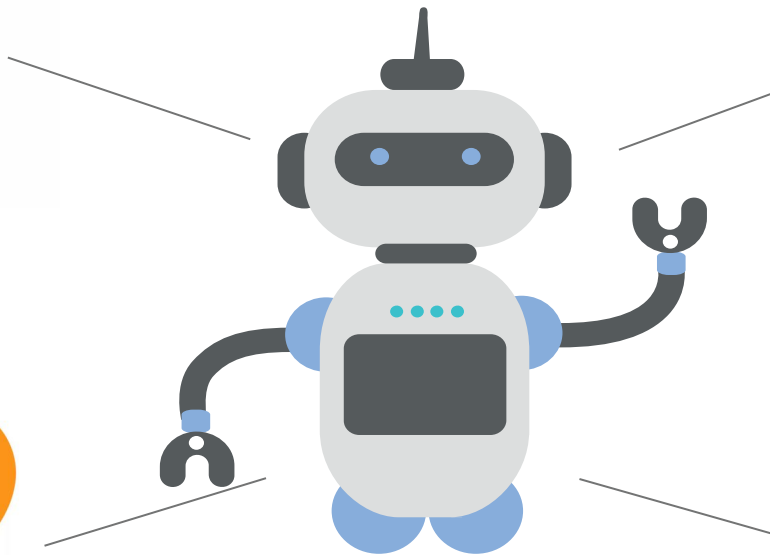
## Neural Network Approach



# Предлагаемая архитектура



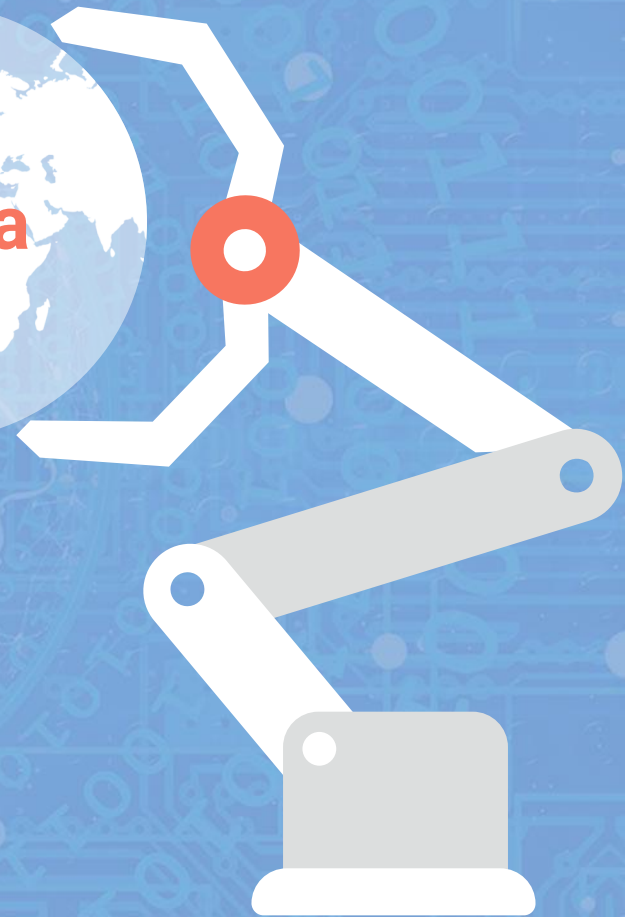
# А ИНСТРУМЕНТЫ



**Андрей Илюхин**  
ilyukhin.av@yandex.ru

**Дмитрий Дудунов**  
dudunovd@mail.ru

**Светлана Бормотова**  
svetlana.bormotova@gmail.com



**A DREAM  
TEAM**