ВТБ

Data Fusion Contest

Разбор публичного решения Защиты

Кузнецов Андрей

Пример решения от организаторов

Будем 9 раз брать 90% процентов данных и делать на них предсказание, далее усредним предсказания.

Чтобы улучшить этот подход можно делать больше повторений (можем позволить, считается быстро), а так же увеличить размер до 95%.

Метрика на данных для дообучения: **0.673 –> 0.684**, т.е. мы не только защитили модель, но и повысили её качество и сделали стабильнее.

Feature engineering

Data Fusion Contest

На основе mcc кода

Для клиента банка по каждому mcc коду считаем количество транзакций. Т.к. при атаке поменяется не более 10 mcc кодов, то реальное значение может изменится на ±10. Чтобы уменьшить влияние такого искажения, поделим нацело все значения на 20.

```
transactions.pivot_table(
    index='user_id', columns=['mcc_code'], values=['transaction_amt'],
    aggfunc=['count'], fill_value=0
)
```

Feature engineering

Data Fusion Contest

На основе времени в секундах

- Функции: сумма, среднее, стандартное отклонение, минимум, максимум, медиана.
- Кажется, что признаки странные, но имеют высокую важность и улучшают качество.

```
transactions.groupby('user_id')['time'].agg(['mean', 'std', 'min', 'max', 'median'])
```

CatBoost solution

Обучение

К признакам добавим предсказание банковской модели, это можно сделать, т.к. она не видела данные для дообучения. Параметры для CatBoostClassifier:

- 'loss_function': 'CrossEntropy', # есть дизбаланс классов
- 'task_type': 'CPU’,
- 'iterations': 750,
- 'max_depth': 3,
- 'learning_rate': 0.01,
- 'colsample_bylevel': 0.9,
- 'feature_weights': {'nn_predict': 0.9} # для защиты уменьшим важность

Mean Harm ROC-AUC: 0.720445

	Feature Id	Importances
0	nn_predict	43.784605
1	tr_time_std	11.847921
2	count-mcc_code:6012	9.637959
3	tr_time_max	6.567692
4	tr_time_min	4.349295
5	tr_time_mean	3.593514
6	tr_time_median	2.643810
7	count-mcc_code:5411	2.360808
8	count-mcc_code:4829	2.163495
9	count-mcc_code:5812	1.391974

Как улучшить?

- Нормализация количества транзакций по mcc кодам

	a	b	c
0	1	3	0
1	2	2	0
2	3	0	3

	a	b	c	total
0	0.25	0.75	0.0	4
1	0.50	0.50	0.0	4
2	0.50	0.00	0.5	6

- Больше признаков
- Медиана суммы транзакций не сильно сдвинется
- Обучение на атакованных данных