Гибридный подход к оценке риска подозрительных транзакций в платёжных системах

С. А. Радченко*, Б. Г. Мубараков‡

Рассматривается гибридный подход к мониторингу транзакций, объединяющий логистическую регрессию и экспертные правила. На выборке из 300 000 операций PaySim полнота обнаружения на тестовой части выросла с 75,32% до 96,10%, precision снизилась с 84,06% до 19,73%; доля алертов составила около 0,63%. Описаны признаки, правила и протокол выбора порогов. Развитие подхода связано с поведенческими признаками и обучаемым объединением оценок.

Ключевые слова: машинное обучение, антифрод, платёжные системы, экспертные правила, поведенческий анализ, оценка риска.

1. Постановка задачи и метод

При мониторинге платёжных операций с редким мошенничеством существенны precision, recall и ложные тревоги [1, 2]. В [5] правила формируются и рекомбинируются по ML-моделям. Здесь оценивается взвешенное объединение ML и заданных правил с решениями ALLOW (пропуск), REVIEW (проверка), BLOCK (ограничение); сам принцип гибридизации не заявляется новым.

В обоих режимах используется одна и та же логистическая регрессия с оценкой p_t, чтобы сравнить решения с экспертными правилами и без них при фиксированном классификаторе. Сравнение с ансамблями не проводилось. Модель использует время, тип и сумму операции, балансы и производные признаки. Числовые признаки стандартизированы, тип операции закодирован методом one-hot. Параметры модели: `lbfgs`, до 1000 итераций, сбалансированные веса классов.

Радченко Сергей Андреевич — магистрант ИВМиИТ КФУ, e-mail: sergei2003r@gmail.com.

Radchenko Sergey Andreevich — Master's student, Kazan Federal University.

‡*Мубараков Булат Газинурович* — канд. техн. наук, доцент каф. САИТ, ИВМиИТ КФУ, e-mail: mubbulat@mail.ru, ORCID: 0000-0002-7628-9870.

Mubarakov Bulat Gazinurovich — docent, Kazan Federal University.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

Для индикаторов правил $I_j \in \{0,1\}$ задаются

$$r_t = \min\left(1, \sum_{j=1}^{7} w_j I_j\right), \quad w = (0{,}01; 0{,}12; 0{,}15; 0{,}25; 0{,}25; 0{,}25; 0{,}50).$$

Правила по порядку: TRANSFER/CASH_OUT; обнуление счёта отправителя; отношение суммы к его положительному исходному балансу $\geq 0{,}90$ для TRANSFER/CASH_OUT; крупная сумма; крупный TRANSFER и крупный CASH_OUT на счёт с нулевым исходным балансом (два правила); цепочка TRANSFER→CASH_OUT в пределах 24 шагов. Границы крупных сумм определяются по train: общая — $Q_{0.995}$, для TRANSFER/CASH_OUT — соответствующие $Q_{0.99}$; в данном запуске это 2 464 049,35, 10 000 000 и 580 099,51. Правило I_4 срабатывает при достижении общего порога суммы или порога для соответствующего типа операции. Суммирование весов с ограничением единицей задаёт обработку комбинаций и нормировку. Итоговый риск $S_t = 0{,}85p_t + 0{,}15r_t$. Коэффициенты объединения заданы заранее и не оптимизировались.

ML-пороги REVIEW и BLOCK равны 0,97826027 и 0,99082319. В гибриде BLOCK также назначается при $S_t \geq 0{,}95$ или при $r_t \geq 0{,}55$ в сочетании с $I_7 \wedge (I_4 \vee I_3)$. При отсутствии BLOCK назначается REVIEW по нижнему ML-порогу, при $S_t \geq 0{,}75$ или при $r_t \geq 0{,}55$ и срабатывании I_7 либо одной из пар (I_4, I_3), (I_4, I_2), (I_5, I_3), (I_6, I_3). В остальных случаях назначается ALLOW.

2. Эксперимент и результаты

Из PaySim [4] стратифицированно отобрали 300 000 операций и разделили их с сохранением долей классов на train/validation/test (60/20/20, `random_state=42`). В этих частях 233, 77 и 77 мошеннических операций соответственно. Предобработка, модель и квантили определены по train. На validation порог REVIEW максимизирует precision при recall $\geq 0{,}80$, порог BLOCK — recall при precision $\geq 0{,}85$ и условии $\theta_{\mathrm{ML,B}} \geq \theta_{\mathrm{ML,R}}$. Пороги риска и правил фиксированы.

Результаты эксперимента на тестовой выборке приведены ниже. ML REVIEW включает все операции, достигшие нижнего порога, в том числе ML BLOCK. Алерты гибрида включают REVIEW и BLOCK.

Режим	Precision	Recall	F_2
ML REVIEW	84,06%	75,32%	76,92%
ML BLOCK	96,43%	70,13%	74,18%
Hybrid	19,73%	96,10%	54,17%

Распределение решений гибрида по классам:

Решение	Мошеннические	Легитимные	Всего
ALLOW	3	59 622	59 625
REVIEW	20	299	319
BLOCK	54	2	56

Гибрид выявил 74 из 77 мошеннических операций. Доля алертов $(319 + 56)/60\,000 \approx 0{,}63\%$. При том же составе группы BLOCK очередь REVIEW выросла с 13 до 319 операций. Из 306 добавленных операций 16 были мошенническими. Precision очереди REVIEW — 6,27%.

3. Развитие подхода

Правило TRANSFER→CASH_OUT на тестовой выборке не сработало. Поведенческие профили и графовые признаки не использовались. Предлагается обучать объединение p_t, r_t и истории клиента логистической регрессией. Текущий опыт использует конечные балансы и случайное разбиение. Для оценки до исполнения платежа нужны временное разбиение с учётом дрейфа [3] и признаки, доступные до операции.

Список литературы

[1] R. J. Bolton, D. J. Hand, “Statistical Fraud Detection: A Review”, *Statistical Science*, **17**:3 (2002), 235–255. DOI: 10.1214/ss/1042727940.

[2] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, G. Bontempi, “Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy”, *IEEE Transactions on Neural Networks and Learning Systems*, **29**:8 (2018), 3784–3797. DOI: 10.1109/TNNLS.2017.2736643.

[3] J. Gama, I. Žliobaité, A. Bifet, M. Pechenizkiy, A. Bouchachia, “A Survey on Concept Drift Adaptation”, *ACM Computing Surveys*, **46**:4 (2014), 44. DOI: 10.1145/2523813.

[4] E. A. Lopez-Rojas, A. Elmir, S. Axelsson, “PaySim: A Financial Mobile Money Simulator for Fraud Detection”, *Proceedings of the 28th European Modeling and Simulation Symposium*, EMSS 2016 (Larnaca, Cyprus), 2016, 249–255.

[5] I. Vorobyev, A. Krivitskaya, “Reducing False Positives in Bank Anti-fraud Systems Based on Rule Induction in Distributed Tree-based Models”, *Computers & Security*, **120** (2022), 102786. DOI: 10.1016/j.cose.2022.102786.

Статья поступила 10 октября 2026 г.

A Hybrid Approach to Risk Assessment of Suspicious Transactions in Payment Systems

S. A. Radchenko, B. G. Mubarakov

A hybrid transaction-monitoring approach combines logistic regression with expert rules. On a sample of 300,000 PaySim transactions, test recall increased from 75.32% to 96.10%, while precision decreased from 84.06% to 19.73%; the alert rate was about 0.63%. Features, rules, and threshold selection are specified. Future work introduces behavioral features and trainable score aggregation.

Keywords: machine learning, fraud detection, payment systems, expert rules, behavioral analysis, risk assessment.

References

[1] R. J. Bolton, D. J. Hand, "Statistical Fraud Detection: A Review", *Statistical Science*, **17**:3 (2002), 235–255. DOI: 10.1214/ss/1042727940.

[2] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy", *IEEE Transactions on Neural Networks and Learning Systems*, **29**:8 (2018), 3784–3797. DOI: 10.1109/TNNLS.2017.2736643.

[3] J. Gama, I. Žliobaité, A. Bifet, M. Pechenizkiy, A. Bouchachia, "A Survey on Concept Drift Adaptation", *ACM Computing Surveys*, **46**:4 (2014), 44. DOI: 10.1145/2523813.

[4] E. A. Lopez-Rojas, A. Elmir, S. Axelsson, "PaySim: A Financial Mobile Money Simulator for Fraud Detection", *Proceedings of the 28th European Modeling and Simulation Symposium*, EMSS 2016 (Larnaca, Cyprus), 2016, 249–255.

[5] I. Vorobyev, A. Krivitskaya, "Reducing False Positives in Bank Anti-fraud Systems Based on Rule Induction in Distributed Tree-based Models", *Computers & Security*, **120** (2022), 102786. DOI: 10.1016/j.cose.2022.102786.

Received on October 10, 2026