V. V. Klimov, M. V. Kuzin, B. A. Shchukin

Monitoring of Fraud Transactions Using Committees of Neural Networks

Key words: fraud monitoring, neural networks, committees of neural networks

The task of detection card fraud transactions using neural networks and their committees is considered.

В. В. Климов, М. В. Кузин, Б. А. Щукин

МОНИТОРИНГ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ С ПОМОЩЬЮ КОМИТЕТОВ НЕЙРОННЫХ СЕТЕЙ

Существуют программные системы и комплекс организационных мер, направленных на предотвращение или усложнение проведения возможных мошеннических операций с банковскими картами. Несмотря на это, исследования в данной области непрерывно продолжаются. Задача распознавания мошеннических транзакций при их авторизации на стороне эмитента карты является неформализованной и чрезвычайно сложной [1]. Под мошеннической будем понимать операцию (транзакцию), совершенную с помощью банковской карты или ее реквизитов, не инициированную или не подтвержденную ее держателем.

Системы, способные обеспечить реализацию этой функции, обычно строятся на основе логических фильтров (правил) и относятся к классу систем fraud prevention («предотвращение мошенничества»), то есть способных, хотя бы частично, предотвращать проведение мошеннических операций, не допуская авторизации отфильтрованных подозрительных транзакций. Однако полностью предотвратить мошенничество невозможно: «слишком» развитые правила проверки приводят к многочисленным отказам в авторизации легальных транзакций. Системы класса fraud monitoring («мониторинг мошенничества») не связаны с процессом авторизации, анализируют уже завершенные транзакции и могут использовать более сложные алгоритмы, основанные на сетях Байеса или *нейросетях* (нейронных сетях — neural networks). Они не связаны с обработкой (процессингом) транзакции, и можно сказать, что основная их задача — выявление новых правил анализа.

В последнее время в материалах конференций по нейронным сетям [2] появились статьи по использованию комитетов нейронных сетей для решения различных задач. Суть этого подхода состоит в том, что смешиваются выходы нескольких автономно обученных нейронных сетей, обрабатывающих входные данные. Смешивание выходов может производиться как с помощью фиксированных алгоритмов, так и на базе дополнительной нейронной сети, которая обучается на основе информации, полученной на сетях, обрабатывающих входные данные. Комитет может состоять из нескольких входных сетей с различной или идентичной архитектурой. Сети независимо друг от друга обучаются на разных наборах обучающих выборок, а при эксплуатации или тестировании анализируют входящие данные параллельно. Считается, что комитет позволяет улучшить качество распознавания, особенно относительно обобщающей способности, и получить приемлемую эффективность при дефиците входной информации.

Постановка задачи

Дан набор реальных транзакций, каждая из которых помечена как легальная, то есть инициируемая владельцем карты, или как мошенническая, то есть выполняемая без ведома владельца или в сговоре с ним.

Требуется построить нейрокомитет, состоящий из N входных нейросетей и сети комитета, схема которого представлена на рис. 1, позволяющий отличить легальную транзакцию от мошеннической.

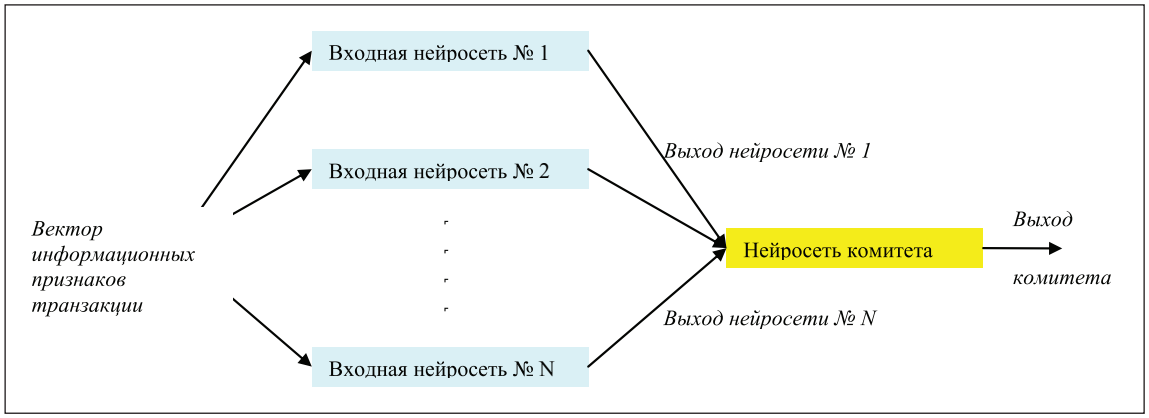


Рис. 1. Общая архитектура нейрокомитета

Транзакция на входе в нейрокомитет представляется вектором информационных признаков. Определение вектора информационных признаков требует достаточно полных знаний об особенностях использования карт эмитента. Вектор информационных признаков одновременно поступает на каждую из N входных нейросетей, на выходе каждой из которых получается число [0, 1]. Эти N чисел образуют входной вектор для сети комитета, которая на выходе получает также число [0, 1], по значению которого и принимается решение.

Таким образом, задача разбивается на несколько подзадач:

1. Определение вектора информационных признаков транзакции.
2. Выбор архитектуры каждой из входных сетей и их числа.
3. Выбор архитектуры сети комитета.
4. Выбор параметров обучения каждой сети и ее обучение.
5. Формирование обучающих наборов векторов информационных признаков.
6. Формирование обучающих наборов из векторов выходов входных нейросетей.
7. Формирование гистограмм значений выхода нейрокомитета.

Отметим сразу, что для решения задач распознавания теория предлагает использовать сети типа «многослойный персептрон» (multi-layer perceptron). Для всего остального — только метод проб и ошибок.

Определение вектора информационных признаков транзакции

Запрос авторизации, посылаемый терминалом, обрабатывающим банковскую карту (банкоматом — ATM, терминалом в пункте продаж — POS, интернет-терминалом — EPOS), обычно содержит около 20 признаков, значимых для целей выявления мошеннических операций. Состав этих признаков может варьироваться.

По одним исходным признакам транзакции нельзя ничего решить относительно ее статуса — мошенническая или легальная. Требуется совместный анализ с предыдущими транзакциями по этой карте. Следовательно, каждую текущую транзакцию перед ее анализом в нейросети необходимо дополнить рядом признаков, вычисляемых по информации из предшествующих транзакций по карте. Это может быть, например, сумма, снятая со счета карты за последние 24 часа, или признак, характеризующий поведение клиента, — количество транзакций за последние 24 часа, выполненных через банкоматы.

Анализ исходного набора признаков, характеризующих транзакцию, позволяет заключить, что в основном это коды. Только три признака, а именно, дата совершения транзакции, время и сумма, являются числами.

Входные данные для нейронной сети должны быть числами, нормированными на 1, что требует задания интервалов разбиения и введения бинарных признаков. В экспериментах использовался

двоичный набор признаков, состоящий из 64 позиций. Число двоичных признаков целесообразно выбирать кратным 4 и каждую транзакцию описывать шестнадцатеричным кодом.

Относительно использования двоичного кода для распознавания мошеннических транзакций целесообразно сделать следующие принципиальные замечания. При обучении распознаваемому объекту должен однозначно сопоставляться некоторый двоичный код. Это принципиальный момент при обучении нейронной сети. При наличии конфликтных ситуаций обучить сеть нельзя.

В случае распознавания мошеннических транзакций принципиально нельзя гарантировать, что зафиксированный двоичный код для некоторой мошеннической транзакции не будет идентичен коду некоторых легальных транзакций, даже по одной и той же карте. Построение бинарного кода, однозначно идентифицирующего мошенническую ситуацию, фактически соответствует построению правила проверки.

Исходный набор данных, на котором проводились эксперименты, состоял из 3 728 713 транзакций, из которых 1006 транзакций были помечены как мошеннические (см. таблицу 1).

Таблица 1.

Количество транзакций (QtyF)	**Терминал**	**Информационный признак**	**Количество мошеннических транзакций (QtyAll)**	**QtyF/QtyAll**
3 728 713	Все		1006	0,00027
2 236 455	ATM	$i_{17} = 1$	707	
2 236 024	ATM + Получение наличных	$i_{17} = 1$ & $i_{21} = 1$	707	0,00032
1 307 765	POS	$i_{18} = 1$	210	0,00016
18	POS + Получение наличных	$i_{18} = 1$ & $i_{21} = 1$	0	
184 491	EPOS	$i_{19} = 1$	89	0,00048
2	Отделение банка	$i_{17} = 0$ & $i_{18} = 0$ & $i_{19} = 0$	0	

Представленные в таблице 1 значения характерны для решаемой задачи: на фоне огромного числа легальных транзакций ничтожное количество мошеннических. При представлении 1006 мошеннических транзакций кодами, состоящими из 64 двоичных информационных признаков, получился набор из 581 уникального кода. При составлении обучающих наборов должно соблюдаться разумное соотношение между мошенническими и легальными транзакциями. Кодирование 50 000 легальных транзакций привело к созданию набора из 7210 уникальных кодов, не пересекающегося с набором кодов мошеннических транзакций. Это база для формирования обучающих и тестирующих наборов для нейросети, созданной в рамках проводимого эксперимента.

Выбор архитектуры сетей нейрокомитета

Для решения задач распознавания теория предлагает использовать сети типа «многослойный персептрон». Это многослойные нейронные сети с фиксированной структурой [4], для которых необходимо определить следующие параметры:

- число уровней нейросети (Neural Network Layers);
- число нейронов на каждом уровне;
- признак использования нейронов смещения (Bias Neurons) — да или нет;
- передаточная функция нейрона (Transfer Function);
- алгоритм обучения (Learning Rule).

Подбор указанных параметров выполняется методом проб и ошибок и может быть ускорен только накоплением опыта работы. Для каждого набора параметров необходимо обучить и протестировать сеть, оценив полученные результаты. Эта работа достаточно объемна и требует использования специальных программных средств для работы с нейронными сетями [5], позволяющих выбирать указанные параметры.

Обучение нейронной сети

Обучение каждой входной нейросети производится автономно с помощью набора векторов информационных признаков транзакций. Каждому вектору набора ставится в соответствие целевое значение — 0, если транзакция легальна, и 1, если транзакция мошенническая. Вместе они составляют обучающую пару. Обычно количество обучающих пар, составляющих набор, не меньше произведения количества нейронов в слоях сети. По каждому вектору параллельно вычисляется выход входных сетей, образуя вектор из N действительных чисел на входе сети комитета. Проходя через сеть комитета, они образуют выход комитета.

Обучение сети комитета производится с помощью набора выходов входных сетей, получающегося при их тестировании. Если автономное обучение каждой входной нейросети может выполняться с помощью набора векторов информационных признаков транзакций, специально подобранного для этой сети, то параллельное их тестирование выполняется на базе единого тестового набора. Сопоставив каждому набору выходов значение 0 или 1, получаем базу для подбора обучающей последовательности сети комитета.

В ходе экспериментов было разработано несколько входных нейросетей, объединенных в комитеты и настроенных на различных обучающих наборах. Каких-либо рекомендаций по построению комитета нет. Априорно предполагается, что от комитета можно ожидать более высокую обобщающую способность, чем от каждой из входных сетей. Выявлено, что входные сети целесообразно оставлять «недоученными», что выражается в допущении более высокой ошибки обучения и ограничении количества итераций. По каждой входной сети и сети комитета представлены гистограммы значений выходов для обучающего набора и всей базы, используемой для формирования обучающих и тестирующих наборов (Рис. 2–6).

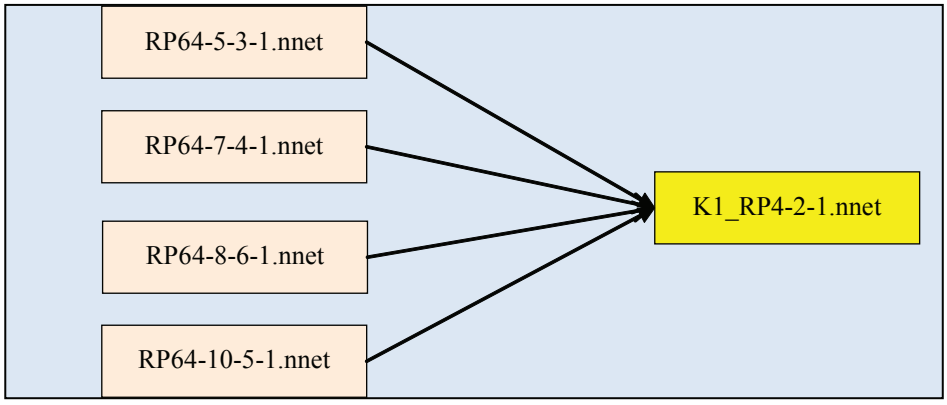
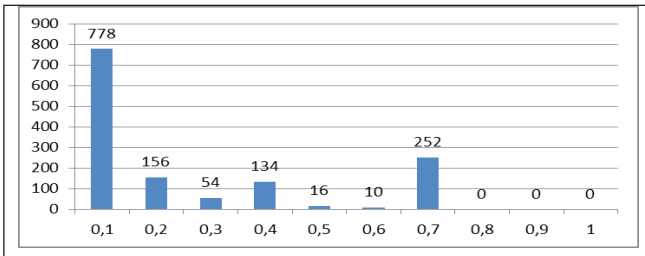


Рис. 2. Комитет нейросетей, построенный на четырех архитектурно различных входных сетях



Net: RP64-7-4-1 Multi-Layer Perceptron
Use Bias Neurons
Learning rule: Resilient Propagation
Training Set: BF202-401_L2001-3200
Max Error: 0,05
Max Iteration: 40
Learning Rate: 0,2

Рис. 3. Результаты обучения сети RP64-7-4-1. По оси абсцисс интервалы значений выхода сети, по оси ординат — количество транзакций (200 — fraud, 1200 — legal transaction)

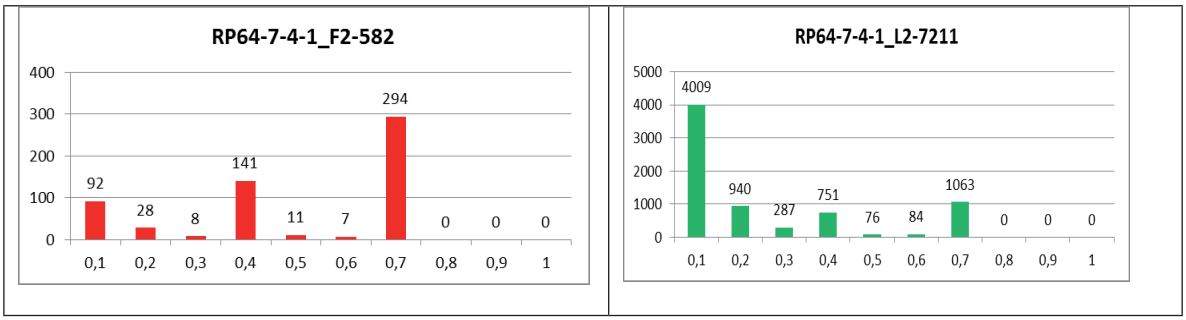
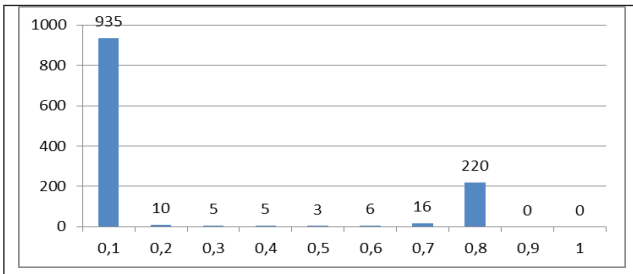


Рис. 4. Гистограмма результатов тестирования сети RP64-7-4-1 на 581 fraud и 7210 legal transaction



Net: K1_RP4-2-1 Multi-Layer Perceptron
Use Bias Neurons
Learning rule: Resilient Propagation
Training Set: KF203-402_L2502-3501
Max Error: 0,01
Max Iteration: 40
Learning Rate: 0,2

Рис. 5. Гистограмма результатов обучения сети комитета K1_RP4-2-1 (200 векторов fraud-выходов, 1000 векторов legal-выходов)

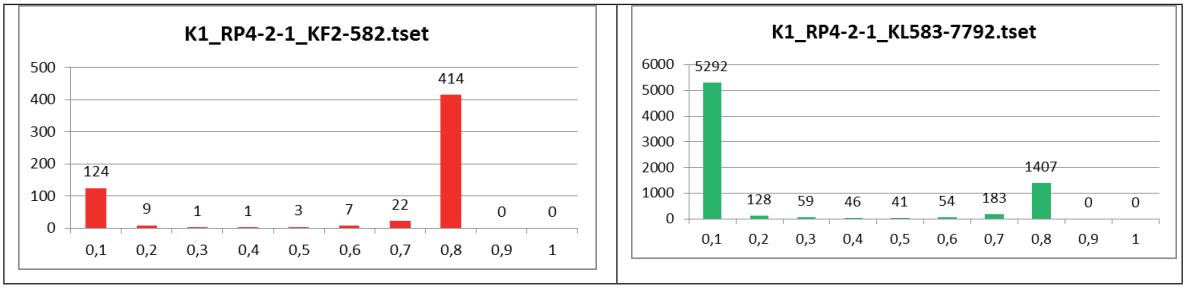


Рис. 6. Гистограмма результатов тестирования сети комитета K1_RP4-2-1 (581 вектор fraud-выходов, 7210 векторов legal-выходов)

На рис. 3 и 4 отражены гистограммы результатов обучения и тестирования для одной из трех архитектурно различных входных нейросетей. На рис. 5 и 6 представлены результаты обучения и тестирования для построенного комитета нейронных сетей.

Результатом проведенного эксперимента явилось ожидаемое улучшение качества распознавания мошеннических и легальных транзакций. Мы считаем, что тенденция просматривается, хотя следует признать, что ошибки достаточно велики. Тем не менее использование комитетов нейронных сетей оказалось для данной задачи оправданным, так как дало улучшение показателей по сравнению с отдельными нейросетями. Исследования будут продолжены, и их целью будет разработка специального программного комплекса, позволяющего подбирать комитет нейросетей, показывающий лучшие результаты по сравнению с процессом подбора комитетов экспериментальным путем вручную.

Заключение

В банковской практике служба безопасности эмитента карт имеет дело, как правило, с двумя видами потоков заявлений клиентов:

- держатели карт жалуются, что им не дают выполнить необходимую операцию, хотя с точки зрения баланса счета карты проведение операции возможно;
- держатели карт жалуются, что они не проводили конкретных операций, изменивших состояние счета карты, и требуют вернуть им средства.

В первом случае система fraud prevention фиксирует транзакцию как мошенническую, но по ней не производится реальной операции. Во втором случае транзакция принимается за легальную, в соответствии с ней изменяется остаток по счету банковской карты, но впоследствии ее держатель заявляет протест. Если банк удовлетворяет протест, то транзакция переводится в разряд мошеннических.

Когда число удовлетворенных заявлений достигнет критической величины, принимается решение о модификации в банке системы fraud prevention. Современные системы выявления и предотвращения мошеннических транзакций с платежными картами включают различные модели анализа, в том числе на основе нейронных сетей. В работе обозначены проблемы использования таких моделей и предложен один из возможных подходов к использованию комитетов нейронных сетей, что позволит увеличить точность распознавания мошенничества и обеспечить приемлемый уровень ошибки.

Дополнительно необходимо отметить, что предложенный подход к применению комитетов нейронных сетей может быть транслирован и на другие задачи, стоящие в настоящее время перед банковским бизнесом. К таким следует отнести выявление и своевременное пресечение операций по счетам клиентов — физических и юридических лиц, имеющих признаки легализации доходов, полученных преступным путем.

СПИСОК ЛИТЕРАТУРЫ:

1. *Кузин М. В.* Оценка рисков эмитента в платежной системе банковских карт с использованием мониторинга транзакций // Безопасность карточного бизнеса: бизнес-энциклопедия. М.: Московская финансово-промышленная академия; ЦИПС и Р, 2012. С. 147–172.

2. *Чернодуб А. Н., Новинский Д. В., Дзюба Д. А.* Прогнозирование временных рядов на основе одиночных нейронных сетей и комитетов нейронных сетей: сравнительный эксперимент // Нейроинформатика. 2011. Часть 2. С. 192–201.

3. *Барский А. Б.* Логические нейронные сети. URL: http://www.intuit.ru/studies/courses/1061/185/info (дата обращения: 07.08.2014).

4. *Галушкин А. И.* Нейронные сети: основы теории. М.: Горячая линия-Телеком, 2012. – 496 с.

5. NeurophStudio. URL: http://neuroph.sourceforge.net/ (дата обращения: 12.09.2014).

REFERENCES:

1. *Kuzin M. C.* Risk assessment of the issuer in the payment system of bank cards with the use of monitoring transactions // Security card business: business encyclopedia. M.: Moscow financial-industrial academy. Zipser, 2012. P. 147–172.
2. *Chernodub A. N., Novinsky D. C., Dzyuba D. A.* Time series forecasting based on a single neural networks and committees of neural networks: a comparative experiment // XIII all-Russian scientific-technical conference "Neuroinformatics. 2011". Part 2. P. 192–201.
3. *Barsky A. B.* Logical neural network. URL: http://www.intuit.ru/studies/courses/1061/185/info.
4. *Galushkin A. I.* Neural networks: basic theory. M.: Hotline-Telecom, 2012. – 496 p.
5. NeurophStudio. URL: http://neuroph.sourceforge.net/.