УДК 004.4 doi: 10.26102/2310-6018/2018.23.4.037

Д.В. Романов, Н.А. Рындин

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ОБНАРУЖЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ В СФЕРЕ МЕЖДУНАРОДНОЙ ЛОГИСТИКИ

Воронежский государственный технический университет

В статье рассматриваются вопросы по разработке эффективной системы для борьбы с мошенническими действиями на основании общедоступных данных клиента сервиса по доставке посылок. Из-за постоянно возрастающих махинаций бизнес несет существенные убытки, а полноценная система фрод-мониторинга способна пресечь подозрительные действия и дать рекомендации по их дальнейшей обработке, что существенно снизит экономические, финансовые и репутационные риски. Система представляет собой отдельный ресурс, выполненный в виде облачного веб-сервиса, который включает в себя интеллектуальное ядро, выполняющее основные трудоемкие операции по анализу и детектированию транзакций. Аналитическая составляющая базируется на хорошо зарекомендовавших себя на практике алгоритмах машинного обучения, в основе которых лежит обучение с учителем. Для определения мошеннических действий строится и тестируется модель, выбирается лучшая. Оперируя исходными данными, она классифицирует каждую транзакцию, и в зависимости от уровня безопасности либо отклоняет ее, либо интерпретирует результат в понятный человеку и дает рекомендации по дальнейшим действиям. Система переобучается каждый раз, после того как уровни безопасности пересматриваются или добавляются новые; данные для обучения хранятся в централизованном хранилище. Разработанный сервис предполагается использовать для компаний, осуществляющих международную логистику, иметь простой и понятный интерфейс интеграции и взаимодействия.

Ключевые слова: интеллектуальное проектирование, алгоритмы машинного обучения, система поддержки принятия решений, мошеннические транзакции, антифрод, международная логистика.

ВВЕДЕНИЕ

Проблема фрода (мошенничества – от англ. fraud) в сети интернет существует уже несколько десятков лет, однако в последние годы приобрела серьезные масштабы, что заставляет обратить на себя внимание отечественных и зарубежных компаний. Во многом этому способствовало возросшее число онлайн-платежей и сервисов для их интеграции: интернет-магазинов, аукционов, торговых площадок. По предварительным оценкам каждая третья компания в своей деятельности сталкивается с данной проблемой, а по общемировой статистике за год бизнес теряет из-за этого десятки миллионов долларов. В связи с этим возникла необходимость найти решение, чтобы обезопасить компании от все увеличивающегося потока

фрода, минимизировать риски и экономические потери.

Уже более десяти лет ведется работа в сфере фрод-мониторинга – системе, обрабатывающей каждую транзакцию (активность) и делающий вывод о ее подозрительности с точки зрения мошенничества. Поток транзакций огромен, поэтому целесообразно доверить проверку современным интеллектуальным экспертным системам. В простейшем случае они базируются на некоторых заранее заложенных правилах (эвристиках), при срабатывании которых транзакция тут же переходит в разряд небезопасных. Количество таких эвристик может достигать порядка 200, однако зачастую некоторые из них оказываются ничем не подкреплены, часть – дублируют или являются следствие одного из другого. Несмотря на кажущуюся простоту, поддержка таких систем оказывается сложной, производительность падает, переобучение модели приводит к побочным эффектам. Распространенными среди таких эффектов являются определение подозрительной заведомо безопасной транзакции или вовсе неправильное распознавание (пропуск фрода).

Одним из способов повышения эффективности подобных систем может быть применение алгоритмов машинного обучения, которые обладают способностью к самообучению как на уже совершенных платежах, так и вновь поступающих. Доказательством эффективности может служить пример платежной системы Visa: применение новых методов в анализе платежей реального времени, используя данные от истории пользователя до терминала совершения оплаты, позволило сэкономить 2 миллиарда долларов.

В сфере международной логистики данная проблема также начала занимать существенную роль. В этой цепочке участвуют покупатель с продавцом, банки, таможня и сам сервис, осуществляющий перевозку – и на каждом из этапов необходим строгий контроль. Необходимость снижения рисков на каждом этапе диктуется и финансовыми, и репутационными рисками, поэтому наличие эффективной системы борьбы с мошенническими транзакциями уже является рыночной необходимостью.

МАТЕРИАЛЫ И МЕТОДЫ

Сама по себе разработка сервиса для предотвращения мошеннических операций сопровождается трудностями. Традиционным подходом является привлечение специалистов из данной области, а также из области основных бизнес-процессов компании, которые выделяют существенные аспекты, касающиеся безопасности совершения действий клиентом; после чего ведется разработка конкретной системы, которая

встраивается в общую информационную структуру компании. Хорошая антифрод-система стоит дорого, а ее реализация может затянутся на продолжительное время, в течение которого бизнес рискует понести серьезные финансовые потери. Поэтому предполагается использование другого метода – построение облачного веб-сервиса, в который будет полностью выделен бизнес-процесс анализа данных и интерпретации результата: является ли данная транзакция подозрительной или нет. И в качестве платформы для такого сервиса будет выступать Microsoft Azure, который позволяет технически просто создать приложение с нуля, используя в своем составе обширный выбор инструментария для разработки. Очевидными преимуществами данного подхода будут являться:

- снижение первоначальных денежных затрат на оборудование и программное обеспечение;
- сокращение количества специалистов, привлеченных к реализации;
- ускоренная разработка и внесение изменений за счет использования готовых решений и компонент.

Целью будет являться создание распределенного масштабируемого веб-сервиса, построенного с учетом RESTful – архитектурного стиля взаимодействия в сетевой модели клиент-сервер без сохранения состояния (то есть необходимые данные полностью передаются в качестве параметров запроса, без промежуточных сохранений). Такой подход позволит удовлетворить всем требованиям, предъявляемых к сервису: надежность, производительность, простота и легкость внесения изменений. Для большей наглядности изобразим полную концептуальную схему взаимодействия с помощью UML-диаграммы последовательности (см. Рисунок 1). Клиент работает с сервисом (в нашем случае – это веб-сайт по международной доставке посылок), данные по событиям сохраняются в самом сервисе; на определенные действия может потребоваться проверка. При возникновении подобного случая сервис с помощью интерфейса взаимодействия (API) антифрод-системы отправляет все имеющиеся данные о клиенте, и после анализа получает и интерпретирует результат о безопасности действия клиента.

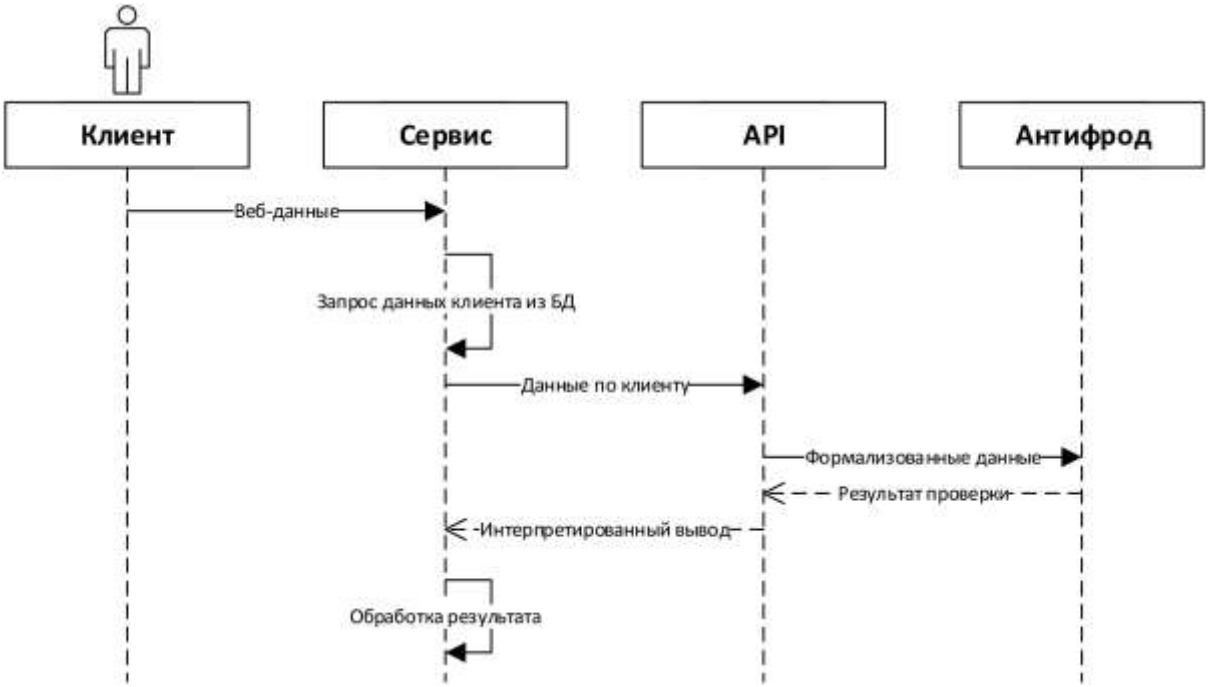

Рисунок 1 – Схема бизнес-процесса по защите от мошеннической деятельности

Опишем, какие данные сервис может получить от клиента в процессе его работы:

- страна на основе IP-адреса;
- дата и время захода на сайт;
- данные об устройстве и браузере;
- персональная информация о клиенте (имя, фамилия, дата рождения, пол, телефон, электронная почта);
- адреса доставки (включающие страну, город и т.д.);
- документ, подтверждающий личность (паспорт, водительское удостоверение);
- совершаемые действия (создание, редактирование объектов внутри веб-сайта);
- данные привязки социальных сетей и сторонних сервисов (например, торговая площадка eBay с OAuth-авторизацией через сторонний сервис);
- привязанные банковские карты;
- данные о банковских операциях.

Все данные хранятся согласно законодательству: это и запрет на хранение полного номера карты и CVV-кода, и хранение данных в зашифрованном виде, как и их передача по защищенных каналам связи. Именно на основании этих исходных данных будет работать антифрод-система.

Также определим, в какие моменты времени будет происходить проверка:

- регистрация и авторизация;
- совершение определенных действий (создание адреса, привязка телефона или социальной сети и др.);
- банковские операции;
- запланированная проверка определенных сегментов пользователей.

После того, как будет интерпретирован результат, совершаемое действие может быть помечено как подозрительное, и все операции по текущему клиенту поставлены в очередь или заблокированы.

Если представить, что такой поток проверок будет огромен, то производительность системы в целом сильно пострадает. Для того чтобы осуществить начальную предпроверку, можно использовать глобальные фильтры – заранее известный список, при попадании в который транзакция автоматически будет считаться подозрительной. Например, у нас имеется список стран, платежные карты из которых запрещены. На момент совершения операции мы пропускаем ее через каждый определенный фильтр, и в том случае, если она по каким-либо критериям не соотносится с имеющимися списками, то только тогда она передается дальше в антифрод-систему. При правильной настройке и определении фильтров это может существенно сузить круг рассматриваемых транзакций. Обозначим, какие глобальные фильтры (запрета) могут быть использованы в сфере международной логистики:

- страны, из которых авторизован клиент;
- страны, недоступные для оплаты банковской картой;
- страны адресов доставки.

Кроме того, дополнительно можно воспользоваться простыми эвристиками (продукционной моделью «ЕСЛИ-ТО») – то есть при срабатывании определенного условия транзакция сразу же будет помечена как небезопасная:

- добавление большого количества адресов;
- частый заход из разных мест (по IP-адресу);
- достижение лимита по денежным средствам;
- оплата различными способами доставки;
- несоответствие плательщика карты и данных профиля.

Таким образом, где существует жесткая логика, мы можем применить несложные эвристики, и только если этот барьер пройден, транзакция со всеми данными будет передана в антифрод-систему.

Базовая версия системы, как было указано ранее, будет размещена на

облачной платформе Microsoft Azure, в которой доступен модуль прогнозной аналитики Machine Learning (ML). В действительности можно использовать аналогичную платформу, однако предлагаемое решение полностью соответствует задаче: сервис предоставляет готовые компоненты, обладает высокой доступностью (не ниже 99,95%), отказоустойчивостью и масштабируемостью, имеет встроенный сервис очередей выполнения шагов модели; кроме того оснащен простым интерфейсом взаимодействия, настройки и мониторинга.

Для начала работы с платформой Azure необходимо создать новый эксперимент в «Студии машинного обучения». После этого каждый компонент модели необходимо добавить к проекту и соединить между собой (используя «drag&drop» мышью), получим готовую модель:

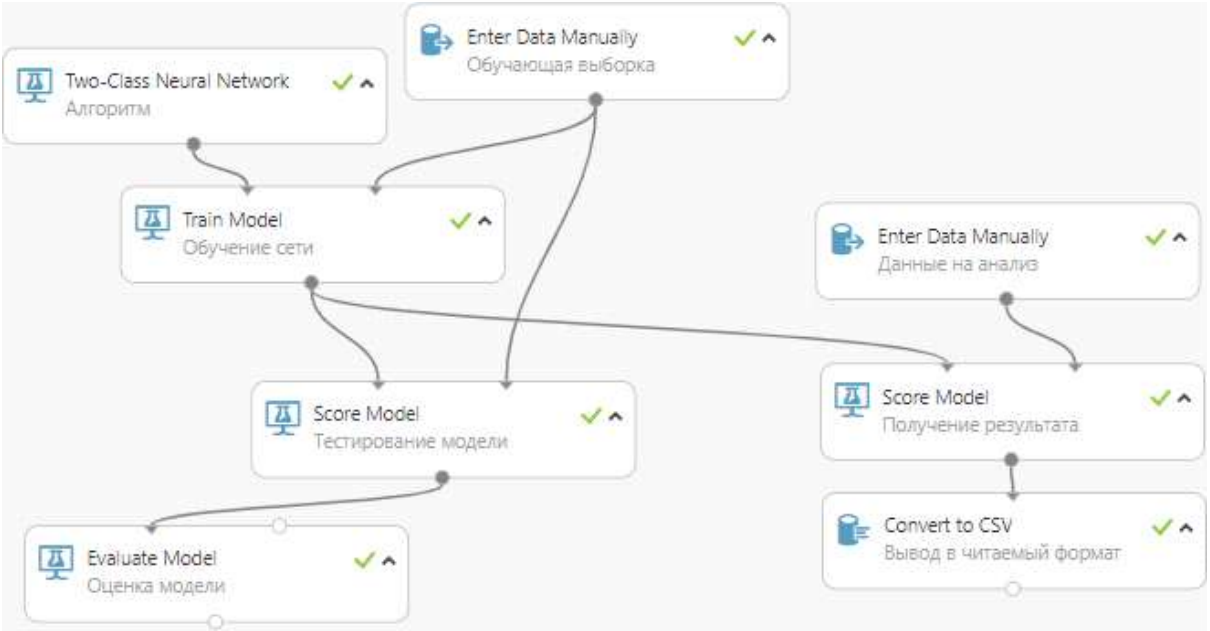

Рисунок 2 – Модель системы

Левая часть компонент отвечает за выбор алгоритма, обучение и оценку его производительности, правая – прогноз модели на поступающих данных для анализа.

В качестве начальной настройки мы будем использовать выборку из реальных данных, предварительно загрузив их в модель в формате CSV:

Data

```
reg_country,auth_false,auth_total,addr_diff,addr_false,addr_total,pack,soc,ph,card_country,card_ip,pay_false,pay_total,result
RU,0,5,0,0,1,0,1,1,RU,RU,0,0,0
RU,7,10,1,1,3,0,1,0,RU,USA,1,1,1
RU,5,73,1,1,7,20,1,1,KZ,RU,1,29,0
RU,0,5,0,0,8,12,0,0,USA,KZ,0,12,1
NG,0,3,0,0,1,0,0,0,RU,RU,0,1,0
UA,1,3,1,1,1,0,0,0,USA,UA,1,1,1
USA,14,25,1,1,1,1,0,0,RU,RU,3,5,0
```

Рисунок 3 – Фрагмент тестовой выборки

Опишем каждый из критериев (столбцов):

1. reg_country – 2-буквенный код страны клиента;
2. auth_false – кол-во неуспешных попыток авторизации;
3. auth_total – кол-во авторизаций;
4. addr_diff – кол-во адресов, не из региона проживания;
5. addr_false – кол-во адресов в запрещенные страны;
6. addr_total – общее кол-во адресов на аккаунте;
7. pack – успешно доставленных посылок;
8. soc – есть привязка социальных сетей (да/нет в формате 1/0);
9. ph – есть привязанный мобильный телефон (да/нет);
10. card_country – страна банка эмитента;
11. card_ip – страна совершения платежа;
12. pay_false – неудачных попыток оплаты;
13. pay_total – общее кол-во платежей на аккаунте;
14. result – является ли транзакция подозрительной (да/нет).

К примеру, разберем строку:

RU,3,18,1,0,3,0,1,0, RU, USA,1,1,1

– это означает, что:

клиент из РФ, имеет 3 из 18 неудачных попыток авторизации, с 3 адресами, один из которых находится не в России, но ни один не входит в список запрещенных, без посылок, с привязанной социальной сетью, но без мобильного телефона, совершил платеж русской картой в США, до этого имел один единственный неуспешный платеж; поэтому такая транзакция будет являться подозрительной (цифра 1 в конце)

На тестовой выборке необходимо выбрать один из алгоритмов классификации, который бы давал лучший (точный) результат. Производительность на реальных данных может отличаться от тестовых, именно поэтому важно понять, что в моделях не было учтено, в зависимости от чего они показывали результат хуже или лучше – и исправить ошибку, повторно запустив обучение. Тестирование необходимо проводить до того

момента, пока не будет получена приемлемая точность.

В рамках поставленной задачи будем тестировать 4 алгоритма двухклассовой классификации:

1. нейронная сеть (Neural Network);
2. логистическая регрессия (Logistic Regression);
3. метод опорных векторов (Support Vector Machine);
4. дерево решений, построенное методом градиентного роста (Boosted Decision Tree).

РЕЗУЛЬТАТЫ

Для каждого из алгоритмов были выбраны рекомендуемые настройки, и после завершения эксперимента представлены результаты оценки.

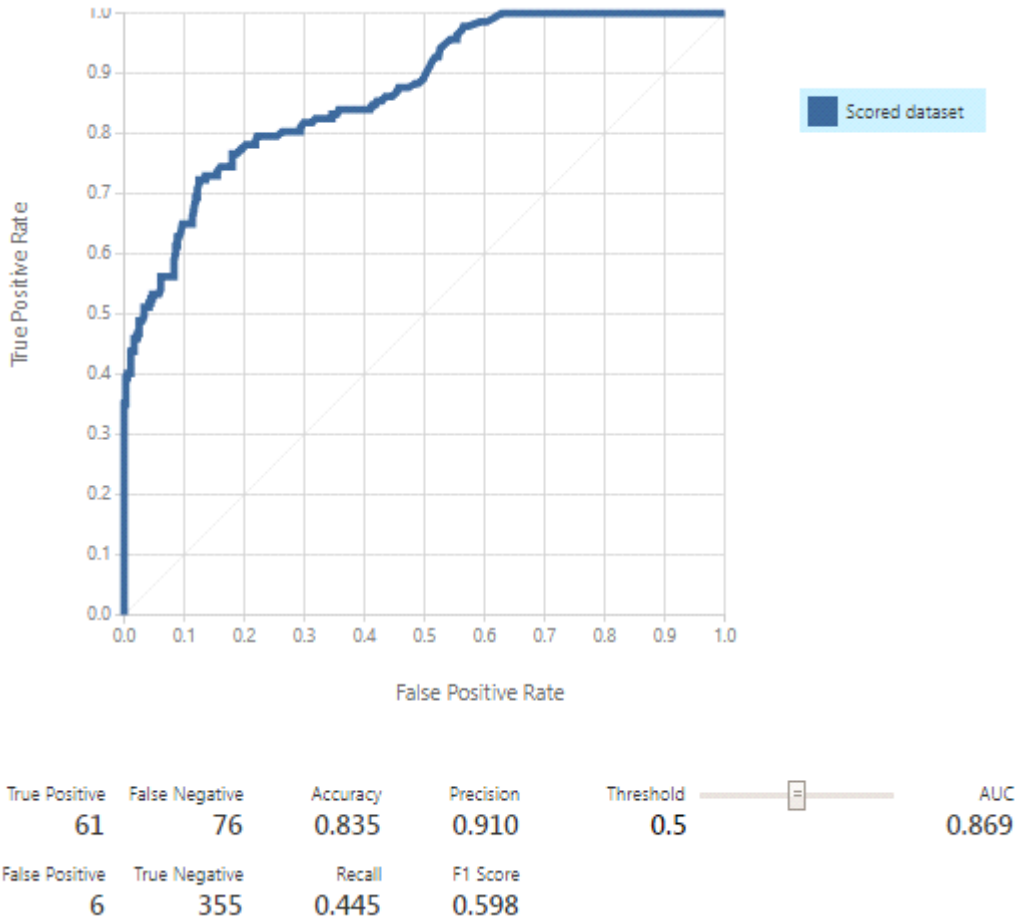

Рисунок 4 – Оценка полученной модели

В качестве простого инструмента оценка отражается в гистограмме и в статистических показателях (минимальное и максимальное значения,

медиана, математическое ожидание и т.п.); а производительность отображается с помощью матрицы неточностей, как показано на Рисунке 4. Под графиком расположены следующие характеристики:

- True Positive (TP) – правильно распознанные примеры, содержащие подозрительные транзакции;
- True Negative (TN) – правильно распознанные примеры безопасных операций;
- False Positive (FP) – кол-во нераспознанных мошеннических платежей;
- False Negative (FN) – кол-во транзакций, принятых за фрод ошибочно;
- Accuracy – точность предсказаний, отношение успешно распознанных примеров к общему числу выборки: *(TP + TN) / (TP + TN + FP + FN)*;
- Precision – соотношение правильно распознанных примеров фрода: *TP / (TP + FP)*;
- Recall – соотношение правильно распознанного фрода с учетом ошибок: *TP / (TP + FN)*;
- F1 Score – средневзвешенное значение Precision и Recall;
- AUC – общий показатель точности распознавания с учетом выбранного порога Threshold.

Показатель AUC лежит в диапазоне [0; 1], и чем значение ближе к 1, тем график выгнут к оси ординат (Y), и тем более точна полученная модель. Сводная таблица результатов эксперимента для AUC:

Таблица 1 – Полученные результаты точности алгоритмов

Neural Network	Logistic Regression	Support Vector Machine	Boosted Decision Tree
0,952	0,63	0,706	0,869

Из таблицы очевидно, что наиболее подходящим вариантом оказалась нейросеть с результатом 95,2%.

Протестируем полученную модель на новых данных, возьмем 2 транзакции (одну заведомо подозрительную, другую – совершенно безопасную):

1. *RU,0,5,1,0,8,0,0,0, USA, KZ,0,1*
2. *RU,3,8,1,0,5,0,0,0, RU, RU,0,0*

– параметры подробно описаны в разделе «Материалы и методы». В первом случае следует обратить внимание на несоответствие страны выпущенной карты (USA) и страны, откуда производится платеж (USA), ко всему прочему человек зарегистрирован в России и имеет один зарубежный адрес – поэтому в качестве результата получаем 1, т.е. транзакция является подозрительной. Во втором случае все страны совпадают, а часть

неуспешных попыток авторизации и один зарубежный адрес не делают операцию подозрительной – модель возвращает 0.

Все это говорит о том, что модель является корректной и может использоваться в качестве системы безопасности в реальном проекте.

ОБСУЖДЕНИЕ

Так как изначально для каждого из алгоритмов были использованы значения по умолчанию, результаты могли получиться слегка заниженными, так как в первую очередь была сделана ставка на производительность системы. Тем не менее каждый из параметров алгоритма (который предоставляет платформа Azure) можно улучшить, и тем самым еще больше повысив точность результатов классификации. Возьмем два алгоритма, которые показали наилучшие результаты и опишем их характеристики.

Нейронная сеть позволяет настраивать такие параметры, как: кол-во скрытых слоев, максимальное кол-во итераций на обучение и начальные веса. В нашем эксперименте были использованы следующие параметры: 10, 100, 0.5. Увеличение или уменьшение скрытых слоев может привести к тому, что сеть не сможет обучиться, а также привести к такому эффекту, что точность на обучающей выборке будет высока, однако на реальных данных она резко снизится. Увеличение числа итераций может повысить точность, однако это и увеличит время анализа; необходимо найти тот баланс, при котором увеличение итераций практически не будет влиять на точность прогнозирования. Корректировка значений весов приводит к тому, что оптимальное решение сможет найтись за меньшее число итераций.

Для алгоритма дерева решений для достижения компромисса между точностью и скоростью работы можно оперировать значениями: кол-вом деревьев, которые необходимо построить, и максимальное и минимальное кол-во листьев на каждом из них; в нашем случае это: 100 в диапазоне от 10 до 20.

На выбор конкретного алгоритма также может повлиять и последующие переобучения модели, так как существует вероятность снижения точности при новых данных. Поэтому необходимо проводить мониторинг базисного алгоритма на предмет его текущей производительности, и, если потребуется, скорректировать значения параметров или заменить алгоритм на другой. На текущий момент в рамках Azure ML существует 14 алгоритмов классификации, каждый из которых можно использовать под конкретную конфигурацию данных.

На данный момент результат работы модели позволяет однозначно интерпретировать его из множества {0, 1} (т.е. полученный ответ либо ДА – транзакция является подозрительной, либо НЕТ). Тем не менее, без постобработки мы можем увидеть, насколько точно результат соответствует действительности, т.е. числом в диапазоне [0;1] обозначен характер принадлежности к одному из двух классов. Таким образом, на стороне сервиса, осуществляющего проверку транзакции, может быть установлен определенный порог, при котором транзакция будет считаться безопасной (сейчас этот порог составляет 0,5). Кроме того в зависимости от заранее настроенных диапазонов каждую транзакцию можно отнести к категориям безопасности: [0, 0.35) – низкий, (0.35, 0.85) – средний и (0.85, 1] – высокий. Выбор таких уровней должен исходить из собственной аналитики и регулярно пересматриваться.

В текущем примере данные уже были загружены в модель, API работы с ней как веб-сервисом не был задействован. Тем не менее настроить его достаточно легко с помощью инструмента «Publish Web Service» через формат обмена JSON. На данном этапе можно столкнуться с такими ограничениями, как максимальное кол-во параллельных запросов и величина обрабатываемых данных. Приведенные сообществом цифры говорят об успешности выполнения 20 параллельных запросов, максимальный же объем данных изучен не был. Наименее критично, но ограничение может быть и на величину обучаемой выборки, были успешно проведены обучения на выборке размеров около 1 Тб. Что касается самого сервиса, то важной его характеристикой будет и время ответа – насколько быстро мы сможем получить результат проверки.

Дальнейшей перспективой разработки и внедрения сервиса будет поиск оптимального баланса между скоростью работы и точностью прогнозирования, а также определение критериев для всестороннего анализа. Также остается открытым вопрос по переобучению моделей, исследованию поведения при изменении определяющих параметров и дальнейшим инструкциям по обработке транзакции.

ЗАКЛЮЧЕНИЕ

Система обнаружения мошеннических транзакций позволяет на начальном этапе осуществлять проверку действий клиента и известных о нем данных в рамках любой существующей информационной инфраструктуры. В рамках сферы международной логистики оптимальным решением является разработка отдельного веб-сервиса, который бы эффективно отмечал безопасность операций. Вместо примитивных систем,

основанных на эвристиках, предполагается строить базис на современных методах прогнозирования. Интеллектуализировав процесс распознавания за счет применения ряда алгоритмов машинного обучения, можно получить мощное адаптивное ядро, выполняющее трудоемкие действия по классификации. Дополнительно осуществляя предобработку данных с помощью простых методов, можно добиться максимальной производительности системы, а с использованием кластеризации по уровням сформировать группы, для которых может быть настроено индивидуальное поведение на стороне сервиса, помогающее в поддержке принятия решений. Более точная настройка модели, в том числе и при переобучении, позволит добиться максимального баланса между точностью и скоростью обработки транзакций.

Очевидными преимуществами описанного подхода являются относительно короткий срок реализации и минимальный размер инвестиций в разработку. А эффективность решения на порядок выше аналогичных систем в отрасли, что позволяет использовать его в качестве надежного инструмента для пресечения и своевременного реагирования на любые возникающие попытки мошенничества.

ЛИТЕРАТУРА

1. Romanov D.V. The concept of anti-fraud management in international logistics // Антропоцентрические науки: инновационный взгляд на образование и развитие личности. Материалы VII Международной научно-практической конференции, 2018 – 323-324 с.
2. Рындин А.А., Сапегин С.В. Автоматизация проектирования корпоративных информационных систем на основе методов многовариантной интеграции // ВГТУ, 2013 – 237 с.
3. Халин В.Г., Чернова Г.В. Системы поддержки принятия решений // Юрайт, 2015 – 494 с.
4. Ясенев В.Н. Информационная безопасность в экономических системах: Учебное пособие // ННГУ, 2006 – 253 с.
5. Петухов Д. Антифрод. Режим доступа: https://habrahabr.ru/post/253725
6. De Ruiter A. Best practices on designing business intelligence solutions using SSAS, SSIS and other Microsoft BI tools. Режим доступа: https://blogs.msdn.microsoft.com/andreasderuiter/

D.V. Romanov, N.A. Ryndin

FRAUDULENT TRANSACTIONS DETECTION SYSTEM DESIGN IN

INTERNATIONAL LOGISTICS

Voronezh State Technical University

The article is devoted to the design of effective system for combat fraud using client's publicly available data of the package delivery service. Because of the growth of frauds, business incurs heavy losses and complete system for fraud monitoring can stop suspicious actions and make recommendations for their further processing, which will significantly reduce economic, financial and reputational risks. The system is a single resource, which is implemented as a cloud web server and include the intellectual core for execution base labor-intensive operations on transaction analysis and detection. The analysis is based on well-proven machine learning algorithms based on supervised learning. For detection of fraudulent transactions model is built and tested, the best one is chosen. It classifies each transaction during data manipulations and make 2 actions depending on the security level: rejects or interprets it and may give recommendations for further action. After security levels are reviewed or added, the system retrained every time; training data is stored in the centralized repository. The developed service is supposed to be used for companies engaged in international logistics and had a simple and clear interface integration and interaction.

Keywords: intelligent design, machine learning algorithms, decision support system, fraud transactions, anti-fraud, international logistics.

REFERENCES

1. Romanov D.V. The concept of anti-fraud management in international logistics // Antropotsentricheskie nauki: innovatsionny vzglyad na obrazovanie i razvitie lichnosti. Materialy VII Mezhdunarodnoy nauchno-prakticheskoy konferentsii, 2018 – 323-324 p.
2. Ryndin A.A., Sapegin S.V. Avtomatizatsiya proektirovaniya korporativnyh informatsionnyh sistem na osnove metodov mnogovariantnoy integratsii // VSTU, 2013 – 237 p.
3. Halin V.G., Chernova G.V. Sistemy podderzhki prinyatiya resheniy // Urait, 2015 – 494 p.
4. Yasenev V.N. Infomatsionnaya bezopasnost v ekonomicheskih sistemah: Uchebnoe posobie // UNN, 2006 – 253 p.
5. Petuhov D. Antifraud, https://habrahabr.ru/post/253725
6. De Ruiter A. Best practices on designing business intelligence solutions using SSAS, SSIS and other Microsoft BI tools, https://blogs.msdn.microsoft.com/andreasderuiter/