ЭФФЕКТИВНОСТЬ КЛАССИФИКАТОРОВ ДЛЯ ВЫЯВЛЕНИЯ ФРОДА В ФИНАНСОВЫХ ТРАНЗАКЦИЯХ

Левашов М.В.[1], Овчинников П.В.[2]

Аннотация

Цель статьи: *экспериментальный расчет эффективности алгоритмического метода выявления мошеннических финансовых транзакций с использованием классификаторов, построенных с помощью большого объема обучающей выборки из реальных транзакций. Сравнение полученных значений эффективностей с аналогичными данными, рассчитанными ранее в статистической модели процесса фрод-мониторинга.*

Метод: *применение стандартного алгоритма построения классификаторов для выявления мошеннических транзакций, основанного на анализе данных обучающей выборки с использованием в качестве оценок эффективности как статистических параметров (ошибки 1-го и 2-го рода), так и алгоритмических параметров точности и полноты.*

Полученный результат: *найдена последовательность классификаторов, эффективности использования которых в целом соответствуют полученным ранее ([1]) с применением близкого к оптимальному статистического метода аналогичным данным, основанным на расчете статистической модели рассматриваемых процессов. Сделан вывод о том, что данная методика позволяет получить близкие к реальным численные значения эффективностей. При использованной реальной обучающей выборки этот метод позволяет достичь определенного эффекта сокращения количества опробуемых вариантов подозрительных на фрод транзакций.*

Ключевые слова: *фрод, фрод мониторинг, транзакция, платежная транзакция, теоретико-вероятностная модель, классификация, обучающая выборка.*

DOI:10.21681/2311-3456-2019-5-63-69

Введение

Обязанность банка противодействовать переводу денежных средств без согласия клиента в явном виде была законодательно установлена еще в 2011 году[3]. В 2018 году[4] также законодательно банкам разрешено приостанавливать исполнение платёжного поручения при наличии признаков мошенничества. В этот промежуток времени киберпреступники развернули настоящую охоту за денежными средствами клиентов банков. По данным компании Group-IB[5] за период с июня 2015 по июнь 2016 года в России в результате целевых атак на финансовые учреждения и физических лиц киберпреступники похитили в общей сложности 3,8 миллиарда рублей. Из них у российских банков украли в общей сложности 2,5 миллиарда рублей. При этом у юридических лиц с помощью троянов удалось похитить почти 1 миллиард рублей. Group-IB зафиксировала взрывной рост числа успешных атак на пользователей Android-устройств, которые потеряли от действий хакеров порядка 350-ти миллионов рублей, что почти на 500% превышает прошлый период.

Злоумышленники используют различные возможности подготовки и отправки мошеннических электронных финансовых транзакций, имеющих легальную штатную криптозащиту. Такие возможности появляются при кибератаках на клиентскую автоматизированную банковскую систему (далее – АБС), включая системы формирования и передачи электронных платежных поручений. Здесь преступники применяют фишинг, зараженные электронные письма, методы социальной инженерии. Такие мошеннические транзакции крипто обработаны (т.е., зашифрованы и подписаны электронными подписями) штатным образом. Это означает, что при крипто проверке этих платежей в банке (т.е., при расшифровке и проверке электронных подписей) никаких нарушений выявлено не будет. В этом случае предотвратить хищение денежных средств поможет только система фрод-мониторинга, которая по различным параметрам как автоматизированных средств отправки транзакций плательщика (то есть, клиента банка), так и самой транзакции оценивает вероятность (или скоринг) того, что транзакция является мошеннической. Простейшим примером системы фрод-мониторинга может являться простое ограничение на сумму платежа. Если платеж больше определенной величины, то он считается подозрительным на фрод и требует дополнительной проверки (подтверждения) его легаль-

3 Статья 27 Федерального закона «О национальной платежной системе» от 27.06.2011 №161-ФЗ.

4 Статья 3 федерального закона «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств» от 27.06.2018 №167-ФЗ.

5 Отчет Group-IB, представленный на конференции «CyberCrimeCon 2016», Москва, Культурный центр ЗИЛ, 13.10.2016, http://bit.samag.ru/news/more/2240.

1 Левашов Михаил Васильевич, кандидат физико-математических наук, старший научный сотрудник, профессор НИУ ВШЭ, Москва, Россия, E-mail: mlevashov@hse.ru

2 Овчинников Пётр Владимирович, студент магистратуры НИУ ВШЭ, E-mail: petr.ovchinnikov.fa@mail.ru

ности. Заметим ([11]), что современные системы фрод-мониторинга учитывают до 100 и более параметров, по которым определяется скоринг.

Системам фрод-мониторинга, используемым в различных ситуациях, посвящено значительное количество работ. В [4] проведен анализ подобных систем в АБС и предложены конкретные новые решения. В [12] рассматривается задача фрод-мониторинга на сетях связи, которые широко используются для подтверждения подлинности финансовых транзакций. В [4] проведена экспертная оценка риска на примерах некоторых наиболее распространенных угроз фрода в сетях связи сети VoIP стандарта сигнализации SIP. В [5] на основе нейронных сетей решается задача выявления мошеннических транзакций, осуществляемых с использованием банковских карт. В [6] изучена возможность применения фрод-мониторинга в структуре внутреннего аудита в банках. В результате были разработаны внутренние индикаторы, сигнализирующие о необходимости проведения проверки. В [8] на основе статистики РФ 2016 года проведен анализ мошеннических действий с банковскими картами. Проведена классификация угроз и на ее основе предложена система фрод-мониторинга. В [10] сделан вывод о необходимости создания единой общероссийской службы фрод-мониторинга и предотвращения мошенничества с электронными денежными средствами. В исследовании Gartner[6] приводятся данные о наиболее распространенных на рынке продуктах, посвященных поведенческому анализу пользователей, который, в свою очередь, применяется в современных сложных системах фрод-мониторинга.

Одной из основных задач в системах фрод-мониторинга является расчет и обоснование оценок их эффективности, полученных в разных математических моделях. Практическими работами в этом направлении занимаются ведущие отраслевые и инновационные компании[7]. Теоретическое обоснование оценок эффективности связано с расчетом подходящих моделей исследуемых процессов с применением различных методов анализа. В уже упомянутой выше работе [4] в расчетах применялась методика исследования нечетких множеств. В [9] изучены параметры математической модели, описывающей работу программного модуля системы фрод-мониторинга. Оптимизируя эти параметры, авторам удалось повысить эффективность всей системы. В [13] рассматриваются вопросы использования машинного обучения в антифрод системах коммерческого банка. На конкретных примерах мошенничества проанализированы характерные особенности применения этого метода и обоснована необходимость его использования. В [14] и [15] предлагаются и анализируются поведенческие характеристики легальных пользователей, которые сравниваются с действиями мошенников. На этой основе построен алгоритм с учителем для их классификации.

Основным механизмом обоснования теоретических оценок эффективности может являться получение и сравнение этих оценок, исходя из разных методов (и, соответственно, математических моделей) выявления подозрительных на фрод транзакций, а также использование в этих методах реального материала. Цель данной работы заключается в применении алгоритмических подходов при построении классификаторов, выявляющих подозрительные транзакции, и сравнении рассчитанных параметров эффективности с известными ([1]) результатами, полученными другими – статистическими – методами. Дополнительным условием исследований является обязательное использование реального материала транзакций.

Постановка задачи

Итак, имеем гипотетическую многоступенчатую систему фрод-мониторинга транзакций, состоящих из электронных платежных документов юридических лиц – клиентов банка. Все транзакции уже штатно расшифрованы и проверены их электронные подписи, которые оказались корректными. Эти транзакции попадают на вход системы фрод-мониторинга. На вход каждой ступени этой системы подаются все оставшиеся от предыдущей ступени подозрительные на фрод транзакции. При обработке часть из них признается легальными и отсеивается. Остальная часть остается подозрительными на фрод и подаётся на вход следующей ступени системы фрод-мониторинга. И так далее, пока все ступени не будут пройдены. На последней ступени оставшиеся подозрительные транзакции проверяются операторами (возможно, роботами) путем дозвона до всех компаний, которые эти транзакции прислали.

В работе [1] была рассмотрена теоретико-вероятностная модель одной ступени фрод мониторинга транзакций, на которой определение подозрительных на фрод транзакций производился с помощью статистического критерия, близкого в определенном смысле к критерию отношения правдоподобия. В классическом виде критерий отношения правдоподобия здесь не может быть применен, так как 2 гипотезы «фрод» и «не фрод», которые необходимо было различить, не являются простыми гипотезами. Для определения параметров распределений, которые должен различить применяемый статистический критерий, был использован материал, полученный из реальных транзакций объема порядка 1-го миллиона. При этом модель расчета предполагала статистическую независимость времени платежа и его суммы. В указанной модели удалось получить достаточно простые выражения для эффективности построенного статистического критерия, определяемой ошибками 1-го рода (вероятность принять фрод за легальную транзакцию) и 2-го рода (вероятность принять легальную транзакцию за фрод). В зависимости от параметров критерия были получены 3 пары ошибок 1-го рода и 2-го рода. Это, соответственно:

(0,0773; 0,8371); (0,6379; 0,2943) и (0,1327; 0,7261) (1)

6 Avivah Litan “Market Guide for User and Entity Behavior Analytics”, Gartner, 2015.

7 https://infosec.ru/glavnye-temy/antifrod / https://www.banki.ru/news/lenta/?id=10766545

УДК 004.942 + 004.056 DOI: 10.21681/2311-3456-2019-5-63-69

Здесь в каждой паре 1-я цифра фактически означает долю мошеннических транзакций, принятых за легальные, а 2-я – фактически означает долю легальных транзакций, которые останутся для проверки на следующей ступени (то есть, принятых за мошеннические).

В настоящей работе, которую можно считать продолжением работы [1], на рассматриваемой одной ступени гипотетической системы фрод-мониторинга для выявления фрода будет использован классификатор транзакций, который конструируется на основе имеющейся обучающей выборки полученной из реальных транзакций. При этом в нашей модели не будут делаться предположения о независимости суммы и времени транзакции. Затем рассчитанные значения эффективности классификатора будут сравниваться с полученными в [1] аналогичными цифрами. Эти сравнения дадут возможность сделать определенные выводы о качестве этих моделей и связи расчётных эффективностей с реальными процессами и эффективностями.

Решение задачи

Итак, в качестве обучающей выборки мы имеем материал, полученный из реальных транзакций конкретного финансового учреждения. Объем исходных данных: 1 млн. легальных и 230 мошеннических транзакций. В каждой транзакции по требованиям конфиденциальности были элиминированы все поля, кроме суммы и суточного времени платежа. Здесь термин «суточное» время означает время создания транзакции без учета даты. Полученные данные мы и называем обучающей выборкой. Весь этот материал после обработки был представлен в следующем виде:

Здесь по вертикальной оси расположена сумма транзакции (в условных единицах – у.е.), по горизонтальной – суточное время транзакции (в минутах). Каждая точка отражает транзакцию с 2-мя параметрами – суммой (в у.е.) и суточным временем (в минутах). Синими точками отмечены легальные транзакции, красными – мошеннические транзакции (фрод). Классификатором мошеннической транзакции (фрод) является, вообще говоря, произвольная область (или подмножество на плоскости рис. 1), при попадании в которую исследуемая «урезанная» транзакция будет считаться подозрительной на фрод и оставаться для дальнейших испытаний на следующей ступени гипотетической системы фрод-мониторинга. Если же эта транзакция не попадет в классификатор, то она считается легальной и отсеивается. Понятно, что при таком алгоритме лучшие классификаторы должны содержать как можно больше красных точек и как можно меньше – синих. Изучая методом «естественного интеллекта» обучающую выборку (рис. 1), как визуально (при большом разрешении), так и различными метриками, мы пришли к качественному выводу, что мошеннические транзакции в данной обучающей выборке слабо отличаются от легальных. Этот вывод соответствует сути вопроса, так как злоумышленники всегда будут стараться приспособиться, по крайне мере, по времени и сумме к транзакциям реальных легальных пользователей. Поэтому вначале были выбраны и исследованы простые по конфигурации классификаторы, имеющие вид прямоугольников. Пример:

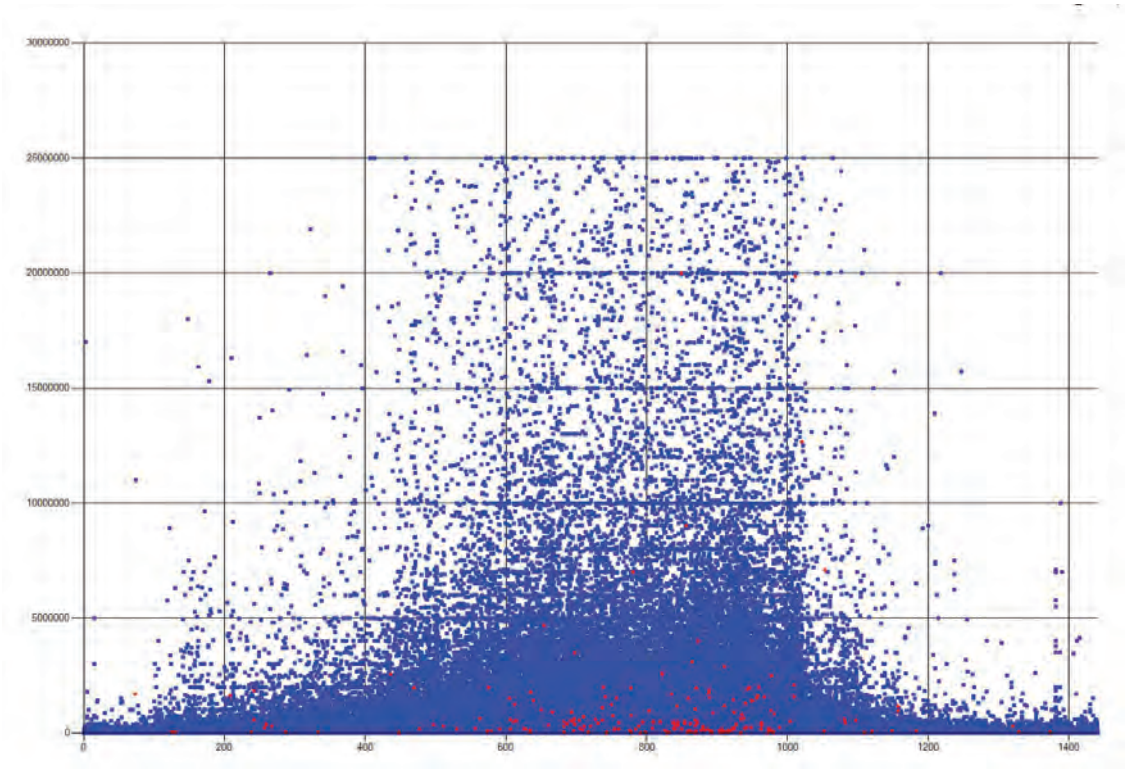

Рис. 1

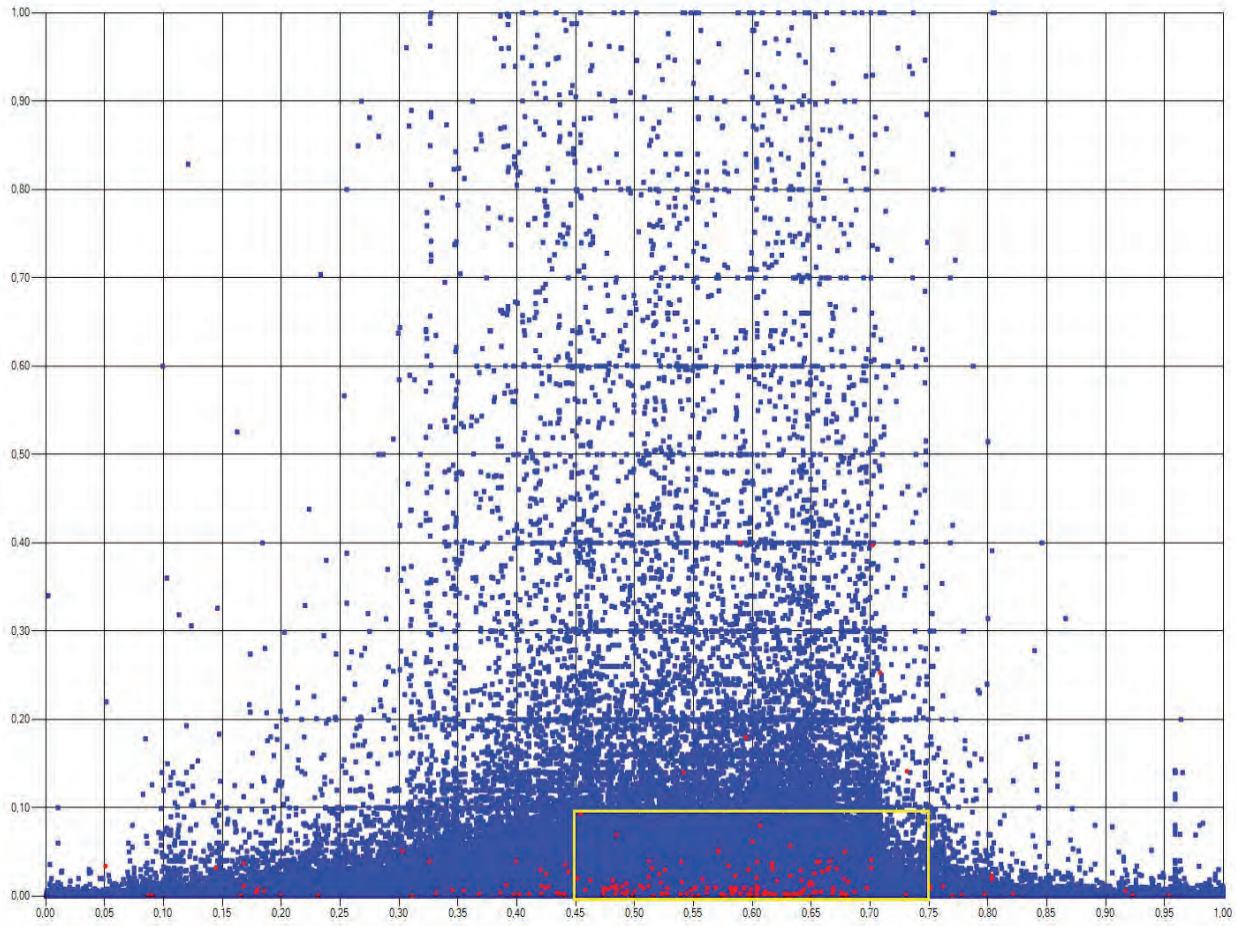

Рис. 2

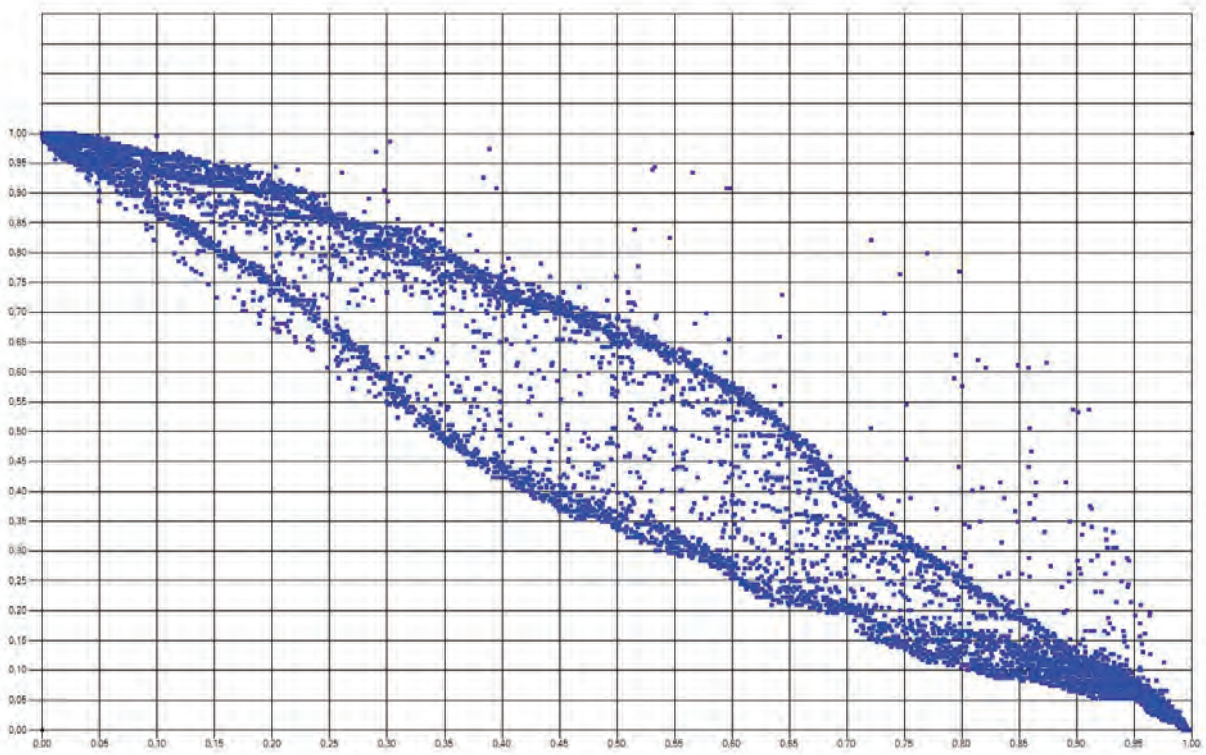

Рис. 3

УДК 004.942 + 004.056 DOI: 10.21681/2311-3456-2019-5-63-69

Эффективность классификатора и в этом алгоритмическом методе принятия решения о фроде или легальности транзакции может быть оценена как статистическими, так и алгоритмическими параметрами. Статистические параметры это - те же ошибки 1-го и 2-го рода, о которых говорилось выше. В терминах красных и синих точек оценкой ошибки 1-го рода является относительная частота (в обучающей выборке) V(k) красных точек (фрод), не попавших в классификатор (т.е., число таких точек, деленное на число всех красных точек). Оценкой ошибки 2-го рода является относительная частота (в обучающей выборке) V(c) синих точек (легальные транзакции), попавших в классификатор (т.е., число таких точек, деленное на число всех синих точек).

В качестве примера был выбран представленный на рис. 2 классификатор, при котором получились удивительно близкие к полученным в работе [1] ошибки (1). После этого были проведены масштабные испытания с выбором 10000 классификаторов и расчётом их ошибок. На следующем рисунке 3 представлены все полученные 10000 пар ошибок.

Здесь по горизонтальной оси – ошибка 1-го рода; по вертикальной – 2-го.

На этом рисунке также прослеживается соответствие полученных результатов значениям работы [1], полученным статистическим методом и рассчитанным в другой теоретико-вероятностной модели.

Рассмотрим теперь иные широко известные и распространенные в алгоритмических методах, например, в методах машинного обучения метрики: точности P и полноты R. Они определяются следующим образом.

P (precision) = tp / tp + fp R (recall) = tp / tp + fn

Здесь (для транзакций из обучающей выборки):

- tp (true positives) истинно-положительные — количество мошеннических транзакций, которые попали в классификатор,
- fp (false positives) ложно-положительные — количество легальных транзакций, которые попали в классификатор,
- fn (false negatives) ложно-отрицательные — количество мошеннических транзакций, которые не попали в классификатор.

Как нетрудно заметить, мера точности характеризует долю попавших в классификатор мошеннических транзакций среди всех попавших в классификатор транзакций, а мера полноты – долю правильно определенных классификатором мошеннических транзакций.

Ниже в таблице приведены знаковые значения эффективностей для 36 (из 10000) классификаторов, выбранных в качестве представителей классов, демонстрирующих существенные различия в этих значениях

(знаковые в том смысле, что значения ошибок Alpha (1-го рода) и Betha (2-го рода), а также точности (R) здесь сгруппированы в несколько классов, внутри которых они близки по своим значениям).

При этом, когда уменьшается ошибка признать фрод не фродом, количество отсеянных на данной ступени системы фрод-мониторинга транзакций также уменьшается, то есть алгоритм оставляет для следующей ступени фрод-мониторинга больше транзакций. Точность здесь получилась везде практически одинаковая и очень близкая к нулю. Это объясняется структурой обучающей выборки, в которой (как и в реальности) очень мало мошеннических транзакций и эти транзакции достаточно близки к легальным. Поэтому практически в любом классификаторе число легальных транзакций на несколько порядков больше, чем мошеннических. Полнота же, как нетрудно видеть из определения, и ошибка 1-го рода дают в сумме единицу. Эта закономерность также приблизительно выполняется в представленной таблице.

В практике использования систем фрод мониторинга доля мошеннических транзакций обычно составляет проценты от числа подозрительных на фрод транзакций, оставшихся к последней ступени проверки (оператором). В свою очередь, доля этих подозрительных

·	Betha	Alpha	Precision	Recall							
1)	0,7794;	0,1572;	0,0002;	0,8428	0,7822;	0,1485;	0,0002;	0,8515	0,7834;	0,1441;	0,0003;	0,8559
	0,7844;	0,1441;	0,0002;	0,8559								
2)	0,7848;	0,1397;	0,0003;	0,8603	0,7852;	0,1397;	0,0003;	0,8603	0,7854;	0,1354;	0,0003;	0,8646
	0,7857;	0,1310;	0,0003;	0,8690								
3)	0,7859;	0,1310;	0,0003;	0,8690	0,6604;	0,2707;	0,0003;	0,7293	0,6628;	0,2620;	0,0003;	0,7380
	0,6639;	0,2576;	0,0003;	0,7424								
4)	0,6647;	0,2576;	0,0003;	0,7424	0,6651;	0,2533;	0,0003;	0,7467	0,6654;	0,2533;	0,0003;	0,7467
	0,6656;	0,2489;	0,0003;	0,7511								
5)	0,6659;	0,2445;	0,0003;	0,7555	0,6661;	0,2445;	0,0003;	0,7555	0,4964;	0,3843;	0,0003;	0,6157
	0,4983;	0,3799;	0,0003;	0,6201								
6)	0,4991;	0,3755;	0,0003;	0,6245	0,4997;	0,3755;	0,0003;	0,6245	0,5000;	0,3755;	0,0003;	0,6245
	0,5003;	0,3755;	0,0003;	0,6245	0,5005;	0,3755;	0,0003;	0,6245	0,5007;	0,3712;	0,0003;	0,6288
7)	0,5008;	0,3712;	0,0003;	0,6288	0,2618;	0,6114;	0,0003;	0,3886	0,2628;	0,6114;	0,0003;	0,3886
8)	0,2633;	0,6070;	0,0003;	0,3930	0,2636;	0,6070;	0,0003;	0,3930	0,2638;	0,6070;	0,0003;	0,3930
9)	0,2639;	0,6070;	0,0003;	0,3930								
10)	0,2640;	0,6070;	0,0003;	0,3930								
11)	0,2641;	0,6026;	0,0003;	0,3974								
12)	0,2642;	0,6026;	0,0003;	0,3974								

Рис. 4

транзакций, обычно, составляет доли процента от общего количества транзакций. Параметры настройки системы фрод мониторинга выбираются таким образом, чтобы, во-первых, вероятность отнесения мошеннической транзакции к легальной на всех ступенях проверки была относительно небольшой. А, во-вторых, общее количество оставшихся подозрительных на фрод транзакций на этапе операторской проверки было приемлемым с точки зрения нагрузки на операторов системы.

Выводы

1. Несмотря на сильные модельные предположения работы [1] о независимости случайных величин, описывающих время и сумму транзакций, а также дальнейшие упрощения, сделанных в этой работе при расчете критерия отношения правдоподобия, ошибки, характеризующие эффективность фрод мониторинга, хорошо согласуются с аналогичными ошибками, полученными в настоящей работе другими методами и в другой математической модели.
1. Наверное, эти ошибки достаточно хорошо отображают реальное положение вещей, так как в 2-х разных моделях получились сходные результаты.
2. При использованной реальной обучающей выборки рассмотренный метод позволяет достичь определенного эффекта сокращения количества опробуемых вариантов подозрительных на фрод транзакций.

Заключение

В предложенных в [1] и в настоящей работе математических моделях, при имеющемся материале в виде суммы и суточном времени транзакций статистический и кластерный подходы дают примерно одинаковые значения эффективностей как по доле пропущенных мошеннических транзакций, так и по степени сокращения числа остающихся для дальнейшей обработки транзакций.

Литература

1. Левашов М.В., Кухаренко А.В. Эффективность критерия отношения правдоподобия в статистической модели фрод-мониторинга в интернет-банкинге // Вопросы защиты информации. 2018. № 2. С. 66-71.
2. Кондратюк П.А. Разработка системы фрод-мониторинга электронных платежей // Дипломный проект. МГТУ им. Н.Э. Баумана. Москва. 2017.
3. Белименко Б.В. Проблемы ИБ в автоматизированных банковских системах // Ученые записки Таврического национального университета имени В.И. Вернадского. Серия «Экономика и управление». Том 27 (66). 2014. № 4. С. 28-31.
4. Бельфер Р.А., Калюжный Д.А., Тарасова Д.В. Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств // Вопросы кибербезопасности. 2014. С.33.
5. Климов В. В., Кузин М. В., Щукин Б. А. Мониторинг мошеннических транзакций с помощью комитетов нейронных сетей // Безопасность информационных технологий. 2015. №1.
6. Разина Ольга, Костерина Татьяна. Инновационные инструменты фрод-мониторинга в практике внутреннего аудита банка // Вопросы инновационной экономики. 2015. Том 5. Выпуск 4. С. 256.
7. 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.
8. Александров В.В., Пономаренко С.В., Бирюков М.В. Предотвращение мошеннических действий по банковским картам с помощью системы фрод-мониторинга // Вестник Белгородского университета кооперации, экономики и права. 2017. № 3. С. 225.
9. Логачев В.Г., Карякин Ю.Е., Игнатьева А.М., Любякина Е.А. Проблема выбора критериев для построения математической модели процесса предотвращения несанкционированных переводов денежных средств // Международный научно-исследовательский журнал. 2017. № 06 (60). С. 149.
10. Божор Ю.А. Необходимость создания в России федеральной системы фрод-мониторинга // Расчеты и операционная работа в коммерческом банке. 2013. № 6. С. 80–87.
11. Бондаренко Т. Г. Рисковые операции по платежным картам: система мониторинга // Сборник статей «Прорывные экономические реформы в условиях риска и неопределенности» / Международная научно-практическая конференция. Изд. Аэтерна. 2015. С. 13-15.
12. Пузанов Д.Е., Литягин П.Е. Методы борьбы с фродом на сетях связи // Мир Телекома. 2014. № 1. С. 10.
13. Замятина Е.В., Лученко А.В. Анализ значимости алгоритмов Machine Learning в антифрод - системах коммерческого банка // материалы и методы инновационных исследований и разработок / сборник статей Международной научно-практической конференции 10 марта 2018. С. 129-131.
14. Крылов П. Схемы хищений в системах ДБО и пять уровней противодействия им // Расчеты и операционная работа в коммерческом банке. 2018. № 3 (145). С. 46-59.
15. Слипенчук П.В. Алгоритм извлечения характерных признаков из данных пользовательских активностей // Вопросы кибербезопасности. 2019. № 1. С. 53-58.

УДК 004.942 + 004.056 DOI: 10.21681/2311-3456-2019-5-63-69

THE EFFECTIVENESS OF CLASSIFIERS FOR IDENTIFY FRAUD IN THE FINANCIAL TRANSACTIONS

M. Levashov[8] P. Ovchinnikov[9]

The purpose of the article: *experimental calculation of the effectiveness of the algorithmic method for detecting fraudulent financial transactions using classifiers built using a large volume of leaning samples from real transactions. Comparison of the obtained efficiency values with similar data calculated earlier in the statistical model of the fraud monitoring process.*

Method: *the use of a standard algorithm for constructing classifiers to identify fraudulent transactions based on the analysis of leaning sample data using both statistical parameters (errors of the 1st and 2nd kind) and algorithmic parameters of precision and recall.*

The obtained result: *a sequence of classifiers is found, the efficiency of which generally correspond to the previously obtained efficiency ([1]) with the use optimal statistical method based on the calculation of the statistical model of the processes under consideration. It is concluded that this technique allows to obtain close to real numerical values of efficiency. With the use of a real leaning sample, this method allows to achieve a certain effect of reducing the number of tested variants of suspicious transactions.*

Keywords: *fraud, fraud monitoring, transaction, payment transaction, probabilistic model, classification, training set.*

References

1. M.V. Levashov, A.V. Kuharenko. Effektivnost' kriteriya otnosheniya pravdopodobiya v statisticheskoj modeli frod-monitoringa v internet-bankinge // Voprosy zashchity informacii. 2018. № 2. S. 66-71.
2. Kondratyuk P.A. Razrabotka sistemy frod-monitoringa elektronnyh platezhej // Diplomnyj proekt. MGTU im. N.E. Baumana. Moskva. 2017.
3. Belimenko B.V. Problemy IB v avtomatizirovannyh bankovskih sistemah // Uchenye zapiski Tavricheskogo nacional'nogo universiteta imeni V.I. Vernadskogo. Seriya «Ekonomika i upravlenie». Tom 27 (66). 2014. № 4. S. 28-31.
4. Bel'fer R.A., Kalyuzhnyj D.A., Tarasova D.V. Analiz zavisimosti urovnya riska informacionnoj bezopasnosti setej svyazi ot ekspertnyh dannyh pri raschetah s ispol'zovaniem modeli nechetkih mnozhestv // Voprosy kiberbezopasnosti. 2014. S. 33.
5. V. V. Klimov, M. V. Kuzin, B. A. SHCHukin. Monitoring moshennicheskih tranzakcij s pomoshch'yu klmitetov nejronnyh setej // Bezopasnost' informacionnyh tekhnologij. 2015. №1.
6. Ol'ga Razina, Tat'yana Kosterina. Innovacionnye instrumenty frod-monitoringa v praktike vnutrennego audita banka // Voprosy innovacionnoj ekonomiki. 2015. Tom 5. Vypusk 4. S. 256.
7. 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. R. 147–172.
8. Aleksandrov V.V., Ponomarenko S.V., Biryukov M.V. Predotvrashchenie moshennicheskih dejstvij po bankovskim kartam s pomoshch'yu sistemy frod-monitoringa // Vestnik belgorodskogo universiteta kooperacii, ekonomiki i prava. 2017. № 3. S. 225.
9. Logachev V.G., Karyakin YU.E., Ignat'eva A.M., Lyubyakina E.A. Problema vybora kriteriev dlya postroeniya matematicheskoj modeli processa predotvrashcheniya nesankcionirovannyh perevodov denezhnyh sredstv // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2017. № 06 (60). S. 149.
10. Bozhor YU.A. Neobhodimost' sozdaniya v Rossii federal'noj sistemy frod-monitoringa // Raschety i operacionnaya rabota v kommercheskom banke. 2013. № 6. S. 80–87.
11. Bondarenko T. G. Riskovye operacii po platezhnym kartam: sistema monitoringa // Sbornik statej «Proryvnye ekonomicheskie reformy v usloviyah riska i neopredelennosti». S. 13.
12. Puzanov D.E., Lityagin P.E. Metody bor'by s frodom na setyah svyazi // Mir Telekoma. 2014. № 1. S. 10.
13. Zamyatina E.V., Luchenko A.V. Analiz znachimosti algoritmov Machine Learning v antifrod - sistemah kommercheskogo banka // Mezhdunarodnaya nauchno-prakticheskaya konferenciya 10 marta 2018. S. 129.
14. Krylov P. Skhemy hishchenij v sistemah DBO i pyat' urovnej protivodejstviya im // Raschety i operacionnaya rabota v kommercheskom banke. 2018. № 3 (145). S. 46-59.
15. Slipenchuk P.V. Algoritm izvlecheniya harakternyh priznakov iz dannyh pol'zovatel'skih aktivnostej // Voprosy kiberbezopasnos. 2019. № 1. S. 53-58.

8 Mikhail Levashov, Ph.D., Professor of HSE, Moscow, Russia, E-mail: mlevashov@hse.ru

9 Peter Ovchinnikov, HSE master's student, E-mail: petr.ovchinnikov.fa@mail.ru