На правах рукописи

Муханов Лев Евгеньевич

Модели выявления и предотвращения несанкционированных транзакций в области банковских карт в системе мягкого реального времени

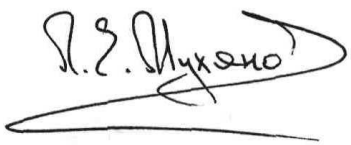
05.13.01 – системный анализ, управление и обработка информации (научное обслуживание)

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Автор:



Москва – 2009

Работа выполнена в Национальном исследовательском ядерном университете «МИФИ».

Научный руководитель:	доктор технических наук, профессор Щукин Борис Алексеевич
Официальные оппоненты:	доктор технических наук, профессор Гетманов Виктор Григорьевич кандидат технических наук, с.н.с. Шилов Валерий Владимирович
Ведущая организация:	Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В.В. Соломатина (ВНИИНС)

Защита состоится «30» декабря 2009 г. в 12 часов 00 мин. на заседании диссертационного совета Д 212.130.03 в аудитории К-608 при НИЯУ МИФИ, расположенном по адресу: 115409, Москва, Каширское шоссе, 31.

С диссертацией можно ознакомиться в библиотеке Национального исследовательского ядерного университета «МИФИ».

Автореферат разослан « » ноября 2009 г.

Отзывы и замечания по автореферату в двух экземплярах, заверенные печатью, просьба высылать по вышеуказанному адресу на имя ученого секретаря диссертационного совета.

Ученый секретарь
диссертационного совета,

д.т.н., профессор *Шумилов Ю.Ю.*

Общая характеристика работы

Актуальность темы диссертации. На сегодняшний день количество людей, использующих банковские карты в качестве безналичной формы оплаты, постоянно увеличивается. Как и в любой сфере деятельности, касающейся финансов или их передвижения, банковские организации при работе с картами сталкиваются с мошенничеством. За последние несколько лет сложилась явная тенденция к увеличению числа мошенничеств в этой области, несмотря на постоянное совершенствование систем защиты. Отмечается ежегодный рост потерь международных платежных сетей и банков из-за подобного вида преступлений. Мошенники пользуются уязвимостью систем защиты банковских карт и систем осуществления транзакций. Поэтому разработчики банковского оборудования и программного обеспечения постоянно совершенствуют данные системы, но мошенники также улучшают свои методы и находят новые способы осуществления мошенничества.

В качестве одного из элементов системы безопасности осуществления транзакций банковские организации используют системы выявления несанкционированных транзакций. Данные системы базируются на проведении постоянного мониторинга транзакций и выявлении подозрительных транзакций на основе значений параметров этих транзакций.

Большинство существующих систем выявления несанкционированных транзакций в области банковских карт используют систему эвристических правил, описывающую значения параметров мошеннических (несанкционированных) транзакций или значения параметров последовательности транзакций, которая характерна для случаев мошенничества. Основной недостаток такого подхода заключается в том, что результаты выявления несанкционированных транзакций зависят от соответствующих сотрудников и эффективности написанных правил.

К недостатку существующих систем выявления несанкционированных транзакций можно отнести и то, что данные системы позволяют только выявлять несанкционированные транзакции, но не отклонять их во время авторизации. Функциональность отклонения подозрительных транзакций позволит сохранить денежные средства в случае реального мошенничества, но в случае ошибочного решения системы будет отклонена легальная или авторизована несанкционированная транзакция. Поэтому можно сформулировать две принципиально разные задачи: выявление несанкционированных транзакций и предотвращение несанкционированных транзакций.

Таким образом, на данный момент актуальна задача создания моделей выявления и

предотвращения несанкционированных транзакций, базирующихся на использовании элементов искусственного интеллекта, и системы, функционирующей на основе данных моделей в режиме мягкого реального времени.

Объектом исследования несанкционированные транзакции в области банковских карт.

Предметом исследования являются модели выявления и предотвращения несанкционированных транзакций, базирующиеся на использовании элементов искусственного интеллекта, методы построения системы, функционирующей на основе данных моделей в режиме мягкого реального времени.

Цель диссертационной работы. Основной целью данной работы является создание моделей выявления и предотвращения несанкционированных транзакций, базирующихся на использовании элементов искусственного интеллекта, исследование и разработка методов построения системы, функционирующей на основе разработанных моделей в режиме мягкого реального времени. Для достижения поставленной цели в рамках данной работы были решены следующие задачи:

1. Сформулирована математическая постановка задач выявления и предотвращения несанкционированных транзакций.

2. Проведены отбор и анализ информативности параметров транзакций.

3. Разработана модель выявления несанкционированных транзакций, базирующаяся на проведении преобразования исходных значений параметров на основе профильной информации.

4. Разработана модель предотвращения несанкционированных транзакций, базирующаяся на использовании исходных значений параметров множества легальных и множества несанкционированных транзакций.

5. Разработана система выявления и предотвращения несанкционированных транзакций, функционирующая на основе предложенных моделей в режиме мягкого реального времени.

6. Проведены реализация и нагрузочное тестирование разработанной системы.

7. Проведено экспериментальное исследование разработанных моделей выявления и предотвращения несанкционированных транзакций.

Методы исследования. При исследовании моделей выявления и предотвращения несанкционированных транзакций в области банковских карт, методов построения системы, функционирующей на основе данных моделей, использовались элементы теории математической статистики, теории нейронных сетей, методов кластеризации, теории информации, теории графов, теории методов оптимизации.

Достоверность полученных теоретических результатов подтверждена результатами экспериментального исследования и практической реализацией разработанной системы выявления и предотвращения несанкционированных транзакций в области банковских карт.

Научная новизна. В рамках данной работы:

1. Сформулирована математическая постановка задач выявления и предотвращения несанкционированных транзакций.

2. Разработан метод снижения мощности множества значений параметров на основе алгоритма k-средних.

3. Разработана модель выявления несанкционированных транзакций, базирующаяся на проведении преобразования исходных значений параметров на основе профильной информации.

4. Разработана модель предотвращения несанкционированных транзакций, базирующаяся на использовании исходных значений параметров множества легальных и множества несанкционированных транзакций.

5. Создана система выявления и предотвращения несанкционированных транзакций, функционирующая на основе разработанных моделей в режиме мягкого реального времени.

Практическая значимость. Разработанная система позволяет свести к минимуму роль человека при решении задач выявления и предотвращения несанкционированных транзакций, так как в данной системе человек отвечает только за рассмотрение жалоб на случаи мошенничества и указание в системе на уже выявленные экземпляры несанкционированных транзакций. Основной практической ценностью данной системы является то, что эта система позволяет оперативно выявлять несанкционированные транзакции, а

в случае использования модели предотвращения несанкционированных транзакций позволяет отклонять авторизацию подозрительных транзакций в режиме мягкого реального времени.

На защиту выносятся следующие основные результаты и положения:

1. Метод снижения мощности множества значений параметров на основе алгоритма k-средних.

2. Модель выявления несанкционированных транзакций, базирующаяся на проведении преобразования исходных значений параметров на основе профильной информации.

3. Модель предотвращения несанкционированных транзакций, базирующаяся на использовании исходных значений параметров множества легальных и множества несанкционированных транзакций.

4. Система выявления и предотвращения несанкционированных транзакций, функционирующая на основе разработанных моделей в режиме мягкого реального времени.

5. Результаты исследования предложенных моделей выявления и предотвращения несанкционированных транзакций.

Реализация результатов работы. Для разработанной системы выявления и предотвращения несанкционированных транзакций «Fraud Adviser» получено авторское свидетельство об официальной регистрации программы для ЭВМ (номер: 2007612001).

Разработанная система выявления и предотвращения несанкционированных транзакций «Fraud Adviser» была внедрена совместно с компанией ООО «Ай Эф Эс Расчетные системы» в ОАО «Акционерный банк Девон-Кредит», что подтверждается актом об использовании результатов диссертации.

Апробация работы. Основные положения и результаты диссертации докладывались и обсуждались на следующих конференциях: «Научная сессия МИФИ»(Москва, 2005, 2008), XVI Международный научно-технический семинар «Современные технологии в задачах управления, автоматики и обработки информации» (Алушта, 2007), Международная молодежная научная конференция XXXIII «Гагаринские чтения» (Москва, 2007), Первая международная конференция «Управление развитием крупномасштабных систем (MLSD 2007)» (Москва, 2007), IASTED International Conference on Artificial Intelligence

and Applications (Innsbruck, Austria, 2008), IEEE SMC UK&RI 7th Conference on Cybernetic Intelligent Systems 2008 (London, 2008)

Публикации. Материалы диссертации опубликованы в 9 печатных работах, из них 7 - в сборниках трудов конференций [A1, A2, A3, A4, A5, A6, A7] и 2 статьи в журнале, включенном ВАК РФ в перечень ведущих рецензируемых научных журналов и изданий [A8, A9].

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, библиографического списка и четырех приложений. Основная часть работы состоит из 150 страниц, включая 24 таблицы, 34 рисунка и перечень использованной литературы из 69 наименований.

Содержание работы

Во Введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе приводится описание банковской карты как средства осуществления финансовых операций. Рассматриваются типы финансовых операций и различные механизмы их осуществления.

В данной главе приводится оценка общемировых потерь от мошенничества с использованием банковских карт и делается вывод о том, что во всем мире наблюдается рост количества случаев мошенничества с использованием банковских карт, несмотря на постоянное совершенствование систем защиты.

В главе рассматриваются современные модели и методы выявления несанкционированных транзакций в области банковских карт, приводятся недостатки и преимущества каждой из рассмотренных моделей или соответствующего метода. В случае использования элементов искусственного интеллекта для выявления несанкционированных транзакций в области банковских карт необходимо найти классификатор, на основе которого и будет определен класс транзакции (несанкционированная или легальная). Для классификации необходимо определить множество классов. Как правило, в задаче выявления несанкционированных транзакций в области банковских карт определяют два класса: класс легальных транзакций и класс несанкционированных (мошеннических) транзакций. Таким образом, транзакция признается подозрительной, если классификатором было определено, что

данная транзакция соответствует классу несанкционированных транзакций. Существует большое количество алгоритмов, которые могут использоваться в качестве классификатора в данной модели. В работе на основе уже проведенных исследований выделяются наиболее эффективные классификаторы для решения задачи выявления несанкционированных транзакций: деревья решений, нейронные сети и сети Байеса. Определить на основе анализа опубликованных исследований классификатор, который лучше всего подходит для решения данной задачи достаточно тяжело, так как результаты исследований могут быть абсолютно разными. Результаты исследований очень сильно зависят от выбора конкретной конфигурации классификатора, признаков, используемых для классификации, методов адаптации классификатора для решения рассматриваемой задачи, методов оценки эффективности и данных, на которых проводилось тестирование.

В главе приводится анализ современных систем выявления несанкционированных транзакций, которые были разработаны ведущими компаниями в данной области. В результате анализа делается вывод, что достаточно тяжело судить об эффективности разработанных систем, так как в большинстве случаев результаты промышленного использования данных систем не приводятся. Необходимо отметить и то, что производители коммерческих систем выявления несанкционированных транзакций по очевидным причинам не раскрывают детали своих разработок.

Во второй главе рассмотрены теоретические основы разработанных моделей выявления и предотвращения несанкционированных транзакций в области банковских карт.

Задачам выявления и предотвращения несанкционированных транзакций соответствуют разные математические постановки. В случае задачи предотвращения несанкционированных транзакций необходимо найти алгоритм a, построенный на обучающей выборке, при использовании которого в среднем на всех контрольных выборках объема K наблюдается максимум критерия:

$$\max_a E(Q'_K(a)) = \max_a E(TP - FP) \tag{1}$$

В данном критерии для определения TP и FP используется характеристика «ROC» («Receiver Operator Characteristic»).

В случае задачи выявления несанкционированных транзакций необходимо найти алгоритм a, построенный на обучающей выборке, при использовании которого на всех контрольных выборках объема K средние значения характеристик TPR и FPR совпадают

со значениями, определенными пользователями:

$$E(TPR) = TPR_{user} \tag{2}$$

$$E(FPR) = FPR_{user} \tag{3}$$

Характеристики TPR и FPR определяются следующим образом:

$$TPR = \frac{TP}{TP + FN} \tag{4}$$

$$FPR = \frac{FP}{FP + TN} \tag{5}$$

Для получения $\max_a Q'_N(a)$ при классификации транзакций из выборки T_K необходимо, чтобы $TPR = 1$ и $FPR = 0$.

Для решения задачи выявления несанкционированных транзакций в работе было предложено рассматривать отдельный класс легальных транзакций для каждой из банковских карт и класс несанкционированных транзакций. Классификация транзакций в данной модели выявления несанкционированных транзакций проводится на основе профильной информации, собранной для легальных транзакций каждой из банковских карты ($Prof_{card}$) и для несанкционированных транзакций ($Prof_{fraud}$). $Prof_{card}$ будем называть совокупность множеств:

$$Prof_{card} = (Prof_{card}(X_1), Prof_{card}(X_2), ..., Prof_{card}(X_k)) \tag{6}$$

Множество $Prof_{card}(X_i)(i = 1, ..., k)$ содержит значения, которые наблюдаются для параметра X_i в легальных транзакциях обучающей выборки, осуществленных с использованием соответствующей банковской карты. Таким же образом на основе всего множества несанкционированных транзакций из обучающей выборки определяется $Prof_{fraud}$.

Считается, что значение параметра $X_i = x$ принадлежит или входит в $Prof_{card}$ ($Prof_{fraud}$), если:

$$X_i = x \begin{cases} \in Prof_{card}(Prof_{fraud}) & , x \in Prof_{card}(X_i)(Prof_{fraud}(X_i)) \\ \notin Prof_{card}(Prof_{fraud}) & , x \notin Prof_{card}(X_i)(Prof_{fraud}(X_i)) \end{cases} \tag{7}$$

В данной модели исходному значению параметра сопоставляется два входных значения. Первое значение определяется на основе $Prof_{card}$:

$$X_i^{card\_profile} = \begin{cases} 1, & X_i = x \in Prof_{card}(X_i) \\ -1, & X_i = x \notin Prof_{card}(X_i) \end{cases} \tag{8}$$

Второе значение $X_i^{fraud\_profile}$ определяется таким же образом на основе $Prof_{fraud}$.

Для определения степени близости классифицируемой транзакции к $Prof_{card}$ и к $Prof_{fraud}$ можно воспользоваться линейной функцией (по аналогии с линейным классификатором):

$$a_{card\_profile} = a(X^{card\_profile} = x^{card\_profile}, w) = \sum_{i=1}^{k} \omega_i \times x_i^{card\_profile} \tag{9}$$

$$a_{fraud\_profile} = a(X^{fraud\_profile} = x^{fraud\_profile}, w) = \sum_{i=1}^{k} \omega_i \times x_i^{fraud\_profile} \tag{10}$$

В данных соотношениях $a_{card\_profile}$ соответствует степени близости классифицируемой транзакции к $Prof_{card}$, $a_{fraud\_profile}$ соответствует степени близости классифицируемой транзакции к $Prof_{fraud}$. $\omega = (\omega_1, \omega_2, ..., \omega_k)$ соответствуют весовым коэффициентам, причем:

$$\sum_{i=1}^{k} \omega_i = 1 \tag{11}$$

Таким образом, получается, что $-1 \leq a(x, w) \leq 1$. Окончательный класс транзакции определяется как (решающее правило):

$$C = \begin{cases} \Omega_{legal} & , if\ (a_{card\_profile} \geq a_{fraud\_profile})\ and\ (a_{fraud\_profile} \leq 0) \\ \Omega_{fraud} & , else \end{cases} \tag{12}$$

В дальнейшем данный классификатор в модели выявления несанкционированных транзакций будем обозначать скоринговым классификатором.

Параметры $X_i (i = 1, ..., k)$ могут принимать достаточно большое количество значений, поэтому для хранения всех значений множеств $Prof_{card}(X_i)(i = 1, ..., k)$ и $Prof_{fraud}(X_i)(i = 1, ..., k)$ необходимо будет использовать большой объем памяти. В главе рассматривается метод сжатия профильной информации, построенный на основе разработанного метода снижения мощности множества значений параметра. Также в данной главе приводится описание адаптации модели сетей Байеса и Байесовского решающего правила для проведения классификации в предложенной модели выявления несанкционированных транзакций, базирующейся на преобразовании исходных значений на основе профильной информации.

Для решения задачи предотвращения несанкционированных транзакций в работе предложено рассматривать класс, соответствующий множеству всех легальных транзакций, и класс, соответствующий множеству всех несанкционированных транзакций. В качестве

классификатора в данной модели используются сети Байеса и Байесовское решающее правило. Все параметры, используемые для проведения классификации в данной модели, принимают дискретные значения. Поэтому в качестве функции распределения значений параметров предложено использовать функцию дискретного распределения.

В случае если параметр принимает слишком большое количество значений, то необходимо применять метод снижения мощности множества значений параметра (СММЗП). Допустим, что для i-го параметра X_i максимально допустимое количество значений - α_i, тогда для снижения мощности множества значений i-го параметра необходимо будет определить α_i кластеров, которые будут содержать все наблюдаемые значения параметра. Каждый кластер определяется как среднее значение e_j и соответствующее максимально допустимое отклонение d_j от e_j для данного кластера. Таким образом, в результате применения метода СММЗП для i-го параметра получается α_i значений $e = e_1, e_2, ..., e_{\alpha_i}$ и соответствующих отклонений $d = d_1, d_2, ..., d_{\alpha_i}$. В результате каждому значению параметра соответствует два значения: входное и исходное. Входное значение параметра определяется как:

$$Value_{in} = cluster\_num, |Value_{initial} - e_{cluster\_num}| \leq d_{cluster\_num} \tag{13}$$

В данном соотношении $Value_{in}$ - входное значение параметра, $Value_{initial}$ - исходное значение параметра, $cluster\_num$ - номер кластера, образовавшегося в результате применения метода СММЗП, которому принадлежит исходное значение $Value_{initial}$ (то есть $|Value_{initial} - e_{cluster\_num}| <= d_{cluster\_num}$). При классификации и обучении используется именно входное представление значений параметров. Для поиска α_i кластеров в работе было предложено адаптировать алгоритм k-средних. Так как мощность множества значений большинства параметров невелика и распределение вероятностей неравномерно, то в алгоритме поиска k-средних для данной модели используются только различные значения параметров.

В связи с тем, что между параметрами может присутствовать зависимость, то для вычисления вероятностей необходимо найти структуру зависимостей между всеми используемыми параметрами. Для поиска данной структуры в работе было предложено воспользоваться характеристикой минимальной длины описания («Minimum Description Length»):

$$\lambda(\alpha) = \min_{m_P}[-\log_2(p(s|m_P)) + K(m_P) : p(s|m_P) > 0, K(m_P) \leq \alpha] \tag{14}$$

Здесь s - это случайная величина, для которой определяется характеристика минимальной длины описания, m_P - модель, которая определяет распределение значений для s, $K(m_P)$

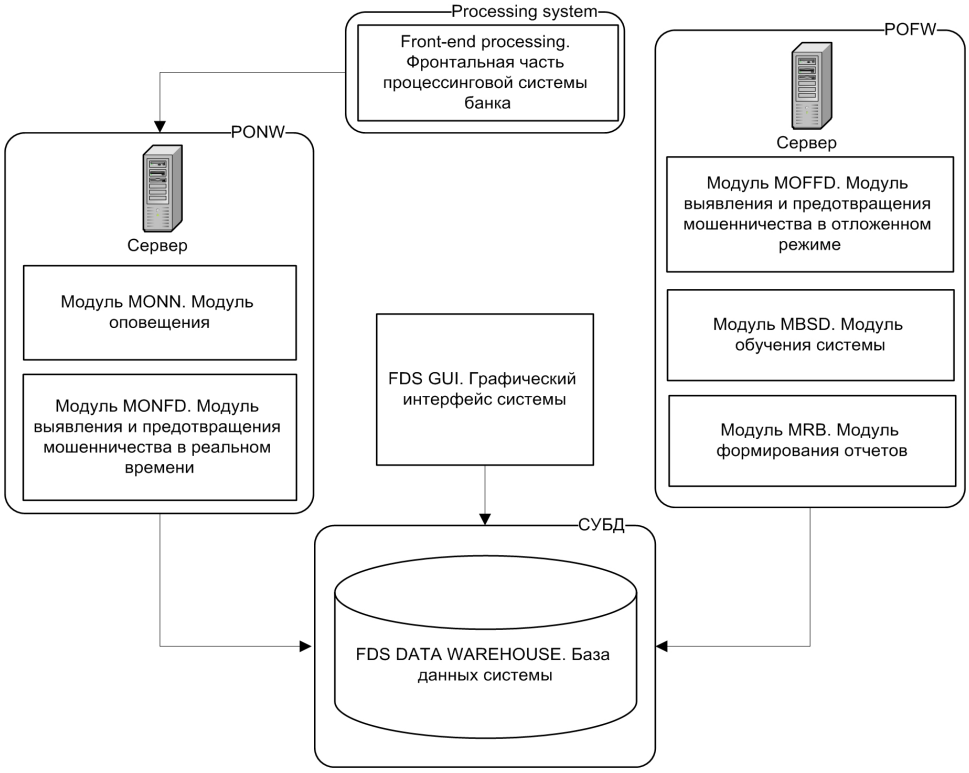


Рис. 1. Архитектура системы выявления и предотвращения несанкционированных транзакций

- это минимальное количество бит, с помощью которого можно описать модель m_P (сложность Колмогорова). В работе приведено описание адаптации данной характеристики для поиска структуры зависимостей между параметрами в сети Байеса с использованием метода ветвей и границ.

В третьей главе приводится описание архитектуры и реализации разработанной системы выявления и предотвращения несанкционированных транзакций в области банковских карт.

Архитектура разработанной системы представлена на рисунке 1. Все модули данной системы распределены между двумя процессами «PONW» и «POFW». Такое распределение необходимо для того, чтобы освободить вычислительные ресурсы платформы, на которой запускаются модули, функционирующие в режиме мягкого реального времени, от функциональности, которая может быть выполнена в отложенном режиме. В процессе «PONW» запускаются модули, которые работают в режиме мягкого реального времени: «MONDF» и «MONN». В модуле «MONFD» в режиме мягкого реального времени запускаются механизмы выявления и предотвращения несанкционированных транзакций. Транзакции поступают в модуль «MONFD» из фронтальной части процессинговой систе-

мы во время их авторизации. При использовании механизмов предотвращения несанкционированных транзакций в случае, если проверяемая транзакция была классифицирована как несанкционированная, то во фронтальную часть процессинговой системы отправляется соответствующее сообщение. При получении подобного сообщения фронтальная часть процессинговой системы отклоняет авторизацию проверяемой транзакции. Если транзакция классифицирована как несанкционированная механизмом выявления или предотвращения несанкционированных транзакций, то владельцу банковской карты может быть отправлено уведомление о проведении подозрительной транзакции (модуль «MONN»).

В процессе «POFW» запускаются модули, которые работают в отложенном режиме: «MOFFD», «MBSD» и «MRB».

Разработанная система позволяет автоматизировать процессы выявления и предотвращения несанкционированных транзакций.

Нагрузочное тестирование разработанной системы показало, что в каждой из реализованных моделей выявления и предотвращения несанкционированных транзакций может быть обработано, как минимум, 1398204 транзакции в день на вычислительной платформе «Pentium 4», работающей на частоте 1,4 МГц с кэш-памятью данных второго уровня 256 Кбайт.

В четвертой главе приводятся результаты экспериментального исследования и промышленного внедрения системы. Для проведения исследований была использована реальная выборка транзакций одного из банков. Данная выборка содержит 5756124 транзакций, которые были зарегистрированы в процессинговой системе одного из банков за 5 месяцев.

Для проведения классификации транзакций в моделях выявления и предотвращения несанкционированных транзакций было отобрано 19 параметров. Результаты исследования информативности 19 отобранных для проведения классификации параметров показали, что, исходя из критерия авто-информативности, можно отказаться от использования двух параметров. Для анализа авто-информативности в работе предложено использовать линейный коэффициент корреляции Пирсона. Проведенный анализ также показал, что все остальные параметры являются информативными, исходя из критерия внешней информативности. Для анализа внешней информативности предложено использовать информацию о распределении значений параметров для каждого из классов и расстояние Кульбака.

В рамках исследования модели выявления несанкционированных транзакций, базирующейся на использовании скорингового классификатора, был проведен анализ эффектив-

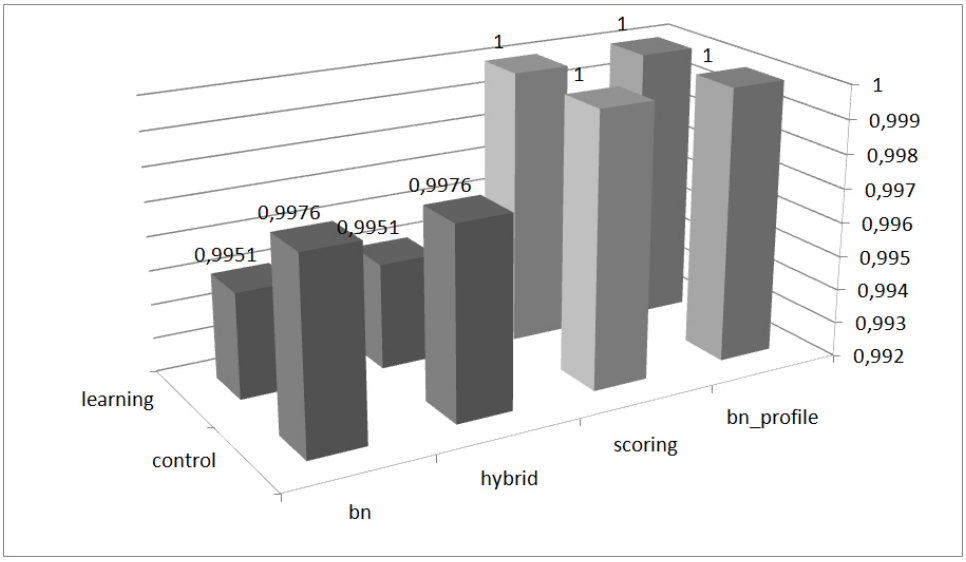


Рис. 2. Средние значения характеристики TPR

ности предложенных правил обновления для поиска весовых коэффициентов ω. Для модели выявления несанкционированных транзакций, базирующейся на использовании сетей Байеса, с помощью метода поиска минимальной длины описания была найдена структура зависимостей между параметрами. Проведено исследование эффективности предложенных классификаторов в модели выявления несанкционированных транзакций на основе разных обучающих и контрольных выборок. Проведенное исследование показало, что точность модели выявления несанкционированных транзакций, базирующейся на использовании скорингового классификатора или сетей Байеса, может изменяться за счет введения дополнительных ограничений в предложенных правилах классификации. Экспериментально были найдены ограничения, при которых предложенные классификаторы в модели выявления несанкционированных транзакций эффективны для решения задачи предотвращения несанкционированных транзакций, исходя из критерия (1).

Исследование показало, что для решения задачи предотвращения несанкционированных транзакций наиболее эффективной, исходя из критерия (1), является гибридная модель. В гибридной модели транзакция признается несанкционированной на основе результатов работы предложенных классификаторов в модели выявления несанкционированных транзакций с решающими правилами, адаптированными для решения задачи предотвращения несанкционированных транзакций, и результатов работы классификатора в модели предотвращения несанкционированных транзакций.

Для получения средних значений характеристик TPR и FPR было проведено отдель-

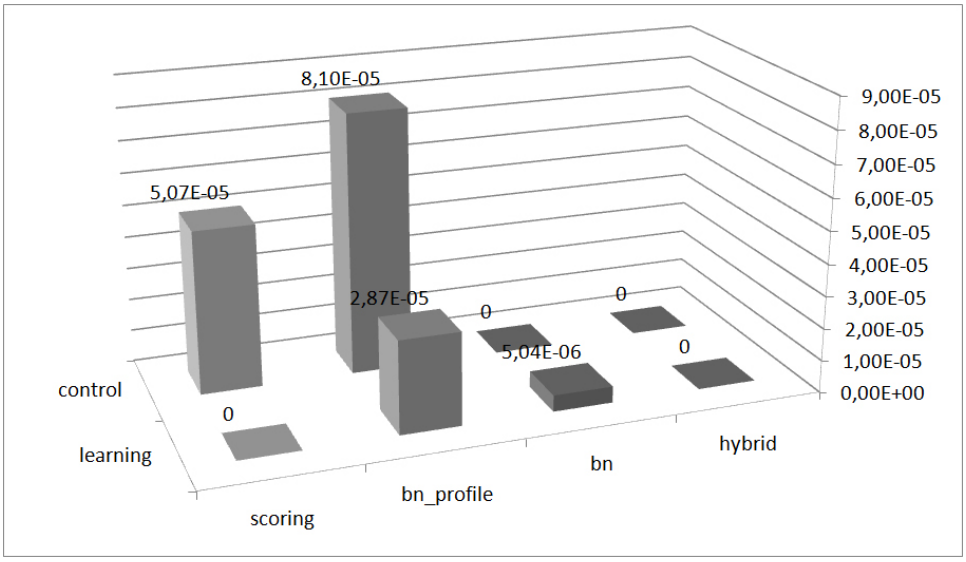


Рис. 3. Средние значения характеристики FPR

ное тестирование разработанных моделей. Для оценки обобщающей способности классификаторов и соответствующих алгоритмов обучения была проведена не только классификация транзакций из контрольных выборок, но и была проведена классификация транзакций из обучающих выборок. Средние значения характеристик TPR и FPR приведены на рисунках 2 и 3. На данных рисунках:

- «scoring» соответствует результатам, которые получены для модели выявления несанкционированных транзакций, базирующейся на использовании скорингового классификатора;
- «bn_profile» соответствует результатам, которые получены для модели выявления несанкционированных транзакций, базирующейся на использовании сетей Байеса;
- «bn» соответствует результатам, которые получены для модели предотвращения несанкционированных транзакций, базирующейся на использовании сетей Байеса и исходных значений параметров;
- «hybrid» соответствует результатам, которые получены для гибридной модели;
- «learning» соответствует результатам классификации транзакций из обучающих выборок;
- «control» соответствует результатам классификации транзакций из контрольных выборок.

В данном тестировании решающие правила классификаторов в модели выявления несанкционированных транзакций были адаптированы для решения задачи предотвращения несанкционированных транзакций. Средние значения характеристик TPR и FPR, полу-

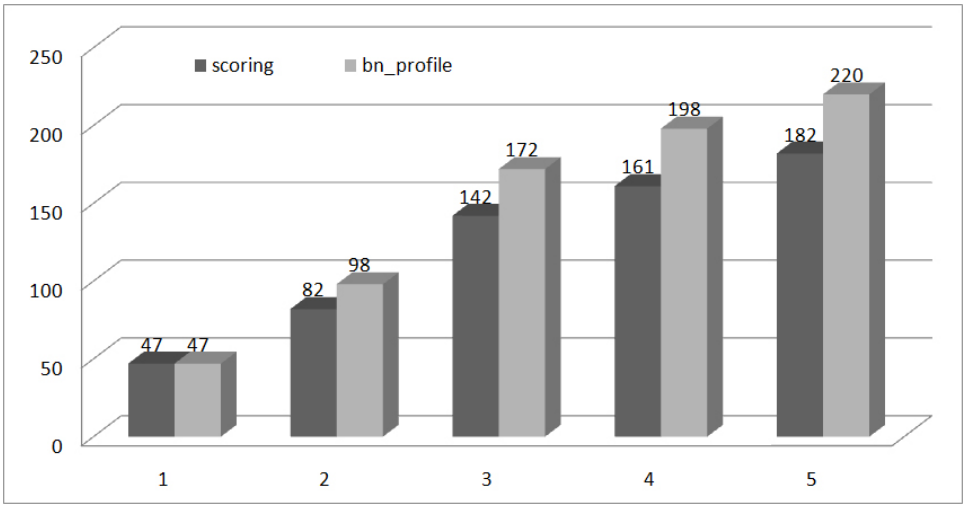


Рис. 4. Количество выявленных подозрительных транзакций за 5 месяцев работы системы

ченные при классификации транзакций из обучающих и контрольных выборок, говорят о том, что все предложенные классификаторы в разработанных моделях обладают обобщающей способностью.

Разработанная система выявления и предотвращения несанкционированных транзакций была внедрена в ОАО «Акционерный банк Девон-Кредит». На первом этапе внедрения пользователями системы было решено использовать только модель выявления несанкционированных транзакций, функционирующую на основе разных классификаторов, в режиме мягкого реального времени. Решающие правила для данных классификаторов были адаптированы для решения задачи предотвращения несанкционированных транзакций. Результаты классификации транзакций с использованием скорингового классификатора и сетей Байеса за 5 месяцев работы системы приведены на рисунке 4.

В заключении необходимо отметить, что банком не была предоставлена информация о реальном количестве несанкционированных транзакций среди выявленных подозрительных транзакций из-за конфиденциальности данной информации.

В Заключении приведены основные результаты диссертации и сформулированы выводы. Итогом диссертационной работы являются следующие научные и практические результаты:

1. Сформулирована математическая постановка задач выявления и предотвращения несанкционированных транзакций.

2. Предложены методы оценки информативности параметров для проведения классификации, исходя из критерия авто - информативности и критерия внешней инфор-

мативности. Проведен отбор параметров транзакций и анализ их информативности.

3. Разработан метод снижения мощности множества значений параметров, базирующийся на использовании алгоритма k-средних.

4. Для решения задачи выявления несанкционированных транзакций введены понятия профиль легальных транзакций для каждой из банковских карт и интегральный профиль несанкционированных транзакций, которые используются для построения скорингового классификатора и классификатора на основе сетей Байеса.

5. Для решения задачи предотвращения несанкционированных транзакций рассматриваются множества всех легальных и несанкционированных транзакций. Классификация в данной модели проводится на основе исходных значений параметров с использованием сетей Байеса.

6. Разработана архитектура системы выявления и предотвращения несанкционированных транзакций, которая позволяет проводить выявление и предотвращение несанкционированных транзакций в режиме мягкого реального времени. Данная система допускает параллельное выполнение процесса проверки транзакций, функционирующего в режиме мягкого реального времени, и процесса обучения системы.

7. Проведены реализация и нагрузочное тестирование разработанной системы.

8. Проведено экспериментальное исследование, подтверждающее эффективность разработанных моделей выявления и предотвращения несанкционированных транзакций.

9. Разработанная система выявления и предотвращения несанкционированных транзакций была внедрена в ОАО «Акционерный банк Девон-Кредит».

Список публикаций

[A1] *Л.Е.Муханов.* Система обнаружения мошенничества // Научная сессия МИФИ-2005.Сборник научных трудов. — МИФИ, 2005. — С. 81.

[A2] *Л.Е.Муханов.* Применение сетей Байеса для обнаружения мошенничества с платежными картами // XXXIV Гагаринские чтения. Научные труды Международной молодежной научной конференции в 8 томах. — МАТИ, 2007. — С. 243 –244.

[A3] *Л.Е.Муханов.* Сравнение различных моделей обнаружения мошенничества в сфере пластиковых карт // Труды XVI международного научно-технического семинара «Современные технологии в задачах управления, автоматики и обработки информации". — ТулГУ, 2007. — С. 81.

[A4] *Л.Е.Муханов, Б.А. Щукин.* Методы представления входных значений сети Байеса для обнаружения мошенничества // Научная сессия МИФИ-2008.Сборник научных трудов. — МИФИ, 2008. — С. 81 –82.

[A5] *В.А. Филиппов, Б.А. Щукин, Л.Е.Муханов.* Мониторинг банковской системы с использованием простого классификатора Байеса // Труды первой международной конференции «Управление развитием крупномасштабных систем (MLSD 2007)". — ИПУ им. В.А.Трапезникова РАН, 2007. — С. 318–323.

[A6] *L.E. Mukhanov.* Using Bayesian Belief Networks for Credit Card Fraud Detection // Proceedings of the IASTED International Conference on Artificial Intelligence and Applications. — Canada: ACTA Press, 2008. — Pp. 221–225.

[A7] *V. Filippov, L. Mukhanov, B.Shchukin.* Credit card fraud detection system // Proceedings of the 7th IEEE Conference on Cybernetic Intelligent Systems 2008. — IEEE Press, 2008. — Pp. 73–79.

[A8] *Л.Е. Муханов.* Адаптация модели сетей Байеса для обнаружения мошенничества с платежными картами // *Информационные технологии.* — 2008. — № 2. — С. 74–78.

[A9] *Л.Е. Муханов.* Система обнаружения мошенничества в области платежных карт // *Информационные технологии.* — 2008. — № 5. — С. 62–66.