УДК 62-50

Бидюк П.И., Катеринич С.А.

ИСПОЛЬЗОВАНИЕ БАЙЕСОВСКОЙ СЕТИ ДЛЯ РЕШЕНИЯ ЗАДАЧ МОНИТОРИНГА В ТЕХНИЧЕСКИХ СИСТЕМАХ

Введение

Понятие мониторинга семантически означает осуществление непрерывного наблюдения за неким объектом. Наблюдение в свою очередь подразумевает отслеживание и фиксирование некоторых параметров (состояний) объекта. Однако в современном мире интеллектуальных технологий и автоматизации наблюдение как таковое все реже и реже встречается в виде реализации обособленного процесса. Автоматизация дала возможность использовать мониторинг в качестве инструмента систем поддержки и принятия решений (СППР) [1]. Таким образом, интеллектуализация мониторинга трансформировала его из пассивного наблюдения в процесс интерактивного взаимодействия с оператором и объектом наблюдения.

Тогда понятие мониторинга (автоматизированного) можно определить как систему организационно-технических мер и процедур, направленных на решение задач непрерывного наблюдения за состоянием (поведением) некоторой системы, анализа и классификации состояний системы и принятия некоторого решения по результатам классификации.

Если рассматривать мониторинг как систему наблюдения с последующим анализом и выработкой некоторого решения, то использование данного элемента в автоматизированных системах можно расценивать как внедрение инструмента контроля [2]. В зависимости от конкретного предназначения технической системы (ТС), объектом контроля, соответственно, может являться:

1) либо сама система, т.е. оператора интересует текущее поведение системы, при котором, например, состояние системы не должно выходить за некоторые допустимые рамки;
2) либо внешний процесс, за поддержку которого ответственна данная ТС. При этом она может являться неотъемлемой составляющей данного процесса (например, системы

 ISSN 1562-9945

процессинга операций по платежным карточкам) либо надстройкой, выполняющей функции аккумулирования и обработки данных о процессе (например, ПО поддержки торговых операций на биржах). Однако и надстройка, и составляющий элемент несет в себе информацию о процессе, что по сути определят их как отражение данного процесса либо части процесса, в рамках которого имеется интерес осуществлять мониторинг.

Таким образом, техническая система либо как таковая, либо как отражение процесса является объектом мониторинга. Поэтому имплементация в систему процесса мониторинга по сути является организацией автоматизированного самоконтроля системы. Безусловно, такой механизм самоконтроля может и должен включаться в систему общего контроля функционирования ТС и взаимодействовать с соответствующими экспертами, вовлеченными в систему общего контроля [2].

Необходимость решения задачи мониторинга процессов обусловлена объективными причинами, которые определяются присутствием в любой системе (1) фактора риска непредвиденных ситуаций и (2) необходимости своевременного принятия решений.

Фактор риска непредвиденных ситуаций непосредственно связан с различными аспектами сложности. Теоретический аспект включает в себя сложность системы и предметной области, в которой функционирует данная система, на этапе проектирования и разработки данной системы. Практический аспект сложности связан с особенностями практической реализации системы. Одновременно эти же составляющие делают крайне затруднительной работу экспертов, ответственных за сопровождение данной системы, из-за больших объемов анализируемой информации. Это в свою очередь определяет необходимость автоматизации процесса мониторинга.

Необходимость своевременного принятия решений является ключевой в вопросе о разработке системы вообще, т.к. именно в этом и заключается цель большинства СППР. В результате интегрирования мониторинга в функциональность системы наблюдается увеличение уровня сложности данной системы. Таким образом, сложность системы рождает необходимость организации мониторинга как элемента данной системы, а мониторинг в свою

очередь требует расширения спектра автоматически принимаемых решений, закладываемых в данную систему. В итоге получаем замкнутую цепь взаимосвязей между такими характеристиками и элементами системы, как сложность системы, спектр автоматически принимаемых решений и функция самоконтроля системы. Разрастание каждой из этих элементов стимулирует рост двух других. Так перед проектировщиком встает задача разработки наиболее оптимального проекта системы с позиции затрат на реализацию, поддержку и функционирование системы. Таким образом, внедрение мониторинга как элемента самоконтроля системы требует дополнительного анализа всего проекта с позиции системного подхода.

Постановка задачи мониторинга операций по платежным карточкам

При автоматизации процесса мониторинга наиболее часто используются экспертные знания о предметной области, которые сводятся к набору правил анализа ситуации и принятия решений. Поскольку фактор риска связан с различными видами сложности [2], а соответственно и неопределенности, то для анализа риска удобно использовать вероятностные инструменты, одним из которых являются байесовские нейронные сети (БНС).

В частности, для мониторинга мошеннических операций [3,4,5,6] с платежными карточками реализация системы на основе моделирования с помощью БНС расширяет возможности анализа рисков мошенничества.

Для начала определим понятие риска в данной предметной области. Под мошеннической операцией понимают любую операцию по платежной карточке, осуществленную мошенниками с целью нанесения ущерба держателю данной карточки либо банку-эмитенту, либо торговой точке, в которой был приобретен товар/услуги в результате данной операции. Неопределенность относительно того, является ли данная операция мошеннической либо правомерной, определяет риск мошеннических операций. В зависимости от вида мошенничества данный риск может описываться различными сочетаниями вероятности мошенничества и ущерба.

Для каждого банка наиболее актуальной является задача определения статуса операции по карточкам его клиентов (операции по эмиссии), особенно категории VIP. Это определяется

 ISSN 1562-9945

особенностями данных операций по сравнению с операциями по эквайрингу, т.е. операциями по карточкам в торговых точках, которые обслуживаются данным банком. В случае мошенничества по эвайрингу ответственность за данные операции достаточно легко перекладывается на торговую точку, при этом потери банка являются незначительными в большинстве случаев. В то же время ответственность за компенсацию ущерба от операций по эмиссии обычно возлагается либо на картодержателя (а значит, у банка возникают проблемы, как заставить клиента выплатить данную компенсацию) либо делится между картодержателем и банком.

Ущерб от мошеннических операций определяется суммами данных операций и затратами на расследование и ведение работ по опротестованию данных операций.

Как показывает опыт работы по противодействию мошенничеству, у большинства картодержателей вырабатывается своего рода паттерны использования платежных карточек. Т.е. в зависимости от личного опыта обращения с карточками у клиентов появляется склонность к осуществлению тех или иных видов операций, на те или иные суммы, в то или иное время суток и т.д. Следовательно, между конкретными значениями таких параметров операции, как сумма, время, вид товара, количество операций в день и др., устанавливаются вероятностные взаимосвязи, отличные от случайного распределения вероятностей. При этом мошеннические операции также имеют свой «рисунок» взаимосвязей. Как результат, данные взаимосвязи могут быть объектом моделирования с помощью вероятностных инструментов.

Таким образом, главную задачу системы мониторинга на основе поведенческих характеристик можно сформулировать следующим образом.

Пусть получен авторизационный запрос, содержащий n полей, инициированных в соответствии с характером текущей операции:

$\overline{\mathbf{X}} = \{X_1 = \mathbf{X}_1; ...; X_n = \mathbf{X}_n\}$ – конкретная инициализация текущим наблюдением набора полей (переменных) авторизационного запроса;

X_i – i-ое поле авторизационного запроса;

$\mathbf{X}_i$ – конкретное значение, которое присваивается полю X_i в текущем авторизационном запросе.

Пусть за определенный период была накоплена база данных D, в которой каждому авторизационному запросу поставлено в соответствие значение 0 или 1 в зависимости от того, была ли операция санкционированной или мошеннической:

$$D : \overline{\mathbf{X}} \to Fraud \in \{0;1\}.$$

Необходимо оценить вероятность конкретного вида мошенничества по факту получения авторизационного запроса на проведение операции с платежной карточкой либо оценить вероятность того, что данная операция характерна для картодержателя:

$$P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}}).$$

Как и в большинстве технических систем, каждое наблюдение базы данных D описывается определенным набором параметров (в данном случае – полей авторизационного запроса). При этом все из них имеют конкретные значения, т.е. нет пропущенных данных. В таких условиях, применяя вероятностный вывод в БНС, можно вычислить вероятность получения данной операции. При установлении порога доверия достаточно легко реализовать отбор подозрительных операций.

Одним из достоинств системы на основе БНС является возможность получения графического изображения модели причинно-следственных связей между параметрами операций, т.е. «рисунка» взаимосвязей. Данная графическая интерпретация результатов моделирования позволяет эксперту проводить анализ процесса использования платежных карт. При разбиении карточек на группы, обучение БНС на операциях конкретной группы дает на выходе модель поведенческих характеристик картодержателей данной группы. При этом система автоматически выявляет зависимости, существенные с точки зрения вероятностей, описываемых накопленной базой операций. На эксперта возлагается задача логического описания выявленных взаимосвязей с использование информации о психологическом портрете данной группы.

Совместная реализация в системе методов обучения и адаптации БНС позволяет повысить эффективность применения данного инструмента моделирования.

 ISSN 1562-9945

Применение вероятностного вывода для задачи мониторинга

Рассмотрим пример реализации мониторинга мошеннических операций с помощью байесовской нейронной сети. В качестве предметной области будет выступать система оборота платежных карточек. Организация работы по предотвращению мошеннических операций по платежным карточкам является обязательным требованием международных платежных систем, контролирующих карточное обращение (в частности, Visa International [3, 4, 5] и MasterCard International [6]). Поэтому функционирование процессинговых центров банков требует от членов платежных систем внедрения on-line мониторинга операций по платежным карточкам. В процессинговый центр поступают авторизационные запросы на проведение той или иной операции по карточке. Каждый запрос имеет строго определенную структуру, включающую ряд полей, содержащих информацию о данной транзакции.

Пусть система мониторинга в результате первичной обработки каждого очередного запроса накапливает собственную базу наблюдений. Каждое наблюдение содержит n полей. Предположим, что поле с номером n отвечает за характеристику, является ли данная операция мошеннической или нет, т.е. переменная, соответствующая данному полю, относится к булевому типу:

$$X_n \equiv Fraud \ .$$

Поставим в соответствие каждому полю дискретную переменную X_i, при этом будем полагать, что предварительная обработка запросов реализует дискретизацию для полей с непрерывными значениями, например, сумма операции.

$\mathbf{X}_i$ – конкретное значение, которое присваивается переменной X_i в конкретном наблюдении.

$\overline{\mathbf{X}} = \{X_1 = \mathbf{X}_1; ...; X_{n-1} = \mathbf{X}_{n-1}\}$ – конкретная инициализация текущим наблюдением набора переменных.

Пусть система мониторинга обучила байесовскую нейронную сеть на основе накопленной базы наблюдений. При получении очередного авторизационного запроса перед системой ставится задача определить вероятность того, что данная операция является мошеннической. В математической форме данная задача формулируется как необходимость вычисления вероятности того, что переменная $Fraud$

принимает значение 1 при условии, что остальные переменные $\overline{X}$ проинициализированы набором значений $\overline{\mathbf{X}}$:

$$P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}}).$$

Запишем данной выражение с помощью формулы условной вероятности:

$$P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}}) \cdot P(\overline{X} = \overline{\mathbf{X}}) = P(Fraud = 1; \overline{X} = \overline{\mathbf{X}})$$

$$P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}}) = \frac{P(Fraud = 1; \overline{X} = \overline{\mathbf{X}})}{P(\overline{X} = \overline{\mathbf{X}})}$$

Введем переменную I, обозначающую набор индексов переменных X_i, в множество узлов-предков $pa(X_i)$ которых входит узел $Fraud$:

$$I = \{i : Fraud \in pa(X_i)\},\ i \in \{1;...;n\}.$$

Далее будем использовать свойство байесовской нейронной сети касательно декомпозиции совместного распределения вероятностей: совместная вероятность равна произведению условных вероятностей по каждому узлу, при этом условная вероятность для отдельного узла обусловливается только набором узлов-предков данного узла.

$$P(X_1,...,X_n) = \prod_{i=1}^{n} P(X_i \mid pa(X_i)).$$

Тогда получаем следующее:

$$P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}}) =$$

$$= \frac{\prod_{i \in I} P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i))\Big|_{Fraud=1} \times \prod_{i \notin I} P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i))\Big|_{Fraud=1}}{\prod_{i \in I} P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i)) \times \prod_{\substack{i \notin I \\ i \neq n}} P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i))}$$

Как видно, второе произведение числителя отличается от второго произведения знаменателя только индексом $i \neq n$, что позволяет их сократить, оставив в числителе только элемент произведения для $i = n$, т.е. для узла $Fraud$:

$$P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}}) =$$

$$= \frac{\prod_{i \in I} P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i))\Big|_{Fraud=1} \times P(Fraud = 1 \mid pa(Fraud) = \mathbf{pa}(Fraud))}{\prod_{i \in I} P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i))}.$$

 ISSN 1562-9945

В полученном выражении знаменатель содержит произведение элементов, каждый из которых содержит уловную вероятность от инициализации узлов-предков. При этом в набор узлов-предков входит переменная $Fraud$, не инициализированная для знаменателя. Однако события $\{Fraud = 1\}$ и $\{Fraud = 0\}$ являются непересекающимися и образуют полную группу событий. Поэтому можно привести последнее выражения к следующему виду:

$$P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}}) =$$

$$= \frac{\prod_{i \in I} P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i))\Big|_{Fraud=1} \times P(Fraud = 1 \mid pa(Fraud) = \mathbf{pa}(Fraud))}{\prod_{i \in I} \left\{ \sum_{k=\{0;1\}} P(Fraud = k \mid pa(Fraud) = \mathbf{pa}(Fraud)) \cdot P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i))\Big|_{Fraud=k} \right\}}.$$

Данная формула является конечной для вычисления вероятности мошенничества по конкретной операции. При формальном подходе, превышение 50-процентного порога свидетельствует о возможном мошенническом характере текущей операции. Однако с учетом того, что база данных может быть не достаточно презентативной в силу отсутствия всех возможных вариантов наблюдении в количестве, адекватно отражающем реальное распределение, данный порог может смещаться в сторону увеличения как поправка на неполноту информации.

Анализ формулы вероятностного вывода для задачи мониторинга

Рассмотрим формулу вероятностного вывода для задачи мониторинга более детально. В общем случае, можно выделить три группы узлов сети, включенных в данную формулу.

Как видно из структуры индексов операторов произведения числителя и знаменателя, непосредственное влияние на значение $P(Fraud = 1 \mid \overline{X} = \overline{\mathbf{X}})$ оказывают узлы сети, включенные в набор индексов I. По определению, это те узлы, в множество узлов-предков которых входит узел $Fraud$. То есть узлы, непосредственно зависимые от узла $Fraud$. Это первая группа.

Рассматривая условные части условных вероятностей числителя и знаменателя, можно заключить, что в вычисления включены узлы-предки $pa(X_i)$ тех узлов X_i, которые являются непосредственными наследниками узла $Fraud$. Это вторая группа.

И, наконец, в третью группу включены узлы, которые являются непосредственными предками узла $Fraud$, что следует из условной части условной вероятности $P(Fraud = 1 \mid pa(Fraud) = \mathbf{pa}(Fraud))$.

В отличие от общего случая, логика узла $Fraud$ такова, что данный узел является определяющим относительно характера операции с платежной карточкой. То есть данный узел является корневым и, как результат, не имеет непосредственных узлов-предков. Тогда определяющими становятся узлы первой и второй группы.

Ниже приведен конкретный пример [7], в котором моделирование осуществлялось на следующем наборе параметров операций.

Таблица №1

Перечень и описание полей базы данных, поставленных в соответствие параметрам операций с платежными карточками

Название поля базы данных	Количество возможных значений переменной, соответствующей данному полю	Логический смысл значения данного поля
FRAUD	2 возможные значения	Определяет, является ли данная операция мошеннической.
DAYSBEFO	8 возможных значений	Определяет количество дней между данной операцией и предыдущей.
ACCNT_AMT	6 возможных интервалов сумм	Определяет сумму текущей операции.
SPENT_AM	6 возможных интервалов сумм	Определяет общую сумму всех операций за текущий день.
TRAN_CCY	5 возможных значений	Определяет код валюты, в которой совершена текущая операция.
MCCCLASS	10 возможных значений	Определяет код вида деятельности торговой точки, в которой осуществлена текущая операция (т.е. то, какой товар/услугу предоставляет данный предприниматель).
CITY	10 возможных значений	Определяет город, в котором совершена данная операция.
COUNTRY	4 возможные значения	Определяет страну, в которой совершена данная операция.

Ниже приведена графическая интерпретация результатов моделирования на вышеуказанном наборе переменных [7].

 ISSN 1562-9945

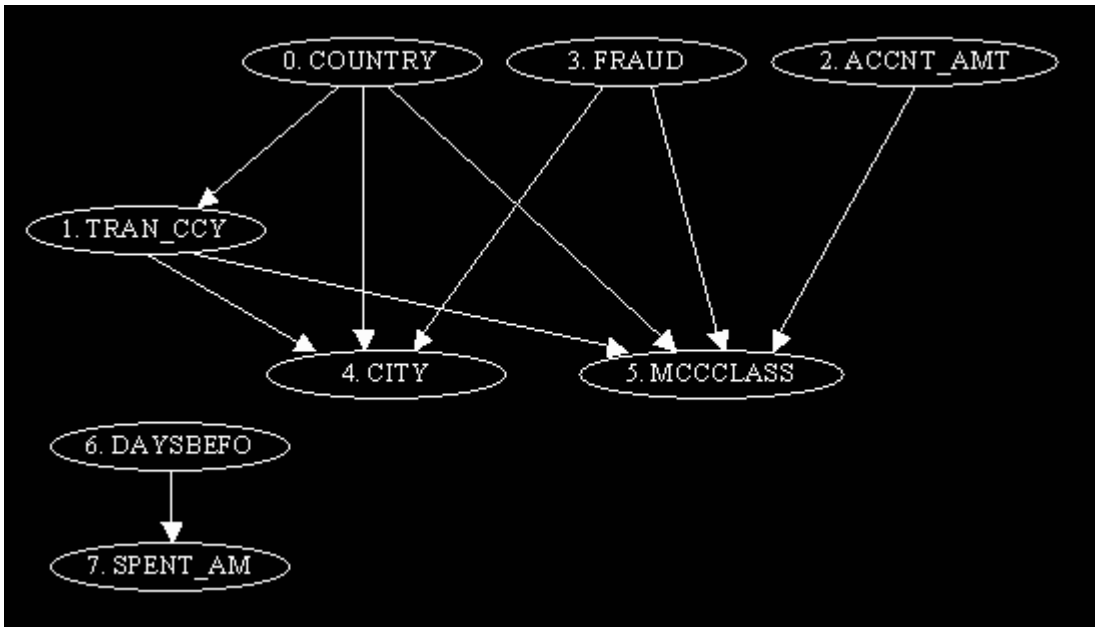

Рисунок 1 - Графическая интерпретация структуры сети

Как видно из рис.1, формула вероятностного вывода будет включать только первую и вторую группы узлов.

Первая группа включает 2 узла: CITY и MCCCLASS.

Вторая группа состоит из 4 узлов: TRAN_CCY, COUNTRY, FRAUD, ACCNT_AMT.

При этом видно, что вторая группа определяется узлами, входящими в состав первой группы. Поэтому в данном случае формула вероятностного вывода имеет достаточно простой вид:

$$I = \{CITY; MCCCLASS\}$$

$$pa(CITY) = \{TRAN\_CYY = н_1; COUNTRY = н_0; FRAUD = 1\}$$

$$pa(MCCCLASS) = \{TRAN\_CYY = н_1; COUNTRY = н_0; FRAUD = 1; ACCNT\_AMT = н_2\}$$

$н_i$ – значение i-ого поля для текущей операции. При этом значение для узла *Fraud* переопределяется в знаменателе в зависимости от индекса суммирования.

$$P(Fraud = 1 \mid \bar{X} = \bar{\mathbf{X}}) =$$

$$= \frac{P(CITY = н_4 \mid pa(CITY)) \times P(MCCCLASS = н_5 \mid pa(MCCCLASS)) \times P(Fraud = 1)}{\prod_{i \in I} \left\{ \sum_{k=\{0;1\}} P(Fraud = k) \cdot P(X_i = \mathbf{X}_i \mid pa(X_i) = \mathbf{pa}(X_i)) \Big|_{Fraud=k} \right\}}.$$

Понятно, что данный подход является приемлемым для случая, когда БНС построена по базе наблюдений, которая представляет оба класса операций: как санкционированные, так и мошеннические.

Однако обучение БНС в условиях отсутствия мошеннических операций гарантирует в результате получение такой модели, в которой узел *Fraud* не будет связан с другими узлами. Подобную ситуацию достаточно просто встретить на начальном этапе сбора наблюдений, когда база данных еще начинает сформировываться. Тогда сам инструмент БНС утрачивает смысл классификатора как такового, т.к. настройка БНС ведется только на класс санкционированных операций. Следовательно, формулировка задачи мониторинга в терминах условной вероятности не имеет практического значения.

Тогда в качестве возможного варианта можно рассматривать следующие подход, при котором используется БНС, обученная по базе наблюдений санкционированных операций. Для текущей структуры БНС выбираются характерные представители санкционированных операций. Из них может выбираться представитель, наиболее схожий с текущей операцией, которую нужно оценить. Выдвигаются 2 гипотезы. Первая – о том, что в последний момент пришла операция, подлежащая оценке. Вторая – о том, что в последний момент пришла операция, аналогичная характерному представителю санкционированных операций. Соответственно каждой гипотезе, виртуально формируются 2 БНС как результат адаптации вероятностной составляющей текущей БНС к одной и другой гипотезе. После этого вычисляется значение функционала качества К2 для обеих БНС и сравнивается его «отрицательный» прирост относительно значение функционала качества К2 для БНС, имеющейся на текущий момент (с увеличением наблюдений в базе значение функционала уменьшается). Как показывает эксперимент, абсолютный прирост в случае характерных операций в среднем в 2 раза меньше, чем прирост при нехарактерных операциях.

Выводы

Таким образом, внедрение систем мониторинга является объективно обусловленной необходимостью, и реализация данных систем на основе байесовских нейронных сетей способна решить основные задачи мониторинга такие, как наблюдение, анализ, классификация и принятие решения.

 ISSN 1562-9945

Использование алгоритмов обучения и адаптации позволяет повысить эффективность данной реализации. Вероятностный вывод обеспечивает решение задачи классификации и дает базу для дальнейшего принятие решений. Графическая интерпретация позволяет экспертам контролировать функционирование системы мониторинга и предоставляет агрегированную информацию для более специфического анализа.

Подобные системы могут использоваться в качестве реализации как post-action подхода (анализ и обработка производятся после происшедшего события), так и pro-action (блокирование нежелательных операций по результату предварительного анализа).

Безусловно, данные системы ни чуть не умаляют роли экспертов в системе общего контроля. Подобная автоматизация имеет свей целью повышение эффективности работы экспертов и напрямую зависит от их знаний, хотя и в меньшей степени, чем системы других видов.

В дальнейшем планируется уточнение процедуры вероятностного вывода и практическое внедрение в сфере банковского бизнеса.

Литература

1. Heckerman D. A tutorial on learning Bayesian networks. Technical report MSN-TR-95-06. – Microsoft Research, Advanced Technology Division. – 1995. – 52 p.
2. Антонов А.В. Системный анализ. Учебник для ВУЗов. – М.: Высш. Школа, 2004. – 454 с.
3. Visa International Operation Regulations. Volume I – General Rules. – San Francisco: Visa International Inc., USA. – 2002. – 692 p.
4. Visa Regional Operation Regulations. Visa CEMEA. – San Francisco: Visa International Inc., USA. – 2002. – 212 p.
5. Issuer Fraud Management Best Practices. – San Francisco: Visa International Inc., USA. – 2000. – 189 p.
6. MasterCard Bylaws and Rules. – Waterloo: MasterCard International Inc., Belgium. – 1999. – 295 p.
7. Метод адаптації байєсівської нейронної мережі на основі алгоритму К2 / Бідюк П.І., Катеринич С.А. // Наукові вісті „КПІ”. – 2006. – № 4. – С. 98–106.

Получено 20.11.2006 г.